Quantum Position Verification: Loss-tolerant Protocols and Fundamental Limits

P.H. Verduyn Lunel

Quantum Position Verification: Loss-tolerant Protocols and Fundamental Limits

Philip Hein Verduyn Lunel

Quantum Position Verification:

Loss-tolerant Protocols and Fundamental Limits

Philip Hein Verduyn Lunel

Quantum Position Verification:

Loss-tolerant Protocols and Fundamental Limits

ILLC Dissertation Series DS-2024-08

INSTITUTE FOR LOGIC, LANGUAGE AND COMPUTATION

For further information about ILLC-publications, please contact

Institute for Logic, Language and Computation
Universiteit van Amsterdam
Science Park 107
1098 XG Amsterdam
phone: +31-20-525 6051
e-mail: illc@uva.nl
homepage: http://www.illc.uva.nl/

The investigations were supported by the Dutch Research Council (NWO) through the Gravitation-grant NETWORKS-024.002.003.

Printed and bound by Ipskamp Printing.

ISBN: 978-94-6473-561-1

Quantum Position Verification: Loss-tolerant Protocols and Fundamental Limits

ACADEMISCH PROEFSCHRIFT

ter verkrijging van de graad van doctor
aan de Universiteit van Amsterdam
op gezag van de Rector Magnificus
prof. dr. ir. P.P.C.C. Verbeek
ten overstaan van een door het College voor Promoties ingestelde commissie,
in het openbaar te verdedigen in de Agnietenkapel
op vrijdag 4 oktober 2024, te 10.00 uur

door Philip Hein Verduyn Lunel
geboren te Amsterdam

Promotiecommissie

Promotores:	prof. dr. H.M. Buhrman	Universiteit van Amsterdam
	dr. F. Speelman	Universiteit van Amsterdam
Overige leden:	prof. dr. R.M. de Wolf	Universiteit van Amsterdam
	prof. dr. C. Schaffner	Universiteit van Amsterdam
	prof. dr. A.P.A. Kent	University of Cambridge
	dr. M. Ozols	Universiteit van Amsterdam
	dr. W. Löffler	Universiteit Leiden

Faculteit der Natuurwetenschappen, Wiskunde en Informatica

The results in this thesis are based on the following articles. For all articles, the authors are ordered alphabetically and co-authorship is shared equally.

1. [ABSV22b] Rene Allerstorfer, Harry Buhrman, Florian Speelman, and Philip Verduyn Lunel. Towards practical and error-robust quantum position verification. *arXiv preprint arXiv:2106.12911*, 2022.

2. [ABSV22a] Rene Allerstorfer, Harry Buhrman, Florian Speelman, and Philip Verduyn Lunel. On the role of quantum communication and loss in attacks on quantum position verification. *arXiv preprint arXiv:2208.04341*, 2022.

3. [ACG$^+$23] Rene Allerstorfer, Matthias Christandl, Dmitry Grinko, Ion Nechita, Maris Ozols, Denis Rochette, and Philip Verduyn Lunel. Monogamy of highly symmetric states. *arXiv preprint arXiv:2309.16655*, 2023
Presented at QIP 2024

4. [ABB$^+$23] Rene Allerstorfer, Andreas Bluhm, Harry Buhrman, Matthias Christandl, Llorenç Escolà-Farràs, Florian Speelman, and Philip Verduyn Lunel. Making existing quantum position verification protocols secure against arbitrary transmission loss. *arXiv preprint arXiv:2312.12614*, 2023
Presented at QIP 2024, QCrypt 2024

5. [ABM$^+$23] Rene Allerstorfer, Harry Buhrman, Alex May, Florian Speelman, and Philip Verduyn Lunel. Relating non-local quantum computation to information theoretic cryptography. *Quantum*, 8:1387, 2024
Presented at QIP 2024, QCrypt 2024

The author has additionally co-authored the following articles that are not included in this thesis.

1. [GAVC23] Ian George, Rene Allerstorfer, Philip Verduyn Lunel, and Eric Chitambar. Time-Constrained Local Quantum State Discrimination. *arXiv preprint arXiv:2311.00677*, 2023

2. [AER$^+$23] Rene Allerstorfer, Llorenç Escolà-Farràs, Arpan Akash Ray, Boris Škorić, Florian Speelman, and Philip Verduyn Lunel. Security of a Continuous-Variable based Quantum Position Verification Protocol. *arXiv preprint arXiv:2308.04166*, 2023

3. [BGVW24] Harry Buhrman, Dmitry Grinko, Philip Verduyn Lunel, and Jordi Weggemans. Permutation tests for quantum state identity. *arXiv preprint arXiv:2405.09626*, 2024
Presented at TQC 2024

Contents

Chapter 1

Introduction

1.1 Introduction

The fundamental idea of quantum cryptography is to use a generalization of the Heisenberg uncertainty principle to our advantage in building cryptography schemes that are based on the most fundamental level of physics. To explain how we leverage the principles of quantum mechanics with the development of cryptographic schemes, we start with a brief history of quantum mechanics.

One of the greatest scientific advances in recent history has been in the field of quantum mechanics. Before the early 1900s, the field of physics was based on *classical* mechanics. Classical mechanics allowed us to understand and predict physical phenomena at a *macroscopic* level. Physical models were deterministic and continuous, such as Maxwell's equations for electric and magnetic fields. It was in 1900, when Max Planck introduced the theory of the quantization of energy, that quantum theory was born. Einstein further built upon this and used Planck's theory to explain the photoelectric effect.

A problem that remained open for all this time was the wave-particle duality concept. In the 17th century, Newton's belief was that light was a particle, while Huygens believed that light was a wave. The interference experiments by Thomas Young in 1801 validated that light was in fact a wave, and for the rest of the 19th century this was the common belief. However, Planck's quantization idea, combined with Einstein's explanation of the photoelectric effect, suggested that light also had particle-like properties. By then, it was understood that light could sometimes behave as a wave and sometimes as a particle. In 1924 Louis de Broglie proposed that this also goes the other way: particles, like electrons or protons, could also be seen as waves. Building on de Broglie's wave-particle duality proposal, Erwin Schrödinger developed the wave equation for electron motion, known as the *Schrödinger equation.*

The description of elementary particles as waves is counterintuitive to how people previously thought about particles. Intuitively, people often see, and draw, particles as some sort of very small dot, fully localized at a certain position. This is actually not correct. In general, the position of a particle is not precisely defined; instead, there is only a probability that a particle is in a certain location. A particle is represented as an amplitude wave throughout the space. It is only when we measure the position of a particle that it becomes localized to a specific position in space, where the probabilities of measuring a particle in a certain location correspond to the norm of the amplitude.

A direct consequence of the particle-wave duality is Heisenberg's uncertainty principle. Just like the position of a particle is a wave with some amplitudes in space, its *momentum* is also a wave in its momentum space. The proposal of de Broglie relates the position x of a particle to its momentum p via a Fourier transform. Heisenberg showed that one cannot know both the position and momentum of a particle with perfect accuracy at the *same* time. When you measure the location of a particle, you localize it in space, which fundamentally increases the uncertainty in the momentum space. It is exactly this fundamental relationship that will be of importance in this thesis and which allows us to use the very fundamental properties of quantum mechanics to construct cryptographic protocols that have capabilities beyond what we could construct with classical mechanics!

Formally, we say that the momentum and position operators do not commute, and the order in which you apply these operators on a quantum system matters. This uncertainty principle was later generalized to any pair of non-commuting observables. In other words, if two observables do not commute, we can never learn both measurement outcomes of a single quantum system at the same time. This property is intrinsically related to the fundamental concept of *no-cloning*. The no-cloning principle states that it is impossible to create an exact copy of an arbitrary unknown quantum state. It can be derived from the linear structure of quantum mechanics and the fact that the allowed transformations are unitary operators on the Hilbert space the quantum state lives in. One can also see that if we could clone a quantum state, we could afterward measure the position of one and the momentum of the other, thus violating Heisenberg's uncertainty principle.

The fundamental idea of quantum cryptography is to actually harness the no-cloning theorem and use its inherent nonclassical properties for the purpose of performing cryptographic tasks. Around 1970 (but published in 1983 [Wie83]) Stephen Wiesner wrote the first paper on this concept that would become a huge influence and essentially start the field of quantum information theory. Wiesner proposed a scheme for *quantum money*, which would be physically impossible to clone, thus not allowing any forgeries. In the scheme, each bank note has a serial number s, and a quantum state consisting of n qubits. The qubits are two-state quantum systems encoded as eigenstates of one of two possible sets of non-commuting observables, with only the bank knowing which set is used. For example, consider the polarization of a photon. In this case, the observables correspond to measurements made in a specific polarization basis, which affects the photon's state accordingly. If we encode photons either in a $\{0°, 90°\}$ polarization basis or in a $\{45°, 135°\}$ basis, they are encoded in two possible sets of non-commuting observables. The bank keeps a ledger of all the serial numbers and the corresponding encoding of the quantum systems. If someone wants to check if a note is real, this person can go to the bank and ask them to verify the note. The bank then measures all the quantum systems in the correct basis, and checks if the measurement outcomes correspond to the ledger. Security against forgery now comes from the fact that these quantum systems cannot be copied without knowing the basis.

The work of Wiesner was the foundation on which the BB84 quantum key distribution protocol by Bennett and Brassard was based [BB14]. Key distribution is a fundamental task in cryptography, it consists of two parties, often called Alice and Bob, who need to share a secret key when they did not have one previously. In the BB84 protocol, Alice sends quantum states to Bob, similar to the states in Wiesner's quantum money scheme. On a high level, the idea behind the security of the protocol is that no attacker can intercept and read out the messages sent by Alice without disturbing the quantum system, and Alice and Bob can detect whether anyone tried to disturb the quantum messages, thus detecting attackers. Moreover, the no-cloning theorem prevents an attacker from copying the qubits for later measurement.

A necessary component to implement the BB84 protocol is a publicly authenticated channel between Alice and Bob. This ensures that while the information exchange is public, both Alice and Bob can be certain that the messages are indeed from one another and not from an attacker. If they did not have such a channel, there could be a so-called *man-in-the-middle* attack, where an attacker pretends to be Bob to Alice. In this way, the attacker could learn the secret key that Alice would establish with Bob. This raises the question: Is there a way to verify that a message from Alice actually originated from Alice?

One way to increase the assurance of the authentication of a message is to verify the location of the sender. If Alice knows Bob's supposed location, and she knows that a message came from this location, this at least gives her some more confidence that the message also came from Bob. The idea of using somebody's geographical location as a cryptographic credential is known as *position-based cryptography*. We might be interested in sending messages that can only be read at a certain location. Or, as mentioned before, it can be useful to know that a message that you expect comes from some party, also comes from the location of this party. If, for example, someone calls for a taxi, we would like to be sure that the person is at his claimed location. This task is known as *position verification*, and is the central topic of this thesis.

The setup of position verification is as follows. Suppose that there is some *prover* P who has to convince a coalition of *verifiers* $V_0, \ldots, V_k$, placed in space around P, that he is present at a specific location. According to Einstein's theory of relativity, information cannot be transmitted faster than the speed of light. If

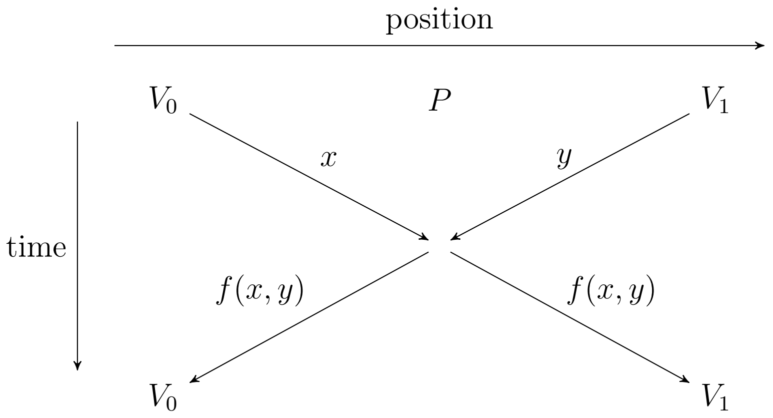


Figure 1.1: Space-time diagram of a position verification protocol. The prover P is placed in the middle between two verifiers V_0, V_1. The verifiers send inputs x, y, for example two random strings, and ask the prover to answer $f(x, y)$ for some function known to everybody. All messages are sent with the speed of light. Afterwards the verifiers check if they received the answers on time.

the verifiers send some message to the prover and ask him to send it back and this takes time t, the verifiers know for sure that the prover is no further than $c \cdot t$ away (where c is the speed of light). This is the idea behind the technique of distance bounding, which was introduced in [BC93]. An intuitive implementation of a distance bounding protocol involves each verifier sending a random string to the prover at the speed of light and asking the prover to return the message. By measuring how long it takes for the messages to return, each verifier can establish a bound on the distance. By combining all the distance bounds, the verifiers can determine the position of P. However, this protocol is not secure as there is a simple attack. A coalition of attackers placed between the verifiers and the claimed location of P can intercept the messages, store them for a moment, and send them back to the verifiers. In this way, they satisfy the task of the verifier and convince them that there was someone at the location P even though it is empty.

An immediate improvement to the above protocol would be to have the answers of P depend on all the received messages. Consider the 1-dimensional case, where two verifiers are on a line, and assume for simplicity that the prover P is placed in the middle. Then, both verifiers send a random string x, y, respectively, and ask the prover to compute some publicly known function $f(x, y)$, and send the answer back to the, as shown in Figure 1.1.

This approach is again not secure, a coalition of attackers *not* at the claimed location of P, but placed in between each verifier and this location, can intercept the inputs x, y, send the inputs to each other, compute $f(x, y)$, and send back the correct answer in time to the verifiers, as shown in Figure 1.2.

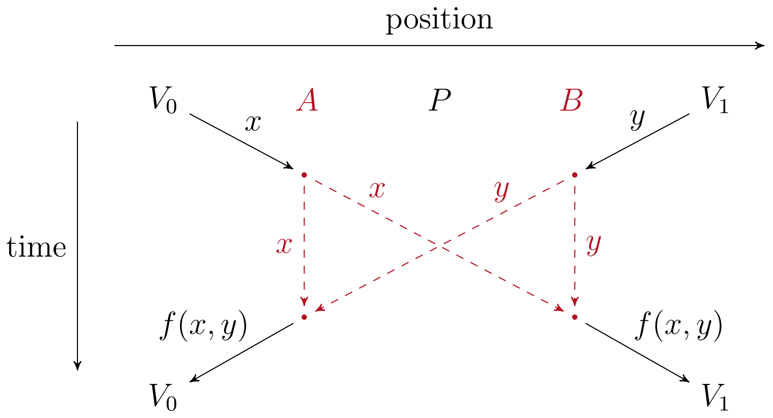


Figure 1.2: Space-time diagram of an attack on the protocol in Figure 1.1. Two attackers A, B placed between the verifiers and the prover, intercept the messages, copy them and send them over, then compute $f(x, y)$ and answer on time.

Different types of position verification protocols have been designed in the classical world, but these will all be insecure; the work by Chandran, Goyal, Moriart, and Ostrovsky [CGMO09] showed an impossibility result in the classical world for *any* position-based cryptography protocol that does not have extra assumptions. Intuitively, this is due to the attack described in Figure 1.2, a coalition of attackers can always copy and share their inputs between each other. This brings up the idea of using quantum information. Since it is impossible to copy a general quantum state, it immediately follows that attacks that merely copy the inputs are not possible.

The possibility of using quantum information was first considered by Kent in 2002, where it was referred to as quantum tagging. In 2006 a U.S. patent was granted to Kent, Beausoleil, Munro, and Spiller for a quantum tagging protocol [BKMS06]. Subsequent work in the scientific literature only appeared later in 2010 [KMS11]. The addition of quantum information was also done by Chandran, Fehr, Goyal, Moriart, and Ostrovsky [CFG$^+$10], which includes some of the authors of the earlier classical impossibility results, and independent work by Malaney [Mal10].

Interestingly, it later turned out that these proposed protocols were also not secure. In fact, it turns out that none of these protocols can be unconditionally secure as a general impossibility result of Buhrman, Chandran, Fehr, Gelles, Goyal, Ostrovsky, and Schaffner [BCF$^+$14] showed. This impossibility construction utilized quantum entanglement between the attackers to achieve any given task, at the cost of a doubly exponential amount of entanglement relative to the input sizes. This was later improved by Beigi and König to a single exponential amount [BK11], using new ideas from port-based teleportation [IH09].

Thus, there are no unconditionally-secure quantum position-verification protocols. However, from a practical point of view, not all is lost. The exponential upper bound for a general attack is still astronomically large for only a relatively small input. So the question has changed to whether we can prove that this exponential upper bound is actually tight, or get a bound that is still hard to achieve in practice. So far, the best-known lower bounds on the amount of entanglement are linear. In this thesis, we will give another example of a protocol with linear lower bounds.

Another central topic in this thesis is the actual implementation of a quantum position verification (QPV) protocol. When we consider a realistic setting, we have to deal with many extra nuances. For example, the easiest and most stable way to send quantum information from the verifiers to the prover would be by using photons via an optical fiber. However, the speed of light in an optical fiber is only roughly 2/3 of the speed of light through free space. This is something that a coalition of colluding attackers could exploit, but, realistically, free-space communication of photons over large distances is very challenging. Secondly, *most* photons will not even arrive at the prover! In a good optical fiber the typical attenuation rate per km would be around 0.2 dB (or 4.6%) [SJ09], thus over longer distances a large fraction of photons will never arrive. As we shall see later, this opens up a whole new way for attackers to attack the protocol. Third, the operations an honest prover has to do must not take too long to implement because if the task takes too long, the uncertainty of its position to the verifiers grows. Developing solutions for the second problem is be one of the most important points in this thesis. We will also highlight its importance with the following example.

1.2 Introduction to the $\mathrm{QPV}^f_{\mathrm{BB84}}$ protocol

The $\mathrm{QPV}^f_{\mathrm{BB84}}$ protocol is a variation of the $\mathrm{QPV}_{\mathrm{BB84}}$ protocol. In the $\mathrm{QPV}_{\mathrm{BB84}}$ protocol two verifiers V_0, V_1 decide on a basis to encode their input, either the computational basis $|0\rangle, |1\rangle$, or the Hadamard basis $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Then V_0 sends one of these two states, which we can denote by $H^\theta |a\rangle$ with $a, \theta \in \{0, 1\}$. Verifier V_1 sends the basis information θ to the prover P, so that he receives both inputs at the same time. Prover P then measures his quantum input in the basis specified by the message of V_1, and sends his measurement outcome a to both verifiers. All messages are sent with the speed of light, and the verifiers finally check if the answers were correct and sent on time. This protocol was proven to be secure against *unentangled* attackers who are only allowed to send classical messages to each other in the work of Buhrman et al. [BCF+14], later the security was extended to also include *quantum communication* and *parallel repetition* but without pre-shared entanglement by Tomamichel, Fehr, Kaniewski, and Wehner [TFKW13].

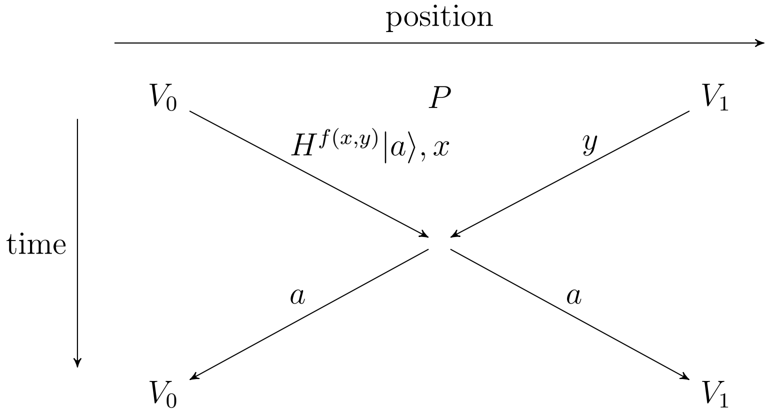


Figure 1.3: Space-time diagram of the $\mathrm{QPV}^f_{\mathrm{BB84}}$ position verification protocol for some boolean function f. The prover P is placed in the middle between two verifiers V_0, V_1. Verifier V_1 sends a classical string y. V_0 sends a classical string x and one of the four BB84 states, encoded in the basis determined by the function value $f(x,y)$. The prover P computes the function value $f(x,y)$, and sends back his answer to the verifiers. All messages are sent with the speed of light. Afterwards the verifiers check if the answer is correct and if they received it on time.

This protocol can be easily broken by a coalition of attackers placed between the verifiers and P, with access to pre-shared entanglement. Two attackers Alice and Bob only need a single EPR pair to successfully attack the protocol. The attack goes as follows:

- Alice teleports her quantum input to Bob, getting two bits from the teleportation measurement.
- Bob measures his local qubit in the basis specified by his input and gets some measurement outcome.
- Both players send their measurement outcomes to each other after which they can both answer perfectly correct and on time.

We will see why this attack works correctly. First, Alice gets some input state $H^\theta |a\rangle$, then she teleports the state and gets teleportation measurement outcomes b_1, b_2. Bob then holds the state $X^{b_1}Z^{b_2}H^\theta |a\rangle$. Note that $X|0\rangle = |1\rangle, X|1\rangle = |0\rangle$, $X|+\rangle = |+\rangle, X|-\rangle = -|-\rangle$, and similarly $Z|0\rangle = |0\rangle, Z|1\rangle = -|1\rangle$, $Z|+\rangle = |-\rangle, Z|+\rangle = |-\rangle$. In other words, the Pauli X gate leaves the states in the Hadamard basis invariant up to a global phase, while it flips the states in the computational basis. The Pauli Z gate flips the states in the Hadamard basis and leaves the computational basis states invariant. Since Bob measures in the correct basis θ, his answer will be either correct or flipped depending on the teleportation measurement outcome. After the exchange of the measurement outcomes between Alice and Bob, they have all the information to determine the answer a and they respond to the verifiers on time.

An improvement to this protocol is the so-called $\mathrm{QPV}^f_{\mathrm{BB84}}$ protocol, where instead of sending the basis from one side, the basis information comes from the joint messages from the verifiers. We introduce some boolean function f that takes as input two n-bit strings x, y, and whose function value $f(x, y)$ determines the basis in which the prover has to measure. Depending on the complexity of the function f, this protocol is secure against attackers restricted to a limited amount of entanglement [BCS22]. For a random function, the attackers need at least $n/2 - 5$ EPR pairs to successfully attack the protocol[1], and for an explicit function such as the inner product, the attackers need at least $\log(n)/2 - 5$ EPR pairs[2] or need to apply at least n quantum gates or measurements [ACCM24]. Furthermore, the protocol remains secure if the input quantum information is sent beforehand, which is an advantage in a practical setting where the quantum information must be sent beforehand to account for the speed of light in fiber-optic cables.

Although such linear bounds are still far away from exponential bounds, an important advantage of this protocol is that the required entanglement scales with the size of the *classical* messages. Since sending larger classical messages is much easier compared to storing more EPR pairs, we can still argue for some practical security. However, a major drawback of this protocol is that it is broken in regimes with loss higher than 50%. As mentioned before, in a realistic setting one will deal with losses, and with an attenuation rate of 0.2 dB/km, the loss rate will exceed 50% already after around 15 km. And then we also get an extra loss on top of that from every mirror, beam splitter, etc. Therefore, the verifiers do not expect the prover to answer most of the rounds. The attackers can use this to their advantage; Alice can intercept the message close to the verifier, then guess a basis to measure in. Alice then sends her measurement outcome to Bob, and Bob sends the basis information to Alice. When Alice's guess was correct both attackers reply, otherwise they simply declare a loss. This perfectly breaks the protocol! Work by Qi and Siopsis [QS15] works around this by introducing a decoy-state method that uses coherent states as quantum inputs sent with different intensities. Another way to circumvent this is to introduce multiple bases to tolerate higher loss rates [Spe16b, ES23], but this does not allow full loss tolerance. The work of Lim, Xu, Siopsis, Chitambar, Evans, and Qi [LXS$^+$16] circumvents this issue by designing a protocol whose inputs are purely classical and able to show full loss tolerance against attackers restricted to classical communication. Therefore, a central question in this thesis is:

[1] This lower bound is still in sharp contrast to the best known attack that uses an exponential amount of entanglement

[2] Again there is still an exponential gap between this lower bound and the best known attack that uses a linear amount of entanglement.

Can we design quantum position verification protocols that are easy to implement, resistant against photon loss, and secure against entanglement?

1.3 Chapter Overview

The results in this thesis revolve around two central topics. First, we discuss the problem of dealing with loss in QPV protocols. We introduce a new protocol and prove it is loss-tolerant, even in a parallel setting, against classical attackers. Additionally, we prove new separations between QPV security models, attackers that are allowed to communicate *quantum messages* can break certain protocols that are provably secure against classical attackers. We also investigate the role of loss in this quantum communication setting. Finally, we propose a modification that makes the $\mathrm{QPV}^{f}_{\mathrm{BB84}}$ protocol loss-tolerant paving the way for practically secure, implementable protocols.

Secondly, we show that certain known QPV protocols can be related to classical analogues, and we discuss some (surprising) implications of this relationship.

In **Chapter 2** we introduce some terminology and background to the basics of quantum computation and quantum information. We show how to teleport an unknown quantum state via a teleportation procedure. We introduce the SWAP test, which is the optimal measurement that distinguishes two either equal or orthogonal quantum states. Finally, we provide a general introduction to semidefinite programming, including an example of how to find an optimal POVM measurement for a state distinguishing task, where the measurements have a positive partial transpose (PPT).

In **Chapter 3** we propose a new protocol $\mathrm{QPV}_{\mathsf{SWAP}}$ fully loss-tolerant against classical attackers. The honest prover has to implement a SWAP test to determine the overlap between his input states. Similarly to the work by Lim et al. [LXS⁺16], all the inputs to the prover are quantum states. We show that the protocol has several desirable properties. By formulating the optimal attack as an SDP, which we solve analytically, we give optimal bounds on the success probability of attackers and show that the protocol obeys strong parallel repetition. Furthermore, we propose an easy experimental setup for the protocol, and argue that such an implementation is realistic in practice. One of its advantages is a passive setup for the prover P, whose measurement remains the same in every round and consists only of a 50/50 beamsplitter and two photon detectors.

In **Chapter 4** we extend the security model of QPV protocols and investigate the security of protocols when we allow the attackers a simultaneous round of quantum communication when they do not pre-share entanglement. We give a separating example of a QPV protocol provably secure against attackers restricted to classical communication and no pre-shared entanglement, but the protocol can be trivially broken if the attackers have access to a quantum channel between them. We then show that any protocol secure against classical communication can be transformed into a protocol secure against quantum communication. We further show, using arguments based on the monogamy of entanglement, that the task of Bell state discrimination cannot be done with only local operations and a single round of simultaneous quantum communication, not even probabilistically (when we allow attackers to say loss sometimes), making this the first fully loss-tolerant QPV task secure against quantum communication attacks. Furthermore, we show that the techniques used to prove security of the Bell discrimination task also imply security of the SWAP test protocol from Chapter 3 against attackers allowed to use quantum communication.

In **Chapter 5** we modify the usual structure of QPV protocols and prove that this modification makes the potentially high transmission loss between the verifiers and the prover security-irrelevant for a class of protocols that includes the $\mathrm{QPV}^f_{\mathrm{BB84}}$ protocol. This modification, which involves photon presence detection, a small time delay at the prover, and a commitment to play before proceeding, reduces the overall loss rate to just the prover's laboratory. The adapted protocol $\mathsf{c}\text{-}\mathrm{QPV}^f_{\mathrm{BB84}}$ then becomes a practically feasible QPV protocol with strong security guarantees, even against attackers using adaptive strategies. As the loss rate between the verifiers and the prover is mainly dictated by the distance between them, secure QPV over longer distances becomes possible. We also show possible feasible implementations of the required photon presence detection, making $\mathsf{c}\text{-}\mathrm{QPV}^f_{\mathrm{BB84}}$ a protocol that solves all major practical issues in QPV. It is secure against slow quantum communication and loss, and the prover's operations are relatively simple, since he only needs to manipulate a single qubit and make a classical computation.

In **Chapter 6** we invert the picture, and consider the task of non-local quantum computation (NLQC), which corresponds to the operations of the attackers in a QPV protocol. We connect NLQC to the wider context of information-theoretic cryptography by relating it to a number of other cryptographic primitives. We show that one special case of NLQC, known as f-routing, is equivalent to the quantum analogue of the conditional disclosure of secrets (CDS) primitive, where by equivalent we mean that a protocol for one task gives a protocol for the other with only small overhead in resource costs. We further consider another special case of position verification, which we call coherent function evaluation (CFE), and show that CFE protocols induce similarly efficient protocols for the private simultaneous message passing (PSM) scenario. By relating position-verification to these cryptographic primitives, a number of results in the information-theoretic cryptography literature give new implications for NLQC, and vice versa. These include the first sub-exponential upper bounds on the worst case cost of f-routing of $2^{O(\sqrt{n \log n})}$ entanglement, the first example of an efficient f-routing strategy for a problem believed to be outside $P/poly$, linear lower bounds on quantum resources for CDS in the quantum setting, linear lower bounds on communication cost of CFE, and efficient protocols for CDS in the quantum setting for functions that can be computed with quantum circuits of low T depth.

Chapter 2

Preliminaries

We introduce some basic terminology and some background into the basics of quantum computation and quantum information. We show how to teleport an unknown quantum state via a teleportation procedure. We introduce the SWAP test, which is the optimal measurement that distinguishes two either equal or orthogonal quantum states. We give a general introduction to semidefinite programming, with an example on how to find an optimal POVM measurement for a state distinguishing task, where the measurements have positive partial transpose (PPT).

2.1 Notation and Terminology

We will start with some definitions that we will use throughout this thesis. We write $\mathbb{N}$ for the set of natural numbers, $\mathbb{R}$ for the real numbers, and $\mathbb{C}$ for the complex numbers. We write $[n]$ to refer to the set $\{1, 2, 3, \ldots, n\}$. Bits b are integers that are either 0 or 1, these are often taken from $\mathbb{F}_2$, such that the addition of two bits corresponds to taking the XOR. We write $\{0,1\}^n$ for the set of all n-bit strings. For a string $x \in \{0,1\}^n$ we write x_i to denote its i-th bit, and $|x|$ denotes its *Hamming weight*, which is the number of 1's in the string. For two strings $x, y \in \{0,1\}^n$ we write $x \oplus y$ for their element-wise XOR, and $x \cdot y$ for their inner product $\sum_{i=1}^{n} x_i \cdot y_i$ which is often taken mod 2.

For two real vectors $v, w \in \mathbb{R}^n$ we write $\langle v, w \rangle := v^T w$ for the inner product, where T denotes the transpose. For two complex vectors $v, w \in \mathbb{C}^n$, the inner product is written as $v^\dagger w$, where $\dagger$ denotes the conjugate transpose. A matrix $M \in \mathbb{C}^{n \times n}$ is Hermitian if $M^\dagger = M$. And a matrix is *positive semidefinite* (psd) if it is Hermitian and all its eigenvalues are non-negative. The notation $M \succeq 0$ indicates that M is positive semidefinite. For two matrices M, N we write $M \succeq N$ if $M - N \succeq 0$.

Often we are interested in the asymptotic behavior of functions. Let f, g be two functions from $\mathbb{N}$ to $\mathbb{N}$, to analyze its asymptotic behavior we use the big O notation defined as follows:

$$f(n) = O(g(n)) \Leftrightarrow \exists\, c, N \geq 0 \text{ such that } \forall n > N : f(n) \leq cg(n). \tag{2.1}$$

Similarly we define big Ω notation for lower bounds:

$$f(n) = \Omega(g(n)) \Leftrightarrow \exists\, c, N \geq 0 \text{ such that } \forall n > N : f(n) \geq cg(n), \tag{2.2}$$

or equivalently

$$f(n) = \Omega(g(n)) \Leftrightarrow g(n) = O(f(n)). \tag{2.3}$$

When $f(n) = \Theta(g(n))$ we have both $f(n) = O(g(n))$ *and* $f(n) = \Omega(g(n))$.

2.2 Quantum Information

We will introduce some basic concepts in quantum computing that we use in this thesis. For a more complete background on the subject, we refer the reader to the well-known textbook by Nielsen and Chuang [NC10] and the lecture notes by de Wolf [Wol19].

2.2.1 Quantum States

In this thesis, we will only consider quantum systems of finite dimensions. We will write vectors in bra-ket notation, as introduced by Dirac. For a $\psi \in \mathbb{C}^d$ we write

$$|\psi\rangle = \begin{pmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_d \end{pmatrix}, \tag{2.4}$$

which is called a *ket*. The *bra* is the complex conjugate of a vector:

$$\langle\psi| = \begin{pmatrix} \psi_1^* & \psi_2^* & \dots & \psi_d^* \end{pmatrix}, \tag{2.5}$$

where $*$ denotes the complex conjugate. The advantage of Dirac notation is that the inner product between two vectors can be written as $\langle\psi|\phi\rangle$, as a shorthand for $\langle\psi|\,|\phi\rangle$.

We can also write a vector as a sum of unit vectors that span $\mathbb{C}^d$ denoted by $|0\rangle, \dots, |d-1\rangle$, where $|i\rangle$ denotes the unit vector of dimension d with a single 1 in position i. These unit vectors are also known as the *computational basis*. A pure quantum state $|\phi\rangle$ of a quantum system in dimension d is a vector of unit length, which we denote as:

$$|\phi\rangle = \sum_{i=0}^{d-1} \alpha_i |i\rangle. \tag{2.6}$$

Here, $\alpha_i \in \mathbb{C}$ are called amplitudes, since the vector is of unit length, we must have $\sum_{i=0}^{d} |\alpha_i|^2 = 1$. When there is more than one nonzero α_i we call such a sum over quantum states a *superposition*.

Often we just consider *qubits* which are quantum states in $\mathbb{C}^2$. We can write any pure one-qubit state $|\psi\rangle$ as a superposition over the two computational basis vectors:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \text{ where } \alpha, \beta \in \mathbb{C} \text{ and } |\alpha|^2 + |\beta|^2 = 1, \tag{2.7}$$

and the computational basis states are defined as:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{2.8}$$

When we combine two quantum systems, their joint system is a vector that is an element of the tensor product of the original spaces. So, if we take one vector $|\phi\rangle \in \mathbb{C}^{d_1}$ and one vector $|\psi\rangle \in \mathbb{C}^{d_2}$, their joint system is a vector in $\mathbb{C}^{d_1 d_2}$ and in Dirac notation we write this as $|\phi\rangle \otimes |\psi\rangle$ or sometimes simply $|\phi\rangle|\psi\rangle$.

The simplest example would be to take a two-qubit system. A pure quantum state in a two-qubit system can be described by a vector in $\mathbb{C}^4$, with computational basis states.

$$|0\rangle \otimes |0\rangle = |00\rangle = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, \qquad |0\rangle \otimes |1\rangle = |01\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, \tag{2.9}$$

$$|1\rangle \otimes |0\rangle = |10\rangle = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, \qquad |1\rangle \otimes |1\rangle = |11\rangle = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}. \tag{2.10}$$

A state in the joint space of two quantum systems that can be written as a tensor product of two states in the original systems, such as the basis states described above, are called *separable states*. States that cannot be written as a product state are called *entangled states*. A well-known example of an entangled state is the EPR-state, named after Einstein, Podolski and Rosen who wrote a famous paper on the properties of entanglement [EPR35]:

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{2.11}$$

2.2.2 Measurements

Importantly, if we have some quantum state $|\phi\rangle$ that is in a superposition, we cannot access the exact values in the superposition. Instead, we get measurement outcomes with some probability distribution according to Born's rule, which says that the probability density of finding a quantum system in a given state is proportional to the square of the amplitude of that state. Thus, if we have some quantum state as in Equation 2.6, we can get a measurement outcome 'i' with probability $|\alpha_i|^2$. Afterwards, the quantum system will collapse from the superposition $|\phi\rangle$ to just the quantum state $|i\rangle$. This measurement corresponds to a projective measurement onto the computational basis, but we can extend this notion of measurement.

A *projective* measurement is described by a collection of projectors $\{P_1, \ldots, P_m\}$ that sum up to identity and project to subspaces $\{V_1, \ldots, V_m\}$ respectively. Since the projectors sum up to identity they must be pairwise orthogonal, and thus the spaces they project to must be orthogonal to each other as well. Any state $|\phi\rangle$ in the entire space can then be decomposed as a superposition over these subspaces as follows:

$$|\phi\rangle = \sum_{i=1}^{m} |\phi_i\rangle, \tag{2.12}$$

where we have $|\phi_i\rangle = P_i|\phi\rangle$, i.e. the projection of the state to that subspace. By Born's rule, we then find that the probability to get outcome i is its square amplitude $\|P_i|\phi\rangle\|^2$. Afterwards the state collapses to this subspace, but, as the post-measurement state is a valid quantum state, we normalize the state $\frac{P_i|\phi\rangle}{\|P_i|\phi\rangle\|}$.

As an example, suppose we measure the state $|\phi\rangle = \frac{1}{\sqrt{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle$ in the computational basis. Then our projectors are simply

$$\{|0\rangle\langle 0|, |1\rangle\langle 1|\} = \left\{\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\right\}, \tag{2.13}$$

which indeed sum to identity. Then the probability to have outcome 0 is:

$$\left\| |0\rangle\langle 0| \left(\frac{1}{\sqrt{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle\right)\right\|^2 = \left\|\frac{1}{\sqrt{3}}\right\|^2 = \frac{1}{3}, \tag{2.14}$$

with post-measurement state $|0\rangle$.

We can also apply a computational-basis measurement to one system, but leave the rest of the system intact. For example, we can measure the first qubit in the EPR-state from Equation 2.11, while leaving the second state invariant. Our set of projectors is then:

$$\{|0\rangle\langle 0| \otimes \mathbb{1}, |1\rangle\langle 1| \otimes \mathbb{1}\}. \tag{2.15}$$

Both projectors again add up to identity. When we apply the measurement to $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, we see that we get with equal probability $\frac{1}{2}$ measurement outcome 0 or 1. The quantum states to which we collapse are $|00\rangle$ and $|11\rangle$, respectively.

Projective measurements are not the most general measurement we can apply. The most general type of measurement is the so-called POVM measurement which stands for *positive operator valued measurement*. A POVM is a collection of positive semidefinite matrices $E_1, \ldots, E_m$ that sum up to identity. The probability of getting measurement outcome i after measuring some state $|\phi\rangle$ corresponds to $\langle\phi| E_i |\phi\rangle = \mathrm{Tr}[E_i |\phi\rangle\langle\phi|]$. Note that in the last equation, by the cyclicity of the trace, we can multiply $|\phi\rangle$ by any complex phase $e^{i\theta}$ and it will cancel out. Because of this, we often say that states are equivalent up to a global phase, since this phase does not change the probabilities of the measurements.

2.2.3 Unitaries and Gates

Besides measurements, which are non-linear and collapse the state, by the postulates of quantum mechanics we can evolve quantum systems by a unitary transformation. We write U for such a unitary matrix, and write $U|\phi\rangle$ when we apply U to some state $|\phi\rangle$. The outcome of this transformation $U|\phi\rangle = |\psi\rangle$ will also be a quantum state as its norm remains unchanged. Since U is unitary, we have

$U^\dagger U = \mathbb{1}$, and $U^\dagger |\psi\rangle = |\phi\rangle$. Note that, by linearity, if we know how U transforms all the computational basis states, we know how U transforms any state.

For the qubit case there is a commonly used set of unitaries called the *Pauli matrices* which are also represented by $\mathbb{1}, X, Y, Z$:

$$\sigma_0 := \mathbb{1} := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \sigma_1 := X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{2.16}$$

$$\sigma_2 := Y := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \sigma_3 := Z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.17}$$

The Pauli matrices have some similarities to the classical operations we can do to bits, but the operations are now reversible. The X gate flips the computational basis states $|0\rangle$ and $|1\rangle$, and the Z gate adds a -1 phase to the $|1\rangle$ state but leaves the $|0\rangle$ state invariant.

We often call unitaries on a single qubit or two qubits a *gate*. Another important single-qubit gate is the Hadamard gate which sends the computational basis states to a superposition over the two:

$$H := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{2.18}$$

The Hadamard is its own inverse, and sends $|0\rangle$ to $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, which is often denoted by the $|+\rangle$, and sends $|1\rangle$ to $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, which is often denoted by $|-\rangle$. We write $|0^n\rangle$ for the all-zero n-qubit state, and when we apply a Hadamard gate to each individual qubit we get a superposition over all possible computational basis states in the $\mathbb{C}^{2^n}$ dimensional space:

$$H^{\otimes n} |0^n\rangle = \frac{1}{\sqrt{2^n}} \sum_{s \in \{0,1\}^n} |s\rangle . \tag{2.19}$$

An important 2-qubit gate is the CNOT operation. The CNOT is a controlled-X gate, controlled on the first qubit it applies a X gate to the second qubit:

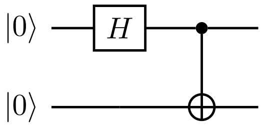
$$\mathrm{CNOT} |0\rangle |b\rangle = |0\rangle |b\rangle \tag{2.20}$$

$$\mathrm{CNOT} |1\rangle |b\rangle = |1\rangle |1 \oplus b\rangle , \tag{2.21}$$

as a matrix the CNOT looks as follows:

$$\mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{2.22}$$

We can use the combination of the Hadamard gate and the CNOT gate to construct the EPR-state mentioned in Equation 2.11. In what follows, we give a



circuit that maps the $|00\rangle$ input to the $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ state: A circuit should be read from left to right. Each wire represents a qubit, the qubits here are initialized in the $|0\rangle$ state, then a Hadamard gate is applied to the first qubit. When no gate is applied on a wire, we can imagine the identity matrix is applied to that qubit. After which a CNOT gate controlled to the first qubit is applied. After the Hadamard the state looks as follows:

$$(H \otimes \mathbb{1})\,|00\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle),$$

then a CNOT is applied:

$$\text{CNOT}\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

As a result of the fact that operations have to be unitary we also have that there cannot exist a general operation that *copies* a general quantum state. This is known as the *no-cloning theorem* and is an important result in the area of cryptography. The statement is easy to prove and we will show it by contradiction. Assume that there is some unitary U that can copy any state $|\phi\rangle$ into some second register, so we have $\forall\,|\phi\rangle : U\,|\phi\rangle\,|0\rangle = |\phi\rangle\,|\phi\rangle$. Then we have on the computational basis inputs

$$U\,|0\rangle\,|0\rangle = |0\rangle\,|0\rangle\,, \tag{2.23}$$

and similarly

$$U\,|1\rangle\,|0\rangle = |1\rangle\,|1\rangle\,. \tag{2.24}$$

When we apply U to the state $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|0\rangle$ we get

$$\begin{aligned} U\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) = |{+}{+}\rangle\,. \end{aligned} \tag{2.25}$$

However, by linearity we should also get:

$$U\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|0\rangle = \frac{1}{\sqrt{2}}(U\,|0\rangle\,|0\rangle + |1\rangle\,|0\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \tag{2.26}$$

which is not equal to $|{+}{+}\rangle$. So we get a contradiction and conclude that such a unitary U cannot exist.

2.3 Teleportation

As we have mentioned before, the EPR-state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ cannot be written as a tensor product of two single qubit states, thus the state is entangled. After generating this state, we can separate these two qubits, but they will remain entangled. An important protocol that makes use of the entanglement in these EPR-states is *quantum teleportation* [BBC+93]. We will show that it is possible to send a quantum state from one location to another using an EPR-state whose qubits are at each location, and by only communicating two bits of classical information.

Say Alice is at one location and Bob at the other, and Alice wants to send a general qubit $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ to Bob. They share an EPR-state $\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$, where the indices A, B denote which qubits Alice and Bob hold, respectively.

First consider the following four states, also known as the *Bell states*, one of which is the EPR-state:

$$|\Phi^+\rangle := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \qquad |\Phi^-\rangle := \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \tag{2.27}$$

$$|\Psi^+\rangle := \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \qquad |\Psi^-\rangle := \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \tag{2.28}$$

These states are also known as the *Bell basis* as they are orthogonal to each other and span the entire two-qubit $\mathbb{C}^4$ space. What is also interesting is that we can transform any Bell state into another by applying local Pauli gates, for example, $|\Psi^+\rangle = (\mathbb{1} \otimes X)|\Phi^+\rangle$. We can also measure in this Bell basis, which we call a *Bell state measurement.* One can verify that the quantum circuit mentioned above not only sends the $|00\rangle$ state to $|\Phi^+\rangle$, but also sends the other computational basis states to a Bell state. Thus, when we want to perform a Bell state measurement, we can apply the reverse of this circuit and measure in the computational basis.

Now we have the tools to state the teleportation protocol. We start with the following state:

$$\begin{aligned} &\frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})(\alpha|0\rangle_Q + \beta|1\rangle_Q) \\ &\quad = \frac{1}{\sqrt{2}}(\alpha|00\rangle_{AQ}|0\rangle_B + \beta|01\rangle_{AQ}|0\rangle_B + \alpha|10\rangle_{AQ}|1\rangle_B + \beta|11\rangle_{AQ}|1\rangle_B), \end{aligned} \tag{2.29}$$

where Q indicates the qubit that Alice wants to teleport to Bob. First we write Alice's qubits into the Bell basis and we get:

$$\begin{aligned} &\frac{1}{2}\Big(\Big(|\Phi^+\rangle_{AQ} + |\Phi^-\rangle_{AQ}\Big)\alpha|0\rangle_B + \Big(|\Psi^+\rangle_{AQ} + |\Psi^-\rangle_{AQ}\Big)\beta|0\rangle_B \\ &\qquad + \Big(|\Psi^+\rangle_{AQ} - |\Psi^-\rangle_{AQ}\Big)\alpha|1\rangle_B + \Big(|\Phi^+\rangle_{AQ} - |\Phi^-\rangle_{AQ}\Big)\beta|1\rangle_B\Big). \end{aligned} \tag{2.30}$$

Then we can group the Bell state on the AQ subsytems together to get:

$$\frac{1}{2}\Big(\left|\Phi^+\right\rangle_{AQ}(\alpha\left|0\right\rangle_B+\beta\left|1\right\rangle_B)+\left|\Phi^-\right\rangle_{AQ}(\alpha\left|0\right\rangle_B-\beta\left|1\right\rangle_B)$$
$$\left|\Psi^+\right\rangle_{AQ}(\beta\left|0\right\rangle_B+\alpha\left|1\right\rangle_B)+\left|\Psi^-\right\rangle_{AQ}(\beta\left|0\right\rangle_B-\alpha\left|1\right\rangle_B)\Big). \tag{2.31}$$

Now Alice applies the map that sends the Bell states to the computational basis on her two-qubits, and we get:

$$\frac{1}{2}\Big(\left|00\right\rangle_{AQ}(\alpha\left|0\right\rangle_B+\beta\left|1\right\rangle_B)+\left|01\right\rangle_{AQ}(\alpha\left|0\right\rangle_B-\beta\left|1\right\rangle_B)$$
$$\left|10\right\rangle_{AQ}(\beta\left|0\right\rangle_B+\alpha\left|1\right\rangle_B)+\left|11\right\rangle_{AQ}(\beta\left|0\right\rangle_B-\alpha\left|1\right\rangle_B)\Big). \tag{2.32}$$

Now see what happens if Alice measures the AQ subsystem, that she holds, in the computational basis. She will get one of the four computational basis states as a measurement outcome with equal probability. Note that if Alice's measurement outcome was 00, that in the post-measurement state Bob holds the qubit Q that Alice wanted to teleport! In fact, for all possible measurement outcomes $(a,b)\in\{0,1\}^2$ for Alice, there is a mapping consisting of Pauli gates X^aZ^b for Bob that maps his local qubit to the qubit Q that Alice initially held. Thus, if Alice sends over her measurement outcome of two bits to Bob, he can perfectly recover the qubit Q that Alice held, and indeed Alice has teleported her state to Bob. Note that the pre-shared EPR pair is consumed in the process, and after Alice's measurement there is no entanglement left. Since we can transform the Bell states into each other using only local Pauli gates, any other pre-shared Bell state instead of the $\left|\Phi^+\right\rangle$ state would also have sufficed to perform the teleportation protocol.

2.4 Mixed States

So far we have only considered the so-called *pure* quantum states which are represented by a vector of unit length. In some settings, especially in quantum cryptography, we consider so-called *mixed* quantum states which are a probability distribution over pure states. A *mixed state* is represented by a matrix called a *density matrix*, which is a trace 1 positive semidefinite matrix. For example, if we have the mixture of with probability $\frac{3}{4}$ the state $\left|0\right\rangle$ and with probability $\frac{1}{4}$ the state $\left|1\right\rangle$ we can write the density matrix ρ as:

$$\frac{3}{4}\left|0\right\rangle\!\left\langle 0\right|+\frac{1}{4}\left|1\right\rangle\!\left\langle 1\right|. \tag{2.33}$$

In general, if for $i\in[r]$ we get the state $\left|\phi_i\right\rangle$ with probability p_i then we have an ensemble of pure states $\{p_i,\left|\phi_i\right\rangle\}$, with density matrix:

$$\rho=\sum_{i=1}^{r}p_i\left|\phi_i\right\rangle\!\left\langle\phi_i\right|. \tag{2.34}$$

The density matrix of a pure state $|\phi\rangle$ is simply the rank 1 matrix $|\phi\rangle\langle\phi|$. Unitary operations on a density matrix ρ transform the state from ρ to $U\rho U^\dagger$. We can also apply a POVM $\{E_1, \dots, E_m\}$, and the probability of getting measurement outcome $i \in [m]$ is $\mathrm{Tr}[E_i\rho]$.

Distance measures and inequalities

Two density matrices can be similar, and it is useful to define a notion of overlap between two states. The *Fidelity* does this. Let $\mathcal{D}(\mathcal{H}_A)$ be the set of density matrices on the Hilbert space $\mathcal{H}_A$. Given two density matrices ρ, $\sigma \in \mathcal{D}(\mathcal{H}_A)$, define the fidelity,

$$F(\rho, \sigma) \equiv \left(\mathrm{Tr}\left(\sqrt{\sqrt{\rho}\,\sigma\sqrt{\rho}}\right)\right)^2. \tag{2.35}$$

The reason we use this definition instead of, e.g. $\mathrm{Tr}[\rho\sigma]$, is that we want the fidelity of a state with itself to be 1, and $\mathrm{Tr}[\rho^2] = \sum_{i=1}^r p_i^2$ does not capture this! The fidelity is related to the one norm distance $||\rho - \sigma||_1$ by the Fuchs-van de Graaf inequalities [FvdG99],

$$1 - \sqrt{F(\rho, \sigma)} \leq \frac{1}{2}||\rho - \sigma||_1 \leq \sqrt{1 - F(\rho, \sigma)}. \tag{2.36}$$

2.4.1 Quantum one-time pad

The formalism of mixed states also allows us to define a useful procedure in quantum cryptography called the *Quantum one-time pad* [AMTW00]. The quantum one-time pad uses classical randomness to conceal quantum information. To understand this, suppose that Alice wishes to give Bob a quantum system B, but wants Bob to only obtain B if he also knows a classical key k. Suppose that B consists of qubits, Alice can do this by applying a random Pauli string P_B^k. If Bob does not know k, B is hidden to him since

$$\frac{1}{2^{|k|}} \sum_k P_B^k \rho_{AB} P_B^k = \rho_A \otimes \frac{\mathbb{1}_B}{d_B}, \tag{2.37}$$

where the index k ranges over all choices of Pauli strings. On the other hand, if Bob knows k he can undo the Pauli string and recover the B system.

2.5 The SWAP test

The SWAP test was first introduced in [BBD+97, BCWW01] for quantum fingerprinting as a useful tool to determine whether two unknown states are identical or not. The quantum circuit of the SWAP test is depicted in Figure 2.1.

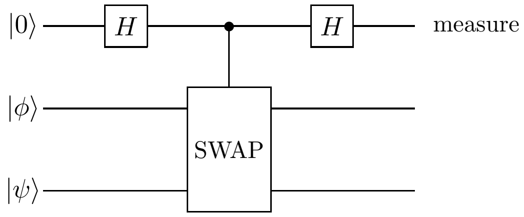


Figure 2.1: The SWAP test, taken from [BCWW01]. H denotes the Hadamard gate.

Before the final measurement, the state can be written as:

$$\begin{aligned}(H \otimes \mathbb{1})\text{c-SWAP}(H \otimes \mathbb{1}) |0\rangle |\phi\rangle |\psi\rangle = \\ \frac{1}{2} |0\rangle (|\phi\rangle |\psi\rangle + |\psi\rangle |\phi\rangle) + \frac{1}{2} |1\rangle (|\phi\rangle |\psi\rangle - |\psi\rangle |\phi\rangle).\end{aligned} \tag{2.38}$$

When the first qubit gets measured in the computational basis we get the outcomes '0' or '1' with the following probabilities:

$$\mathbb{P}[0] = \frac{1 + |\langle\psi|\phi\rangle|^2}{2} \qquad \text{and} \qquad \mathbb{P}[1] = \frac{1 - |\langle\psi|\phi\rangle|^2}{2}. \tag{2.39}$$

The output distribution only depends on the overlap $|\langle\psi|\phi\rangle|$ between the input states. A notable special case is when $|\phi\rangle = |\psi\rangle$ and the SWAP operation has no effect, so we get $\mathbb{P}[0] = 1$. Another advantage of the SWAP test is that it is easily implemented experimentally with a single beam splitter and two photon detectors [JAC04, GECP13]. Its flexibility regarding input states and the simplicity of its experimental realization make it a good candidate for a practical implementation of QPV.

We can also apply the SWAP test to entangled inputs. When we apply the SWAP test to the Bell states in Equation 2.27, we see that the three Bell states $|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle$ always have measurement outcome 0, since they remain invariant under the SWAP operator. Contrarily, the $|\Psi^-\rangle$ state always has measurement outcome 1, since it gets an overall minus phase under the SWAP operator. The space of 2-qubit states can be split into a *symmetric subspace* spanned by $|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle$, and an *antisymmetric subspace* spanned by just $|\Psi^-\rangle$.

2.6 Semidefinite Programming

Semidefinite programming is a powerful technique that allows us to efficiently solve optimization problems numerically, but can also be useful from an analytical point of view. SDPs have many use cases, but we will use them in the application to quantum information theory to find optimal POVM measurements [Eld03].

A semidefinite program (SDP) is a constrained optimization problem where we optimize over a positive semidefinite matrix X, where the objective and constraints are linear in the entries of X. We use the definition and follow some derivations from [Wat18]:

2.6.1. Definition. A semidefinite program is a triple (Φ, A, B), where

1. $\Phi \in T(\mathcal{X}, \mathcal{Y})$ is a Hermiticity-preserving linear map, and
2. $A \in \mathrm{Herm}(\mathcal{X})$ and $B \in \mathrm{Herm}(\mathcal{Y})$ are Hermitian operators,

for Euclidean spaces $\mathcal{X}, \mathcal{Y}$. Two optimization problems are associated to this triple, a **primal** and **dual**:

$$\begin{array}{rlrl} & \textbf{Primal Problem} & & \textbf{Dual Problem} \\ \textbf{maximize:} & \langle A, X\rangle & \textbf{minimize:} & \langle B, Y\rangle \\ \textbf{subject to:} & \Phi(X) = B & \textbf{subject to:} & \Phi^*(Y) \succeq A \\ & X \in \mathrm{Pos}(\mathcal{X}). & & Y \in \mathrm{Herm}(\mathcal{Y}). \end{array}$$

Here, the inner product is defined as $\langle A, X\rangle = \mathrm{Tr}[A^\dagger X]$. Φ^* represents the *adjoint operator* of Φ, namely the unique map that satisfies $\langle \Phi^*(Y), X\rangle = \langle Y, \Phi(X)\rangle$. And we say that some matrix $A \succeq B$, when $A - B$ is positive semidefinite.

An operator $X \in \mathrm{Pos}(\mathcal{X})$ is *primal feasible* if it satisfies $\Phi(X) \leq B$, and similarly an operator $Y \in \mathrm{Herm}(\mathcal{Y})$ is *feasible* if $\Phi^*(Y) \succeq A$. We can define two sets of all feasible operators:

$$\begin{aligned} \mathcal{A} &= \{X \in \mathrm{Pos}(\mathcal{X}) \text{ such that } \Phi(X) \leq B\} \\ \mathcal{B} &= \{Y \in \mathrm{Herm}(\mathcal{Y}) \text{ such that } \Phi^*(Y) \succeq A\}. \end{aligned}$$

The optimal primal and dual value are defined as:

$$\alpha = \sup_{X \in \mathcal{A}} \langle A, X\rangle \tag{2.40}$$

$$\beta = \inf_{Y \in \mathcal{B}} \langle B, Y\rangle, \tag{2.41}$$

respectively. If there are no feasible solutions to either the primal or dual, we write $\alpha = -\infty$ or $\beta = \infty$.

The primal and dual problems have the property that they are related via the concept of *duality*. There are two concepts of duality, one being *weak duality* which holds for any SDP and says:

2.6.2. Proposition (Weak Duality). *For every semidefinite program (Φ, A, B) it necessarily holds that $\alpha \leq \beta$.*

As α is the supremum over all feasible solutions, this implies that every feasible solution to the primal problem gives a *lower bound* to the optimal value β and therefore $\beta \leq \langle B, Y \rangle$ for any feasible Y. Every feasible solution to the dual problem gives an upper bound to $\langle A, X \rangle \leq \alpha$ for any feasible X. This implies that *if* you can find feasible operators X, Y such that $\langle A, X \rangle = \langle B, Y \rangle$, then it must be that $\alpha = \beta$ and we find an *optimal* solution to our maximization problem. Normally, showing optimality of a solution for a certain optimization problem can be difficult or even impossible, but in this case we are immediately done if we find feasible solutions to the primal and dual problems that are equal.

Definition 2.6.1 can be extended to also include inequality constraints as follows [Wat18]:

$$
\begin{array}{rl@{\qquad}rl}
 & \textbf{Primal Problem} & & \textbf{Dual Problem} \\
\textbf{maximize:} & \langle A, X \rangle & \textbf{minimize:} & \langle B_1, Y_1 \rangle + \langle B_2, Y_2 \rangle \\
\textbf{subject to:} & \Phi_1(X) = B_1 & \textbf{subject to:} & \Phi_1^*(Y_1) + \Phi_2^*(Y_2) \succeq A \\
 & \Phi_2(X) \leq B_2 & & Y_1 \in \mathrm{Herm}(\mathcal{Y}) \\
 & X \in \mathrm{Pos}(\mathcal{X}). & & Y_2 \in \mathrm{Pos}(\mathcal{Y}).
\end{array}
$$

2.6.3. Example (Finding optimal PPT Measurement Operators).
As mentioned before, one can use SDPs to find optimal POVM measurements. In this example we will use the SDP formalism to find optimal POVM measurements that have the extra restriction that they have Positive Partial-Transpose (PPT). A partial transpose over two subsystems A, B of some larger system $\mathbb{Z}_{AB}$ transposes the B part. We say an operator has positive partial transpose if $Z_{AB}^{T_B} \succeq 0$. The Peres–Horodecki criterion tells us that if a quantum state has positive partial transpose, then it must be separable [Per96, Hor97]. Similarly, the set of all operators that have positive partial transpose is a superset of all operators that are separable, which is a superset of all LOCC operators.

We will now give an example of an SDP for finding an optimal POVM measurement that discriminates between two inputs ρ_0, ρ_1 that are sent with equal probability $1/2$, where the POVM elements have to be PPT over some partition A, B of our quantum inputs.

$$
\begin{array}{rl}
 & \textbf{Primal Problem} \\
\textbf{maximize:} & \frac{1}{2}\,\mathrm{Tr}[\Pi_0 \rho_0 + \Pi_1 \rho_1] \\
\textbf{subject to:} & \Pi_0 + \Pi_1 = \mathbb{1}_{AB} \\
 & \Pi_k \in \mathrm{PPT}(\mathsf{A} : \mathsf{B}), \quad k \in \{0, 1\} \\
 & \Pi_k \succeq 0, \quad k \in \{0, 1\}
\end{array}
$$

We can write this in the standard form of Definition 2.6.1 by defining the following block matrices:

$$X = \begin{pmatrix} \Pi_0 & 0 \\ 0 & \Pi_1 \end{pmatrix}, A = \frac{1}{2}\begin{pmatrix} \rho_0 & 0 \\ 0 & \rho_1 \end{pmatrix}. \tag{2.42}$$

Note that if $X \succeq 0$ we have both $\Pi_0 \succeq 0$ and $\Pi_1 \succeq 0$. We take $\Phi_1(M) = \sum_i M_i$ to be the map that sums the diagonal blocks, and we take $\Phi_2(M)$ to be the map that sends every block to minus their partial transpose, then

$$\Phi_2(X) = \begin{pmatrix} -\Pi_0^{T_B} & 0 \\ 0 & -\Pi_1^{T_B} \end{pmatrix}. \tag{2.43}$$

Then if $\Phi_2(X) \preceq 0$ we have $\Pi_0^{T_B} \succeq 0$ and $\Pi_1^{T_B} \succeq 0$. The map Φ_1 is clearly a Hermiticity-preserving linear map, as we must have that all the blocks are Hermitian if the input is Hermitian. Map Φ_2 is linear, and to see it is Hermiticity-preserving note that for any Hermitian matrix $(C^{T_B})^\dagger = (C^\dagger)^{T_B} = C^{T_B}$. We thus get the following primal and corresponding dual:

	Primal Problem		**Dual Problem**
maximize:	$\langle A, X \rangle$	**minimize:**	$\mathrm{Tr}[Y_1]$
subject to:	$\Phi_1(X) = \mathbb{1}$	**subject to:**	$\Phi_1^*(Y_1) + \Phi_2^*(Y_2) \succeq A$
	$\Phi_2(X) \leq 0$		$Y_1 \in \mathrm{Herm}(\mathcal{Y})$
	$X \in \mathrm{Pos}(\mathcal{X})$.		$Y_2 \in \mathrm{Pos}(\mathcal{Y})$.

The adjoint operator of summing the diagonal blocks is multiplication with the identity-matrix, and the adjoint of the partial transpose is itself. We write Y_2 as a block matrix $\begin{pmatrix} Q_{00} & Q_{01} \\ Q_{10} & Q_{11} \end{pmatrix}$. Then we can rewrite the first constraint to:

$$\begin{gathered} \Phi_1^*(Y_1) + \Phi_2^*(Y_2) \succeq A \Leftrightarrow \\ \begin{pmatrix} Y_1 & 0 \\ 0 & Y_1 \end{pmatrix} - \begin{pmatrix} Q_{00}^{T_B} & Q_{01}^{T_B} \\ Q_{10}^{T_B} & Q_{11}^{T_B} \end{pmatrix} \succeq \frac{1}{2}\begin{pmatrix} \rho_0 & 0 \\ 0 & \rho_1 \end{pmatrix} \Leftrightarrow \\ \begin{pmatrix} Y_1 & 0 \\ 0 & Y_1 \end{pmatrix} - \begin{pmatrix} Q_{00}^{T_B} & Q_{01}^{T_B} \\ Q_{10}^{T_B} & Q_{11}^{T_B} \end{pmatrix} - \frac{1}{2}\begin{pmatrix} \rho_0 & 0 \\ 0 & \rho_1 \end{pmatrix} \succeq 0. \end{gathered} \tag{2.44}$$

If a block matrix is positive semidefinite, then it is also positive semidefinite if its off-diagonal blocks are set to zero. Taking the optimal solution Y_1, Y_2, we then see that if we set the off-diagonal blocks of Y_2 to zero, the first constraint is still satisfied and the solution does not change. The final constraint is also satisfied since if $\begin{pmatrix} Q_{00} & Q_{01} \\ Q_{10} & Q_{11} \end{pmatrix} \succeq 0$, then we also have $\begin{pmatrix} Q_{00} & 0 \\ 0 & Q_{11} \end{pmatrix} \succeq 0$. As the objective does not depend on Y_2, we see that Y_2 with its off-diagonal blocks set to zero is also an optimal solution. This means we can also optimize over the smaller set of matrices Y_2 that have off-diagonal blocks set to zero. Thus we can further simplify our dual to get:

$$
\begin{array}{rl}
 & \textbf{Dual Problem} \\
\textbf{minimize:} & \mathrm{Tr}[Y] \\
\textbf{subject to:} & Y - Q_i^{T_B} - \rho_i/2 \succeq 0, \ \text{for } i \in \{0,1\} \\
 & Y \in \mathrm{Herm}(\mathcal{Y}) \\
 & Q_i \in \mathrm{Pos}(\mathcal{Y}), \ \text{for } i \in \{0,1\}.
\end{array}
$$

A particular nice property about the dual in this form is that we can try to find Q_i for every i individually. Since any feasible solution to the dual problem upper bounds the optimal primal value, we get upper bounds to the optimal state-discrimination probability over all POVM measurements that have positive partial transpose. Sometimes, our intuition says that a particular measurement is clearly optimal, but there is no way to actually prove this. In this SDP framework, if you want to show that some POVM measurement (which is a feasible solution to the primal) is optimal, you just need to find a single feasible solution to the dual that has the same value, and you are done. SDPs can also be solved numerically, and numerical solvers can show (numerical) optimality by finding feasible primal and dual solutions.

