Position-based Quantum Cryptography: From Theory towards Practice

René Allerstorfer

Position-based Quantum Cryptography: From Theory towards Practice

René Allerstorfer

Position-based Quantum Cryptography: From Theory towards Practice

ILLC Dissertation Series DS-2024-09

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 research in this dissertation was supported by the Dutch Research Council (NWO/OCW), as part of the Quantum Software Consortium program with project number 024.003.037.

Cover design by René Allerstorfer.
Printed and bound by Ipskamp Printing.

ISBN: 978-94-6473-578-9

Position-based Quantum Cryptography: From Theory towards Practice

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 maandag 28 oktober 2024, te 14.00 uur

door René Allerstorfer
geboren te Linz

Promotiecommissie

Promotor:	prof. dr. H.M. Buhrman	Universiteit van Amsterdam
Copromotor:	dr. F. Speelman	Universiteit van Amsterdam
Overige leden:	prof. dr. C. Schaffner	Universiteit van Amsterdam
	dr. W. Löffler	Universiteit Leiden
	prof. dr. C.J.M. Schoutens	Universiteit van Amsterdam
	prof. dr. M. Christandl	University of Copenhagen
	prof. dr. F.E. Schreck	Universiteit van Amsterdam

Faculteit der Natuurwetenschappen, Wiskunde en Informatica

This dissertation is based on the following articles. Co-authorship is shared equally and authors are ordered alphabetically, unless otherwise stated. For the work [GALC23], the principal author is listed first.

1. [ABSV21] Rene Allerstorfer, Harry Buhrman, Florian Speelman, and Philip Verduyn Lunel. Towards practical and error-robust quantum position verification. *arXiv preprint*, 2021. arXiv:2106.12911

2. [ABSV22] 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*, 2022. arXiv:2311.00677. *To appear in Quantum.*

3. [GALC23] Ian George, Rene Allerstorfer, Philip Verduyn Lunel, and Eric Chitambar. Time-constrained local quantum state discrimination. *arXiv preprint*, 2023. arXiv:2311.00677.

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*, 2023. arXiv:2312.12614. *Contributed talk at QIP 2024. Contributed talk at QCRYPT 2024.*

5. [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*, 2023. arXiv:2308.04166.

In addition, the author has co-authored the following articles, which are not included in this dissertation.

6. [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. doi:10.22331/q-2024-06-27-1387. *Contributed talk at QIP 2024. Invited plenary talk at QCRYPT 2024.*

7. [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*, 2023. arXiv:2309.16655. *Contributed talk at QIP 2024.*

8. [AEFR+24] Rene Allerstorfer, Llorenç Escolà-Farràs, Arpan Akash Ray, Boris Škorić, and Florian Speelman. Continuous-variable quantum position verification secure against entangled attackers. *arXiv preprint*, 2024. arXiv:2404.14261

Contents

Acknowledgments

First, I would like to thank my supervisor Harry and co-supervisor Florian for their guidance, patience and for all the opportunities you provided me with throughout the years. Thank you for fostering a relaxed, yet very productive research environment.

I also thank my committee members Matthias Christandl, Wolfgang Löffler, Christian Schaffner, Kareljan Schoutens and Florian Schreck for their time and feedback.

Then I want to extend my gratitude to all my collaborators. To all of them for countless hours of meeting, brainstorming and pushing projects and ideas forward. Thank you Alex for organising a great workshop in Waterloo and for your hospitality during it. Thanks to Eric for hosting us generously for a week of research in Urbana-Champaign. Happy to see that a whole paper emerged from that visit, together with Ian whom I thank for taking an active role in it. Thank you to Dmitry for being a great office mate for some time and for the rigour and endless curiosity you do research with. It was very fun when you, Philip and I were trying to find structure and counterexamples, sometimes way too late in the evening, in the problem that became our paper together with Denis, Ion, Maris and Matthias. Thank you Matthias for careful readings of manuscripts and for giving thoughtful suggestions. Thank you Arpan and Boris for teaching me a lot about the continuous-variable formalism in quantum mechanics. Special thanks also to Andreas for your contributions and careful feedback to our paper, and for pushing us to a great level of detail in our analysis. Finally, many thanks to Llorenç for being an overall great colleague.

Also many thanks to Wolfgang and Kirsten, and also Petr, for our collaboration and for teaching me a lot about linear optics and single photons.

Philip, you deserve your own paragraph. A massive dankjewel to you for everything over the years. For being a great, enthusiastic and supportive colleague and friend. For helping me so much with all things Netherlands. For educating me on Dutch history and culture. For helping me find an apartment and move.

And much more. We share many interests and complemented each other very well in our work, I think, looking at our many papers together. I thoroughly enjoyed working together and the support we gave each other throughout the last few years.

On to my second paranymph, Adam. I want to deeply thank you for your empathy and support in some difficult times during my PhD. Thank you also for being a great travel companion. I hope we will share many more cycles, hikes and swims from time to time.

QuSoft would not be such a fantastic place to do research at without the great bunch of colleagues there. Thank you Adam, Ailsa, Akshay, Amira, Arie, Arjan, Chris, Chris, Daan, Davi, Dmitry, Dyon, Farokh, Filippo, Florian, Fran, Francesco, Freek, Galina, Garazi, Gina, Harold, Harry, Ido, Jana, Jelena, Jeroen, John, Jonas, Jop, Joran, Jordi, Kareljan, Koen, Koen, Leo, Llorenç, Luca, Ludovico, Lynn, Marten, Manideep, Maris, Maxim, Mehrdad, Michael, Niels, Nikhil, Peter, Philip, Poojith, Quinten, Randy, Ronald, Salvatore, Sarah, Sebastian, Seenivasan, Stacey, Subha, Victor, Yanlin, Yaroslav, and to the QuSoft visitors Kfir and Markus, and everyone I forgot to name, for making the time over the last years at QuSoft so enjoyable, both in- and outside of CWI.

Special appreciation goes to my longer-term regular office mates Amira, Dmitry, Philip, Quinten and Yaroslav. Thank you for all your helpful advice and support towards the end of my PhD, Amira. I always enjoyed our occasional out-of-the-box discussions Quinten. I really enjoyed working together and the couple days we spent together in beautiful Catalonia, Llorenç. Thank you, Yanlin, for taking us to a Taipei night market and your magic bar. Thank you to the travel crews over the years (you know who you are) for creating unforgettable memories together. Thanks also to the great colleagues at QSC for stimulating discussions and good times at QSC events.

I've also always been grateful for the support of the CWI and QSC staff, making working at CWI and being part of QSC a smooth experience. In particular, thank you to Doutzen and Susanne. You always made me feel welcomed and cared for.

I want to thank Emma for the time we shared during part of my PhD and extend gratitude to Dan, Fiona and Sophie for their warmth, support and memories that I cherish.

And not to forget all the people along the way. You know who you are. Thank you to my friends I grew up with from my small village for everlasting friendships, no matter how far we might be separated for now, and for being a grounding balance to the highbrow world. To the Vienna 5th floor crew, laying the foundation for the last few years and having fun along the way. Special thanks to Felix for staying in touch regularly, always interesting conversations and our supportive friendship. To the Oxford college and sports crews and lockdown family of Regent Street that formed in winter 2020/21. And to my group outside the bubble of academia here in Amsterdam.

Finally, I want to thank my family for supporting and cheering for me from a distance, for enabling me to take the road I took and for their unwavering support, no matter what is needed. Thanks to my siblings for an amazing trip in summer 2023 and countless phone calls, meme sharing and our unique connection.

Off to new adventures.

Chapter 1

Introduction

What if I told you that the money in your accounts will not be safe anymore next week? Or that your messages or health data will be public? What would you do? Now imagine that millions of other people do the same. The result could be local or even global disruption. With the advent of quantum computing, questions like these become increasingly urgent. Large-scale functioning quantum computers are able to break widely used asymmetric encryption schemes, and quantum-secure cryptography aims to prevent such threats. Hence, there is a pressing need to research quantum-secure cryptography. There are two possible avenues to this: classical cryptography that is secure against quantum attacks (post-quantum cryptography) and cryptography that actively uses quantum information to achieve security (quantum cryptography). This thesis sits in the realm of quantum cryptography.

But first, what is the fuss about 'quantum'? Quantum theory is arguably the most profound theory of nature we have come up with so far and aims to describe the fundamental interactions of matter – with astounding success over the past century. It is, however, beyond the scope of this thesis to discuss the equally old and fascinating debate about what this theory 'means'. Many different arguments and interpretations have been proposed, some claiming that quantum theory is *the* theory of processing information under reasonable axioms [Har01, CDP11, Har11, MMAPG13], giving theoretical foundation to the idea that 'information is physical' [Lan91].

The focus of this work will be more on what it enables us to do in certain areas, specifically in cryptography.

But why is there even a need for quantum theory? And how do you even come up with a theory that is so counterintuitive and whose interpretation still puzzles us more than 100 years after its first inception? Again, many books can be written aiming to partially answer these questions. We will just briefly comment a few sentences on this.

It is an established fact by now that classical physics cannot accurately pre-

dict all observed phenomena, particularly not on an atomic and subatomic scale. Quantum theory started with Planck's law, for the first time accurately describing black-body radiation by introducing the idea that the energy of electromagnetic radiation is fundamentally made up of discrete packets, or 'quanta', thereby giving birth to the idea of the photon. This idea shook the foundation of theoretical physics and in the following decades a new theory of matter – quantum theory – was developed, revamping our understanding of nature at a fundamental level. Some time later, in the 1960s, John Bell delivered the final blow to the classical understanding of our world by proposing a testable inequality that could show that our world *cannot be* classical in the sense of being governed by a local realistic hidden variable theory [Bel64]. And indeed, another few decades later it was demonstrated in a loophole-free way that nature violates Bell's inequality, and therefore our intuitive classical understanding of the world is fundamentally not true [HBD+15]. In some sense, however, one can argue that quantum theory is more natural than classical theory, because it actually takes into account the observer[1], rather than giving a Platonic observer-independent theory of nature. And after all, observers are part of nature and must be accounted for in a proper theory of nature.

Since the inception of quantum theory, its crucial differences to the classical worldview have been distilled, of which some of the most prominent are: the existence of non-commuting observables (which leads to the uncertainty principle), the existence of pure superposition states (rejecting classical definiteness, and leading to interference phenomena), the existence of entangled states (which lead to stronger-than-classical correlations between events) and the existence of randomness as a fundamental feature of nature (which leads to true random numbers). Moreover, quantum states can constructively *and* destructively interfere and observing a quantum system can change its state.

Quantum theory has already changed our world by enabling a comprehensive understanding of semiconductors and the invention of the transistor, which are the backbone of all modern technology. In this sense, it has already enabled the information age we live in on a physical level, even though on a mathematical level current technology has not leveraged it for information processing yet. But this appears to be changing, and we may be on the brink of entering the quantum information age. Research on quantum information theory and practice since the 1980s has been very fruitful, and we are able to build (very) small-scale quantum computers and quantum networks today.

But what are they good for? This is still unclear to some degree, but potential applications are sometimes modest polynomial, sometimes drastic exponential, speedups for certain algorithms solving specific problems. Such speedups may lead to efficiency and productivity gains, or even allow to solve problems that

[1] Although it is not fully understood yet, and the measurement problem is one of the central conceptual difficulties in quantum theory.

are simply too hard for classical computers to solve. At this point, much is still speculative, but giving us the ability to solve certain problems that are intractable for any current or future classical computer could lead to significant advances in the fields where quantum computing is applicable, like material science or simulating life processes. Equally important, it may lead to purely scientific advances in our understanding of nature by allowing us to simulate quantum systems natively using quantum computers.

Another large space for applications, and related to the topic of this thesis, is quantum cryptography. It is enabled by the aforementioned central properties of quantum mechanics that differentiate it from classical theory from an information-theoretic point of view. For example, the security of quantum key distribution (QKD) can be intuitively understood from several such angles and unconditional and everlasting security for QKD can be proven [BB84, TL17]. Furthermore, quantum mechanics enables completely new primitives that are classically not possible, one of which will be the topic of this thesis: position-based quantum cryptography.

The primary principle enabling position-based quantum cryptography is that of no-cloning, and stronger-than-classical correlations are also frequently used. Unknown quantum information cannot be copied perfectly, in contrast to the classical data our computers copy every day all day. This property crucially prevents the attack based on copying the input information to which any classical position verification protocol is vulnerable. As described extensively throughout this thesis, from that, and together with the constraint that the speed of light is finite, one can build protocols that allow for (somewhat) secure position verification of an untrusted party without any extra cryptographic credentials like a key, a shared secret or a previous interaction. What this means is detailed in the review in Chapter 3, and a summary of our results can be found in the abstract at the end of this thesis.

With quantum computers steadily progressing, securing our data against quantum attacks has high priority, and in order to prevent disruption we better have quantum-secure cryptography in place before a cryptographically relevant quantum computer exists. Making a contribution to this effort, and improving our understanding of fundamental aspects of quantum theory, have been the main goals of the research in this thesis.

Chapter 2

Preliminaries

In this chapter we lay the plumbing for this dissertation. We will focus on standard finite-dimensional Hilbert space quantum theory[1]. Familiarity with the quantum information formalism, and graduate-level maturity in mathematics are assumed. The tools we introduce are standard and can mostly be found, for example, in [NC10, Wat18].

We start with some basic definitions. An *inner product* induces a geometry in a vector space. The *standard inner product* for two vectors is defined by $\langle u, v\rangle \coloneqq \sum_i u_i^* v_i$. For linear operators, it is called the *Hilbert Schmidt inner product* and is defined by $\langle M, N\rangle \coloneqq \mathrm{Tr}\big[M^\dagger N\big]$. A norm is a function that generalises measuring the length of an object. By measuring the length of a difference, it can also calculate distances between objects. The *p-norm* of a vector is given by $\|v\|_p \coloneqq (\sum_i v_i^p)^{\frac{1}{p}}$. The *Schatten p-norm* of a linear operator M is defined as $\|M\|_p \coloneqq \mathrm{Tr}\big[(M^\dagger M)^{\frac{p}{2}}\big]^{\frac{1}{p}}$.

An important norm inequality for linear operators is *Hölder's inequality*, which reads $|\langle M, N\rangle| \leq \|M\|_p \|N\|_{p_*}$ with $1/p + 1/p_* = 1$. An inner product canonically induces a norm function, the 2-norm. Vector spaces equipped with an inner product, and thus a norm, are called *inner product spaces* and complete inner product spaces are called *Hilbert spaces*, commonly denoted by $\mathcal{H}$. Those spaces are the playground of quantum mechanics.

2.1 Quantum information theory tools

In this section, we introduce some basic tools to deal with quantum information, as needed throughout this thesis. First, we will talk about the fundamental objects: quantum states and quantum channels.

[1] Many of the things we introduce in this chapter could be formulated more generally or, at times, more rigorously, but that is not the point here. We would like to keep things simple and clear for the start.

Quantum states

Let $\mathcal{H}$, $\mathcal{H}'$ be finite-dimensional Hilbert spaces. *Isometries* V are linear maps from $\mathcal{H}$ to $\mathcal{H}'$ that preserve the geometry of the space (i.e. inner products) and thus fulfil $V^\dagger V = \mathbb{1}_{\mathcal{H}}$. *Unitaries* are isometries with $\dim \mathcal{H}' = \dim \mathcal{H}$ and thus $UU^\dagger = U^\dagger U = \mathbb{1}$. We denote the set of unitaries acting on a Hilbert space $\mathcal{H}$ by $\mathcal{U}(\mathcal{H})$ or just $\mathcal{U}$ if the Hilbert space is clear from the context. Denote by $\mathrm{D}(\mathcal{H})$ the set of *quantum states* on $\mathcal{H}$, which is defined as $\mathrm{D}(\mathcal{H}) \coloneqq \{\rho \succeq 0 \mid \mathrm{Tr}[\rho] = 1\}$. The operator defining a quantum state is called *density matrix* and to indicate the registers it lives on we often write ρ_{AB} or ρ^{AB}. If the density matrix of a state ρ has rank one, then it is a *pure state* and can be written as a projector onto a state vector $|\psi\rangle \in \mathcal{H}$, i.e. $\rho = |\psi\rangle\langle\psi|$. If it has rank higher than one, ρ is called a *mixed state*. If a multipartite quantum state can be decomposed into smaller ones as $\rho_{AB} = \rho_A \otimes \rho_B$ we call it a *product state*, if it is a mixture of product states we call it *separable*, otherwise it is an *entangled state*.

Relating quantum states

An important measure of distance between quantum states is the *trace distance*.

2.1.1. Definition. The trace distance between two quantum states ρ, σ is defined as

$$D_{\mathrm{tr}}(\rho, \sigma) \coloneqq \frac{1}{2}\|\rho - \sigma\|_1. \tag{2.1}$$

For pure states $|\phi\rangle, |\psi\rangle$ this reduces to $D_{\mathrm{tr}}(|\phi\rangle\langle\phi|, |\psi\rangle\langle\psi|) = \sqrt{1 - |\langle\phi|\psi\rangle|^2}$. Furthermore, the trace distance can be obtained variationally by optimising over unitaries U in

$$D_{\mathrm{tr}}(\rho, \sigma) = \max_{U \in \mathcal{U}} \frac{1}{2}\Big|\,\mathrm{Tr}[U(\rho - \sigma)]\Big|. \tag{2.2}$$

Likewise, one can think about the similarity of quantum states. This is quantified by the *fidelity*.

2.1.2. Definition. The fidelity between two quantum states ρ, σ is defined as

$$F(\rho, \sigma) \coloneqq \|\sqrt{\rho}\sqrt{\sigma}\|_1 = \mathrm{Tr}\left[\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}}\right]. \tag{2.3}$$

For pure states $|\phi\rangle, |\psi\rangle$ this reduces to $F(\phi, \psi) \coloneqq F(|\phi\rangle\langle\phi|, |\psi\rangle\langle\psi|) = |\langle\phi|\psi\rangle|$ and, moreover, $F(\rho, |\psi\rangle\langle\psi|) = \sqrt{\langle\psi|\rho|\psi\rangle}$.

The fidelity function has a nice composition property for product states. For quantum states $\rho_0 \otimes \rho_1, \sigma_0 \otimes \sigma_1$ we have $F(\rho_0 \otimes \rho_1, \sigma_0 \otimes \sigma_1) = F(\rho_0, \sigma_0)F(\rho_1, \sigma_1)$. The *Fuchs-van de Graaf* inequalities relate the fidelity and the trace distance.

2.1.3. PROPOSITION. *For any quantum states ρ, σ the trace distance and fidelity are related by*

$$1 - F(\rho,\sigma) \leq D_{\mathrm{tr}}(\rho,\sigma) \leq \sqrt{1 - F(\rho,\sigma)^2}. \tag{2.4}$$

It is a consequence of the quantum formalism that any mixed quantum state ρ_A of a system A can be regarded as a pure state $|\psi\rangle\langle\psi|_{AB}$ of a larger system AB. Then we say that $|\psi\rangle_{AB}$ is a *purification* of ρ_A, and they must be related by $\mathrm{Tr}_B[|\psi\rangle\langle\psi|_{AB}] = \rho_A$. Often we are not interested in the detailed structure of system B and call it a reference system or the environment. This property could, at first sight, be regarded as inconspicuous, but appears to be the defining property that separates quantum theory from other reasonable probabilistic theories of information processing [CDP11].

The purification of a state is not unique, but any two purifications of a state are related by a local unitary acting on the environment.

2.1.4. LEMMA. *Let $|\psi\rangle_{AB}, |\phi\rangle_{AB}$ be two purifications of ρ_A, which means we have $\mathrm{Tr}_B[|\psi\rangle\langle\psi|_{AB}] = \rho_A = \mathrm{Tr}_B[|\phi\rangle\langle\phi|_{AB}]$. Then there exists a unitary on system B such that $|\phi\rangle_{AB} = \mathbb{1} \otimes U\, |\psi\rangle_{AB}$.*

This unitary equivalence of purifications can be used to prove Uhlmann's theorem, which characterises the fidelity in terms of an inner product of purifications.

2.1.5. THEOREM. (Uhlmann) *For quantum states ρ_A, σ_A it holds that*

$$F(\rho_A,\sigma_A) = \max_{|\phi\rangle_{AB},|\psi\rangle_{AB}} F(\phi_{AB},\psi_{AB}) = \max_{|\phi\rangle_{AB},|\psi\rangle_{AB}} |\langle\phi|\psi\rangle|, \tag{2.5}$$

where the optimisation runs over all purifications $|\phi\rangle_{AB}, |\psi\rangle_{AB}$ of ρ_A, σ_A, respectively. By Lemma 2.1.4, this can be restated as

$$F(\rho_A,\sigma_A) = \max_{U\in\mathcal{U}} |\langle\phi_\star|\mathbb{1} \otimes U|\psi_\star\rangle|, \tag{2.6}$$

where $|\phi_\star\rangle_{AB}, |\psi_\star\rangle_{AB}$ are some fixed purifications.

Bell states

Bell states are one of the most special families of states, because they are maximally entangled. They have many interesting properties. Too many to list here, so we will just introduce them. The qubit Bell states are

$$\begin{aligned}
|\Phi_+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),\\
|\Phi_-\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle),\\
|\Psi_+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle),\\
|\Psi_-\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).
\end{aligned} \tag{2.7}$$

They can all be generated by acting locally on $|\Phi_+\rangle$ as follows. Define $|\Phi_{ij}\rangle$, where $i \in \{0,1\}$ denotes the parity bit (whether the state is Φ or Ψ) and $j \in \{0,1\}$ denotes the phase bit (whether the phase is $+$ or $-$). Then $|\Phi_{ij}\rangle = \mathbb{1} \otimes X^i Z^j |\Phi_+\rangle$, where X, Z are two of the well-known Pauli matrices. The state $|\Phi_+\rangle$ can be generated by acting on $|00\rangle$ with $\mathrm{CNOT}(H \otimes \mathbb{1})$. They are similarly defined for higher local dimension.

Quantifying entanglement

We can quantify the entanglement of quantum states using *entanglement measures*, which are functions from $\mathrm{D}(\mathcal{H})$ to $\mathbb{R}_{\geq 0}$. Any good entanglement measure E should fulfil at least points 1., 2. and 4. of the following properties [PV07]:

1. E should evaluate to 1 on maximally entangled qubit states, or $\log d$ if the local dimension is d. So $E(\rho_{AB}) = \log d$ if ρ_{AB} is maximally entangled.

2. E should evaluate to 0 on separable states. So $E(\rho_{AB}) = 0$ if we have the form $\rho_{AB} = \sum_i p_i \rho_A^i \otimes \rho_B^i$ for a probability distribution $\{p_i\}_i$.

3. E does not increase on average under local operations and classical communication (LOCC) channels applied to ρ_{AB}. This property is called *LOCC monotonicity*.

4. For a pure state $|\psi\rangle\langle\psi|_{AB}$ it reduces to the entropy of entanglement, i.e. $E(|\psi\rangle\langle\psi|_{AB}) = H(\rho_A) = H(\rho_B)$.

A function that fulfils the first three properties is called an *entanglement monotone*. Entanglement has another intriguing property: it is *monogamous*. That is, if a system A is maximally entangled with system B of the same dimension, then neither of them can be entangled to anything else. Formally, it can be expressed by the inequality

$$E(\rho_{AB}) + E(\rho_{AC}) \leq E(\rho_{A|BC}), \tag{2.8}$$

where $E(\rho_{A|BC})$ denotes the entanglement across the partition $A|BC$. This can be generalised to more subsystems.

There are many entanglement measures, each with different interpretations, for example the entanglement of formation E_F, the squashed entanglement E_{sq} or the distillable entanglement E_D. For a review on the subject we refer to [PV07]. Curiously, not many fulfil all the properties we would like to have, and sometimes it is not known if they do in all generality. Whereas for pure states one can often use the entropy of entanglement, computing the entanglement (or even just checking whether it is entangled or not) for a general mixed state is hard.

Entropy

Entropy in the mathematical sense is a measure of how surprised one is on average about the value of a random variable X (or state of a mixed quantum state ρ), measured in bits. If one knows the value exactly, there is no surprisal at all and if one has no information whatsoever, the surprisal will be maximal. In that sense, entropy quantifies the uncertainty one has about the state of a random variable. The most prominent example is the *Shannon entropy* for random variables, or the analogous *von Neumann entropy* for quantum states.

2.1.6. Definition. The Shannon entropy of a random variable X, which takes values $x \in \mathcal{X}$ with probability $p(x)$, is defined as

$$H(X) \coloneqq -\sum_{x\in\mathcal{X}} p(x)\log p(x). \tag{2.9}$$

We see that $0 \leq H(X) \leq \log|\mathcal{X}|$. The von Neumann entropy of a quantum state ρ is defined as

$$H(\rho) \coloneqq -\operatorname{Tr}[\rho\log\rho]. \tag{2.10}$$

Often $H(\rho_A)$ is written as $H(A)_\rho$ and sometimes the von Neumann entropy is also denoted by $S(\rho)$. Again, we have $0 \leq H(\rho) \leq \log d$, with d the dimension of ρ. Moreover, from the formula with the trace it is clear that $H(\rho)$ reduces to the Shannon entropy of the eigenvalues $\{\lambda_j\}_j$ of ρ.

Many entropic quantities can be encapsulated by the definition of *Rényi entropies*.

2.1.7. Definition. The Rényi entropy of order $\alpha \in (0,1)\cup(1,\infty)$, and the corresponding limits for the edge cases, is defined as

$$H_\alpha(X) \coloneqq \frac{1}{1-\alpha}\log\left(\sum_{x\in\mathcal{X}} p(x)^\alpha\right). \tag{2.11}$$

The limit $\alpha \to 1$ corresponds to the Shannon entropy $H(X)$, $\alpha \to \infty$ to the min-entropy $H_{\min}$ and $\alpha = 1/2$ to the max-entropy $H_{\max}$. The quantum Rényi entropy of order α of a quantum state $\rho \in \mathrm{D}(\mathcal{H})$ is analogously defined by

$$H_\alpha(\rho) \coloneqq \frac{1}{1-\alpha}\log\operatorname{Tr}[\rho^\alpha]. \tag{2.12}$$

Similarly, the case $\alpha \to 1$ recovers the von Neumann entropy.

Of course, having side information may affect how uncertain one is about the value of X or the state of ρ. If I know $X \in \{0,1\}$ and have side information that X is odd, then I know with certainty that $X = 1$. The *conditional entropy*, or in general *conditional Rényi entropies*, quantify this.

2.1.8. Definition. The conditional entropy given a state ρ_{AB} is defined as

$$H(A|B)_\rho \coloneqq H(AB)_\rho - H(B)_\rho. \tag{2.13}$$

More general Rényi conditional entropies are commonly expressed in terms of quantities that relate two probability distributions (or quantum states), called *divergences*.

2.1.9. Definition. (e.g. [CBTW17]) The quantum Rényi divergence of order $\alpha \in [1/2, 1) \cup (1, \infty)$, and the corresponding limits for the edge cases, is defined as

$$D_\alpha(\rho\|\sigma) \coloneqq \frac{1}{\alpha - 1} \log \mathrm{Tr}\Big[\Big(\sigma^{\frac{1-\alpha}{2\alpha}} \rho \sigma^{\frac{1-\alpha}{2\alpha}}\Big)^\alpha\Big], \tag{2.14}$$

and ∞ if ρ has support outside of the support of σ. The general Rényi conditional entropy of order α is then defined via

$$H_\alpha(A|B)_\rho \coloneqq \min_{\sigma_B \in \mathrm{D}(\mathcal{H}_B)} D_\alpha(\rho_{AB}\|\mathbb{1}_A \otimes \sigma_B). \tag{2.15}$$

Again, for $\alpha \to 1$, this reduces to the usual conditional entropy (2.13).

Quantum channels

Quantum channels are operations from $\mathrm{D}(\mathcal{H})$ to $\mathrm{D}(\mathcal{H}')$ that map a quantum state to a quantum state. The set of quantum channels is given by the set of *completely positive trace-preserving* (CPTP) maps. There is also a more general notion of a quantum operation called a *quantum instrument*. Let Ω be a finite outcome set. A quantum instrument $\mathcal{I}$ is a set of completely positive trace non-increasing linear maps $\{\mathcal{I}_i\}_{i\in\Omega}$ such that $\sum_{i\in\Omega}\mathcal{I}_i$ is trace preserving. Given the quantum state $\rho \in \mathrm{D}(\mathcal{H})$, the probability of obtaining outcome i is given by $\mathrm{Tr}[\mathcal{I}_i(\rho)]$ and the subnormalised output state upon outcome i is $\mathcal{I}_i(\rho)$. There are some general ways to represent quantum channels/instruments, one of which is the *Kraus representation*.

2.1.10. 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,*

$$\Phi(\rho) = \sum_{i=1}^{r} K_i \rho K_i^\dagger, \tag{2.16}$$

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

Similarly to purifications for quantum states, a quantum channel on a system A can be regarded as a unitary on a larger system AB, followed by tracing out the B system. We say we *dilate* the channel. This is formalised by the *Stinespring dilation theorem* or *Stinespring representation* of the channel.

2.1.11. Lemma. (Stinespring representation [Sti55]). *A quantum channel* $\Phi : \mathrm{D}(\mathcal{H}_A) \to \mathrm{D}(\mathcal{H}_{A'})$ *can be represented as*

$$\Phi(\rho_A) = \mathrm{Tr}_B\big[V\rho_A V^\dagger\big], \tag{2.17}$$

using an isometry $V : \mathcal{H}_A \to \mathcal{H}_{A'B}$. *Moreover, the isometry can be decomposed into 'adding a register' containing a pure state followed by a unitary* U. *Then*

$$\Phi(\rho_A) = \mathrm{Tr}_B\Big[U_{AC\to A'B}(\rho_A \otimes |\psi\rangle\langle\psi|_C)U^\dagger_{AC\to A'B}\Big], \tag{2.18}$$

with a unitary $U : \mathcal{H}_{AC} \to \mathcal{H}_{A'B}$.

One can distinguish between different types of quantum channels depending on the properties they have. A few examples are classical-to-quantum channels (aka state preparation), LOCC channels, PPT (positive partial transpose) channels, entanglement breaking channels or quantum-to-classical channels (aka measurements). As we will use them extensively, we will describe measurements in a bit more detail. A *positive operator-valued measurement (POVM)* is a collection $\{\Pi_k\}_k$ of Hermitian positive semidefinite operators that sum up to the identity, i.e. $\sum_k \Pi_k = \mathbb{1}$. A measurement is called *projective*, if additionally it holds that the Π_k operators are orthogonal projectors, which means they fulfil $\Pi_k\Pi_l = \delta_{kl}\Pi_k$, where δ_{kl} is the Kronecker delta. Each operator Π_k points to a classical measurement outcome k.

2.2 Quantum information processing tools

Quantum teleportation

Quantum information can be 'teleported', in the sense that Alice can transmit a state $|\psi\rangle$ to Bob, without actually sending $|\psi\rangle$ via a quantum channel. Quantum teleportation not only is an interesting primitive enabled by quantum physics, it is also one of the basic principles behind measurement-based quantum computing [RB01], one of the candidates for a universal quantum computing architecture. There are different types of teleportation protocols, some of which we will introduce now.

Standard teleportation

The standard teleportation circuit, one of the most well-known protocols of quantum information processing and first introduced in [BBC+93], is depicted in Figure 2.1.

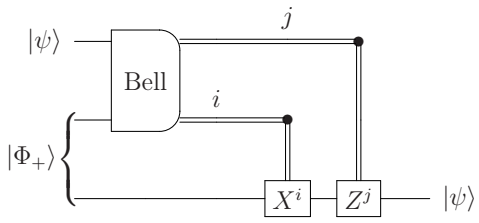


Figure 2.1: The standard teleportation protocol. Alice holds $|\psi\rangle$ and one half of the Bell state $|\Phi_+\rangle$, Bob holds the other half of the Bell state. Alice performs a Bell measurement on her registers and communicates the classical outcomes to Bob, who applies the appropriate corrections to his register to obtain $|\psi\rangle$.

One can check that

$$|\psi\rangle_A \otimes |\Phi_+\rangle_{A'B} = \frac{1}{2} \sum_{i,j=0}^{1} |\Phi_{ij}\rangle_{AA'} \otimes X^i Z^j |\psi\rangle_B \,, \tag{2.19}$$

which immediately explains the circuit. Measuring $|\Phi_{ij}\rangle$ on the AA' registers puts the state $X^i Z^j |\psi\rangle$ into Bob's register B, which is the input state with *teleportation corrections* on it. After receiving the measurement results (i, j) from Alice, Bob can apply X^i followed by Z^j to cancel the teleportation corrections. Then he holds $|\psi\rangle$ in register B, even though only classical information was communicated.

Entanglement swapping

An intriguing property of entanglement, and related to teleportation, is that it enables to entangle two particles that have never interacted before. This is called *entanglement swapping* and the process is shown in Figure 2.2.

(a) Before measurement (b) After measurement

Figure 2.2: Entanglement swapping illustrated. A measurement on the link $A'B'$ swaps entanglement into AB, which could constitute two particles that have never interacted before. In the right picture, we have discarded $A'B'$.

Formally, it can be understood by the following equation,

$$|\Phi_+\rangle_{AA'}|\Phi_+\rangle_{BB'} = \frac{1}{2}\Big[\,|\Phi_+\rangle_{AB}|\Phi_+\rangle_{A'B'} + |\Phi_-\rangle_{AB}|\Phi_-\rangle_{A'B'} + |\Psi_+\rangle_{AB}|\Psi_+\rangle_{A'B'} + |\Psi_-\rangle_{AB}|\Psi_-\rangle_{A'B'}\,\Big]. \tag{2.20}$$

Thus, doing a Bell measurement on $A'B'$ will swap entanglement into the previously unentangled AB. Alternatively, it can be understood by considering another Bell state $|\Phi_+\rangle$ as input instead of $|\psi\rangle$ in the standard teleportation protocol, and performing the Bell measurement on the second register of that $|\Phi_+\rangle$ together with the first register of the shared $|\Phi_+\rangle$ between Alice and Bob. This is the basic process of many proposed quantum repeater protocols, since by chaining many Bell states, and performing entanglement swapping via the links between different Bell states, long-range entanglement can be established without having to physically send quantum states over lossy quantum channels (after preparing a chain of Bell states). Only the classical Bell measurement outcomes need to be communicated. The established entanglement can then be further used for distributed quantum computation or communication.

Port-based teleportation

Port-based teleportation (PBT) is, because of its impractical resource requirements, more of theoretical interest and finds application in attacks on quantum position verification, as we will see in Chapter 3. It was first introduced in [IH08, IH09].

In the standard teleportation protocol, the resource state $|\Phi_+\rangle$ is simple and only one of it is required for perfect teleportation of $|\psi\rangle$. However, the protocol requires active operations on Bob's side to cancel the incurred teleportation corrections. One can ask whether there is a teleportation protocol that does not require Bob to do anything, or only something very simple. This is the premise of port-based teleportation, which is shown in Figure 2.3.

Alice's global measurement as well as the optimal resource state on the N ports are non-trivial. Moreover, one can distinguish between deterministic PBT, where the the procedure always works but the teleportation is imperfect (i.e. Bob holds approximately $|\psi\rangle$ in the end), and probabilistic PBT, where the protocol has an additional 'failure' outcome, but if it succeeds, the teleportation was implemented perfectly (i.e. Bob holds exactly $|\psi\rangle$ in the end). For the general attack on quantum position verification, which we will encounter later, deterministic PBT is used. The asymptotic performance has been studied in detail, see for example [CLM+21]. Most notably for us, deterministic PBT cannot be completed perfectly and to achieve a constant approximation error ε at Bob an exponential amount of ports N in the number of qubits contained in $|\psi\rangle$ is required.