Chapter 3

SWAP Test Protocol and PPT Attackers

Loss of inputs can be detrimental to the security of quantum position verification (QPV) protocols, as it may allow attackers to not answer on all played rounds, but only on those they perform well on. In this chapter, we study *loss-tolerant* QPV protocols. We propose a new fully loss-tolerant protocol $\mathrm{QPV}_{\mathsf{SWAP}}$, based on the SWAP test, with several desirable properties. The task of the protocol, which could be implemented using only a single beam splitter and two detectors, is to estimate the overlap between two input states. By formulating possible attacks as a semidefinite program (SDP), we prove full loss tolerance against unentangled attackers restricted to local operations and classical communication, and show that the attack probability decays exponentially under parallel repetition of rounds. Furthermore, we propose an easy experimental setup for the protocol, and argue that such an implementation is realistic in practice.

This chapter is based on the paper "Towards practical and error-robust quantum position verification" by Rene Allerstorfer, Harry Buhrman, Florian Speelman, and Philip Verduyn Lunel [ABSV22b].

3.1 Introduction

When we consider the implementation for a position verification protocol, there are two major things to consider. Firstly, we would like the protocol to be secure in some security model. Secondly, we want to be able to actually implement the protocol experimentally. Since we know that *any* protocol can be broken if a coalition of attackers pre-shares enough entanglement. A natural question is therefore whether some QPV protocols can be proven secure against attackers that share a limited amount of entanglement or even none at all. Since it is hard to generate entanglement, it is already interesting to study whether protocols are secure against adversaries that are very limited in their access to pre-shared entangled states.

For instance, the QPV_{BB84} protocol [KMS11], inspired by the BB84 quantum key-distribution protocol, involves only a single qubit sent by $\mathsf{V_A}$, in the state $|0\rangle$, $|1\rangle$, $|+\rangle$, or $|-\rangle$, and the choice of basis sent by $\mathsf{V_B}$. Even though this protocol is insecure against attackers sharing a single EPR pair [LL11], security can be proven against unentangled attackers [BCF⁺14], so that $\Theta(n)$ entanglement is required to break the n-fold parallel repetition [TFKW13, RG15]. At the current technological level, such protocols are interesting to analyze and would already give a super-classical level of security if implemented in practice.

Additionally, other protocols have been proposed [KMS11, CL15, Unr14, BCS22], that combine classical and quantum information in interesting ways, sometimes requiring intricate methods to attack [BFSS13, Spe16a, OCCG20].

Unfortunately, implementing many of the mentioned protocols would run into large obstacles: the quantum information involved would have to be sent at the speed of light, i.e., using photons, and in realistic experimental setups, a large fraction of photons will be lost and errors occur. Compensating for this in the most natural way, by ignoring rounds whenever the prover claims that a photon was lost in transmission, lets attackers break these protocols because they are not fully loss-tolerant. For example, in the QPV_{BB84} attackers can simply guess the basis, and if they guess wrong, they declare a loss. This perfectly breaks the protocol with only a loss rate of 50%.

A second important point is that the operations of the honest prover should be easily implementable. Ideally, we wish for his operations to be almost instantaneous. In our contribution, we study loss-tolerant QPV by presenting a new fully loss-tolerant protocol where the quantum operations of the prover are completely passive, making his operations very fast. We give a comprehensive security analysis in the theoretical setting showing that the protocol is secure against a limited amount of entanglement and propose an experimental setup that lies within the reach of current technology.

Loss tolerance in QPV. Throughout, we will use η as rate of transmission, i.e., the probability that an quantum message arrives in realistic protocols. We will distinguish two types of loss tolerance that we might require schemes to satisfy.

The first, *partial loss tolerance*, refers to a protocol that is secure for some values $\eta \geq \eta_{\text{threshold}}$, meaning that the honest parties have a maximum level of allowed loss. Security is only guaranteed in a situation where a high enough fraction of the rounds are played. If significantly more photons than this threshold are lost, then the protocol will have to abort. Examples of partial loss-tolerant schemes are extensions of $\mathrm{QPV}_{\mathrm{BB84}}$ to more bases [QS15, Spe16b], that are secure against unentangled attackers in an environment with some loss.[1]

Full loss tolerance is achieved when a protocol is secure, irrespective of the loss rate. In particular, the protocol stays secure when conditioning on those rounds where the prover replied, fully ignoring rounds where a photon is lost. The protocol by Lim, Xu, Siopsis, Chitambar, Evans, and Qi [QLL$^+$15, LXS$^+$16], the first fully loss-tolerant protocol, consists of $\mathsf{V_A}$ and $\mathsf{V_B}$ both sending a qubit, and having the prover perform a Bell measurement on both, broadcasting the measurement outcome. This protocol is secure against unentangled attackers, no matter the loss rate.

In this Chapter we advance the study of loss-tolerant QPV with the following results:

- We present a new fully loss-tolerant protocol: $\mathrm{QPV}_{\mathsf{SWAP}}$, which is based on the SWAP test [BCWW01]. The new protocol compares favorably to Lim et al.'s protocol [LXS$^+$16] in terms of ease of implementation using linear optics, by requiring only a single, non-polarizing beam splitter – the Hong-Ou-Mandel effect can be viewed as equivalent to the SWAP test [JAC04, GECP13] so that, physically speaking, our protocol is based on two-photon interference.[2]

- We prove fully loss-tolerant security by formulating possible attacks as a semi-definite program (SDP), and show that the protocol is secure against unentangled attackers who can communicate only classically.

  Additionally, we show that the attack probability decays exponentially under *parallel repetition*: when attackers respond to a size-k subset out of n parallel rounds, pretending photon loss on the other inputs, their probability of a successful attack still decays exponentially in k. Such a parallel repetition is not known for the protocol of [LXS$^+$16], and this is the first parallel repetition theorem for fully loss-tolerant QPV. We obtain this result by constructing an SDP formulation of the n-fold parallel repetition

[1] This notion will be satisfied to a small level even by schemes that are not designed to be loss tolerant, simply by having some error-robustness. The basic $\mathrm{QPV}_{\mathrm{BB84}}$ scheme can directly be seen to be partially loss tolerant for loss below $\frac{1}{2} - \frac{1}{2\sqrt{2}}$, and the simplest attack that uses loss only works when the loss is above $\frac{1}{2}$.

[2] The protocol uses two input photons, one generated by each verifier.

of the problem, constructing a dual of this SDP for variable n, and then finding a point in the generalized dual problem.

- We show that the SWAP test can be perfectly simulated with local operations and one round of classical communication if one maximally entangled state is pre-shared. Hence $O(n)$ EPR pairs are sufficient for an entanglement attack on our n-round protocol. We also show that at least $\sim 0.065n$ EPR pairs are necessary.

- Furthermore we propose an experimental setup using beam splitters and photon detectors. We distinguish between two different detector setups. In the one case we use photon number resolving detectors, which allow to have a higher precision because we can discard rounds in which one photon was lost more easily. In a practical scenario, these detectors might be too difficult to implement. Therefore, we also propose a setup with two additional beam splitters and four click/no-click detectors, which achieves partial number resolution and is more readily available and easier to implement.

3.2 The QPV$_{\mathsf{SWAP}}$ protocol

We denote parties in QPV protocols by letters A, B, etc. and their quantum registers as $A_1 \cdots A_n$, $B_1 \cdots B_n$ and so on, respectively. Sometimes we may refer to "all registers party X holds" just by X, giving expression like $\mathrm{Pos}(\mathsf{A} \otimes \mathsf{B})$, for example. The partial transposition of an operator P with respect to B is denoted by $P^{T_{\mathsf{B}}}$. The set of PPT-measurements[3] on two subsystems held by parties A and B, respectively, is $\mathrm{PPT}(\mathsf{A} : \mathsf{B})$. We define the protocol QPV$_{\mathsf{SWAP}}$, depicted in the space-time diagram in Figure 3.1, as follows.

1. Verifiers $\mathsf{V_A}$ and $\mathsf{V_B}$ agree on two uniformly Haar random qubits $|\psi\rangle, |\phi\rangle$ such that they are either equal or orthogonal (up to some global phase) with equal probability $\frac{1}{2}$. Then $\mathsf{V_A}$ prepares the state $|\psi\rangle$ and $\mathsf{V_B}$ prepares $|\phi\rangle$. Each verifier sends their state to P such that they arrive there simultaneously.

2. The honest party P applies the SWAP test, see Preliminaries 2.5, on the two quantum inputs as soon as they arrive at P. This yields an output bit $z \in \{0, 1, \varnothing\}$, indicating P's measurement result or possibly a "loss" event. Then P immediately sends z to both verifiers $\mathsf{V_A}$ and $\mathsf{V_B}$.

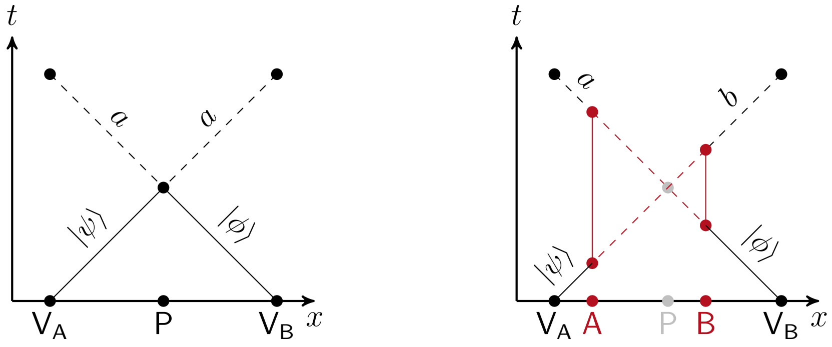
3. The verifiers check if they receive an answer in time and compare what they received. If they got different bits, or if at least one of their bits arrived too

[3] I.e. sets of positive semi-definite operators adding up to the identity, whose partial transposes are positive semi-definite as well.

early/late, they abort and reject. Otherwise both verifiers add z to their lists of answers.

4. After having completed some number of rounds with a conclusive answer $z \in \{0, 1\}$, sequentially or in parallel, the verifiers stop sending inputs, check if the rate of $\varnothing$ symbols is close enough to what is expected from P (they can estimate some answer rate $1 - \eta$ that is expected), discard any rounds with answer $\varnothing$ and proceed to check if the sets of conclusive answers to see if the answers correspond to those that one can expect from the SWAP test.

5. Only if they have received the same answer in time in every single round and if the answers correspond to the statistics of the SWAP test, they accept. Otherwise, they reject.



(a) Point of view of honest prover. (b) Point of view from attackers.

Figure 3.1: Space-time diagram of the $\mathrm{QPV}_{\mathsf{SWAP}}$ protocol. In the figure on the left, the situation without any attackers is shown, both messages from the verifiers are sent to P. In the figure on the right, the situation is shown with attackers that intercept the messages. We assume that all information, quantum (—) and classical (- - -), travels at the speed of light. For graphical simplicity, we have placed P exactly in the middle of $\mathsf{V_A}$ and $\mathsf{V_B}$ (which is not necessary for the purposes of QPV). The attackers, who are not at position P, would like to convince the verifiers that they are at P. Note that to have any chance of winning, attackers need to produce $a = b$.

In essence the task in this protocol is to estimate the overlap of the input states. This is independent of the dimension or nature of the input states, making the protocol very flexible. To attack this protocol, it is evident that there need to be at least two attackers due to the timing constraint. A coalition of attackers has to position at least one party A between $\mathsf{V_A}$ and P and one party B between P and $\mathsf{V_B}$. Since the SWAP test is a joint operation on two quantum states, spatially separated attackers cannot apply the SWAP test, unless they have access to pre-shared entanglement. We will show that if the inputs are qubit states, a single round of the SWAP test can be attacked with a single EPR pair.

Although there exists a perfect attack that uses entanglement, from a practical perspective, it is still hard for attackers to prepare and distribute entanglement. It is relatively much easier for the verifiers to play a round of the Swap test protocol than for attackers to attack a round with an EPR pair. As the verifiers just need to send random quantum states, and do not need any quantum memory. Therefore, the case where the attackers have no pre-shared entanglement and are restricted to classical communication is still interesting.

To assess the security of this protocol we will consider the single-round security of the protocol as well as the parallel repetition setting. One could expand on the notion of security and perform a full statistical analysis of the answers as was done in [ABSV22b], in which the distribution of the answers of an honest prover and attacker was compared, but this goes beyond the scope of this chapter. At its core, its security relies on the single round being secure, which we will focus on here.

When we take two Haar random qubits that are either equal or orthogonal we can write the joint density matrix nicely as projectors to the symmetric and antisymmetric subspaces $\{\Pi_{\text{sym}}, \Pi_{\text{asym}}\}$ [Wat18]. As a convention, we write ρ_0 for the equal inputs, and ρ_1 for the orthogonal inputs. We see that if the verifiers take two equal Haar random states, they are taking a uniform state from the symmetric subspace:

$$\rho_0 = \int (U \otimes U) \left|\psi\psi\right\rangle \left\langle\psi\psi\right| (U \otimes U)^\dagger \, \mathrm{d}\mu(U) = \frac{\Pi_{\text{sym}}}{3}, \tag{3.1}$$

here the division by 3 is the dimension of the symmetric subspace for qubits, which is spanned by the three symmetric Bell states $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle\}$. When we take two states $|\psi\rangle, |\phi\rangle$ that are orthogonal ($|\langle\psi|\phi\rangle = 0$), then we see that the state has both a symmetric part and an antisymmetric part:

$$\rho_1 = \int (U \otimes U) \left|\psi\phi\right\rangle \left\langle\psi\phi\right| (U \otimes U)^\dagger \, \mathrm{d}\mu(U) = \frac{1}{2}\frac{\Pi_{\text{sym}}}{3} + \frac{\Pi_{\text{asym}}}{2}, \tag{3.2}$$

where the antisymmetric subspace for qubits is just spanned by the antisymmetric Bell state $|\Psi^-\rangle$.

One can see that the two different inputs ρ_0, ρ_1 are not orthogonal to each other, thus they cannot be distinguished perfectly. The measurement that has the highest probability to distinguish the two inputs, when they are sent with equal probability $\frac{1}{2}$, is the SWAP test, which succeeds with overall probability $\frac{3}{4}$. When we do not send both inputs with equal probability one can show that for most input distributions the SWAP test is still optimal, unless we start sending orthogonal states with such high probability that the overall best strategy is just to always output 'unequal' [BGLW24].

3.2.1 Entanglement Attack

Before we show security of the protocol against unentangled attackers, we show that one can actually attack the protocol perfectly using a single EPR pair. Firstly, note that the symmetric and antisymmetric space for qubits are spanned by the four Bell states. The three symmetric Bell states $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle\}$ span the symmetric subspace, and the antisymmetric Bell state $\{|\Psi^-\rangle\}$ spans the antisymmetric subspace. As the SWAP test distinguished the symmetric and antisymmetric subspaces, one can the measurement outcome of a Bell state measurement to the measurement outcome of the SWAP test, simply by answering 'symmetric' whenever the measurement outcome was a symmetric Bell state, and 'antisymmetric' otherwise.

Two attackers can apply a Bell state measurement using only a single EPR pair; therefore, the SWAP test also takes one EPR pair. Two attackers A, B who receive as an input one of the four Bell states can apply a Bell state measurement as follows:

- We can write any Bell state as a combination of Pauli operators on a single local qubit. Thus, the input state of the attackers can be written as $(\mathbb{1} \otimes X^a Z^b) |\Phi^+\rangle_{AB}$, $(a, b) \in \{0, 1\}$. Here, the attackers task is to answer a, b to the verifiers using a single round of communication, as these bits determine the input Bell state.

- Attacker A teleports her qubit to B using their shared EPR pair. B receives the qubit of A but with some Pauli gates applied, determined by the measurement outcome (a^*, b^*) of A. Then B holds the state

$$(\mathbb{1} \otimes X^{a^*} Z^{b^*} X^a Z^b) |\Phi^+\rangle_B = -(\mathbb{1} \otimes X^{a^* \oplus a} Z^{b^* \oplus b}) |\Phi^+\rangle_B, \qquad (3.3)$$

  where we have used that $XZ = -ZX$. This global phase does not affect the measurement outcome of the state.

- Then B applies a Bell state measurement to his qubits and learns $a^* \oplus a$ and $b^* \oplus b$. Since A knows a^* and b^*, both attackers forward their (classical) measurement outcome bits to each other using their single round of simultaneous communication. Both attackers can now determine a, b, which corresponds to the Bell state they received as an input, and they answer on time correctly to both verifiers.

3.2.2 Security of QPV$_{\textsf{SWAP}}$ Protocol

In this setting, there is the notion of a correct answer. We will show that there is a finite gap in the success probability of testing for equality between adversaries restricted to LOCC operations and an honest prover who can apply entangling measurements. Extending this single-round protocol to n rounds played in parallel, we will also show that the best strategy for adversaries is to simply apply the optimal single round strategy to every round individually, which shows *strong parallel repetition* for $\mathrm{QPV}_{\mathsf{SWAP}}$. Furthermore, we show that in both cases there is no advantage for the attackers if they have the ability to declare loss on rounds, i.e. the probability of success conditioned on answering is independent of loss. The security of the protocol lies in the fact that an honest prover at his claimed position can apply entangling operations to the two incoming qubits and has a strictly higher probability of answering the question correctly than spatially separated adversaries who are restricted to single round LOCC operations. The loss-tolerant property of the protocol intuitively comes from the fact that all inputs are quantum and there is no way to guess any classical information beforehand.

In general, the operation that has the highest probability of generating the correct answer is the SWAP test [BBD+97, BCWW01], and it gives a success probability:

$$p_{\text{succ}}(\text{SWAP test}) \;=\; 3/4. \tag{3.4}$$

We will show that the best strategy for LOCC adversaries gives at most a success probability of $p_{\text{succ}}^{\max}(\text{LOCC}) = 2/3$. Since attackers return only a classical bit and they discard their post-measurement state, the most general type of measurement the attackers perform is a *positive-operator-valued measure* (POVM). The attackers' success probability for a given admissible POVM strategy $\Pi = \{\Pi_0, \Pi_1\}$ is then given by

$$p_{\text{succ}}(\Pi) := \frac{1}{2}\,\mathrm{Tr}[\Pi_0\rho_0 + \Pi_1\rho_1]. \tag{3.5}$$

Maximizing over all two-qubit LOCC measurements Π^{LOCC} would give us the best probability of success of the attackers. However, characterizing and maximizing over LOCC strategies is a mathematically complex task. We follow the method used in [LXS+16], and maximize our problem over the set of all positive partial transpose (PPT) operations. Since PPT measurements are a proper superset of LOCC measurements, any maximal success probability optimized over PPT measurements immediately upper bounds the success probability of all LOCC measurements. Furthermore, the PPT condition can be represented by a set of linear and positive semidefinite conditions [Cos13] which enables us to write down the maximization problem as a semidefinite program (SDP) [VB96]. SDPs always fulfill *weak duality* which means that any feasible solution to the dual problem upper bounds any feasible solution to the primal problem. This allows us to find exact solutions to the optimization problem if the values of the primal problem and dual problem coincide. In our case, the SDP that maximizes the best attack is as follows:

Primal Problem

$$\begin{aligned}\textbf{maximize:}\quad & \frac{1}{2}\operatorname{Tr}[\Pi_0\rho_0+\Pi_1\rho_1]\\ \textbf{subject to:}\quad & \Pi_0+\Pi_1=\mathbb{1}_{2^2}\\ & \Pi_k\in \mathrm{PPT}(\mathsf{A}:\mathsf{B}),\quad k\in\{0,1\}\\ & \Pi_k\succeq 0\quad k\in\{0,1\}\end{aligned}$$

Dual Problem

$$\begin{aligned}\textbf{minimize:}\quad & \operatorname{Tr}[Y]\\ \textbf{subject to:}\quad & Y-Q_i^{T_{\mathsf{B}}}-\rho_i/2\succeq 0,\quad i\in\{0,1\}\\ & Y\in \mathrm{Herm}(\mathsf{A}\otimes\mathsf{B})\\ & Q_i\in \mathrm{Pos}(\mathsf{A}\otimes\mathsf{B}),\quad i\in\{0,1\}.\end{aligned}$$

The primal problem implies a lower bound and the dual problem an upper bound to $p_{\text{succ}}^{\max}(\Pi^{\text{PPT}})$. We find an exact optimal solution to the SDP of $2/3$ (see Appendix for the analytic solutions 3.A.1), giving an upper bound of the success probability optimized over all LOCC measurements of

$$p_{\text{succ}}^{\max}(\Pi^{\text{LOCC}})\leq\frac{2}{3}. \tag{3.6}$$

The input states ρ_0 and ρ_1 have the exact same mixed state matrices as the result of uniformly choosing a mutually unbiased basis and sending either equal or orthogonal states (from the chosen basis) to P. This indicates an optimal LOCC strategy. Assume the incoming qubits are encoded in MUB b, and that the attackers choose a random MUB b', measure both incoming qubits in the basis b', send the measurement outcome to each other, and return equal if the measurement outcomes are equal and unequal otherwise. Then their probability of success is exactly $2/3$:

$$\begin{aligned}\mathbb{P}(\text{success})&=\mathbb{P}(b'=b)\mathbb{P}(\text{success}|b'=b)+\mathbb{P}(b'\neq b)\mathbb{P}(\text{success}|b'\neq b)\\ &=\frac{1}{3}\cdot 1+\frac{2}{3}\cdot\frac{1}{2}=\frac{2}{3}.\end{aligned}$$

This attack strategy uses only local measurements and a single round of communication, so it is a valid single-round LOCC operation. Thus, we find that the upper bound in (3.6) over LOCC measurements is in fact a tight bound attained by LOCC.

We have shown that the probability of success for identifying if the given inputs were equal or not for the QPV$_{\mathsf{SWAP}}(0,1)$ protocol is strictly lower for attackers restricted to LOCC measurements than for an honest verifier who can apply entangling operations (2/3 versus 3/4 respectively). Over sequential multi-round protocols, where we only perform a new run of the protocol after the previous is finished, the verifiers can increase the precision of detecting LOCC attackers.

3.2.3 Strong Parallel Repetition of $\mathrm{QPV}^n_{\mathsf{SWAP}}$

Another desirable property is whether we can extend the single-round protocol to a general n-round parallel protocol, where the verifiers send n qubits from both sides to form the density matrix $\rho_s = \rho_{s_0} \otimes \rho_{s_1} \otimes \cdots \otimes \rho_{s_{n-1}}$ for $s \in \{0,1\}^n$. Note that the security does not follow naively from the single-round security proof, since attackers can now, in principle, take blocks of inputs and apply entangling operations on them. We will prove that for the $\mathrm{QPV}_{\mathsf{SWAP}}$ protocol strong parallel repetition does indeed hold, i.e. the probability of success of winning n rounds decreases as $(2/3)^n$, implying that the best strategy for attackers is to simply attack each round individually. Again we can write down the problem as an SDP optimization task, where we optimize over all PPT operations on the $2n$ qubits the attackers receive.

Primal Problem

$$\begin{aligned}
\textbf{maximize:}\quad & \frac{1}{2^n} \sum_{s\in\{0,1\}^n} \mathrm{Tr}[\Pi_s \rho_s] \\
\textbf{subject to:}\quad & \sum_{s\in\{0,1\}^n} \Pi_s = \mathbb{1}_{2^{2n}} \\
& \Pi_s \in \mathrm{PPT}(\mathsf{A}:\mathsf{B}), \quad s \in \{0,1\}^n \\
& \Pi_s \succeq 0, \ \text{for} \quad s \in \{0,1\}^n
\end{aligned}$$

Dual Problem

$$\begin{aligned}
\textbf{minimize:}\quad & \mathrm{Tr}[Y] \\
\textbf{subject to:}\quad & Y - Q_s^{T_{\mathsf{B}}} - \rho_s/2^n \succeq 0, \quad s \in \{0,1\}^n \\
& Y \in \mathrm{Herm}(\mathsf{A} \otimes \mathsf{B}) \\
& Q_s \in \mathrm{Pos}(\mathsf{A} \otimes \mathsf{B}).
\end{aligned}$$

In Appendix 3.A.2 we find an explicit analytical solution to the dual problem. The solution is non-trivial and depends on the specifics of the $\mathrm{QPV}_{\mathsf{SWAP}}$ protocol, so it does not generalize naturally to strong parallel repetition results for other protocols. The solution yields a value of $(2/3)^n$, which bounds the probability of success under LOCC measurements by $(2/3)^n$. A feasible solution to the primal problem is to fill in the single-round solution n times, and this has success probability $(2/3)^n$. Since this strategy coincides with the previously mentioned single-round LOCC measurement applied to each of the individual rounds of ρ_{s_i}, we find that the upper bound of $(2/3)^n$ is again attained by a LOCC measurement and tight. Thus, we show strong parallel repetition for the QPV$_{\mathsf{SWAP}}$ protocol against attackers restricted to LOCC operations.

Strong parallel repetition is a useful result for the practical implementation of QPV protocols. First of all, it implies that when playing multiple rounds we don't have to wait until a single round is finished, thus simplifying the timing constraints of multiple rounds, and it allows the verifiers to not have to wait till the first round is over before starting the next. Secondly, it implies a linear lower bound on the entanglement adversaries need to attack the protocol perfectly. To get this lower bound, we use an argument already mentioned in Lemma V.3 in [BK11]. This lemma relates the probability that the verifiers accept the total set of answers over n rounds, $\varepsilon_{\text{succ}}(\tau_{AB})$, of the attackers as sufficient *with* some pre-shared entangled state τ_{AB} to the probability of accepting attackers without pre-shared entanglement as follows:

$$\varepsilon_{\text{succ}}(\tau_{AB}) \leq \dim(A)\dim(B)\varepsilon_{\text{succ}}(\emptyset), \tag{3.7}$$

where $\emptyset$ signifies the absence of entanglement. The idea behind the lemma is that a pre-shared entangled state could be replaced by a maximally mixed state, which has some overlap with the original state. For example, an EPR pair has overlap $\frac{1}{4}$ with the maximally entangled state. Thus, if there exists an attack that uses very little entanglement, then one would also perform well with just shared randomness and no pre-shared entanglement.

Over n rounds the verifiers will send on average $n/2$ rounds with equal inputs, and $n/2$ rounds with orthogonal inputs. The honest prover will always answer correctly on the equal inputs and will be correct with prob $\frac{1}{2}$ on the unequal inputs. We know that over all n rounds the attackers have a probability of being correct of $(2/3)^n$. If the attackers have to be correct with probability $\frac{1}{2}$ half the time on all unequal inputs, they can only be correct on the equal inputs with probability at most $(\frac{5}{6})^{n/2}$. Since the honest prover is correct on all these rounds the attackers need to be as well if they want to fool the verifiers they need to answer all equal rounds correctly. Suppose that the verifiers pre-share m EPR pairs, then the lemma gives:

$$\varepsilon_{\text{succ}}(\tau_{AB}) \leq 2^{2m}\left(\frac{5}{6}\right)^{\frac{n}{2}}. \tag{3.8}$$

It follows that, in expectation,

$$\varepsilon_{\text{succ}}(\tau_{AB}) < 1 \qquad \text{as long as} \qquad m < \frac{1}{4}\log\left(\frac{4}{3}\right)n \approx 0.065n. \tag{3.9}$$

Thus, to break $\mathcal{O}(n)$ rounds in parallel one also needs at least $\mathcal{O}(n)$ pre-shared EPR pairs. Since we know of an attack that attacks a single round using a single EPR pair the $\mathcal{O}(n)$ pre-shared EPR pairs is actually tight.

3.2.4 Loss-Tolerance of $\mathrm{QPV}^n_{\mathsf{SWAP}}$ Protocol

In the previous section we have shown that the $\mathrm{QPV}_{\mathsf{SWAP}}$ protocol is secure against attackers restricted to LOCC attackers in the case where attackers have to answer in every round. However, in practice an honest prover will only answer on a fraction of the rounds played due to channel loss and imperfect measurements. In order to prove security against any coalition of attackers in the setting with channel loss, we must assume that attackers will never suffer any loss when they attack a protocol[4]. When classical information is sent, such as in the $\mathrm{QPV}_{\mathrm{BB84}}$ protocol [KMS11, BCF$^+$14], attackers may guess the classical information that is being sent. If they guess incorrectly, they discard the round and declare a loss ($\varnothing$), if they guess correctly, they can continue and successfully attack the protocol since the classical information is known to both attackers after communication. If the loss rate is high enough, attackers can hide their incorrect guesses in the loss declarations and the verifiers cannot distinguish the attackers from an honest prover. Note that in order to pretend a loss without being detected, attackers must declare a loss with equal probability on every input. To prove loss tolerance, we can incorporate loss in the SDP setting and show that the optimal solution of the SDP is independent of the loss, similar to the method in [LXS$^+$16].

We can relatively straightforwardly add the condition that attackers must mimic a certain loss rate $(1-\eta)$ on all inputs. We will show that in the parallel repetition case p_{succ} is independent of η when attackers either answer conclusively on all $2n$ inputs or don't answer at all. We formulate an SDP to maximize the probability of success conditioned on a conclusive answer $p^{\max}_{\mathrm{succ}}(n,\eta)$ in the n-round parallel repetition case ($n = 1$ corresponds to the previously studied single-round

[4] They could position themselves very close to the verifiers and have perfect communication channels, for example.

protocol).

Primal Problem

$$\begin{aligned}
\textbf{maximize:}\quad & \frac{1}{2^n\eta}\sum_{s\in\{0,1\}^n}\mathrm{Tr}[\tilde{\Pi}_s\rho_s]\\
\textbf{subject to:}\quad & \left(\sum_{s\in\{0,1\}^n}\tilde{\Pi}_s\right)+\tilde{\Pi}_\varnothing=\mathbb{1}_{2^{2n}}\\
& \mathrm{Tr}[\tilde{\Pi}_\varnothing\rho_s]=1-\eta,\quad s\in\{0,1\}^n\\
& \tilde{\Pi}_s\in\mathrm{PPT}(\mathsf{A}:\mathsf{B}),\quad s\in\{0,1\}^n\cup\varnothing\\
& \Pi_s\succeq 0,\ \text{for}\quad s\in\{0,1\}^n
\end{aligned}$$

Dual Problem

$$\begin{aligned}
\textbf{minimize:}\quad & \frac{\mathrm{Tr}[\tilde{Y}]-(1-\eta)\gamma}{\eta}\\
\textbf{subject to:}\quad & \tilde{Y}-\tilde{Q}_s^{T_\mathsf{B}}-\rho_s/2^n\succeq 0,\quad s\in\{0,1\}^n\\
& 2^{2n}(\tilde{Y}-\tilde{Q}_\varnothing^{T_\mathsf{B}})-\gamma\mathbb{1}_{2^{2n}}\succeq 0\\
& \tilde{Y}\in\mathrm{Herm}(\mathsf{A}\otimes\mathsf{B})\\
& \tilde{Q}_s\in\mathrm{Pos}(\mathsf{A}\otimes\mathsf{B}),\quad s\in\{0,1\}^n\cup\varnothing\\
& \gamma\in\mathbb{R}.
\end{aligned}$$

From the analysis in Appendix 3.A.3, we see that the solution of the SDP is again $(2/3)^n$, independent of η, upper bounding the attackers restricted to LOCC measurements. The strategy in which attackers apply with probability η the regular n-round parallel repetition attack and with probability $(1-\eta)$ discard everything again has conditional success probability $(2/3)^n$ so the bound is tight. By Proposition 3.2.1, we have that QPV$^n_{\mathsf{SWAP}}$ is tolerant against loss on any subset of rounds, establishing full loss tolerance.

We show in the following proposition that the property that p_{succ} remains independent of η when declaring a loss on either *all* rounds or none implies that p_{succ} is also independent of η when declaring a loss on any subset of rounds is allowed.

3.2.1. Proposition. *Any multi-round QPV protocol that fulfills strong parallel repetition security against adversaries restricted to LOCC operations and is tolerant against declaring loss on all n rounds, is also tolerant against declaring loss on any subset of rounds.*

Proof:
Suppose we have a secure n-round QPV protocol with strong parallel repetition.

Then the n-round success probability for attackers is $p_n = p_1^n$ for some single round probability p_1. Suppose we perform n rounds and we allow adversaries to only answer on k rounds and to declare a loss on the remaining $(n-k)$ rounds, and suppose that there is some attacking strategy S restricted to LOCC measurements that has a probability $p_S > p_1^k$ of being correct on this subset. We will show that this leads to a contradiction. Consider a protocol like the k-round protocol $\text{QPV}^k_{\mathsf{SWAP}}$, which is secure and loss tolerant on all rounds by assumption and has success probability $p_k = p_1^k$. Since individual rounds are product states, attackers may create $n-k$ independent extra rounds locally of which they can forget the answer. This creates an n-round protocol. The attackers can now apply their strategy S. With probability $1/\binom{n}{k}$ they get an answer on their initial k rounds that is correct with success probability p_S. And with probability $1-1/\binom{n}{k}$ they receive the wrong subset of k rounds, in which case the attackers declare a loss (on all rounds). This defines an LOCC attack with a conditional winning probability $p_S > p_1^k$ and loss rate of $1-1/\binom{n}{k}$, which contradicts our assumption that the maximal success probability of being correct on the k-round protocol is p_1^k for any loss. Therefore, for any subset of k rounds out of the total of n rounds, the maximal success probability p_k on this subset is p_1^k. □

3.3 Practical considerations of $\text{QPV}_{\mathsf{SWAP}}$

The SWAP test has been shown to be equivalent to the Hong-Ou-Mandel (HOM) interference measurement [HOM87] with just one 50/50 beam splitter and two photon detectors [JAC04, GECP13]. We call this the **BS** setup, as only a single beam splitter is used. If the photons bunch into one detector arm, the answer shall be “0”, if both detectors register a click it shall be “1”. However, for click/no-click detectors there is a problem with this simple setup, as signal loss can convert “1” answers to “0” answers. For high loss rates, one would always get $p_\beta(0) \approx 1$, irrespective of the overlap and even without further equipment errors because most of the time only one state will arrive. Hence, the **BS** setup will be insecure unless one uses number-resolution (NR) detectors. With these, single clicks at one detector get filtered out instead of delivering a wrong answer. NR detectors also filter out $k > 2$ click events so that the ideal SWAP test distribution of is fairly well preserved, even with experimental errors. Creating true NR detectors is an active field of research, but at the moment they are still at an early stage and somewhat hard to operate [CHE+21, ESM+21]. We therefore suggest using two further beam splitters and four click/no-click detectors to achieve probabilistic NR. We call this the **3BS** setup, as depicted in Figure 3.2.

We define the following decision rules for the honest prover (for one detection window, corresponding to a round of the protocol):

(**BS**) Answer “0” if D_1 xor D_2 clicks, answer “1” if (D_1, D_2) click, answer “∅” if

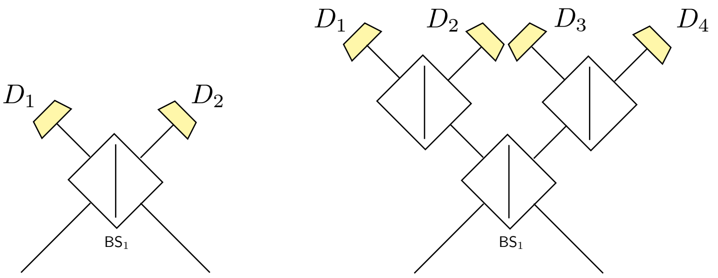


Figure 3.2: The detection setups **BS** (left) and **3BS** (right). The beam splitters are (R, T) and non-polarizing. Unless otherwise specified, the detectors D_i are conventional single-photon click/no-click detectors.

no click occurs.

(**3BS**) Answer “0” if two clicks in one arm after BS_1 are detected $((D_1, D_2)$ or $(D_3, D_4))$, answer “1” if two clicks in different arms are detected $((D_1, D_3)$, (D_1, D_4), (D_2, D_3) or $(D_2, D_4))$, else answer “$\varnothing$”.

This means that in the **3BS** setup we post-select entirely on 2-click events, giving us weak NR, but only with some probability.

In practice, no qubit or channel is perfect and we need to check under which conditions our protocol remains secure. To analyze the security in an experimental setting, the following quantities of the setup are of importance:

- Each verifier holds an imperfect single-photon source, characterized by the probability that at least one photon is emitted $\eta_{\text{source}} = \mathbb{P}(n > 0)$, the brightness $B = \mathbb{P}(n = 1)$ and the accidental pair production rate $p_{\text{pair}} = \mathbb{P}(n = 2)$, where n is the number of single photons. Accidental pair productions can make the protocol less secure.

- A communication channel between each verifier and the prover with a transmittance (at the prover) of η_{BS}[5]. We assume that both channels from $\mathsf{V_A}$ to P and from $\mathsf{V_B}$ to P have the same transmittance. Even though our protocol is secure against loss, one still needs to have enough conclusive rounds.

- The prover uses imperfect beam splitters with reflectance (amplitude) R and transmittance (amplitude) T as well as single-photon detectors characterized by a detection efficiency η_{det} (including loss between BS_1 and the detectors, as well as an imperfect intrinsic detection efficiency, per detector) and a dark count rate p_{dark} (per detector).

[5] The beam splitter at P is where quantum interference between the incoming photons happens.

- The final parameter is the overlap β between the input states at the prover. Assuming that the equipment of both verifiers is identical, we can regard the photons leaving the sources as indistinguishable except in the degree of freedom we use to encode our quantum states in. One simple example would be the photon polarization degree of freedom, such that $\beta = |\langle\psi|\phi\rangle|$ for polarization qubits $|\psi\rangle$ and $|\phi\rangle$. In practice, it may happen that a protocol round is started with a target overlap β, but the communication channel disturbs it to some $\tilde{\beta} = \beta + \delta$ with error $|\delta| > 0$.

A detailed further analysis goes beyond the scope of this chapter, but can be found in [ABSV22b]. With the considerations mentioned above, we conclude that an experimental implementation of $\mathrm{QPV}_{\mathsf{SWAP}}$ is possible with current technologies.

3.4 Discussion

We constructed and analyzed a new quantum position verification protocol, $\mathrm{QPV}_{\mathsf{SWAP}}$, and showed that it possesses several desirable properties. The protocol is easy to implement for an honest prover, whose setup consists only of a single beam splitter. It was shown that it is fully loss tolerant against LOCC attackers with no pre-shared entanglement, that it can be attacked with n pre-shared EPR pairs and that at least $\sim 0.065n$ pre-shared EPR pairs are necessary in the $\beta \in \{0, 1\}$ case. Ideally, we would have protocols that require a lot more entanglement to perfectly attack. However, we do not know of any QPV protocol that provably needs more than a linear amount of entanglement. In that sense, the SWAP test protocol is among the best protocols we have, especially considering it's among the easiest implementable protocols.

Moreover, the protocol fulfills strong parallel repetition when the attackers don't pre-share any entanglement and retains the loss tolerance even if all rounds are run in parallel. In addition, the flexibility and simplicity of the SWAP test, both theoretically and experimentally, make it an excellent candidate for practical QPV. However, we only prove security against attackers restricted to classical communication, which raises the question if a round of simultaneous quantum communication can be beneficial to the attackers. We will investigate this question in the next chapter and show that while quantum communication can help *some* protocols, the $\mathrm{QPV}_{\mathsf{SWAP}}$ protocol will remain secure.

3.A Appendices

3.A.1 Optimal PPT Measurements for $\mathrm{QPV}_{\mathsf{SWAP}}$ Protocol

We prove the upper bound of the success probability of answering the protocol correctly for adversaries restricted to PPT operations in equation (3.6). For simplification, we will refer to the equal case as the 0 case and unequal as the 1 case. The idea of the proof is to find analytical feasible solutions to the primal and dual problems of the SDP. In general, a feasible solution to the primal problem defines a lower bound to the maximization value, whereas a feasible solution to the dual problem defines an upper bound. This is the property of *weak duality*, which holds for any SDP [VB96]. In all of our further proofs we find feasible primal values and dual values that coincide and thus our solutions are optimal and we have *strong duality*.

From the density matrices we see that there is no difference between picking two random equal states or picking two equal states in a random mutually unbiased basis, see ρ_0. Similarly, picking two random orthogonal states or picking two orthogonal mutually unbiased basis (MUB) states is equal, see ρ_1. These become[6]

$$\rho_0 = \frac{1}{6}\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}, \qquad \rho_1 = \frac{1}{6}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & -1 & 0 \\ 0 & -1 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

It is useful to note that both density matrices ρ_0, ρ_1 are a mixture of unentangled states and thereby unentangled. Thus, by the Peres-Horodecki separability criterion, the partial transpose of ρ_0 and ρ_1 are positive semidefinite [Sim00]. The optimization over all strategies of the single round protocol is written as follows in an SDP:

$$\begin{aligned}
& \textbf{Primal Problem} \\
\textbf{maximize:}\quad & \frac{1}{2}\operatorname{Tr}[\Pi_0\rho_0 + \Pi_1\rho_1] \\
\textbf{subject to:}\quad & \Pi_0 + \Pi_1 = \mathbb{1}_{2^2} \\
& \Pi_k \in \mathrm{PPT}(\mathsf{A} : \mathsf{B}), \quad k \in \{0,1\} \\
& \Pi_k \succeq 0, \text{ for } k \in \{0,1\} \\
& \textbf{Dual Problem} \\
\textbf{minimize:}\quad & \operatorname{Tr}[Y] \\
\textbf{subject to:}\quad & Y - Q_i^{T_{\mathsf{B}}} - \rho_i/2 \succeq 0, \quad i \in \{0,1\} \\
& Y \in \mathrm{Herm}(\mathsf{A} \otimes \mathsf{B}) \\
& Q_i \in \mathrm{Pos}(\mathsf{A}, \mathsf{B}), \quad i \in \{0,1\}.
\end{aligned}$$

[6] Note that this is a slight change of notation with respect to the main text, where we used ρ_β for overlap β. Here, ρ_0 denotes the mixed state of sending identical states and ρ_1 denotes the one sending orthogonal states.

A feasible solution for the primal problem is

$$\Pi_0 = \frac{1}{3}\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}, \qquad \Pi_1 = \frac{1}{3}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & -1 & 0 \\ 0 & -1 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

with solution $\frac{1}{2}\operatorname{Tr}[\Pi_0\rho_0 + \Pi_1\rho_1] = 2/3$. These measurement projectors correspond to attackers choosing a random MUB to measure in and returning 0 if the measurement outcomes were equal and 1 otherwise, which is also a single-round LOCC strategy, and thus the PPT constraint is fulfilled. Indeed:

$$\begin{aligned} &\frac{1}{3}(|00\rangle\langle 00| + |11\rangle\langle 11| + |{+}{+}\rangle\langle {+}{+}| + |{-}{-}\rangle\langle {-}{-}| \\ &\qquad\qquad + |i^+i^+\rangle\langle i^+i^+| + |i^-i^-\rangle\langle i^-i^-|) = \Pi_0, \\ &\frac{1}{3}(|10\rangle\langle 10| + |01\rangle\langle 01| + |{-}{+}\rangle\langle {-}{+}| + |{+}{-}\rangle\langle {+}{-}| \\ &\qquad\qquad + |i^-i^+\rangle\langle i^-i^+| + |i^+i^-\rangle\langle i^+i^-|) = \Pi_1. \end{aligned}$$

A feasible solution to the dual problem is:

$$Y = \frac{\mathbb{1}_4}{6}, \quad Q_0 = 0 \succeq 0, \quad Q_1 = \frac{\mathbb{1}_4}{6} - \frac{\rho_1^{T_\mathsf{B}}}{2} = \frac{1}{12}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} = \frac{1}{6}|\Phi^+\rangle\langle\Phi^+| \succeq 0.$$

Which adhere to the constraints in the dual problem:

$$\begin{aligned} Y - Q_0^{T_\mathsf{B}} - \frac{\rho_0}{2} &= \frac{\mathbb{1}_4}{6} - \frac{\rho_0}{2} = \frac{1}{12}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \frac{1}{6}|\Psi^-\rangle\langle\Psi^-| \succeq 0 \\ Y - Q_1^{T_\mathsf{B}} - \frac{\rho_1}{2} &= \frac{\mathbb{1}_4}{6} - \left(\frac{\mathbb{1}_4}{6} - \frac{\rho_1}{2}\right) - \frac{\rho_1}{2} = 0 \succeq 0. \end{aligned}$$

Since also $Y \in \operatorname{Herm}(\mathsf{A} \otimes \mathsf{B})$ we get a feasible solution for the dual with value $\operatorname{Tr}[Y] = \frac{2}{3}$. Thus, we have a feasible solution of the primal and dual problem that both give the same value, so we conclude that the maximal probability of success for attackers under the PPT restriction is 2/3.

3.A.2 Optimal PPT Measurements for $\mathrm{QPV}^n_{\mathsf{SWAP}}$ Protocol

We will prove that the optimal probability of success for attackers in the n-round parallel repetition case is $(2/3)^n$. The SDP of the n-round parallel repetition protocol is given by:

$$\begin{aligned}
&\textbf{Primal Problem}\\
\textbf{maximize:}\ & \frac{1}{2^n}\sum_{s\in\{0,1\}^n}\mathrm{Tr}[\Pi_s\rho_s]\\
\textbf{subject to:}\ & \sum_{s\in\{0,1\}^n}\Pi_s = \mathbb{1}_{2^{2n}}\\
& \Pi_s \in \mathrm{PPT}(\mathsf{A}:\mathsf{B}),\quad s\in\{0,1\}^n\\
& \Pi_s \succeq 0,\ \text{for}\quad s\in\{0,1\}^n\\
&\textbf{Dual Problem}\\
\textbf{minimize:}\ & \mathrm{Tr}[Y]\\
\textbf{subject to:}\ & Y - Q_s^{T_\mathsf{B}} - \rho_s/2^n \succeq 0,\quad s\in\{0,1\}^n\\
& Y\in\mathrm{Herm}(\mathsf{A}\otimes\mathsf{B})\\
& Q_s\in\mathrm{Pos}(\mathsf{A}\otimes\mathsf{B}).
\end{aligned}$$

Here s is a bit string of length n, where s_i denotes the inputs of the i-th round, i.e.

$$\rho_s = \rho_{s_0}\otimes\cdots\otimes\rho_{s_{n-1}}. \tag{3.10}$$

Repeating the strategy of the single round protocol gives a feasible solution for the primal problem with success probability $(2/3)^n$. A feasible solution to the dual problem would yield an upper bound to the problem, but requires finding a general solution for the matrices Y, Q_s. We will give a general solution which is based on the educated guess that we can set Y to be the identity matrix with some proper normalization

$$Y = \frac{\mathbb{1}_{2^{2n}}}{2^{2n}}\left(\frac{2}{3}\right)^n = \frac{\mathbb{1}_{2^{2n}}}{6^n},\ \text{such that}\ \mathrm{Tr}[Y] = \left(\frac{2}{3}\right)^n. \tag{3.11}$$

We will construct a general feasible solution for Q_s for any string $s\in\{0,1\}^n$ from $Q_{T(s)}$ where $T(s)$ is the reversed sorted version of s.

First, we show a general solution for the $s = 0^n$ and $s = 1^n$ strings. A solution for the all-0 input case is $Q_{0^n} = 0 \succeq 0$. The first constraint for $s = 0^n$ in the dual problem of the SDP then reduces to

$$\frac{\mathbb{1}_{2^{2n}}}{6^n} - \frac{\rho_0^{\otimes n}}{2^n}. \tag{3.12}$$

The eigenvectors of ρ_0 are the four Bell states $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$, with respective eigenvalues $\{1/3, 1/3, 1/3, 0\}$, one can check this by hand. But this can also be seen from the fact that ρ_0 corresponds to a random symmetric state, and the symmetric subspace is spanned by the symmetric Bell states.

Then the eigenvalues of $\frac{\rho_0^{\otimes n}}{2^n}$ are $1/6^n$ or 0. Thus, the eigenvalues of (3.12) are either 0 or $1/6^n$ and (3.12) is positive, since it is also Hermitian.

For the $s = 1^n$ case we get the following.

$$Q_{1^n} = \frac{\mathbb{1}_{2^{2n}}}{6^n} - \frac{(\rho_1^{T_{\mathsf{B}}})^{\otimes n}}{2^n},$$

is feasible. The eigenvectors of $\rho_1^{T_{\mathsf{B}}}$ are again the Bell states, with respective eigenvalues $\{0, 1/3, 1/3, 1/3\}$. The eigenvectors of Q_{1^n} are all combinations of tensor products of the four Bell states. If one of these states is the $|\Phi^+\rangle$ state, the corresponding eigenvalue of Q_{1^n} is $(\frac{1}{6})^n$, otherwise the corresponding eigenvalue is 0. Since Q_{1^n} is also Hermitian and has only non-negative eigenvalues $Q_{1^n} \succeq 0$, as desired. The corresponding constraint in the dual problem of the SDP reduces to

$$\frac{\mathbb{1}_{2^{2n}}}{6^n} - \left(\frac{\mathbb{1}_{2^{2n}}}{6^n} - \frac{\rho_1^{\otimes n}}{2^n}\right) - \frac{\rho_1^{\otimes n}}{2^n} = 0 \succeq 0.$$

We see that for the inputs $s = 0^n$ and $s = 1^n$ for any n the values of the primal and dual coincide and the optimal probability of success is $(2/3)^n$.

The idea is now to use induction to get optimality of sorted strings, we note that we can add a '0' round to a valid solution via a tensor product. Suppose we have a valid solution Q_s for some $s \in \{0,1\}^n$, thus

$$Y - Q_s^{T_{\mathsf{B}}} - \rho_s/2^n \succeq 0. \tag{3.13}$$

And to this n-round protocol we add an extra round of equal inputs, so the input is now $\rho_s \otimes \rho_0$. We will show that

$$Q_{s,0} = Q_s \otimes \rho_0^{T_{\mathsf{B}}}/2, \tag{3.14}$$

is a valid solution for the $(n+1)$-round SDP. As $\rho_0^{T_{\mathsf{B}}} \succeq 0$ and $Q_s \succeq 0$ (by assumption), we have $Q_{s,0} \succeq 0$. Rewriting the first dual constraint we get

$$\begin{aligned}
\frac{\mathbb{1}_{2^{2n+2}}}{6^{n+1}} - Q_{s,0}^{T_{\mathsf{B}}} - \frac{\rho_s \otimes \rho_0}{2^{n+1}} &= \frac{\mathbb{1}_{2^{2n+2}}}{6^{n+1}} - Q_s^{T_{\mathsf{B}}} \otimes \frac{\rho_0}{2} - \frac{\rho_s \otimes \rho_0}{2^{n+1}} \\
&= \frac{\mathbb{1}_{2^{2n}}}{6^n} \otimes \frac{\mathbb{1}_4}{6} - Q_s^{T_{\mathsf{B}}} \otimes \frac{\rho_0}{2} - \frac{\rho_s \otimes \rho_0}{2^{n+1}} \\
&= \frac{\mathbb{1}_{2^{2n}}}{6^n} \otimes \frac{\rho_0 + \rho_1}{3} - Q_s^{T_{\mathsf{B}}} \otimes \frac{\rho_0}{2} - \frac{\rho_s \otimes \rho_0}{2^{n+1}} \\
&= \underbrace{\left(\frac{\mathbb{1}_{2^{2n}}}{6^n} - Q_s^{T_{\mathsf{B}}} - \frac{\rho_s}{2^n}\right) \otimes \frac{\rho_0}{2}}_{\mathbf{A}} + \underbrace{\frac{\mathbb{1}_{2^{2n}}}{6^n} \otimes \left(\frac{2\rho_1 - \rho_0}{6}\right)}_{\mathbf{B}}.
\end{aligned}$$

We see that part $\mathbf{A}$ is a tensor product of two positive semi-definite matrices, our starting point in (3.13) and $\rho_0/2$, so $\mathbf{A}$ is also positive semi-definite. Part $\mathbf{B}$ is Hermitian, and we can compute its eigenvalues explicitly. The eigenvectors of $\frac{2\rho_1-\rho_0}{6}$ are again the Bell states with respective eigenvalues $\{0,0,0,1/6\}$, so part $\mathbf{B}$ is positive semi-definite. Since sums of positive semi-definite matrices are positive semi-definite the whole constraint is positive semi-definite. Since for any number of rounds n we have a feasible solution for the $s=1^n$ case, by repeatedly adding the equal case, we can repeat the previous steps to get a feasible solution for any reversed sorted string 1^n0^k for all n,k, namely

$$Q_{1^n0^k} = Q_{1^n} \otimes \frac{(\rho_0^{T_\mathsf{B}})^{\otimes k}}{2^k}. \tag{3.15}$$

Now take some string $s \in \{0,1\}^n$, and let P_s be a unitary consisting only of 2-qubit SWAP operations that reverse sorts the n-rounds, such that $P_s\rho_sP_s^\dagger = \rho_{T(s)}$, and $P_s^\dagger = P_s$.

We can now write down the general solution of Q_s using the corresponding map P_s applied to the sorted version. Let $Q_s = (P_sQ_{T(s)}^{T_\mathsf{B}}P_s)^{T_\mathsf{B}}$, using the fact that P is a unitary matrix we then get for the corresponding constraint in the dual SDP:

$$\begin{aligned} Y - Q_s^{T_\mathsf{B}} - \rho_s/2^n \succeq 0 &\Leftrightarrow P_s(Y - Q_s^{T_\mathsf{B}} - \rho_s/2^n)P_s \succeq 0 \\ &\Leftrightarrow Y - P_sQ_s^{T_\mathsf{B}}P_s - \rho_{T(s)}/2^n \succeq 0 \\ &\Leftrightarrow Y - P_s((P_sQ_{T(s)}^{T_\mathsf{B}}P_s)^{T_\mathsf{B}})^{T_\mathsf{B}}P_s - \rho_{T(s)}/2^n \succeq 0 \\ &\Leftrightarrow Y - P_s(P_sQ_{T(s)}^{T_\mathsf{B}}P_s)P_s - \rho_{T(s)}/2^n \succeq 0 \\ &\Leftrightarrow Y - Q_{T(s)}^{T_\mathsf{B}} - \rho_{T(s)}/2^n \succeq 0. \end{aligned}$$

Here, the last expression is positive semi-definite by (3.15). Thus we see that the first constraint in the dual problem of the n-round SDP for any string s is positive semi-definite for any combination of rounds.

The final step is to show that $Q_s = (P_sQ_{T(s)}^{T_\mathsf{B}}P_s)^{T_\mathsf{B}}$ is positive. Note that P_s permutes both registers held by A and B of the states together, since it consists only of 2-qubit SWAP operations. The action is thus independent of the partial transpose on the second party B. We therefore have $Q_s = P_sQ_{T(s)}P_s$. Now, since P_s is unitary and $Q_{T(s)}$ is positive semi-definite we have that Q_s is positive semi-definite.

We have shown that all the constraints in the dual problem of the n-round SDP are satisfied by our constructed Q_s matrices, thus we have a feasible solution to the dual problem with value $\mathrm{Tr}[Y] = (2/3)^n$, which is equal to the primal value and is attainable by a LOCC strategy. This shows that the best attacking strategy for adversaries restricted to LOCC operations playing n rounds in parallel is to simply apply the single-round strategy n times in parallel.

3.A.3 Optimal PPT Measurements for loss-tolerant $\mathrm{QPV}^n_{\mathsf{SWAP}}$ Protocol

We shall now modify the solution to the parallel repetition case in Appendix 3.A.2 to give a solution to the maximization of conditional success probability under LOCC restrictions. We will optimize the probability of being correct conditioned on answering. The SDP for the lossy n round parallel repetition protocol in which attackers either answer on all rounds or on none is given as:

Primal Problem

$$\begin{aligned}
\textbf{maximize:}\quad & \frac{1}{2^n \eta} \sum_{s \in \{0,1\}^n} \mathrm{Tr}[\tilde{\Pi}_s \rho_s] \\
\textbf{subject to:}\quad & \left(\sum_{s \in \{0,1\}^n} \tilde{\Pi}_s \right) + \tilde{\Pi}_\varnothing = \mathbb{1}_{2^{2n}} \\
& \mathrm{Tr}[\tilde{\Pi}_\varnothing \rho_s] = 1 - \eta, \quad s \in \{0,1\}^n \\
& \tilde{\Pi}_s \in \mathrm{PPT}(\mathsf{A} : \mathsf{B}), \quad s \in \{0,1\}^n \cup \varnothing \\
& \Pi_s \succeq 0, \ \text{for} \quad s \in \{0,1\}^n
\end{aligned}$$

Dual Problem

$$\begin{aligned}
\textbf{minimize:}\quad & \frac{\mathrm{Tr}[\tilde{Y}] - (1-\eta)\gamma}{\eta} \\
\textbf{subject to:}\quad & \tilde{Y} - \tilde{Q}_s^{T_\mathsf{B}} - \rho_s / 2^n \succeq 0, \quad s \in \{0,1\}^n \\
& 2^{2n} (\tilde{Y} - \tilde{Q}_\varnothing^{T_\mathsf{B}}) - \gamma \mathbb{1}_{2^{2n}} \succeq 0 \\
& \tilde{Y} \in \mathrm{Herm}(\mathsf{A} \otimes \mathsf{B}) \\
& \tilde{Q}_s \in \mathrm{Pos}(\mathsf{A} \otimes \mathsf{B}), \quad s \in \{0,1\}^n \cup \varnothing \\
& \gamma \in \mathbb{R}.
\end{aligned}$$

Here η is the transmission rate and $\mathrm{Tr}[\tilde{\Pi}_\varnothing \rho_s] = 1 - \eta$ is the condition that attackers can only say loss with equal probability on every input. We suspect our protocol is loss-tolerant, thus we want the solution to be independent of η. It turns out multiplying the POVM elements by η and picking $\tilde{\Pi}_\varnothing$ accordingly, i.e. $\tilde{\Pi}_s = \eta \Pi_s$ for every $s \in \{0,1\}^n$ and $\tilde{\Pi}_\varnothing = (1-\eta)\mathbb{1}_{2^{2n}}$ gives a feasible solution for the primal problem with solution $(2/3)^n$.

For the dual problem, we pick

$$\tilde{Y} = \frac{\mathbb{1}_{2^{2n}}}{6^n}, \qquad \tilde{Q}_s = Q_s \qquad \tilde{Q}_\varnothing = 0, \qquad \gamma = (2/3)^n, \tag{3.16}$$

then trivially $Y \in \mathrm{Herm}(\mathsf{A} \otimes \mathsf{B}), \tilde{Q}_s \in \mathrm{Pos}(\mathsf{A} \otimes \mathsf{B}), \gamma \in \mathbb{R}$ and the first condition remains satisfied since we have not changed Y, Q_s in Appendix 3.A.2. The second constraint becomes

$$2^{2n}(\tilde{Y} - \tilde{Q}_\varnothing^{T_\mathsf{B}}) - \gamma \mathbb{1}_{2^{2n}} = \mathbb{1}_{2^{2n}} \frac{2^n}{3^n} - (2/3)^n \mathbb{1}_{2^{2n}} = 0 \succeq 0. \tag{3.17}$$

So, all constraints in the dual are satisfied. We thus get an upper bound of

$$\frac{\mathrm{Tr}[\tilde{Y}] - (1-\eta)\gamma}{\eta} = \frac{(2/3)^n - (1-\eta)(2/3)^n}{\eta} = \frac{\eta(2/3)^n}{\eta} = (2/3)^n. \tag{3.18}$$

Thus, we finally have $p^{\max}_{\mathrm{succ},n}(\eta) = (2/3)^n$ for any $\eta \in (0, 1]$. Together with Proposition 3.2.1 in the main text, this gives full loss tolerance for the n-round parallel repetition of our protocol.

Chapter 4

Quantum Communication Attacks and Loss

In the previous chapter, we restricted the attackers to only have access to a classical communication channel. In this chapter, we investigate the setting of having a quantum communication channel but no quantum memory to store pre-shared entanglement. We investigate the relation between quantum communication and loss in attacks on Quantum Position Verification (QPV) schemes. From a practical point of view this setting is still relevant because while a quantum communication channel *allows* attackers to pre-share entanglement, actually *storing* the entanglement in a quantum memory is still a hard task. From a theoretical point of view, it is interesting whether there can even be an advantage of quantum communication over classical communication. We start by presenting a protocol that is provably secure against attackers restricted to classical communication and no pre-shared entanglement, but can be trivially broken if the attackers have access to a quantum channel between them. We then show that any protocol secure against classical communication can be transformed into a protocol secure against quantum communication. We further show, using arguments based on the monogamy of entanglement, that the task of Bell state discrimination cannot be done locally with a single round of quantum communication, not even probabilistically (when we allow attackers to say loss sometimes), making this the first fully loss-tolerant QPV task secure against quantum communication attacks. We also show that we can use similar techniques to prove the same properties for the $\mathrm{QPV}_{\mathsf{SWAP}}$ protocol of Chapter 3. Finally, we observe that any multi-round QPV protocol can be attacked with a linear amount of entanglement if the loss is high enough.

This chapter is based on the papers “On the Role of Quantum Communication and Loss in Attacks on Quantum Position Verification” by Rene Allerstorfer, Harry Buhrman, Florian Speelman and Philip Verduyn Lunel [ABSV22a] and “Monogamy of highly symmetric states” by Rene Allerstorfer, Matthias Christandl, Dmitry Grinko, Ion Nechita, Maris Ozols, Denis Rochette and Philip Verduyn Lunel [ACG+23].

4.1 Introduction

In this chapter we dive deeper into the role of quantum communication without pre-shared entanglement in Quantum Position Verification (QPV) schemes, expanding on the security results presented in the previous chapter. From a practical point of view, not allowing the attackers to pre-share entanglement is still interesting, because even though attackers might be able to send quantum communication to each other, having access to a stable quantum memory is a much harder task. Secondly, it is also possible for attackers to run out of pre-shared entanglement, thus understanding how well they can attack the protocol with just quantum messages remains of interest. Finally, from a theoretical point of view, it is also interesting to learn what exactly the power is of using a single round of simultaneous quantum communication over classical communication.

Some works [BRSW11, TFKW13, BFSS13, BCS22] attempt to lower bound the pre-shared entanglement required from attackers that are allowed a round of simultaneous *quantum* communication, while other results, such as [BK11, RG15, QS15, QLL+15, LXS+16, GC20, OCCG20] assume attackers that are restricted to communicate only classically.

Even though quantum communication can potentially be simulated by teleportation, it is not immediately clear how to compare bounds between these two settings, especially in case where the exact size of the lower bound is of interest. The simplest version of this question can be asked for unentangled attackers: If a (quantum-question, classical-reply) QPV protocol is secure against unentangled attackers that communicate classically, is that protocol also secure against unentangled attackers that are allowed to use quantum communication?

To that end, we present the following results:

- First, we answer the above question in the negative: We construct a protocol that is provably secure against unentangled attackers that can use classical communication, but can be broken by a single round of simultaneous quantum communication. This shows that some care has to be taken when interpreting results that restrict to classical messages only.

- Interestingly, we are additionally able to show that our counter-example is in some sense artificial: Given a protocol that is secure against classical messages, but insecure when quantum communication is allowed, it is always possible to transform this protocol into one that is secure when quantum communication is allowed.

  This new protocol can be constructed from the given protocol by applying local maps to the messages from the verifiers $\mathsf{V_A}$, $\mathsf{V_B}$, without having to modify the output predicate. Our proof for this statement involves a recursive argument, where we view the states after quantum communication of a successful attack as the input messages to two new protocols. We then recursively consider an increasing number of new possible protocols and use *emergent classicality* [QR21] to show that a secure protocol of the required form has to exist.

- We proceed by considering the task of Bell state discrimination[1] and prove that this task cannot be done perfectly with only local operations and one round of simultaneous (quantum) communication. The proof relies on new arguments based on the monogamy of entanglement. We consider a purified version of this task in the QPV setting (delaying the honest measurement to the end of the protocol) and show that the squashed entanglement [CW04] of the state $\rho_{V_A V_B}$, on which the honest Bell measurement is applied to, is upper bounded by $E_{sq}(V_A : V_B)_\rho \leq 1/2$. Hence attackers won't be able to perfectly predict the honest result. To get an explicit upper bound on the attack success probability with quantum communication $p^{\mathrm{qc}}_{\mathrm{succ}}$ we use the *hashing bound* from [DW05] which lower bounds the squashed entanglement, allowing us to upper bound a parameter that leads to $p^{\mathrm{qc}}_{\mathrm{succ}} \leq 0.926$. We further improve this bound to $p^{\mathrm{qc}}_{\mathrm{succ}} \leq \ln(2)$ via a different argument based on a state-existence argument. We show that the existence of good attack implies the existence of certain states. We then show in what regime these states can exist by means of an SDP, which in turn bounds the success probability.

- Even though the method based on the squashed entanglement measure gives a worse bound, it can be more generally applied. Using a reduction argument we further show that for the $\mathrm{QPV}_{\mathsf{SWAP}}$ protocol any attack that uses only quantum communication and no pre-shared entanglement cannot have a success probability higher than $p^{\mathrm{qc}}_{\mathrm{succ}} \leq 0.7315$.

- We additionally show that even in the lossy scenario it remains that $p^{\mathrm{qc}}_{\mathrm{succ}}(\eta) < 1$ for any transmission rate $0 < \eta \leq 1$. This makes the task of Bell state discrimination, and by implication the QPV protocol based on the SWAP test in the previous chapter, the first fully loss-tolerant QPV protocol that remains secure in the setting where attackers are allowed quantum communication.

Finally, we present a result relating loss tolerance and entanglement attacks in QPV:

- We observe that, in a setting with loss, any multi-round QPV protocol can be broken with only a linear amount of pre-shared entanglement if the loss rate is high enough. In that sense, creating a fully loss-tolerant QPV protocol which requires superlinear entanglement (in the number of qubits involved) is impossible. This follows directly from a simple observation: if

[1] Where the input is a randomly chosen Bell state.

> there is no limit to the loss, the adversaries can attempt quantum teleportation and guess the teleportation corrections, claiming 'loss' if the guess is incorrect. In the next chapter we will see that not all is lost, and by changing the structure of the QPV protocol slightly we can get protocols that are secure when there are classical inputs.

The aspects of loss and quantum communication are practically very relevant, since in realistic settings loss rates will be high and, although attackers are restricted to only one round of simultaneous communication due to the timing constraints of QPV, they could in principle be able to communicate quantum messages and this might give them an advantage.

The structure of the chapter is as follows. In Section 4.2.1 we present the first QPV protocol that is provably secure against attackers restricted to quantum communication but broken by a single round of quantum communication. However, in Section 4.2.2, we show that any protocol insecure against quantum communication, but secure against classical communication, can be transformed into a protocol secure against quantum communication. In Section 4.2.3 we show that the task of Bell state discrimination is secure against attackers who are allowed to use quantum communication by giving two different approaches to compute upper bounds on the success probability of attacking this protocol, in Section 4.2.5 thereafter we show security for $\mathrm{QPV}_{\mathsf{SWAP}}$. Extending on this result in Section 4.2.4 we also show that this protocol is strictly secure if we allow attackers to also say loss in addition to quantum communication. With strictly secure, we mean that $p_{succes} < 1$, so a perfect attack does not exist. We show that both results can be extended to also show security against quantum communication for the SWAP-test, also in a lossy setting. Finally, in Section 4.2.6 we make the observation that allowing loss for pre-shared entangled attackers allows any protocol with high enough loss rate to be broken with linear entanglement.

4.2 QPV and quantum communication

For simplicity, we treat the one-dimensional case here, where all parties are located on a line. The time needed to implement local operations is considered negligibly short compared to the time span of the entire protocol. In order to verify the position of an untrusted party P, two trusted and spatially separated verifiers $\mathsf{V}_\mathsf{A}, \mathsf{V}_\mathsf{B}$ send quantum inputs to P from each side and ask them to apply a specific quantum operation. P has to apply the operation and respond immediately. In the end, the verifiers check if they received an answer in time and consistent with the input and the demanded task. The attack model is as follows. Attackers trying to break the protocol are *not* located at P but want to convince the verifiers that they are. Two attackers[2] A, B can position themselves between $\mathsf{V_A}, \mathsf{P}$ and $\mathsf{V_B}, \mathsf{P}$, respectively, and intercept the inputs, act locally, communicate one message to each other, and then act locally again before they have to commit to answers τ_A, τ_B. They hence have to simulate the honest quantum operation using only local actions and 1 round of simultaneous communication. This situation is depicted in Figure 4.1.

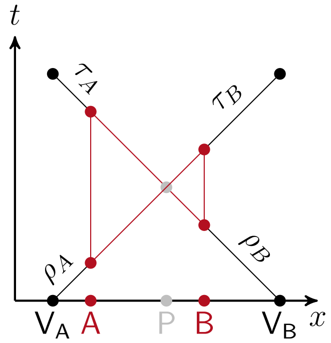


Figure 4.1: Space-time diagram of a general QPV protocol. We assume all information travels at the speed of light. For graphical simplicity we have put P exactly in the middle of $\mathsf{V_A}$ and $\mathsf{V_B}$ (which is not necessary). The attackers, not being at position P, would like to convince the verifiers that they are at P by simulating the honest operation via local operations and one round of simultaneous communication.

4.2.1 A protocol for which quantum communication gives an advantage over LOCC

A natural question one might ask is whether there is any advantage for attackers in QPV protocols if they are allowed to perform local operations and simultaneous quantum communication (LOSQC) instead of classical communication. In what follows, we will construct an explicit example of a QPV protocol with classical outputs where there is a finite gap in the success probability for LOSQC strategies over LOCC strategies, thus separating both classes.

First, consider the protocol where two verifiers both send half of either one randomly picked symmetric Bell state $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle\}$ or the antisymmetric Bell state $|\Psi^-\rangle$, and ask an honest prover whether the entangled state they have sent is symmetric or antisymmetric. An honest prover who can apply entangling operations can answer this question with success probability 1 by applying a SWAP test [BCWW01] on the state. From the analysis of the corresponding SDP optimized over PPT measurements it turns out that the best LOCC strategy is

[2] The scenario of more attackers can be reduced to the one described above. Indeed, the attackers closest to P could simply simulate all the other attackers themselves.

upper bounded by 5/6 (see Appendix 4.A.1). The LOCC strategy of measuring both qubits in the computational basis and answering the XOR of the outcomes attains this success probability, so the upper bound over PPT measurements is attained by a LOCC measurement.

Now suppose the verifiers send two parallel rounds of the previous protocol under the condition that the two rounds are either both a random symmetric Bell state or they are both an antisymmetric Bell state, and we ask the prover whether the input consisted of two symmetric or two antisymmetric states. An honest prover who can apply entangling operations can still solve this protocol with success probability 1 by applying a SWAP-test to one of the two pairs. Now note that attackers who have access to a quantum channel can send half of their input state to each other such that both attackers locally end up with a Bell state which they can perfectly determine. Thus, attackers restricted to quantum communication without pre-shared entanglement can attack this protocol perfectly. Interestingly, it turns out that this is not possible for attackers restricted to classical communication.

From the analysis of the SDP it turns out that the upper bound for two attackers restricted to PPT measurements is 17/18, cf. Appendix 4.A.1. Again, there is a LOCC strategy that makes this bound tight, namely measuring both pairs in the computational basis and only answering "antisymmetric" if both pairs have unequal measurement outcomes and respond "symmetric" otherwise. This strategy is always correct on antisymmetric inputs. And it is only incorrect on symmetric inputs if both times the state $|\Psi^+\rangle$ was sent, this happens with probability 1/18, so the total probability of success of the LOCC protocol becomes 17/18. By incorporating loss in the SDP program as done in [LXS$^+$16] and the previous chapter, we also find that this protocol is loss-tolerant.

Thus, we have constructed a QPV protocol where the probability of success for attackers restricted to single-round LOCC measurements is strictly lower than attackers restricted to LOSQC measurements. This shows that there can be an advantage for quantum communication over classical communication, and it could be important in the analysis of the security of QPV protocols. However, it is clear that our construction is not a very good protocol as there is redundant information given to the attackers, and sending just one of the two symmetric or antisymmetric states would give a seemingly better protocol.

4.2.2 Splitting Scheme

Our separating example had some redundancy in it, in the sense that the correct answer was present more than once. In this section, we present a procedure that distills a QPV protocol secure against attackers using a single round of simultaneous quantum communication from the existence of a QPV protocol that is secure against adversaries restricted to LOCC operations. We will use the fact that the existence of a perfect quantum communication attack on a QPV protocol generates two new QPV protocols, which, when applied recursively, ultimately leads to the existence of a QPV protocol that is secure against adversaries restricted to LOCC *and* cannot be perfectly attacked by adversaries using quantum communication. Morally, this recursion removes the redundancy of the correct answer in the original protocol.

Take any QPV protocol in which two verifiers $\mathsf{V_A}, \mathsf{V_B}$ send states ρ_A, ρ_B and ask for the outcome of, say, some entangling measurement on the joint state ρ_{AB}. Suppose the protocol is secure against adversaries restricted to LOCC, i.e., there is a finite gap in the probability of success between an honest prover and adversaries restricted to LOCC operations, but also assume that the protocol can be broken perfectly by adversaries using quantum communication. In the most general setting, the actions of the adversaries are as follows:

- Adversaries A, B receive ρ_A, ρ_B respectively as input states.
- Apply some local channel $\mathcal{A}(\rho_A) = \sigma_{A_1A_2}$, $\mathcal{B}(\rho_B) = \sigma_{B_1B_2}$.
- Send some share of their local outcome to the other adversary.
- Apply a measurement on the new local states $\sigma_{A_1B_1}$ and $\sigma_{A_2B_2}$.
- Send the measurement outcome to their respective verifiers.

Now note that both $\sigma_{A_1}, \sigma_{B_1}$ and $\sigma_{A_2}, \sigma_{B_2}$ can be used as input states to define two new QPV protocols, where the measurement an honest prover needs to apply is equal to the measurement the attackers would apply in the quantum communication attack in the original protocol. Then the probability of success for the honest verifier in the newly defined protocol is the probability of success of the adversaries using quantum communication in the previous protocol, which we assumed to be perfect.

Note that any LOCC attack on one of these newly arising protocols was already a valid LOCC attack in the previous protocol with the inputs ρ_A and ρ_B. The attackers can simply apply the local channels $\mathcal{A}, \mathcal{B}$, discard the state they don't use, and apply their attack. Also note that if the input states ρ_A, ρ_B were product states, the input states in the newly created protocol are also product states. We have therefore split the QPV protocol into two new protocols using only the existence of a perfect quantum communication attack.

Now there are two options for the newly defined protocols:

- There does not exist a perfect attack using quantum communication for at least one of the two new QPV protocols, in which case we have shown the existence of a QPV protocol that is safe against adversaries using quantum communication and we are done.

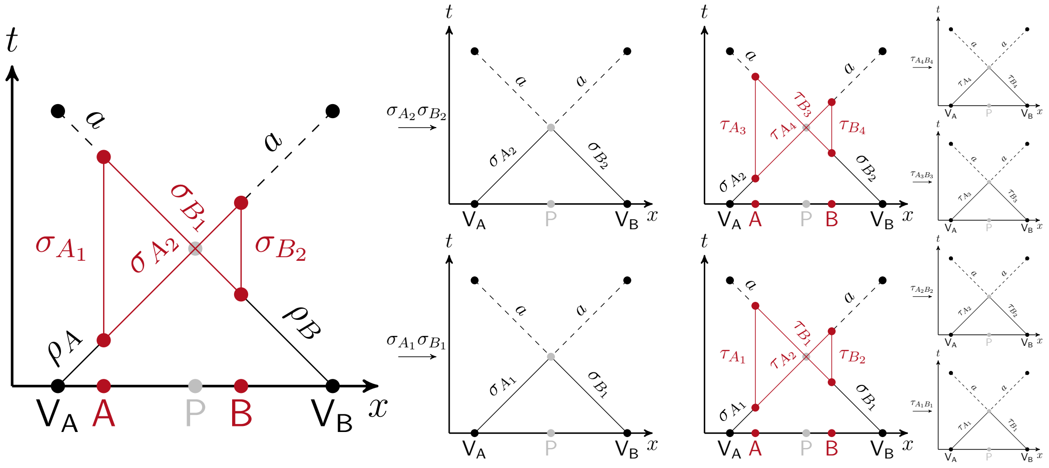


Figure 4.2: Visual representation of splitting into two new QPV protocols from the existence of a quantum communication attack on a single QPV protocol. Two attackers A, B receive inputs ρ_A, ρ_B and apply some channel $\mathcal{A}(\rho_A) = \sigma_{A_1A_2}, \mathcal{B}(\rho_B) = \sigma_{B_1B_2}$ and send parts of their outcome to the other party. This procedure defines two new QPV protocols. If again there exists a perfect quantum communication attack for both new protocols, then by the same argument we can define 4 new QPV protocols, and so on.

- For both protocols, there exists a perfect attack using quantum communication. In which case we can apply our previous argument to generate 4 new QPV protocols. See Figure 4.2 for a visual representation of this splitting argument.

The previous options are true for all QPV protocols that arise after splitting, and we wish to show the existence of a QPV protocol safe against quantum communication. We therefore suppose that all of the induced QPV protocols after splitting n times can be attacked perfectly using quantum communication for any $n \geq 2$.

Note that the input states sent from verifier $\mathsf{V_A}$ in the induced QPV protocols after splitting only depend on the previous input states sent from $\mathsf{V_A}$ and vice-versa for the input states from $\mathsf{V_B}$. We can write this action as channels $\Lambda_n^A : \mathcal{D}(A) \to \mathcal{D}(A_1 \otimes \cdots \otimes A_{2^n})$, mapping $\rho_A \mapsto \sigma_{A_1 \ldots A_{2^n}}$, and $\Lambda_n^B : \mathcal{D}(B) \to \mathcal{D}(B_1 \otimes \cdots \otimes B_{2^n})$, mapping $\rho_B \mapsto \sigma_{B_1 \ldots B_{2^n}}$. The idea of this proof is that the reduced states σ_{A_i} and σ_{B_i} become approximately classical, and that attackers could immediately measure their incoming states and share the classical measurement outcome instead of sending some quantum message. This would lead to a contradiction since the success probability of this procedure would be upper bounded by the LOCC bound of the original QPV protocol, while at the same time, by assumption, this attack should become approximately close to a perfect one. To be more precise, we use Theorem 4.2.1 on the emergent classicality of channels from [QR21].

4.2.1. Theorem (Qi-Ranard). *Consider a quantum channel $\Lambda : \mathcal{D}(A) \to \mathcal{D}(B_1 \otimes ... \otimes B_n)$. For output subsets $R \subset \{B_1, ..., B_n\}$, let $\Lambda_R \equiv \mathrm{Tr}_{\bar{R}} \circ \Lambda : \mathcal{D}(A) \to \mathcal{D}(R)$ denote the reduced channel onto R, obtained by tracing out the complement $\bar{R}$. Then for any $|Q|, |R| \in \{1, ..., n\}$, there exists a measurement, described by a positive-operator valued measure (POVM) $\{M_\alpha\}$, and an "excluded" output subset $Q \subset \{B_1, ..., B_n\}$ of size $|Q|$, such that for all output subsets R of size $|R|$, disjoint from Q, we have*

$$\|\Lambda_R - \mathcal{E}_R\|_\diamond \le d_A^3 \sqrt{2\ln(d_A)\frac{|R|}{|Q|}}, \tag{4.1}$$

using a measure-and-prepare channel

$$\mathcal{E}_R(X) := \sum_\alpha \mathrm{Tr}(M_\alpha X)\sigma_R^\alpha, \tag{4.2}$$

for some states $\{\sigma_R^\alpha\}_\alpha$ on R, where $d_A = dim(A)$ and $\|...\|_\diamond$ is the diamond norm on channels. The measurement $\{M_\alpha\}$ does not depend on the choice of R, while the prepared states σ_R^α may depend on R.

Applying the theorem and setting the size of the excluded output set for both channels Λ_n^A, Λ_n^B to $|Q_A| = |Q_B| = 2^{n-1} - 1$, we have, by the pigeonhole principle, that for some index $i \in \{1, \ldots, 2^n\}$ both output sets A_i, B_i must be in the sets disjoint from Q_A and Q_B. Setting the size of the reduced channels to $|R_A| = |R_B| = 1$, we see that in both cases the reduced channel $\mathrm{Tr}_{\bar{R}} \circ \Lambda_n^{A/B}$ converges to a measure-and-prepare channel in the number of splittings n for any output:

$$\| \mathrm{Tr}_{\bar{R}_{A/B}} \circ \Lambda_n^{A/B} - \mathcal{E}_{R_{A/B}} \|_\diamond \le 8\sqrt{\frac{2\ln(d_{A/B})}{2^{n-1}-1}}. \tag{4.3}$$

The theorem implies that the reduced channels that maps the input states $\rho_A \mapsto \sigma_{A_i}$ and $\rho_B \mapsto \sigma_{B_i}$ become approximately close to measure-and-prepare channels. Crucially, the measurements $\{M_\alpha^{A/B}\}$ in the respective measure-and-prepare channels do not depend on the choice of R. This gives rise to an LOCC attack in the original QPV protocol from which we started. Two attackers A, B simply apply the local measure-and-prepare channels $\mathcal{E}_{R_A}, \mathcal{E}_{R_B}$ and exchange the classical measurement outcomes α_1, α_2. Both attackers then know the state $\sum_{\alpha_1} p_{\alpha_1}\sigma_{A_i}^{\alpha_1} \otimes \sum_{\alpha_2} p_{\alpha_2}\sigma_{B_i}^{\alpha_2}$ which is arbitrarily close to $\sigma_{A_i} \otimes \sigma_{B_i}$ in n. Since for any QPV protocol the POVM measurement that the honest verifier has to apply is publicly known, both attackers can calculate the probability distribution of the answers of an honest prover. Using shared randomness to generate an equal answer both attackers can now mimic the probability of success of an honest verifier arbitrarily well.

This LOCC attack allows attackers to answer correctly with a probability of success that converges to the honest probability of success in the number of splittings n. By assumption n can be arbitrarily large and thus the attackers have an LOCC attack that performs arbitrarily well. However, since for our protocol at the start there is a finite gap between the LOCC probability of success and the honest probability of success, we have a contradiction and conclude that at some level in the recursion there must exist a QPV protocol that cannot be attacked perfectly. That protocol must then be safe against unentangled adversaries restricted to quantum communication arises.

4.2.3 Security of QPV$_{\textsf{Bell}}$ against quantum communication

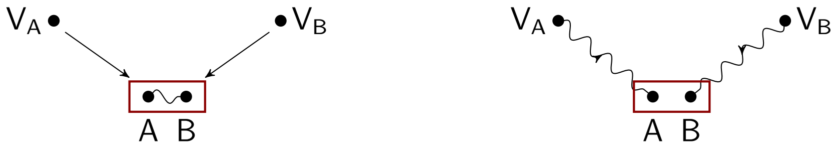
In this section, we give the first example of a classically loss-tolerant QPV protocol that is secure against attackers restricted to quantum communication. Furthermore, we will show that there is no perfect attack with loss in the quantum communication setting for this protocol, making it the first example of a protocol that is secure against lossy quantum communication attacks with no pre-shared entanglement.

The protocol we investigate is the Bell state discrimination problem. Two verifiers send as inputs the respective qubits of one of the four Bell states $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$ and ask the prover which Bell state he receives. An honest prover can answer this task perfectly by doing a Bell measurement. With an SDP and a similar analysis as in the previous chapter, we can show that this protocol is secure and loss-tolerant against attackers restricted to classical communication. An optimal attacking strategy turns out to measure the qubits in the computational basis, which distinguishes $\{|\Phi^+\rangle, |\Phi^-\rangle\}$ from $\{|\Psi^+\rangle, |\Psi^-\rangle\}$ and then to guess one of the two Bell states as an answer. This has success probability 1/2.

To analyze security against attackers restricted to quantum communication, we look at the protocol in the following equivalent purified way.

- The inputs of the protocol will be half of a maximally entangled state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{V_AP_A}$ and $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{V_BP_B}$. Where the other half is kept by the verifier. This is visualized in Figure 4.3.

- The honest prover has to do a Bell state measurement. This measurement now acts as an entanglement swapping operation, where the entanglement between the verifiers and the prover gets swapped to entanglement between the two verifiers, and entanglement between the two qubits the prover holds. The measurement outcome of the prover will be one of the four Bell states



(a) Original protocol

(b) Equivalent protocol

Figure 4.3: By Equation 4.4 these two settings are equivalent. On registers A, B a Bell measurement is supposed to happen. In Figure 4.3a the verifier knows which Bell state they send beforehand, in Figure 4.3b a Bell state is swapped into the registers $\mathsf{V_A}, \mathsf{V_B}$. The players need to simulate this as well as possible.

with equal probability, and determines which Bell state the verifiers hold. The prover then sends his classical measurement outcome i to the verifiers.

- The verifiers check whether the entanglement swapping operation was successful by applying a Bell measurement on their joint state, and check whether their measurement outcome is the same as the answer of the prover. The probability of successfully attacking the protocol now corresponds to the verifiers having the correct Bell state as their measurement outcome, averaged over all possible Bell states, i.e. $p_{\text{succ}} = \frac{1}{4}\sum_{i=0}^{3} \mathrm{Tr}[|\mathrm{Bell}_i\rangle\langle\mathrm{Bell}_i|\, \rho^i_{V_A V_B}]$.

Note that from the point of prover nothing changes from the original Bell state discrimination protocol. The honest prover still needs to perform a Bell state measurement on his incoming qubits and send his measurement outcome to both verifiers.

To see that the operation of the prover swaps entanglement to the registers of the verifiers, note the following relation:

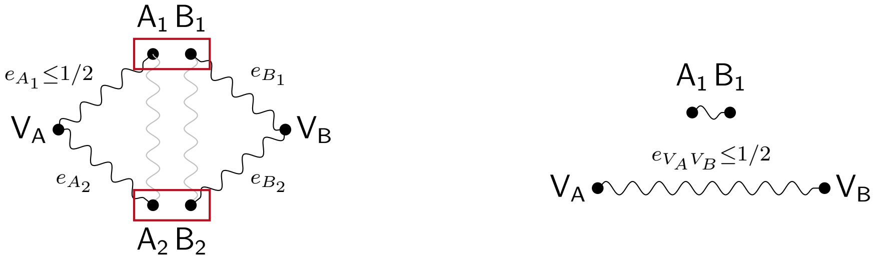
$$|\Phi^+\rangle_{V_A,P_A}|\Phi^+\rangle_{P_B,V_B} = \frac{1}{2}\Big(|\Phi^+\rangle_{V_A,V_B}|\Phi^+\rangle_{P_A,P_B} + |\Phi^-\rangle_{V_A,V_B}|\Phi^-\rangle_{P_A,P_B} + |\Psi^+\rangle_{V_A,V_B}|\Psi^+\rangle_{P_A,P_B} + |\Psi^-\rangle_{V_A,V_B}|\Psi^-\rangle_{P_A,P_B}\Big). \quad (4.4)$$

We see that when P applies a Bell state measurement to his local systems P_A, P_B (as is his task in the protocol), the post-measurement state between the two verifiers will collapse to one of the four Bell states, and the measurement outcome of P determines which one.

The idea to show security against quantum communication is that by reformulating the $\mathrm{QPV}_{\mathsf{Bell}}$ protocol as an entanglement swapping protocol we can use the monogamy of entanglement property between the qubits that remain at the verifiers and the quantum systems attackers create. Furthermore, while it is hard to say anything about the quantum systems attackers might send to each other, the states the verifiers keep are always under their control.

As stated in Section 4.2.2 the most general quantum communication attack is for attackers A, B to split their inputs into two quantum systems A_1, A_2 and

B_1, B_2, respectively. They hold on to one and forward the other system to the other attacker. After the quantum communication round, the attackers A, B locally hold the reduced states $\rho_{A_1} \otimes \rho_{B_1}$ and $\rho_{A_2} \otimes \rho_{B_2}$, respectively. Note that while the A_1 subsystem is in a product state with the B_1 subsystem, the A_1 and A_2 subsystems can be as entangled as the attackers like. As there is no more further communication, for a quantum attack to be successful in generating entanglement between the two verifiers, it is sufficient to look only at one of the two attackers' quantum systems locally[3]. We will use this fact in our proof to show that they cannot perform this task perfectly using quantum communication. The idea behind the proof is that V_A cannot be sufficiently entangled to both subsystems A_1, A_2 at the same time. But both joint subsystems A_1B_1 and A_2B_2 individually must be sufficient to attack the protocol, as both attackers need to answer correctly.



(a) Entanglement structure when attackers measure and commit to an answer. W.l.o.g. $e_{A_1} \leq 1/2$.

(b) Measuring $\mathsf{A}_1\mathsf{B}_1$ and sending the result to V_A is an LOCC operation on $V_\mathsf{A}(\mathsf{A}_1\mathsf{B}_1 V_\mathsf{B})$.

Figure 4.4: Illustration of the argument based on monogamy of entanglement to bound the entanglement $e_{V_AV_B} \leq 1/2$ as described in the main text. Tracing out $\mathsf{A}_2\mathsf{B}_2$, attacker A can only swap $e_{V_AV_B} \leq 1/2$ ebits to $\mathsf{V}_\mathsf{A}\mathsf{V}_\mathsf{B}$.

As an entanglement measure we will use the squashed entanglement. This measure satisfies several properties useful for our analysis, such as monotonicity under LOCC operations, general monogamy with no restrictions on the size of the quantum registers, and it is lower bounded by distillable entanglement [CW04]. Consider the sketch of the entanglement structure between all quantum registers in Figure 4.4. By monogamy, we have that

$$0 \leq E_{sq}(V_A : A_1)_\rho + E_{sq}(V_A : A_2)_\rho \leq E_{sq}(V_A : A)_\rho = E_{sq}(|\Phi^+\rangle\langle\Phi^+|) = 1. \quad (4.5)$$

Suppose without loss of generality that $E_{sq}(V_A : A_1)_\rho \leq E_{sq}(V_A : A_2)_\rho$, then the inequality implies that $E_{sq}(V_A : A_1)_\rho \leq 1/2$. Let Φ be the LOCC operation (on $\mathsf{V}_\mathsf{A}(\mathsf{A}_1\mathsf{B}_1\mathsf{V}_\mathsf{B})$) of measuring the $\rho_{A_1B_1}$ register and sending the classical measurement result to V_A. Using that squashed entanglement is monotone under LOCC

[3] Attackers have to act in a coordinated way in QPV, but in particular each attacker also needs to have a local success probability at least as big as the global one.

we get the following:

$$\begin{aligned} E_{sq}(V_A : V_B)_{\Phi(\rho)} &\leq E_{sq}(V_A : A_1 B_1 V_B)_{\Phi(\rho)} \\ &\leq E_{sq}(V_A : A_1 B_1 V_B)_{\rho} \\ &= E_{sq}(V_A : A_1) \leq 1/2. \end{aligned} \tag{4.6}$$

Thus, the squashed entanglement between the two verifiers after any attack using quantum communication is upper bounded by $1/2$. Recall that for an attack to be successful, the verifiers must share the same Bell state on their registers $\rho_{V_A V_B}$ as the answer i they receive from the attackers in this case single. Since $E_{sq}(|B_i\rangle \langle B_i|) = 1$ it is immediately clear that $p_{\text{succ}} = \sum_i \mathrm{Tr}[|B_i\rangle \langle B_i| \rho^i_{V_A V_B}]/4 < 1$ and no perfect attack is possible.

Ideally, we want p_{succ} not only to be strictly smaller than 1, but also to be smaller than 1 by some finite gap. In what follows, we will show that $E_{sq}(V_A : V_B) \leq 1/2$ implies $p_{\text{succ}} \leq 0.926$, which implies security against quantum communication. Our proof uses the *hashing bound* from [DW05], which lowers the squashed entanglement [CW04]. The inequality states that for any quantum state ρ_{AB},

$$S(B)_\rho - S(AB)_\rho \leq E_{sq}(A : B)_\rho, \tag{4.7}$$

where $\rho_B = \mathrm{Tr}_A[\rho_{AB}]$, and S is the von Neumann entropy.

The idea of this proof is to apply the *Werner twirling channel* $\mathcal{W}$, where we integrate over the final two-qubit state between the verifiers. This channel leaves the antisymmetric (qubit) state invariant and projects the remaining part to the symmetric subspace. Furthermore, this channel is an LOCC channel and by monotonicity of the squashed entanglement under LOCC operations, we have

$$1/2 \geq E_{sq}(V_A : V_B)_{\Phi(\rho)} \geq E_{sq}(V_A : V_B)_{\mathcal{W}(\Phi(\rho))}. \tag{4.8}$$

The resulting state $\mathcal{W}(\Phi(\rho)_{V_A V_B})$ can then be written as a mixture of the antisymmetric Bell state with the maximally mixed state characterized by some $\alpha > 0$, that is,

$$\mathcal{W}(\Phi(\rho)_{V_A V_B}) = \alpha \, |\Psi^-\rangle\langle\Psi^-| + (1-\alpha)\frac{\mathbb{1}_4}{4}. \tag{4.9}$$

A property of Bell states is that they can be locally transformed into one another. Therefore, verifiers can always locally change the Bell state that they receive as an answer from the honest prover to the antisymmetric Bell state. Therefore, any successful attack can be characterized by the probability of having measurement outcome $|\Psi^-\rangle$ on $\mathcal{W}(\rho_{V_A V_B})$. Combining the entanglement bound (4.8) with the hashing bound (4.7) we get the following numerical bound on α:

$$\begin{aligned} 1/2 &\geq E_{sq}(V_A : V_B)_{\mathcal{W}(\Phi(\rho))} \\ &\geq S(B)_{\mathcal{W}(\Phi(\rho))} - S(AB)_{\mathcal{W}(\Phi(\rho))} \\ &= 1 - S(AB)_{\mathcal{W}(\Phi(\rho))} \\ \iff \qquad \alpha &\leq 0.902. \end{aligned} \tag{4.10}$$

The probability of success is now upper bounded as follows

$$\begin{aligned} p_{\text{succ}} &= \operatorname{Tr}\big[\lvert\Psi^-\rangle\langle\Psi^-\rvert\,\Phi(\rho)_{V_AV_B}\big] = \mathcal{F}(\lvert\Psi^-\rangle\langle\Psi^-\rvert\,,\Phi(\rho)_{V_AV_B}) \\ &\leq \mathcal{F}(\mathcal{W}(\lvert\Psi^-\rangle\langle\Psi^-\rvert),\mathcal{W}(\Phi(\rho)_{V_AV_B})) \\ &= \operatorname{Tr}\big[\lvert\Psi^-\rangle\langle\Psi^-\rvert\,\mathcal{W}(\rho_{V_AV_B})\big] = \alpha + \frac{1-\alpha}{4} \leq 0.926, \end{aligned} \tag{4.11}$$

where we have used the data process inequality for the fidelity in the first inequality. This concludes our proof and shows that there is a finite gap between the optimal attack attackers restricted to quantum communication can do and what an honest prover can do. We suspect that this gap can be made even larger, the upper bound that we find arises only due to restrictions on the A_1 part, the B_1 part could be unchanged from the input state of B. So, our bound gives an expression for the maximal probability if you split the A part into two parts but get the full B part. Also, we have not yet made use of the fact that both attackers have to answer equally. In the following section, we try to improve the bound using a different approach making use of both the A_1 and the A_2 part.

An improved bound via a state existence argument

We will connect the existence of good strategies for Bell state discrimination using a single round of simultaneous quantum communication to the existence of a cyclic graph state whose value p_W depends on the probability p_{succ} of correctly distinguishing the Bell state. To make this connection, we again consider an equivalent setting in which we purify the local inputs.

The verifiers locally generate an EPR pair, keep half of the pair locally, and send the other half as the input to the players. The task for A, B does not change, they need to perform a Bell State measurement and answer their outcome to the verifiers, who check if the answer they receive matches their local state. From the point of view of A, B nothing changes if the verifiers measure their local qubits before receiving an answer, or even before sending the qubits to A, B (which was our regular setting). Therefore, the probability that the verifiers have the same measurement outcome as the answer they receive in this purified setting is exactly the probability p_{succ} with which A, B can distinguish the Bell states in the non-purified protocol. The settings are in this sense equivalent.

Consider the state the verifiers hold in the purified picture after receiving the answers from A, B, but *before* they apply a Bell state measurement to check if the answer is correct. We know that this state has overlap p_{succ} with the Bell state that corresponds to the answer they received. We can now do the following:

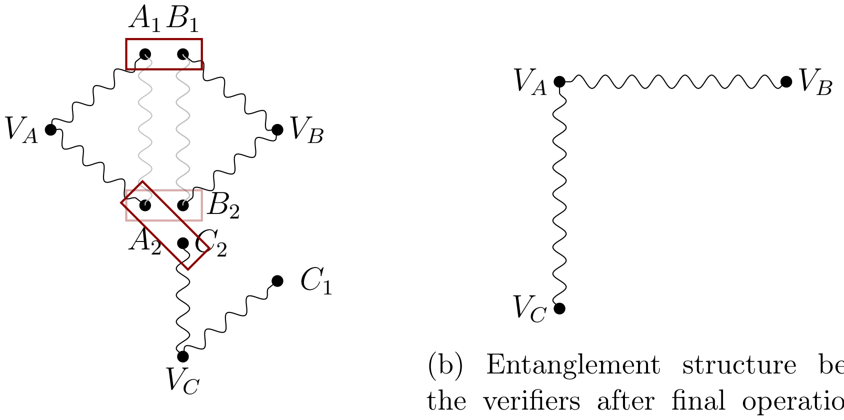
1. Apply a local Pauli operation that maps the answer they received to the antisymmetric Bell state.
2. Apply the same Haar random single-qubit unitary to both qubits, i.e. a *Werner twirling channel.*

Then, the state that we end up with is again a Werner state:

$$p\,|\Psi^-\rangle\langle\Psi^-| + (1-p)\left(\frac{\mathbb{1}_4}{4} - |\Psi^-\rangle\langle\Psi^-|\right), \tag{4.12}$$

where p is the parameter corresponding to the probability p_{succ} of successfully distinguishing the Bell states under quantum communication.

In its most general form, two players A, B will apply some map on their local inputs with two output registers, one that they keep and one that they send on to the other player. As we have established, the task of players A, B is to swap entanglement into the registers of V_A, V_B. Crucially, in the task of Bell state discrimination it is clear that the answer of only a single player suffices to distinguish the correct state since both players have to answer correctly. Conversely, this implies that only a single final operation at one of the players swaps an entangled state with overlap p to some Bell state into the registers of the verifiers.



(a) After the round of communication.

(b) Entanglement structure between the verifiers after final operations on A_1, B_1 and A_2, C_2.

Figure 4.5: Entanglement structure including a third hypothetical verifier V_C and player C who applies the same operation as B to his input. After the final measurement operation entanglement will be swapped to the shared state of the verifiers. We have omitted the entanglement structure with the individual registers here.

Now consider the situation in which there is a third verifier V_C, who behaves exactly like V_B, and we consider a third player C who applies the same quantum map as B on the input he receives from V_C. As a thought experiment, we now apply the same final operation on the A_2, C_2 register as would have been applied on the A_2, B_2 register. In Figure 4.5a we see the entanglement structure visualized after the communication round, but before the final operations. After the final operations, we get the structure as in Figure 4.5b. By the previous argument, the reduced states on V_A, V_B and V_A, V_C now both have overlap p_{succ} with some Bell state that corresponds to the answer the players get. Note that these Bell states do not have to be equal. By applying a local Pauli gate on the qubits of V_B and V_C we can bring both the two-qubit states between $V_A V_B$ and $V_A V_C$ to corresponding to the antisymmetric Bell state $|\Psi^-\rangle$. We can apply a *Werner Twirling Channel* on the joint state of the verifiers to end up with a line graph state with 3 vertices, where the reduced 2-qubit states are of the form as in Equation 4.12, where the parameter p for the reduced states on adjacent pairs of qubits is equal to p_{succ}.

We can extend the above argument by introducing more hypothetical verifiers, and combining them in the same way, to get a line graph state of odd length with any amount of vertices, where all the 2-qubit states on the line have overlap p_{succ} with a specific Bell state (as the attack is successful whenever the verifiers measure the Bell state that corresponds to the answer they receive). On a line we can apply Pauli gates to the individual qubits such that all the 2-qubit states have overlap with the antisymmetric $|\Psi^-\rangle$ state. A way to do this is to simply start at the left side of the graph and look what Bell state the first edge is supposed to be, and apply the Pauli gate on the right-hand qubit of the edge that brings this Bell state to the antisymmetric state $|\Psi^-\rangle$. Then the neighboring edge also gets mapped to another Bell state, but we can do the same procedure and map it to $|\Psi^-\rangle$ by applying a Pauli gate to the qubit on the right. Keep on doing this until you reach the other side of the chain, now the final Pauli gate only fixes the last edge, and what we end up with is a line graph state where all the neighboring qubits have overlap p_{succ} with $|\Psi^-\rangle$. This leads to the following proposition that relates strategies that use quantum communication to the existence of states:

4.2.2. PROPOSITION. *If there exists a strategy using a single round of simultaneous quantum communication for the task of Bell state discrimination, where the Bell states are picked uniformly at random, that succeeds with probability p_{succ}, then there exists a line graph state of any length n of qubits, such that all neighboring pairs of qubits are in Werner states with parameter $p = p_{\text{succ}}$.*

We now end up at a fundamental question of what p_{succ} are even possible for such a line graph state. Clearly $p_{\text{succ}} = 1$ is not possible due to monogamy of entanglement, but what range is possible? This problem can again be formulated as an SDP where we define a graph $G = (V, E)$, and we write $\Pi_e := \Pi \otimes \mathbb{1}_{\bar{e}}$ for the operators that are only applied to a single edge e.

Primal Problem

$$\begin{aligned} \max_{\rho} \quad & p \\ \textbf{subject to:} \quad & \forall e \in E : \mathrm{Tr}[\Pi_e^{\text{asym}} \rho] = p \\ & \mathrm{Tr}[\rho] = 1 \\ & \rho \succeq 0. \end{aligned}$$

The corresponding dual problem is:

Dual Problem

$$\textbf{min}\quad \lambda_{\max}\left(\sum_{e\in E} x_e \Pi_e^{\text{asym}}\right)$$
$$\textbf{subject to:}\quad \sum_{e\in E} x_e = 1.$$

Here, x_e are real numbers that have the restriction that they sum up to 1, and $\lambda_{\max}$ denotes the largest eigenvalue of the operator. By weak duality any feasible solution to the dual problem upper bounds the primal problem and thus p_{succ}. In general, for projectors to the antisymmetric subspace we can write $\Pi^{\text{asym}} = \frac{\mathbb{1}-\text{SWAP}}{2}$. Thus for the objective function in the Dual Problem we can write:

$$\begin{aligned}\lambda_{\max}\left(\sum_{e\in E} x_e \Pi_e^{\text{asym}}\right) &= \lambda_{\max}\left(\sum_{e\in E} x_e \frac{\mathbb{1}_e - \text{SWAP}_e}{2}\right)\\ &= \frac{1}{2} + \frac{1}{2}\lambda_{\max}\left(-\sum_{e\in E} x_e \text{SWAP}_e\right)\\ &= \frac{1}{2} - \frac{1}{2}\lambda_{\min}\left(\sum_{e\in E} x_e \text{SWAP}_e\right). \end{aligned}\tag{4.13}$$

For qubits we can write the SWAP operator between two systems i, j as a sum of the same Pauli operators applied on both systems $\text{SWAP}_{i,j} = \frac{1}{2}(\mathbb{1}_i \otimes \mathbb{1}_j + X_i \otimes X_j + Y_i \otimes Y_j + Z_i \otimes Z_j)$. Filling this into the above equation we get:

$$\begin{aligned}&\frac{1}{2} - \frac{1}{2}\lambda_{\min}\left(\sum_{e\in E} \frac{x_e}{2}(\mathbb{1}_{e_1} \otimes \mathbb{1}_{e_1} + X_{e_1} \otimes X_{e_2} + Y_{e_1} \otimes Y_{e_2} + Z_{e_1} \otimes Z_{e_2})\right)\\ &\quad = \frac{1}{4} - \frac{1}{2}\lambda_{\min}\left(\sum_{e\in E} \frac{x_e}{2}(X_{e_1} \otimes X_{e_2} + Y_{e_1} \otimes Y_{e_2} + Z_{e_1} \otimes Z_{e_2})\right). \end{aligned}\tag{4.14}$$

By weak duality we have that p_{succ} is less or equal to Equation 4.14 above for any feasible input on the line graph. Consider the feasible input on a line graph of length n where all the weights x_e are equal, then we get the following.

$$p_{\text{succ}} \leq \frac{1}{4} - \frac{1}{2}\lambda_{\min}\left(\frac{1}{2(n-1)}\sum_{i=1}^{n}(X_i \otimes X_{i+1} + Y_i \otimes Y_{i+1} + Z_i \otimes Z_{i+1})\right). \tag{4.15}$$

The operator whose minimal eigenvalue we seek is actually equal to the Hamiltonian of the well known spin 1/2 Heisenberg XXX model, and one can compute its spectrum using the Bethe Ansatz [Fad96]. The bound of p_{succ} can be computed with an SDP solver for the line graph and decreases for larger values of n. Taking the limit of $n \to \infty$ the value of p for the line coincides with the value for the infinite circle graph [ABB+87, Equation (2.50)], of which exact analytic solutions are known [Fad96]. The minimal eigenvalue converges to the ground state energy per site which converges to $1/2 - 2\ln(2)$. Plugging this into Equation 4.15 we get the following corollary.

4.2.3. Corollary. *The success probability of discriminating Bell states* p_{succ} *using a single round of simultaneous quantum communication is upper bounded by the value* $\ln(2) \approx 0.69$*. In particular, the attack success probability of* QPV_{Bell} *with no pre-shared entanglement is bounded by the same value.*

4.2.4 Lossy Quantum Communication Attack on $\text{QPV}_{\textsf{Bell}}$

In the previous part we considered attacks where attackers were allowed to use quantum communication but were not allowed to answer loss. Allowing attackers to also answer loss would be the most general setting for attackers who cannot pre-share entanglement. Unfortunately, our previous proof does not hold in the lossy case, since the operations attackers can apply to their local quantum registers after quantum communication are not LOCC operations (between the local attacker registers and the corresponding verifier) if attackers are allowed to postselect, but rather SLOCC. Thus, the monotonicity of the squashed entanglement no longer holds. Similarly, the measurement outcome can be alternating inconclusive when we try our state existence approach, thus getting no usable bounds. However, we still prove that there cannot be a perfect lossy quantum communication attack on the Bell state discrimination protocol, i.e. $p_{\text{succ}}(\eta) < 1$ for any transmission rate $\eta \in (0, 1]$.

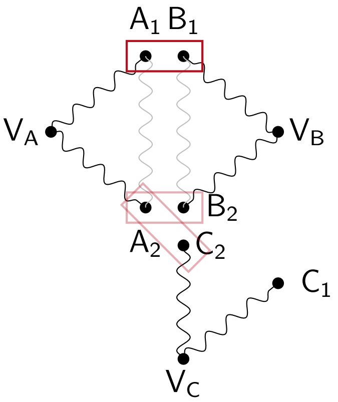


Figure 4.6: Entanglement structure including a third hypothetical verifier $\mathsf{V_C}$ and attacker C who applies an isometry $W_{C \to C_1 C_2}$ to his hypothetical input.

The argument goes as follows. Suppose there is a perfect lossy quantum communication attack, then for any loss rate, there must be some moment where both attackers decide to play. Condition on this event taking place, and consider the moment before both attackers measure their quantum systems. Suppose we now perform the measurement on the A_1B_1 quantum system, then by assumption we must get some Bell state i (indicating the correct one) as a measurement outcome with probability 1, thus generating a maximally entangled state between the verifiers V_A, V_B. Now consider the possibility of another verifier V_C who also sends as an input a half of an EPR pair, and some attacker C who applies the exact same splitting operation on her input as attacker B (see figure 4.6), thus locally $\rho_{B_2} = \rho_{C_2}$. By definition of a QPV protocol the measurement outcome we get from A_2, B_2 will be i with probability 1.

What would now happen if we apply the measurement of the attackers on the A_2, C_2 system? If this measurement is conclusive, then it must be correct with probability 1, thus creating a maximally entangled state between V_A, V_C, which would violate monogamy of entanglement since V_A is already maximally entangled with V_B. We conclude that the only possible measurement outcome on the A_2, C_2 system is an inconclusive '$\varnothing$' outcome.

There are now two options for the state $\rho_{A_2B_2}$, it can be either a product state or not. If it is a product state, it is indistinguishable from $\rho_{A_2} \otimes \rho_{C_2}$, which cannot be since the same measurement outcome on the A_2, C_2 systems will always be inconclusive, while on the A_2, B_2 systems it will be conclusive.

Suppose $\rho_{A_2B_2}$ is not a product state. Then again, the measurement on $\rho_{A_2B_2}$ will always be conclusive, while the measurement on $\rho_{A_2C_2} = \rho_{A_2} \otimes \rho_{C_2} = \rho_{A_2} \otimes \rho_{B_2}$ will always be inconclusive. Using this fact, we can perfectly distinguish the state $\rho_{A_2B_2}$ from $\rho_{A_2} \otimes \rho_{B_2}$, by simply applying the measurement an attacker would apply. However, the states $\rho_{A_2B_2}$ and $\rho_{A_2} \otimes \rho_{B_2}$ are never orthogonal to each other, thus there can be no procedure that perfectly discriminates the two quantum states without saying loss. This contradicts our findings, because the above is a hypothetical procedure that perfectly distinguishes the two quantum states.

We conclude that our assumption of a perfect lossy quantum communication attack must be wrong, which proves our claim. Thus we see that in general the $\mathrm{QPV}_{\mathsf{Bell}}$ cannot be perfectly attacked by unentangled attackers, which is the strongest statement we can make if we require attackers to not pre-share any entanglement. This argument cannot be extended to a finite gap in the attacking probability because of the subtlety that the measurements on $\rho_{A_1B_1}$ and $\rho_{A_2C_2}$ can be correlated. If attackers are allowed to make some errors, then the measurements on these states can be correlated such that they can be both conclusive but the measurement on $\rho_{A_2C_2}$ will then just be wrong, so monogamy of entanglement may not be violated.

4.2.5 Security of QPV$_{\mathsf{SWAP}}$ against quantum communication

Our technique to show security against quantum communication by considering the protocol in a purified setting and then analyzing the entanglement structure does not immediately allows us to show bounds on the QPV$_{\mathsf{SWAP}}$ protocol. As in this protocol the inputs are either equal or orthogonal product states, the answers of the attackers imply that the verifiers will hold two states that are either orthogonal or equal to each other. These states are not entangled, thus if we follow the reasoning and purify the inputs, the task of the attackers is to swap either an equal or orthogonal state between the two verifiers, which is not prohibited by any entanglement inequalities. However, we can reduce attacks on the QPV$_{\mathsf{SWAP}}$ protocol to attacks on a similar protocol where some inputs are entangled states, with similar success probabilities. We then show that for certain success probabilities such attacks do not exist, implying security with a finite gap of the QPV$_{\mathsf{SWAP}}$ against attackers with access to quantum communication, but no pre-shared entanglement.

Suppose we have an attack on the QPV$_{\mathsf{SWAP}}$ protocol that has a success probability of $3/4 - \alpha$, where $\alpha \geq 0$ is some value that indicates how close our attack is to the optimal success probability of 3/4. We write $\{\Pi^{qc}_{=}, \Pi^{qc}_{\neq}\}$ for the attackers POVM elements that attain this value. Write $\rho_{=}, \rho_{\neq}$ for the density matrices of the input qubits that are either equal or orthogonal in some uniformly random basis. Then we can write for the success probability:

$$p_{\text{succ}} = \frac{1}{2}\big(\mathrm{Tr}[\Pi^{qc}_{=}\rho_{=}] + \mathrm{Tr}[\Pi^{qc}_{\neq}\rho_{\neq}]\big) = \frac{3}{4} - \alpha. \tag{4.16}$$

From Equation 3.2 we know that we can write $\rho_{=}, \rho_{\neq}$ as a linear combination of projectors to the symmetric and antisymmetric subspace:

$$\rho_{=} = \frac{\Pi_{\text{sym}}}{3}, \qquad\qquad \rho_{\neq} = \frac{1}{2}\left(\frac{\Pi_{\text{sym}}}{3} + \Pi_{\text{asym}}\right). \tag{4.17}$$

Then Equation 4.16 becomes:

$$\frac{1}{2}\,\mathrm{Tr}\left[\Pi^{qc}_{=}\left(\frac{\Pi_{\text{sym}}}{3}\right)\right] + \frac{1}{2}\,\mathrm{Tr}\left[\Pi^{qc}_{\neq}\frac{1}{2}\left(\frac{\Pi_{\text{sym}}}{3} + \Pi_{\text{asym}}\right)\right] = \frac{3}{4} - \alpha. \tag{4.18}$$

Multiplying both sides by 2, and using that $\Pi^{qc}_{=} + \Pi^{qc}_{\neq} = \mathbb{1}$, we can rewrite this to

$$\begin{aligned} \mathrm{Tr}\left[\Pi^{qc}_{=}\left(\frac{\Pi_{\text{sym}}}{3}\right)\right] + \frac{1}{2}\,\mathrm{Tr}\left[(\mathbb{1} - \Pi^{qc}_{=})\left(\frac{\Pi_{\text{sym}}}{3}\right)\right] + \frac{1}{2}\,\mathrm{Tr}\left[\Pi^{qc}_{\neq}(\Pi_{\text{asym}})\right] &= \frac{3}{2} - 2\alpha \\ \Leftrightarrow \frac{1}{2}\,\mathrm{Tr}\left[\Pi^{qc}_{=}\left(\frac{\Pi_{\text{sym}}}{3}\right)\right] + \frac{1}{2}\,\mathrm{Tr}\left[\Pi^{qc}_{\neq}(\Pi_{\text{asym}})\right] &= 1 - 2\alpha. \end{aligned} \tag{4.19}$$

For qubits we have $\Pi_{\text{asym}} = |\Psi^-\rangle\langle\Psi^-|$. So, one can interpret the last equation as the probability of success of the POVM defined by the optimal attack on the $\text{QPV}_{\mathsf{SWAP}}$ protocol, where one gets either a random symmetric state with probability $\frac{1}{2}$, or the antisymmetric state with probability $\frac{1}{2}$. Thus, if an attack with probability $3/4 - \alpha$ exists, then we can also attack this new protocol with probability $1 - 2\alpha$.

For this new protocol, we can use our technique of showing upper bounds by purifying the protocol and analyzing the entanglement structure, as we did in Section 4.2.3. When we purify the inputs, and the attackers apply their measurement, they should answer half of the time 'symmetric' or 'antisymmetric'. From Equation 4.4 we see again that if the attackers need to swap the respective state into the registers of the verifiers. As a symmetric state does not have to be entangled, this is possible for the attackers to do, but whenever the attackers answer 'antisymmetric' they need to swap the $|\Psi^-\rangle$ to the registers of the verifiers. The success probability of this task is upper bounded by 0.926 as in Equation 4.11. Thus, the overall probability of success of the induced protocol is upper bounded by $1/2 + 1/2 \cdot 0.926 = 0.963$. And we get a bound on p_{succ} in Equation 4.16:

$$1 - 2\alpha \leq 0.963 \Leftrightarrow p_{\text{succ}} = \frac{3}{4} - \alpha \leq 0.7315. \tag{4.20}$$

This implies that the best attack on the $\text{QPV}_{\mathsf{SWAP}}$ protocol if we allow the attackers to have quantum communication but no pre-shared entanglement cannot be higher than 0.7315.

Security against lossy quantum communication for $\text{QPV}_{\mathsf{SWAP}}$

The proof in Section 4.2.4 of security of the Bell state measurement for any transmission rate against unentangled attackers with access to quantum communication can also be reduced to the security of the $\text{QPV}^{\eta}_{\mathsf{SWAP}}$ protocol with the same attack model.

As we have seen in Equation 4.19, if a success probability of 3/4 can be achieved for attacking the SWAP test, then there is also a strategy that perfectly answers another protocol, where the inputs are either a random symmetric state or the antisymmetric state. In particular, this allows one to perfectly distinguish $|\Psi^-\rangle$ from the other Bell states. We will show that if the SWAP test could be implemented perfectly with local actions and one round of quantum communication for some $0 < \eta \leq 1$, then so could the Bell measurement with some different $\eta' < \eta$, contradicting our result in 4.2.4, thus implying that there exists no perfect lossy attack of the SWAP test.

4.2.4. Proposition. *$\text{QPV}_{\mathsf{SWAP}}$ cannot be perfectly attacked if attackers A, B can use quantum communication between them, regardless of the loss rate $1 - \eta$, for any $\eta \in (0, 1]$.*

Proof:
Assume there is a procedure, using only local actions and one round of simultaneous quantum communication, perfectly simulating $\{\Pi_{\text{sym}}, \Pi_{\text{a-sym}}\}$ with probability $0 < \eta \leq 1$. Then, conditioned on their procedure giving a conclusive result (which happens with probability η), attackers A, B could apply the following to attack QPV$_{\mathsf{Bell}}$ with a Bell measurement at P and an input chosen uniformly at random from $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$:

- Whenever their procedure returns “anti-symmetric”, return $|\Psi^-\rangle$
- Whenever it returns “symmetric”, return the loss symbol $\varnothing$

However, this would be suspicious, because the only conclusive answers would be $|\Psi^-\rangle$. In order to achieve $\mathbb{P}(\varnothing \,|\, B_i) = 1 - \eta$ for all Bell states $|B_i\rangle$ and $\mathbb{P}(B_i \,|\, \text{concl.}) = 1/4$, as the honest P would do in QPV$_{\mathsf{Bell}}$, they could apply $\mathbb{1}_A \otimes (X^a Z^b)_B$ with $a, b \in \{0, 1\}$ chosen uniformly at random in each round as soon as they receive the inputs. This just transfers the input to a different Bell state. If they adjust their responses to

- When this procedure returns “anti-symmetric”, answer $\mathbb{1}_A \otimes (Z^b X^a)_B |\Psi^-\rangle$
- When it returns “symmetric”, answer the loss symbol $\varnothing$

They achieve $\mathbb{P}(\varnothing \,|\, B_i) = 1 - \eta$ as well as $\mathbb{P}(B_i \,|\, \text{concl.}) = 1/4$ and whenever they do answer conclusively, they will be correct (by assumption). But this would give them a perfect attack on QPV$_{\mathsf{Bell}}$ with some play rate $\eta' < \eta$ (because they throw away the “symmetric” measurement results). This contradicts the fact that $p_{\text{succ}}(\eta) < 1$ for all η in QPV$_{\mathsf{Bell}}$. □

4.2.6 Considerations on loss tolerance in QPV

Ideally, for QPV to become feasible, one would like to have a protocol that is fully loss tolerant, secure against attackers being able to pre-share a bounded amount of entanglement and to use quantum communication between them. So far, there has been no such protocol. Here we give a no-go result, based on a simple observation. We show that no such protocol can exist that fulfills all three of the above properties. However, not all is lost for two reasons. In practice, one may be able to achieve *good enough* partial loss tolerance, for example by increasing the quantum input dimension or the number of possible quantum operations P can apply. Secondly, as we will see in Chapter 5, we can construct a modification of the regular QPV protocol where we introduce a *commitment round* for the prover, rendering lossy attacks irrelevant for a certain class of protocols.

For simplicity, consider the following quite-general two-verifier QPV protocol[4]:

- Verifiers $\mathsf{V_A}, \mathsf{V_B}$ send d_A, d_B dimensional quantum inputs, respectively, to P. They also send classical information x, y (of any size), respectively.
- P computes a function $f(x, y)$ and, based on that result, applies a quantum operation $\mathcal{Q}_{f(x,y)}$ to the inputs. This yields two outputs, one intended for $\mathsf{V_A}$ and one for $\mathsf{V_B}$. These outputs are forwarded to the corresponding verifier.
- The verifiers check if what they received matches the specific honest protocol and that the responses arrived in time.

We will denote this as $\mathrm{QPV}(d_A, d_B, f)$ and the protocol will be repeated for n rounds, either sequentially or in parallel. Now let $k := |\operatorname{Im}(f)|$ be the number of possible quantum operations to be applied by the prover. It turns out that there always exists a perfect attack consuming at most $O(n \log d)$ (qubit) EPR pairs, where $d = \max\{d_A, d_B\}$, as long as the loss is high enough. We make this precise in the following statement.

4.2.5. Proposition. *Let* $d = \max\{d_A, d_B\}$ *and* $k = |\operatorname{Im}(f)|$. *Any* n*-round* $\mathrm{QPV}(d_A, d_B, f)$ *protocol can be attacked with* $O(n \log(d))$ *EPR pairs if the fraction* η *of rounds that is used for security analysis fulfills* $\eta \leq \frac{1}{kd^2}$.

Proof:
Without loss of generality, let attacker A receive classical input x. As soon as A receives his quantum input, quantum teleportation [BBC+93] can be used to teleport the state to B (consuming a $d = \max\{d_A, d_B\}$ dimensional maximally entangled state[5]), after which A sends to B which teleportation corrections were to apply and the classical information x. With probability $p_{00} = 1/d^2$ there are no teleportation corrections to apply, in which case B holds both input states locally and before the honest party P would have received them. B can guess the value of $f(x, y)$ and immediately apply the operation P was asked to apply, send the part (e.g. a subsystem or a measurement result) that $\mathsf{V_A}$ is supposed to receive to A and keep the part that $\mathsf{V_B}$ is supposed to receive. With probability $1/k$ attacker B guesses the value of $f(x, y)$ correctly. If the quantum state picked up teleportation corrections in the first place or if it turns out that B guessed $f(x, y)$ wrongly (of which both get to know as soon as they receive the communication from the other attacker), the attackers deny to answer and both send the corresponding loss symbol '$\varnothing$'. If there were no corrections to apply and B guessed $f(x, y)$ correctly, both send their respective parts that the verifiers are supposed to receive to them.

[4] The result that follows can be straightforwardly generalized to m verifiers, for which a general attack would be to teleport all quantum inputs to one fixed attacker, who then performs the guessing attack. In that case, the probability that teleportation does not need corrections is much lower, i.e. $1/d^{2(m-1)}$.

[5] Attackers do not know the dimension of their local inputs a priori.

As they are only required to answer $\eta \leq \frac{1}{kd^2}$ of all rounds, they can simply choose those perfect rounds without teleportation corrections and a correct guess for $f(x, y)$. Applying this strategy in each round costs them $n \log d$ (qubit) EPR pairs. □

The statement shines light on another facet of loss tolerance – the attacker's ability to post-select on a "correct" guess after communication. They can always do that, if they pre-share entanglement, by simply guessing the teleportation corrections. In protocols with quantum input from one side and classical information determining the action of P, like [KMS11, CL15, Unr14, JKPPG21, BCS22], attackers can, even without pre-shared entanglement, do this post-selection simply by first guessing $f(x, y)$, then applying the operation $\mathcal{Q}_{f(x,y)}$ on the quantum input and communicating x, y to each other so that both attackers know if the initial guess was correct or not. This is captured in the above bound, identifying all-classical input from one side with $d = 1$. In that sense, QPV protocols that contain classical input cannot be fully loss-tolerant. It is now also clearer why the protocol in [LXS+16] and our QPV$_{\mathsf{SWAP}}$ [ABSV22b] are fully loss-tolerant if attackers do not pre-share any entanglement. Without shared entanglement, the attackers simply have no way of ever knowing if their guess was correct because there is no information about it leaving the verifiers.

We see that for this structure of QPV protocols, there cannot exist a fully loss-tolerant QPV protocol if the loss is high enough. However, in the next chapter we show that there is actually a way around Proposition 4.2.5 by slightly altering the structure of a QPV protocol. We will introduce a so-called commitment round, where the attackers have to commit to receiving the quantum information before they receive the classical information that determines, for example, the basis they have to measure in. By forcing attackers to commit, they cannot hide their wrong guesses in the loss answers.

4.3 Discussion

In this chapter, we gave an explicit example of the first QPV protocol in which there is an advantage for attackers who share no entanglement to use quantum communication over classical communication. The protocol depends on determining whether two states were either both symmetric or both antisymmetric. The probability of success under LOCC operations was analytically shown to be equal to 17/18, while attackers with access to quantum communication could attack this protocol perfectly with a single round of simultaneous quantum communication. This suggests that the role of quantum communication may be more important than previously thought.

Diving into the idea that there can be an advantage in using quantum communication over classical communication, we also showed that this separation between quantum communication and classical communication was somewhat constructed. The existence of a quantum communication attack on a protocol that is safe against attackers restricted to classical communication implies the existence of a similar protocol that is safe against quantum communication. In order to prove this, we showed that for every quantum communication attack, two new QPV protocols arise. By repeating this argument whenever there was a quantum communication attack, we used the theorem of emergent classicality of channels from [QR21] to show that the quantum inputs become approximately classical, which in turn implies the existence of a classical communication attack on the original protocol which violated the assumption of the original being secure against classical communication. Thus, ultimately showing that somewhere in the recursion there must have been a protocol that was secure against attackers allowed to use a single round of simultaneous quantum communication.

Setting out to find an explicit example of a protocol that is safe against quantum communication, we prove that the task of Bell state discrimination cannot have a higher success probability than $\ln(2) = 0.6931...$ when two attackers are restricted to local operations and a single round of quantum communication. This is higher than the optimal success probability of $1/2$ for attackers restricted to classical communication. We suspect that the quantum communication bound to be lower than $\ln(2)$, but have been unable to make the bound tighter. This is the first example of a protocol that is fully loss-tolerant against classical communication and stays secure against attackers using quantum communication.

The previous statement immediately brings up the question whether the protocol is also safe against attackers allowed to use quantum communication and allowed to say loss. We answer this question in the affirmative and prove that there cannot be a strategy that perfectly distinguishes all Bell states. However, we only find a strict inequality, i.e. that $p^{\mathrm{qc}}_{\mathrm{succ}}(\eta) < 1$ for any transmission rate $\eta \in (0,1]$. An interesting follow-up question is whether we can make this bound into a finite gap, just as with the case where the attackers were not allowed to say loss but could use quantum communication. Nevertheless, this is the first example of a QPV protocol that remains fully loss tolerant and secure even in the quantum communication setting. This is of interest since it is the most general setting in the case where we do not allow attackers to pre-share entanglement.