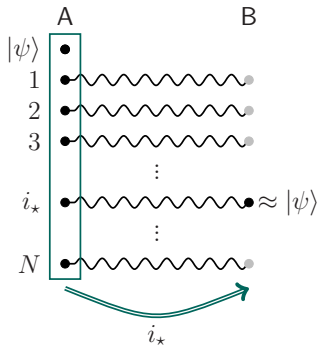


Figure 2.3: The port-based teleportation primitive. Alice holds $|\psi\rangle$ and N halves of entangled states, called *ports*. Bob holds the other N halves of the entangled states. Then Alice applies a global measurement on all her registers, obtaining a result $i_\star$, which she communicates to Bob. The bit string $i_\star$ indicates the 'correct' port and Bob throws away all ports except $i_\star$. Ideally, he then would hold $|\psi\rangle$ in port $i_\star$, but it is only possible approximately for finite N.

The no-cloning principle

The no-cloning theorem is one of the most profound differences of quantum theory compared to the classical world from an information-theoretic point of view. It states that quantum information cannot be perfectly copied, in vast contrast to the classical data in our computers that we copy every day. The fact that quantum information cannot be cloned is the basis of much of quantum cryptography, and in particular position-based quantum cryptography.

2.2.1. Theorem. *There exists no unitary operation U on $\mathcal{H} \otimes \mathcal{H}$ such that for all quantum states $|\psi\rangle, |\phi\rangle \in \mathcal{H}$ it acts as*

$$U |\psi\rangle \otimes |\phi\rangle = e^{i\alpha(\psi,\phi)} |\psi\rangle \otimes |\psi\rangle , \tag{2.21}$$

with some phase $\alpha(\psi, \phi)$.

Note that this covers the no-cloning principle in all generality, since mixed states can always be purified and quantum channels can always be diluted to a unitary on a bigger space. Furthermore, the 'for all' quantifier is crucial. Clearly, classical information such as $|0\rangle, |1\rangle$ can be copied, for example the CNOT gate maps $|10\rangle \mapsto |11\rangle$. However, it will fail on other inputs and the no-cloning theorem asserts that there is no copying unitary that works on arbitrary inputs.

That begs the question of how well one can copy quantum information approximately, and this has been studied widely and in different settings [SIGA05]. One can distinguish, for example, between symmetric and asymmetric cloning,

which refers to whether the fidelities of the output states to the input state are equal or are allowed to differ from each other, respectively. In particular, for universal asymmetric $1 \to 2$ cloning, mapping $|\psi\rangle$ to ρ_{AB}, the fidelities of the two outputs ρ_A, ρ_B to $|\psi\rangle$ are governed by the *no-cloning inequality*

$$\frac{1}{2} - (1 - F_A) - (1 - F_B) \leq \sqrt{1 - F_A}\sqrt{1 - F_B}, \tag{2.22}$$

and the optimal such cloner achieves equality. Applying the inequality between arithmetic and geometric mean in the form of $\sqrt{1 - F_A}\sqrt{1 - F_B} \leq \frac{(1-F_A)+(1-F_B)}{2}$ and simplifying from there yields the upper bound on the average fidelity of

$$\frac{F_A + F_B}{2} \leq \frac{5}{6}. \tag{2.23}$$

State discrimination

Often in quantum information processing it is important to distinguish between different states. How well can you distinguish two states ρ_0, ρ_1? This is answered, in all generality, by the celebrated *Holevo-Helström theorem.*

2.2.2. THEOREM. (Holevo-Helström) *Consider two quantum states $\rho_0, \rho_1 \in \mathrm{D}(\mathcal{H})$ with prior probabilities $p, 1-p$. Then the optimal probability of distinguishing the states correctly is*

$$p_{\text{succ}}^{\max} = \frac{1}{2} + \frac{1}{2}\|p\rho_0 - (1-p)\rho_1\|_1. \tag{2.24}$$

If the prior probabilities are uniform, i.e. $p = 1/2$, then this reduces to

$$p_{\text{succ}}^{\max} = \frac{1}{2} + \frac{1}{2}D_{\text{tr}}(\rho_0, \rho_1). \tag{2.25}$$

Moreover, the optimal measurement achieving this is projective.

2.3 Continuous-variable quantum information theory tools

In this section, we introduce some facts regarding continuous-variable quantum information theory to the extent we need it in Chapter 7.

Gaussian states

The Wigner function fully describes an N-mode bosonic quantum state ρ and can be obtained from ρ by the Wigner formula [Wig32]

$$W(\mathbf{x}, \mathbf{p}) = \frac{1}{\pi^N}\int_{\mathbb{R}^N} e^{2i\mathbf{p}\cdot\mathbf{y}}\langle \mathbf{x} - \mathbf{y}|\rho|\mathbf{x} + \mathbf{y}\rangle \, \mathrm{d}\mathbf{y}. \tag{2.26}$$

Gaussian states are defined by the property that their Wigner function is a Gaussian function in phase space. The Wigner function of Gaussian states reads

$$W_{\mathrm{G}}(\mathbf{r}) = \frac{1}{\pi^N \sqrt{\det \Gamma}} \exp\big\{-(\mathbf{r}-\mathbf{d})^T \Gamma^{-1} (\mathbf{r}-\mathbf{d})\big\}, \tag{2.27}$$

where $\mathbf{r} = (x_1, p_1, \ldots, x_N, p_N)$ are the quadrature variables. The vector $\mathbf{d}$ is the displacement vector with components

$$d_i = \mathbb{E}[\hat{r}_i] = \mathrm{Tr}[\rho \hat{r}_i], \tag{2.28}$$

and Γ is the covariance matrix with components

$$\Gamma_{ij} = \mathrm{Tr}\big[\rho\big((\hat{r}_i - d_i)(\hat{r}_j - d_j) + (\hat{r}_j - d_j)(\hat{r}_i - d_i)\big)\big]. \tag{2.29}$$

Displacement measurements of CV states

Here we describe homodyne and heterodyne measurements, the two types of possible displacement measurements. For the physics of the measurement process, we refer to the first chapter of [GPS07].

Homodyne

Consider a Wigner function $W(\mathbf{x}, \mathbf{p})$. A homodyne measurement of the quadrature x_i, yields the following marginal probability distribution

$$f_{X_i}(x_i) = \int_{\mathbb{R}^{2N-1}} W(\mathbf{x}, \mathbf{p})\, \mathrm{d}\mathbf{p}\, \mathrm{d}x_1 \ldots \mathrm{d}x_{i-1}\, \mathrm{d}x_{i+1} \ldots \mathrm{d}x_N, \tag{2.30}$$

and similarly for p_i. One can choose any axis x_θ along which to perform a homodyne measurement, given a mode. In this case, we rotate our reference frame corresponding to the mode to be measured by an angle θ. We can then perform an integral similar to the one above to obtain $f_{X_\theta}(x_\theta)$.

Heterodyne

A heterodyne measurement is essentially a double homodyne measurement. The selected mode from $W(\mathbf{x}, \mathbf{p})$ is mixed with the vacuum on a balanced beam splitter. Then a homodyne measurement is performed on the two output modes, each in conjugate directions. The result obtained is captured by the following theorem.

2.3.1. Lemma. *The heterodyne measurement of a one-mode Gaussian state with displacement (x_0, p_0), produces two Gaussian distributions, centred around $x_0/\sqrt{2}$ and $-p_0/\sqrt{2}$ respectively.*

Proof:
A balanced beam splitter is represented by the following symplectic matrix

$$S = \begin{pmatrix} \sqrt{\frac{1}{2}}\mathbb{1}_2 & \sqrt{\frac{1}{2}}\mathbb{1}_2 \\ -\sqrt{\frac{1}{2}}\mathbb{1}_2 & \sqrt{\frac{1}{2}}\mathbb{1}_2 \end{pmatrix}. \tag{2.31}$$

As the input state is Gaussian, and mixing preserves Gaussian states, the output states are also Gaussian. The new displacements under this transformation are the given by

$$(x_0, p_0, 0, 0)S^T = (x_0/\sqrt{2}, p_0/\sqrt{2}, -x_0/\sqrt{2}, -p_0/\sqrt{2}). \tag{2.32}$$

□

Noisy CV channel

Whereas a discrete state passing through a noisy channel suffers from loss, bit and phase errors, a continuous-variable state gets attenuated and acquires excess noise. Consider a coherent state with displacement (x_0, p_0). Let $t \in [0, 1]$ be the transmission parameter, and let $u \geq 0$ be the excess noise power. The effect of the channel is that the displacement becomes $(\sqrt{t}x_0, \sqrt{t}p_0)$ and the covariance matrix goes from $\mathbb{1}_2$ to $(1 + 2u)\mathbb{1}_2$. The outcome of a homodyne measurement now has the variance $\frac{1}{2} + u$ instead of just the $\frac{1}{2}$ from shot noise. In terms of signal and noise, the signal has changed by a factor t and the noise has increased by a factor $1+2u$. Overall, the signal-to-noise ratio has changed by a factor $\frac{t}{1+2u}$.

Continuous-variable EPR state and teleportation

Consider two modes labelled A and B. The Wigner function of the two-mode squeezed vacuum state (TMSV) with squeezing parameter $\zeta \geq 0$ is given by

$$\begin{aligned} W_{\text{TMSV}}(x_a, p_a, x_b, p_b) &= \frac{1}{\pi^2} \exp\{-e^{-2\zeta}[(x_a + x_b)^2 + (p_a - p_b)^2] - e^{2\zeta}[(x_a - x_b)^2 + (p_a + p_b)^2]\} \\ &= \frac{1}{\pi^2} \exp\left\{ -\begin{pmatrix} x_a & p_a & x_b & p_b \end{pmatrix} \Gamma(\zeta)^{-1} \begin{pmatrix} x_a \\ p_a \\ x_b \\ p_b \end{pmatrix} \right\}, \end{aligned} \tag{2.33}$$

with covariance matrix

$$\Gamma(\zeta) = \begin{pmatrix} \cosh(2\zeta)\mathbb{1}_2 & \sinh(2\zeta)Z \\ \sinh(2\zeta)Z & \cosh(2\zeta)\mathbb{1}_2 \end{pmatrix}, \qquad \text{where} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.34}$$

In the limit $\zeta \to \infty$ of the squeezing parameter we have $W_{\text{TMSV}}(x_a, p_a, x_b, p_b) \to C\delta(x_a - x_b)\delta(p_a + p_b)$, for a constant C, which corresponds to the continuous-variable maximally entangled EPR state.

Consider a heterodyne measurement performed on the A mode. The state of the A mode, viewed in isolation, is a thermal state with covariance matrix $K_A = \cosh(2\zeta)\mathbb{1}_2$. Using a 50/50 beam splitter this state gets mixed with the vacuum, resulting in a two-mode state on $A'A''$ with covariance matrix

$$K_{A'A''} = \frac{1}{2}\begin{pmatrix} \mathbb{1}_2 + K_A & \mathbb{1}_2 - K_A \\ \mathbb{1}_2 - K_A & \mathbb{1}_2 + K_A \end{pmatrix} = \begin{pmatrix} \cosh^2(\zeta)\mathbb{1}_2 & -\sinh^2(\zeta)\mathbb{1}_2 \\ -\sinh^2(\zeta)\mathbb{1}_2 & \cosh^2(\zeta)\mathbb{1}_2 \end{pmatrix}. \tag{2.35}$$

In mode A' the x-quadrature is measured and in mode A'' the p-quadrature. The Wigner function for $x_{a'}$ and $p_{a''}$ is obtained by integrating out $p_{a'}$ and $x_{a''}$ from the Wigner function $A'A''$, resulting in a product of two Gaussian distributions given by $\mathcal{N}_{0,\frac{1}{2}\cosh^2\zeta}(x_{a'})\mathcal{N}_{0,\frac{1}{2}\cosh^2\zeta}(p_{a''})$.

The post-measurement state on B, after a heterodyne measurement with result $(x_{a'}, p_{a''})$, is a Gaussian state with displacement $(x_B, p_B) = (x_{a'}, p_{a''})\sqrt{2}\tanh\zeta$ and covariance $\mathbb{1}_2$, i.e. a coherent state. Note that the components x_B and p_B are Gaussian distributed with variance $\frac{1}{2}\cosh^2\zeta \cdot (\sqrt{2}\tanh\zeta)^2 = \sinh^2\zeta$. In Section 7.2.2 we set $\sinh\zeta = \sigma$ so that x_B, p_B have Gaussian statistics with variance σ^2.

Teleportation

The teleportation of an unknown continuous-variable quantum state using a CV EPR pair was proposed by Vaidman [Vai94] and is described as follows:

1. Alice and Bob share a CV-EPR pair described by the Wigner function (2.33). Alice possesses the single-mode quantum state $|\psi\rangle$ to be teleported.

2. With a balanced beam splitter, Alice mixes $|\psi\rangle$ with her mode of the CV-EPR pair and then does a measurement of the x-quadrature in one mode and the p-quadrature in the other mode (i.e. she performs a heterodyne measurement). We denote the outcome of the measurement as (d_x, d_p). The result is that Bob's half of the EPR pair is transformed to a displaced version of $|\psi\rangle$, with displacement $(\sqrt{2}d_x, -\sqrt{2}d_p)$. Alice sends the classical (d_x, d_p) to Bob.

3. Bob applies a displacement $(-\sqrt{2}d_x, \sqrt{2}d_p)$ to his state to obtain $|\psi\rangle$.

CV information theory

Now we define some basic notions of CV information theory that will be used in Chapter 7. First, we present some definitions and properties regarding CV entropies and start with the *differential Shannon entropy*.

2.3.2. Definition. Let X be a continuous random variable with probability density function $f(x)$, and let $\mathcal{X}$ be its support set. The differential Shannon entropy $h(X)$ is defined as

$$h(X) = -\int_{\mathcal{X}} f(x) \log f(x) \, \mathrm{d}x. \tag{2.36}$$

2.3.3. Lemma. *Let $\alpha > 0$ and $X \in \mathbb{R}$. Then we have $h(\alpha X) = h(X) + \log \alpha$.*

Another useful quantity to compare two quantum states is the *relative entropy*.

2.3.4. Definition. Let ρ and σ be two density matrices. Their Umegaki quantum relative entropy is defined as

$$D(\rho \| \sigma) \coloneqq \mathrm{Tr}[\rho \log \rho - \rho \log \sigma]. \tag{2.37}$$

As introduced in [FBT+14], the continuous quantum conditional von Neumann entropy is defined as follows. We first have to introduce an equivalent definition of the quantum conditional von Neumann entropy, of which the continuous limit will be the *differential quantum conditional von Neumann entropy*. This way of defining it allows for completely general (possibly continuous-variable) side information. Let ρ_{AB} be a bipartite quantum state. Let X be a continuous random variable and $\alpha = 2^{-n}$ for some $n \in \mathbb{N}$. Moreover, consider the intervals $\mathcal{I}_{k;\alpha} \coloneqq (k\alpha, (k+1)\alpha]$ for $k \in \mathbb{Z}$. Denote $\rho_B^{k;\alpha}$ the subnormalised density matrix on B when x is measured in $\mathcal{I}_{k;\alpha}$ and denote ρ_B^x the conditional reduced density matrix on B such that $\int_{\mathcal{I}_{k;\alpha}} \rho_B^x \, \mathrm{d}x = \rho_B^{k;\alpha}$. Finally, X_α denotes the random variable that indicates which interval x belongs to.

2.3.5. Definition. The quantum conditional von Neumann entropy is equivalently defined as

$$H(X_\alpha|B)_\rho \coloneqq -\sum_{k \in \mathbb{Z}} D(\rho_B^{k;\alpha} \| \rho_B). \tag{2.38}$$

2.3.6. Definition. We define the differential quantum conditional von Neumann entropy as

$$h(X|B)_\rho \coloneqq -\int_{\mathbb{R}} D(\rho_B^x \| \rho_B) \, \mathrm{d}x. \tag{2.39}$$

The basis of our security proofs in Chapter 7 is the quantum mechanical uncertainty principle. We use the following entropic uncertainty relation in terms of the differential entropy for the setting of a tripartite guessing game, as is often useful in the context of quantum cryptography [CBTW17].

2.3.7. Lemma. ([FBT+14]) *Let ρ_{ABC} be a tripartite density matrix on systems A, B and C. Let Q and P denote the random variables of position and momentum, respectively, resulting from a homodyne measurement on the A system and let the following hold: $h(Q|B)_\rho, h(P|C)_\rho > -\infty$ and $H(Q_\alpha|B)_\rho, H(P_\alpha|C)_\rho < \infty$ for any $\alpha > 0$. Then*

$$h(Q|B)_\rho + h(P|C)_\rho \geq \log(2\pi). \tag{2.40}$$

Furthermore, we will make use of the following estimation inequality, which is a continuum version of Fano's inequality.

2.3.8. Theorem. ([Cov99]) *Let X be a random variable and $\hat{X}(Y)$ an estimator of X given side information Y, then*

$$\mathbb{E}\left[\left(X - \hat{X}(Y)\right)^2\right] \geq \frac{1}{2\pi e} e^{2h_{\text{nats}}(X|Y)}, \tag{2.41}$$

where $h_{\text{nats}}(X|Y)$ is the differential conditional entropy in natural units. Moreover, if X is Gaussian and $\hat{X}(Y)$ is its mean, then equality holds.

2.4 Semidefinite programming

We will use semidefinite programs extensively in this thesis to obtain upper bounds on success probabilities of attackers in different scenarios. Semidefinite programming is essentially the matrix extension to linear programming. In a *linear program* one seeks to find a vector x that maximises the (linear) objective function $f(x) = \langle a, x\rangle$ under the (linear) constraints that $Mx \geq b$ for a matrix M and vector b as well as $x \geq 0$, component-wise, respectively. The triple (M, a, b) constitutes the linear program in x. Any linear program has a *dual program*, seeking to find a vector y that minimises $\langle b, y\rangle$ under the constraints that $M^T y \geq a$ and $y \geq 0$. For a *semidefinite program (SDP)* the vectors a, b are replaced by matrices A, B and the matrix M is replaced by a linear map Φ on matrices that preserves hermiticity. The vector inner product is replaced by the Hilbert-Schmidt inner product $\langle A, B\rangle := \mathrm{Tr}\left[A^\dagger B\right]$. Semidefinite programs are widely used in quantum information theory.

2.4.1. Definition. A semidefinite program is a triple (Φ, A, B), where Φ maps linear operators to linear operators while preserving hermiticity, and A, B are hermitian matrices, that constitutes the two optimisation problems, called primal and dual, as follows:

Primal program		**Dual program**	
maximize:	$\langle A, X\rangle$	**minimize:**	$\langle B, Y\rangle$
subject to:	$\Phi(X) = B,$	**subject to:**	$\Phi^*(Y) \succeq A,$
	$X \succeq 0.$		Y hermitian.

(2.42)

The primal and dual values of feasible solutions are closely related. In fact, if α is the value of a feasible solution to the primal program, and β the one to the dual program, then $\alpha \leq \beta$. Denoting the optimal values by $\alpha_\star$ and $\beta_\star$, this means $\alpha \leq \alpha_\star \leq \beta_\star \leq \beta$. This property is called *weak duality*. If it holds that $\alpha_\star = \beta_\star$, then the semidefinite program fulfils *strong duality*. In particular, we note that any solution to the primal program lower bounds the optimal value and any solution to the dual program upper bounds it.

One can also consider semidefinite programs with equality and inequality constraints, and that is the type we will most encounter in this thesis. Then (2.42) can be formulated as follows.

$$\begin{array}{rl} & \textbf{Primal program} \\ \textbf{maximize:} & \langle A, X\rangle \\ \textbf{subject to:} & \Phi_1(X) = B_1, \\ & \Phi_2(X) \preceq B_2, \\ & X \succeq 0. \end{array} \qquad \begin{array}{rl} & \textbf{Dual program} \\ \textbf{minimize:} & \langle B_1, Y_1\rangle + \langle B_2, Y_2\rangle \\ \textbf{subject to:} & \Phi_1^*(Y_1) + \Phi_2^*(Y_2) \succeq A, \\ & Y_1 \text{ hermitian}, \\ & Y_2 \succeq 0. \end{array} \tag{2.43}$$

In particular, many state discrimination problems are naturally semidefinite programs and we will use them extensively to find maximal success probabilities of distinguishing a given set of states. There, one can define $A = \operatorname{diag}(p_1\rho_1, \ldots, p_n\rho_n)$ and $X = \operatorname{diag}(\Pi_1, \ldots, \Pi_n)$, where $\{p_k, \rho_k\}_k$ is the ensemble to be distinguished and $\{\Pi_k\}_k$ are the measurement operators to be optimised over. By definition, measurement operators are positive semidefinite so $X \succeq 0$ becomes $\Pi_k \succeq 0$ for all k. They also need to sum up to the identity, which we can capture by setting Φ_1 to be the map that sums up the diagonal blocks of the size of the measurement operators and B_1 the identity matrix of the same size. Then $\Phi_1(X) = \sum_k \Pi_k = \mathbb{1}$. The map Φ_2 could capture other constraints, depending on the situation. We will often consider PPT (positive partial transpose) measurements on a bipartite system AB, which means $\Pi_k^{T_B} \succeq 0$ for all k. We can include this by letting Φ_2 be the negative of the map that partially transposes every block of the size of the measurement operators in its input and B_2 the corresponding zero matrix. Then $\Phi_2(X) = \operatorname{diag}(-\Pi_1^{T_B}, \ldots, -\Pi_n^{T_B}) \preceq 0$, which becomes $\Pi_k^{T_B} \succeq 0$ for all k. Using (2.43), the dual program can then be found in a straightforward way. Finding a solution to the primal program will give a lower bound and a solution to the dual program will yield an upper bound on the optimal success probability of distinguishing $\{p_k, \rho_k\}_k$ under the constraints considered. And if the primal and dual values coincide, the optimal value is found.

Chapter 3

Position-based Quantum Cryptography

In this chapter, we provide an overview of the field of position-based quantum cryptography.

Imagine the following situation: You are sitting in front of your computer screen, looking at a website that looks like the website of your bank. But how can you make sure it is authentic? One way would be to verify that the server you interact with is indeed placed in the basement of your bank or that the message must have originated from the bank's building. Or, you would like to give location-based access to a database or server – you can only access it if you are physically present in a certain building for example. In another scenario, say, you see a photo or video online. One way to verify that it is most likely authentic, rather than fake or created by powerful AI, would be to unambiguously verify *where* it was created. With the advent of increasingly sophisticated generative AI, this type of protection becomes important in preventing fraud [CNN24]. For example, it would be useful to have a simple check mark in the corner of your video in a video call guaranteeing, in a quantum-secure way, that the data making up your video was indeed created where it should have been created and not in a data centre far away.

This is the idea behind position-based cryptography, in which the geographic location of a party is used to authenticate it, without further cryptographic credentials or assumptions. Unfortunately, secure position-based cryptography with only classical resources is impossible without further assumptions [CGMO09], since classical information can be copied and therefore easily distributed among attackers. If all involved information is classical, attackers can intercept the inputs, which in general will be bit strings (call them x at Alice and y at Bob), copy them and send the copies to each other (cf. Figure 3.3). After communication, all attackers have all the protocol inputs and can complete the task, which in general will be the computation of some classical function f. Then they can respond the protocol output $f(x, y)$ to both verifiers in time. However, quantum information cannot be perfectly copied [WZ82]. Therefore, quantum physics might enable

secure position-based cryptography.

Another possible application of position-based cryptography is to protect against man-in-the-middle attacks in other tasks. By definition, a man in the middle (who is not located where the corresponding honest party should be) would not be able to successfully complete a position-based protocol with the honest parties, and thus would always expose himself when an extra position-based cryptographic layer is present.

3.1 The basic primitives

We will now introduce the different primitives of position-based quantum cryptography: verification, authentication, and key distribution. For simplicity, we treat the one-dimensional case, where all parties are located on a line. Note that such 1D position verification also verifies the 3D position of the prover [LL11] and if the verifiers are geometrically constrained, one can still execute the primitive without adding any loopholes by putting more verifier stations at certain positions [LL11, Unr14]. Moreover, in all that follows, the time needed to implement local operations is assumed to be negligibly short compared to the time span of the entire protocol. The basic building block is quantum position verification, from which authentication and key distribution can be constructed [BCF+14, Unr14].

3.1.1 Quantum position verification

The task of quantum position verification (QPV) aims to verify the geographical location of an a priori untrusted prover P in a quantum-secure way. To do so, two trusted and spatially separated verifiers $\mathsf{V_A}, \mathsf{V_B}$ send quantum inputs ρ_A, ρ_B, possibly chosen from an ensemble of protocol states $\{p_k, \rho_k^{AB}\}$, to P from each side and ask them to apply a specific, publicly known quantum operation, say a unitary U_{AB} or a measurement $\{\Pi_{AB}^k\}_k$. P's task is 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 (for example, a certain measurement result). The scenario is sketched in Figure 3.1.

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[1] A, B can position themselves between $\mathsf{V_A}, \mathsf{P}$ and $\mathsf{V_B}, \mathsf{P}$, respectively, and intercept inputs, act locally, communicate one message to each other, and then act locally again before they have to respond with some answers τ_A, τ_B (or k) that depend on the specific protocol at hand. In other words, they have to simulate the honest quantum operation using only local actions and 1 round of simultaneous communication. In general, they could also pre-share an entangled resource state

[1] The scenario of more attackers can be reduced to the one of just two. The attackers closest to P could simply simulate all other attackers on their respective side.

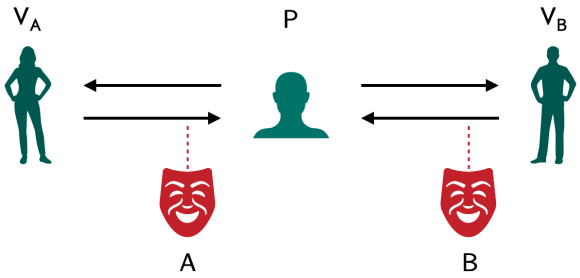


Figure 3.1: In QPV the verifiers send protocol inputs to an untrusted prover, who has to complete a known task, and send back his answers immediately to both verifiers. The goal of QPV is to build a protocol that can only be successfully completed at the geographical location of P. Attackers A, B try to convince the verifiers they are at this location, without actually being there.

$|\Psi\rangle_{A'B'}$ at the start of the protocol. Since the fundamental question is whether a given task can be simulated in this fashion, it is usually assumed that the location of P is empty when we talk about QPV[2]. This situation is depicted in Figure 3.4. The question of security boils down to comparing the honest success probability of the task to the one of attackers, where 'success probability' could, for example, mean a fidelity to a target state, an average correctness of a measurement result, or a sample close enough to an expected distribution. This depends on the specific protocol at hand. If there is a finite gap between the honest case and the optimal attack for a given QPV protocol, it is secure. The above constitutes a single round of QPV and commonly it gets repeated many times, either sequentially or in parallel, to amplify security. The end goal is to define a protocol that can only be completed successfully by being present at the location of P, i.e. that accepts P with very high probability of at least $1-\varepsilon_c$, while rejecting attackers with a very high probability of at least $1-\varepsilon_s$. Such a protocol is then called ε_c *complete* and ε_s *sound*.
QPV can be formally defined in a general way [BCF+14]. We refrain from doing so here for simplicity.

The QPV literature usually has the following implicit assumptions on the honest protocol:

(i) The verifiers and the prover control their laboratories and can at least do basic quantum operations.

(ii) The verifiers share a private and authenticated channel to communicate.

[2]By definition, a secure QPV protocol can only be successfully completed if the computation happens at P. Thus, only an impersonation attack (with P empty) makes sense, as substituting P's responses (when P is present) would introduce errors and expose an attack.

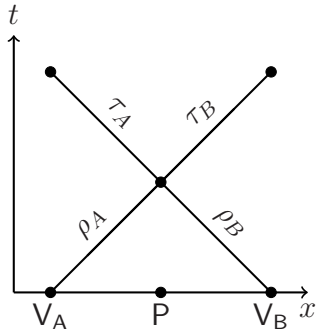


Figure 3.2: Honest scenario

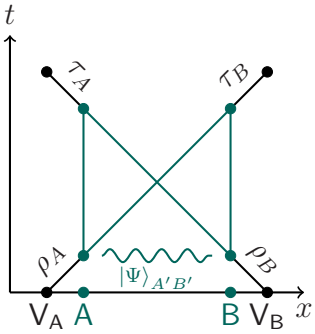


Figure 3.3: Attack scenario

Figure 3.4: Space-time diagram of a general 1D 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 $\mathsf{V_B}$ and the attackers A, B equidistant from them (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.

(iii) The verifiers and the prover have synchronised clocks.

(iv) Classical information travels at the speed of light.

(v) Any local computation time of the parties is negligible relative to the time span of one round of the protocol.

(vi) The verifiers and the prover remain stationary while executing the protocol.

(vii) The verifiers and the prover do not pre-share any secret information unknown to attackers.[3]

(viii) Unless stated otherwise, a flat background space-time is assumed.

And the following on the attackers:

(i) The attackers control anything, except the laboratories of the verifiers and the prover.

(ii) They are only constrained by the laws of physics.

(iii) They can send information through the prover's location, but cannot access it.

[3] If this assumption is discarded, secure QPV is, in fact, possible [Ken11].

(iv) They can pre-agree on a strategy.

(v) Kerckhoff's principle: The set of protocol inputs and tasks are publicly known.

3.1.2 Quantum position-based authentication

The task of quantum position-based authentication (QPA) aims to authenticate that a message must have originated from a certain geographical location, at which a prover P claims to be. The setting is analogous to QPV with two verifiers $\mathsf{V_A}, \mathsf{V_B}$ and P in between. For the authentication of a message bit $m \in \{0,1\}$, P is supposed to create an authentication tag $t(m)$ based on the input of the verifiers. So far, there exist two QPA schemes, one construction that works generically, albeit inefficiently, for any QPV protocol [BCF+14], and one more efficient one based on the random oracle model for a specific protocol [Unr14]. We will briefly discuss them later in this chapter. Both of them use QPV under the hood, but modify the protocol responses depending on the message m.

The attack model differs from the one of QPV, because now the extra piece of information $m \in \{0,1\}$ determines what response is expected from P. Attackers may want to authenticate a different message $m' \in \{0,1\}$ with $m' \neq m$. Practically speaking, P may want to authenticate the message 'Transfer $100 to account X', while the attackers try to replace it and authenticate 'Transfer $100,000 to account Y'. Therefore, in QPA we must consider not just an impersonation attack but also a substitution attack. Again, the end goal is to define a protocol that accepts P with very high probability of at least $1 - \varepsilon_c$ for message m, while rejecting attackers with a very high probability of at least $1 - \varepsilon_s$ when $m' \neq m$. Such a protocol is then called ε_c *complete* and ε_s *sound*.

3.1.3 Quantum position-based key distribution

The task of quantum position-based key distribution (PB-QKD) aims to generate a secret key between the verifiers and the prover P at a certain geographical position. Once such a key is established, it enables the verifiers to send messages that can only be decrypted and read at the location of the prover, for example by one-time-padding the message with the generated key.

[BCF+14] provided a general construction that allows one to go from a QPA protocol to a PB-QKD protocol by bootstrapping the QPA protocol to any QKD protocol that requires authenticated communication between the parties, like the well known BB84 protocol [BB84]. Taking such a QKD protocol, one can in principle establish authentication between the QKD parties by means of a QPA protocol to end up with a PB-QKD protocol. This then enables position-based encryption.

3.2 History of position-based quantum cryptography

As mentioned previously, the no-cloning theorem motivated the study of quantum information protocols for secure position verification. The first proposals to this end resulted in a patent published in 2006 [BKMS06]. More proposals that were claimed to be secure followed in the academic literature in 2010 [Mal10a, Mal10b]. However, first ad hoc attacks were found to compromise the security of these protocols [KMS11, LL11], before a general attack on any QPV protocol was presented in [BCF+14][4]. The attack makes clever use of recursive quantum teleportation and requires a doubly exponential amount of pre-shared entangled pairs in the resources used by the verifiers and prover. This amount was later reduced to exponential by [BK11] with the help of port-based teleportation [IH08, IH09] and the idea was subsequently generalised to other settings in [GLW16, Dol19]. Other general attacks were found that use an exponential amount of entangled pairs in the number of T gates, or in the T depth, of the quantum circuit of the honest operation decomposed in the Clifford+T gate set [Spe16a], or that are exponential in a geometric locality property of the honest quantum circuit [DC22b]. Some other more efficient attacks on certain classes of unitaries have also been found. For example, any two-qubit unitary can be implemented up to error ε using $O(\log 1/\varepsilon)$ EPR pairs [GC20], and any hermitian bipartite binary controlled unitary can be implemented with just one EPR pair. Hermiticity was crucial in the latter result, as [GC20] also shows a logarithmic lower bound on the entanglement entropy of the resource state for general bipartite binary controlled unitaries.

Currently, there does not exist a QPV protocol with a superlinear lower bound on the attack resource requirements. It is *the* major open question in the field of position-based quantum cryptography whether we can find a protocol that provably needs superlinear attack resources, or whether all QPV protocols can be efficiently attacked. Much of the work in the QPV literature has aimed to find secure protocols [CL15, GC20, ABSV21, LLQ22, AER+23, ABB+23, AEFR+24], although more recently a line of work from a very different angle, via a novel connection to holography and based on the AdS/CFT conjecture, tries to argue for efficient attacks on all QPV protocols [MPS20, May19, DC22a, May22]. Moreover, resource bounds on QPV attacks have been shown to be related to several topics in mathematics [JKPP22], theoretical computer science [BFSS13, ABM+24], and theoretical physics [May19, ACH+24]. Using further assumptions, the security of QPV has been established assuming a pre-shared secret between the verifiers and the prover [Ken11], the random oracle model [Unr14], or LWE (learning with errors) hardness [LLQ22].

We go on to describe some of the most studied QPV protocols in more detail.

[4] This paper appeared online in 2011, but was only later published in 2014.

3.2.1 First protocols

$\mathbf{QPV_{BB84}}$

First introduced in [KMS11], this is one of the simplest and most well-studied QPV protocols and inspired by the BB84 protocol [BB84]. A single round of this protocol is defined as follows and is depicted in Figure 3.5. To boost security, the protocol can be repeated n-fold, either in parallel or sequentially.

1. Verifiers $\mathsf{V_A}$, $\mathsf{V_B}$ draw two bits $\theta, z \in \{0,1\}$ uniformly at random. $\mathsf{V_A}$ sends the qubit $H^\theta |z\rangle$, $\mathsf{V_B}$ sends the bit θ to P such that the qubit and the bit arrive at P simultaneously.

2. Upon receiving the inputs, P measures the qubit in basis θ, with $\theta = 0$ corresponding to the computational basis and $\theta = 1$ to the Hadamard basis, obtaining result z'. P immediately sends off z' to both verifiers.

3. Knowing θ and z, the verifiers check if $z' = z$ and if the answers were received in time (i.e. $\Delta t_\mathsf{A} = 2d(\mathsf{V_A}, \mathsf{P})/c$ and $\Delta t_\mathsf{B} = 2d(\mathsf{V_B}, \mathsf{P})/c$ after they sent out the inputs, respectively). If both tests are passed, they *accept*. Otherwise, they *reject*.

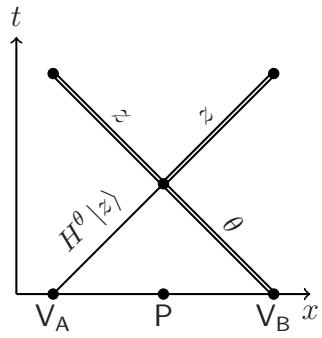


Figure 3.5: The $\mathrm{QPV}_{\mathrm{BB84}}$ protocol.