We find that our techniques also allow us to give bounds on the success probability of attacking the $\mathrm{QPV}_{\mathsf{SWAP}}$ from the previous chapter with quantum communication. By reducing an attack on $\mathrm{QPV}_{\mathsf{SWAP}}$ to an attack on a protocol in which some inputs are entangled, we apply our technique of purifying the inputs and looking at the entanglement structure to bound the success probability to 0.7315, which is also still higher than the best classical attack of $2/3$. One could improve this bound via the route of a state existence argument again, which requires getting solutions the optimization of maximizing the overlap of reduced two-qubit states where the pairs of qubits have to be either highly symmetric or antisymmetric. We also find that there exists no perfect lossy attack using quantum communication on $\mathrm{QPV}_{\mathsf{SWAP}}$, by proving that if such an attack exists, there exists an even lossier attack on $\mathrm{QPV}_{\mathsf{Bell}}$.

Extending on the idea of incorporating loss in different settings for attackers, we note that in order for QPV to become feasible, not only do we want our protocols to be loss-tolerant against quantum communication, but we also want our protocols to be loss-tolerant against some amount of pre-shared entanglement among the attackers. However, we show that any QPV protocol can be attacked by only a linear amount of entanglement in this setting, given that the loss is high enough. This is based on the simple observation that in such a scenario attackers can post-select on those rounds in which the attempted quantum teleportation did not incur teleportation corrections.

4.A Appendices

4.A.1 Optimal PPT Measurements for $\mathrm{QPV}_{\mathbf{Sym/Antisym}}$

In this section, we will solve the SDP program that optimizes the probability of success for two adversaries restricted to LOCC operations of discriminating a random symmetric state from the antisymmetric state. The SDP formulation of this protocol is as follows:

$$\begin{aligned}
&\textbf{Primal Problem}\\
\textbf{maximize:}\quad & \frac{1}{2}\operatorname{Tr}[\Pi_0\rho_0+\Pi_1\rho_1]\\
\textbf{subject to:}\quad & \Pi_0+\Pi_1=\mathbb{1}_{2^2}\\
& \Pi_k\in \mathrm{PPT}(\mathsf{A}:\mathsf{B}),\quad k\in\{0,1\}\\
& \Pi_i\succeq 0,\ \text{for}\quad i\in\{0,1\}\\
&\textbf{Dual Problem}\\
\textbf{minimize:}\quad & \operatorname{Tr}[Y]\\
\textbf{subject to:}\quad & Y-Q_i^{T_{\mathsf{B}}}-\rho_i/2\succeq 0,\quad i\in\{0,1\}\\
& Y\in \mathrm{Herm}(\mathsf{A}\otimes\mathsf{B})\\
& Q_i\in \mathrm{Pos}(\mathsf{A},\mathsf{B}),\quad i\in\{0,1\}.
\end{aligned}$$

Where we write ρ_0 for ρ_{sym} and ρ_1 for ρ_{antisym} whose respective density matrices are:

$$\rho_0=\frac{1}{6}\begin{pmatrix}2&0&0&0\\0&1&1&0\\0&1&1&0\\0&0&0&2\end{pmatrix},\qquad \rho_1=\frac{1}{2}\begin{pmatrix}0&0&0&0\\0&1&-1&0\\0&-1&1&0\\0&0&0&0\end{pmatrix}.$$

A feasible solution for the primal problem, is to measure both states in the computational basis and answer the XOR of the measurement outcomes, so $\Pi_0=|00\rangle\langle 00|+|11\rangle\langle 11|,\Pi_1=|01\rangle\langle 01|+|10\rangle\langle 10|$. This strategy has success probability $\frac{1}{2}\operatorname{Tr}[\Pi_0\rho_0+\Pi_1\rho_1]=5/6$. A feasible solution to the corresponding dual is:

$$Y=\begin{pmatrix}\frac{1}{6}&0&0&0\\0&\frac{1}{4}&-\frac{1}{12}&0\\0&-\frac{1}{12}&\frac{1}{4}&0\\0&0&0&\frac{1}{6}\end{pmatrix},\quad Q_0=0,\quad Q_1=\frac{1}{6}\begin{pmatrix}1&0&0&1\\0&0&0&0\\0&0&0&0\\1&0&0&1\end{pmatrix}=\frac{1}{3}\left|\Phi^+\right\rangle\left\langle\Phi^+\right|.$$

Y is hermitian, Q_0,Q_1 are both positive, $Y-Q_0^{T_B}-\rho_0/2=1/6\,|\Psi^-\rangle\langle\Psi^-|\succeq 0$, and $Y-Q_1^{T_B}-\rho_1/2=0\succeq 0$. Thus, Y is feasible to the dual problem and

$\mathrm{Tr}[Y] = 5/6$ is a lower bound of the success probability of the protocol optimized over all PPT measurements. We see that these feasible solutions for the primal and dual problem are equal, thus we know that the value is optimal over all PPT measurements. So the highest probability of success for adversaries restricted to LOCC operations is 5/6, which can also be attained by the measurement described in the primal problem.

Now for the protocol where we double the input rounds, but restrict the inputs to be either both symmetric or antisymmetric states, we will show that there is no perfect LOCC attack. The corresponding SDP that optimizes over all PPT strategies looks as follows:

$$\begin{aligned}
& \textbf{Primal Problem} \\
\textbf{maximize: } & \frac{1}{2}\mathrm{Tr}[\Pi_0(\rho_0 \otimes \rho_0) + \Pi_1(\rho_1 \otimes \rho_1)] \\
\textbf{subject to: } & \Pi_0 + \Pi_1 = \mathbb{1}_{2^4} \\
& \Pi_k \in \mathrm{PPT}(\mathsf{A} : \mathsf{B}), \quad k \in \{0,1\} \\
& \Pi_i \succeq 0, \text{ for } \quad i \in \{0,1\} \\
& \textbf{Dual Problem} \\
\textbf{minimize: } & \mathrm{Tr}[Y] \\
\textbf{subject to: } & Y - Q_i^{T_\mathsf{B}} - (\rho_i \otimes \rho_i)/2 \succeq 0, \quad i \in \{0,1\} \\
& Y \in \mathrm{Herm}(\mathsf{A} \otimes \mathsf{B}) \\
& Q_i \in \mathrm{Pos}(\mathsf{A}, \mathsf{B}), \quad i \in \{0,1\}.
\end{aligned}$$

We will show that the following is a feasible solution to the dual

$$\begin{aligned}
Y = \frac{1}{18}(9(\rho_0 \otimes \rho_0) + 8(\rho_1 \otimes \rho_1)),\ & Q_0 = 0 \succeq 0, \\
Q_1 = \frac{1}{18}\Big((3\rho_0^{T_\mathsf{B}} \otimes 3\rho_0^{T_\mathsf{B}}) - (\rho_1^{T_\mathsf{B}} \otimes \rho_1^{T_\mathsf{B}})\Big).&
\end{aligned}$$

Note that in contrast to the optimizations for $\mathrm{QPV}^n_{\mathrm{SWAP}}$ protocols, the matrix Y is not equal to the identity matrix with some factor, but nevertheless it is Hermitian. The eigenvectors of $3\rho_0^{T_\mathsf{B}}$ and $\rho_1^{T_\mathsf{B}}$ are the 4 Bell states $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$ with eigenvalues $\{3/2, 1/2, 1/2, 1/2\}$ and $\{-1/2, 1/2, 1/2, 1/2\}$ respectively. We see for any of the 16 possible eigenvectors of Q_1 that the corresponding eigenvalues will be $0, \frac{1}{9}$ or $\frac{1}{18}$. We conclude that $Q_1 \succeq 0$ since all its eigenvalues are non-negative and it is Hermitian (the partial transpose maps Hermitian matrices to Hermitian matrices).

For Q_0 the first constraint in the dual problem becomes:

$$\begin{aligned} Y - Q_0^{T_{\mathrm{B}}} - \frac{(\rho_0 \otimes \rho_0)}{2} &= \frac{1}{18}(9(\rho_0 \otimes \rho_0) + 8(\rho_1 \otimes \rho_1)) - \frac{(\rho_0 \otimes \rho_0)}{2} \\ &= \frac{4}{9}(\rho_1 \otimes \rho_1) \succeq 0. \end{aligned}$$

And for Q_1 we get:

$$\begin{aligned} Y - Q_1^{T_{\mathrm{B}}} - \frac{(\rho_1 \otimes \rho_1)}{2} &= \frac{1}{18}(9(\rho_0 \otimes \rho_0) + 8(\rho_1 \otimes \rho_1)) \\ &\qquad - \frac{1}{18}(9(\rho_0 \otimes \rho_0) - (\rho_1 \otimes \rho_1)) - \frac{(\rho_1 \otimes \rho_1)}{2} \\ &= 0 \succeq 0. \end{aligned}$$

Thus we have shown that all conditions in the dual problem are met, and we get an upper bound on the success probability over all PPT measurements of

$$\mathrm{Tr}[Y] = \mathrm{Tr}\left[\frac{1}{18}(9(\rho_0 \otimes \rho_0) + 8(\rho_1 \otimes \rho_1))\right] = \frac{17}{18}.$$

There is an LOCC strategy that attains this upper bound, namely applying the single-round strategy twice, where we only answer asymmetric if both pairs have unequal measurement. This strategy is correct on all input states except when as an input twice the $|\Psi^+\rangle$ input is sent. This happens with probability 1/18. Thus, the best attack for adversaries restricted to LOCC operations has success probability $\frac{17}{18}$, in contrast to adversaries who may use quantum communication for whom there is a perfect attack with success probability 1 by simply swapping the second register and applying the SWAP test locally.

Chapter 5

Full Loss Tolerance via Commitment Rounds

Signal loss poses a significant threat to the security of quantum cryptography when the chosen protocol lacks loss-tolerance. In quantum position verification (QPV) protocols, even relatively small loss rates can compromise security. The goal is thus to find protocols that remain secure under practically achievable loss rates. In this chapter, we modify the usual structure of QPV protocols and prove that this modification makes the potentially high transmission loss between the verifiers and the prover security-irrelevant for a class of protocols that includes a practically interesting candidate protocol inspired by the BB84 protocol ($\mathrm{QPV}_{\mathrm{BB84}}^{f}$). This modification, which involves photon presence detection, a small time delay at the prover, and a commitment to play before proceeding, reduces the overall loss rate (for security purposes) to just the prover's laboratory. The adapted protocol $\mathsf{c}\text{-}\mathrm{QPV}_{\mathrm{BB84}}^{f}$ then becomes a practically-feasible QPV protocol with strong security guarantees, even against attackers using adaptive strategies. As the loss rate between the verifiers and the prover is mainly dictated by the distance between them, secure QPV over longer distances becomes possible. We also show possible implementations of the required photon presence detection, making $\mathsf{c}\text{-}\mathrm{QPV}_{\mathrm{BB84}}^{f}$ a protocol that solves all major practical issues in QPV. Finally, we discuss experimental aspects and give parameter estimations.

This chapter is based on the paper "Making Existing Quantum Position Verification Protocols Secure Against Arbitrary Transmission Loss" by Rene Allerstorfer, Andreas Bluhm, Harry Buhrman, Matthias Christandl, Llorenç Escolà-Farràs, Florian Speelman, and Philip Verduyn Lunel [ABB+23].

5.1 Introduction

To practically implement a QPV protocol in a realistic setting, several crucial properties must be taken into consideration. Firstly, the protocol must be secure against attackers with access to quantum communication and restricted to a reasonable amount of entanglement. Secondly, it must be secure against *slow* quantum information. This is a point that we have not yet discussed, but qubits in a fiber-optic cable will only travel at typically 2/3 of the speed of light. Third, the operations of the honest prover have to be reasonably simple that he can apply them fast enough. Lastly, the protocol must be secure against loss. As we have seen before, some protocols are completely insecure if the loss rates are high enough.

As any QPV protocol can be attacked using an exponential amount of entanglement, we know that unconditionally secure protocols for QPV are impossible. Therefore, the aim has shifted to proving practical security of QPV protocols. Since it is hard to generate and maintain entanglement, it would suffice to find protocols that require an unrealistically large amount of entanglement for an attack, thereby achieving information-theoretic security in practice. Therefore, the main interest at present is to consider security against bounded attackers. For example, the $\text{QPV}_{\mathsf{SWAP}}$ introduced in Chapter 3, while not being secure against slow quantum communication, has some desirable properties. The protocol is very easy to implement for an honest prover, and when executed in parallel attackers need to pre-share an amount of entanglement that scales with the number of rounds. In practice, the fact that the entanglement needed scales with the amount of rounds played in parallel is not a very strong security guarantee since the number of qubits the honest prover also scales with the number of rounds. Ideally, we would like to find protocols where the honest prover has to manipulate a small quantum system, while the attackers need to pre-share a very large entangled state, i.e., many EPR pairs.

Significant progress towards solving these properties was made in [BCS22], with a different version of the protocol, $\text{QPV}^f_{\text{BB84}}$. Here, the basis in which the honest prover needs to apply his measurement is determined by a classical function f depending on two n-bit input strings x, y. In the paper, the authors prove security against $\Omega(n)$ entangled pairs pre-shared by the attackers for a random function f. Note that in this protocol there is only a single qubit, but the required quantum resources for an attack scale at least linearly in the classical information sent. For an honest prover, it is much easier to do some computation on classical inputs than on quantum inputs. It has the additional advantage of being secure even with slowly traveling qubits such as, for example, qubits sent over optical fiber, where the transmission speed is 2/3 the speed of light. Moreover, in a future quantum network it will likely often be the case that there is no direct link between the verifiers and the prover wanting to run a QPV protocol, underscoring the need for protocols that can deal with slow quantum information. Other protocols combining classical and quantum information can be found in [KMS11, CL15, Unr14, JKPPG21, QS15, AER$^+$23]. Attacks for such protocols have also been analyzed in [BFSS13, Spe16a, OCCG20].

Although the protocol $\text{QPV}^f_{\text{BB84}}$ is also resistant against small amounts of noise and loss as shown in [BCS22, ES23], none of the above protocols is proved secure under conditions consistent with current technologies, where the main source of error is photon loss. Using optical fiber, photon transmission decays exponentially in the distance and at some point almost all photons will be lost. This can compromise security in QPV protocols that are not loss tolerant, and immediately makes $\text{QPV}^f_{\text{BB84}}$ insecure in basically any practical setting. This is a major downside of $\text{QPV}^f_{\text{BB84}}$, since apart from this issue it has the most desirable properties of all known proposed protocols.

A common approach to deal with photon loss is to disregard rounds in which the prover claims that a photon was lost during transmission. Regrettably, this approach renders these protocols vulnerable to attackers since the attacks can take advantage of the photon loss by claiming the photon was lost if they risk being detected. Recent progress toward addressing this major obstacle to protocols that can be implemented on current devices has been made in [ABSV22b, ABSV22a], where fully loss-tolerant protocols were studied. However, these protocols were found to be vulnerable against simple entanglement-based attacks. Even though loss is not an issue in [LLQ22] as all the communication is classical, their protocol requires a large quantum computer at the prover to prepare the states used in it and therefore is not viable in the near-term. So far, a protocol has been lacking that is both provably secure against realistic attacks while still being implementable with current technologies.

In this chapter, we focus on the design of such a practically-feasible and secure QPV protocol. We introduce a structural modification to QPV where, instead of the verifiers sending the information to the prover such that all information arrives at the same time, the quantum information shall arrive slightly before the classical information. The prover confirms the reception of the quantum information, and *commits* to playing, after which he receives the classical information to complete the task. In this way, for every QPV protocol P, we define its *committing* version $\mathsf{c}\text{-}\mathsf{P}$.

Consider a secure QPV protocol P with classical prover responses, which remains secure when played in sequential repetition and in which the honest quantum information is allowed to travel slowly (like $\text{QPV}^f_{\text{BB84}}$). This implies that the protocol is *state-independent*, in the sense that the attackers can replace the input state with any other quantum state. Then our main result states that for every such QPV protocol P, its committing version $\mathsf{c}\text{-}\mathsf{P}$ inherits the security of P, while becoming fully loss tolerant against transmission loss. Denoting by η_V the transmission rate from the verifiers to the prover and by η_P the one within the prover's laboratory (between committing and receiving the classical information), we informally state our main result, Theorem 5.4.10, as follows:

5.1.1. THEOREM (Informal). *The success probability of attacking* $\mathsf{c}\text{-}\mathsf{P}$ *(with both* η_V *and* η_P*) reduces to the probability of attacking* P *(with only* η_P*):*

$$\mathbb{P}[\text{attack}\,\mathsf{c}\text{-}\mathsf{P}_{\eta_V,\eta_P}] \leq \mathbb{P}[\text{attack}\,\mathsf{P}_{\eta_P}] + (1-2\tilde{c})8\sqrt{\varepsilon} + 2\tilde{c}, \tag{5.1}$$

where ε *and* $\tilde{c}$ *are parameters that can be made arbitrarily small by running more rounds.*

This means that the potentially very high loss between the verifiers and the prover, $1-\eta_V$, becomes irrelevant to security in $\mathsf{c}\text{-}\mathsf{P}_{\eta_V,\eta_P}$ and only the much smaller loss at the prover's laboratory, $1-\eta_P$, matters. And for sufficiently high values of η_P we often have security guarantees, e.g. for $\text{QPV}^f_{\text{BB84}}$ [BCS22, ES23]. In theory, for an ideal prover, $\mathsf{c}\text{-}\mathsf{P}_{\eta_V,\eta_P}$ becomes fully loss-tolerant.

If we demand perfect coordination in commitments for all possible inputs, which is expected from the honest prover, this will correspond to $\varepsilon = \tilde{c} = 0$. Then our result reduces to

$$\mathbb{P}[\text{attack}\,\mathsf{c}\text{-}\mathsf{P}_{\eta_V,\eta_P}] = \mathbb{P}[\text{attack}\,\mathsf{P}_{\eta_P}], \tag{5.2}$$

as the other direction $\mathbb{P}[\text{attack}\,\mathsf{P}_{\eta_P}] \leq \mathbb{P}[\text{attack}\,\mathsf{c}\text{-}\mathsf{P}_{\eta_V,\eta_P}]$ is simple to see[1]. The above theorem allows for $\varepsilon \neq 0 \neq \tilde{c}$ in attack strategies to make our argument robust, as very small values of ε (relative to the number of committed rounds) or $\tilde{c}$ (relative to the 2^{2n} input pairs x, y) could in principle help attackers, while leaving them undetected.

Applying our results to $\text{QPV}^f_{\text{BB84}}$, we show that quantum position verification is possible even if the loss is arbitrarily high, the (constant-sized) quantum information is arbitrarily slow, and attackers pre-share some entanglement (bounded in the classical message length n). The question of a super-linear lower bound on the required resources for a quantum attack still remains open.

Finally, we study two possible ways of implementing the non-demolition photon presence detection step of our protocol: true photon presence detection as demonstrated in [NFLR21] as a potential long-term solution, and a simplified photon presence detection based on a partial Bell measurement [MMWZ96] at the prover that is technologically feasible today. In the latter, the honest prover essentially teleports the input state of the protocol to himself and concludes the presence of that state based on a conclusive click pattern in the partial Bell measurement, in which case the quantum state got teleported and can be further acted on by the prover (e.g. by a polarization measurement). We note that for the committing version of $\text{QPV}^f_{\text{BB84}}$, $\mathsf{c}\text{-}\text{QPV}^f_{\text{BB84}}$, no active feedforward for the teleportation corrections is required, as they predictably alter the subsequent

[1] The attackers can just pre-agree to commit with a rate η_V and use the strategy of P_{η_P} to produce the answers for $\mathsf{c}\text{-}\mathsf{P}_{\eta_V,\eta_P}$.

measurement outcome and thus can be classically corrected by the prover post-measurement. We identify the experimental requirements at the prover as: being able to generate an EPR pair, to do a partial Bell measurement, to store the teleported quantum state in a short delay loop until the classical input information (x, y) arrives, and the ability to perform the protocol measurement based on (x, y). The latter should be possible fast enough such that the protocol rounds can be run with high frequency (say, MHz or ideally GHz). To that end, we argue that with top equipment MHz rate is possible already and GHz rate feasible in principle. Practically, also the signal-to-noise ratio of the photon presence detection is an important figure of merit that is relevant for the security of the protocol, which we discuss further in the experimental section of the paper. We argue that with state-of-the-art equipment our protocol can remain within its secure regime, even in practice.[2]

In summary, our main result holds more generally, but applied to $\mathrm{QPV}_{\mathrm{BB84}}^{f}$ we provide a new QPV protocol, $\mathsf{c}\text{-}\mathrm{QPV}_{\mathrm{BB84}}^{f}$, that is a practically-feasible QPV protocol with decent security guarantees in the most general setting, even in practice. This opens the way for a first experimental demonstration of quantum position verification.

5.2 Introduction to the $\mathrm{QPV}_{\mathrm{BB84}}^{f}$ Protocol

All proposed QPV protocols rely on both relativistic constraints and the laws of quantum mechanics for their security. The QPV literature usually focuses on the one-dimensional case, so verifying the position of a prover P on a line, as it makes the analysis easier and the main ideas generalize to higher dimensions.

The usual general setting for a 1-dimensional QPV protocol is the following: two verifiers V_0 and V_1, placed on the left and right of P, send quantum and/or classical messages to P at the speed of light. P has to pass a challenge and respond correctly to them with a signal at the speed of light as well. The verifiers have perfectly synchronized clocks and if any of them receives an inconsistent answer or if the timing of the answers is not as expected from the honest prover, they abort the protocol[3].

We will mainly focus on one type of QPV protocol, $\mathrm{QPV}_{\mathrm{BB84}}^{f}$ [BCS22]. This protocol is well studied, easy to implement and the lower bounds on the required quantum resources to attack them scale linearly in the classical input size. However, it is not sufficiently loss-tolerant for practical purposes. In this work, we set out to solve this problem.

5.2.1. Remark. We describe the $\mathrm{QPV}_{\mathrm{BB84}}^{f}$ protocol in its *purified* version, where

[2] As the numbers will strongly depend on the actual experimental setup of a demonstration, we only give estimations.

[3] The time consumed by the prover to perform the task is assumed to be negligible relative to the total protocol time

a verifier sends half of an EPR pair instead of a single qubit, as they would do in its *prepare-and-measure* version. Both versions are equivalent, but we use the purified version for our proof analysis.

5.2.2. Definition. *($\mathrm{QPV}^f_{\mathrm{BB84}}$ protocol [BCS22, ES23]).* Let $n \in \mathbb{N}$, and consider a $2n$-bit boolean function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. A round of the $\mathrm{QPV}^f_{\mathrm{BB84}}$ protocol is described as follows.

1. V_0 prepares the EPR pair $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ and sends one qubit Q of $|\Phi^+\rangle$ and $x \in \{0,1\}^n$ to P and V_1 sends $y \in \{0,1\}^n$ to P such that all information arrives at P simultaneously. The classical information is required to travel at the speed of light, the quantum information can be sent arbitrarily slowly.

2. Immediately, P measures Q in the basis $f(x, y)$[4] and broadcasts his outcome $a \in \{0,1\}$ to V_0 and V_1. If the photon is lost, he sends '$\perp$'.

3. The verifiers measure the qubit they kept in the basis $f(x, y)$, getting outcome $v \in \{0,1\}$. They accept if $a = v$ and a arrives on time. They record 'photon loss' if they both receive '$\perp$' on time. If either the answers do not arrive on time or are different, the verifiers abort.

In the end, the verifiers accept the location of the prover P if after multiple repetitions of single rounds they receive answers that are consistent with their known experimental parameters, i.e. if the number of 'photon loss' answers is consistent with the transmission rate η, and the number of wrong answers is consistent with the error in the experimental set-up.

General structure of an attack on $\mathrm{QPV}^f_{\mathrm{BB84}}$

In a general attack on the $\mathrm{QPV}^f_{\mathrm{BB84}}$ protocol, Alice and Bob act as follows.

1. The attackers prepare a joint (possibly entangled) quantum state.

2. Alice intercepts the quantum information sent from V_0 and performs an arbitrary quantum channel. She keeps a part of the resulting state and sends the rest to Bob. Denote by ρ their joint state at this stage (before communication).

3. Alice and Bob intercept x and y, make a copy and send it to the other attacker, respectively. Then both can apply local quantum channels depending on x (at Alice) and y (at Bob) to ρ. Each can keep part of the resulting local state and send the other part to their fellow attacker.

[4] Usually, the two bases correspond to the computational and the Hadamard basis, justifying the nomenclature of $\mathrm{QPV}^f_{\mathrm{BB84}}$. If m basis choices are possible, the range of f will be $\{0, 1, \ldots, m-1\}$.

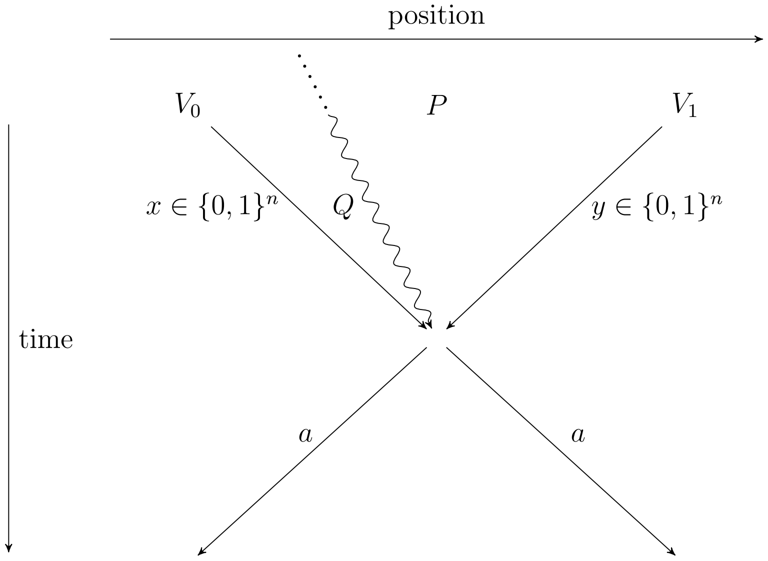


Figure 5.1: Schematic representation of the $\mathrm{QPV}^f_{\mathrm{BB84}}$ protocol. Undulated lines represent quantum information, whereas straight lines represent classical information. The slowly traveling quantum system Q originated from V_0 in the past.

4. Upon receiving the information sent by the other party, each attacker can locally apply an arbitrary POVM depending on (x, y) to obtain classical answers, which will be sent to V_0 and V_1, respectively.

If there is loss in the protocol, the attackers need to mimic the transmission rate of the prover.

Known properties of $\mathrm{QPV}^f_{\mathrm{BB84}}$

Neglecting photon loss, $\mathrm{QPV}^f_{\mathrm{BB84}}$ was proven to be secure [BCS22] even if attackers pre-share a linear amount of qubits in the size of the classical information n. The main advantage of this protocol is that it only requires sending a single qubit, whereas adversaries using an increasing amount of entanglement can be combated solely by increasing the number of classical bits used in the protocol. In addition, $\mathrm{QPV}^f_{\mathrm{BB84}}$ has the advantage that the quantum information can travel arbitrarily slowly. However, photon loss constitutes a major problem. Consider the following easy-to-perform attack, where Alice makes a random guess for the value of $f(x, y)$ and just measures in the guessed basis and broadcasts the result to Bob. Both attackers intercept the classical information, make a copy and send it to their fellow attacker. After one round of simultaneous communication, each can compute $f(x, y)$ and both know if the initial guess was correct. If so, they send the outcome of the measurement, which is correct, to the verifiers. Otherwise, they claim that no photon arrived. Alice's basis guess will be correct half of the time (or $1/m$ of the time for more basis choices), and therefore, if the transmission rate is such that $\eta \leq \frac{1}{2}$ (or $1/m$, respectively), the attackers will be correct whenever they answer, and thus break the protocol.

In [ES23], the range $1/2 < \eta \leq 1$ was studied for $\mathrm{QPV}^{f}_{\mathrm{BB84}}$, and it was shown that the protocol remains secure for attackers who pre-share a linear amount of entanglement in n and arbitrary slow quantum information. However, $\eta > \frac{1}{2}$ is only attainable for short distances. A way to bypass this, first shown independently in [QS15] and [Spe16b, Chapter 5], can be achieved by encoding the qubit Q in more bases than just the computational and Hadamard bases. In the first case, Q is encoded in a uniformly random basis in the Bloch sphere, and security holds for reasonably high loss if the quantum information is sent at the speed of light and the attackers do not pre-share entanglement. Following the second approach, where Q is encoded in m bases in the Bloch sphere, [ES23] showed via semidefinite programming (whose size depends on m) that one can improve the loss tolerance by increasing m, while preserving security against attackers who pre-share a linear amount of entanglement in n and arbitrary slow quantum information. The specific cases of $m = 3, 5$ were worked out, showing that the protocol remains secure, preserving the other two properties, if up to 70% of the photons are lost, making slightly larger distances than with two bases still feasible.

In the next sections, we show how to make QPV for longer distances possible by slightly modifying the structure of the previously known protocols. This opens up a feasible route to the first experimental demonstration of a QPV protocol that captures security against the three major problems that the field faces: bounded attackers, photon loss (for large distances), and slow quantum information.

5.3 QPV with a commitment

One of the major issues in practical quantum cryptography is the transmission loss between the interacting parties. In the context of QPV, a high loss between the verifiers and the prover can compromise security if the QPV protocol is not loss tolerant. Most QPV protocols are not loss tolerant, and those that are have other drawbacks, most notably being broken by an entanglement attack using only one pre-shared EPR pair [LXS+16, ABSV22b] or requiring a large quantum computer at the prover and computational assumptions [LLQ22].

To overcome this, we introduce the following modification to the structure of a certain class of QPV protocols. Let $\mathsf{P}_{\eta_V,\eta_P}$ be a QPV protocol with the verifiers sending quantum and classical information and the prover sending classical answers, where η_V is the transmission rate between the verifiers and the prover, and η_P is the transmission rate in the prover's laboratory. We define its *committing* version (or protocol with *commitment*), denoted by $\mathsf{c}\text{-}\mathsf{P}_{\eta_V,\eta_P}$, by introducing a small time delay $\delta > 0$ between the arrival time of the quantum information and the classical information at the prover. When the quantum information arrives at P, he is required to commit to play ($c = 1$) or not to play ($c = 0$) the round. Only the $c = 1$ rounds are later analyzed for security purposes. We will show that introducing this step will eliminate the relevance of the transmission rate η_V from the verifiers to the prover for security. We prove that only the (potentially small) loss in the prover's laboratory η_P will count now because of this post-selection on "committed" rounds.

This trick can be applied to a class of QPV protocol that fulfills the necessary criteria of our proof. For concreteness and because it is practically most interesting, we will focus on the case $\mathsf{P}_{\eta_V,\eta_P} = \mathrm{QPV}^f_{\mathrm{BB84}}$, where we denote by c-$\mathrm{QPV}^f_{\mathrm{BB84}}$ the protocol with commitment.

5.3.1 The protocol c-QPV$^f_{\mathrm{BB84}}$

The *committing* version of $\mathrm{QPV}^f_{\mathrm{BB84}}$ is described as follows. Again, we describe the protocol in its purified form, whereas in practice it might be simpler to implement its prepare-and-measure version.

5.3.1. Definition. Let $n \in \mathbb{N}$, and consider a $2n$-bit boolean function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. A round of the $\mathrm{QPV}^f_{\mathrm{BB84}}$ protocol with commitment, denoted by c-$\mathrm{QPV}^f_{\mathrm{BB84}}$, is described as follows.

1. V_0 prepares the EPR pair $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ and sends one qubit Q and $x \in \{0,1\}^n$ to P and V_1 sends $y \in \{0,1\}^n$ to P such that x, y arrive a time $\delta > 0$ after Q at P. The classical information is required to travel at the speed of light, the quantum information can be sent arbitrarily slowly.

2. If the prover receives Q, he immediately confirms that and broadcasts the commitment bit $c = 1$. Otherwise, he broadcasts $c = 0$.

3. If $c = 1$, P measures Q in the basis $f(x, y)$[5] as soon as x, y arrive and broadcasts his outcome a to V_0 and V_1. If the photon is lost in the time δ or during the measurement, he sends '$\perp$'.

4. The verifiers collect (c, a) and V_0 measures the qubit he kept in basis $f(x, y)$, getting result v. If $c = 0$ they ignore the round. If $c = 1$ they check whether $a = v$. If c, a arrived at their appropriate times and $a = v$, they accept. They record 'photon loss' if they both receive '$\perp$' on time. If any of the answers do not arrive on time or are different the verifiers abort.

[5] Again, for more basis choices, the range of f would become $\{0, 1, \dots, m-1\}$.

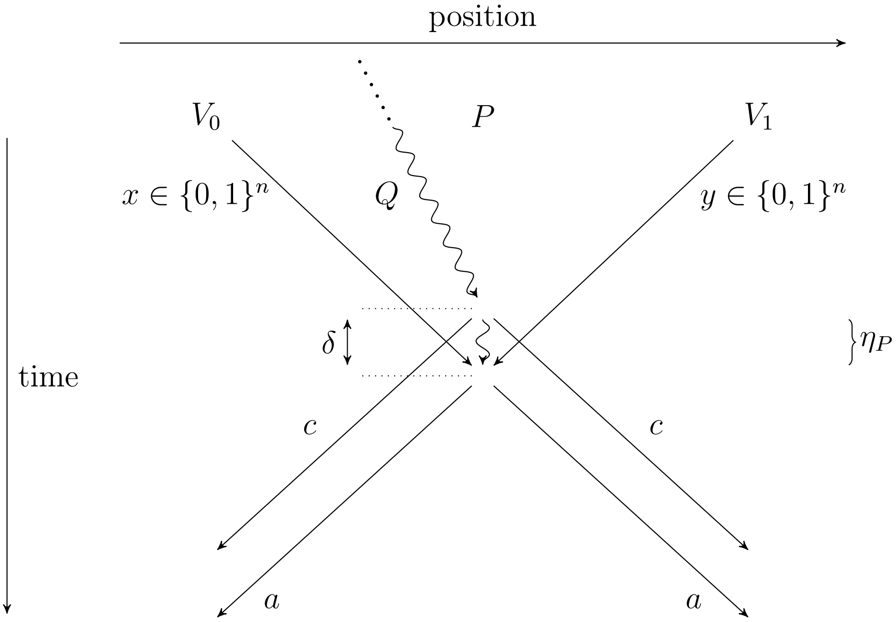


Figure 5.2: Schematic representation of the c-QPV$^f_{\text{BB84}}$ protocol. Undulated lines represent quantum information, straight lines represent classical information. The slowly traveling quantum system Q originated from V_0 in the past. The novel aspects are the time delay $\delta > 0$ at the prover and the prover commitment $c \in \{0,1\}$. We show that for the security of this protocol, the transmission η_V becomes irrelevant.

5.4 Security of QPV with commitment

The most general attack on a 1-dimensional QPV protocol is to place an adversary, who we will call Alice, between V_0 and the position where the prover should be and another adversary, who we will call Bob, between the supposed prover location and V_1. It is easy to see that having more than two adversaries in a 1-dimensional setting does not improve an attack. A general attack on a QPV protocol $\mathsf{P}_{\eta_V,\eta_P}$ in which the verifiers send quantum and classical information and the prover responds with classical answers proceeds as follows. Before the protocol, the attackers prepare a joint (entangled) quantum state σ. Then, Alice and Bob intercept the information sent from their closest verifier, they make a copy and broadcast the classical information to their fellow attacker, and they perform a quantum operation on the intercepted quantum information, keep a register and send another register to the other attacker. After one round of simultaneous communication, they both perform a POVM to obtain a classical answer, and they send it to their closest verifier, respectively.

Denote by x and y the classical information sent from V_0 and V_1, respectively. Without loss of generality, consider them to be n-bit strings, and we assume that they are uniformly distributed. Denote by $\omega^{(x,y)}$ the quantum state after communication, to which attackers apply the POVM. Fix a partition into systems $AA_{\text{com}}BB_{\text{com}}$, where 'com' denotes the subsystems that will be communicated. We can write the attackers two-outcome POVMs as $\{\Pi^{A,(x,y)}_{AB_{\text{com}}}, \mathbb{1} - \Pi^{A,(x,y)}_{AB_{\text{com}}}\}$ and $\{\Pi^{B,(x,y)}_{A_{\text{com}}B}, \mathbb{1} - \Pi^{B,(x,y)}_{A_{\text{com}}B}\}$ respectively, where we can assume without loss of generality that the first outcome corresponds to the correct answer. Then, the probability that the attackers give the correct answers can be written as

$$\mathbb{P}[\text{attack } \mathsf{P}_{\eta_V,\eta_P}] = \frac{1}{2^{2n}} \sum_{x,y} \mathrm{Tr}\Big[\Big(\Pi^{A,(x,y)}_{AB_{\text{com}}} \otimes \Pi^{B,(x,y)}_{BA_{\text{com}}}\Big)\omega^{(x,y)}_{AA_{\text{com}}BB_{\text{com}}}\Big]. \tag{5.3}$$

Note that attackers need to mimic the loss rate of the honest prover, so the rate of $\perp$ responses must be $1-\eta_V\eta_P$, with $\eta_V\eta_P$ being the total transmission between the verifiers and the prover (including his equipment).

5.4.1. Definition. *(State-independent protocol).* We say that a QPV protocol P is *state-independent* if the protocol remains secure independently of the state σ that the attackers pre-share at the start of the protocol[6].

QPV$^f_{\text{BB84}}$ is a state-independent protocol, since it remains secure for any σ whose dimension is linearly bounded (in n) [BCS22].

General structure of an attack on c-P

In a general attack for a c-QPV protocol, Alice and Bob act as follows.

1. The attackers prepare a joint (possibly entangled) quantum state.

2. Alice and Bob intercept the quantum information sent from their closest verifier and each of them performs an arbitrary quantum channel. Both keep a part of their resulting state and send the rest to their fellow attacker. Denote by ρ their joint state at this stage (before communication).

3. Alice and Bob intercept x and y, make a copy and send it to the other attacker, respectively. Due to relativistic constraints, they have to commit before they receive the classical information from the other party. The most general thing they can do is to use local quantum instruments $\{\mathcal{I}^A_{c_A|x}\}_{c_A\in\{0,1\}}$ and $\{\mathcal{I}^B_{c_B|y}\}_{c_B\in\{0,1\}}$ on their registers of ρ to determine the commitments c_A and c_B, respectively. Denote $\mathcal{I}^{xy}_1 = \mathcal{I}^A_{1|x}\otimes\mathcal{I}^B_{1|y}$. To proceed with the protocol, the attackers will use the state post-selected on commitments $c_A = 1$ and $c_B = 1$, denoted by $\tilde{\mathcal{I}}^{xy}_1(\rho) = \mathcal{I}^{xy}_1(\rho)/\mathrm{Tr}[\mathcal{I}^{xy}_1(\rho)]$. Alice can send a share of her state to Bob and vice versa.

[6] As long as this state does not allow for a perfect attack, for example due to sufficiently large pre-shared entanglement, of course. In the regime where security can be shown, it is independent of the adversarial input state.

4. Upon receiving the information sent by the other party, each attacker can again locally apply an arbitrary quantum channel depending on (x, y), followed by local POVMs on the state they share to obtain classical answers, which will be sent to V_0 and V_1, respectively, if $c_A = 1$ and $c_B = 1$. Similarly to before, define a partition $AA_{\text{com}}BB_{\text{com}}$ and denote the final state on which they measure by $\omega^{\mathcal{I}_1,(x,y)}$.

The attack structure is depicted in Figure 5.3. Then the probability that the attackers will answer the correct values to the verifiers is given by

$$\mathbb{P}[\text{attack } \mathsf{c\text{-}P}_{\eta_V,\eta_P}] = \frac{1}{2^{2n}} \sum_{x,y} \mathrm{Tr}\Big[\Big(\Pi^{A,(x,y)}_{AB_{\text{com}}} \otimes \Pi^{B,(x,y)}_{BA_{\text{com}}}\Big)\omega^{\mathcal{I}_1,(x,y)}_{AA_{\text{com}}BB_{\text{com}}}\Big]. \tag{5.4}$$

Here the attackers need to mimic the transmission rate of the prover's laboratory η_P in the rounds they commit to play.

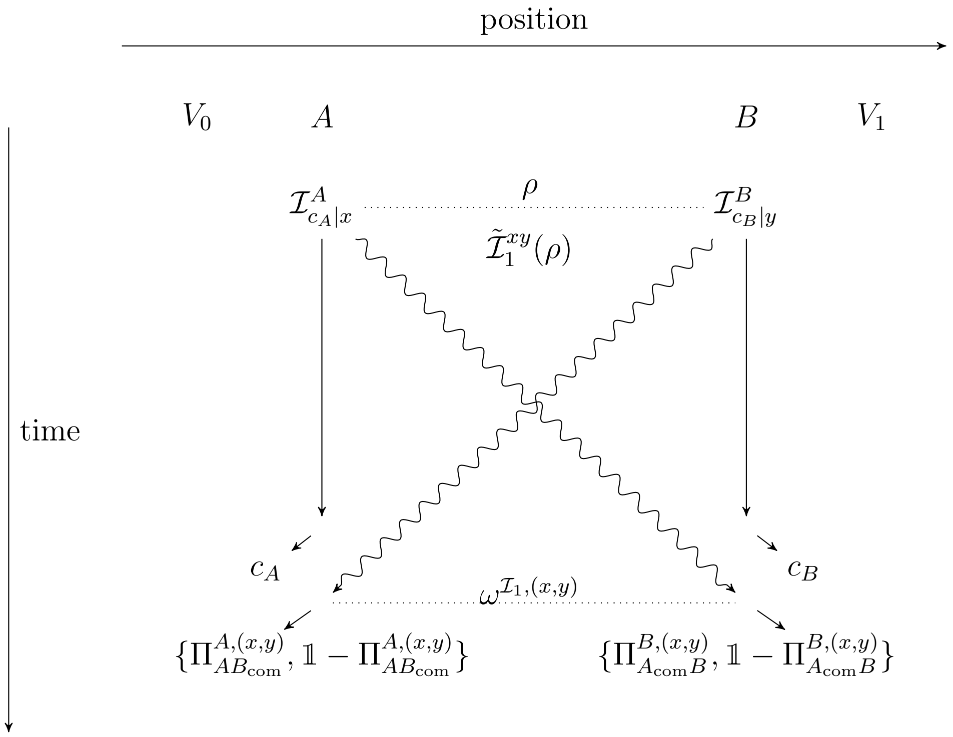

position
V_0
A
B
V_1
time
$\mathcal{I}^A_{c_A|x}$
ρ
$\mathcal{I}^B_{c_B|y}$
$\tilde{\mathcal{I}}_1^{xy}(\rho)$
c_A
c_B
$\omega^{\mathcal{I}_1,(x,y)}$
$\{\Pi^{A,(x,y)}_{AB_{\text{com}}}, \mathbb{1} - \Pi^{A,(x,y)}_{AB_{\text{com}}}\}$
$\{\Pi^{B,(x,y)}_{A_{\text{com}}B}, \mathbb{1} - \Pi^{B,(x,y)}_{A_{\text{com}}B}\}$

Figure 5.3: Schematic representation of a general attack on a c-QPV protocol, where straight lines represent classical information, and undulated lines represent quantum information, including x and y.

5.4.1 Security proof

We now move on to prove the security of c-QPV. The idea is to reduce the security of a protocol with commitment $\mathsf{c\text{-}P}_{\eta_V,\eta_P}$ to that of the underlying protocol without commitment P_{η_P} and (much larger) transmission rate η_P with η_V becoming irrelevant. The intuition is as follows. If we can show that the post-commit state ρ^{xy} (cf. eq. (5.13)) can be replaced by a constant state τ independent of (x, y), then the commitment phase does not help the attackers much. Now note that if the underlying protocol P_{η_P} remains secure for any adversarial input state that is independent of (x, y), the attackers find themselves in the same situation as attacking P_{η_P} (with input τ) when they attack $\mathsf{c}\text{-}\mathsf{P}_{\eta_V,\eta_P}$. This is because the post-commit state ρ^{xy} can be replaced by τ. Then, the success probability of attacking $\mathsf{c}\text{-}\mathsf{P}_{\eta_V,\eta_P}$ should be close to that of attacking P_{η_P}.

Hence, the task is to show that $||\rho^{xy} - \rho^{x'y'}||_1$ is small for any x, y, x', y'. To do so, we can invoke the gentle measurement lemma and the fact that we need to have $c_A = c_B$. Consider classical inputs x, y. Imagine that, say, Alice applies her instrument a tiny bit before Bob[7]. Then Alice's outcome $c_A \in \{0, 1\}$ completely fixes Bob's outcome c_B for any input y on his side. Thus, by the gentle measurement lemma, the instrument on Bob's side cannot disturb this post-commit-at-Alice state he acts on. But that state only depends on x, so ρ^{xy} can only depend on x. Since Alice's and Bob's operations commute, the same argument can be run with Bob instead of Alice applying the instrument first, showing that ρ^{xy} cannot depend on y either. Both must be true simultaneously, and therefore all post-commit states ρ^{xy} are actually independent of (x, y), or equivalently, close to some fixed state τ. But then the attackers find themselves in the exact same situation as attacking P_{η_P} with input τ. The security of the underlying P_{η_P} then guarantees security of $\mathsf{c}\text{-}\mathsf{P}_{\eta_V,\eta_P}$. We also relax the requirement of $c_A = c_B$ to hold only approximately for most input pairs (x, y) and show that the argument is robust.

One subtlety is that the gentle measurement lemma only holds for POVMs, but in our setting Alice and Bob act with arbitrary quantum instruments. So in order to be able to use it as described above, we need to decompose their instruments into measurements followed by a channel. This is precisely what Lemma 5.4.4 does.

We continue by stating the lemmas used in our argument. First, the well-known gentle measurement lemma, stating that if a measurement identifies a state with high probability, then it cannot disturb the state by too much.

5.4.2. Lemma. (Gentle Measurement Lemma [Win99]) *Let ρ be a quantum state and $\{M, \mathbb{1} - M\}$ be a two-outcome measurement. If* $\mathrm{Tr}[M\rho] \geq 1 - \varepsilon$*, then the post-measurement state*

$$\rho' = \frac{\sqrt{M}\rho\sqrt{M}}{\mathrm{Tr}[M\rho]} \tag{5.5}$$

[7] Their measurements commute, since they act on separate registers.

of measuring M fulfills

$$||\rho - \rho'||_1 \leq 2\sqrt{\varepsilon}. \tag{5.6}$$

The following lemma, stating that any quantum instrument can be decomposed into a measurement followed by a quantum channel turns out to be a crucial ingredient in our proof. We include a short proof, with background on the Kraus representation.

5.4.3. Lemma. (Kraus representation [Kra71]). *A linear map Φ is completely positive and trace non-increasing if and only if there exist bounded operators $\{K_i\}_{i=1}^r$ such that for all density operators ρ,*

$$\Phi(\rho) = \sum_{i=1}^{r} K_i \rho K_i^\dagger, \tag{5.7}$$

with $\sum_{i=1}^r K_i^\dagger K_i \leq \mathbb{I}$, where r is the Kraus rank. Moreover, Φ is trace-preserving, i.e. a quantum channel, if and only if $\sum_{i=1}^r K_i^\dagger K_i = \mathbb{1}$.

Let Ω be a finite outcome set. A *quantum instrument* $\mathcal{I}$ is a set of completely positive linear maps $\{\mathcal{I}_i\}_{i\in\Omega}$ such that $\sum_{i\in\Omega}\mathcal{I}_i$ is trace preserving. Given the quantum state $\rho \in \mathcal{S}(\mathcal{H})$, the probability of obtaining outcome i is given by $\mathrm{Tr}[\mathcal{I}_i(\rho)]$ and the sub-normalized output state upon outcome i is $\mathcal{I}_i(\rho)$.

5.4.4. Lemma. (E.g. Thm 7.2 in [Hay16]) *Let $\mathcal{I} = \{\mathcal{I}_i\}_{i\in\Omega}$ be an instrument, and $\{M_i\}_i$ its corresponding POVM, i.e. $\mathcal{I}_i^\dagger(\mathbb{1}) = M_i$. Then, for every $i \in \Omega$, there exists a quantum channel (CPTP map) $\mathcal{E}_i$ such that*

$$\mathcal{I}_i(\rho) = \mathcal{E}_i\Big(\sqrt{M_i}\rho\sqrt{M_i}\Big). \tag{5.8}$$

Proof:
Let $\{K_j\}_j$ be a Kraus decomposition of $\mathcal{I}_i$, whose existence is guaranteed by Lemma 5.4.3. Since

$$\mathrm{Tr}[\mathcal{I}_i(\rho)] = \mathrm{Tr}\left[\sum_j K_j \rho K_j^\dagger\right] = \mathrm{Tr}\left[\rho \sum_j K_j^\dagger K_j\right] = \mathrm{Tr}[\rho M_i], \tag{5.9}$$

for any state ρ, we have $M_i = \sum_j K_j^\dagger K_j$. Denote the pseudo-inverse of $\sqrt{M_i}$ by $(\sqrt{M_i})^-$ and let P be the projection onto the support of $\sqrt{M_i}$, i.e. $P = \sqrt{M_i}\big(\sqrt{M_i}\big)^-$. Then note that

$$\sum_j \Big(\sqrt{M_i}\Big)^- K_j^\dagger K_j \Big(\sqrt{M_i}\Big)^- = \Big(\sqrt{M_i}\Big)^- M_i \Big(\sqrt{M_i}\Big)^- = P^\dagger P = P. \tag{5.10}$$

Hence, if we add $\mathbb{1} - P$ on both sides, we obtain a full Kraus decomposition $\left\{K_j(\sqrt{M_i})^-, \mathbb{1} - P\right\}_j$ of a map, call it $\mathcal{E}_i$, that adds up to the identity. Thus, by Lemma 5.4.3, $\mathcal{E}_i$ is completely positive and trace preserving, i.e. a quantum channel. Finally, we see that

$$\begin{aligned}\mathcal{E}_i\left(\sqrt{M_i}\rho\sqrt{M_i}\right) &= (\mathbb{1} - P)\sqrt{M_i}\rho\sqrt{M_i}(\mathbb{1} - P)\\ &\qquad + \sum_j K_j(\sqrt{M_i})^- \sqrt{M_i}\rho\sqrt{M_i}(\sqrt{M_i})^- K_j^\dagger\\ &= \sum_j K_j \rho K_j^\dagger = \mathcal{I}_i(\rho), \qquad (5.11)\end{aligned}$$

as desired. The last equation follows from the fact that $(\mathbb{1} - P)\sqrt{M_i} = \sqrt{M_i} - \sqrt{M_i}(\sqrt{M_i}^-)\sqrt{M_i} = 0$, which is one of the defining properties of the pseudo-inverse and that $K_j P = K_j$. This follows through $M_i = \sum_j K_j^\dagger K_j$, which implies that $\ker(M_i) \subseteq \ker(K_j)$ for all j. In other words, $\mathrm{supp}(K_j) \subseteq \mathrm{supp}(M_i) = \mathrm{supp}(\sqrt{M_i})$ for all j, and P projects onto the latter. Hence $K_j P = K_j$. □

Combining the Stinespring dilation with Lemma 5.4.4 allows us to see the operations of the attackers after the commit measurement as a unitary in a larger space, and yields the following decomposition of quantum instruments.

5.4.5. Corollary. *Let $\mathcal{I} = \{\mathcal{I}_i\}_{i\in\Omega}$ be an instrument, and $\{M_i\}_{i\in\Omega}$ its corresponding POVM. Then, for every $i \in \Omega$, there exists an environment Hilbert space $\mathcal{H}_E$ and a unitary U_i on $\mathcal{H} \otimes \mathcal{H}_E$ such that*

$$\mathcal{I}_i(\rho) = \mathrm{Tr}_E\left[U_i\left(\sqrt{M_i}\rho\sqrt{M_i} \otimes |0\rangle\langle 0|_E\right)U_i^\dagger\right], \qquad (5.12)$$

for all $\rho \in \mathcal{B}(\mathcal{H})$,

In the case of a commit round of a QPV protocol, the subscript denotes whether the attackers commit ($i = 1$) or not commit ($i = 0$). The unitary U_i in eq. (5.12) is the unitary corresponding to a Stinespring dilation of the channel $\mathcal{E}_i$ appearing in Lemma 5.4.4. We denote the POVMs corresponding to the instruments $\{\mathcal{I}^A_{c_A|x}\}_{c_A}$ and $\{\mathcal{I}^B_{c_B|y}\}_{c_B}$ of Alice and Bob by $\{M_A^x, \mathbb{1} - M_A^x\}$ and $\{M_B^y, \mathbb{1} - M_B^y\}$, respectively. Here, the POVM elements M_A^x and M_B^y correspond to the measurement outcome ‘commit’ ($c_A = 1$ and $c_B = 1$). We denote the post-measurement state corresponding to Alice and Bob committing to a particular input x, y by:

$$\rho^{xy} := \frac{\left(\sqrt{M_A^x} \otimes \sqrt{M_B^y}\right)\rho\left(\sqrt{M_A^x} \otimes \sqrt{M_B^y}\right)}{\mathrm{Tr}[(M_A^x \otimes M_B^y)\rho]}. \qquad (5.13)$$

The observation is now that no two post-commitment states can differ too much from each other by Lemma 5.4.2. This is due to the fact that both players have to output the same commitment, at least with high probability to not be detected. This will be the case for any two inputs x, y and x', y'. The following lemma relates the closeness of states to the probability of answering different commits, given that one party commits.

5.4.6. Lemma. (Paths Between Strings) *Assume that for inputs (x, y), (x', y) and (x', y') in $\{0,1\}^{2n}$ the probability that one party does not commit, given that the other party commits, is upper bounded by some $\varepsilon > 0$. Then,*

$$\|\rho^{xy} - \rho^{x'y'}\|_1 \leq 8\sqrt{\varepsilon}. \tag{5.14}$$

Proof:
Consider the attackers Alice and Bob performing the most general attack described above and the POVMs $\{M_A^x, \mathbb{1} - M_A^x\}$ and $\{M_B^y, \mathbb{1} - M_B^y\}$ as defined above. We write

$$\rho^{x,(\cdot)} = \frac{(\sqrt{M_A^x} \otimes \mathbb{1}_B)\, \rho\, (\sqrt{M_A^x} \otimes \mathbb{1}_B)}{\mathrm{Tr}[(M_A^x \otimes \mathbb{1}_B)\rho]}, \qquad \rho^{(\cdot),y} = \frac{(\mathbb{1}_A \otimes \sqrt{M_B^y})\, \rho\, (\mathbb{1}_A \otimes \sqrt{M_B^y})}{\mathrm{Tr}[(\mathbb{1}_A \otimes M_B^y)\rho]}, \tag{5.15}$$

for the post measurement states corresponding to only Alice or Bob committing before applying the quantum channel. By assumption, we have:

$$\mathrm{Tr}\big[((\mathbb{1}_A \otimes (\mathbb{1} - M_B^y))\rho^{x,(\cdot)}\big] \leq \varepsilon, \qquad \mathrm{Tr}\big[((\mathbb{1} - M_A^x) \otimes \mathbb{1}_B)\rho^{(\cdot),y}\big] \leq \varepsilon. \tag{5.16}$$

Similarly for the input (x', y) and (x', y') we get:

$$\mathrm{Tr}\Big[(\mathbb{1}_A \otimes (\mathbb{1} - M_B^y))\rho^{x',(\cdot)}\Big] \leq \varepsilon, \qquad \mathrm{Tr}\Big[\Big((\mathbb{1} - M_A^{x'}) \otimes \mathbb{1}_B\Big)\rho^{(\cdot),y}\Big] \leq \varepsilon, \tag{5.17}$$

$$\mathrm{Tr}\Big[\Big(\mathbb{1}_A \otimes (\mathbb{1} - M_B^{y'})\Big)\rho^{x',(\cdot)}\Big] \leq \varepsilon, \qquad \mathrm{Tr}\Big[\Big((\mathbb{1} - M_A^{x'}) \otimes \mathbb{1}_B\Big)\rho^{(\cdot),y'}\Big] \leq \varepsilon. \tag{5.18}$$

Therefore, by Lemma 5.4.2 (Gentle Measurement Lemma) we get the following inequalities:

$$\begin{aligned} &\|\rho^{(\cdot),y} - \rho^{xy}\|_1 \leq 2\sqrt{\varepsilon}, \quad \|\rho^{(\cdot),y} - \rho^{x'y}\|_1 \leq 2\sqrt{\varepsilon}, \\ &\|\rho^{x',(\cdot)} - \rho^{x'y}\|_1 \leq 2\sqrt{\varepsilon}, \quad \|\rho^{x',(\cdot)} - \rho^{x'y'}\|_1 \leq 2\sqrt{\varepsilon}. \end{aligned} \tag{5.19}$$

Now we get for the trace distance between the two density matrices:

$$\begin{aligned} \|\rho^{x'y'} - \rho^{xy}\|_1 &= \|\rho^{x'y'} - \rho^{x',(\cdot)} + \rho^{x',(\cdot)} - \rho^{x'y} + \rho^{x'y} - \rho^{(\cdot),y} + \rho^{(\cdot),y} - \rho^{xy}\|_1 \\ &\leq \|\rho^{x'y'} - \rho^{x',(\cdot)}\|_1 + \|\rho^{x',(\cdot)} - \rho^{x'y}\|_1 + \|\rho^{x'y} - \rho^{(\cdot),y}\|_1 + \|\rho^{(\cdot),y} - \rho^{xy}\|_1 \\ &\leq 8\sqrt{\varepsilon}, \end{aligned} \tag{5.20}$$

where we used the triangle inequality and eq. (5.19). □

Note that if the probability of answering different commits on the inputs (x', y) was small, we would get the same inequality between ρ^{xy} and $\rho^{x'y'}$.

In general, an honest prover will never answer different commit bits back to the verifiers. Thus, one could argue that the probability of answering 'no commit' when the other party answers 'commit' should be zero. In that case, by Lemma 5.4.6, we see that all post-commit states are equal, and thus independent of x, y. Then, the quantum instrument that Alice and Bob apply adds no extra power, and their actions are contained in the actions they could do in attacking a state-independent protocol (cf. Definition 5.4.1). And the probability to attack the protocol successfully on rounds in which the attackers commit is equal to the original protocol. This is summarized in the following corollary:

5.4.7. Corollary. *If we demand perfect coordination for the commitments in attack strategies, then for any state-independent quantum position verification* P *its version with commitment* $\mathsf{c}\text{-}\mathsf{P}$ *becomes fully loss tolerant against transmission loss. That is,*

$$\mathbb{P}[\text{attack}\, \mathsf{c}\text{-}\mathsf{P}_{\eta_V,\eta_P}] = \mathbb{P}[\text{attack}\, \mathsf{P}_{\eta_P}]. \tag{5.21}$$

Thus protocols like $\mathrm{QPV}^f_{\mathrm{BB84}}$ *now become secure against transmission loss.*

However, one can argue setting the probability to answer 'no commit' given that the other party answers 'commit' to zero is too restrictive. Also, when this probability is sufficiently low, with high probability the attackers will not get detected by answering different commitments. But it could be that this strategy outperforms the original attack strategy. This stronger setting is not always considered in QPV protocols, but is nonetheless relevant. We will show that allowing for this does not help the attackers much, and we can still show security. We give a continuity statement on the probability of attacking successfully, showing that the protocols with a commitment round are close to the original protocol depending on the probability of answering different commitments. Again, the proof strategy is to show that the post-commit states must be close to each other, depending on the probability of committing differently, given that one party commits (the rounds in which no-one commits are discarded).

The statement of Lemma 5.4.6 can be pictured as a connection problem in a graph. The local inputs x, y are represented as vertices in a bipartite graph, and we connect two vertices x, y if the probability that the two parties send different commitments is upper bounded by ε as in the proof of the above lemma. Then for two pairs of inputs x, y and x', y' (i.e. edges in the graph) $\|\rho^{xy} - \rho^{x'y'}\|_1 \leq 8\sqrt{\varepsilon}$, if there is an edge in the graph that connects either x', y or x, y'. This is represented in Figure 5.4.

Importantly, the statement of Lemma 5.4.6 only holds if the probability of committing different commit bits, given that one party commits, is upper bounded by ε for all three pairs of strings. However, this is not something the verifiers can

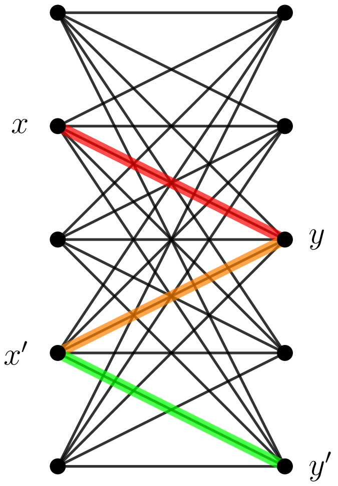


Figure 5.4: Graphical representation of converting the pair (x, y) (red) to (x', y') (green) via (x', y) (orange). Vertices on the left correspond to possible inputs x, on the right to possible inputs y. A connection between two strings means that the probability of committing differently on this input is smaller than ε.

enforce to be true for every pair of strings. The verifiers can only check for the rounds that they play whether the commitments are equal, but given that there are 2^{2n} possible inputs, they cannot get the commit statistics for all of them.

It could be that allowing the attackers to commit differently on a subset of strings can outperform attackers that have to behave well on all strings. Since this subset is unknown to the verifiers (as it is part of the attack strategy), the probability to detect a wrong commit can be made as small as the relative size of the subset to the total set.

We can intuitively visualize the problem of committing differently via the complete bipartite graph in Figure 5.4. In the figure, two vertices are connected if the probability of answering different commitments is upper bounded by ε. Allowing attackers to answer different commits with a higher probability is equivalent to removing certain edges in this graph.

We still have a bipartite graph, but not all edges are connected. What we are now interested in is how many edges can still be reached within two steps from some other edge. It turns out that even if we allow attackers to commit differently with a probability higher than ε on a constant fraction of edges, there will be an edge that will be connected to at least a constant fraction of other edges in two steps (as used in Lemma 5.4.6).

5.4.8. Lemma (Edge Removal). *Consider a complete bipartite graph whose independent sets are of equal size 2^n. After removing a constant fraction $\tilde{c} \leq \frac{1}{2}$ of edges, there exists an edge such that the number of edges that can be reached from this edge in two steps is at least $(1 - 2\tilde{c})2^{2n}$.*

Proof:
The number of edges of a complete bipartite graph with 2^n nodes in its independent sets is 2^{2n}, as there are 2^n edges for any vertex. Now suppose that we remove $\tilde{c} \cdot 2^{2n}$ of these edges. Then, there must be a vertex l on the left with at least $(1-\tilde{c})2^n$ connecting edges. Let one of these edges be your starting edge. Now consider all the vertices on the right that are connected to l. Before we removed any edges, there were 2^n edges connecting each of these vertices to the left. However, we removed $\tilde{c} \cdot 2^{2n}$ of these edges, so the number of edges going back is now at least $(1-\tilde{c}) \cdot 2^{2n} - \tilde{c} \cdot 2^{2n} = (1-2\tilde{c})2^{2n}$. Thus, there are $(1-2\tilde{c})2^{2n}$ edges that can be reached in two steps from the starting edge. □

Now, let us divide the set of all possible inputs into one set where the probability of not committing, given that the other party commits, is lower than ε and its complement. We write

$$\Sigma_\varepsilon := \{x, y \mid \mathrm{Tr}\big[(\mathbb{1} \otimes (\mathbb{1} - M_B^y))\rho^{x,(.)}\big] \leq \varepsilon \wedge \mathrm{Tr}\big[(\mathbb{1} - M_A^x) \otimes \mathbb{1})\rho^{(.),y}\big] \leq \varepsilon\}, \tag{5.22}$$

which can also be written in terms of conditional probabilities

$$\Sigma_\varepsilon = \{x, y \mid \mathbb{P}[c_B = 0 \mid c_A = 1, x_A, y_B] \leq \varepsilon \wedge \mathbb{P}[c_A = 0 \mid c_B = 1, x_A, y_B] \leq \varepsilon\}, \tag{5.23}$$

where the subscript A, B denote that the information about the strings x, y is only known to player A or B and not both. Using this definition we can show the following.

5.4.9. Lemma. *If $|\Sigma_\varepsilon^c| \leq \tilde{c}2^{2n}$, then there is a pair (x^*, y^*) such that there exist at least $(1-2\tilde{c})2^{2n}$ pairs $(x', y') \in \Sigma_\varepsilon$ fulfilling*

$$\|\rho^{x^*y^*} - \rho^{x'y'}\|_1 \leq 8\sqrt{\varepsilon}. \tag{5.24}$$

Proof:
$|\Sigma_\varepsilon^c| \leq \tilde{c}2^{2n}$, so at most there are a fraction of $\tilde{c}$ edges removed from the complete bipartite graph. By Lemma 5.4.8 there is a pair (x^*, y^*) from which there are at least $(1-2\tilde{c})2^{2n}$ edges connected in two steps. Applying Lemma 5.4.6 gives the desired statement. □

We can now formulate a statement about the security of a protocol with a commit round added on top of a regular protocol. This is useful because it does not give attackers the opportunity to use the option of answering ‘loss’ very often anymore and raises the effective transmission of the protocol from $\eta_V \eta_P$ to the usually much larger η_P. The latter may be large enough to protect against lossy attacks that arise in e.g. f-BB84 QPV protocols. On the other hand, it opens up a new possible attack. Attackers can now try to apply some transformation on their state and answer ‘no commit’ when this transformation fails. However, they still need to answer the same commitment to both verifiers. In the following theorem we show that this action cannot help them much. Because the attackers need to give the same commit bit with very high probability, the size of Σ_ε^c will be small relative to all possible inputs. Then a large number of post-commit states will be close to a fixed post-commit state independent of x, y by Lemma 5.4.9. We can now bound the probability of success of the protocol with commitment, because the post-commit state can be replaced by one fixed post-commit state independent of x, y. Thus, the attackers find themselves in the same situation as in the underlying protocol. Any underlying protocol that remains secure for any (constant) adversarial input state as in Definition 5.4.1, thus has a corresponding commitment-protocol with the same security guarantee (up to a small overhead). We make this precise in the following theorem. Note that a particular protocol with the properties considered is $\text{QPV}_{\text{BB84}}^f$ [BCS22].

5.4.10. THEOREM. *Let* P *be a quantum position verification protocol in which the verifiers send classical and quantum information and the prover responds with classical answers. Suppose that for its version with commitment,* $\mathsf{c\text{-}P}$*, we have* $|\Sigma_\varepsilon^c| \leq \tilde{c}2^{2n}$ *for some* $\varepsilon \leq 1/64$*. If* P *is state-independent (cf. Definition 5.4.1) then, on the rounds the attackers play, the following bound on the probability of attackers answering correctly to* $\mathsf{c\text{-}P}$ *holds:*

$$\mathbb{P}[\text{attack}\,\mathsf{c\text{-}P}_{\eta_V,\eta_P}] \leq \mathbb{P}[\text{attack}\,\mathsf{P}_{\eta_P}] + (1-2\tilde{c})8\sqrt{\varepsilon} + 2\tilde{c}. \tag{5.25}$$

Proof:
Both attackers need to generate a commitment bit (c_A, c_B) and send it to the verifiers. The most general operation two attackers can do to generate these bits is a quantum instrument. By Lemma 5.4.4 we can split the quantum instrument into a measurement followed by a quantum channel. Here, the measurement outcome corresponds to the commitment bit the attackers generate and the quantum channel corresponds to the operation they further perform, possibly depending on their inputs (x, y). We want to upper bound the attacking probability in the case that both attackers commit to playing (i.e. $c_A = c_B = 1$, we denote this in the subscript of the instrument). Using the Stinespring dilation theorem we can dilate these quantum channels to unitaries over some larger quantum system, and we get the following for the (renormalized) post-instrument state the attackers hold if they both commit to playing:

$$
\begin{aligned}
\tilde{\mathcal{I}}_1^{xy}(\rho) = \frac{\mathcal{I}_1^{xy}(\rho)}{\operatorname{Tr}[\mathcal{I}_1^{xy}(\rho)]} &= \frac{\mathcal{E}_1^{xy}\Big(\Big(\sqrt{M_A^x}\otimes\sqrt{M_B^y}\Big)\rho\Big(\sqrt{M_B^y}\otimes\sqrt{M_A^x}\Big)\Big)}{\operatorname{Tr}[(M_A^x\otimes M_B^y)\rho]}\\
&= \mathcal{E}_1^{xy}(\rho^{xy})\\
&= \operatorname{Tr}_E\big[U^{xy}(\rho^{xy}\otimes|0\rangle\langle 0|_E)U^{xy\dagger}\big]. \qquad (5.26)
\end{aligned}
$$

By assumption $|\Sigma_\varepsilon^c| \leq \tilde{c}2^{2n}$, so we can invoke Lemma 5.4.9, which says that there must be a reference pair $(x_*, y_*) \in \Sigma_\varepsilon$ such that there are at least $(1-2\tilde{c})2^{2n}$ other pairs $(x, y) \in \Sigma_\varepsilon$ fulfilling:

$$
\|\rho^{x_*y_*} - \rho^{xy}\|_1 \leq 8\sqrt{\varepsilon}. \qquad (5.27)
$$

Combining both results, we get that when we apply some quantum channel depending on (x, y) on both post-measurement states, the outputs are still close. This follows straightforwardly from the data processing inequality for the 1-norm:

$$
\begin{aligned}
\|\mathcal{E}_1^{xy}(\rho^{xy}) - \mathcal{E}_1^{xy}(\rho^{x_*y_*})\|_1 &\leq \|\rho^{xy} - \rho^{x_*y_*}\|_1\\
&\leq 8\sqrt{\varepsilon}. \qquad (5.28)
\end{aligned}
$$

We define $\Lambda_\varepsilon^{(x,y)}$ to be the set of all quantum states close to some reference state ρ^{xy}:

$$
\Lambda_\varepsilon^{(x,y)} = \Big\{(x', y') \in \Sigma_\varepsilon : \|\rho^{xy} - \rho^{x'y'}\|_1 \leq 8\sqrt{\varepsilon}\Big\}, \qquad (5.29)
$$

and write $\Lambda_\varepsilon := \Lambda_\varepsilon^{(x_*,y_*)}$ for the remainder of this proof. By the previous argument, we have $|\Lambda_\varepsilon| \geq (1-2\tilde{c})2^{2n}$, and $|\Lambda_\varepsilon^c| \leq 2\tilde{c}\,2^{2n}$.

After creating the commitment bit both attackers exchange a quantum system and apply some measurement on this. Fix a partition into systems $AA_{\text{com}}BB_{\text{com}}$, where 'com' denotes the subsystems that will be communicated. We can write the attackers two-outcome POVMs as $\{\Pi_{AB_{\text{com}}}^{A,(x,y)}, \mathbb{1}-\Pi_{AB_{\text{com}}}^{A,(x,y)}\}$ and $\{\Pi_{A_{\text{com}}B}^{B,(x,y)}, \mathbb{1}-\Pi_{A_{\text{com}}B}^{B,(x,y)}\}$ respectively, where we can assume without loss of generality that the first outcome corresponds to the correct answer.

Now we have all the ingredients to upper bound the attacking probability of a round in which both attackers committed. For simplicity, denote the final operation of the attackers by $\Pi_{AB_{\text{com}}}^{A,(x,y)} \otimes \Pi_{A_{\text{com}}B}^{B,(x,y)} = \Pi^{xy}$. Then

$$
\begin{aligned}
&\mathbb{P}[\text{attack}\,\mathsf{c\text{-}P}_{\eta_V,\eta_P}] = \frac{1}{2^{2n}}\sum_{(x,y)}\mathrm{Tr}\left[\Pi^{xy}\tilde{\mathcal{I}}_1^{xy}(\rho)\right]\\
&= \frac{1}{2^{2n}}\sum_{(x,y)\in\Lambda_\varepsilon}\mathrm{Tr}[\Pi^{xy}\mathcal{E}_1^{xy}(\rho^{xy})] + \frac{1}{2^{2n}}\sum_{(x,y)\in\Lambda_\varepsilon^c}\mathrm{Tr}[\Pi^{xy}\mathcal{E}_1^{xy}(\rho^{xy})]\\
&\leq \frac{1}{2^{2n}}\sum_{(x,y)\in\Lambda_\varepsilon}\mathrm{Tr}[\Pi^{xy}(\mathcal{E}_1^{xy}(\rho^{xy}) - \mathcal{E}_1^{xy}(\rho^{x_*y_*}) + \mathcal{E}_1^{xy}(\rho^{x_*y_*}))] + \frac{|\Lambda_\varepsilon^c|}{2^{2n}}\\
&= \frac{1}{2^{2n}}\sum_{(x,y)\in\Lambda_\varepsilon}\mathrm{Tr}[\Pi^{xy}(\mathcal{E}_1^{xy}(\rho^{xy}) - \mathcal{E}_1^{xy}(\rho^{x_*y_*}))]\\
&\qquad\qquad + \frac{1}{2^{2n}}\sum_{(x,y)\in\Lambda_\varepsilon}\mathrm{Tr}[\Pi^{xy}\mathcal{E}_1^{xy}(\rho^{x_*y_*}))] + \frac{|\Lambda_\varepsilon^c|}{2^{2n}}\\
&\leq \frac{1}{2^{2n}}\sum_{(x,y)\in\Lambda_\varepsilon}\|\Pi^{xy}\|_\infty\|\mathcal{E}_1^{xy}(\rho^{xy}) - \mathcal{E}_1^{xy}(\rho^{x_*y_*})\|_1\\
&\qquad\qquad + \frac{1}{2^{2n}}\sum_{(x,y)\in\Lambda_\varepsilon}\mathrm{Tr}[\Pi^{xy}\mathcal{E}_1^{xy}(\rho^{x_*y_*}))] + \frac{|\Lambda_\varepsilon^c|}{2^{2n}}\\
&\leq \frac{|\Lambda_\varepsilon|}{2^{2n}}8\sqrt{\varepsilon} + \frac{|\Lambda_\varepsilon^c|}{2^{2n}} + \frac{1}{2^{2n}}\sum_{(x,y)\in\Lambda_\varepsilon}\mathrm{Tr}[\Pi^{xy}\mathcal{E}_1^{xy}(\rho^{x_*y_*}))]\\
&\leq \frac{|\Lambda_\varepsilon^c|}{2^{2n}}(1-8\sqrt{\varepsilon}) + 8\sqrt{\varepsilon} + \mathbb{P}[\text{attack}\,\mathsf{P}_{\eta_P}]\\
&\leq \mathbb{P}[\text{attack}\,\mathsf{P}_{\eta_P}] + (1-2\tilde{c})8\sqrt{\varepsilon} + 2\tilde{c},
\end{aligned}
\tag{5.30}
$$

where we used the triangle inequality, Hölder's inequality for Schatten norms [Wat18], and that $(1-8\sqrt{\varepsilon}) \geq 0$. The fact that $\frac{1}{2^{2n}}\sum_{(x,y)\in\Lambda_\varepsilon}\mathrm{Tr}[\Pi^{xy}\mathcal{E}_1^{xy}(\rho^{x_*y_*}))] \leq \mathbb{P}[\text{attack}\,\mathsf{P}_{\eta_P}]$ follows from the assumption that the protocol is secure against any input state and the fact that $U^{xy} = U^x \otimes U^y$ as $\mathcal{I}_1^{xy} = \mathcal{I}_{1|x}^A \otimes \mathcal{I}_{1|y}^B$. We can neglect this because local unitaries can be absorbed into the attack strategy on the original protocol $\mathsf{P}_{\eta_V,\eta_P}$. □

The idea is now to estimate ε and $\tilde{c}$ to show that, over an increasing number of rounds, $\mathbb{P}[\text{attack}\,\mathsf{c\text{-}P}_{\eta_V,\eta_P}]$ becomes increasingly closer to $\mathbb{P}[\text{attack}\,\mathsf{P}_{\eta_P}]$. This should follow from getting better and better estimates of ε as the verifiers continue to see only equal commitments.

5.4.2 Parameter estimation

Non-adaptive strategies

The above theorem gives us a way to bound the probability of success in any lossy setting, which makes protocols with a commitment round ideal candidates for practical implementation of QPV. The roles of ε and $\tilde{c}$ are important here. Theoretically, if we set ε to 0, i.e. we never allow attackers to answer different commits, we see that the attackers cannot apply any lossy attack! Thus, making the protocol fully loss tolerant against transmission loss $1-\eta_V$.

However, as we have shown before, we cannot set ε to be 0, since a small ε might help the attackers, while still not being detected with high probability. On the other hand, if we play a certain number of rounds in which we see a sufficient amount of committing rounds but never see different commit bits being sent, we can be quite certain that the probability of one party not committing given that the other party commits is small. We want to estimate the conditional probabilities:

$$\mathbb{P}[c_A = 0|c_B = 1] = \frac{1}{2^{2n}} \sum_{x,y} \mathbb{P}[c_A = 0|c_B = 1, x_A, y_B], \tag{5.31}$$

$$\mathbb{P}[c_B = 0|c_A = 1] = \frac{1}{2^{2n}} \sum_{x,y} \mathbb{P}[c_B = 0|c_A = 1, x_A, y_B]. \tag{5.32}$$

Intuitively, if we see a large number of rounds in which both parties commit but we never see different commits, these probabilities should be small. Suppose that we want to upper bound the maximum conditional probability of the two in Eq. (5.31) by some value $\alpha > 0$. Then we can do the following. We keep playing until we get $\frac{r}{\alpha}$ number of rounds in which both parties commit, where r is some fixed constant. This takes an expected number $\frac{r}{\alpha\, p_{\text{commit}}}$ of rounds, where p_{commit} is the probability that the honest prover will commit.

Suppose that the attackers' strategy is non-adaptive. Then, if we detect different commit bits in one of these rounds we immediately abort, because an honest prover would never send these. If the probability of answering different commit bits would be larger than α, the probability to answer equal commit bits (and not get detected) every round in which they commit would be smaller than $(1-\alpha)^{\frac{r}{\alpha}}$.

We will now lower bound the probability to detect attackers due to differing commits. Suppose that the maximum of the two probabilities in Eq. (5.31), (5.32) is at least α and denote the events $C^i_{\text{diff}} = \{(c^i_A, c^i_B) = (0,1) \text{ or } (1,0)\}$, $C^i_{\text{eq}} = \{(c^i_A, c^i_B) = (0,0) \text{ or } (1,1)\}$, $C^i_{(1,1)} = \{(c^i_A, c^i_B) = (1,1)\}$ and $C^i_{\neq 0} = \{(c^i_A, c^i_B) \neq (0,0)\}$. Then for $i, j \in \{1, \ldots, r/\alpha\}$ attackers are detected due to differing commits with probability

$$\begin{aligned}&\mathbb{P}[\text{detect attackers} \,|\, \text{commits} \neq (0,0)] \\ &\quad= \mathbb{P}[\exists j \text{ with } (c_A^j, c_B^j) = (0,1) \text{ or } (1,0) \,|\, \forall i \quad (c_A^i, c_B^i) \neq (0,0)] \\ &\quad= \mathbb{P}[\exists j \text{ with } C_{\text{diff}}^j \,|\, \forall i\ C_{\neq 0}^i]. \end{aligned} \tag{5.33}$$

Using the complementary probability and the fact that attackers act non-adaptively, we can write

$$\begin{aligned}&\mathbb{P}[\text{detect attackers} \,|\, \text{commits} \neq (0,0)] = 1 - \mathbb{P}[\forall i\ C_{\text{eq}}^i \,|\, \forall i\ C_{\neq 0}^i] \\ &\quad= 1 - \prod_{i=1}^{r/\alpha} \mathbb{P}[C_{(1,1)}^i \,|\, C_{\neq 0}^i] = 1 - \prod_{i=1}^{r/\alpha} \big(1 - \mathbb{P}[C_{\text{diff}}^i \,|\, C_{\neq 0}^i]\big) \\ &\quad\geq 1 - \prod_{i=1}^{r/\alpha} \big(1 - \max\{\mathbb{P}[c_B^i = 0 \,|\, c_A^i = 1], \mathbb{P}[c_A^i = 0 \,|\, c_B^i = 1]\}\big) \\ &\quad\geq 1 - \prod_{i=1}^{r/\alpha} (1 - \alpha) = 1 - (1-\alpha)^{r/\alpha} \\ &\quad\geq 1 - e^{-\alpha r/\alpha} = 1 - e^{-r}. \end{aligned} \tag{5.34}$$

In the second equality, we use that $C_{\text{eq}}^i \cap \{C_{\neq 0}^j \forall j\} = C_{(1,1)}^i = C_{(1,1)}^i \cap C_{\neq 0}^i$ and that the attacks are non-adaptive. The first inequality follows from the following argument. Notice that the event $\{(c_A^i, c_B^i) \neq (0,0)\}$ contains $\{c_A^i = 1 \text{ or } c_B^i = 1\}$. Consider the case of $c_A^i = 1$. Then we can write

$$\mathbb{P}[C_{\text{diff}}^i \,|\, c_A^i = 1] = \frac{\mathbb{P}[(c_A^i, c_B^i) = (1,0)]}{\mathbb{P}[(c_A^i, c_B^i) = (1,0)] + \mathbb{P}[(c_A^i, c_B^i) = (1,1)]}, \tag{5.35}$$

$$\mathbb{P}[C_{\text{diff}}^i \,|\, C_{\neq 0}^i] = \frac{\mathbb{P}[(c_A^i, c_B^i) = (1,0)] + \mathbb{P}[(c_A^i, c_B^i) = (0,1)]}{1 - \mathbb{P}[(c_A^i, c_B^i) = (0,0)]}. \tag{5.36}$$

Writing $a = \mathbb{P}[(c_A^i, c_B^i) = (0,0)], b = \mathbb{P}[(c_A^i, c_B^i) = (0,1)], c = \mathbb{P}[(c_A^i, c_B^i) = (1,0)]$ and $d = \mathbb{P}[(c_A^i, c_B^i) = (1,1)]$ one can directly verify that $\frac{c}{c+d} \leq \frac{c+b}{1-a}$ given that $a + b + c + d = 1$. Thus,

$$\mathbb{P}[C_{\text{diff}}^i \,|\, C_{\neq 0}^i] \geq \mathbb{P}[C_{\text{diff}}^i \,|\, c_A^i = 1] = \mathbb{P}[c_B^i = 0 \,|\, c_A^i = 1]. \tag{5.37}$$

The case $c_B^i = 1$ works the same way. Hence,

$$\mathbb{P}[C_{\text{diff}}^i \,|\, C_{\neq 0}^i] \geq \max\{\mathbb{P}[c_B^i = 0 \,|\, c_A^i = 1], \mathbb{P}[c_A^i = 0 \,|\, c_B^i = 1]\}. \tag{5.38}$$

We see that if the probability to commit differently was higher than α we would detect attackers in the $\frac{r}{\alpha}$ committed rounds with a probability exponentially close to 1 in r. When we pick $r = 20$, we have $\mathbb{P}[\text{detect attackers} \,|\, \text{commits} \neq (0,0)] \geq 1 - 10^{-9}$. And, if we do not see any different commit bits in $\frac{r}{\alpha}$ rounds we can say with very high probability that the probabilities in Eq. (5.31), (5.32) are upper bounded by α. The more rounds we run, the smaller we can make α (with high probability), thus controlling the role of ε in Theorem 5.4.10.

For the theorem to be of any use, we also need to control the dependence on $\tilde{c}$ (which comes from $|\Sigma_\alpha^c| \leq \tilde{c}2^{2n}$). Intuitively, if the set Σ_α^c is large, we know that a large part of this set must be close to α in order for the average over all probabilities to still be α. Then, if we look at, for example, $\Sigma_{2\alpha}^c$, we expect the set to be much smaller. We can make this intuition precise. Suppose that we play $k\frac{20}{\alpha}$ number of rounds for some value α that we fix beforehand. Then by the previous argument we can assume with high probability that $\max\{\mathbb{P}[c_A = 0|c_B = 1],\ \mathbb{P}[c_B = 0|c_A = 1]\} \leq \frac{\alpha}{k}$. Then consider the set Σ_α^c. In the worst case, all the values in this set are very close to α and, in order for the average to be $\frac{\alpha}{k}$, we get that the maximal size is $|\Sigma_\alpha^c| \leq \frac{2}{k}2^{2n}$. Indeed, from the condition that $\max\{\mathbb{P}[c_A = 0|c_B = 1],\ \mathbb{P}[c_B = 0|c_A = 1]\} \leq \frac{\alpha}{k}$ it follows that in the worst case both probabilities are equal to α/k and have non-zero values on disjoint pairs of (x, y). More formally, from the definition of Σ_α we know that either $\mathbb{P}[c_A = 0|c_B = 1, x, y] \geq \alpha$ for at least $|\Sigma_\alpha^c|/2$ pairs (x, y) in Σ_α^c or $\mathbb{P}[c_B = 0|c_A = 1, x, y] \geq \alpha$ for at least $|\Sigma_\alpha^c|/2$ pairs (x, y) in Σ_α^c. Let us assume without loss of generality that we are in the former case. We estimate

$$\begin{aligned}
\frac{\alpha}{k} &\geq \frac{1}{2^{2n}} \sum_{x,y} \mathbb{P}[c_A = 0|c_B = 1, x_A, y_B] \\
&\geq \frac{1}{2^{2n}} \sum_{(x,y)\in\Sigma_\alpha^c} \mathbb{P}[c_A = 0|c_B = 1, x_A, y_B] \\
&\geq \frac{1}{2^{2n}} \frac{|\Sigma_\alpha^c|}{2}\alpha. \qquad (5.39)
\end{aligned}$$

Thus, we can set $\tilde{c} = \frac{2}{k}$. For simplicity of the final statement, note that we have the freedom to pick α as we like. Picking α to be of the size $\frac{1}{16k^2}$ we get a clean inequality statement with a single variable that can be set by the verifiers. Notice that $\alpha \leq 1/64$ implies $k \geq 2$, but of course k should be chosen much larger to suppress the additive term $6/k$. Plugging this into Theorem 5.4.10 we get the following corollary for the attacking probability of a *single round* of the protocol:

5.4.11. Corollary. *Consider a quantum position verification protocol* P, *with the properties described as in Theorem 5.4.10 and security under sequential repetition. Let* $k \geq 2$ *and suppose we play its version with commitment* $\mathsf{c\text{-}P}$ *until we have* $320k^3$ *rounds in which both parties commit. This takes an expected number of rounds* $320k^3/p_{\text{commit}}$. *If attackers use a non-adaptive strategy, then either the attackers are detected with probability bigger than* $1 - 10^{-9}$ *by means of a different commitment, or we have the following bound on the probability of attacking a* *single round* $\mathsf{c\text{-}P}$ *depending only on* k*:*

$$\begin{aligned}\mathbb{P}[\text{attack}\,\mathsf{c\text{-}P}_{\eta_V,\eta_P}] &\leq \mathbb{P}[\text{attack}\,\mathsf{P}_{\eta_P}] + \left(1-\frac{4}{k}\right)8\sqrt{\alpha}+\frac{4}{k}\\ &\leq \mathbb{P}[\text{attack}\,\mathsf{P}_{\eta_P}] + \frac{6}{k}. \end{aligned} \tag{5.40}$$

Thus, by running more rounds of the protocol we can get the probability of successfully attacking the protocol to be arbitrarily close to the attacking probability in a setting with no photon loss between the verifiers and the prover. What is also important to emphasize is that there is no overhead in the procedure to obtain bounds in Corollary 5.4.11, since the task of committing is separate from the rounds themselves. Each round the verifiers play gives a better bound for the probability of attack for all the previous rounds played.

Adaptive strategies:

The above proof assumed that attackers use the same strategy in each round. But in general, they could use adaptive strategies, adjusting it each round to how they responded before. We will now provide a bound for this most general scenario. Firstly, note that the statement of Theorem 5.4.10 can also be made for the adaptive setting. In an adaptive strategy, the measurement that determines whether the attackers will commit or not, given that the other party committed, can now depend on the information of the previous rounds. This may change the underlying probability of events. However, the proof already considers arbitrary distributions of commitments, thus we replace ε by its round-dependent version ε_i. The attackers may replace the quantum state by some state that depends on the information of the previous rounds, but by the state-independent property this should not change the probability of successfully attacking the protocol. Therefore, we get the following corollary on the probability of attacking a specific round i:

5.4.12. Corollary. *Consider a quantum position verification protocol* P*, with the properties described as in Theorem 5.4.10 and security under sequential repetition. Suppose that for its version with commitment,* $\mathsf{c\text{-}P}$*, for a given round* i *we have* $|\Sigma^c_{\varepsilon_i}| \leq \tilde{c}_i 2^{2n}$ *for some* $\varepsilon_i \leq 1/64$*. If* P *is state-independent (cf. Definition 5.4.1) then, if the attackers play, the following bound on the probability of attackers answering correctly on the* i*-th round of* $\mathsf{c\text{-}P}$ *holds:*

$$\mathbb{P}[\text{attack}\,\mathsf{c\text{-}P}_{\eta_V,\eta_P}] \leq \mathbb{P}[\text{attack}\,\mathsf{P}_{\eta_P}] + (1-2\tilde{c}_i)8\sqrt{\varepsilon_i}+2\tilde{c}_i. \tag{5.41}$$

The problem is now to estimate the value of ε_i, which we cannot estimate for every i since it can change adaptively from round to round. We will show that if we run sufficiently many rounds, and never see different commits by the attackers, then at least a large fraction of all the ε_i must have been sufficiently low.

We can make a similar argument as in the non-adaptive case, carefully including that attackers can now condition on the past in each round. We will use the general property that

$$\mathbb{P}[A_1, \dots, A_n] = \mathbb{P}[A_1]\mathbb{P}[A_2 \,|\, A_1] \cdots \mathbb{P}[A_n \,|\, A_1, \dots, A_{n-1}], \tag{5.42}$$

for any events $A_1, \dots, A_n$. Consider running r rounds with commitments $(c_A, c_B) \neq (0,0)$. Let $i, j \in \{1, \dots, r\}$. Then we can bound the probability of being detected due to differing commits as follows,

$$\begin{aligned}\mathbb{P}[\text{detect attackers} \,|\, \text{commits} \neq (0,0)] &= 1 - \mathbb{P}[\forall i\ C^i_{\text{eq}} \,|\, \forall i\ C^i_{\neq 0}] \\ &= 1 - \mathbb{P}[\forall i\ C^i_{(1,1)} \,|\, \forall i\ C^i_{\neq 0}].\end{aligned} \tag{5.43}$$

Then Eq. (5.43) can be written as

$$\mathbb{P}[\text{det. attackers}|\text{commits} \neq (0,0)] = 1 - \mathbb{P}[C^1_{(1,1)}, \dots, C^r_{(1,1)} \,|\, C^1_{\neq 0}, \dots, C^r_{\neq 0}].$$

After using Eq. (5.42) and noting that $C^i_{(1,1)} \cap C^i_{\neq 0} = C^i_{(1,1)}$ for any i, this can be rewritten as

$$\begin{aligned}&\mathbb{P}[\text{detect attackers} \,|\, \text{commits} \neq (0,0)] \\ &\quad = 1 - \prod_{i=1}^{r} \mathbb{P}\Big[C^i_{(1,1)} \,\Big|\, C^1_{(1,1)}, \dots, C^{i-1}_{(1,1)}, C^i_{\neq 0}, \dots, C^r_{\neq 0}\Big] \\ &\quad = 1 - \prod_{i=1}^{r} \Big(1 - \mathbb{P}\Big[C^i_{\text{diff}} \,\Big|\, C^1_{(1,1)}, \dots, C^{i-1}_{(1,1)}, C^i_{\neq 0}, \dots, C^r_{\neq 0}\Big]\Big).\end{aligned} \tag{5.44}$$

We can then consider the equations analogous to Eq. (5.35), (5.36), but with all the extra events for rounds $1, \dots, i-1, i+1, \dots, r$ in the conditioning part. Again, labeling these probabilities analogously with a_i, b_i, c_i, d_i (cf. Eq. (5.35), (5.36)) we obtain the inequality $\frac{c_i}{c_i+d_i} \leq \frac{c_i+b_i}{p_i-a_i}$, where now

$$p_i = \mathbb{P}\Big[C^1_{(1,1)}, \dots, C^{i-1}_{(1,1)}, C^i_{\text{any}}, C^{i+1}_{\neq 0}, \dots, C^r_{\neq 0}\Big], \tag{5.45}$$

with $C^i_{\text{any}} = \{(c^i_A, c^i_B) = (0,0) \text{ or } (0,1) \text{ or } (1,0) \text{ or } (1,1)\}$. The inequality can be verified under the condition that $a_i + b_i + c_i + d_i = p_i$. This shows

$$\begin{aligned}&\mathbb{P}[C^i_{\text{diff}} \,|\, C^1_{(1,1)}, \dots, C^{i-1}_{(1,1)}, C^i_{\neq 0}, \dots, C^r_{\neq 0}] \\ &\quad \geq \mathbb{P}\Big[C^i_{\text{diff}} \,\Big|\, C^1_{(1,1)}, \dots, C^{i-1}_{(1,1)}, \{c^i_A = 1\}, C^{i+1}_{\neq 0}, \dots, C^r_{\neq 0}\Big] \\ &\quad = \mathbb{P}\Big[c^i_B = 0 \,\Big|\, C^1_{(1,1)}, \dots, C^{i-1}_{(1,1)}, \{c^i_A = 1\}, C^{i+1}_{\neq 0}, \dots, C^r_{\neq 0}\Big].\end{aligned} \tag{5.46}$$

The same inequality holds for the case with A and B swapped, as before. Thus:

$$\begin{aligned}&\mathbb{P}[\text{detect attackers} \,|\, \text{commits} \neq (0,0)] \geq \\ &\quad 1 - \prod_{i=1}^{r} \Big(1 - \max\big\{\mathbb{P}[c_B^i = 0 \,|\, C_{(1,1)}^1, \ldots, C_{(1,1)}^{i-1}, \{c_A^i = 1\}, C_{\neq 0}^{i+1}, \ldots, C_{\neq 0}^{r}], \\ &\qquad\qquad \mathbb{P}[c_A^i = 0 \,|\, C_{(1,1)}^1, \ldots, C_{(1,1)}^{i-1}, \{c_B^i = 1\}, C_{\neq 0}^{i+1}, \ldots, C_{\neq 0}^{r}]\big\}\Big). \qquad (5.47)\end{aligned}$$

Define ε_i to be the maximum in Eq. (5.47). This quantity can be interpreted as follows. In the i-th round adaptive attackers have the information that in all previous rounds they committed and that they committed equally, otherwise they would have already been caught. They also know that they have to keep playing until they have reached the desired number of non-$(0,0)$ commits.

Now there are two cases, either the probability in Eq. (5.47) is $\geq 1-\delta$ with some security parameter $\delta > 0$, in which case the verifiers catch an attack with high probability by means of a different commit $c_A \neq c_B$ showing up, or it is $\leq 1-\delta$. In the latter case, we still need to bound the attack success probability. Note that then

$$1 - \prod_{i=1}^{r}(1-\varepsilon_i) \leq 1 - \delta.$$

We can rewrite the condition as

$$0 < \delta \leq \prod_{i=1}^{r}(1-\varepsilon_i) \leq e^{-\sum_{i=1}^{r}\varepsilon_i}.$$

Equivalently, $\sum_{i=1}^{r}\varepsilon_i \leq \ln(1/\delta)$. Next, we will need the following lemma, saying that under such a constraint there must be enough "good" rounds with ε_i not too large.

5.4.13. Lemma. *Let $\sum_{j=1}^{r}\varepsilon_j \leq \alpha$. Then for any $0 < q < 1$ such that $qr \in \mathbb{N}$, there exists a subset $\mathcal{R} \subset \{1, \ldots, r\}$ of size $|\mathcal{R}| = qr$ such that for all ε_j with $j \in \mathcal{R}$ we have $\varepsilon_j \leq \frac{\alpha}{(1-q)r}$.*

Proof:
Assume that you cannot find qr elements ε_j with $\varepsilon_j \leq \frac{\alpha}{(1-q)r}$, given $\sum_{j=1}^{r}\varepsilon_j \leq \alpha$. Then there would be at least $(1-q)r$ elements fulfilling $\varepsilon_j > \frac{\alpha}{(1-q)r}$. But then $\sum_{j=1}^{r}\varepsilon_j > \alpha$, a contradiction. Thus, we must be able to find qr such elements and let $\mathcal{R}$ be the set of those. □

That is, for a fraction q of the r rounds, we have a round-independent upper bound on the ε_i of those rounds, namely $\varepsilon_i \leq \frac{\ln(1/\delta)}{(1-q)r}$ for $i \in \mathcal{R}$.

Therefore, a similar argument as in the proof for Corollary 5.4.11 can be run to argue that $\tilde{c}_i \leq 2/k$ for some constant k, while running k times the number of rounds r. Hence, for a fraction q of the r rounds, we have by Corollary 5.4.12 that

$$\mathbb{P}[\text{attack}\,\mathsf{c\text{-}P}_{\eta_V,\eta_P}\text{ in round } i\in\mathcal{R}]\leq\mathbb{P}[\text{attack}\,\mathsf{P}_{\eta_P}]+\left(1-\frac{4}{k}\right)8\sqrt{\frac{\ln(1/\delta)}{(1-q)r}}+\frac{4}{k},\tag{5.48}$$

while kr rounds are run (similar to Corollary 5.4.11). We are free to pick (δ,q,k,r). Pick, for example, $\delta=e^{-20}\leq 3\cdot 10^{-9}$, $q=1-\frac{1}{k}$, and $r=320k^3$. Then

$$\begin{aligned}\mathbb{P}[\text{attack}\,\mathsf{c\text{-}P}_{\eta_V,\eta_P}\text{ in round } i\in\mathcal{R}]&\leq\mathbb{P}[\text{attack}\,\mathsf{P}_{\eta_P}]+\left(1-\frac{4}{k}\right)8\sqrt{\frac{20}{r/k}}+\frac{4}{k}\\&\leq\mathbb{P}[\text{attack}\,\mathsf{P}_{\eta_P}]+\frac{6}{k},\end{aligned}\tag{5.49}$$

to obtain a similar bound as in Corollary 5.4.11, while in total we play until we hit $kr=320k^4$ rounds in which both parties committed. This takes an expected number of rounds $320k^4/p_{\text{commit}}$. In the end, the verifiers may choose k, which will determine the number of rounds they have to run in order to guarantee Eq. (5.49) on a large fraction $1-1/k$ of rounds. Again, the condition $\varepsilon_i\leq 1/64$ necessitates $k\geq 2$, but k shall be chosen much larger to suppress the additive term $6/k$ (while still keeping the number of necessary rounds manageable). We summarize our findings in the following corollary.

5.4.14. Corollary. *Consider a quantum position verification protocol* P, *with the properties described as in Theorem 5.4.10 and security under sequential repetition. Let* $k\geq 2$ *and suppose we play its version with commitment* $\mathsf{c\text{-}P}$ *until we have* $320k^4$ *rounds in which both attackers commit. This takes an expected number of rounds* $320k^4/p_{\text{commit}}$. *We call this protocol* $\mathsf{c\text{-}P}^{\text{seq}}$. *Then either the attackers are detected with a probability bigger than* $1-3\cdot 10^{-9}$ *by means of a different commitment, or there is a set* $\mathcal{R}$ *of size* $1-1/k$ *times the number of rounds such that*

$$\mathbb{P}[\text{attack}\,\mathsf{c\text{-}P}^{\text{seq}}_{\eta_V,\eta_P}\text{ in round } i]\leq\mathbb{P}[\text{attack}\,\mathsf{P}_{\eta_P}]+\frac{6}{k},\tag{5.50}$$

for all $i\in\mathcal{R}$.

5.5 QPV with commitment in practice

For our protocol with commitment, the honest prover needs a device detecting the presence of the input quantum state[8] without destroying it, i.e. a photon

[8] We will focus on photonic qubits.

presence detector, also known as quantum non-demolition (QND) measurement. We will consider two feasible solutions to this. What is important for the security of c-QPV is how much loss and error this introduces in the prover's setup. The main goal of c-QPV is to make the (large) transmission loss between the verifiers and the prover irrelevant for security.

Transmission in the prover laboratory

The relevant transmission rate for security is the one in the prover's laboratory (η_P). It strongly depends on the actual setup used, so we will only give rough estimates of η_P. Note that

$$\begin{aligned}\eta_P &= \mathbb{P}[\text{photon measured} \,|\, \text{presence detected}] \\ &= \frac{\mathbb{P}[\text{photon measured} \wedge \text{presence detected}]}{\mathbb{P}[\text{presence detected}]}. \end{aligned} \tag{5.51}$$

The presence of a photon is concluded either due to the photon being present and detected ($\eta_V \eta_{\text{det}}^{\text{QND}}$) *or* due to a dark count in the presence detection ($p_{\text{dc}}^{\text{QND}}$). Given that the photon is heralded, successful measurement happens if

- either the photon survived the presence detection (η_{surv}) *and* was not lost before measuring it (η_{equip}) *and* the measurement detector registered it (η_{det}) *or*

- (the measurement detector registered a dark count (p_{dc}) when the photon did not survive the presence detection *or* was lost before measurement) *or* (the measurement detector registered a dark count when the presence detection also registered a dark count).

We absorb all losses after the presence detection into one term that denotes the efficiency of the photon measurement $\eta_{\text{meas}} = \eta_{\text{det}}\eta_{\text{equip}}\eta_{\text{surv}}$. Using the above reasoning, we can write the probabilities in Eq. (5.51) as[9]

$$\eta_P = \frac{(\eta_{\text{meas}} + p_{\text{dc}})\eta_V \eta_{\text{det}}^{\text{QND}} + p_{\text{dc}} p_{\text{dc}}^{\text{QND}}}{\eta_V \eta_{\text{det}}^{\text{QND}} + p_{\text{dc}}^{\text{QND}}}. \tag{5.52}$$

Notice that[10]

$$\text{if } \eta_V \ll p_{\text{dc}}^{\text{QND}}: \qquad \eta_P \sim p_{\text{dc}}. \tag{5.53}$$

[9] For the event of a dark count it is implicit that the input photon was not detected. In our notation, factors of $1 - \eta_{\text{meas}}$ or $1 - \eta_V \eta_{\text{det}}^{\text{QND}}$ are included in the corresponding dark count variable.

[10] p_{dc} is negligible compared to the other term, so we neglect the second term in the bracket of eq. (5.52) for eq. (5.53).

If the probability that a photon enters the presence detector (η_V) is much smaller than the dark count rate $p_{\rm dc}^{\rm QND}$ then most photon presence detection events, and thus $c = 1$ commitments, will be due to dark counts! Then the (e.g. polarization) measurement on the photon will not give a click most of the time, making η_P very small. In the limit $\eta_V \to 0$ we obtain $\eta_P \to p_{\rm dc}$ as expected. Single-photon detectors routinely achieve $p_{\rm dc} \sim 10^{-7}$ or similar per detection window [Had09]. For such small η_P the usual lossy attack of guessing the provers' measurement setting (with probability $1/m$) still works because in practice we would not be able to use a high enough number of measurement settings m such that $\eta_P > 1/m$. So, introducing the commitment step would not help when $\eta_V \ll p_{\rm dc}^{\rm QND}$.

Let us write $\eta_V = \gamma p_{\rm dc}^{\rm QND}$ for some constant factor γ. We define the signal-to-noise ratio of the presence detection as

$$\texttt{SNR}_{\rm QND}(\gamma) = \frac{\eta_V \eta_{\rm det}^{\rm QND}}{\eta_V \eta_{\rm det}^{\rm QND} + p_{\rm dc}^{\rm QND}} = \frac{\gamma \eta_{\rm det}^{\rm QND}}{\gamma \eta_{\rm det}^{\rm QND} + 1}. \tag{5.54}$$

We have already argued that in the case $\eta_V \ll p_{\rm dc}^{\rm QND}$ our proposal is useless. Let us therefore focus on the case where η_V is at least the order of magnitude of $p_{\rm dc}^{\rm QND}$, corresponding to $\gamma \geq 1$. Then, using that $p_{\rm dc}$ is usually negligibly small compared to the other quantities, we can simplify η_P as follows:

$$\eta_P \sim \texttt{SNR}_{\rm QND}(\gamma)\eta_{\rm meas}. \tag{5.55}$$

The condition that the input transmission must be greater than $p_{\rm dc}^{\rm QND}$ will limit the distance between the verifiers and the prover. This, however, is not a characteristic of our protocol – it is an issue for any quantum communication protocol, as any protocol fails if most signals are noise originating from dark counts.

Distance between verifiers and prover

The transmission law for optical fibers reads $\eta = 10^{-\alpha L/10}$ [SJ09], where α is the attenuation of the fiber in dB/km and L is the fiber length in km. A standard value for current optical fibers is $\alpha = 0.2\,$dB/km [SJ09], with the most sophisticated achieving $\alpha = 0.14\,$dB/km [HTS+18]. We can solve for L and insert η_V in terms of the presence-detection dark count rate to obtain

$$L = -\frac{10}{\alpha}\log_{10}\left(\gamma p_{\rm dc}^{\rm QND}\right). \tag{5.56}$$

Rate of the protocol

There are several processes that we would like to do at a high rate in our protocol: generating single photons, modulating their polarization state, generating EPR pairs, fast switching between measurement settings depending on $f(x, y)$, and detecting single photons. State-of-the-art equipment is able to achieve the following rates (order of magnitude) today or in the near future:

- Single photon generation: MHz, in principle up to GHz [MSSM20]
- Polarization modulation: up to GHz [LLX+19]
- EPR state generation: up to GHz, depending on pump laser power [LVSL18, APS+21],
- Switching: up to THz [CHW+17]
- Single photon detector count rate: up to GHz [Had09]

Therefore, we expect our protocol can be run at least at MHz rate, and potentially at GHz rate with top equipment, albeit we acknowledge that it may be challenging to run all these processes at high rates simultaneously. The achievable rate of a setup will strongly depend on the equipment/architectures used, thus we only state current maximally achievable values here and refer to the cited articles and reviews for more details. The rate of the protocol will determine the time that is needed to reach the required number of rounds, as stated in Corollary 5.4.14.

The total number of rounds R that we expect to run to get $r = 320k^4$ rounds with commitment to play ($c = 1$) is $R = 320k^4/p_{\text{commit}}$. If the protocol is run at frequency ν, then the expected protocol duration t_{Pc} in seconds is therefore

$$t_{\mathsf{Pc}} = \frac{320k^4}{p_{\text{commit}}\nu}. \tag{5.57}$$

Given a choice of security parameter k, a probability to commit p_{commit} from the prover[11] and an achievable protocol frequency ν, one can then estimate how long it takes to run the protocol with the security guarantee given in Corollary 5.4.14.

5.5.1 True photon presence detection

Recently, a breakthrough paper [NFLR21] demonstrated true non-destructive detection of photonic qubits. To do so, they prepare a ^{87}Rb atom in an optical cavity in the superposition state $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, where $|0\rangle$ and $|1\rangle$ denote certain energetic states of the atom. The optical cavity is tuned such that a photon cannot enter the cavity if the atom is in state $|0\rangle$, but is allowed to enter if the state is $|1\rangle$. In that case, it gets reflected from one wall before leaving the cavity again, acquiring a $\pi/2$ phase shift. This interaction adds a phase to the combined photon-atom state, i.e. $|\psi_{\text{photon}}\rangle |1\rangle \mapsto -|\psi_{\text{photon}}\rangle |1\rangle$, changing the atom state from $|+\rangle$ to $|-\rangle$. Then a rotation is applied, mapping the atomic state $|+\rangle \mapsto |1\rangle$ and $|-\rangle \mapsto |0\rangle$, after which it is measured. If the result is 0 there was a photon interacting with the atom, if the result is 1 there was not. This measurement thus heralds the presence of a photon in the output mode of the optical

[11] Which would just be η_V, if the prover had perfect equipment.

cavity, which can be sent to a polarization measurement for example. [NFLR21] achieves the following relevant experimental parameters for their photon presence detector, which we can expect to improve in the future:

$$\begin{aligned} \text{Photon in output mode given heralding } (\eta_{\text{surv}})\text{:} &\quad \sim 25\text{-}55\%, \\ \text{Dark count rate } (p_{\text{dc}}^{\text{QND}})\text{:} &\quad \sim 3\%, \\ \text{Fidelity of photon in output mode:} &\quad \sim 96\%. \end{aligned} \tag{5.58}$$

Note that η_{surv} depends on the dark count rate and was measured using weak coherent light in [NFLR21] rather than true single photons. We take the stated range from their Figure 3b.

Although this technology is currently unusable for c-QPV due to the high dark count rate (relative to realistic η_V over longer distances), we can expect the parameters to improve significantly in the future. A true photon presence detector such as this could therefore be a clean and viable long-term solution for c-QPV.

5.5.2 Simplified presence detection via partial Bell measurement

For the near term, we consider a simplified photon presence detection based on a partial linear-optical Bell measurement. Essentially, the prover has to prepare a Bell state and teleport the input state to himself when it arrives. A conclusive[12] Bell measurement (BSM) heralds the presence of the input state, after which the prover briefly stores it until he receives the classical information x, y and measures it with the appropriate setting based on x, y. Note that we do not require a full Bell measurement. Even just discriminating 1 out of 4 Bell states via interference at one beam splitter would be enough. The scheme in Figure 5.5 [Wei94, BM95, MMWZ96] can distinguish 2 out of 4 Bell states, doubling the efficiency, while only using linear-optical equipment. Importantly, this scheme has first been demonstrated a long time ago [MMWZ96] and is experimentally feasible today.

First, note that any losses or inconclusive click patterns in the BSM itself will simply reduce the transmission rate η_V. This will jeopardize security only if it makes η_V so small that dark counts take over. Moreover, it may be that the teleportation corrections do not need to be actively applied but can be classically calculated and corrected, as is the case when they just flip the measurement result predictably like in c-QPV$_{\text{BB84}}^{f}$ for example. So then only a partial, linear-optical BSM and (very short) storage of the other EPR qubit would be experimentally required.

[12] We will define which click patterns count as successful further in Figure 5.5.

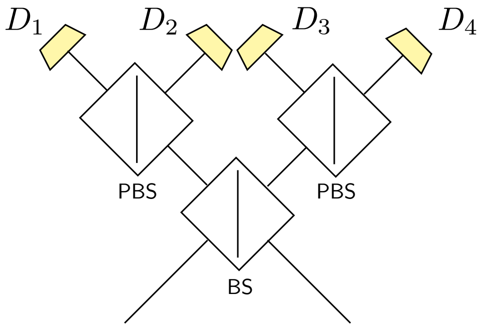


Figure 5.5: Schematically a partial Bell measurement can be implemented via a 50/50 beam splitter (BS), two polarization beam splitters (PBS) and four single photon detectors (D_i). An input state $|\Psi_-\rangle$ triggers one detector in each arm (D_1, D_3 or D_2, D_4), $|\Psi_+\rangle$ triggers two detectors in one arm (D_1, D_2 or D_3, D_4) and the states $|\Phi_+\rangle$, $|\Phi_-\rangle$ could trigger any, but just one, detector. So one can only conclusively distinguish $|\Psi_-\rangle$ and $|\Psi_+\rangle$, giving an efficiency of at most 50%, which is optimal for linear optics [CL01]. Any click patterns other than the ones corresponding to $|\Psi_\pm\rangle$ are deemed as "no-detection" events.

If we assume that the honest prover can generate entanglement when he expects the verifiers' input to arrive, then most of the time there will be one photon (the one from the EPR pair) going into the BSM setup, and only one dark count is needed for a false positive event. The relevant photon presence detection dark count rate would then be just the one of a conventional single photon detector, i.e. $p_{\text{dc}}^{\text{QND}} \sim p_{\text{dc}}$. The presence-detection efficiency $\eta_{\text{det}}^{\text{QND}}$ for such a BSM would be the efficiency of detecting both photons if they are present, i.e. $\eta_{\text{det}}^{\text{QND}} = \eta_{\text{det}}^2$. Moreover, the value of $\eta_{\text{meas}} = \eta_{\text{det}}\eta_{\text{equip}}\eta_{\text{surv}}$ depends on the equipment post-presence-detection, but is certainly upper bounded by η_{det}. So we have an upper bound of

$$\eta_P \sim \texttt{SNR}_{\text{QND}}(\gamma)\eta_{\text{meas}} \leq \frac{\gamma\eta_{\text{det}}^3}{\gamma\eta_{\text{det}}^2 + 1}. \tag{5.59}$$

Easy-to-use single-photon detectors have detection efficiencies of up to 20-65% [Had09], and the most sophisticated detectors reach up to 98%[13] [RNN+20]. In reality, there will also be losses pre-measurement, making the true value in Eq. (5.59) smaller than the upper bound. If these can be kept small enough, however, the true value of η_P will be close to the upper bound in Eq. (5.59) and secure c-QPV becomes possible if this value is large enough to prevent lossy attacks[14].

[13] Note that detection efficiencies always depend on the wavelength of the photons used.

[14] Meaning higher than the basis guessing probability $1/m$ or higher than the values obtained in [ES23] for c-QPV$_{\text{BB84}}^f$, for example.

With regard to the distance L between the verifiers and the prover, we can use Eq. (5.56) to get an estimate of what kinds of distances become possible for QPV with our proposal. As mentioned, with this setup $p_{\text{dc}}^{\text{QND}} \sim p_{\text{dc}} \sim 10^{-7}$. Moreover, η_V should be at least one (preferably more) order of magnitude larger than $p_{\text{dc}}^{\text{QND}}$ to obtain a decent signal-to-noise ratio, say $\gamma \gtrsim 10$. This yields via Eq. (5.56) that

$$L \lesssim 400\,\text{km} \tag{5.60}$$

for the distance between the verifiers and the prover. We summarize our findings in the following remark.

5.5.1. Remark. c-QPV makes a class of previously not loss-tolerant QPV protocols, with $\text{QPV}_{\text{BB84}}^f$ as a prime example, loss-tolerant even in practice as long as both the signal-to-noise ratio of the photon presence detection $\texttt{SNR}_{\text{QND}}$ and the efficiency of the prover measurement η_{meas} are sufficiently high such that η_P is high enough to prevent lossy attacks[15]. The signal-to-noise ratio $\texttt{SNR}_{\text{QND}}$ depends on the transmission η_V between the verifiers and the prover, the dark count rate $p_{\text{dc}}^{\text{QND}}$, and the detection efficiency $\eta_{\text{det}}^{\text{QND}}$. This ultimately limits the maximal distance between the verifiers and the prover[16]. The experimental requirements of our proposal in the prover laboratory are:

- The prover needs to be able to generate an EPR pair on demand
- Photon presence detection, e.g. via a partial BSM (like the scheme in Figure 5.5)
- A short delay loop so the prover can store the teleported qubit until the classical information x, y arrives. This time delay should be made as short as possible.
- The prover needs to be able to do the measurement depending on x, y and should be able to quickly switch between different measurements based on the value of $f(x, y)$.

The verifiers need to be able to generate and modulate single-photon states (e.g. polarization) with high frequency.

All requirements are practically feasible, or within reach, with state-of-the-art equipment.

[15] For example as studied in [ES23] for $\text{QPV}_{\text{BB84}}^f$, which carries over to our c-$\text{QPV}_{\text{BB84}}^f$.

[16] To much larger distances than previously possible for QPV, however.

5.6 Discussion

The three major roadblocks for practically implementable and secure QPV are: entangled attackers, slow honest quantum communication, and signal loss. On top of that, the honest protocol must be experimentally feasible. So far, no QPV protocol has been able to deal with all of these issues. Our work presents the first such protocol: $\mathsf{c}\text{-QPV}^{f}_{\text{BB84}}$. This opens up a feasible route to the first experimental demonstration of a QPV protocol that remains secure in a practical setting over long distances. We propose two options to do the required non-demolition photon presence detection: a clean and viable long-term solution [NFLR21], assuming the non-destructive detector parameters will improve in the future, and a simpler near-term solution via a partial Bell state measurement [MMWZ96] that can be implemented with just a few linear-optical components and conventional click/no-click single photon detectors. Given a sufficiently low dark-count rate in the photon-presence detection and sufficiently low loss in the prover's laboratory, secure QPV can be achieved in principle. $\mathsf{c}\text{-QPV}^{f}_{\text{BB84}}$ has two further major advantages: the quantum resources required for an attack scale in the classical input size (which can easily be made very large) and in case the prover uses the partial Bell measurement for photon presence detection, he does not need to actively apply any teleportation corrections, but can passively calculate and correct them instead, as they predictably flip the measurement outcome. By analyzing the rounds in which both attackers commit, we find that when we run enough rounds attacking the committing version of the protocols becomes as hard as the underlying protocol. It would be interesting if we can use the fact that it is also difficult for attackers to always answer equally on 'no commit' rounds in the analysis to get better bounds on the number of rounds we have to run. We argue that all the experimental requirements are, in principle, feasible and that in principle our protocol can be run at high rates. These properties taken together make $\mathsf{c}\text{-QPV}^{f}_{\text{BB84}}$ the first QPV protocol that can successfully deal with all the major practical issues of QPV.

Our result is not limited to $\text{QPV}^{f}_{\text{BB84}}$ per se, but can be applied to any QPV protocol that shares the same structure as $\text{QPV}^{f}_{\text{BB84}}$ and remains secure if the input state is replaced by any adversarial input state that does not depend on the classical input information x, y. It would be interesting to investigate whether our modification, introducing a prover commitment to play, can find application for other types of QPV protocols, or whether it can make other security models, such as the random oracle model [Unr14], loss tolerant.

Chapter 6

Relating NLQC to Information-Theoretic Cryptography

Non-local quantum computation (NLQC) is a cheating strategy for position-verification schemes, and has appeared in the context of the AdS/CFT correspondence. Here, we connect NLQC to the wider context of information-theoretic cryptography by relating it to a number of other cryptographic primitives. We show that one special case of NLQC, known as f-routing, is equivalent to the quantum analogue of the conditional disclosure of secrets (CDS) primitive, where by equivalent we mean that a protocol for one task gives a protocol for the other with only small overhead in resource costs. We further consider another special case of position-verification, which we call coherent function evaluation (CFE), and show CFE protocols induce similarly efficient protocols for the private simultaneous message passing (PSM) scenario. By relating position-verification to these cryptographic primitives, a number of results in the information-theoretic cryptography literature give new implications for NLQC, and vice versa. These include the first sub-exponential upper bounds on the worst case cost of f-routing of $2^{O(\sqrt{n \log n})}$ entanglement, the first example of an efficient f-routing strategy for a problem believed to be outside $P/poly$, linear lower bounds on quantum resources for CDS in the quantum setting, linear lower bounds on communication cost of CFE, and efficient protocols for CDS in the quantum setting for functions that can be computed with quantum circuits of low T depth.

This chapter is based on the paper "Relating non-local quantum computation to information theoretic cryptography" by Rene Allerstorfer, Harry Buhrman, Alex May, Florian Speelman and Philip Verduyn Lunel [ABM+24].

6.1 Introduction

In the previous chapters, we have discussed many aspects of position-verification scenarios. Position verification may be of interest as a goal in itself, or may serve as an authentication mechanism for use towards further cryptographic goals. In this chapter, we will again consider a coalition of attackers that have to apply some task, but the question is now not what protocols they can break, but more what the power of their model with some amount of entanglement is. This non-adversarial setting is *non-local quantum computation*. A non-local quantum computation replaces local actions within a designated spacetime region with actions outside that region along with entanglement shared across it. The basic setting is shown in Figure 6.1.

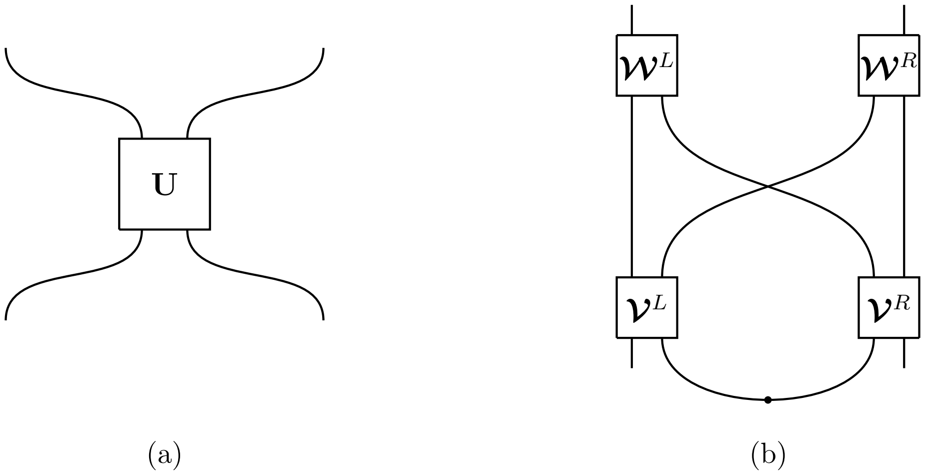


Figure 6.1: (a) Circuit diagram showing the local implementation of a unitary in terms of a unitary $\mathbf{U}$. In position-verification, an honest prover implements the required unitary in this form. (b) Circuit diagram showing the non-local implementation of a unitary $\mathbf{U}$. $\mathcal{V}^L$, $\mathcal{V}^R$, $\mathcal{W}^L$, and $\mathcal{W}^R$ are quantum channels. The lower, bent wire represents an entangled state. In position-verification, a dishonest prover must use a circuit of this form to implement a required unitary.

Non-local quantum computation has also been understood to arise naturally in the context of quantum gravity [May19, DC22, MX24], in particular within the context of the AdS/CFT correspondence. There, a higher-dimensional theory with gravity is given an equivalent description without gravity. In these two descriptions, processes that occur as local interactions in the higher-dimensional theory are reproduced in the dual, lower-dimensional description as non-local computations. This connection has led to consequences for the gravitational theory [MPS20, MSY22], and discussion around consequences for non-local computation [May22].

By definition, the bounds on the entanglement needed to attack the protocol

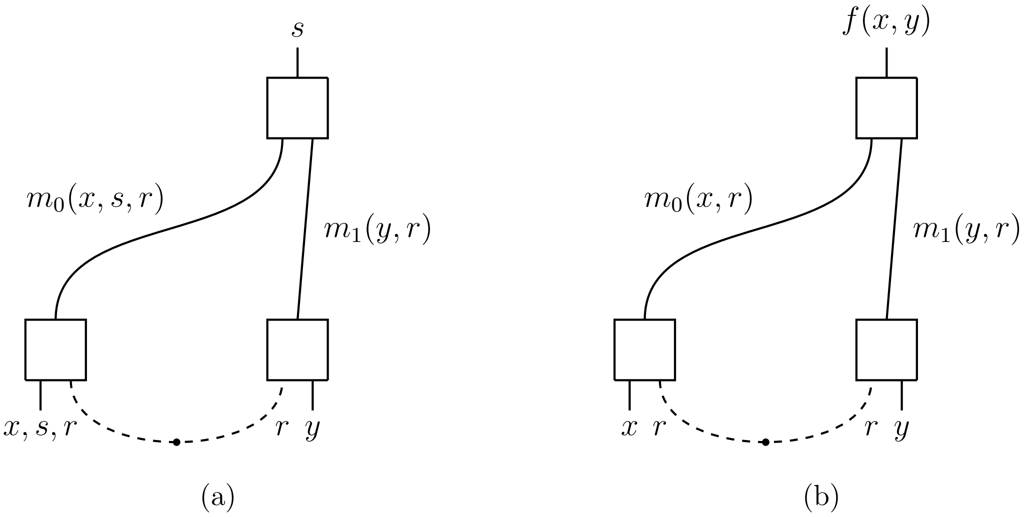


Figure 6.2: (a) A conditional disclosure of secrets (CDS) protocol. In the classical setting, Alice and Bob share randomness, but do not communicate. They receive inputs x and y, respectively. Alice additionally holds a secret s. They send messages to the referee. The protocol is correct if the referee can recover s from the messages if and only of $f(x,y)=1$. In the quantum setting, the randomness may be replaced by entanglement, and the messages and secret can be quantum. (b) A private simultaneous message protocol (PSM). Again Alice and Bob do not communicate, but share randomness. They hold the inputs x and y, respectively. The referee should be able to learn $f(x,y)$ but nothing else about (x,y). In the quantum setting, randomness is replaced with entanglement, and messages can be quantum.

correspond to the entanglement needed in a non-local computation. As a reminder from the previous chapters, we have linear lower bounds on entanglement [TFKW13], and exponential upper bounds [BK11], with only a little known in between. For a special case of a non-local computation known as f-routing, where each instance is defined by a classical Boolean function f, the entanglement cost has been upper bounded by the size of span program computing f [CM23], so that the class Mod_kL/poly[1] can be achieved efficiently.[2] For general unitaries, Clifford unitaries can be implemented with linear entanglement, and circuits with T depth of $\log n$ can be implemented with polynomial entanglement [Spe16a].

In this chapter, we prove connections between two well-studied cryptographic primitives, conditional disclosure of secrets (CDS) [GIKM00] and private simultaneous message passing (PSM) [IK97], and non-local quantum computation. These primitives are studied in the context of information-theoretic cryptography, in

[1] This class is reviewed in Section 6.4.1. It is inside of NC^2, the class of functions computed by $(\log(n))^2$ depth circuits.

[2] This builds on earlier work [BFSS13] achieving the class L.

particular in their relationship to secure multiparty computation [AIR01, IKP10], private information retrieval [GIKM00], secret sharing [AA20], and other cryptographic goals [BKN18]. We illustrate their functionality in Figure 6.2. Both settings generally involve k parties along with a referee, but in this chapter we focus on the $k = 2$ case, which is the setting we relate to non-local computation. In CDS, two non-communicating parties, Alice and Bob, receive inputs x and y, respectively. Alice additionally holds a secret s. Alice and Bob compute messages $m_0(x, s, r)$ and $m_1(y, r)$ based on their inputs and shared randomness, which are then sent to the referee. The referee should be able to recover the secret s if and only if $f(x, y) = 1$. PSM is a similar setting. There, Alice and Bob have inputs x and y along with shared randomness. They send messages $m_0(x, r)$ and $m_1(y, r)$ to the referee. The referee should be able to compute $f(x, y)$ from the messages, but not learn anything else about the inputs (x, y) than is implied by the value of $f(x, y)$. We give formal definitions of both primitives in Section 6.2.2.

To relate these primitives to non-local computation, we first show that the natural quantum generalization of CDS, which we denote as conditional disclosure of quantum secrets (CDQS), is equivalent to the f-routing task. More specifically, protocols for CDQS induce similarly efficient protocols for f-routing, and vice versa. Further, we show that classical CDS protocols induce similarly efficient quantum protocols. We also introduce a special case of non-local quantum computation known as a coherent function evaluation (CFE), which we show is closely related to the PSM model: efficient CFE protocols induce efficient PSM protocols using quantum resources (PSQM). We also give a weak converse that shows good PSQM protocols induce CFE protocols that succeed with constant (independent of the input size) probability.[3] The status of the relationship among these primitives is shown in Figure 6.3.