$\mathrm{QPV}_{\mathrm{BB84}}$ was proven to be secure against unentangled attackers first in [BCF+14], achieving an upper bound on the attack success probability of $p_{\mathrm{succ}} \lesssim 0.89$ using an argument based on the uncertainty principle. This was later improved to the optimal bound $p_{\mathrm{succ}} \leq \frac{1}{2} + \frac{1}{2\sqrt{2}}$ in [TFKW13] by employing an operator-sum inequality, which also showed strong parallel repetition and a lower bound on the necessary pre-shared entanglement of $\Omega(n)$ for a successful attack on the n-round protocol $\mathrm{QPV}_{\mathrm{BB84}}^{\otimes n}$. Originally, $\mathrm{QPV}_{\mathrm{BB84}}$ was believed to be unconditionally secure, but soon after initial publication an entanglement attack using just 1

EPR pair per round was published [LL11], albeit this seems to have already been known by [KMS11]. Thus $\mathrm{QPV}_{\mathrm{BB84}}^{\otimes n}$ is broken via n pre-shared EPR pairs. Moreover, it is not too hard to see that the basic entanglement based attack on $\mathrm{QPV}_{\mathrm{BB84}}$ also works for unitaries of the Clifford group [LL11]. Furthermore, [CL15], and independently [Spe16a], extended efficient attacks to unitaries in the second level of the Clifford hierarchy and constant depth quantum circuits in which individual gates act only on a finite number of qubits while being contained in a low level of the Clifford hierarchy. In the case of attackers restricted to classical communication, an essentially tight lower bound of $n - O(\log n)$ in the max-relative entropy of the attack resource state was proven in [RG15] via a reduction to a protocol called *weak string erasure* [KWW12].

$\mathrm{QPV}_{\mathrm{BB84}}$ is not loss tolerant, and therefore not practical, as the following simple attack for a transmission $\eta \leq 1/2$ shows. Alice can simply guess a basis value θ_{guess} and measure the qubit in that basis, getting result z'. Alice communicates θ_{guess} and z' to Bob, and Bob sends θ to Alice. After communication both know $(\theta, \theta_{\mathrm{guess}}, z')$. If $\theta_{\mathrm{guess}} = \theta$, then $z' = z$ and they successfully broke the protocol. Otherwise, z' is uncorrelated with z. Alice's guess is correct with probability $1/2$. Thus, responding only when $\theta_{\mathrm{guess}} = \theta$, and 'no signal' otherwise, they can successfully break the protocol as long as they are allowed to respond 'no signal' on at least half of the played rounds.

To combat this issue, $\mathrm{QPV}_{\mathrm{BB84}}$ can be extended by adding more basis choices, i.e. $\theta \in \{0, \ldots, m-1\}$ and states $|0_\theta\rangle = \cos\left(\frac{\theta}{m}\frac{\pi}{2}\right)|0\rangle + \sin\left(\frac{\theta}{m}\frac{\pi}{2}\right)|1\rangle$, $|1_\theta\rangle = \sin\left(\frac{\theta}{m}\frac{\pi}{2}\right)|0\rangle - \cos\left(\frac{\theta}{m}\frac{\pi}{2}\right)|1\rangle$ [QS15, Spe16b]. This reduces the probability of correctly guessing to $1/m$. Of course, the guessing attack is just one possible attack in the lossy setting. However, [ES23] demonstrated for small values of m that, indeed, the protocol then becomes more loss resistant also against general unentangled attacks. [ES23] also provides a tight characterisation of the secure regime of $\mathrm{QPV}_{\mathrm{BB84}}$, given an honest error rate p_{err} and loss $1 - \eta$.

$\mathrm{QPV}_{\mathrm{BB84}}$ has also been considered in a slightly generalised form, namely with an angle θ between the two input bases (BB84 states correspond to $\theta = \pi/4$). To that end, [OCCG20] showed attacks for certain families of angles depending on the dimension d of the pre-shared entangled resource state for small d. In particular, they provide an attack for $\theta = \pi/6$, which lies outside of the Clifford hierarchy, using a $d = 6$ dimensional resource state.

[MA24] considered a further generalised version of this protocol, where the qubit is encoded in the eigenbasis of a projector Π chosen uniformly at random from the set of all orthogonal projectors onto one-dimensional subspaces of $\mathbb{C}^2$. Instead of θ Bob sends a description of Π, and P has to measure $\{\Pi, \mathbb{1} - \Pi\}$. Then, [MA24] shows that this protocol requires infinite resources for a *perfect* attack. Note that this doesn't contradict the general port-based teleportation attack, since that attack is approximate with arbitrary $\varepsilon > 0$.

Moreover, $\mathrm{QPV}_{\mathrm{BB84}}$ can be generalised to the CV setting [QS15, AER+23], where $H^\theta|z\rangle$ is replaced by a coherent state $|\psi\rangle$ with quadratures $(x(\theta), p(\theta))$

and θ is chosen from a set of angles in $[0, 2\pi)$. The task of the prover then is to perform a homodyne measurement on $|\psi\rangle$ in the θ direction to essentially estimate the quadrature values $x(\theta), p(\theta)$. However, as argued in [QS15], a simple attack exists for $\eta \leq 1/2$, to which currently no workaround is known due to the properties of CV quantum states.

f-routing

This protocol was also first introduced in [KMS11] and has been extensively studied since then. A single round of this protocol is defined as follows and is depicted in Figure 3.6. To boost security, again the protocol can be repeated (with the same f), although it is currently unknown if f-routing fulfils parallel repetition.

1. Verifiers $\mathsf{V_A}$, $\mathsf{V_B}$ draw two bit strings $x, y \in \{0,1\}^n$ uniformly at random and agree on a Boolean function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. $\mathsf{V_A}$ sends the qubit $|\psi\rangle$ and x, $\mathsf{V_B}$ sends y to P such that the qubit and the bit strings arrive at P simultaneously.

2. Upon receiving the inputs, P calculates $f(x, y)$ and immediately routes $|\psi\rangle$ to $\mathsf{V_A}$ if $f(x, y) = 0$ and to $\mathsf{V_B}$ if $f(x, y) = 1$.

3. The verifiers measure $\{|\psi\rangle\langle\psi|, \mathbb{1} - |\psi\rangle\langle\psi|\}$ to check whether the correct verifier received the qubit and if the state was received in time (i.e. $\Delta t_{\mathsf{A}} = 2d(\mathsf{V_A}, \mathsf{P})/c$ or $\Delta t_{\mathsf{B}} = 2d(\mathsf{V_B}, \mathsf{P})/c$ after they sent out the inputs, respectively). If both tests are passed, they *accept*. Otherwise, they *reject*.

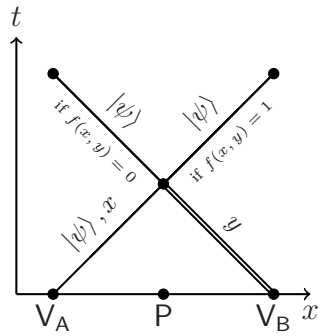


Figure 3.6: The f-routing QPV protocol.

The security of f-routing strongly depends on the complexity of computing f. The nature of the qubit $|\psi\rangle$ is irrelevant, but it is necessary to be included, as it is unclonable information. This also makes f-routing practically attractive, because

the honest prover's action is very simple, easy to implement and otherwise just classical computation of $f(x, y)$.

Attacks on f-routing were first studied in [BFSS13], defining a new model of communication complexity called *garden hose complexity* of f, denoted by $GH(f)$. The garden hose model is directly inspired by the attack setting of f-routing. This allows one to study both $GH(f)$ for specific functions and general properties of $GH(f)$. The analogy goes as follows: there is a water tap at Alice (the qubit $|\psi\rangle$), Alice and Bob share a number of hoses (EPR pairs) and based on their local inputs x and y, respectively, they have to connect certain hoses locally (do local Bell measurements on the corresponding qubits of 2 EPR pairs) such that finally the water (the qubit $|\psi\rangle$) ends up at Alice if $f(x, y) = 0$ and at Bob if $f(x, y) = 1$. It is simple to see that any garden hose strategy to compute f corresponds to an attack on f-routing. However, an attack on f-routing does not necessarily have to be of the garden hose form. Notable results from [BFSS13] regarding QPV are that: (i) the set of functions with polynomial $GH(f)$, and thus an efficient entanglement attack, is equal to the complexity class $\mathsf{L}_{(2)}$, i.e. functions computable in log-space with local pre-processing, (ii) there exist functions whose $GH(f)$ is exponential, indicating that such functions might be harder to attack, and (iii) for perfect attacks the dimension of the quantum resources of the attackers must be $\Omega(n)$ for a random function. Later, in [BCS22] it was shown that the latter result holds more generally in the robust and noisy setting, establishing another very attractive practical property of f-routing: the quantum attack resources robustly scale in the *classical* input information.

Since the definition of the protocol, attacks on f-routing have been connected to more properties of f. [CM23] found an explicit attack using $O(\mathtt{Span}_{p,(2)}(f))$ EPR pairs, where $\mathtt{Span}_{p,(2)}(f)$ is the minimal size of a span program over the field $\mathbb{Z}_p$ that computes f with local pre-processing. Since the set of functions with $\mathtt{Span}_p(f) = \mathrm{poly}(n)$ corresponds to the complexity class $\mathrm{Mod}_p\,\mathsf{L}$ this result also extended the class of efficiently attackable functions from $\mathsf{L}_{(2)}$ to the (potentially) larger class $\mathrm{Mod}_p\,\mathsf{L}_{(2)}$. Moreover, for tasks where f can be realised as an indicator function of a quantum secret sharing scheme, [CM23] proves that any quantum secret sharing scheme with f as its indicator function yields, via their new code-routing protocol, an attack on f-routing. Hence, the entanglement cost is upper bounded by the size of any quantum secret sharing scheme with f as its indicator function.

f-routing has also been connected to classical information theoretic cryptography, most notably to *conditional disclosure of secrets* (CDS) protocols [ABM+24]. It turns out that the classical analogue to f-routing *is* CDS. Among other things, [ABM+24] shows that f-routing is equivalent to the quantum generalisation of CDS, *conditional disclosure of quantum secrets* (CDQS) in the sense that a protocol for one induces a protocol for the other using similar resource and that a CDS protocol induces a CDQS protocol using similar resources. Thus, lower bounds on f-routing imply lower bounds on the randomness complexity of CDS proto-

cols. The connections drawn in [ABM+24] had further surprising implications for f-routing. Using the corresponding result for CDS [LVW17], quite unexpectedly the first sub-exponential upper bound on the entanglement cost for generic f-routing of $2^{O(\sqrt{n \log n})}$ was found. Furthermore, for a function related to the *quadratic residuosity problem* that is conjectured to be outside of $\mathsf{P}_{(2)}$ but inside of BQP, an efficient f-routing protocol was found.

More recently, lower bounds on f-routing attacks in terms of the Schmidt rank of the entangled resource state were found [ACM24], albeit only for perfect attacks. In [ACCM24] a $\Omega(n)$ lower bound on the necessary number of quantum gates or measurements attackers must apply was proven for the inner product function $f(x, y) = \sum_{i=1}^{n} x_i y_i$. This result also holds in the robust setting and is the first linear lower bound on quantum attack resources for a concrete function.

Practically speaking, essentially the same considerations as to $\mathrm{QPV}_{\mathrm{BB84}}$ apply. Unfortunately, f-routing is not natively loss tolerant, as attackers can always simply guess the value of $f(x, y)$. Another disadvantage is that it requires two-way quantum communication, from the verifiers to P and back. Sending quantum information without destroying or losing it is still a very hard task.

$\mathbf{QPV_{Bell}}$

The flavour of this protocol is slightly different, as it contains only quantum input information. It was first studied in [Mal10b] and a related version of it in [Mal10a], although it was claimed unconditionally secure, which turned out to be wrong. Similar variations were studied in [LL11], which also found the first attack on this protocol. Another closely related protocol was further analysed in [LXS+16] with a focus on loss tolerance and separable inputs instead of entangled ones for practicality. In all of those, the main task of the honest prover is to perform a Bell state measurement (BSM). The protocol we consider here has the following description and is shown in Figure 3.7.

1. Verifiers $\mathsf{V_A}$, $\mathsf{V_B}$ draw two bits $i, j \in \{0, 1\}$ uniformly at random. They create the Bell state $|\Phi_{ij}\rangle_{V_A V_B} = \mathbb{1} \otimes X^i Z^j |\Phi_+\rangle_{V_A V_B}$ and $\mathsf{V_A}$ sends the V_A part, $\mathsf{V_B}$ the V_B part to P such that both qubits arrive at P simultaneously.

2. Upon receiving the inputs, P performs a Bell measurement on the inputs, obtaining the encoded bits i, j. P immediately sends i, j to both verifiers.

3. The verifiers check if the answer they received is correct (i.e. equal to i, j) and if the answers were received in time (i.e. $\Delta t_{\mathsf{A}} = 2d(\mathsf{V_A}, \mathsf{P})/c$ and $\Delta t_{\mathsf{B}} = 2d(\mathsf{V_B}, \mathsf{P})/c$ after they sent out the inputs, respectively). If both tests are passed, they *accept*. Otherwise, they *reject*.

$\mathrm{QPV}_{\mathrm{Bell}}$ is secure against unentangled attackers and the currently best known upper bound on the attack success probability is $\ln(2) \approx 0.69$ [ABSV22, ACG+23].

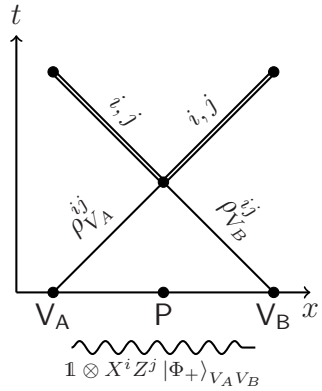


Figure 3.7: The QPV_{Bell} protocol.

Although it is suspected that the bound should be 1/2, like for attacks with classical communication only. However, a round of QPV_{Bell} can be broken with just 1 EPR pair [LL11] and creating, distributing and sending a Bell state to the prover coherently over long distances is a hard task, so this protocol has some disadvantages over others. It has one very interesting property, though: it is *fully loss tolerant*, meaning that in its secure regime it cannot be attacked for any transmission value $\eta \in (0, 1]$. This was proven for attackers restricted to classical communication in [LXS+16], which also considered a practical implementation based on decoy states, and further extended to general unentangled attacks in [ABSV22], parts of which we will encounter in Chapter 5 of this thesis. By looking at this protocol in the purified setting, it becomes evident that QPV_{Bell} is equivalent to completing the task of entanglement swapping. This can be used to show that 1 EPR pair is necessary to break one round of QPV_{Bell}, and n EPR pairs are necessary to break n sequential or parallel rounds. Another nice property for practice is that the prover is passive and always applies the same fixed measurement in each round.

The protocol QPV_{SWAP} that we will encounter in Chapter 4 is related to QPV_{Bell}, but experimentally more flexible and simpler to implement.

$\text{QPV}^{f}_{\text{BB84}}$

This protocol is in some sense a combination of f-routing and QPV_{BB84}, except that the prover does not route the qubit, but measures it in the basis given by $f(x, y)$. It was first introduced in [KMS11] and was later analysed in [BCS22, ES23] and combines the desired properties of both protocols. The protocol description is analogous to QPV_{BB84}, except that now Alice encodes $H^{f(x,y)} |z\rangle$ and also sends $x \in \{0, 1\}^n$, Bob sends $y \in \{0, 1\}^n$ instead of θ and P

measures in basis $f(x, y)$ instead of θ. The protocol is depicted in Figure 3.8.

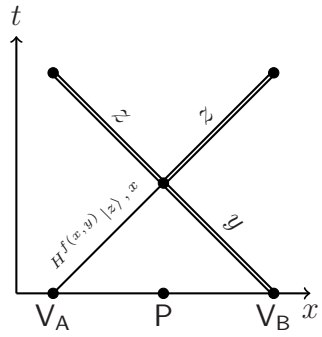


Figure 3.8: The $\text{QPV}^{f}_{\text{BB84}}$ protocol.

$\text{QPV}^{f}_{\text{BB84}}$ would be a very interesting practical candidate for QPV, and a similar characterisation in terms of p_{err} and $1 - \eta$ as for QPV_{BB84} was done in [ES23]. However, it is not loss tolerant. Even though some loss-resistance can be achieved by adding more basis options to the image of f [ES23], this only shifts the problem to slightly longer distances without really solving it, because loss scales exponentially in the distance. Moreover, like QPV_{BB84}, also $\text{QPV}^{f}_{\text{BB84}}$ can be generalised to the CV setting [AEFR+24] and analogous security statements were proven.

Other protocols

A few other protocols that we will not describe in much detail have been published [Mal10a, Mal10b, LL11, CL15, GLW16, DS21]. Some of them are variations or extensions of QPV_{BB84}, $\text{QPV}^{f}_{\text{BB84}}$ or QPV_{Bell}. Notable exceptions are [CL15], where the measurement basis is encoded in an interleaved product of unitaries coming from $\mathsf{V_A}$ and $\mathsf{V_B}$, respectively, as well as [GLW16], which relaxes the demand that the inputs reach P simultaneously and encodes the measurement basis in whether the input from $\mathsf{V_A}$ or the one of $\mathsf{V_B}$ arrives first. None of those other protocols are secure or have significant advantages over the ones we described.

3.2.2 Universal attack on QPV

Soon after the first attacks on specific protocols were found, [BCF+14] proved a general attack on QPV, showing that information-theoretically secure QPV is impossible. It is based on a rather involved recursive back-and-forth teleportation scheme known as the Vaidman scheme [Vai03]. The amount of entanglement this attack consumes to achieve success probability $1 - \varepsilon$ in applying a generic unitary U_{AB} to a generic $2n$-qubit state $|\psi\rangle_{AB}$ is a doubly exponential $O\big(2^{\log(1/\varepsilon)2^{4n}}\big)$

[CCJP10]. This enormous amount was later reduced to the still enormous exponential $O\left(\frac{2^{8n}}{\varepsilon^2}\right)$ in [BK11] employing port-based teleportation. The port-based attack is much simpler and proceeds as follows:

1. Alice intercepts her share of the input and teleports the n qubits to Bob, incurring a teleportation correction P_k.
2. Bob now holds $\mathbb{1} \otimes P_k \left|\psi\right\rangle_{AB}$, but doesn't know P_k. He port-teleports that entire $2n$-qubit state back to Alice, learning the correct port $i_\star$.
3. Alice applies $U_{AB}\mathbb{1} \otimes P_k^\dagger$ to *all* ports. On port $i_\star$ the state now is $U_{AB} \left|\psi\right\rangle_{AB}$ up to error ε.
4. Alice sends the B part of all ports to Bob, Bob sends the correct port index $i_\star$ to Alice.
5. Both of them discard all ports except $i_\star$ and send what is contained in port $i_\star$ to their respective verifiers. They have indeed collectively applied U_{AB} to $\left|\psi\right\rangle_{AB}$ up to error ε.

This scheme works almost identically if a POVM $\{\Pi_{AB}^k\}_k$ is considered at P. The only difference is that Alice then applies, after correcting P_k by $P_k^\dagger$, the measurement instead of the unitary to all ports and sends all tuples (j, α_j) to Bob, where α_j denotes the outcome of the measurement at port j. After communication, they select the correct measurement outcome $\alpha_{i_\star}$ and send it to the verifiers.

We briefly sketch how to estimate the number of EPR pairs required to carry out this attack. Alice first teleports an n-qubit state to Bob using n EPR pairs. For the port-based teleportation, by [BK11, Corollary II.2],

$$\|\mathcal{E}^{\mathrm{PBT}}_{|\Phi\rangle^{\otimes N}} - \mathcal{I}_{\mathbb{C}^d}\|_\diamond \leq \frac{4d^2}{\sqrt{N}}, \tag{3.1}$$

Bob needs to use $N = 2^{8n+4}/\varepsilon^2$ ports to ε-approximate the identity channel on port $i_\star$. Thus, he needs another $2^{8n+4}/\varepsilon^2$ EPR pairs of dimension $2n$. Hence, they use up $O\left(\frac{2^{8n}}{\varepsilon^2}\right)$ EPR pairs in total. [BK11] is the best known general attack on QPV and since the required entanglement resources are huge, the hope is that we can find QPV protocols with a matching (or at least superlinear) lower bound such that an attack is practically infeasible. Finding such a protocol is one of the main research directions in position-based quantum cryptography.

3.2.3 Ways around the universal attack

A pre-shared secret between the verifiers and the prover

[Ken11] considers a different security model in which the verifiers and the prover share a secret unknown to the attackers. This is not an unreasonable assumption

and such a secret could be expanded indefinitely via quantum key distribution between at least one verifier and the prover, and indeed, this is how the protocol in [Ken11] works. One verifier, say $\mathsf{V_A}$, and the prover are assumed to share an initial secret bit string in order to authenticate their channel[5]. Given that, QKD can expand the secret indefinitely and in an unconditionally secure way [TL17]. The QPV protocol then simply sends random bits a_i, b_i from the verifiers to the prover, which together point to a certain index $f(a_i, b_i)$ in the key string, which the prover has to send back to the verifiers. In the end, they check whether the key bit is correct. Security follows from the security of QKD. The weakness of this protocol is that QKD requires an authenticated channel. Common powerful authentication schemes require a pre-shared secret. For that, the prover would have had to interact with the verifiers (at some point in the past, perhaps), which might be an undesirable assumption.

The quantum random oracle model

[Unr14] employs the quantum random oracle model (QROM) to show that the protocol $\mathrm{QPV}^{f}_{\mathrm{BB84}}$, with $H(x, y) = x \oplus y$, is unconditionally secure in the QROM (the basis being the output of a function f modelled by a random oracle H on input $x \oplus y$). This work also carefully considers the spatially higher-dimensional scenario and even allows for curved space-times. [Unr14] shows that no space-time event outside of P's location can achieve a success probability higher than $2q2^{-\ell/2} + \left(2^{h(\gamma)}\left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)\right)^{n}$ when at most q queries to the random oracle are made, n parallel rounds are played, the input bit strings have length ℓ, and the honest prover is allowed an error rate γ. Notably, this bound is independent of the size of the other quantum resources used. For $\gamma \leq 0.037$ the term in brackets is smaller than 1, and thus exponentially suppressed in n. Moreover, as long as q is polynomially bounded in ℓ, the first term is also exponentially suppressed and the attack success probability becomes negligible with increasing ℓ and n.

LWE hardness

An interesting QPV protocol was proposed in [LLQ22] under an additional cryptographic assumption, namely that the task of *learning with errors* (LWE) is hard even for a quantum computer. Under this assumption, a QPV protocol based entirely on classical inputs and outputs can be constructed (despite the classical impossibility of position verification) and parallel repetition can be shown. To be more precise, assuming sub-exponential hardness of LWE they define a QPV protocol secure against attackers with linear amounts of pre-shared entanglement and sub-exponential time. And assuming exponential hardness of LWE, the unconditional security of [Unr14] in the QROM carries over to this protocol as well

[5] QKD assumes an authenticated channel between the involved parties.

(with polynomial-time attackers), by letting the basis information be the output of a random oracle.

Their protocol is based on the fact that if LWE is hard even for a quantum computer, then a certain class of functions called *noisy trapdoor claw-free functions* (NTCFs) can be constructed. The QPV protocol then has two stages. First, the verifiers send some classical information to P, who is asked to compute the NTCF of the protocol f_{pk} in superposition[6] and measure the function register. Based on the properties of NCTFs, this creates a computationally unclonable post-measurement state $(|x_0\rangle + |x_1\rangle)/\sqrt{2}$, where the x_i are elements of some set $\mathcal{X}$. In stage two, the verifiers send a basis choice to P and the prover is asked to measure the created state in this basis and report the result. If completed successfully, the statistics of the prover supply a *proof of quantumness* of his operations.

The protocol of [LLQ22] has the stark advantage that only classical communication is involved and all quantum computation happens locally. This would make it practically very appealing. However, in the protocol the prover has to create and manipulate a large quantum state of dimension $|\mathcal{X}|$, making this protocol not viable for the foreseeable future. Moreover, it may turn out to be possible that a quantum computer can compute LWE efficiently.

3.2.4 A protocol with conjectured exponential lower bound

The mentioned ways around the universal attack all have additional assumptions. In terms of finding protocols with no further assumptions and superlinear lower bounds, [JKPP22] made progress by connecting QPV to Banach space geometry with their protocol $\mathrm{QPV}_{\mathrm{Rad}}$. Their protocol is of theoretical interest, but has some practical drawbacks like two-way quantum communication. It is depicted in Figure 3.9 and is described as follows.

1. The verifiers draw a vector $\boldsymbol{\varepsilon} = (\varepsilon_{ij})_{i,j=1}^{n}$ of length n^2 with $\varepsilon_{ij} \in \{-1, 1\}$ uniformly at random and prepare the state $|\psi\rangle_{ABV} = \frac{1}{n}\sum_{i,j} |ij\rangle_{AB} |ij\rangle_V$. $\mathsf{V_A}$ sends registers AB and $\mathsf{V_B}$ sends ε to the prover such that all information arrives simultaneously at P.

2. The task of P is to apply the diagonal unitary $U_{AB} = \mathrm{diag}(\boldsymbol{\varepsilon})$ to the registers AB and immediately send back A to $\mathsf{V_A}$ and B to $\mathsf{V_B}$.

3. The verifiers check if the correct unitary was performed by applying the measurement $\{|\psi_{\boldsymbol{\varepsilon}}\rangle\langle\psi_{\boldsymbol{\varepsilon}}|, \mathbb{1} - |\psi_{\boldsymbol{\varepsilon}}\rangle\langle\psi_{\boldsymbol{\varepsilon}}|\}$ to registers ABV, where $|\psi_{\boldsymbol{\varepsilon}}\rangle = \frac{1}{n}\sum_{i,j} \varepsilon_{ij} |ij\rangle_{AB} |ij\rangle_V$. They accept if the answer was received in time and the measurement outcome is the one associated with $|\psi_{\boldsymbol{\varepsilon}}\rangle$. Otherwise they reject.

[6] I.e. create the state $\frac{1}{\sqrt{|\mathcal{X}|}}\sum_{x\in\mathcal{X}} |x\rangle |f_{\mathsf{pk}}(x)\rangle$.

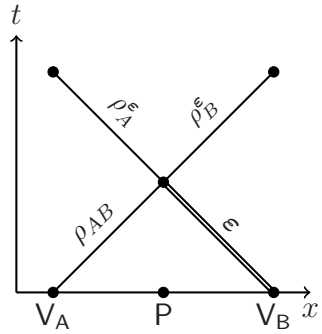


Figure 3.9: The QPV_{Rad} protocol.

The main result of [JKPP22] is that this protocol requires an exponential amount of pre-shared entanglement (in n) to be attacked, under a regularity assumption on the attack strategy. Hence, this is also not an unconditional exponential lower bound. However, [JKPP22] further connects the validity of the exponential lower bound in the unconditional setting to a conjecture in Banach space theory, namely on the conjectured properties of certain *type constants* of certain Banach spaces. If this purely mathematical conjecture is proven to the positive, this protocol has an exponential lower bound. However, the conjecture is a long standing open problem and expected to be hard to solve.

3.2.5 Quantum position-based authentication protocols

The setting of QPA is a bit different from that of QPV, as mentioned before. In particular, one has to be careful about substitution attacks in which attackers substitute the message to be authenticated with a message of their choice. [BCF+14] proposed a general construction to use QPV for QPA and we will briefly describe it now. The basic building block is what they call weakQPA, a protocol to authenticate a bit $m \in \{0, 1\}$, which is a priori known to all parties. It employs QPV in a generic way as follows.

1. The verifiers generate the inputs of a QPV protocol and send them to the prover such that all information arrives simultaneously.

2. P computes the authentication tag $t(m)$. If $m = 1$, P just completes the QPV task and responds. If $m = 0$, he completes the QPV task, but responds only with probability $1 - q$ and some other symbol $\perp$ with probability q.

3. The verifiers check if they received the same responses and if they arrived at the appropriate time. Moreover, they check if the response $t(m)$ corresponds

to the correct answer of the QPV task, or whether both $t(m) = \perp$ and $m = 0$. If these tests are passed, they accept. Otherwise they reject.

This protocol assumes an underlying QPV protocol with perfect completeness, i.e. the prover can complete the task perfectly and there is the notion of correct answers. The crucial ingredient is, in fact, not responding with the QPV answer with probability q. For the attackers it is easy to substitute $m = 1$ by $m' = 0$ by just intercepting the prover's response and replacing it with $\perp$ with probability q. However, if they want to replace $m = 0$ by $m' = 1$ they need to replace $\perp$ with the correct QPV answer and thus need to break the underlying QPV protocol. Likewise, if they want to impersonate P when he's not present, they also have to break the QPV protocol. Security of weakQPA thus follows from the security of the underlying QPV protocol.

The protocol weakQPA can be extended to longer messages $m \in \{0,1\}^\mu$, but one has to be careful how to encode m. To protect against substitution attacks and gain good security, one would like to have many slots in the code word $c(m)$ that are difficult to hack for attackers for *any* $m' \neq m$. To that end, [BCF+14] defines λ-dominating codes, which guarantee to have at least a certain amount of $c_i = 0$ and $c'_i = 1$ slots for any two different code words (originating from different $m' \neq m$). For the precise extended QPA scheme we refer to [BCF+14], but essentially it is bit-wise weakQPA of the encoded $c(m) \in \{0,1\}^N$ using a λ-dominating code on the input message m. [BCF+14] shows exponential completeness and soundness of this construction in the security parameter λ for unentangled attackers and also gives an explicit example of a λ-dominating code. In addition, they discuss how to use the QPA protocol as a step to achieve PB-QKD.

[Unr14] pointed out that the above generic construction is inefficient and its security under adaptive attacks is unclear. They go on to provide a secure QPA scheme based on $\mathrm{QPV}^f_{\mathrm{BB84}}$ in the QROM by including the message m in the oracle queries.

It remains open and crucial for a real implementation of PB-QKD to find an efficient and secure QPA protocol in the standard setting without random oracles.

3.2.6 Towards understanding non-local quantum computation

The question of simulating a bipartite operation by means of local operations and one round of simultaneous communication is interesting in its own right from a theory standpoint and has been studied under the name of *non-local quantum computation* (NLQC)[7]. It could also lead to faster distributed quantum

[7] Also under the name *instantaneous non-local quantum computation* (INQC), *local operations and broadcast communication* (LOBC) or *local operations and simultaneous quantum communication* (LOSQC).

computing [YGC12]. We will focus on the simplest scenario of two parties non-locally simulating a bipartite operation, as above for QPV, but one can think about this in more general relativistic quantum tasks [Ken12, Dol19]. NLQC has been connected to many different fields of study, as illustrated in Figure 3.10.

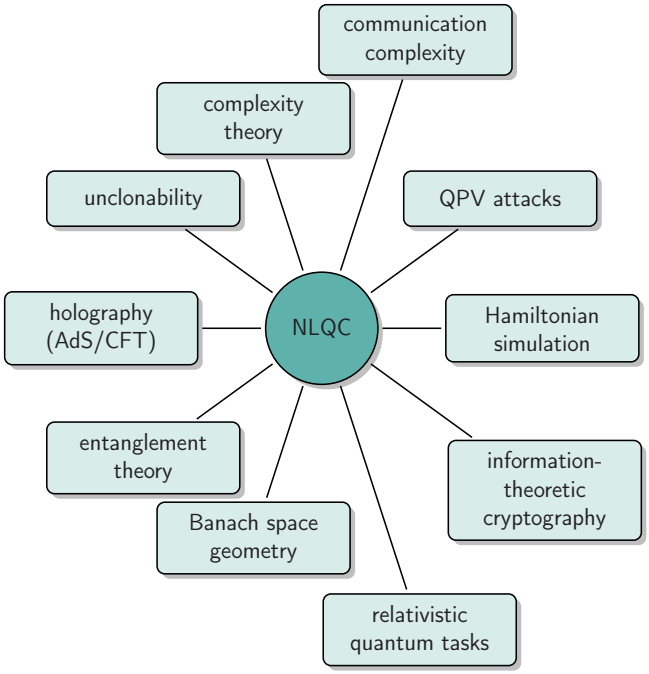


Figure 3.10: The currently known connections of NLQC to other fields of study.

Partially, we've already covered these connections in the sections above. In addition, [May22] showed that, for tasks where one input side is some classical x (like QPV_{BB84}), the complexity[8] of the entangled part of the task $\{U^x_{AB}\}_x$, denoted $C_{\{U_x\}_x}$, controls the entanglement cost, using that any bipartite unitary can be decomposed into local pre- and post-processing and some entangled part in between. In particular, this gives a doubly logarithmic lower bound $\Omega(\log\log C_{\{U_x\}_x})$ in terms of $C_{\{U_x\}_x}$, which was later improved to $\Omega(\log C_{\{U_x\}_x})$ by improving the efficiency of the involved port-based teleportation [FTH23, GBO23, Ngu23]. The exponential upper bound from the port-based attack can also be recast in terms of $C_{\{U_x\}_x}$ as $O(C_{\{U_x\}_x} 2^{C_{\{U_x\}_x}})$.

[Bro16] showed that if Alice and Bob share Popescu-Rohrlich (PR) boxes [PR94], a form of post-quantum correlations, they can implement any unitary via NLQC using only linear entanglement and a linear number of uses of a PR box.

[8] Any notion of complexity you'd like, for example circuit complexity.

Interestingly, and perhaps surprisingly, the line of work in [MPS20, May19, DC22a, May22] shows an intriguing connection between holography, particularly the AdS/CFT conjecture, and NLQC. Based on the AdS/CFT conjecture, these papers argue, among other things, that efficient polynomial attacks can be constructed for all QPV protocols. In particular, [May19] argued that 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. This puts forward an exciting tension between the fields of quantum gravity and position-based quantum cryptography: either holographic arguments allow for an efficient attack on generic QPV, or, if a super-polynomial lower bound can be shown for QPV from the cryptographic side, this poses constraints on possible theories of quantum gravity and the currently widely believed AdS/CFT conjecture could not be fully true. Moreover, the tension carries over to pure mathematics via the connection to Banach space geometry from [JKPP22].

Furthermore, as already alluded to in the section on f-routing, NLQC has been connected to topics in information-theoretic cryptography [CM23, ABM+24, AGLL24]. In particular, conditional disclosure of secrets (CDS), private simultaneous message (PSM) passing and secret sharing (SS) schemes turn out to be related to f-routing and thus NLQC.

Recently, another connection to Hamiltonian simulation was discovered in [ACH+24]. If a superlinear lower bound can be shown for QPV attacks, then there are new fundamental lower bounds for resources required for one Hamiltonian to simulate another.

In view of how difficult it is to say anything general about NLQC, all these drawn connections are useful, because results from any of those connected fields of study may give new insights into NLQC and vice versa. Moreover, different attack scenarios can be considered depending on the entanglement and communication the attackers use. We can distinguish between

- LOSCC: Local operations and 1 round of simultaneous classical communication,
- eLOSCC: Local operations and 1 round of simultaneous classical communication plus pre-shared entanglement,
- LOSQC: Local operations and 1 round of simultaneous quantum communication and
- eLOSQC or NLQC: Local operations and 1 round of simultaneous quantum communication plus pre-shared entanglement.

The difference between those settings has only been explicitly studied recently, in [ABSV22, GALC23], which we will encounter in Chapter 5. There, we study fundamental properties and differences of LOSCC and LOSQC. First, a separation between LOSCC and LOSQC was shown in [ABSV22], but only for entangled inputs. In [GALC23], we give necessary and sufficient conditions for perfect attacks in each model and an error lower bound for ensembles containing a certain structure. Moreover, we demonstrate that LOSQC can be strictly more powerful than LOSCC even for product inputs. [ABSV22] also gives a non-constructive argument showing that one can distill a QPV protocol secure in the LOSQC setting from a QPV protocol secure only in the LOSCC setting.