Our results relate position-verification to the wider setting of information-theoretic cryptography. This provides a partial explanation of the difficulty of finding better upper and lower bounds in non-local computation, since we now see that doing so would resolve other long-standing questions in cryptography[4]. In a positive direction, we use results in NLQC to give new results on CDS and PSM, and vice versa. Our key results are,

- Sub-exponential upper bounds on entanglement cost in f-routing for an arbitrary function (Corollary 6.7.3)

- Efficient CDQS and f-routing protocols for the quadratic residuosity problem, the first problem not known to be in P/poly with an efficient non-local computation protocol (Corollaries 6.6.5 and 6.6.6)

These results represent significant changes in our understanding of the efficiency

[3] We only prove this in the exact setting, while all other implications allow for small errors in correctness and small security leakage.

[4] For example lower bounds on f-routing give lower bounds on (classical) CDS.

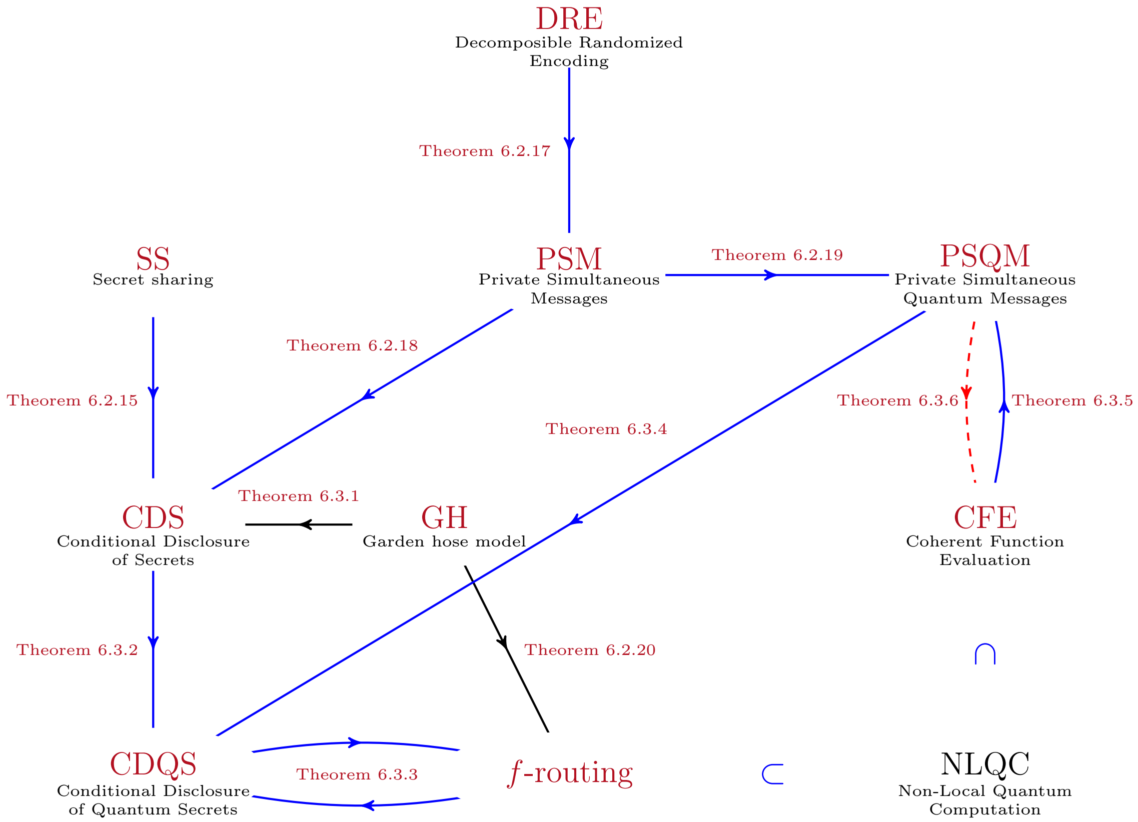

DRE
Decomposible Randomized Encoding
Theorem 6.2.17
SS
Secret sharing
PSM
Private Simultaneous Messages
Theorem 6.2.19
PSQM
Private Simultaneous Quantum Messages
Theorem 6.2.18
Theorem 6.2.15
Theorem 6.3.4
Theorem 6.3.6
Theorem 6.3.5
Theorem 6.3.1
CDS
Conditional Disclosure of Secrets
GH
Garden hose model
CFE
Coherent Function Evaluation
Theorem 6.3.2
Theorem 6.2.20
∩
CDQS
Conditional Disclosure of Quantum Secrets
Theorem 6.3.3
f-routing
⊂
NLQC
Non-Local Quantum Computation

Figure 6.3: Implications among primitives: an arrow from X to Y says that a protocol for X implies a protocol for Y with the same efficiencies (up to constant overheads). All implications shown in blue hold in the robust setting where we allow small errors and leakages. The dashed red line indicates that a perfect PSQM protocol that succeeds with high probability implies a CFE protocol that succeeds with constant probability. The subset symbol ⊂ indicates that f-routing and CFE are special cases of NLQC. Primitive abbreviations (DRE, PSM, ...) and theorem numbers link to relevant proofs or definitions.

of f-routing protocols. Previously, the best upper bounds for arbitrary functions were exponential, and the highest complexity functions with known efficient schemes were in $\mathrm{Mod}_k\mathrm{L}/\mathrm{poly}$.

From our connections between CDS, PSM, and NLQC, we also obtain a number of other implications,

- Linear lower bounds on communication complexity in CFE (Corollary 6.5.2)
- Linear lower bounds on entanglement in CDQS and PSQM for random functions (Corollaries 6.5.4 and 6.5.5), and logarithmic lower bounds on entanglement for the inner product function (Corollary 6.5.7 and 6.5.8)
- An entanglement efficient protocol for CDQS and PSQM when the target function f can be evaluated by a quantum circuit with low T-depth (Corollaries 6.6.11 and 6.6.13)

More broadly our results take position-verification from being an 'island' in the space of cryptographic primitives, with no known classical analogues or connections to other more standard notions, to being richly connected to a web of interrelated primitives, which themselves are related to central goals in information-theoretic cryptography. We hope these results lead to new perspectives on position-verification, and new perspectives in the study of CDS, PSM and related primitives. In particular a number of classical results on CDS and PSM may find natural quantum extensions in the context of NLQC. In the discussion, we comment on some cases where quantum analogues in the NLQC setting of classical cryptographic results are not yet known.

Outline of this Chapter

In Section 6.2, we present some relevant background. Section 6.2.1 gives a summary of the quantum information tools that we exploit. Section 6.2.2 summarizes the various cryptographic primitives that we study and relate. Section 6.2.3 gives the relations already known among these primitives.

In Section 6.3, we prove new relationships among our set of cryptographic primitives. The full set of connections is presented as Figure 6.3. The relationships between CDS and CDQS, CDQS and f-routing, CFE and PSQM, and CDQS and PSQM are new to the best of our knowledge.

In Section 6.4, we summarize the known results on the complexity of efficiently achievable functions in the PSQM, CDQS, and f-routing settings. The status of the complexity of efficiently achievable functions in the general case is not too changed by our results: existing CDS protocols give f-routing protocols, but in the existing literature on both f-routing and CDS the most efficient protocols have a cost like $(\log p) \cdot SP_p(f)$ where $SP(f)$ denotes the minimal size of a span program over $\mathbb{Z}_p$ computing f [GIKM00, CM23].

Sections 6.5 and 6.6 spell out the implications for non-local computation and its special cases that follow from known results in CDS and PSM, and conversely the implications for CDS and PSM that follow from known results in non-local computation. In Section 6.5 we give new lower bounds that follow in this way. In Section 6.6 we give new upper bounds for a collection of problems, one of the most important being a function believed to be outside of *P*/*poly* for which an efficient f-routing protocol exists. In Section 6.7 we include the most significant implication that follows from the connections we find, which is a sub-exponential upper bound on f-routing for arbitrary functions. Relating to this construction, we find that super-polynomial lower bounds on f-routing schemes are tied to open problems in computational complexity.

Section 6.8 concludes with some discussion and open problems, in particular commenting on connections to quantum gravity and to some results in the classical cryptography literature that may have quantum analogues relevant to the NLQC setting.

6.2 Background

6.2.1 Tools from quantum information theory

In this section, we briefly recall some standard tools of quantum information theory. We follow the conventions of [Wil13], where an overview of these tools and further references can also be found.

We define the diamond norm distance, which is a distance measure on the space of quantum channels.

6.2.1. Definition. Let $\boldsymbol{\mathcal{N}}_{B\rightarrow C}, \boldsymbol{\mathcal{M}}_{B\rightarrow C} : \mathcal{L}(\mathcal{H}_A) \rightarrow \mathcal{L}(\mathcal{H}_B)$ be quantum channels. The **diamond norm distance** is defined by

$$||\boldsymbol{\mathcal{N}}_{B\rightarrow C} - \boldsymbol{\mathcal{M}}_{B\rightarrow C}||_\diamond = \sup_d \max_{\rho_{A_dB}} ||\boldsymbol{\mathcal{N}}_{B\rightarrow C}(\Psi_{A_dB}) - \boldsymbol{\mathcal{M}}_{B\rightarrow C}(\Psi_{A_dB})||_1, \tag{6.1}$$

where $\rho_{A_dB} \in \mathcal{D}(\mathcal{H}_{A_d} \otimes \mathcal{H}_B)$ and $\mathcal{H}_{A_d}$ is a d dimensional Hilbert space.

The diamond norm distance has an operational interpretation in terms of the maximal probability of distinguishing quantum channels [KSV02, Wil13].

Decoupling and recovery

The basic idea underlying the connection between CDS and f-routing that we will give is the notion of decoupling and complementary recovery. To develop this, consider a quantum channel $\boldsymbol{\mathcal{N}}_{B\rightarrow C} : \mathcal{L}(\mathcal{H}_B) \rightarrow \mathcal{L}(\mathcal{H}_C)$. We would like to understand when this channel has an (approximate) inverse. Consider any unitary extension of the channel, call it $\mathbf{V}_{BE'\rightarrow CE}$, which satisfies

$$\boldsymbol{\mathcal{N}}_{B\rightarrow C}(\cdot) = \mathrm{Tr}_E(\mathbf{V}_{BE'\rightarrow CE} \cdot \mathbf{V}^\dagger_{BE'\rightarrow CE}). \tag{6.2}$$

A classic result [SW02b, SW02a] says that if we input a maximally entangled state $|\Psi^+\rangle_{AB}$ and find that $I(A:E)_{\mathcal{N}(\Psi^+)}$ is small, say less than ϵ, then there exists an inverse channel $\mathcal{N}^{-1}_{B\to C}$ which works well in the sense that the fidelity

$$F(\Psi^+, \mathcal{N}^{-1}_{B\to C} \circ \mathcal{N}_{B\to C}(\Psi^+)) \geq 1-\sqrt{\epsilon}. \tag{6.3}$$

The inverse channel is succeeding when acting on the maximally entangled state, which can also be understood as acting correctly in an averaged (over input states) sense.

We will make use of a stronger notion of decoupling, which shows that a worst-case notion of decoupling implies the existence of an inverse channel that always succeeds. The theorem was proved in [KSW08b].

6.2.2. Theorem. *Let $\mathcal{N}_{A\to B} : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$ be a quantum channel, and let $\mathcal{N}^c_{A\to E}$ be the complementary channel. Let $\mathcal{S}_{A\to E}$ be a completely depolarizing channel, which traces out the input and replaces it with a fixed state σ_E. Then we have that*

$$\begin{aligned}\frac{1}{4}\inf_{\mathcal{D}_{B\to A}} ||\mathcal{D}_{B\to A}\circ\mathcal{N}_{A\to B} - \mathcal{I}_{A\to A}||_\diamond^2 &\leq ||\mathcal{N}^c_{A\to E} - \mathcal{S}_{A\to E}||_\diamond \\ &\leq 2\inf_{\mathcal{D}_{B\to A}} ||\mathcal{D}_{B\to A}\circ\mathcal{N}_{A\to B} - \mathcal{I}_{A\to A}||_\diamond^{1/2},\end{aligned} \tag{6.4}$$

where the infimum is over all quantum channels $\mathcal{D}_{B\to A}$.

6.2.2 Definitions of the primitives

In this section, we give the definitions of each of the primitives that we discuss in this chapter. Note that we focus on information-theoretic definitions of security. In all cases there are meaningful versions of these primitives with computational security, but we have not explored their connections to non-local computation.

Conditional disclosure of secrets

We first define the classical CDS setting, which we also illustrate in Figure 6.2a.

6.2.3. Definition. A **conditional disclosure of secrets (CDS)** task is defined by a choice of function $f : \{0,1\}^{2n} \to \{0,1\}$. The scheme involves inputs $x \in \{0,1\}^n$ given to Alice, and inputs $y \in \{0,1\}^n$ given to Bob. Alice and Bob share a random string $r \in R$. Additionally, Alice holds a string s drawn from the distribution S, which we call the secret. Alice sends message $m_0(x,s,r)$ to the referee, and Bob sends message $m_1(y,r)$. We require the following two conditions on a CDS protocol.

- **ϵ-correct:** There exists a decoding function $D(m_0,x,m_1,y)$ such that

$$\forall s\in S,\ \forall\,(x,y)\in X\times Y\ s.t.\ f(x,y)=1,\ \Pr_{r\leftarrow R}[D(m_0,x,m_1,y)=s]\geq 1-\epsilon. \tag{6.5}$$

- **δ-secure:** There exists a simulator producing a distribution Sim on the random variable $M = M_0M_1$ such that

$$\forall s \in S,\, \forall\, (x,y) \in X \times Y \;s.t.\; f(x,y) = 0,\;\; ||Sim_{M|xy} - P_{M|xys}||_1 \leq \delta. \tag{6.6}$$

Notice that in our definition of CDS we have imposed that the secret be held only by Alice. We can easily transform protocols that succeed with the secret held on both sides to one where the secret is held only on one side. This is a standard remark about CDS, though we do not know a reference where this is shown in the imperfect setting, so we give a simple proof of this fact here.

6.2.4. Remark. A CDS task in which s is initially held by Alice and Bob can be turned into one where only Alice holds s at the cost of $|s|$ shared random bits, and $|s|$ bits of communication. If the CDS protocol is ϵ-correct and δ-secure, the one-sided protocol will be ϵ-correct and $O(\sqrt{\delta})$ secure.

Proof:
To see this, suppose that we have a perfectly correct and secure CDS protocol which works when s is held on both sides. Then run this protocol on a randomly chosen s', and have Alice send $s' \oplus s$ to the referee. Only Alice needs to know s to run this protocol.

Suppose that our initial CDS protocol is ϵ-correct and δ-secure. Then the new CDS will also be ϵ-correct, since s can be computed deterministically from s' and the bit $\tilde{s} = s \oplus s'$. To understand security, note that δ-security of the original protocol implies

$$||P_{S'M} - P_{S'}P_M||_1 \leq \delta. \tag{6.7}$$

Using this, $P_{S\tilde{S}} = P_S P_{\tilde{S}}$ (from the properties of the one-time pad), and that S and M are independent conditioned on $\tilde{S}$, we have

$$\begin{aligned} ||P_{S\tilde{S}M} - P_S P_{\tilde{S}} P_M||_1 &= ||P_{S|\tilde{S}M} P_{\tilde{S}M} - P_S P_{\tilde{S}} P_M||_1 \\ &= ||P_{S|\tilde{S}} P_{\tilde{S}M} - P_S P_{\tilde{S}} P_M||_1 \\ &\leq ||P_{S|\tilde{S}} P_{\tilde{S}} P_M - P_S P_{\tilde{S}} P_M||_1 + \delta \\ &= ||P_{S\tilde{S}} P_M - P_S P_{\tilde{S}} P_M||_1 + \delta \\ &= \delta, \end{aligned} \tag{6.8}$$

which is exactly δ security of the one-sided CDS protocol. □

Finally, we remark that a CDS for secret s_1 and a CDS for secret s_2 can be run in parallel using fresh randomness while maintaining security and correctness of each CDS scheme. To see this, call the message for the first CDS M_1 and the message for the second CDS M_2. If we consider how much the referee can learn about the secret s_1, message M_2 does not reveal anything, because it depends only on the randomness r_2, the inputs (which the referee knows already as part of the CDS for s_1), and s_2. All of these variables are already known by the referee as part of the CDS for s_1, or are uncorrelated with s_1. More succinctly, the distribution on s_1 is independent of M_2 when conditioning on XY, so revealing M_2 does not help the referee learn s_1, given that they already know XY, or in notation

$$P_{M_1M_2|xys} = P_{M_1|xys_1}P_{M_2|xys_2}. \tag{6.9}$$

A similar statement establishes security of the CDS hiding s_2 in the presence of message M_1.

As a consequence of the above comments, the CDS hiding secret $s = (s_1, s_2)$ given by running the CDS for each secret in parallel has good security and correctness, as we capture in the next lemma.[5]

6.2.5. Lemma. *Suppose we have a CDS for function f which is ϵ-correct and δ-secure, hides k bits and uses r bits of randomness and c bits of communication. Then we can build a CDS for function f that hides mk bits, is $m\epsilon$ correct and $m\delta$ secure and which uses mr bits of randomness and mc bits of communication.*

Proof:
The strategy is to repeat the CDS protocol that hides k bits m times in parallel. To understand the correctness of the new protocol, notice that on 1 instances the probability of the referee guessing s_i correctly is at least $1-\epsilon$, so their probability of guessing all m strings s_i correctly is at least $(1-\epsilon)^m \geq (1-mk)$. To understand security, we define a simulator for the composed protocol by taking the product of the distributions for a single instance of the protocol,

$$Sim_{M_1...M_m|xy} \equiv Sim_{M_1|xy}...Sim_{M_m|xy}. \tag{6.10}$$

We also note that, using fresh randomness for each instance of the CDS, we can extend Equation 6.9 to

$$P_{M_1...M_m|xys} = P_{M_1|xys_1}...P_{M_m|xys_m}. \tag{6.11}$$

Then by repeated application of the triangle inequality, and using security of each instance of the CDS, we have that on 0 instances

$$\begin{aligned}||Sim_{M_1...M_m|xy} - P_{M_1...M_m|xys}||_1 &= ||Sim_{M_1|xy}...Sim_{M_m|xy} - P_{M_1|xys_1}...P_{M_m|xys}||_1 \\ &\leq m\delta,\end{aligned}$$

as claimed. □

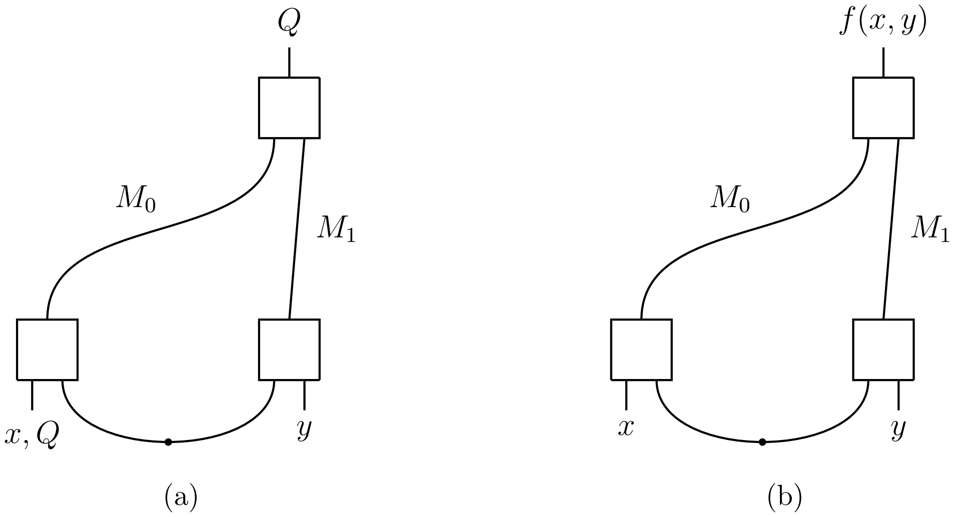


Figure 6.4: (a) Illustration of a CDQS protocol. Alice and Bob share an entangled resource state, illustrated as the solid curved line. Alice receives the classical string $x \in \{0,1\}^n$ as input, and a quantum system Q, which we take to be maximally entangled with a reference R. Bob receives input $y \in \{0,1\}^n$. Alice and Bob prepare quantum systems M_0 and M_1, which they pass to the referee. The protocol is correct if when $f(x,y) = 1$ the map from Q to M_0M_1 can be reversed, and secure when for $f(x,y) = 0$ the $M = M_0M_1$ system is independent of the input state on Q. See definition 6.2.6. (b) A PSQM protocol. Again Alice and Bob share an entangled resource state. Alice receives input $x \in \{0,1\}^n$, Bob receives input $y \in \{0,1\}^n$. Alice and Bob prepare quantum systems M_0 and M_1, which they pass to the referee. The protocol succeeds if the referee can determine $f(x,y)$, but the system $M = M_0M_1$ otherwise reveals nothing about the inputs x, y. See definition 6.2.8.

Conditional disclosure of quantum secrets

To the best of our knowledge the quantum analogue of the CDS model has not been studied explicitly in the literature.[6] We give a definition here which features quantum resources and a quantum secret. The CDQS primitive is illustrated in Figure 6.4a.

6.2.6. Definition. A **conditional disclosure of quantum secrets (CDQS)** task is defined by a choice of function $f : \{0,1\}^{2n} \to \{0,1\}$, and a d_Q dimensional Hilbert space $\mathcal{H}_Q$ which holds the secret. The task involves inputs $x \in \{0,1\}^n$ and system Q given to Alice, and input $y \in \{0,1\}^n$ given to Bob. Alice sends message system M_0 to the referee, and Bob sends message system M_1. Label the combined message systems as $M = M_0M_1$. Label the quantum channel defined by Alice and Bob's combined actions $\boldsymbol{\mathcal{N}}^{xy}_{Q\to M}$. We put the following two conditions on a CDQS protocol.

- ϵ**-correct:** There exists a channel $\boldsymbol{\mathcal{D}}^{x,y}_{M\to Q}$, called the decoder, such that

$$\forall (x,y) \in X \times Y \;\; s.t. \;\; f(x,y)=1, \;\; ||\boldsymbol{\mathcal{D}}^{x,y}_{M\to Q} \circ \boldsymbol{\mathcal{N}}^{x,y}_{Q\to M} - \boldsymbol{\mathcal{I}}_{Q\to Q}||_\diamond \leq \epsilon. \tag{6.12}$$

- δ**-secure:** There exists a quantum channel $\boldsymbol{\mathcal{S}}^{x,y}_{\varnothing\to M}$, called the simulator, such that

$$\forall (x,y) \in X \times Y \;\; s.t. \;\; f(x,y)=0, \;\; ||\boldsymbol{\mathcal{S}}^{x,y}_{\varnothing\to M} \circ \mathrm{Tr}_Q - \boldsymbol{\mathcal{N}}^{x,y}_{Q\to M}||_\diamond \leq \delta. \tag{6.13}$$

The notions of ϵ-correctness and δ-security given here closely mimic the classical ones. In words, the correctness condition says that when $f(x,y)=1$ the referee can reverse the effect of Alice and Bob's actions on the Q system. The security condition says that when $f(x,y)=0$ the system M seen by the referee is close to one that they could have prepared with no access to Q.

In our definition of CDQS, we require that a quantum system Q be taken as the secret, and allow the use of quantum resources. Another quantum variant of CDS we could have defined would allow quantum resources but restrict to a classical secret. We could call this CDQS'. This variant is in fact equivalent to the above definition. This follows from our proof below that classical CDS protocols gives quantum CDS protocols, which is easily modified to show a CDQS' gives CDQS with similar resources. Then one can observe that a CDQS protocol can be modified to a CDQS' protocol by choosing the secret to be a state in a chosen basis. Together, these observations give that CDQS' and CDQS are equivalent.

Private simultaneous message passing

[5] This is a simple, but weak, method of obtaining a CDS for a long secret from CDS for a short secret. It will suffice for our purposes, but see [AARV21, AA20] for improved results.

[6] It has been studied in an indirect way, since (as we show later) it is equivalent to f-routing.

Next, we move on to discuss another basic cryptographic primitive of interest in this chapter, which is private simultaneous message passing. This primitive is illustrated in Figure 6.2b.

6.2.7. Definition. A **private simultaneous message (PSM)** task is defined by a choice of function $f : X \times Y \to Z$. The inputs to the task are n-bit strings x and y given to Alice and Bob, respectively. Alice then sends a message $m_0(x, r)$ to the referee, and Bob sends message $m_1(y, r)$. From these inputs, the referee prepares an output bit z. We require that the task be completed in a way that satisfies the following two properties.

- **ϵ-correctness:** There exists a decoder Dec such that

$$\forall (x, y) \in X \times Y, \quad \Pr[Dec(m_0, m_1) = f(x, y)] \geq 1 - \epsilon. \tag{6.14}$$

- **δ-security:** There exists a simulator producing a distribution Sim on the random variable $M = M_0 M_1$ such that

$$\forall (x, y) \in X \times Y, \quad ||Sim_{M|f(x,y)} - P_{M|xy}||_1 \leq \delta. \tag{6.15}$$

  Stated differently, the distribution of the message systems is δ-close to one that depends only on the function value, for every choice of x, y.

In PSM we can allow the function f to take Boolean or other values. For instance, we can take f to be a natural number valued and defined by a counting problem. Another comment is that PSM protocols can be run in parallel, in the sense that ϵ-correct and δ-secure protocols for $f_1(x, y)$ and $f_2(x, y)$ can be run together to give a 2ϵ-correct and 2δ-secure protocol for the function $f(x, y) = (f_1(x, y), f_2(x, y))$. This is straightforward to show from the security definition.

Private simultaneous quantum message passing (PSQM)

As with CDS, there is a natural quantum version of PSM. In this case, the functionality of the protocol is unchanged, but the allowed resources are now quantum mechanical. A PSQM protocol is shown in Figure 6.6a.

6.2.8. Definition. A private simultaneous quantum message (PSQM) task is defined by a choice of function $f : X \times Y \to Z$. The inputs to the task are n-bit strings x and y given to Alice and Bob, respectively, each of which are chosen independently and at random. Alice then sends a quantum message system M_0 to the referee, and Bob sends a quantum message system M_1. From the combined message system $M = M_0 M_1$, the referee prepares an output bit z. We require that the task be completed in a way that satisfies the following two properties.

- **ϵ-correctness:** There exists a decoding map $\mathbf{V}_{M\to Z\tilde{M}}$ such that $\forall(x,y) \in X \times Y$:

$$\left|\left|\mathrm{Tr}_{\tilde{M}}(\mathbf{V}_{M\to Z\tilde{M}}\rho_M(x,y)\mathbf{V}^{\dagger}_{M\to Z\tilde{M}}) - |f_{xy}\rangle\langle f_{xy}|_Z\right|\right|_1 \leq \epsilon. \tag{6.16}$$

  where $\rho_M(x,y)$ is the density matrix on M produced on inputs x, y.

- **δ-security:** There exists a simulator, which is a quantum channel $\boldsymbol{\mathcal{S}}_{Z\to M}(\cdot)$, such that $\forall(x,y) \in X \times Y$:

$$\left|\left|\rho_M(x,y) - \boldsymbol{\mathcal{S}}_{Z\to M}(|f_{xy}\rangle\langle f_{xy}|_Z)\right|\right|_1 \leq \delta. \tag{6.17}$$

  Stated differently, the state of the message systems is δ-close to one that depends only on the function value, for every choice of input.

Just like in the classical case, PSQM protocols can be run in parallel with only small relaxations in security and correctness.

Decomposable randomized encodings

A related primitive, which we shall make briefer use of, is the notion of a decomposable randomized encoding. We recall some definitions given in [CPS13].

6.2.9. Definition. Let $X, Y, \hat{Y}, R$ be finite sets and let $f : X_1 \times ... \times X_n \to Y$. A function $\hat{f} : X \times R \to \hat{Y}$ is an ϵ-correct and δ-private **randomized encoding** for f if it satisfies

- **ϵ-correctness:** There exists a function *Dec* called a decoder such that for every $x \in X$ and $r \in R$ we have

$$\Pr[Dec(\hat{f}(x,r)) = f(x)] \geq 1 - \epsilon. \tag{6.18}$$

- **δ-privacy:** There exists a randomized function, called a simulator, producing the random variable *Sim* such that

$$||Sim_{\hat{Y}|Y} - P_{\hat{Y}|X}||_1 \leq \delta. \tag{6.19}$$

6.2.10. Definition. A **decomposable randomized encoding (DRE)** for a function $f : X_1 \times ... \times X_n \to Y$ is a randomized encoding of f that has the form

$$\hat{f}(x_1, ..., x_n; r) = (\hat{f}_1(x_1, r), ..., \hat{f}_n(x_n, r)). \tag{6.20}$$

A DRE is ϵ-correct and δ-secure under the same conditions as a randomized encoding, given above.

We will in fact only use that certain randomized encodings are decomposable across a single splitting of the inputs. That is we are interested in functions $f : X \times Y \to Z$ and need the randomized encoding to take the form

$$\hat{f}(x, y; r) = (\hat{f}_1(x, r), \hat{f}_2(y, r)). \tag{6.21}$$

In this setting we will say $f(x, y)$ has a randomized encoding decomposable across $X \times Y$.

Non-local computation

Finally, we come to the notion of a non-local computation, which was first studied in the context of cheating strategies for position-verification tasks. The general setting is shown in Figure 6.1. A non-local computation takes the form shown in Figure 6.1b, with the goal being to simulate the action of a local unitary (Figure 6.1a).

We will not give a formal definition of a fully general NLQC here but instead focus on two special cases. The first, f-routing, was introduced in [KMS11] and studied further in [BFSS13]. It has been especially well studied in the non-local computation literature because it is of interest in developing practical position-verification schemes. We will also see that it is closely related to the CDQS primitive.[7]

6.2.11. Definition. An **f-routing** task is defined by a choice of Boolean function $f : \{0,1\}^{2n} \to \{0,1\}$, and a d dimensional Hilbert space $\mathcal{H}_Q$. Inputs $x \in \{0,1\}^n$ and system Q are given to Alice, and input $y \in \{0,1\}^n$ is given to Bob. Alice and Bob exchange one round of communication, with the combined systems received or kept by Bob labeled M and the systems received or kept by Alice labeled M'. Label the combined actions of Alice and Bob in the first round as $\boldsymbol{\mathcal{N}}^{x,y}_{Q\to MM'}$. The f-routing task is completed ϵ-correctly if there exists a channel $\boldsymbol{\mathcal{D}}^{x,y}_{M\to Q}$ such that,

$$\forall (x, y) \in X \times Y \, s.t. \, f(x, y) = 1, ||\boldsymbol{\mathcal{D}}^{x,y}_{M\to Q} \circ \mathrm{Tr}_{M'} \circ \boldsymbol{\mathcal{N}}^{x,y}_{Q\to MM'} - \boldsymbol{\mathcal{I}}_{Q\to Q}||_\diamond \leq \epsilon, \tag{6.22}$$

and there exists a channel $\boldsymbol{\mathcal{D}}^{x,y}_{M'\to Q}$ such that

$$\forall (x, y) \in X \times Y \, s.t. \, f(x, y) = 0, ||\boldsymbol{\mathcal{D}}^{x,y}_{M'\to Q} \circ \mathrm{Tr}_{M} \circ \boldsymbol{\mathcal{N}}^{x,y}_{Q\to MM'} - \boldsymbol{\mathcal{I}}_{Q\to Q}||_\diamond \leq \epsilon. \tag{6.23}$$

In words, Bob can recover Q if $f(x, y) = 1$ and Alice can recover Q if $f(x, y) = 0$.

[7] Our definition here gives a particular notion of an ϵ-correct f-routing scheme, which requires the protocol route an arbitrary quantum state correctly. Other definitions [BCS22] require correct action on only the maximally entangled state. For inputs of a fixed size, these are equivalent.

The second special case that we study is coherent function evaluation. We introduce this as the special case of NLQC that implies the PSQM primitive, as we show below. In addition, it is similar to non-local computations studied in [JKPPG21], which used Banach space techniques to study lower bounds on quantum resources in these non-local computations.

6.2.12. Definition. A **coherent function evaluation (CFE)** task is defined by a choice of a Boolean function $f : \{0,1\}^{2n} \to \{0,1\}$. The task is to implement the isometry

$$\mathbf{V}_f = \sum_{xy} |xy\rangle_{Z'} |f_{xy}\rangle_Z \langle x|_X \langle y|_Y \,, \tag{6.24}$$

in the non-local form of Figure 6.1b. We say that a CFE protocol is ϵ-correct if the diamond norm distance between $\mathbf{V}_f$ and the implemented channel is not larger than ϵ.

Secret sharing

An important tool throughout cryptography, and in particular in our context, is the notion of a secret-sharing scheme. We introduce this next.

6.2.13. Definition. A **secret sharing scheme S** is a map from a domain K and randomness R to variables $S_1, ..., S_n$, here called shares. Let A be a subset of the S_i, $\mathcal{S}_A$ the distribution on the shares A, and $\mathbf{A}$ a set of subsets of the S_i. Then a scheme $\mathbf{S}$ realizes the access structure $\mathbf{A}$ with **ϵ-correctness** if, for each subset of shares $A \in \mathbf{A}$ there exists a decoding map $D_A : A \to K$ such that

$$\forall s \in K, \quad \Pr[D_A(\mathcal{S}_A) = s] \geq 1 - \epsilon. \tag{6.25}$$

A scheme $\mathbf{S}$ is **δ-secure** if, whenever $U \notin \mathbf{A}$, there exists a map that produces a distribution Sim on U such that

$$||\mathrm{Sim}_U - \mathcal{S}_{U|K}||_1 \leq \delta. \tag{6.26}$$

If $\epsilon = \delta = 0$ we say that the scheme $\mathbf{S}$ is perfect.

The access structure of a secret scheme can be specified as a set of subsets of shares, as in the above definition, or equivalently in terms of an **indicator function**. The indicator function is defined by

$$f_I(x) = \begin{cases} 1 & \text{if } \{S_i : x_i = 1\} \in \mathcal{A}, \\ 0 & \text{otherwise.} \end{cases} \tag{6.27}$$

We can observe that if $A \in \mathcal{A}$ then necessarily $A \cup S_i \in \mathcal{A}$. This follows because if we can reconstruct the secret from A, we can also reconstruct it from a larger set. This means that valid indicator functions will always be monotone.

The garden hose game

The garden hose game [BFSS13] is a model of communication complexity defined, informally, as follows. Alice and Bob are neighbors and wish to compute a function $f(x, y)$, where Alice holds the input x and Bob the input y. They have a set of m pipes that run through their fence and connect the two yards. Alice has a tap, which she can connect to any of the pipe openings on her side of the fence. Alice and Bob additionally have hoses, which they can use to connect the ends of the pipes on the same side of the fence. Their strategy is to choose how to connect the tap to the pipes, and connect pipes to each other with hoses, in a way that depends on their respective inputs. Then, Alice turns on the tap. Alice and Bob win the garden hose game if the water spills on Alice's side of the fence when $f(x, y) = 0$, and on Bob's side of the fence when $f(x, y) = 1$. For a formal definition of the garden-hose game, we refer the reader to [BFSS13].

The garden hose game gives an interesting notion of the communication complexity of a function, which we formalize next.

6.2.14. Definition. The **garden-hose complexity** of a function $f : \{0, 1\}^n \times \{0, 1\}^n \to \{0, 1\}$ is the minimal number of pipes needed to complete the garden hose game for the function $f(x, y)$ deterministically.

All functions can be computed in the garden hose game. To see why, observe that for any $f(x, y)$ Alice and Bob can carry out the following strategy. They prepare 2^{n+1} pipes, which we label as $\{p_i, p'_i\}_{i=1}^n$. Upon receiving input x, Alice connects her tap to pipe p_x. Bob connects pipe p_i to p'_i whenever $f(i, y) = 0$, and leaves it open otherwise. Upon turning on the tap, the water flows through pipe p_x, then back to Alice if $f(x, y) = 0$ and spills on the right otherwise, as needed. A sightly smarter strategy lowers the worst case garden-hose complexity to $2^n + 1$. See [BFSS13].

Other related primitives

Each of the primitives discussed above is, in turn, related to others in various ways. Reviewing these further connections is beyond the scope of this chapter. Instead, we have included in our discussion only new connections among primitives, or primitives for which we have found that the connection to NLQC gives a new result on NLQC, or for which NLQC implies a new result on the primitive. We briefly mention, however, some settings with natural relationships to the ones discussed here; our list and references are not exhaustive. CDS and PSM are related to zero-knowledge proofs [AR17], secret sharing [ABNP20], communication complexity [AV21], private information retrieval [IK97], and secure multiparty computation [IK97]. A useful review of these primitives and the broader context of information-theoretic cryptography is given in [Ben20]. Quantum secret sharing was related to f-routing in [CM23]. All of these connections may be interesting to revisit in the quantum setting, and in light of the connection to non-local computation and position-verification.

6.2.3 Existing relations among primitives

SS gives CDS

In [GIKM00], the authors upper bound the randomness complexity of a CDS scheme in terms of the size of a secret sharing scheme whose access structure is related to f. We recall their result next, narrowing their result to the two-player case for simplicity.

6.2.15. Theorem. *Let $f_M : \{0,1\}^m \times \{0,1\}^m \to \{0,1\}$ be a monotone Boolean function and let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ be a projection of f_M, that is $f(x,y) = f_M(g_1(x), g_2(y))$. Let $\mathbf{S}$ be a perfect secret sharing scheme realizing the access structure f_M, in which the total share size is c, and let s denote a secret (from the domain of $\mathbf{S}$) which is known to all players. Then there exists a CDS protocol for disclosing s subject to the condition f with randomness c, and a (perhaps different) protocol with communication complexity bounded above by c.*

The protocol which establishes this theorem is, heuristically, the following. We start by illustrating the case where $f = f_M$ is already a monotone function, and so can be realized as the indicator function of some secret sharing scheme $\mathbf{S}$. Then the protocol is as follows. Without loss of generality, take Alice and Bob to both hold the secret s (see Remark 6.2.4). To carry out the protocol, both parties prepare a secret sharing scheme $\mathbf{S}$ which has indicator function f_M, using their shared randomness as the randomness R needed to prepare the scheme. Then, Alice sends those shares S_i to the referee for which $x_i = 1$, and Bob sends those shares S_{i+n} for which $y_i = 1$. Then if $f_M(x,y) = 1$, following this local rule, they will have collectively sent an authorized set of shares, and the referee can reconstruct the secret s. If $f_M(x,y) = 0$, they will have sent an unauthorized set of shares and the referee cannot learn the secret. To extend this to non-monotone functions, Alice and Bob first locally compute g_1 and g_2 respectively, and then perform the same secret sharing protocol now with bits of $g_1(x)$ or $g_2(y)$ controlling which shares are sent to the referee. Notice that the communication complexity is at most the total size of the shares of the secret sharing scheme.

To see the protocol that gives an upper bound for the randomness complexity[8], we now have only Alice prepare the shares of the secret sharing scheme. For shares $i \leq n$, she sends share S_i if $x_i = 1$ as before. For shares $i > n$, she sends $S_i \oplus r_i$, where the XOR is taken bitwise with a random string r_i of length $|S_i|$. Bob then sends r_i iff $y_i = 1$. Notice that the randomness complexity now is at most $\sum_i r_i \leq \sum_i |S_i|$, which is just the size of the scheme. The communication complexity is now somewhat larger, but is bounded by twice the size.

We can also generalize the above theorem to the case of approximate secret sharing schemes. In particular, if we use an approximate secret sharing scheme in the second of the protocols above, we find that an ϵ-correct and δ-secure secret

[8] This protocol is not given in [GIKM00], but is a straightforward extension of their idea.

sharing scheme of size c for an indicator function f_I leads to an ϵ-correct and δ-secure CDS for the same function, using randomness complexity c. A similar observation holds for the protocol bounding the communication complexity. We collect these observations as the following remark.

6.2.16. Remark. Let $f_M : \{0,1\}^m \times \{0,1\}^m \to \{0,1\}$ be a monotone Boolean function and let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ be a projection of f_M, that is, $f(x,y) = f_M(g_1(x), g_2(y))$. Let **S** be a ϵ-correct and δ-secure secret sharing scheme realizing the access structure f_M, in which the total share size is c, and let s denote a secret (from the domain of **S**) which is known to all players. Then there exists an ϵ-correct and δ-secure CDS protocol disclosing s subject to the condition f with randomness c, and a (perhaps different) ϵ-correct and δ-secure protocol with communication complexity bounded above by c.

DRE gives PSM

See for example [CPS13] for the connection between DRE and PSM. We give a robust version of this connection as the next theorem.

6.2.17. Theorem. *Suppose that $f : X \times Y \to Z$ has an ϵ-correct and δ-secure decomposable randomized encoding using n_R bits of randomness, and n_M message bits. Then there is a ϵ-correct and δ-secure PSM protocol for f that uses the same amount of randomness and message bits.*

Proof:
Let the DRE for f be

$$\hat{f}(x,y;r) = (\hat{f}_X(x,r), \hat{f}_Y(y,r)). \tag{6.28}$$

To implement the PSM protocol, Alice prepares $\hat{f}_X(x,r)$ and sends this to the referee, while Bob prepares $\hat{f}_Y(y,r)$ and sends this to the referee. The referee then uses the decoder for the DRE to determine $f(x)$. Noticing that the conditions on the DRE and PSM are in fact exactly the same under these identifications, we have that the PSM is also ϵ-correct and δ-secure. □

Notice that a PSM for f also gives a randomized encoding for the function f, albeit one that is decomposable across a particular splitting of the input bits into $X \times Y$, and not necessarily decomposable bitwise, as required in the definition of a DRE.

PSM gives CDS

Next, we relate the PSM and CDS primitives. See for example [GIKM00, AR17].

6.2.18. Theorem. *Suppose that a ϵ-correct and δ-private PSM protocol exists for $f(x,y)$ using messages of at most n_M bits and no more than n_E shared random bits. Then a CDS protocol using n_M+1 bits of message and n_E random bits exists which is ϵ-correct and $O(\delta \log d_R)$ private, and hides one bit.*

Proof:
We wish to carry out the CDS task using the given PSM protocol. First, we note that by adding one bit of randomness we can assume s is held by both Alice and Bob. This is because of remark 6.2.4.

Next, we show that given the PSM protocol for f there is a similarly efficient PSM for the function $f(x,y) \wedge s$, with s held on both sides. To show this, first consider the case where $f(x,y)$ is a constant function. Then Alice and Bob can follow a fixed strategy (reveal s or not), and we are done. Thus we assume $f(x,y)$ is non-constant, and choose any input values for which it is 0 and label them (x_*, y_*). Run the PSM on inputs $x' = sx + (1-s)x_*$ and $y' = sy + (1-s)y_*$. Then notice that $f(x',y') = f(x,y) \wedge s$.

To see ϵ-correctness, we have the referee output the outcome of the modified PSM protocol as their guess for the secret s. Then their success probability conditioned on $f(x,y) = 1$ is exactly $1-\epsilon$, so the CDS protocol is $1-\epsilon$ correct.

Next, consider security. Let the distribution of values of $f(x,y)$ be F, the distribution of values of $f(x',y')$ be F', and the distributions of x' and y' be X' and Y', respectively. Security of the original PSM protocol implies

$$||Sim_{M|F'} - P_{M|X'Y'}||_1 \leq \delta. \tag{6.29}$$

Then notice that because $X'Y'$ are determined by XYS, we have $P_{M|X'Y'} = P_{M|XYS}$. Next, restrict to the distributions where $f(x,y) = 0$, leading to

$$||Sim_{M|F'=0} - P_{M|XYS}||_1 \leq \delta, \tag{6.30}$$

which is δ security of the CDS. □

PSM gives PSQM

Next, we prove that a protocol for PSM also gives a protocol for PSQM. This might seem trivial, since the quantum resources available in the PSQM can simulate the classical resources used in the PSM, but establishing security requires that we show that the classical security definition is strong enough to enforce the quantum security definition. As far as we are aware this is not written in the literature (but see [KN21] for the introduction of PSQM), but it is straightforward enough that we include it in this section.

6.2.19. Theorem. *Suppose we have a PSM protocol which is ϵ-correct and δ-secure. Then we can construct a PSQM protocol which is $2\sqrt{\epsilon}$ correct and δ-secure.*

Proof:
Correctness of the PSM protocol implies that there exists a decoder $Dec(m_0, m_1)$ such that

$$\forall (x, y) \in X \times Y \quad \Pr[Dec(m_0, m_1) = f(x, y)] \geq 1 - \epsilon, \tag{6.31}$$

where the probability is over choices of the random string r. In quantum notation, we have that the message system is described by the density matrix

$$\rho_M(x, y) = \sum_m p(m|x, y) \left|m\right\rangle\!\left\langle m\right|, \tag{6.32}$$

and can write the output of the decoder as

$$\boldsymbol{\mathcal{D}}_{M\to Z}(\rho_M(x, y)) = \sum_m p(m|x, y) \left|D(m)\right\rangle\!\left\langle D(m)\right|. \tag{6.33}$$

Then notice that

$$F(\boldsymbol{\mathcal{D}}_{M\to Z}(\rho_M(x, y)), |f_{xy}\rangle) = \sum_m p(m|x, y)| \left\langle D(m)\right\rangle f_{xy}|^2 \geq 1 - \epsilon, \tag{6.34}$$

where the last line follows because we see the fidelity is exactly the guessing probability, which is bounded from below by the classical correctness definition. Using the Fuchs-van de Graaf inequalities, we get

$$||\boldsymbol{\mathcal{D}}_{M\to Z}(\rho_M(x, y)) - \left|f_{xy}\right\rangle\!\left\langle f_{xy}\right| ||_1 \leq 2\sqrt{\epsilon}, \tag{6.35}$$

as needed.

Next recall security of the PSM means that there exists a simulator which takes in $f(x, y)$ and produces output distribution Sim on the message system such that

$$\forall (x, y) \in X \times Y, \quad ||Sim_{M|f(x,y)} - P_{M|xy}||_1 \leq \delta. \tag{6.36}$$

To obtain security of the PSQM, we need to upgrade this simulator to a quantum channel. In particular if the simulator is defined by the conditional probability distribution $p(m|f)$, define the Kraus operators

$$S_{m,f} = \sqrt{p(m|f)} \left|m\right\rangle\!\left\langle f\right|. \tag{6.37}$$

Calling the corresponding simulator channel $\boldsymbol{\mathcal{S}}$, we have that

$$||\boldsymbol{\mathcal{S}}(\left|f_{xy}\right\rangle\!\left\langle f_{xy}\right|) - \rho_M(x, y)||_1 = ||Sim_{M|f(x,y)} - P_{M|xy}||_1 \leq \delta, \tag{6.38}$$

so we have exactly δ security of the PSQM. □

GH gives f-routing

In [BFSS13], the following statement is shown.

6.2.20. Theorem. *The number of EPR pairs needed to implement an f-routing protocol for a function f is upper bounded by the garden-hose complexity of f.*

We will not reproduce a careful proof of this, but it is easy to see: each pipe in the garden hose protocol is replaced with an EPR pair in the f-routing strategy. Connecting pipes corresponds to measuring pairs of systems in the Bell basis. Doing so, the input system Q will end up recorded into the Hilbert space corresponding to spilling end of one of the pipes. Pauli corrections appear on this state, but the one round of communication in the f-routing strategy can be used to communicate all the measurement outcomes and then undo the corresponding corrections.

6.3 New relations among primitives

This section begins our study of the relationships among the cryptographic primitives introduced in Section 6.2.2.

6.3.1 Garden hose strategies give CDS

We point out that the garden hose game defines strategies for CDS.

6.3.1. Theorem. *The garden-hose complexity of a function $f(x, y)$ upper bounds the CDS cost,*

$$CDS(f) \leq GH(f). \tag{6.39}$$

Proof:
To show this, we construct a CDS protocol given a garden-hose protocol that uses a number of shared random bits equal to the number of pipes in the garden hose protocol.

Label the set of pipes used in the garden hose game p_i with the tap labeled p_0, the connections on Alice's side by $C_x = \{(p_i, p_j)\}$, and the connections on Bob's side by $C_y = \{(p_i, p_j)\}$. Note that because no hose can be connected to two pipes, each p_i appears in C_x at most once, and in C_y at most once. Correctness of the garden hose protocol means that for all (x, y), there is a path from the tap to the side labeled by $f(x, y)$.

To turn this into a CDS protocol, we proceed as follows. Each pipe p_i, $i > 0$, becomes a shared random bit held by Alice and Bob. The secret s corresponds to the tap p_0. For each connection in C_x, say (p_i, p_j), Alice computes $c_{ij} = p_i \oplus p_j$ and sends this to the referee. Bob does the same for each connection in C_y. Finally, Bob sends each shared random bit p_k not appearing in any connection in C_y to the referee. In contrast, Alice's unused random bits are kept hidden from the referee.

To see why this is correct and secure, consider the chain of connection bits $c_{i_k i_{k+1}} = p_{i_k} \oplus p_{i_{k+1}}$, where $p_{i_0} = s$ is the secret. If the chain is of length 0, this corresponds to an unconnected tap in the garden-hose picture, so that $f(x, y) = 0$ and the water spills on the left. In the CDS protocol, the secret, being an un-XOR'd bit, is not sent to the referee, so that the referee cannot learn the secret, as needed. Now suppose the chain has length > 1. Then $c_{i_0 i_1} = s \oplus p_{i_1}$ is sent to the referee, and no other bits which are computed from s are sent, so that the referee learns s if and only if they learn p_{i_1}. Continuing in this way down the chain of connection bits, we see that the referee learns s if and only if they learn p_{i_m}, the final random bit (corresponding to the final pipe in the waters path). But then p_{i_m} is not used to compute any other bits (by virtue of being at the end of the chain), and is sent if and only if it is unused on the right. But it is unused on the right if and only if the corresponding pipe spills on the right, which by our assumption of correctness of the garden hose strategy is if and only if $f(x, y) = 1$. □

6.3.2 Classical CDS gives quantum CDS

In this section, we observe that a classical CDS scheme immediately gives a quantum CDS scheme, via a use of the one-time pad.

6.3.2. THEOREM. *An ϵ-correct and δ-secure CDS protocol hiding $2n$ bits and using n_M bits of message and n_E bits of randomness gives a CDQS protocol which hides n qubits, is $2\sqrt{\epsilon}$ correct and δ-secure using n_M classical bits of message plus n qubits of message, and n_E classical bits of randomness.*

Proof:
Let the quantum system to be hidden in the CDQS be labeled Q. The basic idea is to use the CDS protocol to hide the key of a one-time pad applied to the system Q. The encoded system Q is sent to the referee. The one-time pad key, call it s, consists of $2 \log d_Q$ bits, which we choose independently and at random and hide in the CDS. The channel applied by Alice and Bob's combined actions is then

$$\boldsymbol{\mathcal{N}}^{xy}_{Q\to QM}(\cdot) = \frac{1}{2^{|s|}} \sum_{m,s} P^s_Q(\cdot) P^s_Q \otimes p_{m|xys} |m\rangle\langle m|_M . \tag{6.40}$$

We first study correctness. To do this, we recall that correctness of the classical CDS guarantees the existence of a decoder which produces an outcome which is equal to the secret value with probability $1 - \epsilon$. In quantum notation, we can describe this channel as

$$\mathrm{Dec}^{xy}_{M\to S}(\cdot) = \sum_{m,s'} p_{s'|mxy} |s'\rangle_S \langle m|_M \cdot |m\rangle_M \langle s'|_S . \tag{6.41}$$

The correctness condition for CDS states that, for $(x,y)\in f^{-1}(1)$ this produces a guess s' which agrees with the secret s, or more precisely,

$$F\left(\mathrm{Dec}^{xy}(\sum_m p_{m|sxy}\,|m\rangle\langle m|),|s\rangle\langle s|\right)\geq 1-\epsilon. \tag{6.42}$$

Relating this to the trace distance via the Fuchs-van de Graaf inequalities, this becomes,

$$\sum_{s'}\left(\sum_m p_{s'|mxy}p_{m|sxy}-\delta_{s'|s}\right)\leq 2\sqrt{\epsilon}, \tag{6.43}$$

where $\delta_{s|s'}=1$ if $s=s'$ and is zero otherwise. We will use this statement in establishing correctness of the CDQS.

Define the decoding channel for the CDQS by combining the classical decoder with a conditional application of $P_Q^{s'}$, then a trace over the register S holding the secret, so that our decoder is

$$\boldsymbol{\mathcal{D}}^{xy}_{QM\to Q}(\cdot)=\sum_{m,s'}p_{s'|mxy}P_Q^{s'}\otimes\langle m|_M\cdot P_Q^{s'}\otimes|m\rangle_M\,. \tag{6.44}$$

We need to bound the diamond norm $||\boldsymbol{\mathcal{D}}^{xy}_{QM\to Q}\circ\boldsymbol{\mathcal{N}}^{xy}_{Q\to M'}-\boldsymbol{\mathcal{I}}_{Q\to Q}||_\diamond$ from above. From the definition of the diamond norm and the channels $\boldsymbol{\mathcal{D}}^{xy}_{QM\to Q},\boldsymbol{\mathcal{N}}^{xy}_{Q\to M'}$, this is

$$\begin{aligned}
&||\boldsymbol{\mathcal{D}}_{QM\to Q}\circ\boldsymbol{\mathcal{N}}^{xy}_{Q\to M'}-\boldsymbol{\mathcal{I}}_{Q\to Q}||_\diamond\\
&\quad=\sup_n\max_{\Psi_{R_nQ}}||\frac{1}{2^{|s|}}\sum_{m,s,s'}p_{s'|mxy}p_{m|sxy}P_Q^{s+s'}\Psi_{R_nQ}P_Q^{s+s'}-\Psi_{R_nQ}||_1\\
&\quad=\sup_n\max_{\Psi_{R_nQ}}||\frac{1}{2^{|s|}}\sum_{m,s,s'}p_{s'|mxy}p_{m|sxy}P_Q^{s+s'}\Psi_{R_nQ}P_Q^{s+s'}\\
&\qquad\qquad-\frac{1}{2^{|s|}}\sum_{s,s'}\delta_{s|s'}P_Q^{s+s'}\Psi_{R_nQ}P_Q^{s+s'}||_1\\
&\quad=\frac{1}{2^{|s|}}\sum_{s,s'}(\sum_m p_{s'|mxy}p_{m|sxy}-\delta_{s'|s})\sup_n\max_{\Psi_{R_nQ}}||P_Q^{s+s'}\Psi_{R_nQ}P_Q^{s+s'}||_1\\
&\quad=\frac{1}{2^{|s|}}\sum_{s,s'}(\sum_m p_{s'|mxy}p_{m|sxy}-\delta_{s'|s})\\
&\quad\leq 2\sqrt{\epsilon}.
\end{aligned} \tag{6.45}$$

where we used Equation 6.43 in the last line, which recall held for all $(x,y)\in f^{-1}(1)$.

To establish security of the CDQS, we define the simulator channel as[9]

$$\boldsymbol{\mathcal{S}}^{xy}_{\varnothing\to MQ} = \frac{\mathcal{I}_Q}{d_Q} \otimes \sum_m \mathrm{Sim}_{M|xy} \left|m\right\rangle\!\left\langle m\right|_M . \tag{6.46}$$

We need to show $\boldsymbol{\mathcal{S}}^{xy}_{\varnothing\to MQ}\circ\mathrm{Tr}_Q$ is close to the channel 6.40 in diamond norm for all $(x,y)\in f^{-1}(0)$. This follows from security of the CDQS and a simple calculation. Start with the definition of the diamond norm,

$$\begin{aligned}
&||\boldsymbol{\mathcal{S}}^{xy}_{\varnothing\to MQ}\circ\mathrm{Tr}_Q - \boldsymbol{\mathcal{N}}_{Q\to QM}||_\diamond \\
&\qquad = \sup_n \max_{\Psi_{R_nQ}} ||\boldsymbol{\mathcal{S}}^{xy}_{\varnothing\to MQ}\circ\mathrm{Tr}_Q(\Psi_{R_nQ}) - \boldsymbol{\mathcal{N}}^{xy}_{Q\to QM}(\Psi_{R_nQ})||_1 \\
&\qquad = \sup_n \max_{\Psi_{R_nQ}} ||\Psi_{R_n}\otimes\frac{\mathcal{I}_Q}{d_Q}\otimes\sum_m \mathrm{Sim}_{m|xy}\left|m\right\rangle\!\left\langle m\right|_M \\
&\qquad\qquad\qquad - \frac{1}{2^{|s|}}\sum_{m,s} P^s_Q\Psi_{R_nQ}P^s_Q\otimes p_{m|xys}\left|m\right\rangle\!\left\langle m\right|_M ||_1 \\
&\qquad = \sup_n \max_{\Psi_{R_nQ}} ||\frac{1}{2^{|s|}}\sum_{m,s} P^s_Q\Psi_{R_nQ}P^s_Q\otimes \mathrm{Sim}_{m|xy}\left|m\right\rangle\!\left\langle m\right|_M \\
&\qquad\qquad\qquad - \frac{1}{2^{|s|}}\sum_{m,s} P^s_Q\Psi_{R_nQ}P^s_Q\otimes p_{m|xys}\left|m\right\rangle\!\left\langle m\right|_M ||_1,
\end{aligned} \tag{6.47}$$

where we used that

$$\Psi_{R_n}\otimes\frac{\mathcal{I}}{d_Q} = \frac{1}{2^{|s|}}\sum_s P^s_Q\Psi_{R_nQ}P^s_Q. \tag{6.48}$$

To bound our remaining expression, we take the sum over s out of the trace distance and find

$$\begin{aligned}
&||\boldsymbol{\mathcal{S}}^{xy}_{\varnothing\to MQ}\circ\mathrm{Tr}_Q - \boldsymbol{\mathcal{N}}_{Q\to QM}||_\diamond \\
&\quad = \frac{1}{2^{|s|}}\sum_s ||(P^s_Q\Psi_{R_nQ}P^s_Q)\otimes\left(\sum_m \mathrm{Sim}_{m|xy}\left|m\right\rangle\!\left\langle m\right|_M - \sum_m p_{m|xys}\left|m\right\rangle\!\left\langle m\right|_M\right)||_1 \\
&\quad = \frac{1}{2^{|s|}}\sum_s ||\mathrm{Sim}_{M|xys} - p_{M|xys}||_1 \leq \delta.
\end{aligned} \tag{6.49}$$

where the last inequality is coming from security of the classical CDS. □

[9] Notice a potential confusion around the notation here: M is the message system of the CDS, $M' = MQ$ is the message system of the CDQS.

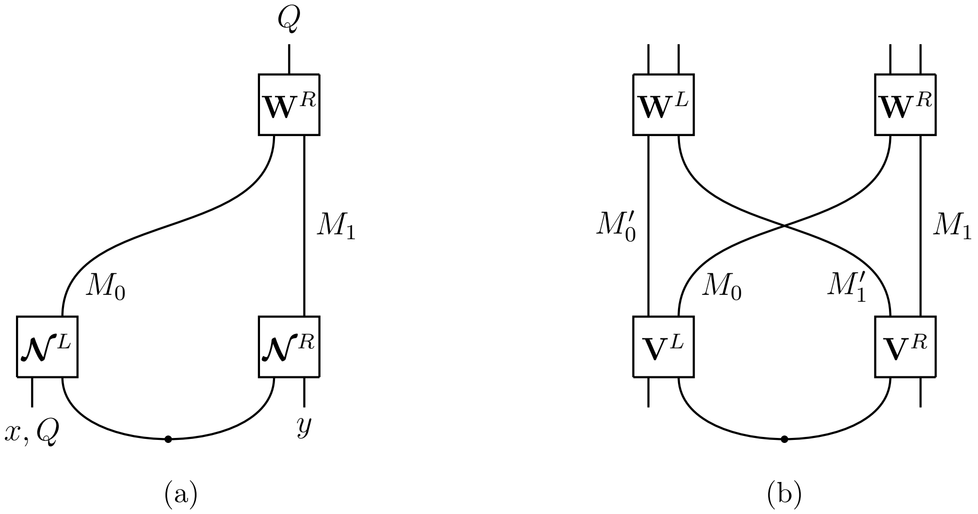


Figure 6.5: Corresponding CDQS (left) and f-routing (right) protocols. To define the CDQS protocol from the f-routing protocol, we have Alice and Bob trace out systems M_0' and M_1'. Systems M_0 and M_1 are sent to the referee rather than to Bob. To define the f-routing protocol from the CDQS, purify the local channels $\boldsymbol{\mathcal{N}}^L$ and $\boldsymbol{\mathcal{N}}^R$ to isometries $\mathbf{V}^L$ and $\mathbf{V}^R$. Send the original outputs of the channel to Bob on the right, and the purifying systems to Alice on the left. We adopt the notation $M = M_0M_1$ and $M' = M_0'M_1'$.

6.3.3 Equivalence of f-routing and CDQS

Our main claim of this section is that the CDQS and f-routing scenarios are equivalent, in that a protocol for one induces a protocol for the other using similar resources. The basic idea underlying the equivalence, and labeling of the various subsystems used in the proof, is illustrated in Figure 6.5.

6.3.3. Theorem. *A ϵ-correct f-routing protocol that routes n qubits implies the existence of a ϵ-correct and $\delta = 2\sqrt{\epsilon}$-secure CDQS protocol that hides n qubits using the same entangled resource state and the same message size. A ϵ-correct and δ-secure CDQS protocol hiding secret Q using a n_E qubit resource state n_M qubit messages implies the existence of a* $\max\{\epsilon, 2\sqrt{\delta}\}$*-correct f-routing protocol that routes system Q using n_E qubits of resource state and $4(n_M + n_E)$ qubits of message.*

Proof:
Begin by considering an f-routing protocol. Figure 6.5 establishes the subsystem labels we will use here. We will first show that an f-routing protocol is easily modified to construct a CDQS protocol. To do so, we send systems M_0 and M_1 that Bob would receive in the second round of the f-routing protocol to the referee of the CDQS protocol. Then, if $f(x, y) = 1$, ϵ-correctness of the f-routing scheme is immediately ϵ-correctness of the CDQS.

To show secrecy of the CDQS protocol, we first establish some notation. We label the channel realized by the first round operations of Alice and Bob $\boldsymbol{\mathcal{N}}_{Q\to MM'}$, and let $\mathbf{V}_{Q\to MM'E}$ be an isometric extension of this channel. By correctness in 0 instances of the f-routing scheme, we have that there exists a channel $\boldsymbol{\mathcal{D}}^{xy}_{M'\to Q}$ such that

$$\begin{aligned}&||\boldsymbol{\mathcal{D}}^{xy}_{M'\to Q}\circ[\mathrm{Tr}_M \circ\boldsymbol{\mathcal{N}}^{x,y}_{Q\to M'M}]-\boldsymbol{\mathcal{I}}_Q||_\diamond\\&\qquad=||\boldsymbol{\mathcal{D}}^{xy}_{M'\to Q}\circ[\mathrm{Tr}_{ME}(\mathbf{V}^{xy}_{Q\to MM'E}\cdot\mathbf{V}^{xy}_{Q\to MM'E})]-\boldsymbol{\mathcal{I}}_Q||_\diamond\leq\epsilon.\end{aligned}$$

Then the decoupling Theorem 6.2.2 tells us that there exists a completely depolarizing channel $\boldsymbol{\mathcal{S}}_{Q\to ME}$ such that

$$||\,\mathrm{Tr}_{M'}(\mathbf{V}^{xy}_{Q\to MM'E}\cdot\mathbf{V}^{xy}_{Q\to MM'E})-\boldsymbol{\mathcal{S}}^{xy}_{Q\to ME}||_\diamond\leq 2\sqrt{\epsilon}. \tag{6.50}$$

Adding a trace over part of the outputs of channels can only make the channels less distinguishable, and hence the diamond norm smaller, so that

$$||\,\mathrm{Tr}_{M'E}(\mathbf{V}^{xy}_{Q\to MM'E}\cdot\mathbf{V}^{xy}_{Q\to MM'E})-\boldsymbol{\mathcal{S}}^{xy}_{Q\to M}||_\diamond\leq 2\sqrt{\epsilon}, \tag{6.51}$$

but this is just

$$||\boldsymbol{\mathcal{N}}^{xy}_{Q\to M}-\boldsymbol{\mathcal{S}}^{xy}_{Q\to M}||_\diamond\leq 2\sqrt{\epsilon}, \tag{6.52}$$

which is exactly $2\sqrt{\epsilon}$-security of the CDQS. Note that the CDQS protocol defined by the f-routing protocol uses the same entangled resource state and no more communication.