3.2.7 Towards practicality

The three major problems that prevent QPV from being feasible at present are: entangled attackers, slow quantum information and signal loss. The first one is unavoidable even in a perfect execution of the protocols and can hopefully be mitigated by finding a protocol with decent security guarantees against bounded entanglement attacks, but the latter two arise from experimental constraints. Whereas the transmission of classical information at the speed of light is technologically feasible in an almost lossless fashion, the quantum counterpart faces obstacles. Firstly, most QPV protocols require quantum information to be transmitted at the speed of light in vacuum, because if it travels slower then attackers, who are assumed to be able to quantum communicate at the speed of light, could always position themselves such that one attacker has all the input information before P would get it, thus breaking the protocol. However, for practical applications, this is often unattainable. Therefore, a good QPV protocol should be able to tolerate slow quantum communication. The speed of light in optical fibres is significantly lower than in vacuum. Moreover, in a future quantum network with fibres it may often be the case that there is no straight point-to-point connection between the verifiers and the prover. Secondly, a sizable fraction of photons will be lost in transmission in practice. For example, in optical fibres this loss grows exponentially with the distance.

None of the QPV protocols mentioned so far have been able to successfully circumvent those three problems simultaneously at a useful scale. Any protocol that was able to solve one or two of the mentioned issues had shortcomings with respect to the other(s). $\mathrm{QPV}^{f}_{\mathrm{BB84}}$ bypasses them but only for relatively short distances [ES23] and without fundamentally solving the loss issue. If one wants to implement QPV in a future quantum internet, the goal would be to attain it for essentially arbitrarily long distances. In Chapter 6 we will define and study precisely such a protocol that overcomes all the major practical issues of QPV [ABB+23].

The study of QPV using CV quantum states in [QS15, LXS+16, AER+23, AEFR+24] is also motivated by practicality. CV systems are much simpler to

handle and leverage several decades of experience in coherent optical communication technology. Unlike discrete variable systems, no true single-photon preparation or detection is necessary, which is still expensive and technically challenging (especially if photon number resolution is desired). In contrast, homodyne and heterodyne measurements are much easier and cheaper to implement. Much existing infrastructure is geared towards handling light at low-loss telecom wavelengths (e.g. 1310nm, 1550nm), whereas an ideal single-photon source in these wavelength bands still has to be discovered, and frequency up-conversion is challenging and introduces new losses and errors. However, as mentioned for $\mathrm{QPV}_{\mathrm{BB84}}$, a simple attack exists for $\eta \leq 1/2$ to which currently no workaround is known due to the properties of CV quantum states. It remains an interesting open question whether transmission loss can also be made irrelevant for security in the CV setting, as has been the case in the discrete case [ABB+23].

Finally, for an actual implementation, one has to consider all kinds of imperfections in the equipment used. The computations of the prover actually do take some time (albeit probably very little) and thus limit the achievable protocol rate[9], the state preparation of the verifiers will be imperfect and also have limited rate, the equipment will be imperfectly calibrated, there are some inherent errors one cannot really get rid of like dark counts in detectors or accidental multi-photons, small environmental noises, some of the implicit assumptions on QPV only hold approximately, and so on. In an experimental demonstration and further practice, it is necessary to take care of all those headaches and ensure that the implemented protocol remains secure up to some achievable threshold. To that end, [CKPG23] studies some of the technical details of a real implementation.

3.3 Open problems to be tackled in this thesis

Loss tolerance and practicality

As mentioned before, signal loss is one of the main obstacles for QPV. In fact, given that $\mathrm{QPV}^{f}_{\mathrm{BB84}}$ can handle slow quantum information and has a desirable scaling of the entanglement attack, it is the last major theoretical implementation issue to be solved for QPV. Ideally, one would like to have full loss-tolerance, but loss-tolerance good enough for practical purposes would also be fine. A fully loss-tolerant QPV protocol has been proposed [LXS+16], but is unfortunately easily broken through an entanglement attack.

Moreover, a good chunk of the research in this thesis is motivated by practicality, and we intended to make progress on that by studying QPV under realistic conditions or overcoming issues that previously made it infeasible.

In Chapter 4 we study a protocol $\mathrm{QPV}_{\mathrm{SWAP}}$ based on the SWAP test, which

[9] For example, detectors have a short dead time after each detection event, or the honest processing also takes some time.

experimentally simplifies [LXS+16], while remaining fully loss tolerant and having other nice properties. We will also demonstrate that the new protocol remains reasonably robust against experimental imperfections.

In Chapter 6 we prove that a small modification of the standard QPV setting can make the transmission loss from the verifiers to the prover irrelevant for security for a class of QPV protocols that includes $\mathrm{QPV}^{f}_{\mathrm{BB84}}$. Therefore, we obtain the first explicit protocol, based on $\mathrm{QPV}^{f}_{\mathrm{BB84}}$, which solves all the major practical issues of QPV, bridging the gap that prevents QPV from being feasible with current technology.

In Chapter 7 we begin to extend the results of QPV with finite-dimensional quantum states to the continuous variable setting by studying a continuous variable version of $\mathrm{QPV}_{\mathrm{BB84}}$, which we further extended to $\mathrm{QPV}^{f}_{\mathrm{BB84}}$ in [AEFR+24].

Quantum communication

In QPV the attackers can use one round of simultaneous communication, which can be classical or quantum. In principle, using quantum communication could be more powerful than the classical counterpart, and at the start of this PhD it was an open question whether this could be proven. Indeed, quantum communication can be more powerful in this setting, as we first showed in [ABSV22] for entangled inputs and will show in Chapter 5 also for product state inputs.

Moreover, the basic communication model and operational capabilities when the adversaries do not share any entanglement are still not well understood. Considering quantum input and classical output protocols in the QPV setting, one can view this scenario as a form of time-constrained local quantum state discrimination. If restricted to classical communication, the success probability of this task can often be reduced to solving an SDP. However, not so with quantum communication. This places a gap in the study of QPV, relativistic quantum cryptography, and local quantum state discrimination in general. In Chapter 5 we make progress on closing this gap, thereby further clarifying the interplay between cryptography, quantum communication, and locality. Our main goal is to identify fundamental limitations in the task of time-constrained state discrimination when either classical or quantum communication is employed.

Chapter 4

Quantum Position Verification with the SWAP Test

Chapter summary. In this chapter, we study loss-tolerant QPV. We propose a new fully loss-tolerant protocol $\mathrm{QPV}_{\mathrm{SWAP}}$, 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. We show that the protocol remains secure even if unentangled attackers are allowed to quantum communicate. A detailed analysis is conducted under experimental conditions, indicating that $\mathrm{QPV}_{\mathrm{SWAP}}$ remains fairly robust against equipment errors. We simulate one instance of our protocol with currently realistic experimental parameters, gathering that an attack success probability of $\leq 10^{-6}$ can be achieved by collecting just a few hundred conclusive protocol rounds.

This chapter is based on the following paper:

[ABSV21] Rene Allerstorfer, Harry Buhrman, Florian Speelman, and Philip Verduyn Lunel. Towards practical and error-robust quantum position verification. *arXiv preprint*, 2021. arXiv:2106.12911

4.1 Introduction

Loss tolerance in QPV. Throughout, we will use η to denote the transmission rate in realistic protocols. We will distinguish two types of loss tolerance.

The first, *partial loss tolerance*, refers to a protocol that is secure for some values $\eta \geq \eta_{\mathrm{threshold}}$, meaning that the honest parties have a maximum level of

allowed loss. Security is only guaranteed in a situation where a high enough percentage of rounds is played. If significantly more photons than this threshold are lost, then the protocol will have to abort.

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.

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

1. We present a new fully loss-tolerant protocol: $\mathrm{QPV}_{\mathrm{SWAP}}$. It is based on the SWAP test [BCWdW01] and compares favourably with [LXS+16] in terms of ease of implementation using linear optics, by requiring only a single, non-polarising beam splitter. Physically, it is based on two-photon Hong-Ou-Mandel interference [OHM87], which is equivalent to the SWAP test [JAC04, GECP13]. Another notable property is that the setup of the prover is static and does not require any sophisticated fast switching between measurement settings.

2. We prove fully loss tolerant security by formulating possible attacks as a semidefinite program (SDP), and show that the protocol is secure against LOSCC attackers. Furthermore, 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. 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 of the problem, constructing a dual of this SDP for variable n, and then finding a solution for the generalised dual problem. We extend the security to LOSQC attackers, employing an argument based on the monogamy of entanglement from [ABSV22]. $\mathrm{QPV}_{\mathrm{SWAP}}$ is the first fully loss-tolerant QPV protocol with this property.

3. We show that the SWAP test can be perfectly simulated with local operations and one round of classical communication if one EPR pair is preshared. Hence, n EPR pairs are sufficient for an entanglement attack on the n-round protocol. We also show a lower bound of $\Omega(n)$.

4. We provide a detailed analysis of our protocol under experimental conditions, treating all equipment errors that can occur in the setup, from source to detection. We show that $\mathrm{QPV}_{\mathrm{SWAP}}$ remains fairly robust against equipment errors. An attack success probability of $\leq 10^{-6}$ can be achieved by collecting just a few hundred conclusive protocol rounds, given achievable experimental conditions.

4.2 Preliminaries

Notation

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 expressions like $\mathrm{Pos}(\mathsf{A} \otimes \mathsf{B})$, for example. Cumulative distribution functions are written as F_X, where X is either a random variable or explicitly the distribution. Unless otherwise indicated, $\|\cdot\|_p$ is the usual p-norm. Partial transposition of an operator P with respect to party B is denoted by P^{T_B}. The set of PPT-measurements[1] on two subsystems held by parties A and B, respectively, is $\mathrm{PPT}(\mathsf{A} : \mathsf{B})$.

The SWAP test

The SWAP test was first introduced in [BCWdW01] for quantum fingerprinting as a tool to determine whether two unknown states are identical or not. More generally, it can be used to estimate the overlap between two arbitrary states $|\psi\rangle, |\phi\rangle$. Its quantum circuit is depicted in Figure 4.1.

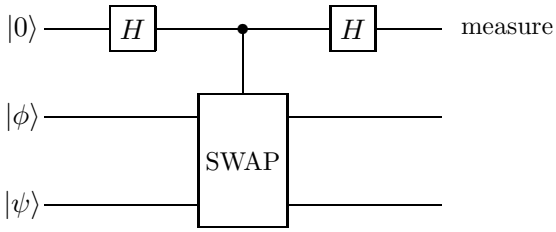


Figure 4.1: The SWAP test. H denotes the Hadamard gate.

The end state of the circuit is

$$(H \otimes \mathbb{1})\text{c-SWAP}(H \otimes \mathbb{1}) |0\rangle |\phi\rangle |\psi\rangle = \frac{1}{2} |0\rangle (|\phi\rangle |\psi\rangle + |\psi\rangle |\phi\rangle) + \frac{1}{2} |1\rangle (|\phi\rangle |\psi\rangle - |\psi\rangle |\phi\rangle). \tag{4.1}$$

Measuring the first qubit in the computational basis gives the measurement statistics

$$\mathbb{P}(0) = \frac{1 + |\langle\psi|\phi\rangle|^2}{2} \qquad \text{and} \qquad \mathbb{P}(1) = \frac{1 - |\langle\psi|\phi\rangle|^2}{2}. \tag{4.2}$$

[1] I.e. sets of positive semidefinite operators adding up to the identity, whose partial transposes are positive semidefinite as well.

The output distribution only depends on the overlap $|\langle\psi|\phi\rangle|$ between the input states. For $|\phi\rangle = |\psi\rangle$ the SWAP operation has no effect and 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 concerning input states and the simplicity of its experimental realisation make it a good candidate for QPV.

Uniformly random states

The inputs $|\psi\rangle, |\phi\rangle$ in our protocol will be uniformly random states. Hence, the overall mixed input state for a given overlap $\beta = |\langle\psi|\phi\rangle|$ will be

$$\begin{aligned}\rho_\beta &= \int_{\mathrm{U}(2)} U \otimes U \,|\psi\phi\rangle\langle\psi\phi|\, U^\dagger \otimes U^\dagger d\mu(U) \\ &= \frac{1}{3}\frac{1+\beta^2}{2}\Pi_{\mathrm{sym}} + \frac{1-\beta^2}{2}\Pi_{\mathrm{asym}}. \end{aligned} \tag{4.3}$$

Here, Π_{sym} and Π_{asym} are the projectors onto the symmetric and antisymmetric subspaces, respectively, and μ is the Haar measure on the unitary group U(2) [Wat18].

4.3 The $\mathrm{QPV}_{\mathrm{SWAP}}$ protocol

We define the protocol $\mathrm{QPV}_{\mathrm{SWAP}}(\beta_1, \ldots, \beta_k)$ for a set of overlaps $\{\beta_1, \ldots, \beta_k\}$ as follows. It is depicted in Figure 4.2. It intrinsically requires multiple rounds, because the task of the prover is to build up the measurement statistics of the SWAP test for each input overlap.

1. $\mathsf{V_A}$ and $\mathsf{V_B}$ draw a random overlap $\beta \in \{\beta_1, \ldots, \beta_k\}$ uniformly at random and agree on two uniformly random states $|\psi\rangle, |\phi\rangle$ such that $|\langle\psi|\phi\rangle| = \beta$. 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. P applies the SWAP test on the two quantum inputs. This yields an output bit $z \in \{0, 1, \varnothing\}$, where $\varnothing$ denotes a 'signal loss' event[2]. Then P immediately sends z to both verifiers.

3. The verifiers check if the answers were received in time and assure they received the same answer. If one of those checks fails, they abort. Otherwise both verifiers add z to their (ordered) lists of answers L_β.

[2] In particular, $\mathbb{P}(z = 0 \mid \beta, \text{not loss}) = (1+\beta^2)/2$ and $\mathbb{P}(z = 1 \mid \beta, \text{not loss}) = (1-\beta^2)/2$.

4. After having completed $R_\beta \geq R_{\text{threshold}}$ rounds with a conclusive answer $z \in \{0, 1\}$ for each β, they stop sending inputs, check if the rate of $\varnothing$ symbols is close enough to what is expected from P, discard any rounds with answer $\varnothing$ and proceed to the statistical analysis on the sets of conclusive answers $C_\beta = L_\beta - \{\varnothing\}$ for each β. They test if the sample parameter $\hat{p}_\beta = \#\{z \in C_\beta : z = 0\}/R_\beta$ on conclusive answers is contained in the $(1-\alpha)$-quantile around the expected $p_\beta = (1+\beta^2)/2$.

5. Only if they have received the same answer in time in every single round and if the statistical test was passed on all L_β, they accept. Otherwise, they reject.

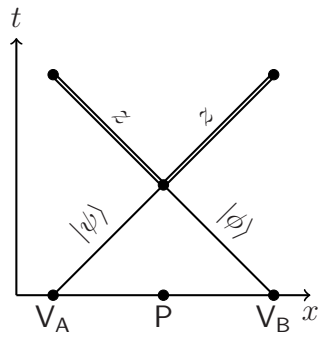


Figure 4.2: The $\mathrm{QPV}_{\mathrm{SWAP}}$ protocol.

Estimating the overlap is independent of the dimensionality/nature of the input states, making the protocol very flexible. The degree of freedom to encode the inputs states in can be chosen freely.

4.3.1 Security arguments for LOSCC

To assess the security of the protocol in this setting, we consider unentangled attackers restricted to local operations and 1 round of classical communication (LOSCC). As the individual rounds are independent, the subsets L_β of answers given input ρ_β will be samples of a binomial distribution with parameters R_β and p_β[3]. The verifiers can then test if what they received matches closely enough with what they expect from an honest party, i.e. the SWAP test statistics. We define the statistical test to be done by the verifiers as follows:

[3]Here and in the following the parameter describes the fraction of '0' answers and we abbreviate $p_\beta(0) = p_\beta$

1. For each overlap β, they calculate the $(1-\alpha)$-quantile[4] around the ideal $p_\beta = (1+\beta^2)/2$, which gives a lower and an upper bound

$$\begin{aligned} L_{\alpha,\beta} &\coloneqq z_{\frac{\alpha}{2}}(\beta, R_\beta)/R_\beta = F^{-1}_{\mathrm{Bin}(R_\beta,p_\beta)}\Big(\frac{\alpha}{2}\Big)/R_\beta \\ U_{\alpha,\beta} &\coloneqq z_{1-\frac{\alpha}{2}}(\beta, R_\beta)/R_\beta = F^{-1}_{\mathrm{Bin}(R_\beta,p_\beta)}\Big(1-\frac{\alpha}{2}\Big)/R_\beta, \end{aligned} \tag{4.4}$$

   with F^{-1} being the inverse cumulative distribution function. This defines an acceptance interval

$$\mathsf{acc}_\beta(\alpha, R_\beta) \coloneqq [L_{\alpha,\beta}, U_{\alpha,\beta}]. \tag{4.5}$$

2. For each overlap β, they check if the sample parameter $\hat{p}_\beta$ they receive satisfies $\hat{p}_\beta \in \mathsf{acc}(\alpha, R_\beta)$. If this is the case for all β, they accept. Otherwise, they reject.

By definition, the honest party will return a sample $\hat{p}^{\mathsf{P}}_\beta \in \mathsf{acc}_\beta(\alpha, R_\beta)$ with probability $1-\alpha$ and therefore the test will accept P with high probability $(1-\alpha)^k = 1 - O(k\alpha)$.

To optimise the overlap between the sample they respond with and the acceptance regions, the attackers will attempt to respond as close to each p_β as possible, with a binomial parameter of $p^{\mathsf{AB}}_\beta = p_\beta - \Delta_\beta$, defining a vector of errors

$$\Delta = \begin{pmatrix} \Delta_{\beta_1} \\ \vdots \\ \Delta_{\beta_k} \end{pmatrix}. \tag{4.6}$$

The attackers could also decide to just respond with a deterministic list with some fraction $\hat{p}^{\mathsf{AB}}$ of '0' answers. They could perfectly break the protocol if $\hat{p}^{\mathsf{AB}} \in \bigcap_\beta \mathsf{acc}_\beta(\alpha, R_\beta)$. However, we can always prevent this by choosing the R_β's large enough for the acceptance regions for different overlaps to become disjoint. Thus, we need to evaluate

$$\begin{aligned} \mathbb{P}(\mathsf{acc}|\mathsf{attack}) &\coloneqq \mathbb{P}\big(\hat{p}^{\mathsf{AB}}_\beta \in \mathsf{acc}_\beta(\alpha, R_\beta) \quad \forall\beta\big) \\ &= \prod_\beta \mathbb{P}\big(\hat{p}^{\mathsf{AB}}_\beta \in \mathsf{acc}_\beta(\alpha, R_\beta)\big) =: \prod_\beta \mathbb{P}(\mathsf{acc}_\beta|\mathsf{attack}). \end{aligned} \tag{4.7}$$

Now, there are several cases to consider:

1. $\|\boldsymbol{\Delta}\|_{\mathbf{1}} = \mathbf{0}$. Then $\Delta_\beta = 0$ for all β and the attackers respond with the identical distribution as P, therefore $\mathbb{P}(\mathsf{acc}|\mathsf{attack}) = (1-\alpha)^k = 1 - O(k\alpha)$.

2. $\mathbf{p_\beta \neq 1}$ **and** $\hat{\mathbf{p}}^{\mathsf{AB}}_{\boldsymbol{\beta}} = \mathbf{1}$. Then $\mathbb{P}(\mathsf{acc}|\mathsf{attack}) = 0$ as the $(1-\alpha)$-quantile around p_β will exclude the value 1 (for sufficiently large R_β).

[4] In order to capture P with high probability, α can be set to a small number, e.g. 10^{-6}.

3. $\mathbf{p_\beta = 1}$ **and** $\hat{\mathbf{p}}_{\boldsymbol{\beta}}^{\mathsf{AB}} \neq \mathbf{1}$. Then $\mathbb{P}(\mathsf{acc}_\beta|\mathsf{attack}) = \left(p_\beta^{\mathsf{AB}}\right)^{R_\beta}$.

4. $\|\boldsymbol{\Delta}\|_1 \neq \mathbf{0}$ **and** $\mathbf{p_\beta}, \hat{\mathbf{p}}_{\boldsymbol{\beta}}^{\mathsf{AB}} \in \left[\frac{\mathbf{1}}{\mathbf{2}}, \mathbf{1}\right)$. Then there exists a $\beta \in \{\beta_1, \ldots, \beta_k\}$ such that $\Delta_\beta \neq 0$. By using the Gaussian approximation for the binomial distributions (which we may apply because we can always make the number of rounds sufficiently large), one can show (see Appendix 4.7.1) that

$$\mathbb{P}(\mathsf{acc}_\beta|\mathsf{attack}) \lesssim \frac{\sqrt{2} f_\beta^{\mathsf{AB}}}{\sqrt{\pi R_\beta}\Delta_\beta} e^{-\left(\sqrt{R_\beta}\Delta_\beta - f_\beta^{\mathsf{P}} c_\alpha\right)^2 / \left(f_\beta^{\mathsf{AB}}\right)^2} \tag{4.8}$$

for functions c_α, f_β that are independent of R_β and Δ_β. Hence, the success probability of attackers is also in this case exponentially suppressed for sufficiently large R_β.

So, unless $\Delta_\beta = 0$ for all β, we have exponential suppression in the attacker success probability $\mathbb{P}(\mathsf{acc}|\mathsf{attack})$ in the number of rounds. In the end, we can set a threshold $R_{\mathrm{threshold}}$ for the number of rounds, and the protocol will run until $R_\beta \geq R_{\mathrm{threshold}}$ for all β. This will guarantee that any desired security level can be achieved by uniformly increasing $R_{\mathrm{threshold}}$ over all β.

We end up with a protocol that accepts an honest party with high probability and rejects (unentangled, classically communicating) attackers with high probability. A sketch of this is shown in Figure 4.3.

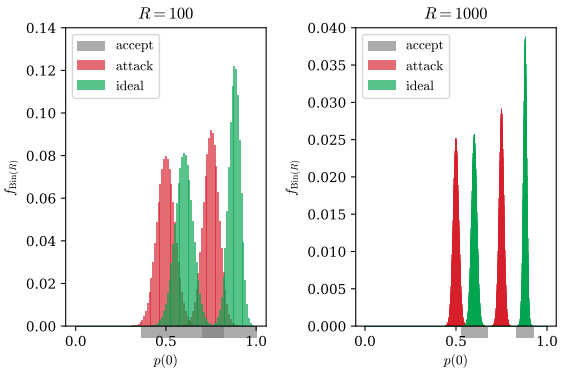


Figure 4.3: Illustrating the statistical test. Acceptance regions around the expected honest p_β's are defined such that P will pass with high probability. Attackers trying to spoof verifiers by minimizing all Δ_β as well as possible have exponentially low (in $R_{\mathrm{threshold}}$) probability of returning a sample contained in the acceptance regions for all β.

The analysis also suggests that optimally attackers want to minimize all $|\Delta_\beta|$

simultaneously[5]. We therefore choose to minimise $\|\Delta\|_1$. As LOSCC $\subset$ LOCC $\subset$ PPT [CLM+14], the following optimisation program will provide a lower bound on $\|\Delta\|_1$ for LOSCC attackers. To account for imperfect quantum channel transmission, we include a parameter $\eta \in (0, 1]$ and a third answer option $\varnothing$ ('signal loss'). Then Δ_β shall be evaluated conditioned on conclusive answers, i.e. $\Delta_\beta = p_\beta - \mathrm{Tr}[\Pi_0 \rho_\beta]/\eta$. We end up with the following optimisation:

$$\begin{aligned} \textbf{minimize:} \quad & \|\Delta\|_1 \\ \textbf{subject to:} \quad & \Pi_0 + \Pi_1 + \Pi_\varnothing = \mathbb{1}_4 \\ & \Pi_k \in \mathrm{PPT}(\mathsf{A} : \mathsf{B}), \qquad k \in \{0, 1, \varnothing\} \\ & \mathrm{Tr}[\Pi_\varnothing \rho_\beta] = 1 - \eta, \qquad \beta \in \{\beta_1, \ldots, \beta_k\}. \end{aligned} \tag{4.9}$$

The constraints involving η stem from the fact that P will produce the same 'signal loss' rate on all overlaps β and the attackers need to mimic that. An analogous statistical test with a $(1-\alpha)$-quantile around η can be performed to check for this, and it is evident that attackers will choose to reply inconclusive at the exact same rate as P would do for each β to always pass this hurdle. The above program can be solved with conventional optimisation libraries, e.g. `MOSEK` [ApS20], and any example of $\{\beta_1, \ldots, \beta_k\}$ we have tried yields an optimal $\|\Delta\|_1 > 0$ independent of η, indicating (but not proving) the loss tolerance of the protocol. Next, we rigorously prove the loss tolerance for the special case of $\beta \in \{0, 1\}$, for which we get $\|\Delta\|_1 \geq 1/4$.

The security of $\mathrm{QPV}_{\mathrm{SWAP}}$ in the setting where attackers are allowed to use one round of simultaneous quantum communication follows from [ABSV22], as shown in Section 4.3.2.

4.3.2 Security of the $\mathrm{QPV}_{\mathrm{SWAP}}(0, 1)$ protocol

We will now proceed and analyze a special case, arguably the simplest, of overlaps $\{0, 1\}$ (i.e. sending orthogonal or identical states) in more detail and show analytically and numerically that it has desirable properties.

Single round security for LOSCC

In this context, there is the notion of a correct answer. On equal inputs, the verifiers *always* expect the answer '0'. This allows for an SDP formulation to maximise the average success probability of identifying if the input states were equal/unequal. In Appendix 4.7.1 it is shown that the relation between the

[5] Minimizing $|p_\beta - p_\beta^{\mathsf{AB}}|$ also minimizes the Kullback-Leibler divergence $D_{\mathrm{KL}}(P \,\|\, Q)$ between the corresponding binomial distributions P and Q.

success probability p_{succ} of correctly identifying equal/orthogonal and $\|\Delta\|_1$ is

$$p_{\mathrm{succ}} \leq u \implies \|\Delta\|_1 \geq \frac{3}{2} - 2u. \tag{4.10}$$

We will now proceed to show that there is a finite gap in the success probability of testing for equality between LOSCC adversaries and the honest prover.

In general, the operation that has the highest average probability when testing state equality is, in fact, the SWAP test [MW16] and it gives a success probability $p_{\mathrm{succ}}(\text{SWAP test}) = 3/4$. We will show that the best strategy for LOSCC adversaries has at most $p^{\max}_{\mathrm{succ}}(\text{LOSCC}) = 2/3$. Since attackers return only a classical bit and discard their post-measurement state, the most general type of measurement the attackers perform is a *positive-operator-valued meaure* (POVM). The attackers' success probability for a POVM strategy $\Pi = \{\Pi_0, \Pi_1\}$ is then given by

$$p_{\mathrm{succ}}(\Pi) := \frac{1}{2}\operatorname{Tr}[\Pi_0\rho_0 + \Pi_1\rho_1]. \tag{4.11}$$

Characterising and maximising over LOCC strategies is a mathematically complex task. We follow the method used in [LXS+16], and maximise our problem over the set of all positive partial transpose (PPT) operations. Any maximal success probability optimised over PPT measurements immediately upper bounds the success probability of all LOCC measurements and thus also LOSCC. The PPT condition can be represented by a set of linear and positive semidefinite conditions [Cos13], enabling us to write down the maximisation problem as the following SDP:

$$\begin{aligned} &\textbf{Primal program} \\ \textbf{maximize:}\quad & \frac{1}{2}\operatorname{Tr}[\Pi_0\rho_0 + \Pi_1\rho_1] \\ \textbf{subject to:}\quad & \Pi_0 + \Pi_1 = \mathbb{1}_{2^2}, \\ & \Pi_k \in \mathrm{PPT}(\mathsf{A}:\mathsf{B}), \\ & k \in \{0,1\}. \end{aligned} \tag{4.12}$$

$$\begin{aligned} &\textbf{Dual program} \\ \textbf{minimize:}\quad & \operatorname{Tr}[Y] \\ \textbf{subject to:}\quad & Y - Q_i^{T_{\mathsf{B}}} - \rho_i/2 \succeq 0, \\ & Y \in \mathrm{Herm}(\mathsf{A}\otimes\mathsf{B}) \\ & Q_i \in \mathrm{Pos}(\mathsf{A}\otimes\mathsf{B}), \\ & i \in \{0,1\}. \end{aligned} \tag{4.13}$$

Note that the primal program implies a lower bound and the dual program an upper bound on $p_{\text{succ}}^{\max}(\Pi^{\text{PPT}})$. We find an exact optimal solution to the SDP of $2/3$ (see Appendix 4.7.1), and hence

$$p_{\text{succ}}^{\max}(\text{LOSCC}) \leq \frac{2}{3}. \tag{4.14}$$

Repeating the protocol over many rounds will amplify this gap. 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 (MUB) and sending equal or orthogonal states (from the chosen basis) to P. This allows us to guess an optimal LOSCC 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 'orthogonal' otherwise. Then their probability of success is

$$\begin{aligned} p_{\text{succ}} &= \mathbb{P}(b'=b)\mathbb{P}(\text{success}\,|\,b'=b) + \mathbb{P}(b'\neq b)\mathbb{P}(\text{success}\,|\,b'\neq b) \\ &= \frac{1}{3}\cdot 1 + \frac{2}{3}\cdot\frac{1}{2} = \frac{2}{3}, \end{aligned} \tag{4.15}$$

achieving the upper bound.

Parallel repetition for LOSCC

Can we extend this to the parallel repetition scenario, 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 $s = s_0 s_1 \ldots s_{n-1} \in \{0,1\}^n$?

Note that this does not follow naively from the single-round security proof, since attackers could now take blocks of inputs and apply joint operations on them. We will prove that for the $\text{QPV}_{\text{SWAP}}(0,1)$ protocol strong parallel repetition does indeed hold, i.e. the average probability of success of testing equality over n rounds decreases as

$$(p_{\text{succ}}^{\max})^{\otimes n}(\text{LOSCC}) \leq \left(\frac{2}{3}\right)^n. \tag{4.16}$$

Again we can write down the problem as an SDP, where we optimize over all PPT operations on the $2n$ qubits the attackers receive.

$$\begin{aligned} &\textbf{Primal program} \\ \textbf{maximize:}\quad & \frac{1}{2^n}\sum_{s\in\{0,1\}^n}\mathrm{Tr}[\Pi_s\rho_s] \\ \textbf{subject to:}\quad & \sum_{s\in\{0,1\}^n}\Pi_s = \mathbb{1}_{2^{2n}}, \\ & \Pi_s \in \mathrm{PPT}(\mathsf{A}:\mathsf{B}), \\ & s\in\{0,1\}^n. \end{aligned} \tag{4.17}$$

$$\begin{aligned} &\textbf{Dual program} \\ \textbf{minimize:}\quad & \mathrm{Tr}[Y] \\ \textbf{subject to:}\quad & Y - Q_s^{T_{\mathsf{B}}} - \rho_s/2^n \succeq 0, \\ & Y \in \mathrm{Herm}(\mathsf{A}\otimes\mathsf{B}), \\ & Q_s \in \mathrm{Pos}(\mathsf{A}\otimes\mathsf{B}), \\ & s\in\{0,1\}^n. \end{aligned} \tag{4.18}$$

In Appendix 4.7.1 we find an explicit analytical solution to the dual problem. The solution is nontrivial and depends on the specifics of the $\mathrm{QPV}_{\mathrm{SWAP}}(0,1)$ protocol, so it does not naturally generalise to other protocols. We obtain an upper bound of $(2/3)^n$, which is clearly attained by applying the optimal single round strategy n times in parallel.

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. Secondly, it implies a linear lower bound on the entanglement adversaries need to attack the protocol perfectly, as shown in Section 4.3.3.

Loss-tolerance for LOSCC

In the previous section we have shown that the $\mathrm{QPV}_{\mathrm{SWAP}}(0,1)$ protocol is secure against LOSCC attackers when they have to answer in every round. In practice, an honest prover will only answer on a fraction of the rounds played due to channel loss and imperfect measurements. Note that in order to pretend 'signal loss' without being detected, attackers must declare loss with equal probability on every input overlap. 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 transmission rate η.

We first show that in the parallel repetition case p_{succ} is independent of η when attackers either answer conclusively on all inputs or do not answer at all and use this as a step to show full loss-tolerance of n parallel rounds.

4.3.1. PROPOSITION. *If an n-round QPV protocol fulfils strong parallel repetition security against attackers and is tolerant against declaring loss on all n rounds, it 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 allow adversaries to answer only on k rounds and to declare a loss on the remaining $n-k$ rounds.

Assume that there is some attacking strategy S with a success probability $p_S > p_1^k$ of being correct on this subset. We will show that this leads to a contradiction. Consider a protocol secure and loss tolerant against declaring loss on all rounds and that has success probability $p_k = p_1^k$. Attackers may create $n-k$ independent extra rounds, of which they can forget the answer, themselves. This creates a n-round protocol out of the initial k rounds. The attackers can now apply their strategy S, say, by choosing k random rounds out of the n to actually respond. With probability $1/\binom{n}{k}$ they get a conclusive answer on their initial k rounds, thus being correct with 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 signal loss (on all rounds). This defines an attack with a conditional winning probability $p_S > p_1^k$ and a loss rate of $1-1/\binom{n}{k}$. But that 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 maximum success probability p_k on this subset is p_1^k. □

Next, we formulate an SDP to maximise the probability of success conditioned on a conclusive answer $(p_{\text{succ}}^{\max})^{\otimes n}(\eta)$ in the n-round parallel repetition case.

Primal program

$$\begin{aligned}
\textbf{maximize:}\quad & \frac{1}{2^n\eta}\sum_{s\in\{0,1\}^n}\operatorname{Tr}[\tilde{\Pi}_s\rho_s] \\
\textbf{subject to:}\quad & \sum_{s\in\{0,1\}^n}\tilde{\Pi}_s+\tilde{\Pi}_\varnothing = \mathbb{1}_{2^{2n}} \\
& \operatorname{Tr}[\tilde{\Pi}_\varnothing\rho_s] = 1-\eta, \quad s\in\{0,1\}^n \\
& \tilde{\Pi}_s \in \mathrm{PPT}(\mathsf{A}:\mathsf{B}), \quad s\in\{0,1\}^n\cup\varnothing
\end{aligned} \tag{4.19}$$

$$
\begin{aligned}
&\textbf{Dual program}\\
\textbf{minimize:}\quad & \frac{\mathrm{Tr}[\tilde{Y}]-(1-\eta)\gamma}{\eta}\\
\textbf{subject to:}\quad & \tilde{Y}-\tilde{Q}_s^{T_{\mathsf{B}}}-\rho_s/2^n\succeq 0, \quad s\in\{0,1\}^n\\
& 2^{2n}(\tilde{Y}-\tilde{Q}_{\varnothing}^{T_{\mathsf{B}}})-\gamma\mathbb{1}_{2^{2n}}\succeq 0\\
& \tilde{Y}\in\mathrm{Herm}(\mathsf{A}\otimes\mathsf{B})\\
& \tilde{Q}_s\in\mathrm{Pos}(\mathsf{A}\otimes\mathsf{B}), \quad s\in\{0,1\}^n\cup\varnothing\\
& \gamma\in\mathbb{R}.
\end{aligned}
\tag{4.20}
$$

From the analysis in Appendix 4.7.1, we see that the solution of the SDP is again $(2/3)^n$, independent of η. The strategy in which attackers apply the n-round parallel repetition attack with probability η and discard everything with probability $1-\eta$ attains $(2/3)^n$. By Proposition 4.3.1, we find that $\mathrm{QPV}_{\mathrm{SWAP}}^{\otimes n}$ is tolerant against loss on any subset of rounds, establishing full loss tolerance.

Security and loss tolerance for LOSQC

We now show that no matter the transmission rate η, the SWAP test cannot be perfectly simulated even by LOSQC attackers. Our argument relies on the same fact for the Bell measurement [ABSV22] (see Chapter 5).

The SWAP test implements the POVM $\{\Pi_{\mathrm{sym}},\Pi_{\mathrm{asym}}\}$ of projecting onto either the symmetric or the antisymmetric subspace. In particular, it allows one to perfectly distinguish $|\Psi_-\rangle$ from the other Bell states. Hence, the analogous result for $\mathrm{QPV}_{\mathrm{Bell}}$ implies that there is a finite gap between the best LOSQC attack (without loss), establishing LOSQC security.

Considering loss, we will show that if the SWAP test could be implemented perfectly via LOSQC for some $0<\eta\leq 1$, then so could the Bell measurement with some different $\eta'<\eta$, contradicting our result in [ABSV22]. Therefore, there exists no perfect lossy unentangled attack on $\mathrm{QPV}_{\mathrm{SWAP}}$.

4.3.2. Proposition. $\mathrm{QPV}_{\mathrm{SWAP}}$ *is secure and fully loss tolerant against unentangled attacks, i.e. in the LOSQC setting.*

Proof:
Assume that there is an LOSQC procedure perfectly simulating $\{\Pi_{\mathrm{sym}},\Pi_{\mathrm{asym}}\}$ with probability $0<\eta\leq 1$. Then, conditioned on a conclusive result, A,B could do the following in $\mathrm{QPV}_{\mathrm{Bell}}$:

- Whenever their procedure returns 'anti-symmetric', return $(i,j)=(1,1)$, standing for $|\Psi_-\rangle$, and

- whenever it returns 'symmetric', return 'signal loss'.

This would be suspicious, because the only conclusive answers would be for $|\Psi_-\rangle$. However, their strategy can be randomised. In order to achieve $\mathbb{P}(\varnothing \,|\, \Phi_{ij}) = 1-\eta$ for all Bell states $|\Phi_{ij}\rangle$ and $\mathbb{P}(\Phi_{ij} \,|\, \text{concl.}) = 1/4$, as the honest P would do, they can 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:

- Whenever their procedure returns 'anti-symmetric', answer $(i,j) = (1 \oplus a, 1 \oplus b)$, standing for $\mathbb{1} \otimes X^a Z^b \,|\Psi_-\rangle$, and
- whenever it returns 'symmetric', answer 'signal loss',

then this implies $\mathbb{P}(\varnothing \,|\, \Phi_{ij}) = 1 - \eta$ as well as $\mathbb{P}(\Phi_{ij} \,|\, \text{concl.}) = 1/4$ and whenever they do answer conclusively, they will be correct (by assumption). But this would give them a perfect attack on $\mathrm{QPV}_{\mathrm{Bell}}$ with some probability $\eta' < \eta$ (because they throw away the 'symmetric' measurement results), contradicting the fact that $p_{\mathrm{succ}}(\eta) < 1$ for *all* η in $\mathrm{QPV}_{\mathrm{Bell}}$. □

4.3.3 Entanglement attack

It is easy to see that 1 EPR suffices to attack $\mathrm{QPV}_{\mathrm{SWAP}}$, since the SWAP test can be regarded as a coarse-grained version of a Bell measurement. The attackers can simply implement a Bell measurement non-locally and clump together the three symmetric Bell states to a single response 'symmetric'.

4.3.3. Theorem. *One round of* $\mathrm{QPV}_{\mathrm{SWAP}}$ *can be perfectly attacked with 1 pre-shared EPR pair. Thus, n pre-shared EPR pairs are sufficient to attack* $\mathrm{QPV}_{\mathrm{SWAP}}^{\otimes n}$. *A linear* $\Omega(n)$ *lower bound applies to* $\mathrm{QPV}_{\mathrm{SWAP}}^{\otimes n}(0,1)$.

Proof:
The entanglement attack is evident, as argued just before. To get a lower bound on the required entanglement resource in order to break $\mathrm{QPV}_{\mathsf{SWAP}}(0,1)$ we can use an argument already mentioned in [BK11, Lemma V.3]. It says that if the attackers pre-share a d-dimensional resource state $\Psi_{\mathsf{A'B'}}$ then the success probability (of the attackers achieving that the verifiers accept them) is related to the success probability without a pre-shared resource in the following way:

$$p_{\mathrm{succ}|\Psi_{\mathsf{A'B'}}} \leq d p_{\mathrm{succ}|\emptyset}. \tag{4.21}$$

For the case $\beta \in \{0,1\}$, we have described one optimal strategy in (4.15). That strategy produces $\hat{p}_1 = 2/3$ on equal inputs and $\hat{p}_0 = 2/3$ on orthogonal inputs, while the correct frequencies would be $p_1^{\mathsf{P}} = 1$ and $p_0^{\mathsf{P}} = 1/2$. The above strategy

can be improved in terms of $\|\Delta\|_1$ by flipping whenever they would respond '1' to a '0' response with probability 1/4 to obtain $\hat{p}_1 = 3/4$ and $\hat{p}_0 = 1/2$.

Then, the probability that the verifiers accept attackers is basically $(3/4)^{n_1}$, where n_1 is the number of rounds with identical inputs. Since each overlap is chosen with probability 1/2 in each round, we have for n rounds that $\mathbb{E}[n_1] = n/2$. Hence, we expect $p_{n,\mathrm{succ}|\Psi_{\mathsf{A}'\mathsf{B}'}} \leq d\left(\frac{3}{4}\right)^{n/2}$ and thus

$$p_{n,\mathrm{succ}|\Psi_{\mathsf{A}'\mathsf{B}'}} < 1 \qquad \text{as long as} \qquad d < \left(\frac{4}{3}\right)^{n/2}. \tag{4.22}$$

If m is the number of EPR pairs in $\Psi_{\mathsf{A}'\mathsf{B}'}$, so that $d = 2^{2m}$, it follows that, in expectation,

$$p_{n,\mathrm{succ}|\Psi_{\mathsf{A}'\mathsf{B}'}} < 1 \qquad \text{as long as} \qquad m < \frac{1}{4}\log\left(\frac{4}{3}\right)n \approx 0.103n. \tag{4.23}$$

□

4.4 $\mathrm{QPV}_{\mathrm{SWAP}}$ with realistic experimental conditions

4.4.1 Practical considerations

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 $p_\beta(0) = \frac{1+\beta^2}{2}$ is fairly well preserved[6], even with experimental errors. Creating true NR detectors is an active field of research, but at the moment they are still in an early stage and difficult to operate [CHE+21, ESM+21]. We therefore use two further beam splitters and four click/no-click detectors to achieve probabilistic NR. We call this the **3BS** setup, as depicted in Figure 4.4. This setup still has an advantage over [LXS+16], as it does not require polarisation beam splitters and thus does not require careful polarisation alignment.

[6] With a generic (R, T) beam splitter, one has $p_\beta(0) = 4|R|^2|T|^2\frac{1+\beta^2}{2}$

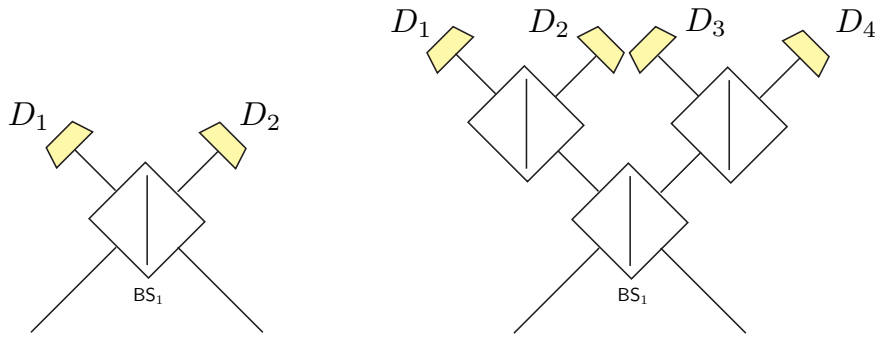


Figure 4.4: The detection setups **BS** (left) and **3BS** (right). The beam splitters are (R, T) and non-polarising. Unless otherwise specified, the detectors D_i are conventional single photon click/no-click detectors.

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 '$\varnothing$' if 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)), otherwise answer '$\varnothing$'.

This means that in the **3BS** setup we post-select entirely on 2-click events, giving us weak number resolution, 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 that end we will parametrise the entire setup from the single photon sources (at the verifiers) to the detection (at the prover) in terms of the errors that can appear. The setup consists of the following:

- Each verifier holds an imperfect single photon source, characterised 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. We consider accidental multi-photon terms $\mathbb{P}(n > 2)$ to be negligible.

- A communication channel between each verifier and the prover with a transmittance (at the prover) of η_{BS}[7]. We assume that both channels from $\mathsf{V_A}$ to P and from $\mathsf{V_B}$ to P have the same transmittance.

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

- The prover uses imperfect beam splitters with reflectance (amplitude) R and transmittance (amplitude) T as well as single photon detectors characterised 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).

- 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, for example the polarisation degree of freedom. 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 $|\delta| > 0$.

We will denote the set of experimental parameters as

$$\Omega_\beta = (\eta_{\mathrm{source}}, B, p_{\mathrm{pair}}, \eta_{\mathrm{BS}}, |R|^2, |T|^2, \beta, \delta, \eta_{\mathrm{det}}, p_{\mathrm{dark}}). \tag{4.24}$$

Some comments about these parameters are to be made. From an experimental point of view the second order autocorrelation function (at zero time delay) $g^{(2)}$, describing how bunched or anti-bunched the photons are coming from the source (see Figure 4.5), is easier to determine. The quantities η_{source}, B and $g^{(2)}$ can be obtained in the lab and the latter has become a standard parameter to describe the quality of a single photon source [TFVM20].

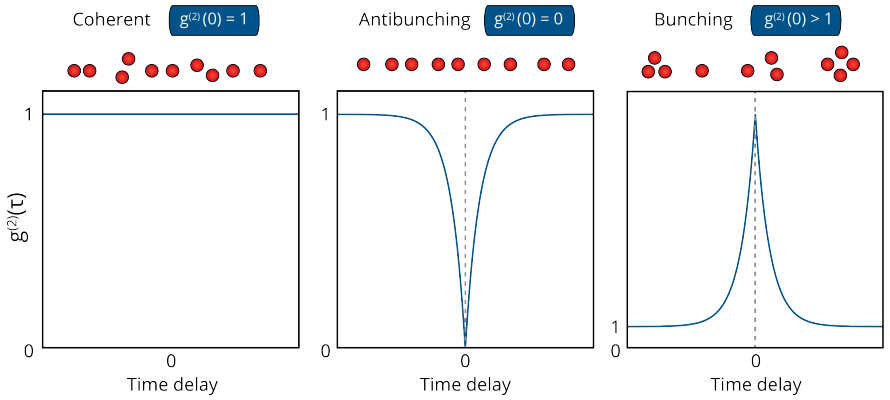


Figure 4.5: Bunching described by $g^{(2)}$ for photons coming from a single photon source. Image from [Del19].

However, more important for us is the probability p_{pair} that there accidentally *are* two photons produced at one source, because this may influence the interference at

the beam splitter with the photon from the other source. Assuming $\mathbb{P}(n > 2) \approx 0$, we can relate $g^{(2)}$ and $\mathbb{P}(n = 2)$ as follows, [MPFB13],

$$p_{\text{pair}} = \mathbb{P}(n = 2) = \frac{g^{(2)}}{2}\mu^2 \approx \frac{g^{(2)}}{2}(2\eta_{\text{source}} - B)^2, \tag{4.25}$$

with μ being the mean photon number produced by the source. Moreover, we account for errors in the communication channels as follows. If the verifiers expect a protocol with Ω_β and in reality the overlap between the input states changes from β to $\tilde{\beta} = \beta + \delta$ on the way to the prover, then the honest party will run the protocol with $\Omega_{\tilde{\beta}} = \Omega_{\beta+\delta}$. That means P will reproduce the expected distribution slightly worse. Note also that the verifiers do not need to know/trust the detection system parameters but could in principle base their security checks simply on industry standard values of $\{\eta_{\text{det}}, p_{\text{dark}}\}$. Moreover, η_{BS} and δ can be estimated by the verifiers because they know in which way they send out the inputs (e.g. free space or in a quantum network). In this sense, the verifiers have control over all parameters.

4.4.2 Imperfect honest prover

We will analyse the honest statistics in the realistic scenario. We will do so in a hardware-agnostic way.

First, we will argue that all we are interested in are the two probability distributions $\mathbb{P}_{\Omega_\beta}(\mathsf{D}_1, \mathsf{D}_2)$ and $\mathbb{P}_{\Omega_\beta}(\mathsf{D}_1, \mathsf{D}_4)$ of these detector click patterns happening given an experimental configuration Ω_β. This follows from the symmetry of the setup and the fact that photons bunch or anti-bunch into each bunch/anti-bunch output configuration with the same probability[8]. Hence

$$\begin{aligned} \mathbb{P}_{\Omega_\beta}(\mathsf{D}_1, \mathsf{D}_2) &= \mathbb{P}_{\Omega_\beta}(\mathsf{D}_3, \mathsf{D}_4), \\ \mathbb{P}_{\Omega_\beta}(\mathsf{D}_1, \mathsf{D}_4) = \mathbb{P}_{\Omega_\beta}(\mathsf{D}_2, \mathsf{D}_4) &= \mathbb{P}_{\Omega_\beta}(\mathsf{D}_1, \mathsf{D}_3) = \mathbb{P}_{\Omega_\beta}(\mathsf{D}_2, \mathsf{D}_3). \end{aligned} \tag{4.26}$$

An intuitive example of this is the Hong-Ou-Mandel (HOM) effect [OHM87]. For overlap β and an (R, T) beam splitter, the probability to bunch to each output port is $|R|^2|T|^2(1 + \beta^2)$ [Lou00]. This uniform distribution on the output ports (given bunch or anti-bunch) also holds for the cases of 3 incoming photons, as we prove in Appendix 4.7.3. That means

$$\begin{aligned} \mathbb{P}_{\Omega_\beta}(0) &= \mathbb{P}_{\Omega_\beta}(\text{2-click in one arm}) = 2 \cdot \mathbb{P}_{\Omega_\beta}(\mathsf{D}_1, \mathsf{D}_2), \\ \mathbb{P}_{\Omega_\beta}(1) &= \mathbb{P}_{\Omega_\beta}(\text{2-click in two arms}) = 4 \cdot \mathbb{P}_{\Omega_\beta}(\mathsf{D}_1, \mathsf{D}_4), \\ \mathbb{P}_{\Omega_\beta}(\varnothing) &= 1 - \mathbb{P}_{\Omega_\beta}(0) - \mathbb{P}_{\Omega_\beta}(1). \end{aligned} \tag{4.27}$$

[8] Explicitly, we mean $\mathbb{P}((0,2)) = \mathbb{P}((2,0))$, $\mathbb{P}((0,3)) = \mathbb{P}((3,0))$ and $\mathbb{P}((1,2)) = \mathbb{P}((2,1))$ for any $|R|^2$ and $|T|^2$.

Finally, we post-select on conclusive answers and test the probability distributions of '0' and '1' answers there. So we are looking for

$$\begin{aligned} p_{\Omega_\beta}(0) &\coloneqq \mathbb{P}_{\Omega_\beta}(0\,|\,\text{concl.}) = \frac{\mathbb{P}_{\Omega_\beta}(0)}{1-\mathbb{P}_{\Omega_\beta}(\varnothing)}, \\ p_{\Omega_\beta}(1) &\coloneqq \mathbb{P}_{\Omega_\beta}(1\,|\,\text{concl.}) = \frac{\mathbb{P}_{\Omega_\beta}(1)}{1-\mathbb{P}_{\Omega_\beta}(\varnothing)}. \end{aligned} \tag{4.28}$$

Next, we find explicit expressions for the probability distributions of the required detector click patterns. To that end, we expand

$$\begin{aligned} &\mathbb{P}_{\Omega_\beta}(\mathsf{D}_1,\mathsf{D}_2) = \\ &= (1-p_{\mathrm{dark}})^2 \sum_k \mathbb{P}_{\Omega_\beta}(\mathsf{D}_1,\mathsf{D}_2\,|\,k \text{ photons at } \mathsf{BS}_1)\mathbb{P}_{\Omega_\beta}(k \text{ photons at } \mathsf{BS}_1) \\ &= (1-p_{\mathrm{dark}})^2 \sum_k \Bigg[\mathbb{P}_{\Omega_\beta}(\mathsf{D}_1,\mathsf{D}_2\,|\,\text{bunch},k)\frac{\mathbb{P}_{\Omega_\beta}(\text{bunch}\,|\,k)}{2} \\ &+ \mathbb{P}_{\Omega_\beta}(\mathsf{D}_1,\mathsf{D}_2\,|\,\text{anti-bunch},k)\mathbb{P}_{\Omega_\beta}(\text{anti-bunch}\,|\,k)\Bigg]\mathbb{P}_{\Omega_\beta}(k \text{ photons at } \mathsf{BS}_1), \end{aligned} \tag{4.29}$$

where

$$\begin{aligned} &\mathbb{P}_{\Omega_\beta}(k \text{ photons at } \mathsf{BS}_1) = \\ &\qquad \sum_{\ell\geq k} \mathbb{P}_{\Omega_\beta}(k \text{ photons at } \mathsf{BS}_1\,|\,\ell \text{ produced})\mathbb{P}_{\Omega_\beta}(\ell \text{ produced}). \end{aligned} \tag{4.30}$$

The factor $(1-p_{\mathrm{dark}})^2$ accounts for the fact that the other two detectors D_3 and D_4 should not click. The factor $1/2$ in $\mathbb{P}_{\Omega_\beta}(\text{bunch}\,|\,k)/2$ stems from the fact that for a non-negligible contribution to $\mathbb{P}_{\Omega_\beta}(\mathsf{D}_1,\mathsf{D}_2)$ the photons have to bunch into the $(\mathsf{D}_1,\mathsf{D}_2)$ output arm, which happens with probability $1/2$. Otherwise, we would require both D_1 and D_2 to have a dark count (and loose all photons), which would dominate that contribution via p_{dark}^2[9]. We neglect terms of order $O(p_{\mathrm{dark}}^2)$. Furthermore, we consider up to $k=3$ photons incoming to BS_1 and up to $\ell=3$ photons in total being produced by the sources in a round of the protocol. The probabilities for $k\geq 4$ incoming photons are considered negligible because assuming $\mathbb{P}(n>2)\approx 0$ for each source gives $\mathbb{P}_{\Omega_\beta}(4 \text{ photons at } \mathsf{BS}_1)\sim \eta_{\mathrm{BS}}^4 p_{\mathrm{pair}}^2$, which is only $\sim 10^{-12}$ for the parameters we will encounter later. Higher photon number terms are even smaller. In the process of treating the 3-photon case we had to generalise the HOM output port distribution to 3 photons, as formulated in the following lemma. The proof can be found in Appendix 4.7.3.

4.4.1. Lemma. *Consider photonic qubits* $|\psi\rangle, |\phi\rangle$ *arriving at one input port of a (symmetric)* (R,T) *beam splitter and* $|\chi\rangle$ *at the other input port. Then the output*

[9] In practice values like $p_{\mathrm{dark}}\sim 10^{-7}$ per detection window can be achieved.

port distribution is given by

$$\mathbb{P}((3,0) \text{ or } (0,3)) = 4|R|^2|T|^2 \frac{|\langle\psi|\phi\rangle|^2 + |\langle\psi|\chi\rangle|^2 + |\langle\phi|\chi\rangle|^2}{2 \cdot (1 + |\langle\psi|\phi\rangle|^2)}, \tag{4.31}$$

$$\mathbb{P}((2,1) \text{ or } (1,2)) = 1 - \mathbb{P}((3,0) \text{ or } (0,3)). \tag{4.32}$$

In the same vein we expand

$$\begin{aligned}
&\mathbb{P}_{\Omega_\beta}(\mathsf{D}_1, \mathsf{D}_4) = \\
&= (1 - p_{\text{dark}})^2 \sum_k \mathbb{P}_{\Omega_\beta}(\mathsf{D}_1, \mathsf{D}_4 \,|\, k \text{ photons at } \mathsf{BS}_1) \mathbb{P}_{\Omega_\beta}(k \text{ photons at } \mathsf{BS}_1) \\
&= (1 - p_{\text{dark}})^2 \sum_k \Big[\mathbb{P}_{\Omega_\beta}(\mathsf{D}_1, \mathsf{D}_4 \,|\, \text{bunch}, k) \mathbb{P}_{\Omega_\beta}(\text{bunch} \,|\, k) \\
&+ \mathbb{P}_{\Omega_\beta}(\mathsf{D}_1, \mathsf{D}_4 \,|\, \text{anti-bunch}, k) \mathbb{P}_{\Omega_\beta}(\text{anti-bunch} \,|\, k) \Big] \mathbb{P}_{\Omega_\beta}(k \text{ photons at } \mathsf{BS}_1).
\end{aligned} \tag{4.33}$$

Here there is no factor $1/2$ after $\mathbb{P}_{\Omega_\beta}(\text{bunch} \,|\, k)$ because no matter into which output arm the photons bunch only one extra detector dark count is needed, incurring only a factor p_{dark} instead of p_{dark}^2, which we do not neglect.

Given all this, one has to explicitly write out all these probability contributions in (4.29) and (4.33), which gives very long overall expressions. These can be found in Appendix 4.7.2. Finally, note that for example for overlaps $\beta \in \{0, 1\}$ an ideal honest party with the set of parameters $\Omega_\beta = (1, 1, 0, 1, 1/2, 1/2, \beta, 0, 1, 0)$ will produce

$$\mathbb{P}(0 \,|\, \rho_0, \text{concl.}) = \frac{1}{3} \qquad \mathbb{P}(0 \,|\, \rho_1, \text{concl.}) = 1, \tag{4.34}$$

$$\mathbb{P}(1 \,|\, \rho_0, \text{concl.}) = \frac{2}{3} \qquad \mathbb{P}(1 \,|\, \rho_1, \text{concl.}) = 0, \tag{4.35}$$

$$\mathbb{P}(\varnothing \,|\, \rho_0) = \frac{1}{4} \qquad \mathbb{P}(\varnothing \,|\, \rho_1) = \frac{1}{2} \tag{4.36}$$

using the **3BS** setup, because for orthogonal inputs (ρ_0), if the photons bunch, half of the time they get filtered out by a '$\varnothing$' response when the probabilistic number resolution fails, while the case when they don't bunch will always yield a conclusive response. This can be generalised to any β as

$$\begin{aligned}
\mathbb{P}(0 \,|\, \rho_\beta, \text{concl.}) &= \frac{1 + \beta^2}{3 - \beta^2}, \\
\mathbb{P}(1 \,|\, \rho_\beta, \text{concl.}) &= 1 - \frac{1 + \beta^2}{3 - \beta^2}, \\
\mathbb{P}(\varnothing \,|\, \rho_\beta) &= \frac{1 + \beta^2}{4}.
\end{aligned} \tag{4.37}$$

Since an ideal P would produce this with the proposed setup it makes sense to consider this one as 'the ideal distribution' instead of the usual SWAP test distribution. However, the essential quantum interference occurs in the first beam splitter BS_1 that implements the SWAP test.

4.4.3 Statistical testing

The SWAP test is a probabilistic measurement and in a realistic scenario with errors it also won't give a deterministic answer on identical inputs of the form $|\psi\rangle \otimes |\psi\rangle$. In order to distinguish the honest prover from attackers the verifiers therefore need to test between the hypotheses 'the sample received comes from P' and 'the sample received comes from attackers', considering that P will make some (predictable) errors. As each round is run independently and identically distributed (i.i.d.), the samples generated over many rounds will be samples from a binomial distribution. In the problem there are three involved distributions: the ideal one, the imperfect honest one, and the attacker one. To distinguish them, we will perform a binomial test. Similarly to the ideal scenario, we will define acceptance regions around the ideal distributions for each β in such a way that we still capture the imperfect P with high probability. These acceptance regions depend on the experimental conditions Ω_β. If the conditions are too bad, these regions are forced to be wide, possibly even largely overlapping for different β. Then the test will be impaired and, for example, if all acceptance regions overlap, the protocol can be broken. Or else, the conditions could be bad enough so that we have to run an infeasibly large number of rounds. In such cases, we say that the experimental conditions are too weak for $\mathrm{QPV}_{\mathrm{SWAP}}$. Intuitively, if the experimental conditions are good enough, the more rounds we run, the narrower the acceptance regions will become[10] and the lower the probability that attackers produce a sample which reaches all acceptance regions simultaneously. This behaviour is depicted in Figure 4.6. Then we can see how many rounds we need to run in order to achieve enough confidence in distinguishing attackers from P as a function of the experimental parameters Ω_β. The worse the conditions, the more rounds we will need to run and if the conditions are too weak for QPV the protocol can be broken.

In order to still capture the honest prover with high probability even in the presence of errors, we need to widen the acceptance regions of the errorless protocol as given by (4.4). The new lower bound will be the smaller of the two α-quantiles of the ideal and the imperfect distribution. The new upper bound will be the larger of the two $(1-\alpha)$-quantiles. In other words,

$$\begin{aligned} L_{\alpha,\Omega_\beta} &= \min\{z_\alpha(\beta, R_\beta), z_\alpha(\Omega_\beta, R_\beta)\}/R_\beta \\ U_{\alpha,\Omega_\beta} &= \max\{z_{1-\alpha}(\beta, R_\beta), z_{1-\alpha}(\Omega_\beta, R_\beta)\}/R_\beta. \end{aligned} \tag{4.38}$$

[10] While still accepting P with high probability, because we will define the acceptance region accordingly.

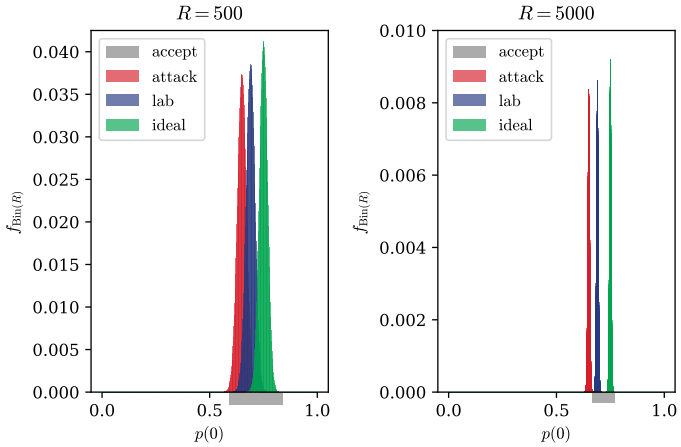


Figure 4.6: On the left, we have not run enough rounds yet and a large part of the attacker distribution (red) overlaps with the acceptance region (gray). Thus attackers would have a decently high probability of returning a sample that gets accepted. On the right, after many more rounds, the probability of returning a sample that lies in the acceptance region is negligibly small. These plots are for $\beta = 3/4$, $f_{\mathrm{Bin}}(R)$ denotes the binomial probability density function for R rounds and $p(0)$ the fraction of '0' results.

Here again, the values of $z_q(\beta, R_\beta)$ and $z_q(\Omega_\beta, R_\beta)$ can be obtained by inverse of the cumulative distribution function $F_{\mathrm{Bin}(R_\beta, p_\beta(0))}$ and $F_{\mathrm{Bin}(R_\beta, p_{\Omega_\beta}(0))}$, respectively. This defines the round-dependent acceptance regions $\mathsf{acc}_{\Omega_\beta}(\alpha, R_\beta) = [L_{\alpha,\Omega_\beta}, U_{\alpha,\Omega_\beta}]$. Defining these regions in this way ensures that we still capture P with high probability $\geq 1 - O(k\alpha)$, with k the number of different overlaps used in the protocol and α can be set very small, like 10^{-6}. Meanwhile, attackers need to get $\hat{p}_\beta(0) \in \mathsf{acc}_{\Omega_\beta}(\alpha, R_\beta)$ for all β in order to succeed. If the experimental conditions Ω_β are so bad that all $\mathsf{acc}_{\Omega_\beta}(\alpha, R_\beta)$ overlap, attackers can succeed by choosing to answer with some fixed list producing $\hat{p}(0) \in \bigcap_\beta \mathsf{acc}_{\Omega_\beta}(\alpha, R_\beta)$. Indeed, all acceptance regions overlap very quickly when one tries to implement the SWAP test with just one beam splitter and two click/no-click detectors. We therefore *demand* that not all acceptance regions overlap, that is, $\bigcap_\beta \mathsf{acc}_{\Omega_\beta}(\alpha, R_\beta) = \emptyset$.

Finally, one subtlety is that with the proposed **3BS** setup the rate of inconclusive answers is overlap dependent, as seen in equation (4.37). However, we still want to maintain a uniform distribution over the input overlaps $\{\beta_1, \ldots, \beta_k\}$. To do so, we send uniformly random input states ρ_β until the number of conclusive rounds reaches $R_\beta \geq R_{\mathrm{threshold}}$ for all β. Eventually, with sufficiently nice Ω_β and

sufficiently high $R_{\text{threshold}}$, we may achieve

$$\mathbb{P}_{\Omega_\beta}(\mathsf{acc}|\mathsf{att}) = \prod_\beta \mathbb{P}_{\Omega_\beta}(\mathsf{acc}_\beta|\mathsf{att}) = \prod_\beta \mathbb{P}(\hat{p}_\beta(0) \in \mathsf{acc}_{\Omega_\beta}(\alpha, R_\beta)) \leq \varepsilon, \tag{4.39}$$

with any desired ε. For example, we could set $\varepsilon = \alpha$ and, in the end, choose α very small, say $\alpha \sim 10^{-6}$. Then we would accept P with a high probability at least $1 - O(k\alpha)$ and accept attackers with a vanishing probability at most α.

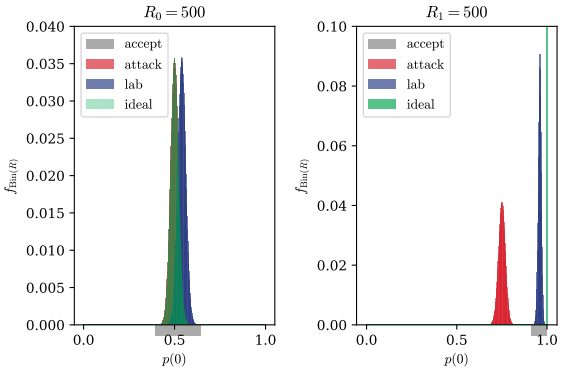


Figure 4.7: Illustrating the test via the example of the protocol with overlaps $\{0, 1\}$, so that $p_{\beta=0}(0) = 1/2$ and $p_{\beta=1}(0) = 1$. Note that in the left plot the attack distribution is the same as the ideal one (hence overlaying red and green), but they perform badly on identical inputs.

4.4.4 LOSCC attack strategy in practice

We now go on to describe LOSCC attack strategies in the presence of experimental errors. Our result on parallel repetition implies that the optimal strategy for multiple rounds is to use the optimal single-round strategy many times. Attackers will therefore maximise their chance to get accepted by trying to bring their $\hat{p}_\beta(0)$ as close as possible to $\max\{p_\beta(0), p_{\Omega_\beta}(0)\}$ for all β. This is because generally attackers want to answer '0' as often as they can[11] in order to perform better on high overlap inputs. We take this into account by allowing them to adaptively optimise towards $\max\{p_\beta(0), p_{\Omega_\beta}(0)\}$. The relevant parameter is therefore[12] $\Delta_\beta = |\max\{p_\beta(0), p_{\Omega_\beta}(0)\} - \hat{p}_\beta(0)|$.

As before, attackers are restricted to PPT measurements $\{\Pi_0, \Pi_1, \Pi_\varnothing\}$ to capture attacks using classical communication. In Section 4.3.2 we proved full loss

[11] while performing as well as possible overall

[12] Since, conditioned on a conclusive answer, we have $\Delta_\beta(0) = \Delta_\beta(1)$ we can just use the '0' answers and write Δ_β.

tolerance of our protocol. Adding two more beam splitters in the **3BS** setup does not change that, as the quantum interference that is hard to simulate for attackers happens in BS_1 and the effect of the extra beam splitters can be classically calculated by each attacker. In the **3BS** setup there is a non-zero inconclusive-answer rate even with perfect transmission, namely when the probabilistic number resolution fails. We assume they have some way of getting the honest loss pattern (4.37) right by adding the constraints[13]

$$\mathrm{Tr}[\Pi_\varnothing \rho_\beta] = \frac{1+\beta^2}{4} \qquad \forall \beta. \tag{4.40}$$

In total, this leaves us with the following optimisation problem:

$$\begin{aligned} &\textbf{minimize:} && \|\Delta\|_1 \\ &\textbf{subject to:} && \Pi_0, \Pi_1, \Pi_\varnothing \succeq 0 \\ &&& \Pi_0^{T_\mathsf{B}}, \Pi_1^{T_\mathsf{B}}, \Pi_\varnothing^{T_\mathsf{B}} \succeq 0 \\ &&& \Pi_0 + \Pi_1 + \Pi_\varnothing = \mathbb{1} \\ &&& \mathrm{Tr}[\Pi_\varnothing \rho_\beta] = \left(1+\beta^2\right)/4 \qquad \forall \beta, \end{aligned} \tag{4.41}$$

with

$$\Delta_i = \begin{cases} p_{\beta_i}(0) - \frac{\mathrm{Tr}[\Pi_0 \rho_{\beta_i}]}{1-\left(1+\beta_i^2\right)/4} & \text{if } p_{\beta_i}(0) \geq p_{\Omega_{\beta_i}}(0) \\ p_{\Omega_{\beta_i}}(0) - \frac{\mathrm{Tr}[\Pi_0 \rho_{\beta_i}]}{1-\left(1+\beta_i^2\right)/4} & \text{if } p_{\beta_i}(0) \leq p_{\Omega_{\beta_i}}(0) \end{cases}. \tag{4.42}$$

The solution will give us the optimal PPT measurement attackers can apply to do as well as possible on all β for the statistical test. Since practically one will have $p_{\text{pair}} > 0$, attackers will have access to three or four photons sometimes and possibly they can do better with these extra resources. Therefore, we will also solve the above optimisation problem for higher photon numbers by adjusting the dimensions of the involved operators. In particular, for k photons attackers will apply a POVM $\left\{\Pi_0^{(k)}, \Pi_1^{(k)}, \Pi_\varnothing^{(k)}\right\}$ on 2^k dimensional states $\rho_\beta^{(k)}$. In general, the state prepared by the verifiers takes the form

$$\rho_\beta^{(k)} = \int_{\mathrm{U}(2)} U^{\otimes k} P_{\psi\phi}^{(k)} \left(U^\dagger\right)^{\otimes k} d\mu(U), \tag{4.43}$$

where $P_{\psi\phi}^{(k)}$ is some pure k-qubit state describing two states $|\psi\rangle, |\phi\rangle$ with $|\langle\psi|\phi\rangle| = \beta$ making up a k-photon state[14]. Here μ is the Haar measure on the unitary group $\mathrm{U}(2)$. Integrals of the form (4.43) can be explicitly calculated using Weingarten calculus [Wei78, CŚ06]. We used the Mathematica package IntU [PM11] to calculate $\rho_\beta^{(3)}$ and $\rho_\beta^{(4)}$.

[13] If they don't get it right, they are caught right away.

[14] For example, if one source produces a pair we'd have $P_{\psi\phi}^{(3)} = |\psi\psi\phi\rangle\langle\psi\psi\phi|$

The above optimisation then gives $\Delta^{(k)}_{\min}$. Clearly, it is beneficial for attackers to choose to answer as much as possible in rounds with more photons. The overall $\Delta_{\beta,\min}$ will then be composed as

$$\Delta_{\beta,\min} = p_{(2)}\Delta^{(2)}_{\beta,\min} + p_{(3)}\Delta^{(3)}_{\beta,\min} + p_{(4)}\Delta^{(4)}_{\beta,\min}, \tag{4.44}$$

where $p_{(m)}$ is the fraction of rounds of m photons among the attackers' conclusive answer rounds. In particular, the attackers control $p_{(m)}$ and it could be that $p_{(4)} = 1$ and $p_{(2)} = p_{(3)} = 0$ for example. This is constrained by (4.40). Say, for example, the verifiers expect a conclusive-answer rate of 10^{-9} and the rate of 4 photons (double pair production) is $p_4 \sim 10^{-8}$. Then indeed attackers can choose $p_{(4)} = 1$ and only answer on 4 photon rounds (and even among those not answer on all). If $p_{\text{concl.}} \sim 10^{-6}$ in this example, then attackers will also need to answer on some rounds with 3 photons, thus $p_{(4)} < 1$ and $p_{(3)} > 0$, and possibly also $p_{(2)} > 0$ in order to be able to answer conclusively often enough. All this will affect $\Delta_{\beta,\min}$ and in turn the total $\Delta_{\min}$, which will then affect the statistical test in the end, which affects how we have to set $R_{\text{threshold}}$.