Now suppose we have a CDQS protocol which is ϵ-correct and δ-secure. Then to build the f-routing protocol, purify the channels Alice and Bob perform to isometries, and send the original message systems of the CDQS to Bob and their purifications to Alice. Then, by ϵ-correctness of the CDQS protocol, we immediately have ϵ-correctness of the f-routing protocol when $f(x,y)=1$.

Next, consider the case where $f(x,y)=0$. Then security of the CDQS implies that there exists a simulator channel $\boldsymbol{\mathcal{S}}^{xy}_{\varnothing\to M}$ such that

$$||\boldsymbol{\mathcal{S}}^{xy}_{\varnothing\to M}\circ\mathrm{Tr}_Q-\boldsymbol{\mathcal{N}}^{xy}_{Q\to M}||_\diamond\leq\delta. \tag{6.53}$$

We will again apply the decoupling theorem. Notice that now, because of how we have defined the f-routing protocol, the map from Q to MM' is isometric, so $(\boldsymbol{\mathcal{N}}^{xy})^c_{Q\to M}=(\boldsymbol{\mathcal{N}}^{xy})_{Q\to M'}$. Then the decoupling theorem implies the existence of a decoding channel $\boldsymbol{\mathcal{D}}^{xy}_{M'\to Q}$ such that

$$||\boldsymbol{\mathcal{D}}^{xy}_{M'\to Q}\circ(\boldsymbol{\mathcal{N}}^{xy})^c_{Q\to M'}-\boldsymbol{\mathcal{I}}_Q||_\diamond\leq\sqrt{4||\boldsymbol{\mathcal{S}}^{xy}_{\varnothing\to M}\circ\mathrm{Tr}_Q-\boldsymbol{\mathcal{N}}^{xy}_{Q\to M}||}\leq 2\sqrt{\delta}, \tag{6.54}$$

which gives $2\sqrt{\delta}$ correctness on 0 instances. The protocol is then $\max\{2\sqrt{\delta},\epsilon\}$-correct.

To see how the communication in the resulting f-routing protocol is related to the communication in the original CDQS protocol, we can use that a channel $\boldsymbol{\mathcal{N}}_{A\to B}$ can always be purified by an isometry $\mathbf{V}_{A\to BC}$ where $d_C \leq d_A d_B$. Let CDQS have messages that each consist of at most n_M qubits, and use an n_E qubit resource system on systems LR. Then the most general possible protocol is defined by families of channels

$$\{\boldsymbol{\mathcal{N}}^x_{L\to M_0}\}, \quad \{\boldsymbol{\mathcal{N}}^y_{R\to M_1}\}, \tag{6.55}$$

applied on the left and right respectively. We define purifications of these,

$$\{\mathbf{V}^x_{L\to M_0 M_0'}\}, \quad \{\mathbf{V}^y_{R\to M_1 M_1'}\}. \tag{6.56}$$

We see that the message sizes are now at most $n_M + n_E$ qubits, so the total size of the communication is at most $4(n_M + n_E)$. The entangled resource system used in the f-routing protocol is identical to the one used in the CDQS. □

Explicit reconstruction procedure:

It is perhaps counterintuitive that the f-routing protocol built from the CDQS protocol succeeds in the case when $f(x,y) = 0$. This is implied by the general physics of decoupling as captured by Theorem 6.2.2, but for intuition we give a more explicit description in a special case here.

Let us suppose the CDQS protocol is perfectly correct, and works in the following way. Assume that the quantum secret is a single qubit and is stored in system Q. To hide the quantum state on Q, Alice applies the one-time pad using a classical string $s = (s_1, s_2)$ as key. Explicitly she has applied

$$|s_1, s_2\rangle_A |\psi\rangle_Q \to |s_1, s_2\rangle_A (i)^{s_1\cdot s_2} X^{s_1} Z^{s_2} |\psi\rangle_Q . \tag{6.57}$$

A message system M is sent to Bob, which reveals the key if and only if $f(x,y) = 1$. The system A must be sent to Alice on the left. The full state of the message systems then has the form

$$\frac{1}{2} \sum_{s_1,s_2,m_L,m_R} p(m_L, m_R|x,y,s) |m_L\rangle_{M'} |s_1, s_2\rangle_A (i)^{s_1\cdot s_2} X^{s_1} Z^{s_2} |\psi\rangle_Q |m_R\rangle_M . \tag{6.58}$$

Suppose we are in the case where $f(x,y) = 0$. Then, by security, the state on M is independent of s. We can trace it out and the M' system out and obtain the pure state

$$\frac{1}{2} \sum_{s_1,s_2} |s_1, s_2\rangle_A (i)^{s_1\cdot s_2} X^{s_1} Z^{s_2} |\psi\rangle_Q . \tag{6.59}$$

The claim is that Alice can recover the state on Q from the A system. To do this, she maps $|s_1, s_2\rangle$ to the Bell basis, obtaining

$$\frac{1}{2}(III + IXX + IZZ + IYY)\,|\Psi^+\rangle_{A_1A_2}\,|\psi\rangle_Q\,. \tag{6.60}$$

Then notice that

$$\frac{1}{2}(I_{A_2}I_Q + X_{A_2}X_Q + Z_{A_2}Z_Q + Y_{A_2}Y_Q) = SWAP_{A_2Q}, \tag{6.61}$$

so that mapping A_1A_2 into the Bell basis actually swaps the state on Q into A_2, so that Alice recovers the state on Q.

6.3.4 PSQM gives CDQS

Analogous to the observation that PSM gives CDS, we can also show that PSQM gives CDQS.

6.3.4. Theorem. *Suppose that a ϵ-correct and δ-private PSQM protocol exists for $f(x,y) \in \{0,1\}$ using messages of at most n_M bits and an entangled state of no more than n_E qubits. Then there exists a CDQS protocol hiding one qubit using n_M+1 bits of message and n_E qubits of entangled state, which is 2ϵ correct and δ private.*

Proof:
If the function $f(x,y)$ is constant then the CDQS protocol is trivial, so we assume without loss of generality that $f(x,y)$ is non-constant.

Given the PSQM protocol, we build a CDQS protocol as follows. We introduce two random shared bits, which we call $s=(s_1,s_2)$, which are held by Alice and Bob. Alice and Bob also pre-agree on a pair of inputs (x,y) where $f(x,y)=0$, call them (x_*,y_*), which exist because f is non-constant by assumption. Upon receiving inputs x,y Alice and Bob compute

$$\begin{aligned} x_i' &= s_i x + (1-s_i)x_*, \\ y_i' &= s_i y + (1-s_i)y_*, \end{aligned} \tag{6.62}$$

for $i=1,2$. They run the PSQM protocol for f on inputs (x_1,y_1) and (x_2,y_2) in parallel. Note that following the remark made after definition 6.2.8, the PSQM for $F(x,y,s)=(f(x_1,y_1), f(x_2,y_2))$ is 2ϵ correct and 2δ secure. Notice that

$$f(x_i',y_i') = f(x,y)\wedge s_i. \tag{6.63}$$

This means that by running the PSM for $f(x_i',y_i')$, the referee will learn s_i when $f(x,y)=1$. In the CDQS protocol, we have Alice act on the quantum secret Q with the one-time pad using the key $s=(s_1,s_2)$. Then the referee will be able to undo the one-time pad when $f(x,y)=1$ (and so they know s), but not otherwise.

Next, we establish correctness more carefully. First, note that the encoding channel for the CDQS defined by the above protocol is

$$\boldsymbol{\mathcal{N}}^{xy}_{Q\to MQ}(\cdot) = \frac{1}{2^{|s|}}\sum_s P^s_Q \cdot P^s_Q \otimes \rho_M(x,y,s), \tag{6.64}$$

where ρ_M is the state of the message systems prepared by the PSQM. Correctness of the CDQS requires we establish the existence of a channel which approximately inverts this. Note that by 2ϵ-correctness of the PSQM, we have that there exists a channel $\boldsymbol{\mathcal{V}}_{M\to Z}$ such that

$$||\boldsymbol{\mathcal{V}}_{M\to Z}(\rho_M(x,y,s)) - |F'\rangle\langle F'|_Z\,||_1 \leq 2\epsilon, \tag{6.65}$$

where we defined $F' = (f(x'_1,y'_1), f(x'_2,y'_2))$. We define our decoding channel to apply $\boldsymbol{\mathcal{V}}_{M\to Z}$, measure the Z system, then apply a Pauli conditioned on the outcome,

$$\boldsymbol{\mathcal{D}}_{MQ\to Q}(\cdot) = \sum_F P^F_Q \otimes \langle F|_Z\, \boldsymbol{\mathcal{V}}_{M\to Z}(\cdot)\,|F\rangle_Z \otimes P^F_Q. \tag{6.66}$$

We claim this is an approximate inverse to $\boldsymbol{\mathcal{N}}^{xy}_{Q\to MQ}$. Using the definitions of $\boldsymbol{\mathcal{N}}^{xy}_{Q\to MQ}$, $\boldsymbol{\mathcal{D}}_{MQ\to Q}$ and the diamond norm, we obtain the following.

$$\begin{aligned}||\boldsymbol{\mathcal{D}}_{MQ\to Q}\circ\boldsymbol{\mathcal{N}}^{xy}_{Q\to MQ} - \boldsymbol{\mathcal{I}}_Q||_\diamond &= \sup_n \max_{\Psi_{R_nQ}} ||\frac{1}{2^{|s|}}\sum_{s,F} P^{s+F}_Q \Psi_{R_nQ} P^{s+F}_Q \\ &\qquad \otimes \langle F|_Z\, \boldsymbol{\mathcal{V}}_{M\to \bar{M}Z}(\rho_M(x,y,s))\,|F\rangle_Z - \Psi_{R_nQ}||_1 \\ &\leq 2\epsilon + \sup_n \max_{\Psi_{R_nQ}} ||\frac{1}{2^{|s|}}\sum_{s,F} P^{s+F}_Q \Psi_{R_nQ} P^{s+F}_Q \otimes \langle F|_Z\,|F'\rangle\langle F'|\,|F\rangle_Z - \Psi_{R_nQ}||_1.\end{aligned}$$

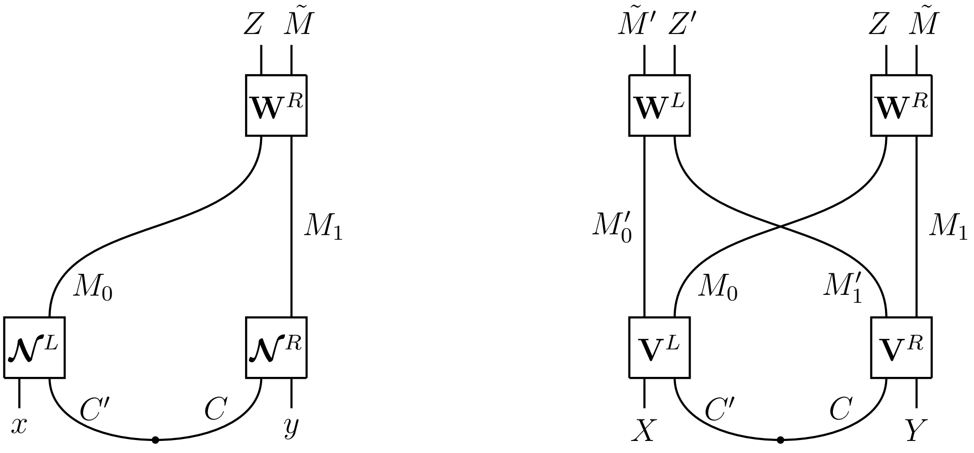
where we replaced the $\boldsymbol{\mathcal{V}}_{M\to\bar{M}Z}(\rho_M(x,y))$ with $|F'\rangle\langle F'|$ at the expense of the added 2ϵ, which is justified by Equation 6.65. Continuing, we can see that the second term is actually zero, since (from Equation 6.63) F' is just s when $f(x_1,y_1) = f(x_2,y_2) = 1$, which removes the Pauli's and so the full diamond norm is bounded by 2ϵ.

Next, we study the security of the CDQS protocol. Recall that security of the PSQM implies that there exists a channel $\boldsymbol{\mathcal{S}}_{Z\to M}$ such that

$$||\rho_M(x,y,s) - \boldsymbol{\mathcal{S}}_{Z\to M}(|F'\rangle\langle F'|)||_1 \leq \delta. \tag{6.67}$$

In the definition of security for CDQS, we need to show the existence of a channel $\boldsymbol{\mathcal{S}}'^{x,y}_{\varnothing\to M}$ such that $\boldsymbol{\mathcal{S}}'^{x,y}_{\varnothing\to M}\circ \mathrm{Tr}_Q$ is close to the action of the protocol $\boldsymbol{\mathcal{N}}^{xy}_{Q\to MQ}$. We define

$$\boldsymbol{\mathcal{S}}'^{x,y}_{\varnothing\to MQ} = \boldsymbol{\mathcal{S}}_{Z\to M}(|F'\rangle\langle F'|) \otimes \frac{\mathcal{I}_Q}{d_Q}, \tag{6.68}$$



(a) (b)

Figure 6.6: Corresponding PSQM (left) and CFE (right) protocols, with labelings of the subsystems involved shown.

then consider,

$$
\begin{aligned}
&||\boldsymbol{\mathcal{S}}'^{x,y}_{\varnothing\to MQ}\circ \mathrm{Tr}_Q - \boldsymbol{\mathcal{N}}^{xy}_{Q\to MQ}||_\diamond \\
&\qquad = \sup_n \max_{\Psi_{R_nQ}} ||\frac{\mathcal{I}_Q}{d_Q}\otimes \boldsymbol{\mathcal{S}}_{Z\to M}(|F'\rangle\langle F'|) \\
&\qquad\qquad - \frac{1}{2^{|s|}}\sum_s P^s_Q \Psi^{R_nQ} P^s_Q \otimes \rho_M(x,y,s)||_1 \\
&\qquad \leq \sup_n \max_{\Psi_{R_nQ}} ||\frac{\mathcal{I}_Q}{d_Q}\otimes \boldsymbol{\mathcal{S}}_{Z\to M}(|F'\rangle\langle F'|) \\
&\qquad\qquad - \frac{1}{2^{|s|}}\sum_s P^s_Q \Psi^{R_nQ} P^s_Q \otimes \boldsymbol{\mathcal{S}}_{Z\to M}(|F'\rangle\langle F'|)||_1 + \delta \\
&\qquad = \delta,
\end{aligned}
$$

where we used 6.67 in the inequality. This is δ-security of the CDQS. □

6.3.5 CFE gives PSQM and weak converse

Finally, we relate coherent function evaluation to PSQM. Note that the relationship is only that good CFE protocols give good PSQM protocols, although a weak converse also exists, as we describe.

6.3.5. Theorem. *A ϵ-correct CFE protocol for the function f using n_E EPR pairs and messages of n_M qubits implies the existence of a ϵ-correct and $\sqrt{\epsilon}$-secure PSQM protocol for the same function, using n_E EPR pairs and no more than n_M message qubits.*

Proof:
We define the PSQM protocol from the CFE protocol as follows. The PSQM protocol uses the same resource state as the CFE, Alice applies the bottom left operation of the CFE, Bob applies the bottom right operation of the CFE, and they send the systems that would reach the top right of the CFE protocol to the referee, which we call the M systems. To produce their output, the referee applies the top-right operation from the CFE. See Figure 6.6 for labels of the relevant subsystems.

Correctness of the CFE protocol means that we have

$$||\mathbf{F}(\cdot)\mathbf{F}^\dagger - \boldsymbol{\mathcal{N}}_{XY\to Z'Z}||_\diamond \leq \epsilon, \tag{6.69}$$

where $\boldsymbol{\mathcal{N}}$ is the channel applied by our CFE protocol and $\mathbf{F}$ denotes the CFE isometry to be implemented. Applying these channels to the input $|x\rangle_X |y\rangle_Y$ and using the definition of the diamond norm distance, we obtain

$$|| \, |xy\rangle\langle xy|_{Z'} \otimes |f_{xy}\rangle\langle f_{xy}|_Z - \rho_{Z'Z}(x,y)||_1 \leq \epsilon. \tag{6.70}$$

Tracing out the Z' system and using that the one-norm distance decreases under the partial trace, we obtain ϵ-correctness of the PSQM.

Next, we study the security of the PSQM. We start again from the correctness of the CFE protocol. To simplify our notation, we define the channels (see also figure 6.6)

$$\begin{aligned}
\boldsymbol{\mathcal{F}}_{XY\to Z'Z}(\cdot) &= \mathbf{F}(\cdot)\mathbf{F}^\dagger, \\
\boldsymbol{\mathcal{W}}^L_{M\to Z\tilde{M}}(\cdot) &= \mathbf{W}^R_{M\to Z\tilde{M}}(\cdot)(\mathbf{W}^R_{M\to Z\tilde{M}})^\dagger \\
\boldsymbol{\mathcal{W}}^R_{M'\to Z'\tilde{M}'}(\cdot) &= \mathbf{W}^L_{M'\to Z'\tilde{M}'}(\cdot)(\mathbf{W}^L_{M'\to Z'\tilde{M}'})^\dagger \\
\boldsymbol{\mathcal{W}}_{MM'\to Z\tilde{M}Z'\tilde{M}'} &= \boldsymbol{\mathcal{W}}^L_{M'\to Z\tilde{M}'} \otimes \boldsymbol{\mathcal{W}}^R_{M\to Z\tilde{M}} \\
\boldsymbol{\mathcal{V}}_{XY\to MM'}(\cdot) &= \\
&\mathbf{V}^R_{YC\to M_1'M_1} \otimes \mathbf{V}^L_{XC'\to M_0M_0'}(\cdot \otimes \Psi_{CC'})(\mathbf{V}^R_{YC\to M_1'M_1} \otimes \mathbf{V}^L_{XC'\to M_0M_0'})^\dagger.
\end{aligned}$$

Then we note that the CFE protocol can be decomposed into two steps, and rewrite the statement of correctness,

$$||\boldsymbol{\mathcal{F}}_{XY\to Z'Z}(\cdot) - \mathrm{Tr}_{\tilde{M}\tilde{M}'}(\boldsymbol{\mathcal{W}}_{MM'\to Z\tilde{M}Z'\tilde{M}'}) \circ (\boldsymbol{\mathcal{V}}_{XY\to MM'})||_\diamond \leq \epsilon.$$

Next, we will use that Stinespring dilations of channels can be chosen to be close if the initial channels are close [KSW08a]. In particular, we have

$$\frac{||T_1 - T_2||_\diamond}{\sqrt{||T_1||_\diamond} + \sqrt{||T_2||_\diamond}} \leq \inf_{V_1,V_2} ||V_1 - V_2||_{op} \leq \sqrt{||T_1 - T_2||_\diamond}, \tag{6.71}$$

where the infimum is over all dilations V_i of T_i. Noting that $\boldsymbol{\mathcal{F}}$ is already isometric, we have that its dilations must consist of adding a state preparation channel, which we label $\mathcal{P}_{\emptyset\to E}$. Furthermore, all dilations are related by a partial isometry on the auxiliary space, so the dilations of the $\mathrm{Tr}_{\tilde{M}\tilde{M}'}\,\mathcal{W}\circ\mathcal{V}$ channel can be written in the form

$$\mathcal{U}_{XY\to ZZ'E} = \mathcal{I}_{\tilde{M}\tilde{M}'\to E}\circ(\mathcal{W}_{MM'\to Z\tilde{M}Z'\tilde{M}'})\circ(\mathcal{V}_{XY\to MM'}). \tag{6.72}$$

Then using the upper bound in 6.71, we have

$$||\mathcal{F}_{XY\to Z'Z}\otimes\mathcal{P}_{\emptyset\to E} - \mathcal{I}_{\tilde{M}\tilde{M}'\to E}\circ\mathcal{W}_{MM'\to Z\tilde{M}Z'\tilde{M}'}\circ\mathcal{V}_{XY\to MM'}||_{op}\leq\sqrt{\epsilon}. \tag{6.73}$$

Next, we will exploit the lower bound in 6.71 to translate this to an upper bound on the diamond norm of these isometries. To do this, note that from 6.71 we have

$$\frac{||V_1-V_2||_\diamond}{\sqrt{||V_1||_\diamond}+\sqrt{||V_2||_\diamond}}\leq\inf_{P_1,P_2}||V_1\otimes P_1 - V_2\otimes P_2||_{op}\leq||V_1-V_2||_{op}. \tag{6.74}$$

Using this in Equation 6.73, we obtain

$$||\mathcal{F}_{XY\to Z'Z}\otimes\mathcal{P}_{\emptyset\to E} - \mathcal{I}_{\tilde{M}\tilde{M}'\to E}\circ\mathcal{W}_{MM'\to Z\tilde{M}Z'\tilde{M}'}\circ\mathcal{V}_{XY\to MM'}||_\diamond\leq 2\sqrt{\epsilon}. \tag{6.75}$$

Next, apply $\mathcal{I}^\dagger_{\tilde{M}\tilde{M}'\to E}$ to both terms, which cannot increase the diamond norm, and obtain

$$||\mathcal{F}_{XY\to Z'Z}\otimes\mathcal{P}_{\emptyset\to\tilde{M}\tilde{M}'} - \mathcal{W}_{MM'\to Z\tilde{M}Z'\tilde{M}'}\circ\mathcal{V}_{XY\to MM'}||_\diamond\leq 2\sqrt{\epsilon}. \tag{6.76}$$

Apply $\mathcal{W}^\dagger_{MM'\to Z\tilde{M}Z'\tilde{M}'}$ to both terms to obtain

$$||\mathcal{W}^\dagger_{MM'\to Z\tilde{M}Z'\tilde{M}'}\circ(\mathcal{F}_{XY\to Z'Z}\otimes\mathcal{P}_{\emptyset\to\tilde{M}\tilde{M}'}) - \mathcal{V}_{XY\to MM'}||_\diamond\leq 2\sqrt{\epsilon}. \tag{6.77}$$

Then, apply these channels to the input $|xy\rangle_{XY}$ and call the output of the protocol on the M system $\rho_M(x,y)$, and trace out the $\tilde{M}'$ system,

$$||\,\mathrm{Tr}_{M'}\,\mathcal{W}^\dagger_{MM'\to Z\tilde{M}Z'\tilde{M}'}\circ\mathcal{F}_{XY\to Z'Z}(|xy\rangle\langle xy|)\otimes\psi_{\tilde{M}\tilde{M}'} - \rho_M(x,y)||_1\leq 2\sqrt{\epsilon}.$$

Simplifying the state on the left using

$$\begin{aligned}\mathcal{W}_{MM'\to Z\tilde{M}Z'\tilde{M}'} &= \mathcal{W}^L_{M\to Z\tilde{M}}\otimes\mathcal{W}^R_{M'\to Z'\tilde{M}'}\\ \mathcal{F}_{XY\to Z'Z}(|xy\rangle\langle xy|) &= |f_{xy}\rangle\langle f_{xy}|_Z\otimes|xy\rangle\langle xy|_{Z'}\,,\end{aligned} \tag{6.78}$$

we obtain

$$||\mathcal{W}^{R\dagger}_{M\to\tilde{M}Z}(|f_{xy}\rangle\langle f_{xy}|\otimes\sigma_{\tilde{M}}) - \rho_M(x,y)||_1\leq 2\sqrt{\epsilon}, \tag{6.79}$$

which is $2\sqrt{\epsilon}$ security of the PSQM protocol, where $\mathcal{W}^{R\dagger}_{M\to\tilde{M}Z}$ along with the state preparation of $\sigma_{\tilde{M}}$ defines the simulator channel. □

Next, we give a weak converse to the above theorem, which shows that a good PSQM protocol implies the existence of a CFE protocol that succeeds with constant probability when acted on the maximally entangled state. Note that this falls short of bounding the diamond norm. We show this only in the exact setting, though a robust version might also exist. We are also limited to the case where the function outputs a single bit.

6.3.6. Theorem. *Suppose there exists a perfectly correct and perfectly secure PSQM protocol for the function $f : X \times Y \to Z$ with $Z \in \{0,1\}$ using n_M bits of communication and n_E qubits of entangled resource system. Then there is a CFE protocol that implements a channel $\tilde{\boldsymbol{\mathcal{V}}}^f_{XY\to Z'Z}$ such that*

$$F(\tilde{\boldsymbol{\mathcal{V}}}^f_{XY\to Z'Z}(\Psi^+_{RXY}), \mathbf{V}^f_{XY\to Z'Z}(\Psi^+)_{RXY}(\mathbf{V}^f_{XY\to Z'Z})^\dagger) \geq \frac{1}{2}, \tag{6.80}$$

and which uses n_E qubits of entangled resource state and $n_M + n_E + 2n$ qubits of communication, where n is the input size.

Proof:
By security of the PSQM protocol, we have that when given input $|xy\rangle$ the protocol produces a reduced state $\rho_M(x,y)$ of the form

$$\rho_M(x,y) = \boldsymbol{\mathcal{S}}_{Z\to M}(|f_{xy}\rangle\langle f_{xy}|) = \sigma_M^{f_{xy}}. \tag{6.81}$$

As part of the CFE protocol that we define, we make a copy of the inputs $|x\rangle_X |y\rangle_Y$ and send this copy in a system labeled Z' to the left. The overall state of the message system then is,

$$|xy\rangle\langle xy|_{Z'} \otimes \sigma_M^{f_{xy}}. \tag{6.82}$$

Now consider purifying the channels used in the PSQM protocol, and sending the purifying systems (call them $\tilde{M}'$) to the left. Then the message system becomes

$$|\Psi_{xy}\rangle_{Z'\tilde{M}'M} = |xy\rangle_{Z'} \sum_k \sqrt{\lambda^k_{f_{xy}}}\, |\psi^k_{f_{xy}}\rangle_{\tilde{M}'} |\psi^k_{f_{xy}}\rangle_M , \tag{6.83}$$

where we used that the reduced density matrix on M depends only on f_{xy} to enforce that the Schmidt coefficients and Schmidt vectors on M can depend only on f_{xy}.

Next, we consider adding to the protocol a unitary

$$\mathbf{U}_{Z'\tilde{M}'} = \sum_{x,y,k} \alpha_{f_{xy}} |xy\rangle\langle xy|_{Z'} \otimes |k\rangle\langle \psi^k_{f_{xy}}|_{\tilde{M}'} , \tag{6.84}$$

where the $\alpha_{f_{xy}}$ are phases, $|\alpha_{f_{xy}}|^2 = 1$. We will later determine how to choose these phases. This means we produce the state

$$\mathbf{U}_{Z'\tilde{M}'} |\Psi_{xy}\rangle_{Z'\tilde{M}'M} = |xy\rangle_{Z'} \sum_k \alpha_{f_{xy}} \sqrt{\lambda^k_{f_{xy}}}\, |k\rangle_{\tilde{M}'} |\psi^k_{f_{xy}}\rangle_M . \tag{6.85}$$

We would like to exploit the correctness of the PSQM protocol to show this state can be made, using an operation on M, to have large overlap with the correct output for the CFE protocol, which here is $|xy\rangle_{Z'}|f_{xy}\rangle_Z$. Looking at the reduced state on M again, we have

$$\sigma_M = \sum_k \lambda^k_{f_{xy}} |\psi^k_{f_{xy}}\rangle\langle\psi^k_{f_{xy}}|_M \,. \tag{6.86}$$

From correctness we have that there exists a map $\mathbf{V}_{M\to\tilde{M}Z}$ such that

$$\sum_k \lambda^k_{f_{xy}} \mathrm{Tr}_{\tilde{M}}(\mathbf{V}_{M\to\tilde{M}Z} |\psi^k_{f_{xy}}\rangle\langle\psi^k_{f_{xy}}|_M \mathbf{V}^\dagger_{M\to\tilde{M}Z}) = |f_{xy}\rangle\langle f_{xy}|_Z \,, \tag{6.87}$$

which is only solved if, for all k,

$$\mathbf{V}_{M\to\tilde{M}Z} |\psi^k_{f_{xy}}\rangle_M = \beta^k_{f_{xy}} |f_{xy}\rangle_Z |\tilde{\psi}^k_{f_{xy}}\rangle_{\tilde{M}} \,. \tag{6.88}$$

with $\beta^k_{f_{xy}}$ being pure phases, $|\beta^k_{f_{xy}}|^2 = 1$. Returning to the form 6.85, we can now add an application of $\mathbf{V}_{M\to Z\tilde{M}}$ as the top-right element of our CFE protocol and we see that we produce the state

$$\begin{aligned}\mathbf{V}_{M\to\tilde{M}Z}\mathbf{U}_{Z'\tilde{M}'} |\Psi_{xy}\rangle_{Z'\tilde{M}'M} &= \alpha_{f_{xy}} |xy\rangle_{Z'} |f_{xy}\rangle_Z \sum_k \beta^k_{f_{xy}} \sqrt{\lambda^k_{f_{xy}}} |k\rangle_{\tilde{M}'} |\tilde{\psi}^k_{f_{xy}}\rangle_{\tilde{M}} \\ &= \alpha_{f_{xy}} |xy\rangle_{Z'} |f_{xy}\rangle_Z |\Phi_{f_{xy}}\rangle_{\tilde{M}'\tilde{M}} \,. \end{aligned} \tag{6.89}$$

By linearity, if we perform the same protocol on the state $|\Psi^+\rangle_{RXY}$ we produce the output

$$|\Psi'_f\rangle_{RZ'Z\tilde{M}'\tilde{M}} = \frac{1}{\sqrt{d_R}} \sum_{xy} \alpha_{f_{xy}} |xy\rangle_R |xy\rangle_{Z'} |f_{xy}\rangle_Z |\Phi_{f_{xy}}\rangle_{\tilde{M}'\tilde{M}} \,. \tag{6.90}$$

We would like to compute the fidelity of the state produced by our protocol on $RZ'Z$ with the correct one when acted on the maximally entangled state. Note that the correct output state would be

$$|\Psi_f\rangle = \frac{1}{\sqrt{d_R}} \sum_{xy} |xy\rangle_R |xy\rangle_{Z'} |f_{xy}\rangle_Z \,. \tag{6.91}$$

Computing the fidelity of this with the partial state of $|\Psi'_f\rangle$ on $RZ'Z$, we find

$$F(\Psi_f, \sigma) = \langle\Psi_f| \sigma_{RZ'Z} |\Psi_f\rangle = \frac{1}{d_R^2} \sum_{xy,x'y'} \alpha^*_{f_{xy}} \alpha_{f_{x'y'}} \langle\Phi_{f_{xy}}\rangle \, \Phi_{f_{x'y'}} . \tag{6.92}$$

Now, we can see how we should choose the phases $\alpha_{f_{xy}}$ that enter through our choice of the unitary $\mathbf{U}$. We should choose the phases such that this sum is lower bounded, which we can achieve by setting

$$\begin{aligned}\alpha_0 &= 1, \\ \alpha_1 &= \frac{\langle\Phi_1\rangle\,\Phi_0}{|\langle\Phi_1\rangle\,\Phi_0|}. \end{aligned} \tag{6.93}$$

This ensures that the terms in the sum where $f_{xy} \neq f_{x'y'}$ are positive, so we bound them below by zero and obtain

$$\begin{aligned} F(\Psi_f, \sigma) &\geq \frac{1}{d_R^2}\left(\sum_{f_{xy}} \sum_{\substack{xyx'y': \\ f_{xy}=f_{x'y'}}} 1\right) \\ &= \frac{1}{d_R^2}\sum_{f_{xy}} N_{f_{xy}}^2 \geq \frac{1}{2}, \end{aligned} \tag{6.94}$$

where N_m is the number of inputs that lead to $f_{xy} = m$. This gives the needed lower bound.

To understand the resource consumption of the protocol constructed above, note that it uses the same resource state, and so n_E qubits of the entangled resource system still exist. Considering the message sizes, notice that in purifying the channels used in the PSQM protocol we need no more than $n_E + n$ qubits in the auxiliary system, and then we added an additional copy of the input sent to the left, so we use at most $n_E + 2n + n_M$ qubit messages. □

6.4 Complexity of efficiently achievable functions

The set of implications summarized in Figure 6.3 imply efficient protocols for one primitive imply efficient protocols for many others. In this section, we briefly summarize what is known about the efficiently achievable functions in various settings, and how they compare across various primitives.

6.4.1 Relevant complexity measures

An important model of computation we will discuss is the modulo-p branching program. These are computational models with close relationships to various non-uniform complexity classes sitting inside of NC.

6.4.1. Definition. A **branching program** is a tuple $\boldsymbol{\mathcal{BP}} = (G, \phi, s, t_0, t_1)$ where,

- $G = (V, E)$ is a directed acyclic graph,
- ϕ is a function from edges in E to either a value "yes" or a tuple (b, i) for b a bit and $i \in \{1, ..., n\}$,
- s, t_0, t_1 are vertices from V.

Given an n-bit string x as input, the branching program specifies a subgraph of G labeled G_x according to the following rule. If for $e \in E$ we have $\phi(e) = (b, j)$ with $x_j = b$, or if $\phi(e) =$"yes", then e is included in G_x. We define a function acc(x) as the number of paths $s \to t_1$ in the graph G_x, and a function rej(x) as the number of paths from s to t_0 in G_x.

6.4.2. Definition. The size of a branching program is defined as the number of vertices in V. We label the minimal-sized branching program computing f as $BP(f)$.

We say a branching program is deterministic if the out degree of every vertex in every G_x is at most 1, and non-deterministic otherwise. The function $f(x)$ computed by a deterministic or non-deterministic branching program is defined such that $f(x) = 1$ iff $acc(x) > 0$. A **Boolean modulo-p branching program** computes the function $f(x)$ defined such that $f(x) = 1$ iff $acc(x) \neq 0 \ mod \ p$. We label the minimal size of a mod p branching program computing f by $BP_p(f)$.

The class of functions with polynomial sized modulo-p branching programs is defined below.

6.4.3. Definition. The complexity class Mod$_pL/poly$ is defined as those Boolean function families $\{f_n\}$ which have polynomial (in n) sized modulo-p branching programs.

The uniform complexity class Mod$_pL$ can be defined similarly in terms of log-space uniform branching programs, or given an equivalent definition in terms of Turing machines [BDHM92]. Another relevant complexity class, also based on branching programs, is the following.

6.4.4. Definition. The class $C_{=}L/poly$ (read as "equality L") is defined as those Boolean function families $\{f_n\}$ which can be decided in the following way. We consider a branching program of polynomial (in n) size. If $acc(x) = rej(x)$, output 1 and otherwise output 0.

A related notion of complexity that we will need is that of a **span program**, defined initially in [KW93].

6.4.5. Definition. A **span program** over a field $\mathbb{Z}_p$ consists of a triple $S = (M, \phi, \mathbf{t})$, where M is a $d \times e$ matrix with entries in $\mathbb{Z}_p$, ϕ is a map from rows of M, labeled r_i, to pairs (k, ε_i), with $k \in \{1, ..., n\}$ and $\varepsilon_i \in \{0, 1\}$, and $\mathbf{t}$ is a non-zero vector of length e with entries in $\mathbb{Z}_p$. A span program S computes a function $f : \{0,1\}^n \to \{0,1\}$ as follows. Given an input string z of n bits, if the vector $\mathbf{t}$ is in span$(\{r_i : \exists j, \phi(r_i) = (j, z_j)\})$, then output 1. Otherwise, output 0.

6.4.6. Definition. The **size** of a span program is defined as d, the number of rows in M. We denote the minimal size of a span program over $\mathbb{Z}_p$ that computes f by $SP_p(f)$.

The size of a span program that computes $\{f_n\}$ and of a branching program computing the same function family are related by the following theorem, noted in [KW93] to follow from techniques in [BDHM92].

6.4.7. THEOREM. *For every prime p, Mod_pL consists of those function families with polynomial-sized span programs over $\mathbb{Z}_p$.*

Thus, the size of span programs and of arithmetic branching programs are related polynomially, and in fact [BG99][10]

$$SP_p(f) \leq 2BP_p(f). \tag{6.95}$$

We will never be interested in constant factor differences, so we can take that span programs are always smaller than modulo-p branching programs.

An important notion for us will be that of *pre-processing*. We will consider functions $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$, and we are interested in the complexity of computing $f(x, y)$ after allowing for arbitrary functions to be applied to x and y separately. We give the following definition.

6.4.8. DEFINITION. A **local part** of $f(x, y) : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ is any function F such that there exist functions $\alpha : \{0,1\}^n \to \{0,1\}^{m_\alpha}$, $\beta : \{0,1\}^n \to \{0,1\}^{m_\beta}$ such that $f(x, y) = F(\alpha(x), \beta(y))$.

We say that the complexity after pre-processing (with respect to some measure of complexity) of a function $f(x, y)$ is the minimal complexity of any local part of $f(x, y)$. More concretely, for span and branching program size, we define the following pre-processed complexity measures.

6.4.9. DEFINITION. The **pre-processed branching program complexity** is defined as

$$BP_{p,(2)}(f) = \min_{F,\alpha,\beta}\{BP_p(F) : f(x, y) = F(\alpha(x), \beta(y))\}, \tag{6.96}$$

6.4.10. DEFINITION. The **pre-processed span program complexity** is defined as

$$SP_{p,(2)}(f) = \min_{F,\alpha,\beta}\{SP_p(F) : f(x, y) = F(\alpha(x), \beta(y))\}, \tag{6.97}$$

The pre-processed branching and span program complexities are related polynomially, because the non pre-processed complexities are.

We define the following pre-processed complexity classes.

[10] Note that this statement is given in [BG99] in terms of *arithmetic branching programs*, which are a generalization of modulo-p branching programs (and so are at least as powerful).

6.4.11. Definition. The complexity class $Mod_kL_{(2)}$ is defined as those functions $f : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$ with a local part that can be computed with a polynomial size (in n) modulo-p branching program.

6.4.12. Definition. The complexity class $C_{=}L_{(2)}$ is defined as those functions $f : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$ with a local part that can be computed according to the following procedure. We consider a branching program of polynomial (in n) size. If $acc(x) = rej(x)$, output 1 and otherwise output 0.

We can analogously define the complexity class $P_{(2)}$ as those families of function families which have a poly-time computable local part.

6.4.2 Efficiency of protocols for PSM, CDS, and related primitives

PSM and PSQM protocols

The largest class of functions for which efficient PSM protocols have been constructed are those with polynomial-sized modulo-p branching programs. The following theorem was proven in [IK97].

6.4.13. Theorem. ***[IK '97]*** *Let p be a prime, and let $\boldsymbol{\mathcal{BP}} = (G, \phi, s, t_0, t_1)$ be a Boolean modulo-p branching program of size $a(n)$ computing a local part of f. Then there exists a PSM protocol for f with randomness complexity and communication complexity both $O(a(n)^2 \log p)$.*

Note that the original statement of this theorem considers f rather than its local part, but the extension is trivial. An immediate consequence of this theorem, along with the implications summarized in Figure 6.3, is that CDS, PSQM, CDQS, and f-routing can all be achieved with the randomness and communication complexity given in the same way, up to constant factor overheads.

To better understand the implications of this theorem, it is helpful to understand which complexity classes can be achieved efficiently. Fixing p, those functions with polynomial-sized branching programs are exactly the class Mod_pL. Running the PSM protocol on the local part, we can therefore achieve the class $\text{Mod}_pL_{(2)}$ efficiently as a PSM. We can also choose p adaptively and, doing so, achieve the class $C_{=}L_{(2)}$. This is shown in [IK97]. It is also interesting to find a complexity class that contains all the functions where $(\log p)BP_p(f)$ can be made polynomial. The smallest class that we can show contains all such functions is $L^{\#L}$, which we state as the following remark.

6.4.14. Remark. Every function family $\{f_n\}$ for which $(\log p) \cdot BP_p(f_n)$ is polynomial in n for some choice of p is contained in the class $L^{\#L}/poly$.

Proof:
By assumption, there is a polynomial-sized branching program, call it BP and denote its size by s, whose number of accepting paths counted mod p is non-zero if $f(x) = 1$, and 0 otherwise. Further, the choice of p needed must have $\log p$ be polynomial. Our algorithm for computing f in $L^{\#L}$ is as follows. We take our advice string to be a description of the branching program BP. We give BP along with the input x to the $\#L$ oracle, and it will return the number of accepting paths of this program, call it N. Notice that $N < 2^s$, since there must be no more accepting paths then there are subsets of vertices in BP. This means that the output of the oracle consists of at most a polynomial-sized string. We then subtract p from N repeatedly until it reaches a number less than p. Since p also consists of a polynomial number of bits, this can be done in log space. □

To relate $L^{\#L}$ to more familiar classes, we can note that it is contained inside of DET which is in turn contained inside of NC, where NC is the class of functions computed by poly-logarithmic depth circuits.

Notice that from Theorem 6.2.19 the result of Theorem 6.4.13 carries over immediately to the setting of PSQM. We move on to understand the implications of Theorem 6.4.13 for the CDS, CDQS, and f-routing primitives below.

CDS protocols

From Theorem 6.4.13 and because PSM protocols give CDS protocols (see Theorem 6.2.18), we obtain the following corollary.

6.4.15. Theorem. *Let p be a prime, and let $\boldsymbol{\mathcal{BP}} = (G, \phi, s, t_0, t_1)$ be a Boolean modulo-p branching program of size $a(n)$ computing f. Then there exists a CDS protocol for f with randomness complexity and communication complexity both $O(a(n)^2 \log p)$.*

Note that the implication from PSM to CDS was already known, so this implication was already clear. Recently, this scaling was improved to linear in the branching program size [IW14].

We can compare this with the most efficient CDS constructions in the literature. A CDS protocol based on secret sharing schemes was given in [GIKM00]. They prove the following theorem[11].

6.4.16. Theorem. ***[GIKM '98]*** *Let $h_M : \{0,1\}^n \to \{0,1\}$ be a monotone Boolean function, and let $h : \{0,1\}^n \to \{0,1\}$ be a projection of h_M; that is, $h(y_1, ..., y_n) = h_M(g_1, ..., g_M)$, where each g_i is a function of a single variable y_i. Let S be a secret sharing scheme realizing the access structure h_M, in which the*

[11] The cost here being $c + |s|$ while the cost in the reference [GIKM00] being c is due to our defining the CDS to have the secret held on only one side, rather than on both as is the convention in [GIKM00].

total share size is c, and let s be a secret that can be hidden in S. Then there exists a protocol P for disclosing s subject to the condition h whose communication and randomness complexity are bounded by $c + |s|$.

Using the span program based constructions of secret sharing schemes [KW93], this upper bounds the CDS cost of f by the minimal size of a monotone span program computing any projection of f, call it f_M. If the span program is over the field $\mathbb{Z}_p$, the cost is $(\log p) \cdot mSP(f_M)$. In [CM23] (see Lemma 5) it is shown that the size of a span program computing the projection f_M is the same as the size of a (non-monotone) span program computing f, up to a constant additive term. This leads to the following corollary.

6.4.17. Corollary. *The randomness and communication complexity to perform CDS on the function f is at most $O(\log p \cdot SP_p(f))$, where $SP_p(f)$ is the size of any span program over $\mathbf{Z}_p$ computing f.*

Notice that this is quite similar to Corollary 6.4.15. Because the span program size and branching program size are related by Equation 6.95, the secret sharing based construction for CDS is always more efficient than the branching program based approach inherited from PSM.

Another protocol based on dependency programs [PS96] was given in [AR17]. Because dependency programs are always larger than span programs (see [PS96], Lemma 3.6)[12], the span program based construction remains the most efficient.

CDQS and f-routing protocols

Notice that efficient CDQS protocols are given by both efficient CDS protocols (Theorem 6.3.2) and by PSQM protocols (Theorem 6.3.4). Further, from Theorem 6.3.3 we have that efficient CDQS leads to efficient f-routing. These implications lead to the following theorem.

6.4.18. Theorem. *The randomness and communication complexity to perform CDQS or f-routing on the function f is at most $O(\log p \cdot SP_p(f))$.*

Since it had not previously been studied in the literature, this gives the largest known class of functions that can be implemented efficiently for CDQS.

We can compare Theorem 6.4.18 with the most efficient protocols known for f-routing. In [CM23], the authors proved an upper bound of $O(\log p \cdot SP_p(f))$ on communication and entanglement complexity of f-routing, exactly matching the result inherited from classical CDS. It is also interesting to note that the protocol given in [CM23] that achieves this bound is a close quantum analogue of the CDS protocol devised in the classical setting in [GIKM00]: both protocols are based on storing the secret in a secret sharing scheme and sending or not sending shares based on the value of bits of the input.

[12] This is true when considering binary inputs, which we do here. The construction in [AR17] extends to non-binary inputs, and in that setting there may be polynomial overheads.

6.5 New lower bounds

6.5.1 Linear lower bounds on CFE

We have the following theorem from [KN21].

6.5.1. Theorem. ***[KN 2021]*** *For a* $(1-o(1))$ *fraction of functions* $f_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$*, the communication complexity of two-party PSQM protocols with shared randomness for* f_n *is at least* $3n - 2\log n - O(1)$*.*

In Theorem 6.3.5, which shows CFE→PSQM, we could replace the shared entanglement in the CFE protocol and obtain a PSQM protocol that only uses shared randomness. In fact, the theorem gives that the resulting PSQM uses the same distributed resource state as the CFE. From this, Theorem 6.5.1 above gives the following.

6.5.2. Corollary. *For a* $(1-o(1))$ *fraction of functions* $f_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$*, the communication complexity of coherent function evaluation protocols with shared randomness for* f_n *is at least* $3n - 2\log n - O(1)$*.*

Note that we would expect no amount of shared random bits to suffice for a CFE, and instead for entangled states to be required. Thus, the consequence of this theorem is very weak in the CFE context.

6.5.2 Linear lower bounds on CDQS

We have the following theorem from [BCS22].

6.5.3. Theorem. ***[BCS 2022, random function].*** *Let* $n \geq 10$*. Assume that the inputs* $x, y \in \{0,1\}^n$ *are chosen at random. Then there exists a function* $f : X \times Y \to Z$ *with* $X, Y \in \{0,1\}^n$*,* $Z \in \{0,1\}$ *such that, if the number* q *of qubits each of the attackers controls satisfies*

$$q \leq n/2 - 5, \tag{6.98}$$

then the attackers are caught with probability at least 2×10^{-2}*. Moreover, a uniformly random function will have this property, except with exponentially small probability.*

Combining this result with Theorem 6.3.3, we find the following result for CDQS.

6.5.4. Corollary. *There exists a function* $f : X \times Y \to Z$ *with* $X, Y \in \{0,1\}^n$*,* $Z \in \{0,1\}$ *such that a CDQS protocol which is* ϵ*-correct and* δ*-secure for* f *with* $\max\{\epsilon, \sqrt{\delta}\} < 2 \times 10^{-2}$ *requires Alice and Bob to have a quantum resource system consisting of at least* $n/2 - 5$ *qubits. Moreover, a uniformly random function will have this property, except with exponentially small probability.*

Now applying Theorem 6.3.4 we obtain the following linear lower bound on the dimension of the resource system in PSQM. Note that previously a $2n - O(\log n)$ linear lower bound on communication complexity was known, but no bound on shared entanglement was previously known.

6.5.5. Corollary. *There exists a function $f : X \times Y \to Z$ with $X, Y \in \{0,1\}^n$, $Z \in \{0,1\}$ such that a ϵ-correct and δ-secure PSQM protocol for f with $\max\{2\epsilon, \sqrt{2\delta}\} < 2 \times 10^{-2}$ requires Alice and Bob to have a quantum resource system consisting of at least $n/2 - 5$ qubits. Moreover, a uniformly random function will have this property, except with exponentially small probability.*

In the same paper [BCS22], the authors prove the following bound for the inner product function.

6.5.6. Theorem. ***[BCS 2022, Inner product]*** *Let $n \geq 10$. Assume that the inputs $x, y \in \{0,1\}^n$ are chosen at random. Then if the number q of qubits each of the attackers controls satisfies*

$$q \leq \frac{1}{2}\log n - 5, \tag{6.99}$$

then the attackers are caught with probability at least 2×10^{-2} when the function f is chosen to be the inner product function.

This immediately leads to two corollaries analogous to the above, but now with a logarithmic bound and a random function replaced with the inner product.

6.5.7. Corollary. *A CDQS protocol for the inner product function on strings of length n which is ϵ-correct and δ-secure with $\max\{\epsilon, \sqrt{\delta}\} < 2 \times 10^{-2}$ requires Alice and Bob to have a quantum resource system consisting of at least $\frac{1}{2}\log n - 5$ qubits.*

6.5.8. Corollary. *A PSQM protocol for the inner product function on strings of length n which is ϵ-correct and δ-secure with $\max\{2\epsilon, \sqrt{2\delta}\} < 2 \times 10^{-2}$ requires Alice and Bob to have a quantum resource system consisting of at least $\frac{1}{2}\log n - 5$ qubits.*

6.6 New protocols

6.6.1 f-routing for problems outside P/poly

As discussed in Section 6.4, all general constructions of CDS and PSM only efficiently implement functions inside of the class $(L^{\#L})_{(2)}$. As we now discuss, there is a special function which is believed to be outside of P but which has an efficient CDS, CDQS, and f-routing protocol. This function is known to be at least as hard as the quadratic residuosity problem modulo a composite of unknown factorization. This efficient protocol is inherited from Remark 6.2.16, which shows that efficient secret sharing schemes give efficient CDS protocols, along with a non-linear secret sharing scheme constructed in [BI05]. A less strong, but also interesting construction of a function outside of $L^{\#L}$ with an efficient PSM, CDS, CDQS, and f-routing scheme is based on a DRE for the quadratic residuosity problem modulo a prime. This function is inside of P but believed to be outside of NC.

We give the two constructions below.

f-routing for a problem outside P from non-linear secret sharing

We define the computational problem that will interest us here.

6.6.1. Definition. The **quadratic residuosity problem** $QR(u, v)$ is defined as follows.

- **Input:** Two integers u and v of n bits.
- **Output:** 1 if $gcd(u, v) = 1$ and there exists an r such that $u = r^2 \bmod v$, and 0 otherwise.

The quadratic residuosity function is believed to be outside of $P/poly$. It's hardness is the basis of a well-studied public-key cryptosystem [GM19], and other cryptographic constructions [Coc01, BBS86].

For linear secret sharing schemes, it is known that efficient schemes have complexity in the class Mod_kL when the scheme is defined over the field $\mathbb{Z}_k$ for k prime. Thus, the connection from secret sharing to CDS to CDQS and f-routing reproduces the known class of functions that can be efficiently implemented in the f-routing setting.

Beyond linear schemes, [BI05] constructed secret sharing schemes with indicator functions that have complexity outside of P. Their scheme realizes the following access structure.

6.6.2. Definition. $\mathbf{NQR}_n$ is an access structure on $n = 4m$ parties for m an integer. We label the $4m$ shares by W_i^b and U_j^b with $b \in \{0, 1\}$ and $j \in \{1, ..., m\}$. Given two bit strings[13] w, u each of length m, we associate a subset $B_{w,u}$ of size $2m$ according to

$$B_{w,u} = \{W_i^{w_i} : 1 \leq i \leq m\} \cup \{U_i^{u_i} : 1 \leq i \leq m\}. \tag{6.100}$$

The access structure $\mathbf{NQR}_n$ is then defined by its minimal authorized sets, which are

[13] To do modular arithmetic with w, u numbers in $\{0, \dots, 2^m - 1\}$ are associated to the strings w, u.

- $\{W_i^0, W_i^1\}$ for any $1 \le i \le m$
- $\{U_i^0, U_i^1\}$ for any $1 \le i \le m$
- $B_{w,u}$ for w, u such that $u \neq 0, 1$ and $QR(w,u) = 0$, so that w is not a quadratic residue modulo u.
- $B_{w,u=0}$ for $w \neq 1$.

Evaluating the indicator function for this access structure is at least as hard as solving the quadratic residuosity problem. To see this, notice that we can reduce computing $QR(u,w)$ to evaluating f_I as follows. From the string w of length m, define the two strings $\tilde{w}$, $\tilde{w}'$ according to

$$\tilde{w}_i = \begin{cases} 1 & \text{if } \ w_i = 1, \\ 0 & \text{otherwise,} \end{cases} \tag{6.101}$$

$$\tilde{w}_i' = \begin{cases} 1 & \text{if } \ w_i = 0, \\ 0 & \text{otherwise,} \end{cases} \tag{6.102}$$

We similarly define $\tilde{u}$ and $\tilde{u}'$, and then notice that

$$QR(w,u) = \neg f_I(\tilde{w}, \tilde{w}', \tilde{u}, \tilde{u}'). \tag{6.103}$$

Since computing $\tilde{w}, \tilde{w}', \tilde{u}, \tilde{u}'$ from (w,u) can be done efficiently, computing f_I is not harder than computing $QR(w,u)$.

Despite the indicator function being of high complexity, there exists an efficient secret sharing scheme for the access structure $\mathbf{NQR}_n$. This is given in the following theorem.

6.6.3. Theorem. ***[BI 2005]*** *There exists an ϵ secure and δ private secret sharing scheme for the access structure $\boldsymbol{NQR}_n$ storing a single bit secret with security parameter k, and*

- *share size $O(k^2 + km)$,*
- *correctness $\epsilon = 2^{-k}$,*
- *security*[14] *$\delta = k/2^k$.*

[14] Note that our security definition in terms of a simulator is different from the definition in [BI05], but it is straightforward to show their security definition with value δ implies ours with the same δ.

We refer the reader to [BI05] for the construction of this scheme.

In the context of these distributed cryptographic tasks, we are interested in functions which remain of high complexity even when allowing for pre-processing. Thus, we would like to construct functions outside of $P_{(2)}$, perhaps starting with NQR. For a function to be a likely candidate to be outside $P_{(2)}$, we need to ensure pre-processing is as unhelpful as possible. We suggest the following function

$$NQR_{4m,(2)}(x,y) = NQR_{4m}(x \oplus y). \tag{6.104}$$

Then, since Alice see's only x and Bob see's only y, pre-processing seems no better than advice, so we expect that $\mathrm{NQR}_{4m,(2)}$ is outside $P_{(2)}$ if we have that NQR_{4m} is outside $P/poly$, as we commented above is believed. We state this as the following assumption.

6.6.4. Conjecture. *The function $NQR_{4m,(2)}(x,y)$ is outside of $P_{(2)}$.*

Next, we claim that there is an efficient CDS scheme for $\mathrm{NQR}_{4m,(2)}(x,y)$. To see this, we have Alice, following remark 6.2.16, prepare the scheme in Theorem 6.6.3 with access structure $\mathrm{NQR}_{4m}(z)$. Then she takes share S_i to be the secret which will be conditionally disclosed in a scheme on the XOR function with inputs x_i and y_i. Correctly implementing each of these CDS schemes for the shares S_i is easily seen to now correctly implement the larger scheme with access structure $\mathrm{NQR}_{(2),4m}$. This CDS can be performed using $O(|S_i|)$ randomness, so the total needed randomness is still given by the size of the secret sharing scheme.

From this construction for CDS and Theorem 6.3.2 we obtain the following.

6.6.5. Corollary. *Assuming conjecture 6.6.4, there exists a function outside of $P_{(2)}$ with n input bits and hiding one (qu)bit for which CDS and CDQS can be performed $\epsilon = 2^{-k}$ correctly and $\delta = k2^{-k}$ securely with $O(k^2+kn)$ shared bits of randomness.*

From Theorem 6.3.3, we then obtain the following consequence for f-routing.

6.6.6. Corollary. *Assuming conjecture 6.6.4, there exists a function outside of $P_{(2)}$ with n input bits and hiding one (qu)bit for which f-routing can be performed $\epsilon = O(k2^{-k})$ correctly with $O(k^2+kn)$ shared entangled pairs.*

f-routing for a problem outside NC from DRE

Next, we construct a CDS scheme for a lower complexity function, albeit one that is still outside of NC, via a second route that begins with a decomposable randomized encoding.[15] The computational problem that will interest us is again quadratic residuosity, but this time where the modulus is taken over a prime.

[15] Another route for a construction of an f-routing scheme for a problem outside NC but inside P, and which is exact, is to begin with (exact) non-linear secret sharing scheme given in [BI05]. We have chosen to use a route beginning with DRE to illustrate that interesting connection.

6.6.7. Definition. The **quadratic residuosity problem over $\mathbb{Z}_p$** is defined as follows.

- **Input:** An integer a of n bits and prime p, also of n bits.
- **Output:** 1 if $a = b^2 \bmod p$ for some b, and 0 otherwise.

While this problem is not known to be within NC, it is easily placed inside of P by recalling the Euler criterion, which states that

$$a^{\frac{p-1}{2}} = 1 \bmod p, \tag{6.105}$$

if and only if a is a square. Given this, modular exponentiation can be used to determine whether a is a square in polynomial time. Note that if we pose the same problem but with the prime p replaced by a composite number, the resulting problem is thought to be outside of P [Kal11]. We focus on the prime case here. See [BI05] for a related discussion of the complexity of the quadratic residuosity functions considered over a field $\mathbb{Z}_p$ for p prime.

The quadratic residuosity problem over primes admits a simple randomized encoding scheme. In particular, take

$$a \to r^2 a, \tag{6.106}$$

for r a randomly chosen integer in $\mathbb{Z}_p$. To understand why this is a randomized encoding, notice that $QR(a) = QR(r^2 a)$, so we can compute the result of the function defined by the residuosity problem from the encoded output correctly, by (in this particular case) simply computing the original function, since $r^2 a$ is a quadratic residue if a is. Next, to show security, one needs to show that if a is a quadratic residue, then $r^2 a$ is randomly distributed over all those integers $\tilde{a}$ in $\mathbb{Z}_p$ which also are, and if a is not a quadratic residue then r^2 is uniformly distributed over all those $\tilde{a}$ which are also not. This amounts to showing that if a and $\tilde{a}$ both are (or both are not) quadratic residues, then there is a unique r such that $r^2 a = \tilde{a}$. This follows because the product of two residues is a residue, and the product of two non-residues is a residue.

We can further extend this to a decomposable randomized encoding as follows [BHI+20]. Use the encoding

$$a_i \to a_i r^2 2^{i-1} + s_i =: y_i, \tag{6.107}$$

for s_i, r drawn independently and at random from $\mathbb{Z}_p$ for all but the last s_i, which we set so that $\sum_i s_i = 0$. Then to decode use

$$QR\left(\sum_i y_i\right) = QR(r^2 a) = QR(a). \tag{6.108}$$

To see security, we assume that a, $\tilde{a}$ are two integers with the same quadratic residue, and then show that there is a choice of r, s_i which makes the bits of a look like the bits of $\tilde{a}$. This means we need to solve

$$a_i 2^{i-1} = \tilde{a}_i 2^{i-1} r^2 + s_i, \tag{6.109}$$

subject also to $\sum_i s_i = 0$. It is easy to see we can do this taking as an assumption the same thing we used in the earlier case, that if a, $\tilde{a}$ have the same quadratic residue then there is a r such that $a = r^2\tilde{a}$.

Given the existence of a decomposable randomized encoding scheme for the quadratic residue problem, we immediately obtain a PSM for this problem as noted above: Alice and Bob simply send the randomized encodings of their input bits to the referee, who runs the decoding procedure. This was already observed in [IK97]. This in turn implies an efficient CDS, CDQS, and f-routing scheme for $f(x) = QR(x)$. We collect these observations as the following remark.

6.6.8. Remark. Consider an n-bit string z and split its bits into arbitrary subsets S and S^c. Let the bits from S define a string z_S and a bit from S^c define a string z_{S^c}. Then the function $f(z_S, z_{S^c}) = QR(z)$ has perfectly correct PSM and CDS schemes that use poly(n) bits of randomness.

We can also use Theorems 6.3.2 and 6.3.3 to upgrade these to quantum schemes, giving the following corollary.

6.6.9. Corollary. *Consider an n-bit string z and split its bits into arbitrary subsets S and S^c. Let the bits from S define a string z_S, and a bit from S^c define a string z_{S^c}. Then the function $f(z_S, z_{S^c}) = QR(z)$ have perfectly correct PSQM and CDQS schemes that use poly(n) EPR pairs as a resource state.*

Ideally, one would show that, assuming $QR(z)$ is outside of NC implies $f(z_S, z_{S^c})$ is outside of $\mathrm{NC}_{(2)}$ but we are unable to do so. Nonetheless, this constructs a second problem not known to be in $\mathrm{NC}_{(2)}$ with an efficient f-routing scheme, although this one is inside of P. Another comment is that this problem has an exact scheme, while the construction in the previous section outside of P is approximate.

6.6.2 Efficient PSQM and CDQS for low T-depth circuits

In [Spe16a], a protocol is given that performs a unitary $\mathbf{U}_{AB}$ non-locally with entanglement cost that depends on the circuit decomposition of $\mathbf{U}_{AB}$. In particular, we write $\mathbf{U}_{AB}$ in terms of a Clifford + T gate set, and obtain the following two upper bounds on entanglement cost.

6.6.10. Theorem. *Any n qubit Clifford + T quantum circuit C which has at most k T-gates can be implemented non-locally using $O(n2^k)$ EPR pairs. Furthermore, if C has T-depth d then there is a protocol to implement C non-locally using $O((68n)^d)$ EPR pairs.*

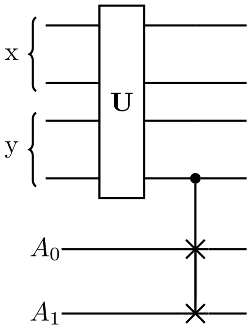


Figure 6.7: The circuit implementing the unitary $\mathbf{U}'$. The unitary $\mathbf{U}$ computes $f(x,y)$ on it's last wire with high fidelity. System A_0 is initially maximally entangled with reference R. At the end of the circuit, R with be highly entangled with system $A_{f(x,y)}$.

From Theorems 6.4.18 and 6.3.5, these results lead to upper bounds on entanglement cost in implementing CDQS, f-routing, and PSQM. These upper bounds depend on the number of T gates needed to compute $f(x,y)$ with a quantum circuit. We first discuss the CDQS setting.

6.6.11. Corollary. *Suppose that a function $f(x,y)$ can be evaluated with probability $1-\epsilon$ by a Clifford + T circuit with T-count k and T-depth d. Then there is a 2ϵ-correct f-routing protocol for the function $f(x,y)$ that uses at most $O(n2^k)$ EPR pairs, or at most $O((68n)^{d+5})$ EPR pairs, whichever is smaller.*

Proof:
Let $\mathbf{U}$ be the unitary that computes f. Recall that this means a measurement in the computational basis on the first qubit of the output of $\mathbf{U}$ returns $f(x,y)$ with probability $1-\epsilon$. Writing the state

$$\mathbf{U}\,|x,y\rangle = \sum_{i_2,...,i_n} \alpha_{0,i_2,...,i_n}\,|0\rangle\,|i_2,...,i_n\rangle + \sum_{i_2,...,i_n} \alpha_{1,i_2,...,i_n}\,|1\rangle\,|i_2,...,i_n\rangle$$
$$= \alpha_0\,|\psi_0\rangle + \alpha_1\,|\psi_1\rangle\,, \tag{6.110}$$

we have that $|\alpha_{f(x,y)}|^2 \geq 1-\epsilon$.

Now consider modifying the circuit that implements $\mathbf{U}$ by adding two ancilla qubits A_0A_1 and a controlled SWAP gate, where we control on the first output qubit of $\mathbf{U}$. We show this as a quantum circuit in Figure 6.7. The controlled SWAP gate can be implemented with 7 T-gates arranged in 5 layers (see, e.g. [KC18]). Thus, our new circuit has T-depth at most $d+5$ and T-count at most $k+7$. We call the unitary $\mathbf{U}$ composed with the controlled swap gate $\mathbf{U}'$.