4.5 Numerical simulation under realistic conditions

We have done all these simulations for the prime example of overlaps $\{0, 1\}$, that is, sending either equal or orthogonal states. First of all, in that case the optimisation (4.41) gives

$$\begin{aligned} \|\Delta^{(2)}_{\min}\|_1 &= \frac{1}{2}, \\ \|\Delta^{(3)}_{\min}\|_1 &= \frac{1}{3}, \\ \|\Delta^{(4)}_{\min}\|_1 &= \frac{1}{6}. \end{aligned} \tag{4.45}$$

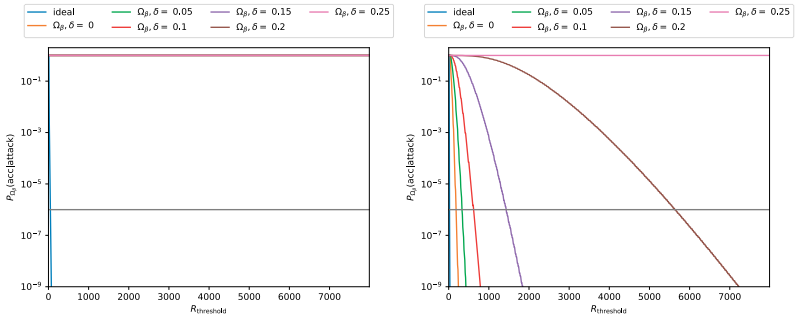
The portions $p_{(m)}$ are chosen adaptively, depending on what the overall expected experimental conclusive-rate $p_{\text{concl.}} = 1 - \frac{1}{k}\sum_\beta p_\varnothing(\Omega_\beta)$ is[15]. Then everything is fed into codes calculating all the $\mathsf{acc}_{\Omega_\beta}(\alpha, R_\beta)$, which depend on the experimental conditions, the number of conclusive rounds we run and how small we set α. Finally, we increase the number of (conclusive) rounds and can plot $\mathbb{P}_{\Omega_\beta}(\mathsf{acc} \,|\, \mathsf{att})$ as a function of $R_{\text{threshold}}$. To illustrate this, realistic experimental parameters

[15] Basically, the attackers use higher m as often as possible before going on to use $m-1$, and so on.

could be close to [TFVM20, MPFB13]

$$\begin{aligned} \eta_{\text{source}} &= 0.12 \\ B &= 0.1197 \\ g^{(2)} &= 0.04 \\ p_{\text{pair}} &= \frac{g^{(2)}}{2}(2\eta_{\text{source}} - B)^2 \approx 3 \cdot 10^{-4} \\ \eta_{\text{BS}} &= 0.20 \\ |R|^2 &= 0.45 \\ |T|^2 &= 0.55 \\ \eta_{\text{det}} &= 0.20 \\ p_{\text{dark}} &= 10^{-7}. \end{aligned} \tag{4.46}$$

We wrote code that calculates $\mathbb{P}_{\Omega_\beta}(\mathsf{acc} \,|\, \mathsf{att})$ as a function of $R_{\text{threshold}}$. The results for both the original **BS** setup and the proposed **3BS** setup are depicted for different values of the polarisation error δ in Figures 4.8a and 4.8b, respectively.



(a) **BS** (b) **3BS**

Figure 4.8: The success probability of LOSCC attackers, $\mathbb{P}_{\Omega_\beta}(\mathsf{acc}|\mathsf{att})$ given the experimental conditions (4.46) and different values of the overlap error δ as a function of $R_{\text{threshold}}$ for the different setups with $\beta \in \{0, 1\}$. The grey horizontal line marks $\mathbb{P}_{\Omega_\beta}(\mathsf{acc}|\mathsf{att}) = 10^{-6}$. As mentioned in the main text, for the original **BS** setup without number resolving detectors signal loss forces $p_{\Omega_\beta}(0) \approx 1$ for all β making the protocol insecure (note that all imperfect lines lie on top of each other). The **3BS** setup removes this insecurity by introducing probabilistic number resolution using just simple click/no-click detectors.

Note that $R_{\text{threshold}}$ in these plots corresponds to *conclusive rounds per overlap* $\beta \in \{\beta_1, \ldots, \beta_k\}$. If, for example, $p_{\text{concl.}} \sim 10^{-6}$ and $R_{\text{threshold}} \sim 10^3$, then we will need to run $\sim k \cdot 10^9$ rounds in total in order to build up enough conclusive rounds

(per β). In general, if $p_{\text{concl.}} \sim 10^{-a}$ and $R_{\text{threshold}} \sim 10^{b}$, then we expect to run at least $\sim k \cdot 10^{a+b}$ rounds in total. So, if in principle security can be achieved, then the time needed per round will determine if QPV is practically feasible under the experimental conditions Ω_β.

4.6 Discussion

We constructed and analysed a new quantum position verification protocol denoted QPV_{SWAP}, and showed that it possesses several desirable properties. It was shown that it is fully loss tolerant against LOSCC attackers, that it can be attacked with n pre-shared EPR pairs and that at least $\Omega(n)$ pre-shared EPR pairs are necessary in the $\beta \in \{0, 1\}$ case. Moreover, it fulfils strong parallel repetition and retains the loss tolerance even if all rounds are run in parallel. QPV_{SWAP} even remains loss tolerant and secure in the LOSQC setting, making it the first QPV protocol with this property. However, we were unable to show a finite gap between the attacker and the honest success probability in the lossy LOSQC scenario.

The flexibility and simplicity of the SWAP test, both theoretically and experimentally, make it a good candidate for practical QPV. One notable advantage is that the setup of the prover is static and does not require any sophisticated fast switching between measurement settings. To that end, we performed a detailed analysis of our protocol under realistic experimental conditions, in which we quantify the entire experimental setup in terms of possible imperfections and take these into account in the attack model. We identified a condition indicating whether the experimental conditions Ω_β allow for security in principle and if so, numerically calculated the figure of merit $R_{\text{threshold}}(\Omega_\beta)$, the number of conclusive rounds (per β) we need to collect to guarantee a sufficiently low attack success probability $\mathbb{P}_{\Omega_\beta}(\mathsf{acc}|\mathsf{attack})$. For the prime example of sending identical or orthogonal states and realistic conditions already $R_{\text{threshold}}(\Omega_\beta) \sim 10^2$-$10^3$ (per β) suffices to achieve $\mathbb{P}_{\Omega_\beta}(\mathsf{acc}|\mathsf{attack}) \leq 10^{-6}$. Our protocol therefore remains fairly robust in the presence of experimental imperfections and the challenge for implementation is to run many rounds fast enough to be able to collect $R_{\text{threshold}}(\Omega_\beta)$ conclusive rounds for each overlap.

However, given that it can be attacked fairly easily with pre-shared entanglement, and that it cannot handle slow quantum information, it is not the 'ultimate' QPV protocol yet.

4.7 Appendix

4.7.1 SDP security proofs

Exponential suppression of attacker success probability

Here we provide the proof of (4.8). Let N_β^{AB} the binomial distributed random variable that describes the number of '0' answers of attackers in L_β. Since $p_\beta, p_\beta^{\mathsf{AB}} \in \left[\frac{1}{2}, 1\right)$, we can approximate the binomial distribution with a normal distribution $\mathcal{N}(\mu, \sigma^2)$ with $\mu = R_\beta p$ and $\sigma^2 = R_\beta p(1-p)$ for $p \in \{p_\beta, p_\beta^{\mathsf{AB}}\}$, respectively. This is valid as long as $R_\beta(1-p)$ is sufficiently large, which we can always achieve by making R_β large enough. Then

$$\begin{aligned}\mathbb{P}(\mathsf{acc}_\beta|\mathsf{attack}) &= \mathbb{P}\left(z_{\frac{\alpha}{2}}^{\mathsf{P}} \leq N_\beta^{\mathsf{AB}} \leq z_{1-\frac{\alpha}{2}}^{\mathsf{P}}\right) \\ &= F_{N_\beta^{\mathsf{AB}}}\left(z_{1-\frac{\alpha}{2}}^{\mathsf{P}}\right) - F_{N_\beta^{\mathsf{AB}}}\left(z_{\frac{\alpha}{2}}^{\mathsf{P}} - 1\right) \\ &\approx \frac{1}{2}\left[1 + \operatorname{erf}\left(\frac{z_{1-\frac{\alpha}{2}}^{\mathsf{P}} - \mu_\beta^{\mathsf{AB}}}{\sqrt{2}\sigma_\beta^{\mathsf{AB}}}\right)\right] - \frac{1}{2}\left[1 + \operatorname{erf}\left(\frac{z_{\frac{\alpha}{2}}^{\mathsf{P}} - \mu_\beta^{\mathsf{AB}}}{\sqrt{2}\sigma_\beta^{\mathsf{AB}}}\right)\right]. \quad (4.47)\end{aligned}$$

Now for $\mathcal{N}(\mu, \sigma^2)$ one has $z_q = F^{-1}(q) = \mu + \sqrt{2}\sigma \operatorname{erf}^{-1}(2q-1)$. Replacing the z_q values and defining $c_\alpha \coloneqq \operatorname{erf}^{-1}(1-\alpha)$ as well as $f_\beta^{\mathsf{X}} = \sqrt{2p_\beta^{\mathsf{X}}(1-p_\beta^{\mathsf{X}})}$ gives

$$\mathbb{P}(\mathsf{acc}_\beta|\mathsf{attack}) \approx \frac{1}{2}\operatorname{erf}\left(\frac{\sqrt{R_\beta}\Delta_\beta + f_\beta^{\mathsf{P}} c_\alpha}{f_\beta^{\mathsf{AB}}}\right) - \frac{1}{2}\operatorname{erf}\left(\frac{\sqrt{R_\beta}\Delta_\beta - f_\beta^{\mathsf{P}} c_\alpha}{f_\beta^{\mathsf{AB}}}\right). \quad (4.48)$$

Using $\operatorname{erf}(x) \approx 1 - \frac{e^{-x^2}}{\sqrt{\pi}x}$ for large x, we can write

$$\begin{aligned}\mathbb{P}(\mathsf{acc}_\beta|\mathsf{attack}) \approx \sqrt{\frac{2}{\pi}} f_\beta^{\mathsf{AB}} \Bigg[&\frac{e^{-\left(\sqrt{R_\beta}\Delta_\beta - f_\beta^{\mathsf{P}} c_\alpha\right)^2 / \left(f_\beta^{\mathsf{AB}}\right)^2}}{\sqrt{R_\beta}\Delta_\beta - f_\beta^{\mathsf{AB}} c_\alpha} \\ &- \frac{e^{-\left(\sqrt{R_\beta}\Delta_\beta + f_\beta^{\mathsf{P}} c_\alpha\right)^2 / \left(f_\beta^{\mathsf{AB}}\right)^2}}{\sqrt{R_\beta}\Delta_\beta + f_\beta^{\mathsf{AB}} c_\alpha}\Bigg]. \quad (4.49)\end{aligned}$$

As $p_\beta^{\mathsf{AB}} \neq 0$ and $p_\beta^{\mathsf{AB}} \neq 1$, we may neglect the terms $f_\beta^{\mathsf{AB}} c_\alpha$ in the denominators because we can make R_β sufficiently large. Moreover, leaving out the second (positive) exponential term gives the approximate upper bound

$$\mathbb{P}(\mathsf{acc}_\beta|\mathsf{attack}) \lesssim \frac{\sqrt{2} f_\beta^{\mathsf{AB}}}{\sqrt{\pi R_\beta}\Delta_\beta} e^{-\left(\sqrt{R_\beta}\Delta_\beta - f_\beta^{\mathsf{P}} c_\alpha\right)^2 / \left(f_\beta^{\mathsf{AB}}\right)^2}. \quad (4.50)$$

Relating p_{succ} to $\|\Delta\|_1$ for $\text{QPV}_{\text{SWAP}}(0,1)$

Relating these two quantities is straightforward and achieved by one application of the triangle inequality. Consider

$$p_{\text{succ}} = \frac{1}{2}\frac{\text{Tr}[\Pi_0\rho_0]}{\eta} + \frac{1}{2}\frac{\text{Tr}[\Pi_1\rho_1]}{\eta} \leq u, \tag{4.51}$$

with $u \leq 3/4$. We want to massage this to get the Δ_0 and Δ_1 expressions into it. Doing so gives

$$1 - \frac{\text{Tr}[\Pi_0\rho_0]}{\eta} + \frac{1}{2} - \frac{\text{Tr}[\Pi_1\rho_1]}{\eta} \geq \frac{3}{2} - 2u. \tag{4.52}$$

This implies

$$\begin{aligned}\|\Delta\|_1 &= \left|1 - \frac{\text{Tr}[\Pi_0\rho_0]}{\eta}\right| + \left|\frac{1}{2} - \frac{\text{Tr}[\Pi_1\rho_1]}{\eta}\right| \\ &\geq \left|1 - \frac{\text{Tr}[\Pi_0\rho_0]}{\eta} + \frac{1}{2} - \frac{\text{Tr}[\Pi_1\rho_1]}{\eta}\right| \geq \frac{3}{2} - 2u.\end{aligned} \tag{4.53}$$

SDP for LOSCC security of $\text{QPV}_{\text{SWAP}}(0,1)$

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 (MUB), see ρ_1. Similarly, picking two random orthogonal states or picking two orthogonal MUB states is the same, see ρ_0. These become

$$\rho_0 = \frac{1}{6}\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 2 & -1 & 0\\ 0 & -1 & 2 & 0\\ 0 & 0 & 0 & 1\end{pmatrix}, \qquad \rho_1 = \frac{1}{6}\begin{pmatrix}2 & 0 & 0 & 0\\ 0 & 1 & 1 & 0\\ 0 & 1 & 1 & 0\\ 0 & 0 & 0 & 2\end{pmatrix}. \tag{4.54}$$

We can then write the following SDP for this discrimination task:

Primal Program

$$\begin{aligned}\textbf{maximize:}\quad & \frac{1}{2}\text{Tr}[\Pi_0\rho_0 + \Pi_1\rho_1] \\ \textbf{subject to:}\quad & \Pi_0 + \Pi_1 = \mathbb{1}_{2^2} \\ & \Pi_k \in \text{PPT}(\mathsf{A}:\mathsf{B}), \quad k \in \{0,1\}.\end{aligned} \tag{4.55}$$

Dual Program

$$\begin{aligned}\textbf{minimize:}\quad & \text{Tr}[Y] \\ \textbf{subject to:}\quad & Y - Q_i^{T_\mathsf{B}} - \rho_i/2 \succeq 0, \quad i \in \{0,1\} \\ & Y \in \text{Herm}(\mathsf{A}\otimes\mathsf{B}) \\ & Q_i \in \text{Pos}(\mathsf{A},\mathsf{B}), \quad i \in \{0,1\}.\end{aligned} \tag{4.56}$$

A feasible solution for the primal program is

$$\Pi_0 = \frac{1}{3}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & -1 & 0 \\ 0 & -1 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad \Pi_1 = \frac{1}{3}\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}, \tag{4.57}$$

with solution $\frac{1}{2}\operatorname{Tr}[\Pi_0\rho_0 + \Pi_1\rho_1] = 2/3$. Note that these measurement projectors correspond to attackers choosing a random MUB to measure in and returning 0 if the measurement outcomes were different and 1 if they were equal, which is also a LOSCC strategy. This can be seen from the fact that

$$\begin{aligned} \frac{1}{3}(|10\rangle\langle 10| + |01\rangle\langle 01| + |-+\rangle\langle -+| + |+-\rangle\langle +-| \\ + |i^-i^+\rangle\langle i^-i^+| + |i^+i^-\rangle\langle i^+i^-|) = \Pi_0, \end{aligned} \tag{4.58}$$

$$\begin{aligned} \frac{1}{3}(|00\rangle\langle 00| + |11\rangle\langle 11| + |++\rangle\langle ++| + |--\rangle\langle --| \\ + |i^+i^+\rangle\langle i^+i^+| + |i^-i^-\rangle\langle i^-i^-|) = \Pi_1. \end{aligned} \tag{4.59}$$

A feasible solution to the dual program is:

$$Y = \frac{\mathbb{1}_4}{6}, \quad Q_0 = \frac{\mathbb{1}_4}{6} - \frac{\rho_1^{T_\mathsf{B}}}{2} = \frac{1}{12}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} = \frac{1}{6}|\Phi^+\rangle\langle\Phi^+| \succeq 0, \tag{4.60}$$

$$Q_1 = 0 \succeq 0. \tag{4.61}$$

These adhere to the constraints in the dual program, because

$$Y - Q_0^{T_\mathsf{B}} - \frac{\rho_0}{2} = \frac{\mathbb{1}_4}{6} - \left(\frac{\mathbb{1}_4}{6} - \frac{\rho_1}{2}\right) - \frac{\rho_1}{2} = 0 \succeq 0, \tag{4.62}$$

$$Y - Q_1^{T_\mathsf{B}} - \frac{\rho_1}{2} = \frac{\mathbb{1}_4}{6} - \frac{\rho_0}{2} = \frac{1}{12}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \frac{1}{6}|\Psi^-\rangle\langle\Psi^-| \succeq 0. \tag{4.63}$$

Since $Y \in \operatorname{Herm}(\mathsf{A}\otimes\mathsf{B})$ we get a feasible solution for the dual with value $\operatorname{Tr}[Y] = 2/3$. The primal and dual values are the same, so the maximum probability of success for LOSCC attackers is 2/3.

SDP for LOSCC security of $\mathrm{QPV}_{\mathsf{SWAP}}^{\otimes n}$

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:

Primal Program

$$\begin{aligned} \textbf{maximize:}\quad & \frac{1}{2^n}\sum_{s\in\{0,1\}^n} \mathrm{Tr}[\Pi_s \rho_s] \\ \textbf{subject to:}\quad & \sum_{s\in\{0,1\}^n} \Pi_s = \mathbb{1}_{2^{2n}} \\ & \Pi_s \in \mathrm{PPT}(\mathsf{A}:\mathsf{B}), \quad s\in\{0,1\}^n. \end{aligned} \tag{4.64}$$

Dual Program

$$\begin{aligned} \textbf{minimize:}\quad & \mathrm{Tr}[Y] \\ \textbf{subject to:}\quad & Y - Q_s^{T_\mathsf{B}} - \rho_s/2^n \succeq 0, \quad s\in\{0,1\}^n \\ & Y \in \mathrm{Herm}(\mathsf{A}\otimes\mathsf{B}) \\ & Q_s \in \mathrm{Pos}(\mathsf{A}\otimes\mathsf{B}). \end{aligned} \tag{4.65}$$

Clearly, repeating the strategy of the single round protocol gives a feasible solution for the primal program with success probability $(2/3)^n$. We will now construct feasible Y, Q_s for the dual.

We start again by setting Y to be the identity matrix with proper normalisation, so

$$Y = \frac{\mathbb{1}_{2^{2n}}}{2^{2n}}\left(\frac{2}{3}\right)^n = \frac{\mathbb{1}_{2^{2n}}}{6^n}, \text{ such that } \mathrm{Tr}[Y] = \left(\frac{2}{3}\right)^n. \tag{4.66}$$

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 sorted version of s. First we show a general solution for $s = 0^n$ and $s = 1^n$ string. Again a solution for the all-1 input case is $Q_{1^n} = 0 \succeq 0$. The constraint for $s = 1^n$ in the dual program of the SDP then reduces to

$$\frac{\mathbb{1}_{2^{2n}}}{6^n} - \frac{\rho_1^{\otimes n}}{2^n}. \tag{4.67}$$

Note that the eigenvectors of ρ_1 are the four Bell states $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$, with respective eigenvalues $\{1/3, 1/3, 1/3, 0\}$. Then the eigenvalues of $\frac{\rho_1^{\otimes n}}{2^n}$ are $1/6^n$ or 0. Thus, the eigenvalues of (4.67) are either 0 or $1/6^n$ and (4.67) is non-negative. Similarly to the single-round protocol, we have the following solution for the $s = 0^n$ case,

$$Q_{0^n} = \frac{\mathbb{1}_{2^{2n}}}{6^n} - \frac{(\rho_0^{T_\mathsf{B}})^{\otimes n}}{2^n}. \tag{4.68}$$

The eigenvectors of $\rho_0^{T_\mathsf{B}}$ are again the Bell states, with respective eigenvalues $\{0, 1/3, 1/3, 1/3\}$. The eigenvectors of Q_{0^n} are all the combinations of tensor

products of these four Bell states. If one of these states is the $|\Phi^+\rangle$ state the corresponding eigenvalue of Q_{0^n} is 0, otherwise it is $(\frac{1}{6})^n$. Since Q_{0^n} is Hermitian and has only non-negative eigenvalues $Q_{0^n} \succeq 0$, as desired. The corresponding constraint in the dual program of the SDP reduces to

$$\frac{\mathbb{1}_{2^{2n}}}{6^n} - \left(\frac{\mathbb{1}_{2^{2n}}}{6^n} - \frac{\rho_0^{\otimes n}}{2^n}\right) - \frac{\rho_0^{\otimes n}}{2^n} = 0 \succeq 0. \tag{4.69}$$

Hence, the all-zero or all-one cases are satisfied. By induction, suppose that we have a valid solution Q_s for some $s \in \{0,1\}^n$ and add a round $n+1$ of equal inputs. First, by assumption,

$$Y - Q_s^{T_\mathsf{B}} - \rho_s/2^n \succeq 0, \tag{4.70}$$

and adding the extra round of equal inputs, we will show that

$$Q_{s,1} = Q_s \otimes \rho_1^{T_\mathsf{B}}/2 \tag{4.71}$$

is a valid solution for the $(n+1)$-round SDP. We have already shown in Appendix 4.7.1 that $\rho_1^{T_\mathsf{B}} \succeq 0$. Since the tensor product of positive semidefinite matrices is again positive semidefinite, we have $Q_{s,1} \succeq 0$. Rewriting the first dual constraint, we get

$$\begin{aligned}
&\frac{\mathbb{1}_{2^{2n+2}}}{6^{n+1}} - Q_{s,1}^{T_\mathsf{B}} - \frac{\rho_s \otimes \rho_1}{2^{n+1}} \\
&\qquad = \frac{\mathbb{1}_{2^{2n+2}}}{6^{n+1}} - Q_s^{T_\mathsf{B}} \otimes \frac{\rho_1}{2} - \frac{\rho_s \otimes \rho_1}{2^{n+1}} \\
&\qquad = \frac{\mathbb{1}_{2^{2n}}}{6^n} \otimes \frac{\mathbb{1}_4}{6} - Q_s^{T_\mathsf{B}} \otimes \frac{\rho_1}{2} - \frac{\rho_s \otimes \rho_1}{2^{n+1}} \\
&\qquad = \frac{\mathbb{1}_{2^{2n}}}{6^n} \otimes \frac{\rho_0 + \rho_1}{3} - Q_s^{T_\mathsf{B}} \otimes \frac{\rho_1}{2} - \frac{\rho_s \otimes \rho_1}{2^{n+1}} \\
&\qquad = \underbrace{\left(\frac{\mathbb{1}_{2^{2n}}}{6^n} - Q_s^{T_\mathsf{B}} - \frac{\rho_s}{2^n}\right) \otimes \frac{\rho_1}{2}}_{\mathbf{A}} + \underbrace{\frac{\mathbb{1}_{2^{2n}}}{6^n} \otimes \left(\frac{2\rho_0 - \rho_1}{6}\right)}_{\mathbf{B}}.
\end{aligned} \tag{4.72}$$

The tensor product of two positive semidefinite matrices $\mathbf{A}$ is also positive semidefinite. For part $\mathbf{B}$, note that the eigenvectors of $\frac{2\rho_0-\rho_1}{6}$ are again the Bell states with respective eigenvalues $\{0,0,0,1/6\}$, so part $\mathbf{B}$ is positive semidefinite. Since sums of positive semidefinite matrices are positive semidefinite, the whole constraint is positive semidefinite. Since for any number of rounds n we have a feasible solution for the $s = 0^n$ case, by repeatedly adding the 'equal' case, we can repeat the previous steps to get a feasible solution for any sorted string 0^n1^k for all n, k, namely

$$Q_{0^n1^k} = Q_{0^n} \otimes \frac{(\rho_1^{T_\mathsf{B}})^{\otimes k}}{2^k}. \tag{4.73}$$

Now take a string $s \in \{0,1\}^n$, and let P_s be a unitary consisting only of 2-qubit SWAP operations that sorts the n-rounds, such that $P_s \rho_s P_s^\dagger = \rho_{T(s)}$ and $P_s^\dagger = P_s$. We can then write down the general solution of Q_s using the corresponding map P_s applied to the sorted version. Let $Q_s = (P_s Q_{T(s)}^{T_\mathsf{B}} P_s)^{T_\mathsf{B}}$. Using the fact that P_s is a unitary matrix, we get for the corresponding constraint in the dual SDP:

$$\begin{aligned} Y - Q_s^{T_\mathsf{B}} - \rho_s/2^n \succeq 0 &\Leftrightarrow P_s(Y - Q_s^{T_\mathsf{B}} - \rho_s/2^n)P_s \succeq 0 \\ &\Leftrightarrow Y - P_s Q_s^{T_\mathsf{B}} P_s - \rho_{T(s)}/2^n \succeq 0 \\ &\Leftrightarrow Y - P_s((P_s Q_{T(s)}^{T_\mathsf{B}} P_s)^{T_\mathsf{B}})^{T_\mathsf{B}} P_s - \rho_{T(s)}/2^n \succeq 0 \\ &\Leftrightarrow Y - P_s(P_s Q_{T(s)}^{T_\mathsf{B}} P_s)P_s - \rho_{T(s)}/2^n \succeq 0 \\ &\Leftrightarrow Y - Q_{T(s)}^{T_\mathsf{B}} - \rho_{T(s)}/2^n \succeq 0, \end{aligned} \tag{4.74}$$

where the last expression is positive semidefinite by (4.73). Thus, the first constraint in the dual program of the n-round SDP is fulfilled for any string s.

The final step is to show that $Q_s = (P_s Q_{T(s)}^{T_\mathsf{B}} P_s)^{T_\mathsf{B}}$ is positive semidefinite. Note that P_s permutes both registers held by A and B, respectively, 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 $Q_s = P_s Q_{T(s)} P_s$. Now, since P_s is unitary and $Q_{T(s)}$ is positive semidefinite we see that Q_s is positive semidefinite.

All the constraints in the dual program of the n-round SDP are thus satisfied by our constructed Q_s matrices, and thus we obtain a feasible solution to the dual program with value $\mathrm{Tr}[Y] = (2/3)^n$, which is equal to the primal value (and is attainable by the single-round LOSCC strategy repeated n times). This shows that the optimal LOSCC attacking strategy for n parallel rounds is just the single-round strategy applied n times in parallel.

SDP for lossy LOSCC parallel repetition of $\mathbf{QPV}_{\mathsf{SWAP}}^{\otimes n}(0,1)$

We will now optimise 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:

$$\begin{aligned} &\textbf{Primal Program} \\ \textbf{maximize:}\quad & \frac{1}{2^n \eta} \sum_{s \in \{0,1\}^n} \mathrm{Tr}[\tilde{\Pi}_s \rho_s] \\ \textbf{subject to:}\quad & \left(\sum_{s \in \{0,1\}^n} \tilde{\Pi}_s \right) + \tilde{\Pi}_\varnothing = \mathbb{1}_{2^{2n}} \\ & \mathrm{Tr}[\tilde{\Pi}_\varnothing \rho_s] = 1 - \eta, \quad s \in \{0,1\}^n \\ & \tilde{\Pi}_s \in \mathrm{PPT}(\mathsf{A} : \mathsf{B}), \quad s \in \{0,1\}^n \cup \varnothing. \end{aligned} \tag{4.75}$$

$$\begin{aligned}
&\textbf{Dual Program}\\
\textbf{minimize:}\quad & \frac{\mathrm{Tr}[\tilde{Y}]-(1-\eta)\gamma}{\eta}\\
\textbf{subject to:}\quad & \tilde{Y}-\tilde{Q}_s^{T_\mathsf{B}}-\rho_s/2^n\succeq 0, \quad s\in\{0,1\}^n\\
& 2^{2n}(\tilde{Y}-\tilde{Q}_\varnothing^{T_\mathsf{B}})-\gamma\mathbb{1}_{2^{2n}}\succeq 0\\
& \tilde{Y}\in\mathrm{Herm}(\mathsf{A}\otimes\mathsf{B})\\
& \tilde{Q}_s\in\mathrm{Pos}(\mathsf{A}\otimes\mathsf{B}), \quad s\in\{0,1\}^n\cup\varnothing\\
& \gamma\in\mathbb{R}.
\end{aligned} \tag{4.76}$$

Here η is the transmission rate and $\mathrm{Tr}[\tilde{\Pi}_\varnothing\rho_s]=1-\eta$ is the loss condition attackers have to fulfil. 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 program with solution $(2/3)^n$.

For the dual program, we pick

$$\tilde{Y}=\frac{\mathbb{1}_{2^{2n}}}{6^n}, \qquad \tilde{Q}_s=Q_s \qquad \tilde{Q}_\varnothing=0, \qquad \gamma=(2/3)^n. \tag{4.77}$$

Then clearly $Y\in\mathrm{Herm}(\mathsf{A}\otimes\mathsf{B}),\tilde{Q}_s\in\mathrm{Pos}(\mathsf{A}\otimes\mathsf{B}),\gamma\in\mathbb{R}$ and the first condition remains satisfied since we have not changed the Y,Q_s of Appendix 4.7.1. The second constraint becomes

$$2^{2n}(\tilde{Y}-\tilde{Q}_\varnothing^{T_\mathsf{B}})-\gamma\mathbb{1}_{2^{2n}}=\mathbb{1}_{2^{2n}}\frac{2^n}{3^n}-(2/3)^n\mathbb{1}_{2^{2n}}=0\succeq 0. \tag{4.78}$$

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

$$\frac{\mathrm{Tr}[\tilde{Y}]-(1-\eta)\gamma}{\eta}=\frac{(2/3)^n-(1-\eta)(2/3)^n}{\eta}=\frac{\eta(2/3)^n}{\eta}=(2/3)^n. \tag{4.79}$$

Thus, we finally have $p^{\max}_{\mathrm{succ},n}(\eta)=(2/3)^n$ for any $\eta\in(0,1]$. Together with Proposition 4.3.1 in the main text, this gives full loss tolerance for the n-round parallel repetition of our protocol.

4.7.2 Explicit descriptions for $\mathbb{P}_{\Omega_\beta}(\mathsf{D}_1,\mathsf{D}_2)$ and $\mathbb{P}_{\Omega_\beta}(\mathsf{D}_1,\mathsf{D}_4)$

As argued in the main text, we only need to find expressions for $\mathbb{P}_{\Omega_\beta}(\mathsf{D}_1,\mathsf{D}_2)$ and $\mathbb{P}_{\Omega_\beta}(\mathsf{D}_1,\mathsf{D}_4)$ in terms of experimental parameters. Then we can recover $\mathbb{P}_{\Omega_\beta}(0)$ as well as $\mathbb{P}_{\Omega_\beta}(1)$ and therefore also $\mathbb{P}_{\Omega_\beta}(0\,|\,\mathrm{concl.})$ and $\mathbb{P}_{\Omega_\beta}(1\,|\,\mathrm{concl.})$, which are the probabilities of interest for security analysis. In what follows we will find explicit

expressions of each term in our expansion

$$\begin{aligned}
&\mathbb{P}_{\Omega_\beta}(\mathsf{D}_1, \mathsf{D}_2) = \\
&= (1 - p_{\text{dark}})^2 \sum_k \mathbb{P}_{\Omega_\beta}(\mathsf{D}_1, \mathsf{D}_2 \,|\, k \text{ photons at } \mathsf{BS}_1) \mathbb{P}_{\Omega_\beta}(k \text{ photons at } \mathsf{BS}_1) \\
&= (1 - p_{\text{dark}})^2 \sum_k \Bigg[\mathbb{P}_{\Omega_\beta}(\mathsf{D}_1, \mathsf{D}_2 \,|\, \text{bunch}, k) \frac{\mathbb{P}_{\Omega_\beta}(\text{bunch} \,|\, k)}{2} \\
&\quad + \mathbb{P}_{\Omega_\beta}(\mathsf{D}_1, \mathsf{D}_2 \,|\, \text{anti-bunch}, k) \mathbb{P}_{\Omega_\beta}(\text{anti-bunch} \,|\, k) \Bigg] \mathbb{P}_{\Omega_\beta}(k \text{ photons at } \mathsf{BS}_1),
\end{aligned} \tag{4.80}$$

and the analogous formula for $\mathbb{P}_{\Omega_\beta}(\mathsf{D}_1, \mathsf{D}_4)$. We will first treat the terms that are part of both probabilities $\mathbb{P}_{\Omega_\beta}(\mathsf{D}_1, \mathsf{D}_2)$ and $\mathbb{P}_{\Omega_\beta}(\mathsf{D}_1, \mathsf{D}_4)$. Note that the sources produce $\ell \leq 3$ photons with the following probabilities p_ℓ:

$$\begin{aligned}
p_0 &= (1 - \eta_{\text{source}})^2, \\
p_1 &= 2B(1 - \eta_{\text{source}}), \\
p_2 &= B^2 + 2p_{\text{pair}}(1 - \eta_{\text{source}}), \\
p_3 &= 2p_{\text{pair}} B, \\
p_4 &= p_{\text{pair}}^2.
\end{aligned} \tag{4.81}$$

Then the probabilities that k photons arrive at BS_1 given $\ell \leq 3$ photons produced is

$$\begin{aligned}
\mathbb{P}_{\Omega_\beta}(k \text{ photons at } \mathsf{BS}_1) &= \sum_{\ell=k}^{3} \mathbb{P}_{\Omega_\beta}(k \text{ photons at } \mathsf{BS}_1 \,|\, \ell \text{ produced}) \mathbb{P}_{\Omega_\beta}(\ell \text{ produced}) \\
&= \sum_{\ell=k}^{3} \binom{\ell}{k} \eta_{\text{BS}}^k (1 - \eta_{\text{BS}})^{\ell - k} p_\ell.
\end{aligned} \tag{4.82}$$

Next, we consider the probabilities to bunch or anti-bunch given k photons interfering at the beam splitter. To that end, we first had to derive the output port distribution for 3 incoming photons (2 from one side, 1 from the other)[16], see Lemma 4.31 in the main text and Appendix 4.7.3 for the proof. From Lemma 4.31 we gather that for $|\psi\rangle = |\phi\rangle$ and overlap $\beta = |\langle\psi|\chi\rangle|$ we have

$$\mathbb{P}_{\text{ideal}}(\text{bunch} \,|\, 3) = 4|R|^2|T|^2 \frac{1 + 2\beta^2}{4}, \tag{4.83}$$

$$\mathbb{P}_{\text{ideal}}(\text{anti-bunch} \,|\, 3) = 1 - \mathbb{P}_{\text{ideal}}(\text{bunch} \,|\, 3). \tag{4.84}$$

[16] This is a generalisation of the Hong-Ou-Mandel output port distribution $\mathbb{P}((0,2) \text{ or } (2,0)) = \frac{1 + |\langle\psi|\phi\rangle|^2}{2}$ to 3 photons.

In the imperfect case, we have to consider all cases that can appear with k incoming photons, such as 2 photons in one input port, or 1 in one and 2 in the other input port. The case of $k = 0$ does not matter because we neglect the terms proportional to p_{dark}^2. The case of $k = 1$ is trivial, as one could say that the photon always 'bunches'. Hence, we can set $\mathbb{P}_{\Omega_\beta}(\text{bunch} \,|\, 1) = 1$. For two photons, we need to distinguish between the cases of both photons coming into the same input port (no interference) or one photon in each input port (interference). The respective probabilities are

$$\begin{aligned}
&\mathbb{P}_{\Omega_\beta}(\text{all in one mode} \,|\, 2) \\
&\quad = \frac{2p_{\text{pair}}(1-\eta_{\text{source}})\eta_{\text{BS}}^2 + 2p_{\text{pair}}B\eta_{\text{BS}}^2(1-\eta_{\text{BS}}) + 2p_{\text{pair}}^2\eta_{\text{BS}}^2(1-\eta_{\text{BS}})^2}{\mathbb{P}_{\Omega_\beta}(2 \text{ photons at } \mathsf{BS}_1)}, \quad (4.85)\\
&\mathbb{P}_{\Omega_\beta}(\text{one in each mode} \,|\, 2) = 1 - \mathbb{P}(\text{all in one mode} \,|\, 2). \quad (4.86)
\end{aligned}$$

Then the overall probability to bunch given 2 incoming photons is

$$\begin{aligned}
\mathbb{P}_{\Omega_\beta}(\text{bunch} \,|\, 2) = \big(|R|^4 + |T|^4\big)&\mathbb{P}_{\Omega_\beta}(\text{all in one mode} \,|\, 2) \\
&+ 4|R|^2|T|^2\frac{1+\beta^2}{2}\mathbb{P}_{\Omega_\beta}(\text{one in each mode} \,|\, 2). \quad (4.87)
\end{aligned}$$

For 3 photons, we get

$$\mathbb{P}_{\Omega_\beta}(\text{bunch} \,|\, 3) = 4|R|^2|T|^2\frac{1+2\beta^2}{4}. \quad (4.88)$$

Finally, note that a single photon click/no-click detector clicks if at least one photon triggers it [MPFB13]. Hence, the probability for a click gets higher if more than one photon reach the detector. To account for that, we define $p_{\text{click}}(m) = \mathbb{P}(\text{photon 1 detected} \cup \cdots \cup \text{photon } m \text{ detected})$, describing the probability that a detector clicks if m photons go into it. This can be expanded via the inclusion-exclusion principle and the independence of the events of each photon being detected. Fundamentally, we parameterize $\mathbb{P}(\text{photon } x \text{ detected}) = \eta_{\text{det}}$ so that $p_{\text{click}}(m)$ is a function of η_{det} only. For completeness, we give them here:

$$\begin{aligned}
p_{\text{click}}(1) &= \eta_{\text{det}}, \quad (4.89)\\
p_{\text{click}}(2) &= 2\eta_{\text{det}} - \eta_{\text{det}}^2, \quad (4.90)\\
p_{\text{click}}(3) &= 3\eta_{\text{det}} - 3\eta_{\text{det}}^2 + \eta_{\text{det}}^3. \quad (4.91)
\end{aligned}$$

We now continue with the separate expressions for detectors $(\mathsf{D}_1, \mathsf{D}_2)$ and $(\mathsf{D}_1, \mathsf{D}_4)$ respectively.

Clicking probabilities for $(\mathsf{D}_1, \mathsf{D}_2)$

Again, we will distinguish the cases for different numbers of $k \leq 3$ interfering photons. Since we condition on k photons having bunched or anti-bunched, we

just need to go through the next beam splitter (where no interference happens) and add up the events for which we get a $(\mathsf{D}_1, \mathsf{D}_2)$ click pattern. In the bunching case, we may assume that the photons bunched into the $(\mathsf{D}_1, \mathsf{D}_2)$ arm, because otherwise two dark counts would be needed, dominated by a factor p_{dark}^2. The results are

$$\begin{aligned}
\mathbb{P}_{\Omega_\beta}(\mathsf{D}_1, \mathsf{D}_2 \,|\, \text{bunch}, 0) &= O\big(p_{\text{dark}}^2\big) && (4.92)\\
\mathbb{P}_{\Omega_\beta}(\mathsf{D}_1, \mathsf{D}_2 \,|\, \text{bunch}, 1) &= p_{\text{click}}(1)p_{\text{dark}} + O\big(p_{\text{dark}}^2\big), && (4.93)\\
\mathbb{P}_{\Omega_\beta}(\mathsf{D}_1, \mathsf{D}_2 \,|\, \text{bunch}, 2) &= 2|R|^2|T|^2 p_{\text{click}}(1)^2 \\
&\quad + \big(|R|^4 + |T|^4\big)p_{\text{click}}(2)p_{\text{dark}} + O\big(p_{\text{dark}}^2\big), && (4.94)\\
\mathbb{P}_{\Omega_\beta}(\mathsf{D}_1, \mathsf{D}_2 \,|\, \text{bunch}, 3) &= 3\big(|R|^4|T|^2 + |R|^2|T|^4\big)p_{\text{click}}(1)p_{\text{click}}(2) \\
&\quad + \big(|R|^6 + |T|^6\big)p_{\text{click}}(3)p_{\text{dark}} + O\big(p_{\text{dark}}^2\big). && (4.95)
\end{aligned}$$

Similarly, one gets[17]

$$\begin{aligned}
\mathbb{P}_{\Omega_\beta}(\mathsf{D}_1, \mathsf{D}_2 \,|\, \text{anti-bunch}, 0) &= O\big(p_{\text{dark}}^2\big) && (4.96)\\
\mathbb{P}_{\Omega_\beta}(\mathsf{D}_1, \mathsf{D}_2 \,|\, \text{anti-bunch}, 1) &= 0, && (4.97)\\
\mathbb{P}_{\Omega_\beta}(\mathsf{D}_1, \mathsf{D}_2 \,|\, \text{anti-bunch}, 2) &= (1 - p_{\text{click}}(1))p_{\text{click}}(1)p_{\text{dark}} + O\big(p_{\text{dark}}^2\big), && (4.98)\\
\mathbb{P}_{\Omega_\beta}(\mathsf{D}_1, \mathsf{D}_2 \,|\, \text{anti-bunch}, 3) &= \frac{1}{2}\Big(2|R|^2|T|^2(1 - p_{\text{click}}(1))^2 + \big(|R|^4 + |T|^4\big) \\
&\quad \cdot (1 - p_{\text{click}}(2))\Big) \cdot p_{\text{click}}(1)p_{\text{dark}} \\
&\quad + \frac{1}{2}(1 - p_{\text{click}}(1))\mathbb{P}_{\Omega_\beta}(\mathsf{D}_1, \mathsf{D}_2 \,|\, \text{bunch}, 2) \\
&\quad + O\big(p_{\text{dark}}^2\big). && (4.99)
\end{aligned}$$

Clicking probabilities for $(\mathsf{D}_1, \mathsf{D}_4)$

Analogously we treat the case for the $(\mathsf{D}_1, \mathsf{D}_4)$ click pattern. This yields

$$\begin{aligned}
\mathbb{P}_{\Omega_\beta}(\mathsf{D}_1, \mathsf{D}_4 \,|\, \text{bunch}, 1) &= |T|^2 p_{\text{click}}(1)p_{\text{dark}} + O\big(p_{\text{dark}}^2\big), && (4.100)\\
\mathbb{P}_{\Omega_\beta}(\mathsf{D}_1, \mathsf{D}_4 \,|\, \text{bunch}, 2) &= |T|^4 p_{\text{click}}(2)p_{\text{dark}} + 2|R|^2|T|^2 p_{\text{click}}(1) \\
&\quad \cdot (1 - p_{\text{click}}(1))p_{\text{dark}} + O\big(p_{\text{dark}}^2\big), && (4.101)\\
\mathbb{P}_{\Omega_\beta}(\mathsf{D}_1, \mathsf{D}_4 \,|\, \text{bunch}, 3) &= |T|^6 p_{\text{click}}(3)p_{\text{dark}} \\
&\quad + 3|R|^2|T|^4 p_{\text{click}}(2)(1 - p_{\text{click}}(1))p_{\text{dark}} \\
&\quad + 3|R|^4|T|^2 p_{\text{click}}(1)(1 - p_{\text{click}}(2))p_{\text{dark}} \\
&\quad + O\big(p_{\text{dark}}^2\big). && (4.102)
\end{aligned}$$

[17] For $\mathbb{P}_{\Omega_\beta}(\mathsf{D}_1, \mathsf{D}_2 \,|\, \text{anti-bunch}, 1)$ we consider the photon to be leaving into the $(\mathsf{D}_3, \mathsf{D}_4)$ arm because we already have the $(\mathsf{D}_1, \mathsf{D}_2)$ case in $\mathbb{P}_{\Omega_\beta}(\mathsf{D}_1, \mathsf{D}_2 \,|\, \text{bunch}, 1)$. This again incurs a factor p_{dark}^2.

And for the anti-bunching cases,

$$\mathbb{P}_{\Omega_\beta}(\mathsf{D_1},\mathsf{D_4}\,|\,\text{anti-bunch},0) = O\big(p_{\text{dark}}^2\big) \tag{4.103}$$

$$\mathbb{P}_{\Omega_\beta}(\mathsf{D_1},\mathsf{D_4}\,|\,\text{anti-bunch},1) = 0, \tag{4.104}$$

$$\begin{aligned}\mathbb{P}_{\Omega_\beta}(\mathsf{D_1},\mathsf{D_4}\,|\,\text{anti-bunch},2) &= |T|^4 p_{\text{click}}(1)^2 + 2|R|^2|T|^2 p_{\text{click}}(1)\\ &\quad\cdot(1-p_{\text{click}}(1))p_{\text{dark}} + O\big(p_{\text{dark}}^2\big),\end{aligned} \tag{4.105}$$

$$\begin{aligned}\mathbb{P}_{\Omega_\beta}(\mathsf{D_1},\mathsf{D_4}\,|\,\text{anti-bunch},3) &= |T|^6 p_{\text{click}}(2) + 2|R|^2|T|^4 p_{\text{click}}(1)^2(1-p_{\text{click}}(1))\\ &\quad+\big(|R|^4|T|^2+|T|^6\big)p_{\text{click}}(1)(1-p_{\text{click}}(2))p_{\text{dark}}\\ &\quad+\big(2|R|^2|T|^4+2|R|^4|T|^2\big)p_{\text{click}}(1)(1-p_{\text{click}}(1))^2 p_{\text{dark}}\\ &\quad+|R|^2|T|^4 p_{\text{click}}(2)(1-p_{\text{click}}(1))p_{\text{dark}} + O\big(p_{\text{dark}}^2\big).\end{aligned} \tag{4.106}$$

Now we have expanded all parts of the equations (4.29) and (4.33).

Original SWAP test setup with one beam splitter

We have done the analogous expansions as in the previous Appendix 4.7.2 also for the original setup of the SWAP test with just one (R,T) beam splitter and two detectors D_1, D_2. For brevity, we will not include all the formulae here, but they look very similar to the ones in Appendix 4.7.2. In this case, we break the problem down to finding $\mathbb{P}_{\Omega_\beta}(\mathsf{D_1})$ and $\mathbb{P}_{\Omega_\beta}(\mathsf{D_1},\mathsf{D_2})$, which are similarly expanded as in (4.29) and (4.33).

4.7.3 Proof of 3-photon output port distribution

We generalise the well-known output probability distribution of the HOM effect after 2 photons entered an (R,T) beam splitter in the two different input ports and are detected in the output ports. We denote detector clicks as (c_1,c_2) with c_k indicating the number of photons registered at detector k. Then, if a photon in state $|\psi\rangle$ enters the beam splitter from one input port and $|\phi\rangle$ does so from the other, one gets, [Lou00],

$$\mathbb{P}((2,0)\text{ or }(0,2)) = 4|R|^2|T|^2\frac{1+|\langle\psi|\phi\rangle|^2}{2}, \tag{4.107}$$

$$\mathbb{P}((1,1)) = 1-\mathbb{P}((2,0)\text{ or }(0,2)). \tag{4.108}$$

Here we generalise this to the 3-photon case, yielding the following lemma.

4.7.1. Lemma. *Consider photonic qubits $|\psi\rangle, |\phi\rangle$ arriving at one input port of a (R,T) beam splitter and $|\chi\rangle$ at the other input port. Then the output port distribution is given by*

$$p_{\text{bunch}} = \mathbb{P}((3,0)\text{ or }(0,3)) = 4|R|^2|T|^2\frac{|\langle\psi|\phi\rangle|^2+|\langle\psi|\chi\rangle|^2+|\langle\phi|\chi\rangle|^2}{2\cdot(1+|\langle\psi|\phi\rangle|^2)}, \tag{4.109}$$

$$p_{\text{anti-bunch}} = \mathbb{P}((2,1)\text{ or }(1,2)) = 1-\mathbb{P}((3,0)\text{ or }(0,3)). \tag{4.110}$$

Proof:
For notational simplicity, we give the proof for the 50/50 beam splitter case, for which $|R|^2 = |T|^2 = 1/2$. The same calculation can be done with general coefficients (R, T). Let there be 3 incoming photonic qubits in the states

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle , \tag{4.111}$$
$$|\phi\rangle = \beta_0 |0\rangle + \beta_1 |1\rangle , \tag{4.112}$$
$$|\chi\rangle = \gamma_0 |0\rangle + \gamma_1 |1\rangle , \tag{4.113}$$

with $|\psi\rangle$ and $|\phi\rangle$ entering one input port, and $|\chi\rangle$ entering the other. For simplicity, we consider photons with H/V polarisation as the basis states. The spatial modes entering the input ports of the beam splitter are denoted by a, b. We first need to write down the input Fock state (normalised by $\mathcal{N}$), which is

$$\begin{aligned} |\text{in}\rangle &= \mathcal{N}(\alpha_0 \mathtt{a_H}^\dagger + \alpha_1 \mathtt{a_V}^\dagger)(\beta_0 \mathtt{a_H}^\dagger + \beta_1 \mathtt{a_V}^\dagger)(\gamma_0 \mathtt{b_H}^\dagger + \gamma_1 \mathtt{b_V}^\dagger) |0_a, 0_b\rangle \\ &= \mathcal{N}\Big[\sqrt{2}\alpha_0\beta_0\gamma_0 |2_H, 1_H\rangle + \sqrt{2}\alpha_0\beta_0\gamma_1 |2_H, 1_V\rangle \\ &\quad + (\alpha_0\beta_1 + \alpha_1\beta_0)\gamma_0 |1_H 1_V, 1_H\rangle + (\alpha_0\beta_1 + \alpha_1\beta_0)\gamma_1 |1_H 1_V, 1_V\rangle \\ &\quad + \sqrt{2}\alpha_1\beta_1\gamma_0 |2_V, 1_H\rangle + \sqrt{2}\alpha_1\beta_1\gamma_1 |2_V, 1_V\rangle \Big]. \end{aligned} \tag{4.114}$$

Requiring $\||\text{in}\rangle\| = 1$ gives an expression for the normalisation constant in terms of amplitudes that can be rewritten as $\mathcal{N} = \frac{1}{\sqrt{1+|\langle\psi|\phi\rangle|^2}}$. We needed $|\text{in}\rangle$ in terms of actual Fock states, as in the second line above, to be able to find the normalisation factor $\mathcal{N}$. When passing through it, the 50/50 beam splitter acts as a unitary U on the creation operators as

$$\mathtt{a_H}^\dagger \mapsto \frac{\mathtt{c_H}^\dagger + i\mathtt{d_H}^\dagger}{\sqrt{2}} \qquad \mathtt{b_H}^\dagger \mapsto \frac{i\mathtt{c_H}^\dagger + \mathtt{d_H}^\dagger}{\sqrt{2}}, \tag{4.115}$$
$$\mathtt{a_V}^\dagger \mapsto \frac{\mathtt{c_V}^\dagger + i\mathtt{d_V}^\dagger}{\sqrt{2}} \qquad \mathtt{b_V}^\dagger \mapsto \frac{i\mathtt{c_V}^\dagger + \mathtt{d_V}^\dagger}{\sqrt{2}}. \tag{4.116}$$

Therefore, after a considerable amount of algebra, we arrive at

$$\begin{aligned}|\text{in}\rangle \mapsto |\text{out}\rangle = \frac{\mathcal{N}}{2\sqrt{2}}\Big[& i\sqrt{6}\alpha_0\beta_0\gamma_0\,|3_H,0\rangle \\ & +i\sqrt{2}(\alpha_1\beta_0\gamma_0+\alpha_0\beta_1\gamma_0+\alpha_0\beta_0\gamma_1)\,|2_H1_V,0\rangle \\ & +i\sqrt{2}(\alpha_1\beta_1\gamma_0+\alpha_1\beta_0\gamma_1+\alpha_0\beta_1\gamma_1)\,|1_H2_V,0\rangle \\ & +i\sqrt{6}\alpha_1\beta_1\gamma_1\,|3_V,0\rangle - \sqrt{2}\alpha_0\beta_0\gamma_0\,|2_H,1_H\rangle - \sqrt{2}\alpha_0\beta_0\gamma_1\,|1_H1_V,1_H\rangle \\ & +\sqrt{2}(\alpha_1\beta_1\gamma_0-\alpha_1\beta_0\gamma_1-\alpha_0\beta_1\gamma_1)\,|2_V,1_H\rangle + i\sqrt{2}\alpha_0\beta_0\gamma_0\,|1_H,2_H\rangle \\ & +i\sqrt{2}(\alpha_1\beta_0\gamma_0+\alpha_0\beta_1\gamma_0-\alpha_0\beta_0\gamma_1)\,|1_V,2_H\rangle - \sqrt{6}\alpha_0\beta_0\gamma_0\,|0,3_H\rangle \\ & +\sqrt{2}(\alpha_0\beta_0\gamma_1-\alpha_1\beta_0\gamma_0-\alpha_0\beta_1\gamma_0)\,|2_H,1_V\rangle - 2i\alpha_1\beta_1\gamma_0\,|1_H1_V,1_V\rangle \\ & -\sqrt{2}\alpha_1\beta_1\gamma_1\,|2_V,1_V\rangle + 2i\alpha_0\beta_0\gamma_1\,|1_H,1_H1_V\rangle + 2i\alpha_1\beta_1\gamma_0\,|1_V,1_H1_V\rangle \\ & -\sqrt{2}(\alpha_1\beta_0\gamma_0+\alpha_0\beta_1\gamma_0+\alpha_0\beta_0\gamma_1)\,|0,2_H1_V\rangle \\ & +i\sqrt{2}(\alpha_1\beta_0\gamma_1+\alpha_0\beta_1\gamma_1-\alpha_1\beta_1\gamma_0)\,|1_H,2_V\rangle + i\sqrt{2}\alpha_1\beta_1\gamma_1\,|1_V,2_V\rangle \\ & -\sqrt{2}(\alpha_1\beta_1\gamma_0+\alpha_1\beta_0\gamma_1+\alpha_0\beta_1\gamma_1)\,|0,1_H2_V\rangle \\ & -\sqrt{6}\alpha_1\beta_1\gamma_1\,|0,3_V\rangle\Big], \end{aligned} \tag{4.117}$$

where the red terms indicate states with all 3 photons in one detector arm and the green terms states with photons in both detector arms. One can check that $|\text{out}\rangle$ is normalised, and thus indeed a valid quantum state. This yields

$$\begin{aligned}\mathbb{P}((3,0)\text{ or }(0,3)) = \frac{\mathcal{N}^2}{2}\Big[& 3|\alpha_0|^2|\beta_0|^2|\gamma_0|^2 + 3|\alpha_1|^2|\beta_1|^2|\gamma_1|^2 \\ & + |(\alpha_0\beta_1+\alpha_1\beta_0)\gamma_0+\alpha_0\beta_0\gamma_1|^2 \\ & + |(\alpha_0\beta_1+\alpha_1\beta_0)\gamma_1+\alpha_1\beta_1\gamma_0|^2\Big]. \end{aligned} \tag{4.118}$$

Writing the coefficients α_k, β_k, γ_k in terms of their respective Bloch angles (φ,θ) simplifies this, after some algebra, to

$$\mathbb{P}((3,0)\text{ or }(0,3)) = \mathcal{N}^2\left[\frac{3}{4}+\frac{1}{4}(\mathbf{r}_\psi\cdot\mathbf{r}_\phi+\mathbf{r}_\psi\cdot\mathbf{r}_\chi+\mathbf{r}_\phi\cdot\mathbf{r}_\chi)\right],$$

with the Bloch vectors $\mathbf{r}$ corresponding to their respective states. We now use the correspondence between the dot product between Bloch vectors and the inner product between Hilbert space states, namely

$$|\langle\alpha|\beta\rangle|^2 = \frac{1}{2}(1+\mathbf{r}_\alpha\cdot\mathbf{r}_\beta). \tag{4.119}$$

Inserting this into the above probability and simplifying finally yields

$$\mathbb{P}((3,0)\text{ or }(0,3)) = \frac{|\langle\psi|\phi\rangle|^2+|\langle\psi|\chi\rangle|^2+|\langle\phi|\chi\rangle|^2}{2\cdot(1+|\langle\psi|\phi\rangle|^2)}, \tag{4.120}$$

where we also inserted $\mathcal{N}$. Accordingly, this also gives us

$$\mathbb{P}((2,1) \text{ or } (1,2)) = 1 - \mathbb{P}((3,0) \text{ or } (0,3)) \tag{4.121}$$

□

Chapter 5

On the Structure and Separation of LOSCC vs. LOSQC

Chapter summary. Inspired by protocols in relativistic quantum cryptography protocols like QPV, we investigate quantum state discrimination using local operations and one round of simultaneous classical or quantum communication (LOSCC/LOSQC). First, we demonstrate an LOSQC upper bound for QPV_{Bell} based on the no-cloning principle. We then study the LOSQC and LOSCC settings more generally. Firstly, by giving necessary and sufficient conditions for perfect discrimination. Secondly, showing that perfectly LOSQC discriminable state ensembles can be constructed by 'inverting' quantum secret sharing schemes. Finally, we demonstrate a separation between LOSCC and LOSQC even for separable state ensembles and prove an uncertainty relation that yields error bounds in LOSQC state discrimination for ensembles containing a certain structure.

This chapter is based on parts of the following papers:

[ABSV22] 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*, 2022. arXiv:2311.00677. *To appear in Quantum.*

[GALC23] Ian George, Rene Allerstorfer, Philip Verduyn Lunel, and Eric Chitambar. Time-constrained local quantum state discrimination. *arXiv preprint*, 2023. arXiv:2311.00677

5.1 Introduction

Following Landauer [Lan91], it has become a central tenet of quantum information theory that information is physical – how information is encoded into a physi-

cal system decides the limitations of information processing. No subfield takes this viewpoint more seriously than (relativistic) quantum cryptography, which uses the limitations on information processing imposed by the laws of physics to construct secure cryptographic protocols. In particular, relativistic quantum cryptography uses the assumption of no superluminal communication in relativity along with the standard quantum mechanical formalism to determine security.

As we encountered in Chapter 3, any bipartite quantum operation can be approximately implemented using one round of simultaneous communication, making QPV a cryptographic task that cannot be *unconditionally* secure. Much of the research on QPV now focuses on the construction of QPV protocols that might require a great deal of entanglement to break (see Chapter 3). Yet, the basic communication model and operational capabilities when the adversaries do not share any entanglement are still not well understood. This places an important gap in the study of QPV and relativistic quantum cryptography in general. The motivation of the work in this chapter was to make progress on closing this gap, further clarifying the interplay between cryptography, quantum communication, and locality.

Our main goal is to identify fundamental limitations in the task of a certain class of QPV protocols, which we call time-constrained state discrimination tasks, when either classical (LOSCC) or quantum (LOSQC) communication is employed. We will consider bipartite, globally orthogonal state ensembles $\{p_k, \rho_k^{AB}\}_k$ as protocol inputs and the task of the prover is to identify which state was sent, i.e. to correctly identify the index k. The setting is depicted in Figure 5.3.

The problem of LOSQC state discrimination has previously only been studied for entangled states [ABSV22], where, in fact, a separation between LOSCC and LOSQC was shown for an entangled input ensemble. The entangled state ensemble given there is not discriminable even if one allows for any number of rounds of classical communication (LOCC), but a single round of simultaneous quantum communication allows for perfect discrimination. Otherwise, its advantage over LOSCC is unclear. To focus on the role of communication, we focus mainly on ensembles of globally orthogonal product states $\{p_k, |a_k\rangle_A |b_k\rangle_B\}_k$, since then any quantum correlation in the discrimination protocol must come through the communication and not the states themselves.

5.2 LOSQC bounds for $\mathrm{QPV}_{\mathrm{Bell}}$

In this section we will show a bound for LOSQC attacks on $\mathrm{QPV}_{\mathrm{Bell}}$. Our argument is based on optimal bounds for approximate cloning of quantum information, will give a bound for any local dimension d of the input and has a clear operational interpretation. For the start, assume that the attackers A, B have optimal local success probabilities $p_{\mathrm{succ}}^{\mathsf{A}}, p_{\mathrm{succ}}^{\mathsf{B}}$, respectively. Our argument will be that if these local success probabilities (and thus also the global attack) were too high,

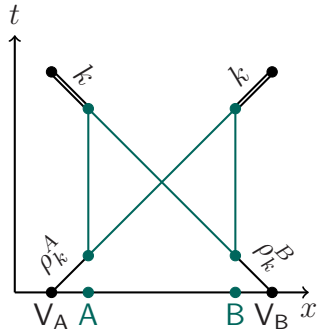


Figure 5.1: LOSQC setting

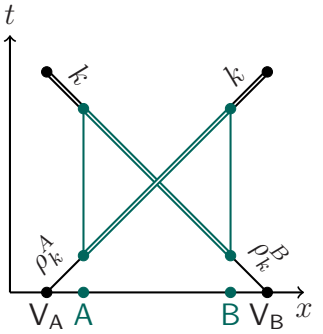


Figure 5.2: LOSCC setting

Figure 5.3: Spacetime diagram of the LOSQC and LOSCC settings in the context of (time-constrained) quantum state discrimination. The verifiers $\mathsf{V_A}$, $\mathsf{V_B}$ simultaneously send ρ_k^A, ρ_k^B drawn from an ensemble $\{p_k, \rho_k^{AB}\}_k$. Alice and Bob, denoted A and B, have to distinguish the index k using only local operations and one round of simultaneous communication. Single lines are quantum, double lines are classical information.

then we would be able to construct a cloning procedure that violates the optimal approximate cloning bound.

First, note that it is beneficial to look at the protocol in the purified setting, where instead of sending a random Bell state, each verifier creates a Bell state $|\Phi_+\rangle$, keeps one register and sends the other to the prover. The 'correct' result is defined by a Bell measurement at the *end* of the protocol (and the prover's response shall be the same). This setting is equivalent to the original protocol. Looking at the entanglement structure of the purified protocol, it is evident that the task is equivalent to entanglement swapping. This is illustrated in Figure 5.4. How does an attack manipulate the entanglement structure?[1] Alice can apply a channel, mapping $A \mapsto A_1A_2$ and so can Bob, mapping $B \mapsto B_1B_2$. The total entanglement (in a measure of your choice that satisfies monogamy and monotonicity) $e_{A_1A_2}$ between V_A and A_1A_2 as well as $e_{B_1B_2}$ between V_B and B_1B_2 is at most one ebit. Thus, by the monogamy of entanglement we have

$$e_{A_1} + e_{A_2} \leq 1 \quad \text{and} \quad e_{B_1} + e_{B_2} \leq 1. \tag{5.1}$$

So at least one connection, say e_{A_1} w.l.o.g., must fulfil $e_{A_1} \leq 1/2$ and similarly on Bob's side. After communication, Alice holds A_1B_1 and Bob A_2B_2, on which they perform their final POVM to produce an answer. This is depicted in Figure 5.5.

[1] For simplicity, we will describe the scenario when qubit EPR pairs are used in the protocol. But the argument holds for any local dimension d, when 1 is replaced by $\log d$.

(a) Original protocol (b) Equivalent protocol

Figure 5.4: By (5.2) these two settings are equivalent. On registers A, B a Bell measurement is supposed to happen. In Figure 5.4a the verifiers prepare a random Bell state and send it to the prover, in Figure 5.4b each verifier prepares $|\Phi_+\rangle$, keeps one qubit and sends one to the prover. By performing the Bell measurement on the inputs, a Bell state is swapped into the registers $\mathsf{V_A}, \mathsf{V_B}$, on which the verifiers project onto a Bell state at the end, defining the correct answer. A and B need to simulate this as well as possible.

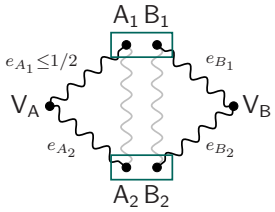


Figure 5.5: Entanglement structure in an attack, at the final stage when attackers have to measure and respond. The grey lines can contain an arbitrary amount of entanglement because it could consist of entanglement the attackers distributed in their round of communication. But, importantly, the entanglement of at least one connection (per attacker) to the respective verifier qubit must be limited by monogamy.

This argument alone allows us to bound $p_{\text{succ}}(\text{LOSQC})$. Consider just Alice (trace out Bob) and her registers A_1B_1. Then whatever POVM she applies and the result she sends back to $\mathsf{V_A}$ comprises an LOCC operation on the registers grouped together as $V_A(A_1B_1V_B)$. Thus, the entanglement between V_A and $A_1B_1V_B$ cannot be increased from the original 1/2. In particular, such an attack can only swap at most 1/2 ebit into V_AV_B. But on that final state in V_AV_B the verifiers perform a Bell measurement, which will inevitably give a probabilistic answer on a state that contains only at most 1/2 ebit, and thus the attackers' response will sometimes be incorrect. In contrast, the honest prover completes entanglement swapping by doing the Bell measurement, swapping 1 ebit into V_AV_B.

By the entanglement swapping identity

$$|\Phi_+\rangle_{V_AA}|\Phi_+\rangle_{V_BB} = \frac{1}{2}\Big[\,|\Phi_+\rangle_{V_AV_B}|\Phi_+\rangle_{AB} + |\Phi_-\rangle_{V_AV_B}|\Phi_-\rangle_{AB} + |\Psi_+\rangle_{V_AV_B}|\Psi_+\rangle_{AB} + |\Psi_-\rangle_{V_AV_B}|\Psi_-\rangle_{AB}\,\Big], \tag{5.2}$$

the honest response will always coincide with the verifiers' measurement result in the end.

Using for example E_F^2, the entanglement of formation squared, as a monogamous and monotonous entanglement measure, one can derive the following weak bound. In [BDSW96] it was shown that

$$E_F(\rho) \geq h\left(\frac{1}{2} + \sqrt{g(1-g)}\right), \tag{5.3}$$

with $g = \max_\Psi \langle\Psi|\,\rho\,|\Psi\rangle$ the *fully entangled fraction* of ρ, where the maximization is over all maximally entangled states Ψ, and h is the binary entropy function. Note that g corresponds to the attackers' success probability. This is because their success probability is at least $1/2$, meaning that the optimal state $\rho^{\mathrm{opt}}_{V_AV_B}$ they swap into V_AV_B has at least fidelity $1/2$ with the correct Bell state the verifiers project onto (and thus at most $1/2$ with any other Bell state). And if the optimal state $|\Psi\rangle$ in g is not one of the four Bell states, then using p_{succ} still provides a lower bound because the function $x \mapsto \sqrt{x(1-x)}$ is monotonically decreasing for $x \geq 1/2$ and so is h for arguments larger than $1/2$. Hence, we have

$$\frac{1}{\sqrt{2}} \geq E_F(\rho^{\mathrm{opt}}_{V_AV_B}) \geq h\left(\frac{1}{2} + \sqrt{p_{\mathrm{succ}}(1-p_{\mathrm{succ}})}\right). \tag{5.4}$$

Inverting h on the decreasing branch, since the argument is always at least $1/2$, leads to a quadratic inequality in $p_{\mathrm{succ}}(\mathrm{LOSQC})$, which can be solved to get

$$p^{\mathsf{AB}}_{\mathrm{succ}}(\mathrm{LOSQC}) \leq \frac{1}{2} + \sqrt{h^{-1}\left(\frac{1}{\sqrt{2}}\right)}\sqrt{1 - h^{-1}\left(\frac{1}{\sqrt{2}}\right)} \simeq 0.894. \tag{5.5}$$

One small subtlety is that E_F^2 is only known to be monogamous for registers that contain qubits. In principle, attackers could use higher-dimensional auxiliary systems in their attack.

In [ABSV22], we also derived a general bound using the squashed entanglement [CW04] as entanglement measure and a hashing bound from [DW05] to obtain $p^{\mathsf{AB}}_{\mathrm{succ}}(\mathrm{LOSQC}) \leq 0.926$ for $d = 2$. Using the no-cloning principle directly, this bound can be improved and generalised.

5.2.1. Theorem. *The optimal LOSQC attack success probability on* $\mathrm{QPV}_{\mathrm{Bell}}$ *is upper bounded by* $3/4$*, i.e.* $p^{\mathsf{AB}}_{\mathrm{succ}}(\mathrm{LOSQC}) \leq 3/4$*. For* $\mathrm{QPV}_{\mathrm{Bell}}$ *using local dimension* d *the bound is* $\frac{5}{6} - \frac{1}{6d}$*.*

Proof:
Denote by $p^{\mathsf{A}}_{\text{succ}}, p^{\mathsf{B}}_{\text{succ}}$ the optimal local success probabilities of A, B and let $p^{\mathsf{AB}}_{\text{succ}}$ be the optimal coordinated attack. Considering just the local success probabilities is a relaxation because, in principle, it allows for different responses from A and B, which is not allowed in a realistic attack. It is clear that

$$p^{\mathsf{AB}}_{\text{succ}} \leq \min\{p^{\mathsf{A}}_{\text{succ}}, p^{\mathsf{B}}_{\text{succ}}\}, \tag{5.6}$$

and we will now proceed to upper bound $\min\{p^{\mathsf{A}}_{\text{succ}}, p^{\mathsf{B}}_{\text{succ}}\}$. The structure of any LOSQC attack on QPV_{Bell} must lead to an entanglement structure as drawn in Figure 5.5.

In particular, the verifiers themselves (or even just one of them) could create the situation of Figure 5.5 themselves in their own lab because they know what the optimal success strategies are. They could simply create the inputs and apply the optimal strategies of A, B to registers A, B. This splits $A \mapsto A_1A_2$ and $B \mapsto B_1B_2$. Imagine now that we add a third input state $|\Phi_+\rangle_{V_CC}$ in the registers V_CC and that the optimal strategy of B is applied to register C, mapping $C \mapsto C_1C_2$. Note that the state in C_1C_2 is identical to the one in B_1B_2. This procedure creates the following entanglement structure:

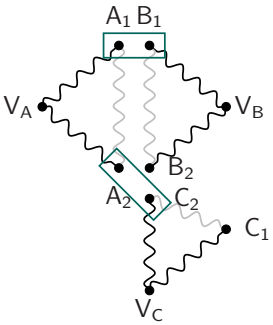


Figure 5.6: Entanglement structure created by someone, say a trusted verifier, who generated three inputs and applied the optimal local attacker channel $\mathcal{A}$ of A on one and the analogous channel $\mathcal{B}$ of B on two of the three inputs. They then apply the optimal measurement of A on registers A_1B_1 and the one of B on registers A_2C_2.

Afterwards, the optimal measurement of A is applied to registers A_1B_1 and the optimal measurement of B is applied to registers A_2C_2. This swaps entanglement to the registers V_AV_B and V_AV_C, respectively. Tracing out all other registers, we end up with the structure depicted in Figure 5.7.