To implement the f-routing protocol, we implement $\mathbf{U}'$ non-locally with A_0X held on the left and A_1Y held on the right. Initially A_0 is in the maximally entangled state with the reference system R. Because $\mathbf{U}'$ can be implemented with $k+7$ T-gates and T-depth of $d+5$, Theorem 6.6.10 gives that this takes no more than $O(n2^k)$ EPR pairs, or at most $O((68n)^{d+5})$ EPR pairs, whichever is smaller. Then we claim that at the end of the protocol that the $A_{f(x,y)}$ system is nearly maximally entangled with R.

To see this, notice that the state of the RA_0A_1XY after the unitary plus controlled swap have been applied is

$$\alpha_0 \left|\Psi^+\right\rangle_{RA_0} \left|0\right\rangle_{A_1} \left|\psi_0\right\rangle_{XY} + \alpha_1 \left|\Psi^+\right\rangle_{RA_1} \left|0\right\rangle_{A_0} \left|\psi_1\right\rangle_{XY}, \tag{6.111}$$

where ψ_0 and ψ_1 are orthogonal states as a consequence of unitarity of $\mathbf{U}$. We take the decoding channel to be the trace over the $A_{1-f(x,y)}XY$ system, followed by a relabeling of $A_{f(x,y)}$ as Q. This produces the state

$$\rho_{RQ} = |\alpha_{f(x,y)}|^2 \Psi^+_{RQ} + |\alpha_{1-f(x,y)}|^2 \frac{\mathcal{I}}{d_R} \otimes |0\rangle\langle 0|_Q \,. \tag{6.112}$$

Then we can calculate the fidelity

$$F(\Psi^+, \rho_{RQ}) \geq |\alpha_{f(x,y)}|^2 \geq 1 - 2\epsilon, \tag{6.113}$$

so that the f-routing protocol is 2ϵ correct, as needed. □

From Theorem 6.4.18, this also leads to a similar upper bound for CDQS.

6.6.12. Corollary. *Suppose that a function $f(x,y)$ can be evaluated with probability $1-\epsilon$ by a Clifford + T circuit with T-count k and T-depth d. Then there is a 2ϵ-correct and $\sqrt{\epsilon \log d_Q}$ secure CDQS protocol for the function $f(x,y)$ that uses at most $O(n2^k)$ EPR pairs, or at most $O((68n)^d n^5)$ EPR pairs, whichever is smaller.*

Proof:
Immediate from Theorem 6.3.3. □

Next, we apply Theorem 6.6.10 to give a class of functions for which PSQM can be efficiently performed.

6.6.13. Corollary. *Suppose that the isometry*

$$\mathbf{V}_f = \sum_{xy} \left|xy\right\rangle_{Z'} \left|f_{xy}\right\rangle_Z \left\langle x\right|_X \left\langle y\right|_Y \tag{6.114}$$

can be implemented with closeness ϵ (according to the diamond norm distance) with a Clifford + T circuit with T-count k and T-depth d. Then there exists a PSQM protocol for $f(x,y)$ which is ϵ-correct and $\sqrt{\epsilon}$-secure that uses at most $O(n2^k)$ EPR pairs, or at most $O((68n)^d n^5)$ EPR pairs, whichever is smaller.

Proof:
Follows immediately from Theorems 6.3.5 and 6.6.10 taken together. □

6.7 Sub-exponential protocols for f-routing on arbitrary functions

In a surprising breakthrough, [LVW17] showed that CDS can be performed for any function using sub-exponential communication and randomness. We summarize their result as the following theorem.

6.7.1. Theorem. ***[LVW 2017]*** *Every function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ has a CDS protocol for single bit secrets using $2^{O(\sqrt{n \log n})}$ bits of randomness and $2^{O(\sqrt{n \log n})}$ bits of communication.*

Combining this with Theorem 6.3.2 we obtain the following corollary.

6.7.2. Corollary. *There exist CDQS protocols with perfect correctness and secrecy for every function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ using $2^{O(\sqrt{n \log n})}$ bits of randomness and $2^{O(\sqrt{n \log n})}$ bits of communication, along with a single qubit of communication.*

Proof:
Recall that CDS protocols for secrets s_1, s_2 can be run in parallel if using fresh randomness for each instance (see the paragraph after remark 6.2.4). Thus, we can create a CDS hiding two bits of secret while still using $2^{O(\sqrt{n \log n})}$ randomness and communication, and then apply Theorem 6.3.2 to see that we can perform CDQS on a single qubit. □

From this, Theorem 6.3.3 leads to the following.

6.7.3. Corollary. *There exists a perfectly correct f-routing protocol for every function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ using $2^{O(\sqrt{n \log n})}$ qubits of resource system and $2^{O(\sqrt{n \log n})}$ qubits of message.*

Proof:
Immediate from Corollary 6.7.2 and Theorem 6.3.3. □

Before moving on, we will dive deeper into the subexponential construction in [LVW17]. Where does the sub-exponential advantage come from and can we use it for other tasks?

The construction begins with a reduction from a CDS protocol for a general function $f(x, y)$ to a particular function, which we denote as $INDEX(x, D_y)$. It takes as input Alice's input x and the database

$$D_y = \{f(x', y) \,|\, x' \in \{0,1\}^n\}. \tag{6.115}$$

The $INDEX$ function simply outputs the value in the database at index x, notice that:

$$f(x, y) = INDEX(x, D_y) = D_y[x]. \tag{6.116}$$

This means in particular that a good CDS protocol for the index function will lead to a good CDS protocol for all functions.

The construction of a CDS for $INDEX$ begins with a connection to the cryptographic task of *private information retrieval* (PIR). In a PIR task, a client interacts with several non-communicating servers to retrieve an item with label x from a database D, call the item $D[x]$. Security of the PIR requires that the databases cannot determine the label x. This primitive has long been noted to be related to CDS, and in fact CDS was first defined in the context of studying PIR schemes [GIKM00]. While it is not known whether all PIR schemes induce CDS schemes, techniques used in PIR constructions have led to CDS schemes. Theorem 6.7.1 was proven by applying tools from a sub-exponential PIR scheme presented in [DG16] to construct a CDS.

The construction in [DG16] is based on the existence of large *matching vector families* (MVF). They define MVF as follows:

6.7.4. Definition (MVF). Let $S \subset \mathbb{Z}_m \setminus \{0\}$, and let $\mathcal{F} = (\boldsymbol{\mathcal{U}}, \boldsymbol{\mathcal{V}})$, where $\mathcal{U} = \{\mathbf{u}_1, \ldots, \mathbf{u}_k\}$ and $\mathcal{V} = \{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ are lists of k vectors $\mathbf{u}_i, \mathbf{v}_i \in \mathbb{Z}_m^d$. Then $\mathcal{F}$ is called an S-MVF over $\mathbb{Z}_m^d$ of size k and dimension d if $\forall i, j$ we have:

$$\begin{aligned} &\langle \mathbf{u}_i, \mathbf{v}_i \rangle = 0 \\ &\langle \mathbf{u}_i, \mathbf{v}_j \rangle \in S, \text{ if } i \neq j. \end{aligned}$$

Of interest is how large k can be for vectors chosen in a given vector space $\mathbb{Z}_k^d$. For our application, we are interested in constructing MVF where k should be as large as possible while $|S|, m, d$ are small. One can show that if m is a prime that the size k of an MVF can only be polynomially larger than the dimension [Gop19]. However, if m is a composite number, we can obtain much better constructions. In [Gro00], the authors constructed an MVF over $\mathbb{Z}_6^d$ of size k, where $d = 2^{O(\sqrt{\log k \log\log k})}$. In the construction of [LVW17], the amount of randomness and communication needed scales with the dimension of the MVF, whose size is equal to the size of the database in 6.115. For a general CDS with n-bit inputs the database has size $|D_y| = 2^n$, so the dimension is $d = 2^{O(\sqrt{n \log n})}$, as in Theorem 6.7.1.

The construction of the MVF in [Gro00] is based on a polynomial representation of $\mathrm{OR}_n \mod m$, defined as:

6.7.5. Definition. Let $x \in \{0,1\}^n$, a polynomial $p(x_1, \ldots, x_n)$ represents OR_n mod m if:

$$p(x_1, \ldots, x_n) \equiv 0 \bmod m \text{ if and only if } x = 0^n. \tag{6.117}$$

When m is a prime, the degree of p scales with n. To see this, note that, by Fermat's Little Theorem, $p(x)^{m-1}$ is exactly equal to the OR mod m function.

As every function has a unique representation as a multilinear polynomial, we must have the following:

$$p(x)^{m-1} = 1 - \prod_{i=1}^{n}(1 - x_i) \bmod m, \tag{6.118}$$

as the right hand side computes the $\mathrm{OR}_n \bmod m$ function. Therefore, $\deg(p) \geq n/(m-1)$.

However, when m is a composite, constructions of a much lower degree are possible. The best known construction has degree $O(\sqrt[t]{n})$ for such polynomials, where t is the number of distinct prime factors of m [BBR94].

The following lemma from [Gop19] relates the degree of polynomials that compute $\mathrm{OR}_n \bmod m$ directly to the existence of a certain dimension by constructing vectors whose length corresponds to the number of monomials in the polynomial.

6.7.6. Lemma. *Suppose $p(x_1, \ldots, x_n)$ is a polynomial representation of OR_n* mod *m of degree r. Then, there exists an MVF over $\mathbb{Z}_m^d$ of size $k = 2^n$ and dimension $d = \binom{n+r}{r}$.*

Proof:
Consider a matrix M whose rows and columns are indexed by strings $x, y \in \{0,1\}^n$. Let the matrix entries M_{xy} be $p(x \oplus y) \bmod m = p(x_1 \oplus y_1, \ldots, x_n \oplus y_n) \bmod m$. As $x_i \oplus y_i = x_i + y_i - 2x_iy_i$, $p(x \oplus y)$ is a polynomial of degree r in variables x and y. Thus, we can write as $p(x \oplus y) = \sum_{\alpha:|\alpha|\leq r} x^\alpha q_\alpha(y)$, where $q_\alpha(y)$ is some polynomial in y with degree at most r. Now, M is a matrix with 0's on the diagonal and non-zero elements off diagonal. Note that its entries $M_{xy} = \sum_{\alpha:|\alpha|\leq r} x^\alpha q_\alpha(y)$ can be written as an inner product between the vector $\mathbf{u}_x = (x^\alpha)_{\alpha:|\alpha|\leq r}$ and $\mathbf{v}_y = (q_\alpha(y))_{\alpha:|\alpha|\leq r}$. These vectors have the properties of an MVF and their dimension d is equal to the number of monomials in p, which is $\binom{n+r}{r}$. □

This recovers a subexponential construction of the $m = 6$ case, as $\binom{n+O(\sqrt{n})}{O(\sqrt{n})} = 2^{O(\sqrt{n}\log n)}$. The subexponential CDS construction relies on $m = 6$, and cannot be extended to use MVF over larger rings with more prime factors.

Little is known about lower bounds on the degree of a polynomial representation of $\mathrm{OR}_n \bmod m$. The best lower bound is $\Omega((\log n)^{\frac{1}{t-1}})$, where t is the number of distinct prime factors of m [TMB98], which is a huge gap compared to the best known upper bound of $O(\sqrt[t]{n})$. Suppose that this lower bound can be attained, then it implies by the above lemma that for $m = 6$ there exists MVF of size $k = 2^n$ and dimension $d = 2^{O(\log(n)^2)}$. This would immediately imply the existence of a CDS that uses $2^{O(\log(n)^2)}$ bits of randomness and communication by the construction of [LVW17]. And, by Corollary 6.7.3, there will exist an f-routing protocol for every function that uses only $2^{O(\log(n)^2)}$ qubits of communication and for the resource system.

The contrapositive of this argument is now an interesting connection between open questions in NLQC and computational complexity. We see that lower bounds on the necessary resource system of an f-routing protocol imply lower bounds on the degree of the polynomial representation of the OR_n mod 6 function. For both problems, we do not know what bounds to expect. For a long time, it was expected that exponential resource systems would be necessary for f-routing schemes. If we can show lower bounds that are better than the $2^{O(\log(n)^2)} = n^{O(\log(n))}$ qubits of the resource system, we improve the best known lower bound of $O(\log(n))$ for the degree of the polynomial representation of OR_n mod 6.

6.8 Discussion

Collapse of CDQS and PSQM complexity with PR boxes

A Popescu-Rohrlich box is a hypothetical device, shared by distant parties Alice and Bob, which allows them to satisfy the CHSH game with probability one. More concretely, given input x on Alice's side and input y on Bob's side, the device returns a to Alice and b to Bob such that $a \oplus b = x \wedge y$. Broadbent [Bro16] showed that if Alice and Bob share PR boxes, they can implement any unitary as a non-local computation using only linear entanglement and a linear number of uses of a PR box. This can be seen as a quantum analogue of a similar collapse that occurs in the setting of classical communication complexity [VD13]. Because efficient non-local computation protocols lead, via Theorems 6.3.3 and 6.3.5, to efficient CDQS and PSQM protocols, Broadbent's result similarly leads to a collapse to linear cost for PSQM and CDQS.

In fact, an even stronger collapse follows for CDQS, PSQM and f-routing by applying the result of [VD13] showing the collapse of classical communication complexity in the presence of PR boxes. In particular, PR boxes can be used to reduce computing $f(x, y)$ with x held by Alice and y held by Bob to computing $\alpha + \beta$, with α computed from x plus the output of PR box uses, and β computed from y along with PR box uses.[16] In the CDS or PSM settings, we need only to execute CDS or PSM on the function $g(\alpha, \beta) = \alpha + \beta$ with the inputs being single bits. This can be done with $O(1)$ randomness. Using Theorems 6.3.2 and 6.2.19, CDQS can then be done with $O(1)$ EPR pairs and PSQM with $O(1)$ shared random bits. We can further note that from Theorem 6.3.3 this means f-routing can be performed for arbitrary functions using only $O(1)$ EPR pairs when given access to PR boxes.

Connections to quantum gravity and holography

[16] See [KKLR11] for results on the number of PR box uses necessary. Note that in our setting, we can use the PR boxes sequentially if desired.

In the study of quantum gravity the holographic principle [Hoo93, Sus95] asserts that gravity in d dimensions should have an alternative quantum mechanical description in just $d-1$ dimensions. This principle is realized manifestly in the context of the AdS/CFT correspondence [Mal99, Wit98]. In [May19], holography and the AdS/CFT correspondence was related to non-local quantum computation. In particular, they argued local interactions in the higher-dimensional gravity picture are reproduced as non-local quantum computations in the lower-dimensional quantum mechanical picture. As a consequence, computations in the presence of gravity may be constrained by limits on entanglement in the dual quantum mechanical picture [May22], or interactions in the gravity picture may imply more computations can be performed non-locally than we have so far found protocols for.

In this chapter, we see that as a consequence of their connections to NLQC, CDQS and PSQM are also related to holography. One can also realize CDQS and PSQM protocols directly in holography, using connections similar to the one in [May19] or the more recent [MX24]. This implies that, as with NLQC, constraints on CDQS and PSQM correspond to constraints on bulk interactions. Conversely, the holographic picture has been argued [MPS20, May22] to suggest that a larger class of unitaries than is currently known should have efficient non-local implementations. Importantly, the connection between CDQS and PSQM is so far limited to the 2 input player case, which is also the case that ties to NLQC. It may be possible to explore a connection between CDQS and PSQM to holography that is realized more directly, not via NLQC, which could extend the connection to settings with many input players.

Recalling [May22], it was argued that the holographic connection suggests that at least unitaries in BQP should be implementable non-locally. From this perspective, it is interesting that, from the connection to secret sharing, we now have at least one function outside of P but inside of BQP with an efficient non-local implementation.

Quantum analogues of recent classical results

Non-local quantum computation was previously thought to have no (non-trivial) classical analogue: taking the inputs and outputs of a computation to be classical, one can immediately perform the computation in the non-local form of figure 6.1b without use of shared randomness.[17] The connections pointed out in this chapter give non-trivial classical analogues of non-local computation: CDQS is equivalent to a special case of NLQC, and has a non-trivial classical version (CDS), and similarly to PSM.

Traditionally, classical analogues are a source of techniques and conjectures in the quantum setting. Taking this perspective on CDS and CDQS, two recent

[17] This amounts to a special case of the impossibility result [CGMO09]. To see why it is true, consider copying the inputs x and y where they are received and forwarding a copy across the communication channel.

results in the CDS literature are natural candidates to revisit in the quantum setting.

First, in [AV21], the authors relate CDS to various communication complexity scenarios. In particular, they consider the communication complexity class AM^{cc}, defined as follows. Alice and Bob hold inputs x and y and share randomness r, while a referee holds (x, y). The referee will send Alice and Bob a proof $p = p(x, y, r)$ that both Alice and Bob should accept when $f(x, y) = 1$, and both should reject if $f(x, y) = 0$. $AM^{cc}(f)$ is the minimal length of the needed proof, and AM^{cc} is the class of functions for which the proof can be taken to be of polylogarithmic length. Relating this to CDS, they show that for some constant $c > 0$,

$$CDS(f) \geq (\max\{AM^{cc}(f), coAM^{cc}(f)\})^c - \mathrm{polylog}(n), \tag{6.119}$$

where CDS(f) is the communication complexity of a CDS protocol for f (allowing for imperfect correctness and imperfect security), and a similar bound differing only by constant factors exists for randomness complexity. Unfortunately, there are no explicit functions known to be outside $AM^{cc} \cap coAM^{cc}$, but nevertheless Equation 6.119 is an intriguing result. A natural question is whether a similar inequality holds when considering CDQS and quantum communication complexity classes.

Second, related work [AR17] studied the relationship between zero-knowledge proofs and both CDS and PSM. The starting point is a zero-knowledge variant of the class AM^{cc} discussed above, where an additional requirement is imposed that the proof p not reveal anything about (x, y). This is referred to as the class ZAM^{cc}. The authors of [AR17] found that a PSM protocol with perfect correctness and privacy leads to a similarly efficient ZAM protocol, and that a ZAM protocol (which may be approximate) leads to a similarly efficient CDS protocol. Again, it is natural to ask for a quantum analogue of these results.

Classical analogues of further non-local computations

In this chapter, we relate two special cases of non-local quantum computation — f-routing and coherent function evaluation — to other cryptographic tasks, CDQS and PSQM. One aspect of these relationships we have emphasized is that while non-local computation naively becomes trivial when considered classically[18], PSQM and CDQS have natural classical variants. This raises the question as to whether NLQC generally has a good classical analogue, perhaps one exploiting the same communication pattern as CDS and PSM, and employing an appropriate secrecy condition. Less ambitiously, we can also ask about classical analogues of other commonly studied non-local quantum computation schemes. One commonly studied non-local computation that we have not considered here is the

[18] In particular we have in mind that a non-local computation with only classical inputs can always be implemented without pre-distributed resources [CGMO09].

BB84 task [BCF+14, TFKW13], and its extension to f-BB84 [BCS22, EFS23]. It would be interesting to understand if f-BB84 is related to a classical primitive.

Bibliography

[AA20] Benny Applebaum and Barak Arkis. On the power of amortization in secret sharing: d-uniform secret sharing and cds with constant information rate. *ACM Transactions on Computation Theory (TOCT)*, 12(4):1–21, 2020.

[AARV21] Benny Applebaum, Barak Arkis, Pavel Raykov, and Prashant Nalini Vasudevan. Conditional disclosure of secrets: Amplification, closure, amortization, lower-bounds, and separations. *SIAM J. Comput.*, 50(1):32–67, jan 2021.

[ABB$^+$87] F. C. Alcaraz, M. N. Barber, M. T. Batchelor, R. J. Baxter, and G. R. W. Quispel. Surface exponents of the quantum XXZ, Ashkin-Teller and Potts models. *Journal of Physics A: Mathematical and General*, 20(18):6397, 1987.

[ABB$^+$23] Rene Allerstorfer, Andreas Bluhm, Harry Buhrman, Matthias Christandl, Llorenç Escolà-Farràs, Florian Speelman, and Philip Verduyn Lunel. Making existing quantum position verification protocols secure against arbitrary transmission loss. *arXiv preprint arXiv:2312.12614*, 2023.

[ABM$^+$24] Rene Allerstorfer, Harry Buhrman, Alex May, Florian Speelman, and Philip Verduyn Lunel. Relating non-local quantum computation to information theoretic cryptography. *Quantum*, 8:1387, 2024.

[ABNP20] Benny Applebaum, Amos Beimel, Oded Nir, and Naty Peter. Better secret sharing via robust conditional disclosure of secrets. In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*, pages 280–293, 2020.

[ABSV22a] Rene Allerstorfer, Harry Buhrman, Florian Speelman, and Philip Verduyn Lunel. On the role of quantum communication and loss in attacks on quantum position verification. *arXiv preprint arXiv:2208.04341*, 2022.

[ABSV22b] Rene Allerstorfer, Harry Buhrman, Florian Speelman, and Philip Verduyn Lunel. Towards practical and error-robust quantum position verification. *arXiv preprint arXiv:2106.12911*, 2022.

[ACCM24] Vahid Asadi, Richard Cleve, Eric Culf, and Alex May. Linear gate bounds against natural functions for position-verification. *arXiv preprint arXiv:2402.18648*, 2024.

[ACG$^+$23] Rene Allerstorfer, Matthias Christandl, Dmitry Grinko, Ion Nechita, Maris Ozols, Denis Rochette, and Philip Verduyn Lunel. Monogamy of highly symmetric states. *arXiv preprint arXiv:2309.16655*, 2023.

[AER$^+$23] Rene Allerstorfer, Llorenç Escolà-Farràs, Arpan Akash Ray, Boris Škorić, Florian Speelman, and Philip Verduyn Lunel. Security of a continuous-variable based quantum position verification protocol. *arXiv preprint arXiv:2308.04166*, 2023.

[AIR01] Bill Aiello, Yuval Ishai, and Omer Reingold. Priced oblivious transfer: How to sell digital goods. In *Advances in Cryptology—EUROCRYPT 2001: International Conference on the Theory and Application of Cryptographic Techniques Innsbruck, Austria, May 6–10, 2001 Proceedings 20*, pages 119–135. Springer, 2001.

[AMTW00] Andris Ambainis, Michele Mosca, Alain Tapp, and Ronald de Wolf. Private quantum channels. In *Proceedings 41st Annual Symposium on Foundations of Computer Science*, pages 547–553. IEEE, 2000.

[APS$^+$21] Ali Anwar, Chithrabhanu Perumangatt, Fabian Steinlechner, Thomas Jennewein, and Alexander Ling. Entangled photon-pair sources based on three-wave mixing in bulk crystals. *Review of Scientific Instruments*, 92(4):041101, 2021.

[AR17] Benny Applebaum and Pavel Raykov. From private simultaneous messages to zero-information Arthur–Merlin protocols and back. *Journal of Cryptology*, 30(4):961–988, 2017.

[AV21] Benny Applebaum and Prashant Nalini Vasudevan. Placing conditional disclosure of secrets in the communication complexity universe. *Journal of Cryptology*, 34:1–45, 2021.

[BB14] Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical computer science*, 560:7–11, 2014.

[BBC$^+$93] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70(13):1895–1899, March 1993.

[BBD$^+$97] Adriano Barenco, Andre Berthiaume, David Deutsch, Artur Ekert, Richard Jozsa, and Chiara Macchiavello. Stabilization of quantum computations by symmetrization. *SIAM Journal on Computing*, 26(5):1541–1557, 1997.

[BBR94] David A Mix Barrington, Richard Beigel, and Steven Rudich. Representing boolean functions as polynomials modulo composite numbers. *Computational Complexity*, 4(4):367–382, 1994.

[BBS86] Lenore Blum, Manuel Blum, and Mike Shub. A simple unpredictable pseudo-random number generator. *SIAM Journal on computing*, 15(2):364–383, 1986.

[BC93] Stefan Brands and David Chaum. Distance-bounding protocols. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 344–359. Springer, 1993.

[BCF$^+$14] Harry Buhrman, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky, and Christian Schaffner. Position-based quantum cryptography: Impossibility and constructions. *SIAM Journal on Computing*, 43(1):150–178, 2014.

[BCS22] Andreas Bluhm, Matthias Christandl, and Florian Speelman. A single-qubit position verification protocol that is secure against multi-qubit attacks. *Nature Physics*, 18(6):623–626, 2022.

[BCWW01] Harry Buhrman, Richard Cleve, John Watrous, and Ronald de Wolf. Quantum fingerprinting. *Physical Review Letters*, 87(16), September 2001.

[BDHM92] Gerhard Buntrock, Carsten Damm, Ulrich Hertrampf, and Christoph Meinel. Structure and importance of logspace-mod class. *Mathematical systems theory*, 25(3):223–237, 1992.

[Ben20] Benny Applebaum, BIU Research Center on Applied Cryptography and Cyber Security. The 10th BIU winter school on cryptography - information theoretic cryptography, 2020.

[BFSS13] Harry Buhrman, Serge Fehr, Christian Schaffner, and Florian Speelman. The garden-hose model. In *Proceedings of the 4th conference on Innovations in Theoretical Computer Science*, pages 145–158, 2013.

[BG99] Amos Beimel and Anna Gál. On arithmetic branching programs. *Journal of Computer and System Sciences*, 59(2):195–220, 1999.

[BGLW24] Harry Buhrman, Dmitry Grinko, Philip Verduyn Lunel, and Jordi Weggemans. Permutation tests for quantum state identity. *arXiv preprint arXiv:2405.09626*, 2024.

[BHI$^+$20] Marshall Ball, Justin Holmgren, Yuval Ishai, Tianren Liu, and Tal Malkin. On the complexity of decomposable randomized encodings, or: how friendly can a garbling-friendly prf be? In *11th Innovations in Theoretical Computer Science Conference (ITCS 2020)*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2020.

[BI05] Amos Beimel and Yuval Ishai. On the power of nonlinear secret-sharing. *SIAM Journal on Discrete Mathematics*, 19(1):258–280, 2005.

[BK11] Salman Beigi and Robert König. Simplified instantaneous non-local quantum computation with applications to position-based cryptography. *New Journal of Physics*, 13(9):093036, 2011.

[BKMS06] Raymond G. Beausoleil, Adrian Kent, William J. Munro, and Timothy P. Spiller. Tagging systems, US patent 7075438, 2006.

[BKN18] Amos Beimel, Eyal Kushilevitz, and Pnina Nissim. The complexity of multiparty PSM protocols and related models. In *Advances in Cryptology–EUROCRYPT 2018: 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29-May 3, 2018 Proceedings, Part II 37*, pages 287–318. Springer, 2018.

[BM95] Samuel L. Braunstein and A. Mann. Measurement of the Bell operator and quantum teleportation. *Physical Review A*, 51:R1727–R1730, 1995.

[Bro16] Anne Broadbent. Popescu-Rohrlich correlations imply efficient instantaneous nonlocal quantum computation. *Physical Review A*, 94(2):022318, 2016.

[BRSW11] Harry Buhrman, Oded Regev, Giannicola Scarpa, and Ronald de Wolf. Near-Optimal and Explicit Bell Inequality Violations. In *2011 IEEE 26th Annual Conference on Computational Complexity*, pages 157–166, San Jose, CA, USA, June 2011. IEEE.

[CFG$^+$10] Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, and Rafail Ostrovsky. Position-based quantum cryptography. *arXiv preprint arXiv:1005.1750*, 2010.

[CGMO09] Nishanth Chandran, Vipul Goyal, Ryan Moriarty, and Rafail Ostrovsky. Position based cryptography. In *Annual International Cryptology Conference*, pages 391–407. Springer, 2009.

[CHE$^+$21] Jacob C Curtis, Connor T Hann, Salvatore S Elder, Christopher S Wang, Luigi Frunzio, Liang Jiang, and Robert J Schoelkopf. Single-shot number-resolved detection of microwave photons with error mitigation. *Physical Review A*, 103(2):023705, 2021.

[CHW$^+$17] Zhen Chai, Xiaoyong Hu, Feifan Wang, Xinxiang Niu, Jingya Xie, and Qihuang Gong. Ultrafast all-optical switching. *Advanced Optical Materials*, 5(7):1600665, 2017.

[CL01] J. Calsamiglia and N. Lütkenhaus. Maximum efficiency of a linear-optical Bell-state analyzer. *Applied Physics B*, 72(1):67–71, January 2001.

[CL15] Kaushik Chakraborty and Anthony Leverrier. Practical Position-Based Quantum Cryptography. *Physical Review A*, 92(5):052304, November 2015. arXiv: 1507.00626.

[CM23] Joy Cree and Alex May. Code-routing: a new attack on position verification. *Quantum*, 7:1079, August 2023.

[Coc01] Clifford Cocks. An identity based encryption scheme based on quadratic residues. *Lecture Notes in Computer Science*, 2260:360–363, 2001.

[Cos13] Alessandro Cosentino. PPT-indistinguishable states via semidefinite programming. *Physical Review A*, 87(1):012321, January 2013. arXiv: 1205.1031.

[CPS13] Secure Multi-Party Computation, MM Prabhakaran, and A Sahai. Randomization techniques for secure computation. *Secure Multi-Party Computation*, 10:222, 2013.

[CW04] Matthias Christandl and Andreas Winter. "Squashed entanglement": an additive entanglement measure. *Journal of mathematical physics*, 45(3):829–840, 2004.

[DC22] Kfir Dolev and Sam Cree. Holography as a resource for non-local quantum computation. *arXiv preprint arXiv:2210.13500*, 2022.

[DG16] Zeev Dvir and Sivakanth Gopi. 2-server PIR with subpolynomial communication. *Journal of the ACM (JACM)*, 63(4):1–15, 2016.

[DW05] Igor Devetak and Andreas Winter. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society A: Mathematical, Physical and engineering sciences*, 461(2053):207–235, 2005.

[EFS23] Llorenç Escolà-Farràs and Florian Speelman. Single-qubit loss-tolerant quantum position verification protocol secure against entangled attackers. *Physical Review Letters*, 131(14):140802, 2023.

[Eld03] Yonina C Eldar. A semidefinite programming approach to optimal unambiguous discrimination of quantum states. *IEEE Transactions on information theory*, 49(2):446–456, 2003.

[EPR35] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical review*, 47(10):777, 1935.

[ES23] Llorenç Escolà-Farràs and Florian Speelman. Single-qubit loss-tolerant quantum position verification protocol secure against entangled attackers. *Physical Review Letters*, 131(14):140802, 2023.

[ESM$^+$21] Mamoru Endo, Tatsuki Sonoyama, Mikihisa Matsuyama, Fumiya Okamoto, Shigehito Miki, Masahiro Yabuno, Fumihiro China, Hirotaka Terai, and Akira Furusawa. Quantum detector tomography of a superconducting nanostrip photon-number-resolving detector. *Optics Express*, 29(8):11728, mar 2021.

[Fad96] LD Faddeev. How algebraic Bethe ansatz works for integrable model. *arXiv preprint arXiv:hep-th/9605187*, 1996.

[FvdG99] C.A. Fuchs and J. van de Graaf. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Transactions on Information Theory*, 45(4):1216–1227, 1999.

[GC20] Alvin Gonzales and Eric Chitambar. Bounds on Instantaneous Nonlocal Quantum Computation. *IEEE Transactions on Information Theory*, 66(5):2951–2963, May 2020. arXiv: 1810.00994.

[GECP13] Juan Carlos Garcia-Escartin and Pedro Chamorro-Posada. The SWAP test and the Hong-Ou-Mandel effect are equivalent. *Physical Review A*, 87(5):052330, May 2013. arXiv: 1303.6814.

[GIKM00] Yael Gertner, Yuval Ishai, Eyal Kushilevitz, and Tal Malkin. Protecting data privacy in private information retrieval schemes. *Journal of Computer and System Sciences*, 60(3):592–629, 2000.

[GM19] Shafi Goldwasser and Silvio Micali. *Probabilistic encryption & how to play mental poker keeping secret all partial information*, page 173–201. Association for Computing Machinery, 2019.

[Gop19] Sivakanth Gopi. Lecture 11: Matching vector families, October 2019.

[Gro00] Vince Grolmusz. Superpolynomial size set-systems with restricted intersections mod 6 and explicit Ramsey graphs. *Combinatorica*, 20(1):71–86, 2000.

[Had09] Robert H. Hadfield. Single-photon detectors for optical quantum information applications. *Nature Photonics*, 3(12):696–705, 2009.

[Hay16] Masahito Hayashi. *Quantum information theory*. Springer, 2016.

[HOM87] C. K. Hong, Z. Y. Ou, and L. Mandel. Measurement of subpicosecond time intervals between two photons by interference. *Phys. Rev. Lett.*, 59:2044–2046, Nov 1987.

[Hoo93] Gerard ’t Hooft. Dimensional reduction in quantum gravity. *arXiv preprint arXiv:gr-qc/9310026*, 1993.

[Hor97] Pawel Horodecki. Separability criterion and inseparable mixed states with positive partial transposition. *Physics Letters A*, 232(5):333–339, 1997.

[HTS$^+$18] Takemi Hasegawa, Yoshiaki Tamura, Hirotaka Sakuma, Yuki Kawaguchi, Yoshinori Yamamoto, and Yasushi Koyano. The first 0.14-db/km ultra-low loss optical fiber. *SEI Technical Review*, 86:18–22, 2018.

[IH09] Satoshi Ishizaka and Tohya Hiroshima. Quantum teleportation scheme by selecting one of multiple output ports. *Physical Review A*, 79(4):042306, 2009.

[IK97] Yuval Ishai and Eyal Kushilevitz. Private simultaneous messages protocols with applications. In *Proceedings of the Fifth Israeli Symposium on Theory of Computing and Systems*, pages 174–183. IEEE, 1997.

[IKP10] Yuval Ishai, Eyal Kushilevitz, and Anat Paskin. Secure multiparty computation with minimal interaction. In *Advances in Cryptology–CRYPTO 2010: 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010. Proceedings 30*, pages 577–594. Springer, 2010.

[IW14] Yuval Ishai and Hoeteck Wee. Partial garbling schemes and their applications. In *Automata, Languages, and Programming: 41st International Colloquium, ICALP 2014, Copenhagen, Denmark, July 8-11, 2014, Proceedings, Part I 41*, pages 650–662. Springer, 2014.

[JAC04] Igor Jex, Erika Andersson, and Anthony Chefles. Comparing the states of many quantum systems. *Journal of Modern Optics*, 51(4):505–523, 2004.

[JKPPG21] Marius Junge, Aleksander M Kubicki, Carlos Palazuelos, and David Pérez-García. Geometry of Banach spaces: a new route towards position based cryptography. *arXiv preprint arXiv:2103.16357*, 2021.

[Kal11] Burt Kaliski. Quadratic residuosity problem. In *Encyclopedia of Cryptography and Security*, pages 1003–1003. Springer US, 2011.

[KC18] Taewan Kim and Byung-Soo Choi. Efficient decomposition methods for controlled-R_n using a single ancillary qubit. *Scientific reports*, 8(1):1–7, 2018.

[KKLR11] Marc Kaplan, Iordanis Kerenidis, Sophie Laplante, and Jérémie Roland. Non-local box complexity and secure function evaluation. *Quantum Information & Computation*, 11(1):40–69, 2011.

[KMS11] Adrian Kent, William J. Munro, and Timothy P. Spiller. Quantum Tagging: Authenticating Location via Quantum Information and Relativistic Signalling Constraints. *Physical Review A*, 84, July 2011.

[KN21] Akinori Kawachi and Harumichi Nishimura. Communication complexity of private simultaneous quantum messages protocols. *arXiv preprint arXiv:2105.07120*, 2021.

[Kra71] Karl Kraus. General state changes in quantum theory. *Annals of Physics*, 64(2):311–335, 1971.

[KSV02] A. Yu. Kitaev, A. H. Shen, and M. N. Vyalyi. *Classical and Quantum Computation.* American Mathematical Society, 2002.

[KSW08a] Dennis Kretschmann, Dirk Schlingemann, and Reinhard F Werner. A continuity theorem for Stinespring's dilation. *Journal of Functional Analysis*, 255(8):1889–1904, 2008.

[KSW08b] Dennis Kretschmann, Dirk Schlingemann, and Reinhard F Werner. The information-disturbance tradeoff and the continuity of Stinespring's representation. *IEEE transactions on information theory*, 54(4):1708–1717, 2008.

[KW93] Mauricio Karchmer and Avi Wigderson. On span programs. In *Proceedings of the Eigth Annual Structure in Complexity Theory Conference*, pages 102–111. IEEE, 1993.

[LL11] Hoi Kwan Lau and Hoi Kwong Lo. Insecurity of position-based quantum cryptography protocols against entanglement attacks. *Physical Review A*, January 2011.

[LLQ22] Jiahui Liu, Qipeng Liu, and Luowen Qian. Beating classical impossibility of position verification. In *13th Innovations in Theoretical Computer Science Conference (ITCS 2022)*, 2022.

[LLX$^+$19] Yang Li, Yu-Huai Li, Hong-Bo Xie, Zheng-Ping Li, Xiao Jiang, Wen-Qi Cai, Ji-Gang Ren, Juan Yin, Sheng-Kai Liao, and Cheng-Zhi Peng. High-speed robust polarization modulation for quantum key distribution. *Optics Letters*, 44(21):5262–5265, 2019.

[LVSL18] Alexander Lohrmann, Aitor Villar, Arian Stolk, and Alexander Ling. High fidelity field stop collection for polarization-entangled photon pair sources. *Applied Physics Letters*, 113(17):171109, 2018.

[LVW17] Tianren Liu, Vinod Vaikuntanathan, and Hoeteck Wee. Conditional disclosure of secrets via non-linear reconstruction. In *Advances in Cryptology–CRYPTO 2017: 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20–24, 2017, Proceedings, Part I*, pages 758–790. Springer, 2017.

[LXS$^+$16] Charles Ci Wen Lim, Feihu Xu, George Siopsis, Eric Chitambar, Philip G. Evans, and Bing Qi. Loss-tolerant quantum secure positioning with weak laser sources. *Physical Review A*, September 2016.

[Mal99] Juan Maldacena. The large-N limit of superconformal field theories and supergravity. *International journal of theoretical physics*, 38(4):1113–1133, 1999.

[Mal10] Robert A Malaney. Location-dependent communications using quantum entanglement. *Physical Review A*, 81(4):042319, 2010.

[May19] Alex May. Quantum tasks in holography. *Journal of High Energy Physics*, 2019(10):1–39, 2019.

[May22] Alex May. Complexity and entanglement in non-local computation and holography. *Quantum*, 6:864, November 2022.

[MMWZ96] Markus Michler, Klaus Mattle, Harald Weinfurter, and Anton Zeilinger. Interferometric Bell-state analysis. *Physical Review A*, 53(3):R1209, 1996.

[MPS20] Alex May, Geoff Penington, and Jonathan Sorce. Holographic scattering requires a connected entanglement wedge. *Journal of High Energy Physics*, 2020(8):1–34, 2020.

[MSSM20] Evan Meyer-Scott, Christine Silberhorn, and Alan Migdall. Single-photon sources: Approaching the ideal through multiplexing. *Review of Scientific Instruments*, 91(4):041101, 2020.

[MSY22] Alex May, Jonathan Sorce, and Beni Yoshida. The connected wedge theorem and its consequences. *Journal of High Energy Physics*, 2022(11):1–65, 2022.

[MX24] Alex May and Michelle Xu. Non-local computation and the black hole interior. *Journal of High Energy Physics*, 2024(2):1–50, 2024.

[NC10] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum information.* Cambridge University Press, 2010.

[NFLR21] Dominik Niemietz, Pau Farrera, Stefan Langenfeld, and Gerhard Rempe. Nondestructive detection of photonic qubits. *Nature*, 591(7851):570–574, 2021.

[OCCG20] Andrea Olivo, Ulysse Chabaud, André Chailloux, and Frédéric Grosshans. Breaking simple quantum position verification protocols with little entanglement. *arXiv preprint arXiv:2007.15808*, July 2020.

[Per96] Asher Peres. Separability criterion for density matrices. *Physical Review Letters*, 77(8):1413, 1996.

[PS96] Pavel Pudlák and Jiri Sgall. Algebraic models of computation and interpolation for algebraic proof systems. *Proof complexity and feasible arithmetics*, 39:279–296, 1996.

[QLL$^+$15] Bing Qi, Hoi-Kwong Lo, Charles Ci Wen Lim, George Siopsis, Eric A. Chitambar, Raphael Pooser, Philip G. Evans, and Warren Grice. Free-space reconfigurable quantum key distribution network. *2015 IEEE International Conference on Space Optical Systems and Applications (ICSOS)*, October 2015.

[QR21] Xiao-Liang Qi and Daniel Ranard. Emergent classicality in general multipartite states and channels. *Quantum*, 5:555, 2021.

[QS15] Bing Qi and George Siopsis. Loss-tolerant position-based quantum cryptography. *Phys. Rev. A*, 91:042337, Apr 2015.

[RG15] Jérémy Ribeiro and Frédéric Grosshans. A Tight Lower Bound for the BB84-states Quantum-Position-Verification Protocol. *arXiv:1504.07171 [quant-ph]*, June 2015. arXiv: 1504.07171.

[RNN$^+$20] Dileep V. Reddy, Robert R. Nerem, Sae Woo Nam, Richard P. Mirin, and Varun B. Verma. Superconducting nanowire single-photon detectors with 98% system detection efficiency at 1550nm. *Optica*, 7(12):1649–1653, 2020.

[Sim00] Rajiah Simon. Peres-horodecki separability criterion for continuous variable systems. *Physical Review Letters*, 84(12):2726, 2000.

[SJ09] John M. Senior and M. Yousif Jamro. *Optical fiber communications: principles and practice.* Pearson Education, 2009.

[Spe16a] Florian Speelman. Instantaneous non-local computation of low T-Depth quantum circuits. In *11th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2016)*, volume 61 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 9:1–9:24. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2016.

[Spe16b] Florian Speelman. *Position-based quantum cryptography and catalytic computation.* PhD thesis, University of Amsterdam, 2016. OCLC: 964061686.

[Sus95] Leonard Susskind. The world as a hologram. *Journal of Mathematical Physics*, 36(11):6377–6396, 1995.

[SW02a] Benjamin Schumacher and Michael D Westmoreland. Approximate quantum error correction. *Quantum Information Processing*, 1:5–12, 2002.

[SW02b] Benjamin Schumacher and Michael D Westmoreland. Entanglement and perfect quantum error correction. *Journal of Mathematical Physics*, 43(9):4279–4285, 2002.

[TFKW13] Marco Tomamichel, Serge Fehr, Jędrzej Kaniewski, and Stephanie Wehner. A monogamy-of-entanglement game with applications to device-independent quantum cryptography. *New Journal of Physics*, 15(10):103002, 2013.

[TMB98] Gábor Tardos and David A Mix Barrington. A lower bound on the mod 6 degree of the or function. *Computational Complexity*, 7(2):99–108, 1998.

[Unr14] Dominique Unruh. Quantum Position Verification in the Random Oracle Model. In *Advances in Cryptology – CRYPTO 2014*, pages 1–18. Springer Berlin Heidelberg, 2014.

[VB96] Lieven Vandenberghe and Stephen Boyd. Semidefinite programming. *SIAM review*, 38(1):49–95, 1996.

[VD13] Wim Van Dam. Implausible consequences of superstrong nonlocality. *Natural Computing*, 12:9–12, 2013.

[Wat18] John Watrous. *The Theory of Quantum Information*, page 418. Cambridge University Press, 1 edition, April 2018.

[Wei94] Harald Weinfurter. Experimental Bell-state analysis. *Europhysics Letters*, 25(8):559, 1994.

[Wie83] Stephen Wiesner. Conjugate coding. *ACM Sigact News*, 15(1):78–88, 1983.

[Wil13] Mark M Wilde. *Quantum information theory.* Cambridge University Press, 2013.

[Win99] Andreas Winter. *Coding theorems of quantum information theory.* PhD thesis, Bielefeld University, 1999.

[Wit98] Edward Witten. Anti de sitter space and holography. *Advances in Theoretical and Mathematical Physics*, 2(2):253–291, 1998.

[Wol19] Ronald de Wolf. Quantum Computing: Lecture Notes. *arXiv preprint arXiv:1907.09415*, July 2019.

Abstract

This thesis explores position-based quantum cryptography zooming in on the task of position verification. In position verification, the idea is to use an individual's geographical location as a cryptographic credential. Practically, such protocols can authenticate that a message originated from a specific location or ensure that messages can only be read at a certain location.

In a position-verification protocol, the limitations imposed by the speed of light, as described by special relativity, are used to verify that a party is at their claimed location. This task has been shown to be impossible to implement using only classical information. Initially, the hope was that using quantum information we could construct secure quantum position verification (QPV) protocols. However, it has been shown that any QPV protocol can be broken by attackers that use an amount of entanglement exponential in the input size.

Thus, unconditionally-secure quantum position-verification protocols do not exist. However, from a practical point of view, not all is lost. The exponential upper bound for a general attack is still astronomically large for only a relatively small input. Thus, we can still hope for practically secure QPV protocols. This raises the problem of designing protocols that are secure in a practical setting. An important problem that immediately arises is that of signal loss. Signal loss can be detrimental as it allows attackers to only answer on a subset of rounds.

We propose a new protocol, $\mathrm{QPV}_{\mathsf{SWAP}}$, which is fully loss-tolerant against classical attackers. The task of the protocol, which could be implemented using only a single beam splitter and two detectors, is to estimate the overlap between two input states. By formulating the optimal attack as a semidefinite program (SDP), which we solve analytically, we give optimal bounds on the success probability of attackers and show that the protocol obeys strong parallel repetition.

We then construct the first known example of a QPV protocol that is provably secure against unentangled attackers restricted to classical communication, but can be perfectly attacked by local operations and a single round of simultaneous quantum communication, indicating that allowing for quantum communication

may break security. We then show that any protocol secure against classical communication can be transformed into a protocol secure against quantum communication. We further show, using arguments based on the monogamy of entanglement, that the task of Bell state discrimination cannot be done with only local operations and a single round of simultaneous quantum communication, not even when attackers are allowed to declare a loss, making this the first fully loss-tolerant QPV task secure against quantum communication attacks. We also show that the security of the Bell state discrimination protocol implies similar security for the $\mathrm{QPV}_{\mathsf{SWAP}}$.

An interesting QPV candidate is the $\mathrm{QPV}^{f}_{\mathrm{BB84}}$ protocol, which is a QPV protocol that consists of a single qubit input with classical n-bit strings that determine the measurement basis in which the qubit has to be measured. This protocol has the desirable property that the entanglement needed to attack the protocol scales with the size of the classical information. However, the protocol can be trivially broken for loss rates higher than 50%. We propose a modified structure of QPV protocols by introducing a commitment to play before proceeding, and prove that this modification makes the potentially high transmission loss between the verifiers and the prover security-irrelevant for a class of protocols that includes the $\mathrm{QPV}^{f}_{\mathrm{BB84}}$ protocol. The adapted protocol $\mathsf{c}\text{-}\mathrm{QPV}^{f}_{\mathrm{BB84}}$ then becomes a practically feasible QPV protocol with strong security guarantees, even against attackers using adaptive strategies. As the loss rate between the verifiers and the prover is mainly dictated by the distance between them, secure QPV over longer distances becomes possible. We also show possible feasible implementations of the required photon presence detection, making $\mathsf{c}\text{-}\mathrm{QPV}^{f}_{\mathrm{BB84}}$ a protocol that solves all major practical issues in QPV. It is secure against slow quantum communication and loss, and the prover's operations are relatively simple, since he only needs to manipulate a single qubit and make a classical computation.

We then invert the picture, and consider the task of non-local quantum computation (NLQC), which corresponds to the operations of the attackers in a QPV protocol. We connect NLQC to the wider context of information-theoretic cryptography by relating it to a number of other cryptographic primitives. We show that one special case of NLQC, known as f-routing, is equivalent to the quantum analogue of the conditional disclosure of secrets (CDS) primitive, where by equivalent we mean that a protocol for one task gives a protocol for the other with only small overhead in resource costs. We further consider another special case of position verification, which we call coherent function evaluation (CFE), and show that CFE protocols induce similarly efficient protocols for the private simultaneous message passing (PSM) scenario. By relating position-verification to these cryptographic primitives, a number of results in the information-theoretic cryptography literature give new implications for NLQC, and vice versa. These include the first sub-exponential upper bounds on the worst case cost of f-routing of $2^{O(\sqrt{n \log n})}$ entanglement, the first example of an efficient f-routing strategy for a problem believed to be outside $\mathrm{P}/poly$, linear lower bounds on quantum re-

sources for CDS in the quantum setting, linear lower bounds on communication cost of CFE, and efficient protocols for CDS in the quantum setting for functions that can be computed with quantum circuits of low T depth.

Samenvatting

Dit proefschrift onderzoekt positiegebaseerde quantumcryptografie, met een focus op de taak van positieverificatie. Bij positieverificatie is het idee om de geografische locatie van een individu te gebruiken als een cryptografisch bewijs. In de praktijk kunnen dergelijke protocollen verifiëren dat een bericht afkomstig is van een specifieke locatie, of ervoor zorgen dat berichten alleen op een bepaalde locatie gelezen kunnen worden.

In een positieverificatieprotocol worden de beperkingen die worden opgelegd door de lichtsnelheid, zoals beschreven door de speciale relativiteitstheorie, gebruikt om te verifiëren dat een partij zich op de geclaimde locatie bevindt. Het is gebleken dat deze taak onmogelijk te implementeren is met alleen klassieke informatie. Aanvankelijk was de hoop dat we met behulp van quantuminformatie veilige quantum positieverificatie (QPV) protocollen zouden kunnen construeren. Echter, onderzoek heeft laten zien dat elk QPV-protocol kwetsbaar is voor aanvallers die een hoeveelheid quantumverstrengeling gebruiken die exponentieel is in de grootte van de input.

Onvoorwaardelijk veilige quantum positieverificatieprotocollen bestaan dus niet. Maar, vanuit een praktisch oogpunt is nog niet alles verloren. De exponentiële bovengrens voor een algemene aanval is nog steeds astronomisch groot, zelfs bij een relatief kleine input. Daarom kunnen we nog steeds hopen op praktisch veilige QPV-protocollen. Dit roept het probleem op van het ontwerpen van protocollen die veilig zijn in een praktische omgeving. Een belangrijk probleem dat hier onmiddellijk opduikt, is dat van signaalverlies. Signaalverlies kan schadelijk zijn omdat het aanvallers in staat stelt slechts in een subset van de rondes te antwoorden.

Wij stellen een nieuw protocol voor, genaamd $\mathrm{QPV}_{\mathsf{SWAP}}$, dat volledig verliesveilig is voor klassieke aanvallers. De taak van het protocol, dat kan worden geïmplementeerd met slechts een enkele straalsplitser en twee detectoren, is om de overlap tussen twee inputtoestanden te schatten. Door de optimale aanval te formuleren als een SDP, die we analytisch oplossen, geven we optimale grenzen

aan voor de succeskans van aanvallers, en tonen we aan dat het protocol aan sterke parallelle herhaling voldoet.

We construeren vervolgens het eerste bekende voorbeeld van een QPV-protocol dat aantoonbaar veilig is tegen niet-verstrengelde aanvallers die beperkt zijn tot klassieke communicatie, maar dat perfect kan worden aangevallen door lokale operaties en een enkele ronde van gelijktijdige quantuminformatie, wat aangeeft dat het toestaan van quantuminformatie de veiligheid van het protocol kan breken. Vervolgens tonen we aan dat elk protocol dat veilig is tegen klassieke communicatie kan worden omgezet in een protocol dat veilig is tegen quantuminformatie. Verder tonen we aan, met behulp van argumenten gebaseerd op de monogamie van verstrengeling, dat de taak van het onderscheiden van Bell toestanden niet kan worden uitgevoerd met alleen lokale operaties en een enkele ronde van gelijktijdige quantumcommunicatie, zelfs niet wanneer aanvallers een verlies mogen claimen, waardoor dit de eerste volledig verlies-tolerante QPV-taak is die veilig is tegen quantuminformatie-aanvallen. We tonen ook aan dat de beveiliging van het protocol wat de Bell toestanden onderscheidt een vergelijkbare mate van veiligheid impliceert voor $\mathrm{QPV}_{\mathsf{SWAP}}$.

Een interessante QPV-kandidaat is het $\mathrm{QPV}_{\mathrm{BB84}}^{f}$protocol, een QPV-protocol dat bestaat uit een enkele qubit-input met klassieke n-bit inputstrings die de basis bepalen waarin de qubit moet worden gemeten. Dit protocol heeft de gewenste eigenschap dat de verstrengeling die nodig is om het protocol aan te vallen, schaalt met de grootte van de klassieke informatie. Echter, het protocol kan op triviale wijze worden doorbroken bij verliespercentages hoger dan 50%. Wij stellen een aanpassing in de structuur van QPV-protocollen voor door een toezegging tot deelname in te voeren voordat men verder gaat, en bewijzen dat deze aanpassing het potentieel hoge transmissieverlies tussen de verifiers en de prover beveiligingsirrelevant maakt voor een klasse protocollen die het $\mathrm{QPV}_{\mathrm{BB84}}^{f}$ protocol bevat. Het aangepaste protocol c-$\mathrm{QPV}_{\mathrm{BB84}}^{f}$wordt dan een praktisch haalbaar QPV-protocol met sterke beveiligingsgaranties, zelfs tegen aanvallers die adaptieve strategieën gebruiken. Aangezien het verliespercentage tussen de verifiers en de prover voornamelijk wordt bepaald door de afstand tussen hen, wordt veilige QPV over langere afstanden mogelijk. We tonen ook mogelijke haalbare implementaties van de vereiste aanwezigheidsdetectie van een foton, waardoor c-$\mathrm{QPV}_{\mathrm{BB84}}^{f}$een protocol wordt dat alle belangrijke praktische problemen in QPV oplost. Het is veilig tegen langzame quantuminformatie en verlies, en de operaties van de prover zijn relatief eenvoudig, aangezien hij alleen een enkele qubit hoeft te manipuleren en een klassieke berekening hoeft uit te voeren.

We draaien vervolgens het perspectief om en beschouwen de taak van niet-lokale quantumcomputatie (NLQC), wat overeenkomt met de operaties van de aanvallers in een QPV-protocol. We verbinden NLQC met de bredere context van informatie-theoretische cryptografie door het te relateren aan een aantal andere cryptografische basistaken. We laten zien dat een speciaal geval van NLQC, bekend als f-routing, equivalent is aan de quantum-versie van de *voorwaardelijke onthulling van geheimen* (CDS) taak, waarbij equivalent betekent dat een protocol voor de ene taak een protocol voor de andere taak oplevert met slechts een kleine overhead in resourcekosten. We beschouwen verder een ander speciaal geval van positieverificatie, dat we coherente functie-evaluering (CFE) noemen, en tonen aan dat CFE-protocollen op vergelijkbare wijze efficiënte protocollen induceren voor het scenario van private gelijktijdige berichtuitwisseling (PSM). Door positieverificatie te relateren aan deze cryptografische primitieve taken, geven een aantal resultaten in de informatie-theoretische cryptografie nieuwe implicaties voor NLQC, en vice versa. Deze omvatten de eerste sub-exponentiële bovengrenzen op de ergste gevalskosten van f-routing van $2^{O(\sqrt{n \log n})}$ verstrengelde deeltjes, het eerste voorbeeld van een efficiënte f-routing strategie voor een probleem waarvan men denkt dat het buiten $P/poly$ ligt, lineaire ondergrenzen voor quantumresources voor CDS in de quantumsetting, lineaire ondergrenzen voor de communicatiekosten van CFE, en efficiënte protocollen voor CDS in de quantumsetting voor functies die kunnen worden berekend met quantumcircuits van beperkte T-diepte.

Acknowledgments

First, I would like to express my deep gratitude to my supervisors, Harry Buhrman and Florian Speelman, for providing me with the opportunity to do this PhD, and introducing me to the very interesting fields of position verification and non-local quantum computation. Most of the beginning of my PhD was during the covid pandemic, and I am happy we could regularly meet online. This also made us venture in a different direction than initially thought, but I'm very excited about where we ended up. Sitting on the couches till very late and thinking about our problems was something I really enjoyed doing.

I want to thank my committee members, namely Adrian Kent, Wolfgang Löffler, Maris Ozols, Christian Schaffner, and Ronald de Wolf, for their time and valuable feedback on this thesis.

A big thanks goes out to all my co-authors, Alex, Andreas, Arpan, Boris, Dennis, Dmitri, Eric, Florian, Harry, Ian, Ion, Jordi, Llorenç, Maris, Matthias, and Rene. I want to especially thank Rene for all the work we have done and time we have spent together. I am very glad it turned out this way.

I would also like to thank everyone at QuSoft for providing an excellent and stimulating environment for doing research.

This all was not possible without the help and support of all my friends. Thanks to my sailing team and skipper Hille on the skûtsje De Tiid Sil't Leare for the fun times during my PhD and the IFKS in summer. Thanks to my roommates, Bruno, Govert and Jurriaan, with whom I spend the lockdown times. And thanks to my family for being there for me.

I want to thank Rene and Oliver for being my paranymphs.

Finally, I would like to thank Galina for the amazing 3 years together.

Titles in the ILLC Dissertation Series:

ILLC DS-2020-01: **Mostafa Dehghani**
Learning with Imperfect Supervision for Language Understanding

ILLC DS-2020-02: **Koen Groenland**
Quantum protocols for few-qubit devices

ILLC DS-2020-03: **Jouke Witteveen**
Parameterized Analysis of Complexity

ILLC DS-2020-04: **Joran van Apeldoorn**
A Quantum View on Convex Optimization

ILLC DS-2020-05: **Tom Bannink**
Quantum and stochastic processes

ILLC DS-2020-06: **Dieuwke Hupkes**
Hierarchy and interpretability in neural models of language processing

ILLC DS-2020-07: **Ana Lucia Vargas Sandoval**
On the Path to the Truth: Logical & Computational Aspects of Learning

ILLC DS-2020-08: **Philip Schulz**
Latent Variable Models for Machine Translation and How to Learn Them

ILLC DS-2020-09: **Jasmijn Bastings**
A Tale of Two Sequences: Interpretable and Linguistically-Informed Deep Learning for Natural Language Processing

ILLC DS-2020-10: **Arnold Kochari**
Perceiving and communicating magnitudes: Behavioral and electrophysiological studies

ILLC DS-2020-11: **Marco Del Tredici**
Linguistic Variation in Online Communities: A Computational Perspective

ILLC DS-2020-12: **Bastiaan van der Weij**
Experienced listeners: Modeling the influence of long-term musical exposure on rhythm perception

ILLC DS-2020-13: **Thom van Gessel**
Questions in Context

ILLC DS-2020-14: **Gianluca Grilletti**
Questions & Quantification: A study of first order inquisitive logic

ILLC DS-2020-15: **Tom Schoonen**
Tales of Similarity and Imagination. A modest epistemology of possibility

ILLC DS-2020-16: **Ilaria Canavotto**
Where Responsibility Takes You: Logics of Agency, Counterfactuals and Norms

ILLC DS-2020-17: **Francesca Zaffora Blando**
Patterns and Probabilities: A Study in Algorithmic Randomness and Computable Learning

ILLC DS-2021-01: **Yfke Dulek**
Delegated and Distributed Quantum Computation

ILLC DS-2021-02: **Elbert J. Booij**
The Things Before Us: On What it Is to Be an Object

ILLC DS-2021-03: **Seyyed Hadi Hashemi**
Modeling Users Interacting with Smart Devices

ILLC DS-2021-04: **Sophie Arnoult**
Adjunction in Hierarchical Phrase-Based Translation

ILLC DS-2021-05: **Cian Guilfoyle Chartier**
A Pragmatic Defense of Logical Pluralism

ILLC DS-2021-06: **Zoi Terzopoulou**
Collective Decisions with Incomplete Individual Opinions

ILLC DS-2021-07: **Anthia Solaki**
Logical Models for Bounded Reasoners

ILLC DS-2021-08: **Michael Sejr Schlichtkrull**
Incorporating Structure into Neural Models for Language Processing

ILLC DS-2021-09: **Taichi Uemura**
Abstract and Concrete Type Theories

ILLC DS-2021-10: **Levin Hornischer**
Dynamical Systems via Domains: Toward a Unified Foundation of Symbolic and Non-symbolic Computation

ILLC DS-2021-11: **Sirin Botan**
Strategyproof Social Choice for Restricted Domains

ILLC DS-2021-12: **Michael Cohen**
Dynamic Introspection

ILLC DS-2021-13: **Dazhu Li**
Formal Threads in the Social Fabric: Studies in the Logical Dynamics of Multi-Agent Interaction

ILLC DS-2021-14: **Álvaro Piedrafita**
On Span Programs and Quantum Algorithms

ILLC DS-2022-01: **Anna Bellomo**
Sums, Numbers and Infinity: Collections in Bolzano's Mathematics and Philosophy

ILLC DS-2022-02: **Jan Czajkowski**
Post-Quantum Security of Hash Functions

ILLC DS-2022-03: **Sonia Ramotowska**
Quantifying quantifier representations: Experimental studies, computational modeling, and individual differences

ILLC DS-2022-04: **Ruben Brokkelkamp**
How Close Does It Get?: From Near-Optimal Network Algorithms to Suboptimal Equilibrium Outcomes

ILLC DS-2022-05: **Lwenn Bussière-Carae**
No means No! Speech Acts in Conflict

ILLC DS-2022-06: **Emma Mojet**
Observing Disciplines: Data Practices In and Between Disciplines in the 19th and Early 20th Centuries

ILLC DS-2022-07: **Freek Gerrit Witteveen**
Quantum information theory and many-body physics

ILLC DS-2023-01: **Subhasree Patro**
Quantum Fine-Grained Complexity

ILLC DS-2023-02: **Arjan Cornelissen**
Quantum multivariate estimation and span program algorithms

ILLC DS-2023-03: **Robert Paßmann**
Logical Structure of Constructive Set Theories

ILLC DS-2023-04: **Samira Abnar**
Inductive Biases for Learning Natural Language

ILLC DS-2023-05: **Dean McHugh**
Causation and Modality: Models and Meanings

ILLC DS-2023-06: **Jialiang Yan**
Monotonicity in Intensional Contexts: Weakening and: Pragmatic Effects under Modals and Attitudes

ILLC DS-2023-07: **Yiyan Wang**
Collective Agency: From Philosophical and Logical Perspectives

ILLC DS-2023-08: **Lei Li**
Games, Boards and Play: A Logical Perspective

ILLC DS-2023-09: **Simon Rey**
Variations on Participatory Budgeting

ILLC DS-2023-10: **Mario Giulianelli**
Neural Models of Language Use: Studies of Language Comprehension and Production in Context

ILLC DS-2023-11: **Guillermo Menéndez Turata**
Cyclic Proof Systems for Modal Fixpoint Logics

ILLC DS-2023-12: **Ned J.H. Wontner**
Views From a Peak: Generalisations and Descriptive Set Theory

ILLC DS-2024-01: **Jan Rooduijn**
Fragments and Frame Classes: Towards a Uniform Proof Theory for Modal Fixed Point Logics

ILLC DS-2024-02: **Bas Cornelissen**
Measuring musics: Notes on modes, motifs, and melodies

ILLC DS-2024-03: **Nicola De Cao**
Entity Centric Neural Models for Natural Language Processing

ILLC DS-2024-04: **Ece Takmaz**
Visual and Linguistic Processes in Deep Neural Networks: A Cognitive Perspective

ILLC DS-2024-05: **Fatemeh Seifan**
Coalgebraic fixpoint logic Expressivity and completeness result

ILLC DS-2024-06: **Jana Sotáková**
Isogenies and Cryptography

ILLC DS-2024-07: **Marco Degano**
Indefinites and their values