The state $\rho^{\text{opt}}_{V_AV_B}$ corresponds to the state giving A her optimal local success probability in attacking QPV_{Bell}, because we applied the optimal split $A \mapsto A_1A_2$

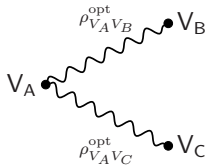


Figure 5.7: Using the optimal attack strategies of A and B we may create this situation.

and the optimal local measurement on A_1B_1 in order to remotely prepare $\rho^{\mathrm{opt}}_{V_AV_B}$. Likewise, the state $\rho^{\mathrm{opt}}_{V_AV_C}$ corresponds to the state giving B his optimal local success probability. At this stage $\mathsf{V_A}$ could take some state $|\phi\rangle_{V'_A}$ and attempt to use the standard teleportation protocol to teleport it to *both* $\mathsf{V_B}$ and $\mathsf{V_C}$. In general, this will result in some states $\rho^{\phi}_{V_B}$ and $\rho^{\phi}_{V_C}$ at $\mathsf{V_B}$ and $\mathsf{V_C}$, respectively. The average teleportation fidelity f between the resultant state and the original one depends only on the maximally entangled fraction of the resource state ρ, [HHH99], and is given by

$$f = \frac{Fd+1}{d+1} = \frac{\langle\Phi_+|\rho|\Phi_+\rangle\, d+1}{d+1}, \tag{5.7}$$

for local dimension d. A consequence of optimal asymmetric $1 \to 2$ cloning is that the arithmetic mean of the average fidelities fulfils [SIGA05],

$$\frac{f_{\mathsf{V_B}} + f_{\mathsf{V_C}}}{2} \leq \frac{5}{6}, \tag{5.8}$$

no matter which resource states was used. Plugging in equation (5.7) for each f in (5.8) yields

$$\frac{\langle\Phi_+|\rho_{V_AV_B}|\Phi_+\rangle + \langle\Phi_+|\rho_{V_AV_C}|\Phi_+\rangle}{2} \leq \frac{5}{6} - \frac{1}{6d}. \tag{5.9}$$

This allows us to bound the average success probability $(p^{\mathsf{A}}_{\mathrm{succ}} + p^{\mathsf{B}}_{\mathrm{succ}})/2$. Note that any Bell state $|B_i\rangle$ can be regarded as $|\Phi_+\rangle$ with a suitable local unitary $\mathbb{1} \otimes U_i$ applied to the latter. Thus, we can write

$$\begin{aligned}
\frac{p^{\mathsf{A}}_{\mathrm{succ}} + p^{\mathsf{B}}_{\mathrm{succ}}}{2} &= \frac{1}{d^2}\sum_{i=0}^{d^2-1} \frac{\langle\Phi_+|\mathbb{1}\otimes U_i^\dagger \rho^i_{V_AV_B} \mathbb{1}\otimes U_i|\Phi_+\rangle + \langle\Phi_+|\mathbb{1}\otimes U_i^\dagger \rho^i_{V_AV_C} \mathbb{1}\otimes U_i|\Phi_+\rangle}{2} \\
&\leq \frac{1}{d^2}\sum_{i=0}^{d^2-1}\left(\frac{5}{6} - \frac{1}{6d}\right) \\
&= \frac{5}{6} - \frac{1}{6d},
\end{aligned} \tag{5.10}$$

where the inequality follows from the fact that (5.9) holds for *any* states $\rho_{V_A V_B}$ and $\rho_{V_A V_C}$. Hence

$$p_{\text{succ}}^{\mathsf{AB}}(d) \leq \min\{p_{\text{succ}}^{\mathsf{A}}(d), p_{\text{succ}}^{\mathsf{B}}(d)\} \leq \frac{p_{\text{succ}}^{\mathsf{A}}(d) + p_{\text{succ}}^{\mathsf{B}}(d)}{2} \leq \frac{5}{6} - \frac{1}{6d}. \tag{5.11}$$

For $d = 2$ this gives $p_{\text{succ}}^{\mathsf{AB}}(2) \leq 3/4$. □

We suspect that this bound is not tight because we relaxed the QPV situation and only looked at the local success probabilities of A and B, and their average. In reality, however, A and B are forced to respond with the same answer. Our argument does not include this coordination, and therefore we think that the realistic success probability $p_{\text{succ}}^{\mathsf{AB}}$ is only loosely upper bounded by (5.11). For $d = 2$ the upper bound of $3/4$ has been further improved to $\ln(2) \simeq 0.69$ in [ACG+23]. The argument there is similar to the one we gave here, but adds more and more auxiliary verifiers, thus building up a 'ring' of entanglement via the local attack strategies. It turns out that this can then be connected to a special case of the quantum marginal problem on cyclic graphs with Werner states as bipartite marginals between neighbours, which in turn is related to spin chains. The maximal nearest-neighbour entanglement of Heisenberg $\text{XXX}_{1/2}$ spin chains in the limit of $N \to \infty$ qubits, which is $\ln(2)$, then bounds $p_{\text{succ}}(\text{LOSQC})$.

5.3 Studying LOSCC and LOSQC more generally

5.3.1 Necessary and sufficient conditions

Unlike traditional local operations and classical communication (LOCC), the maps generated by both LOSCC and LOSQC maps have a relatively simple description.

For LOSQC, Alice (resp. Bob) performs a local isometry $V : A \to A_1 A_2$ (resp. $W : B \to B_1 B_2$) and sends system A_2 to Bob (resp. B_1 to Alice). Alternatively, we can say that Alice holds the outputs of the quantum channels $\mathcal{E}(\cdot) = \text{Tr}_{A_2}\big[V(\cdot)V^\dagger\big]$ and $\mathcal{F}^c(\cdot) = \text{Tr}_{B_2}\big[W(\cdot)W^\dagger\big]$ after communication, while Bob holds the outputs of their complements $\mathcal{E}^c(\cdot) = \text{Tr}_{A_1}\big[V(\cdot)V^\dagger\big]$ and $\mathcal{F}(\cdot) = \text{Tr}_{B_1}\big[W(\cdot)W^\dagger\big]$.

For LOSCC, the local isometries are replaced by local instruments $(\mathcal{A}_x^{A\to A})_x$ and $(\mathcal{B}_y^{B\to B})_y$, which are collections of completely positive maps for which $\mathcal{A}_x \otimes \mathcal{B}_y$ describes the joint evolution when Alice broadcasts classical message x and Bob broadcasts classical message y. Without loss of generality, we can assume that these are 'fine-grained' instruments having the form $\mathcal{A}_x(\cdot) = A_x(\cdot)A_x^\dagger$ and $\mathcal{B}_y(\cdot) = B_y(\cdot)B_y^\dagger$ with Kraus rank one for each x and y, respectively, since the coarse-graining of more general maps can always be delayed until the second round in which the local state discrimination measurement is performed. Up to

normalisation, the local instrument transforms $\rho_{AB} \mapsto A_x \otimes B_y(\rho_{AB}) A_x^\dagger \otimes B_y^\dagger$ given classical messages (x, y).

The conditions for perfect state discrimination using either LOSCC and LOSQC are intuitive to understand. Since no interactive communication is allowed, Alice and Bob must be able to 'distribute the orthogonality' of their states. That is, the communication must transform the initial states $\{\rho_k^{AB}\}_k$ such that afterwards the reduced states are pairwise orthogonal for both Alice and Bob. For LOSQC, this means that

$$\begin{aligned} &\mathrm{Tr}[(\mathcal{E} \otimes \mathcal{F}^c)(\rho_k^{AB})(\mathcal{E} \otimes \mathcal{F}^c)(\rho_{k'}^{AB})] = 0, \\ &\mathrm{Tr}[(\mathcal{E}^c \otimes \mathcal{F})(\rho_k^{AB})(\mathcal{E}^c \otimes \mathcal{F})(\rho_{k'}^{AB})] = 0 \end{aligned} \tag{5.12}$$

for all k and $k' \neq k$. For LOSCC discrimination, the reduced states of $A_x \otimes B_y(\rho_k^{AB}) A_x^\dagger \otimes B_y^\dagger$ must be pairwise orthogonal for $k \neq k'$ and every pair (x, y). Defining the positive operator-valued measure (POVM) operators $M_x \coloneqq A_x^\dagger A_x$ and $N_y \coloneqq B_y^\dagger B_y$, we immediately obtain the following.

5.3.1. Proposition. *The states $\{\rho_k^{AB}\}_k$ can be perfectly distinguished by LOSQC if and only if there exist isometries $V : A \to A_1 A_2$ at Alice and $W : B \to B_1 B_2$ at Bob such that after communication both end up with an orthogonal set of states. That is, for $\mathcal{E}(\cdot) = \mathrm{Tr}_{A_2}\big[V(\cdot)V^\dagger\big]$, $\mathcal{E}^c(\cdot) = \mathrm{Tr}_{A_1}\big[V(\cdot)V^\dagger\big]$ and $\mathcal{F}(\cdot) = \mathrm{Tr}_{B_1}\big[W(\cdot)W^\dagger\big]$, $\mathcal{F}^c(\cdot) = \mathrm{Tr}_{B_2}\big[W(\cdot)W^\dagger\big]$ it holds that*

$$\begin{aligned} &\mathrm{Tr}[(\mathcal{E} \otimes \mathcal{F}^c)(\rho_k^{AB})(\mathcal{E} \otimes \mathcal{F}^c)(\rho_{k'}^{AB})] = 0 \qquad \textit{and} \\ &\mathrm{Tr}[(\mathcal{E}^c \otimes \mathcal{F})(\rho_k^{AB})(\mathcal{E}^c \otimes \mathcal{F})(\rho_{k'}^{AB})] = 0 \end{aligned} \tag{5.13}$$

for all k and $k' \neq k$. The states $\{\rho_k^{AB}\}_k$ can be perfectly distinguished by LOSCC if and only if there exist POVMs $\{M_x^A\}_x$ at Alice and $\{N_y^B\}_y$ at Bob such that

$$\begin{aligned} &\mathrm{Tr}[\mathrm{Tr}_A[(M_x^A \otimes N_y^B)\rho_k^{AB}]\,\mathrm{Tr}_A[(M_x^A \otimes N_y^B)\rho_{k'}^{AB}]] = 0 \qquad \textit{and} \\ &\mathrm{Tr}[\mathrm{Tr}_B[(M_x^A \otimes N_y^B)\rho_k^{AB}]\,\mathrm{Tr}_B[(M_x^A \otimes N_y^B)\rho_{k'}^{AB}]] = 0 \end{aligned} \tag{5.14}$$

for all $x, y, k \neq k'$.

Proofsketch:
($\rightarrow$) It is evident that these conditions are necessary. If they were not fulfilled, at least one of Alice and Bob would end up with a non-orthogonal set of states, which cannot be distinguished perfectly. Hence, at least one of them would incur an error by the Holevo-Helström theorem.

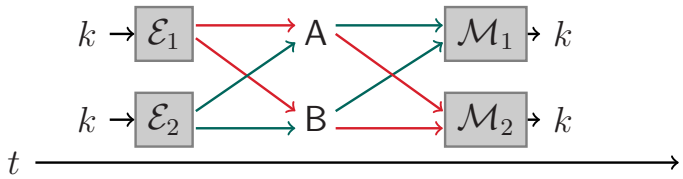
($\leftarrow$) For LOSQC, indeed, if such channels exist, both Alice and Bob end up with orthogonal sets of states, so there exist measurements that perfectly distinguish those sets and allow them to identify the index k. For LOSCC, the argument is similar. There could be many more measurement outcomes (x, y) than indices k,

depending on how they choose their local POVMs. But if those conditions hold, each pair (x, y) uniquely points to one index k, so Alice and Bob can distinguish the set perfectly. □

5.3.2 Constructing perfect LOSQC discriminable ensembles

To get a more concrete feel about LOSQC, we give a recipe for building LOSQC distinguishable ensembles. The key observation is that perfect LOSQC discrimination can be viewed as 'undoing two secret sharing schemes of the same classical secret k (see Figure 5.8). Informally, we are going to show the following.

5.3.2. THEOREM. *(Informal) Consider secret sharing maps $\mathcal{E}_1 : k \mapsto \tau_k^{A_1B_1}$ and $\mathcal{E}_2 : k \mapsto \sigma_k^{A_2B_2}$ such that a single share reveals no local information about k. Then $\{p_k, \tau_k^{A_1B_1} \otimes \sigma_k^{A_2B_2}\}$ is LOSQC discriminable but not locally discriminable.*



(a) Secret Sharing (b) LOSQC

Figure 5.8: Depiction of perfect LOSQC as secret sharing in reverse. The $\mathcal{M}_i$ are the decoding measurements at Alice and Bob after communication. $\mathcal{E}_i$ are the secret sharing scheme channels that produce two shares. Having only one share of each secret sharing scheme reveals no information about k, but if one has both shares one can decode k. Thus, if A and B each get one share of each scheme as input (registers A_1A_2 and B_1B_2, respectively), they can quantum communicate such that A holds both shares A_1B_1 of one scheme and B holds both shares A_2B_2 of the other scheme, to perfectly discriminate k via LOSQC.

To prove Theorem 5.3.2, we need some basic tools regarding state discrimination and min-entropy.

5.3.3. FACT ([KRS09, Tom15]). The optimal state discrimination probability of the ensemble $\{p_k, \rho_A^k\}$ given the A space is $p_{\text{guess}}(K|A) = 2^{-H_{\min}(K|A)_\rho}$.

The above allows us to define a class of natural secret sharing schemes.

5.3.4. Definition. Consider a map $\mathcal{E}_{K\to A_i^m}$, which may be viewed as a quantum secret sharing scheme. $\mathcal{E}$ is single-share perfectly secure if

$$H_{\min}(K|A_i)_{\mathcal{E}(\pi_K)} = \log(|K|) \quad \forall i \in [m], \tag{5.15}$$

where $\pi_K = |K|^{-1}\sum_k |k\rangle\langle k|$.

The idea is then that the type of secret sharing schemes given above have the property that given secret shares from different secret sharing schemes, the secret k is still not locally determinable. To prove this, we need the following lemmas which are easiest to establish in some generality and then simply note that $H_{\min}$ is a specific case, namely $\alpha \to \infty$. These lemmas rely on properties of Rényi divergences, to which we refer the reader to [Tom15].

5.3.5. Proposition. *For any Rényi entropy H_α we have $H_\alpha(X)_\rho = \log(|X|)$ if and only if $\rho_X = \pi_X = \mathbb{1}_X/|X|$.*

Proof:
Consider ρ_X decomposed in its eigenbasis. That is, we can focus on $\rho_X = p_X$ where p_X is diagonal. Let $H_\alpha(X)_\rho = -D_\alpha(\rho_X||\mathbb{1}_X)$ be a Rényi entropy via D_α being a Rényi divergence. Then,

$$H_\alpha(X)_\rho = -D_\alpha(p_X||\mathbb{1}_X) = -D_\alpha(p_X||\pi_X) + \log(|X|)\ , \tag{5.16}$$

where we used the normalisation property. By positive definiteness, one will only equal $\log(|X|)$ if $-D_\alpha(p_X||\pi_X) = 0$, which only happens if $p_X = \pi_X$. □

5.3.6. Lemma. *Given ρ_{XB}, $H_\alpha(X|B)_\rho = \log(|X|)$ if and only if $\rho_{XB} = \pi_X \otimes \rho_B$.*

Proof:
Let $H_\alpha(X|B)_\rho = -D_\alpha(\rho_{XB}||\mathbb{1}_X \otimes \sigma_B)$ be a Rényi divergence, where σ_B may be optimised over.

($\leftarrow$) Let $\rho_{XB} = \pi_X \otimes \rho_B$. Then,

$$\begin{aligned} H_\alpha(X|B)_\rho &= -D_\alpha(\pi_X \otimes \rho_B||\mathbb{1}_X \otimes \sigma_B) \\ &= -D_\alpha(\pi_X \otimes \rho_B||\pi_X \otimes \sigma_B) + \log(|X|) = \log(|X|), \end{aligned} \tag{5.17}$$

where the last equality either follows from $\sigma_B = \rho_B$ or because by positive definiteness, optimising over σ_B results in ρ_B.

($\rightarrow$) First, $H_\alpha(X)_\rho = \log(|X|)$ if and only if $\rho_X = \pi_X$ by the previous lemma. By the data processing inequality and our assumption $\log(|X|) = H(X|B)_\rho \leq$

$H(X)_\rho$. Thus, we may conclude $\rho_X = \pi_X$. Hence, we have $\rho_{XB} = |X|^{-1} \sum_x |x\rangle\langle x| \otimes \rho_B^x$. Next,

$$\begin{aligned} \log(|X|) &= H_\alpha(X|B)_\rho \\ &= -D_\alpha(|X|^{-1} \sum_x |x\rangle\langle x| \otimes \rho_B^x || \mathbb{1}_A \otimes \sigma_B) \\ &= -D_\alpha(\sum_x |x\rangle\langle x| \otimes \rho_B^x || \mathbb{1}_A \otimes \sigma_B) + \log(|X|). \end{aligned} \tag{5.18}$$

This implies $D_\alpha(\sum_x |x\rangle\langle x| \otimes \rho_B^x || \mathbb{1}_A \otimes \sigma_B) = 0$. By positive definiteness, this can only be the case if $\sum_x |x\rangle\langle x| \otimes \rho_B^x = \mathbb{1}_A \otimes \sigma_B$. This implies $\rho_B^x = \sigma_B$ for every x. Thus, $\rho_{XB} = \rho_X \otimes \rho_B$ for some $\rho_B \in \mathrm{D}(\mathcal{H}_B)$. □

Having established these properties, which in particular hold for $H_{\min}(X|B)$, we can prove Theorem 5.3.2, which we restate more formally.

5.3.7. Theorem (Theorem 5.3.2 but formal). *Given any two single-share perfectly secure quantum secret sharing schemes $\mathcal{E}^1_{K\to A_1B_1}$, $\mathcal{E}^2_{K\to A_2B_2}$, the ensemble $\{|K|^{-1}, \rho^k_{A_{1,2}B_{1,2}} := \mathcal{E}^1(|k\rangle\langle k|) \otimes \mathcal{E}^2(|k\rangle\langle k|)\}_k$, where Alice receives $A_{1,2} := A_1A_2$ and Bob receives $B_{1,2} := B_1B_2$, is LOSQC discriminable, but not locally discriminable.*

Proof:
Consider the global state after the secret sharing encoding:

$$\rho_{KA_1B_1A_2B_2} = |K|^{-1} \sum_k |k\rangle\langle k| \otimes \tau^k_{A_1B_1} \otimes \sigma^k_{A_2B_2}, \tag{5.19}$$

which implies

$$\rho_{KA_1A_2} = |K|^{-1} \sum_k |k\rangle\langle k| \otimes \tau^k_{A_1} \otimes \sigma^k_{A_2}, \tag{5.20}$$

$$\rho_{KB_1B_2} = |K|^{-1} \sum_k |k\rangle\langle k| \otimes \tau^k_{B_1} \otimes \sigma^k_{B_2}. \tag{5.21}$$

By the single-share perfect security definition and Lemma 5.3.6,

$$\begin{aligned} \rho_{KA_1} &= \pi_K \otimes \omega^1_{A_1} \quad \rho_{KA_2} = \pi_K \otimes \omega^2_{A_2}, \\ \rho_{KB_1} &= \pi_K \otimes \omega^3_{B_1} \quad \rho_{KA_2} = \pi_K \otimes \omega^4_{B_2}, \end{aligned} \tag{5.22}$$

where each ω^i is in its appropriate space and does not have to be the same as the others. Combining (5.20) and (5.22), by considering the partial traces, this implies

$$\begin{aligned} \rho_{KA_1A_2} &= \pi_K \otimes \omega^1_{A_1} \otimes \omega^2_{A_2}, \\ \rho_{KB_1B_2} &= \pi_K \otimes \omega^3_{B_1} \otimes \omega^4_{B_2}. \end{aligned} \tag{5.23}$$

Now, applying Lemma 5.3.6, we may conclude $H_{\min}(K|A_{1,2})_\rho = \log(|K|)$ and $H_{\min}(K|B_{1,2})_\rho = \log(|K|)$, which means this is still a single-share perfectly secure secret sharing scheme, so no local measurements can reveal any information about k. However, clearly if Alice sends A_2 to Bob and Bob sends B_1 to Alice, then this defines a perfect LOSQC strategy. □

5.3.3 Separation between LOSCC and LOSQC

A separation between LOSCC and LOSQC was first shown in [ABSV22] for an ensemble of entangled input states, where it may be less surprising that quantum communication can help over classical communication. In this section, we will give a product state ensemble with the same property.

5.3.8. Proposition. *The states*

$$\begin{aligned} |\psi_0\rangle &= |0\rangle\,|0\rangle & |\psi_4\rangle &= |2\rangle\,|1+3\rangle \\ |\psi_1\rangle &= |0\rangle\,|1\rangle & |\psi_5\rangle &= |2\rangle\,|1-3\rangle \\ |\psi_2\rangle &= |1\rangle\,|1+2\rangle & |\psi_6\rangle &= |3\rangle\,|2+i3\rangle \\ |\psi_3\rangle &= |1\rangle\,|1-2\rangle & |\psi_7\rangle &= |3\rangle\,|2-i3\rangle\,, \end{aligned} \tag{5.24}$$

where $|i \pm j\rangle = \frac{1}{\sqrt{2}}(|i\rangle \pm |j\rangle)$ *and similarly for the complex states, can be perfectly discriminated via LOSQC, but not via LOSCC. Moreover, for perfect LOSQC discrimination, the distribution of entanglement is necessary.*

Proof:
Since Alice's states are classical, she will just measure in the computational basis and forward her outcome to Bob. We can thus focus on Bob's action and he must ensure that both Alice and him can distinguish the two states corresponding to input $|k\rangle$ at Alice after communication.

First, we demonstrate a perfect LOSQC strategy. Let Bob apply the isometry

$$\begin{aligned} V|0\rangle &= |00\rangle\,, \\ V|1\rangle &= \frac{1}{\sqrt{2}}(|11\rangle + |22\rangle), \\ V|2\rangle &= \frac{1}{\sqrt{2}}(|11\rangle - |22\rangle), \\ V|3\rangle &= \frac{1}{\sqrt{2}}(|12\rangle + |21\rangle). \end{aligned} \tag{5.25}$$

On the other states it acts as

$$\begin{aligned} V|1+2\rangle &= |11\rangle & V|1-2\rangle &= |22\rangle\,, \\ V|1+3\rangle &= |1+2\rangle\,|1+2\rangle & V|1-3\rangle &= |1-2\rangle\,|1-2\rangle\,, \\ V|2+i3\rangle &= |1+i2\rangle\,|1+i2\rangle & V|2-i3\rangle &= |1-i2\rangle\,|1-i2\rangle\,. \end{aligned} \tag{5.26}$$

Bob then keeps one register and sends the other one to Alice. After communication, both Alice and Bob just check which bit k Alice has received, followed by the corresponding measurement to distinguish the two possible inputs of Bob for each k. For $k = 0$ it is $\{|0\rangle\langle 0|, |1\rangle\langle 1| + |2\rangle\langle 2|\}$, for $k = 1$ it is $\{|1\rangle\langle 1|, |2\rangle\langle 2|\}$, for $k = 2$ it is $\{|1+2\rangle\langle 1+2|, |1-2\rangle\langle 1-2|\}$ and for $k = 3$ it is $\{|1+i2\rangle\langle 1+i2|, |1-i2\rangle\langle 1-i2|\}$. Note that for each k we operate in smaller subspaces spanned by either $\{|0\rangle, |1\rangle, |2\rangle\}$ or just $\{|1\rangle, |2\rangle\}$, respectively. Clearly, both Alice and Bob perfectly distinguish the input ensemble this way.

Next, we show that LOSCC cannot distinguish it perfectly. In the following the amplitudes are less relevant, so for notational simplicity we will absorb them into the kets $|x_i\rangle$ or $|\phi_i\rangle$, respectively, which shall be assumed to be unnormalised. Let Bob apply an isometry $W : B \mapsto B_1B_2E$, where he sends B_1 to Alice, keeps B_2 and E denotes the environment. Suppose Bob does *not* distribute entanglement to Alice on input $|\psi_1\rangle$. In general, this means that he maps

$$W|1\rangle_B = \sum_i |x_i\rangle_{B_1} |y_i\rangle_{B_2} |i\rangle_E , \tag{5.27}$$

such that the reduced state on B_1B_2 reads $\sum_i |x_i\rangle\langle x_i|_{B_1} \otimes |y_i\rangle\langle y_i|_{B_2}$. On states $|2\rangle_B$, $|3\rangle_B$ there are no restrictions, so $W|2\rangle_B = \sum_i |\phi_i\rangle_{B_1B_2} |i\rangle_E$ and similarly for $|3\rangle_B$. Therefore,

$$W|1 \pm 2\rangle = \frac{1}{\sqrt{2}} \sum_i \big(|x_i\rangle_{B_1} |y_i\rangle_{B_2} \pm |\phi_i\rangle_{B_1B_2} \big) |i\rangle_E . \tag{5.28}$$

For local orthogonality, we need that the two states in (5.28) are orthogonal on both B_1 and on B_2. Let us write

$$|\phi_i\rangle_{B_1B_2} = |x'_{\{i\}}\rangle_{B_1} |y_i\rangle_{B_2} + \sum_{j\neq i} |x'_{\{j\}}\rangle_{B_1} |y_j\rangle_{B_2} \tag{5.29}$$

in the basis $\{|x_m\rangle_{B_1} |y_m\rangle_{B_2}\}_{m,n}$, where $|x'_{\{k\}}\rangle_{B_1}$ denotes the (unnormalised) superposition of all $|x_j\rangle_{B_1}$ that have $|y_k\rangle_{B_2}$ attached to it in $|\phi_i\rangle_{B_1B_2}$. Then

$$\begin{aligned} |x_i\rangle_{B_1} |y_i\rangle_{B_2} \pm |\phi_i\rangle_{B_1B_2} = \\ \Big(|x_i\rangle_{B_1} \pm |x'_{\{i\}}\rangle_{B_1} \Big) |y_i\rangle_{B_2} \pm \sum_{j\neq i} |x'_{\{j\}}\rangle_{B_1} |y_j\rangle_{B_2} . \end{aligned} \tag{5.30}$$

This state shall have orthogonal marginals on both B_1 at Alice and B_2 at Bob. Alice's marginals are

$$\rho_{B_1}^{1\pm 2} = |x_i \pm x'_{\{i\}}\rangle\langle x_i \pm x'_{\{i\}}|_{B_1} + \sum_{j\neq i} |x'_{\{j\}}\rangle\langle x'_{\{j\}}|_{B_1} . \tag{5.31}$$

The orthogonality condition then is

$$\begin{aligned} 0 &= \mathrm{Tr}\left[\rho_{B_1}^{1+2}\rho_{B_1}^{1-2}\right] \\ &= \sum_{j\neq i}|\langle x_i + x'_{\{i\}}|x'_{\{j\}}\rangle|^2 + \sum_{j\neq i}|\langle x_i - x'_{\{i\}}|x'_{\{j\}}\rangle|^2 + \sum_{j\neq i}\sum_{k\neq i}|\langle x'_{\{j\}}|x'_{\{k\}}\rangle|^2, \end{aligned} \tag{5.32}$$

which implies $|x'_{\{j\}}\rangle = 0$ for all $j \neq i$, since all terms in (5.32) are non-negative an thus have to be equal to zero in order to add up to 0, and in particular, $|\langle x'_{\{j\}}|x'_{\{j\}}\rangle|^2 = 0$. Thus, (5.30) just reads

$$|x_i\rangle_{B_1}|y_i\rangle_{B_2} \pm |\phi_i\rangle_{B_1B_2} = \left(|x_i\rangle_{B_1} \pm |x'_{\{i\}}\rangle_{B_1}\right)|y_i\rangle_{B_2}. \tag{5.33}$$

The orthogonality condition on Bob's marginals is

$$0 = \mathrm{Tr}\left[\rho_{B_2}^{1+2}\rho_{B_2}^{1-2}\right] = \langle x_i + x'_{\{i\}}|x_i + x'_{\{i\}}\rangle\,\langle x_i - x'_{\{i\}}|x_i - x'_{\{i\}}\rangle, \tag{5.34}$$

which implies that $|x'_{\{i\}}\rangle_{B_1} = |x_i\rangle_{B_1}$ or $|x'_{\{i\}}\rangle_{B_1} = -|x_i\rangle_{B_1}$. Thus, we have $|x'_{\{i\}}\rangle_{B_1} = (-1)^{r_i}|x_i\rangle_{B_1}$ for some $r_i \in \{0,1\}$. This establishes that the isometry acts as

$$W|2\rangle_B = \sum_i (-1)^{r_i}|x_i\rangle_{B_1}|y_i\rangle_{B_2}|i\rangle_E. \tag{5.35}$$

The same argument can be repeated for $W|3\rangle_B = \sum_i |\chi_i\rangle_{B_1B_2}|i\rangle_E$ to get

$$W|3\rangle_B = \sum_i (-1)^{s_i}|x_i\rangle_{B_1}|y_i\rangle_{B_2}|i\rangle_E, \tag{5.36}$$

for some $s_i \in \{0,1\}$. But that means on inputs $|2 \pm i3\rangle_B$ it acts, by linearity, as

$$W|2 \pm i3\rangle_B = \sum_i \left((-1)^{s_i} \pm i(-1)^{r_i}\right)|x_i\rangle_{B_1}|y_i\rangle_{B_2}|i\rangle_E. \tag{5.37}$$

These two states cannot have orthogonal marginals on B_1 for Alice and B_2 for Bob. For example, for Alice we get

$$\begin{aligned} 0 \overset{!}{=} \mathrm{Tr}\left[\rho_{B_1}^{2+i3}\rho_{B_1}^{2-i3}\right] &= \frac{1}{2}\sum_i \langle x_i|x_i\rangle\left((-1)^{r_i} + i(-1)^{s_i}\right)\left((-1)^{r_i} - i(-1)^{s_i}\right) \\ &= \frac{1}{2}\sum_i \langle x_i|x_i\rangle\left(1 - i^2\right) \\ &= \sum_i \langle x_i|x_i\rangle = 1, \end{aligned} \tag{5.38}$$

where we remember that the $|x_i\rangle_{B_1}$ are unnormalised and contain the amplitudes such that $\langle x_i|x_i\rangle$ is a probability. To summarise, we showed that if Bob's isometry W does *not* distribute entanglement on input $|1\rangle_B$, then they necessarily make errors on other states of the input ensemble. Therefore, Bob must distribute entanglement, and hence no LOSCC strategy could ever perfectly distinguish the ensemble given in this theorem. □

5.3.4 Uncertainty relation and error lower bound

In this section we establish local error bounds in state discrimination using local operations and simultaneous quantum communication (LOSQC). We first state the core lemma we will need. This establishes a general fact about local state discrimination. Suppose $|\gamma_0\rangle^{AB}$ and $|\gamma_1\rangle^{AB}$ are two orthogonal states which Alice can distinguish by herself with very high probability. This requires the reduced density matrices γ_0^A and γ_1^A to be nearly orthogonal. Consequently, tracing out Alice in any bipartite superposition state $\alpha\,|\gamma_0\rangle^{AB} \pm \beta\,|\gamma_1\rangle^{AB}$ should cause a nearly complete dephasing for Bob's reduced density matrix. Hence, the two states $|\gamma_\pm\rangle^{AB} = \alpha\,|\gamma_0\rangle^{AB} \pm \beta\,|\gamma_1\rangle^{AB}$ should be almost indistinguishable from Bob's perspective. Indeed, the following lemma confirms this intuition.

5.3.9. Lemma (Uncertainty Relation). *Consider orthogonal states $|\gamma_0\rangle^{AB}$ and $|\gamma_1\rangle^{AB}$. Then for $|\gamma_\pm\rangle^{AB} = \alpha\,|\gamma_0\rangle^{AB} \pm \beta\,|\gamma_1\rangle^{AB}$ with $\alpha, \beta \neq 0$, we have*

$$D_{\mathrm{tr}}(\gamma_+^B, \gamma_-^B) \leq 2|\alpha\beta^*| F(\gamma_0^A, \gamma_1^A). \tag{5.39}$$

Proof:
Define $z \coloneqq \alpha\beta^* = |z|e^{i\varphi}$ for some φ and we will usually just write γ for $|\gamma\rangle\langle\gamma|$. Then we have

$$\begin{aligned} D_{\mathrm{tr}}(\gamma_+^B, \gamma_-^B) &= \frac{1}{2}\|\mathrm{Tr}_A\big[\gamma_+^{AB} - \gamma_-^{AB}\big]\|_1 \\ &= \|\mathrm{Tr}_A\Big[z\,|\gamma_0\rangle\langle\gamma_1|^{AB} + z^*\,|\gamma_1\rangle\langle\gamma_0|^{AB}\Big]\|_1. \end{aligned} \tag{5.40}$$

For later use we can rewrite this as follows. By definition of the trace norm, for some unitary $-\mathbb{1} \preceq Q \preceq \mathbb{1}$, we have

$$\begin{aligned} D_{\mathrm{tr}}(\gamma_+^B, \gamma_-^B) &= \max_Q \frac{1}{2}\Big|\,\mathrm{Tr}\big[Q\big(\gamma_+^B - \gamma_-^B\big)\big]\Big| = \max_Q \frac{1}{2}\Big|\,\mathrm{Tr}\big[(\mathbb{1}\otimes Q)\big(\gamma_+^{AB} - \gamma_-^{AB}\big)\big]\Big| \\ &= \Big|\,\mathrm{Tr}\Big[(\mathbb{1}\otimes Q_{\max})\Big(z\,|\gamma_0\rangle\langle\gamma_1|^{AB} + z^*\,|\gamma_1\rangle\langle\gamma_0|^{AB}\Big)\Big]\Big| \\ &= \Big|\,\mathrm{Tr}\Big[(\mathbb{1}\otimes Q_{\max})\Big(|z|\,|\tilde{\gamma}_0\rangle\langle\gamma_1|^{AB} + |z^*|\,|\gamma_1\rangle\langle\tilde{\gamma}_0|^{AB}\Big)\Big]\Big|, \end{aligned} \tag{5.41}$$

where we redefined $|\tilde{\gamma_0}\rangle^{AB} = e^{i\varphi}\,|\gamma_0\rangle^{AB}$. Moreover, by Uhlmann's theorem, Alice's fidelity is lower bounded by

$$\begin{aligned} F(\gamma_0^A, \gamma_1^A) &= \max_U \Big|\mathrm{Tr}\Big[(\mathbb{1}\otimes U)\,|\gamma_0\rangle\langle\gamma_1|^{AB}\Big]\Big| \\ &= \frac{1}{2}\Big(\max_U \Big|\mathrm{Tr}\Big[(\mathbb{1}\otimes U)\,|\gamma_0\rangle\langle\gamma_1|^{AB}\Big]\Big| + \max_U \Big|\mathrm{Tr}\Big[(\mathbb{1}\otimes U)\,|\gamma_1\rangle\langle\gamma_0|^{AB}\Big]\Big|\Big) \\ &\geq \frac{1}{2}\max_U \Big|\mathrm{Tr}\Big[(\mathbb{1}\otimes U)\Big(|\gamma_0\rangle\langle\gamma_1|^{AB} + |\gamma_1\rangle\langle\gamma_0|^{AB}\Big)\Big]\Big|. \end{aligned} \tag{5.42}$$

This we can multiply by $1 = |z|/|z|$ and rewrite

$$\begin{aligned} F(\gamma_0^A, \gamma_1^A) &= F(\tilde{\gamma_0}^A, \gamma_1^A) \\ &\geq \frac{1}{2|z|} \max_U \Big| \mathrm{Tr}\Big[(\mathbb{1} \otimes U) \Big(|z| \, |\tilde{\gamma_0}\rangle\langle\gamma_1|^{AB} + |z^*| \, |\gamma_1\rangle\langle\tilde{\gamma_0}|^{AB} \Big) \Big] \Big|, \end{aligned} \tag{5.43}$$

where the first equality follows from $|\gamma_0\rangle\langle\gamma_0| = |\tilde{\gamma}_0\rangle\langle\tilde{\gamma}_0|$. In particular, choose the unitary $U = Q_{\max}$ to obtain

$$\begin{aligned} F(\gamma_0^A, \gamma_1^A) &= F(\tilde{\gamma_0}^A, \gamma_1^A) \\ &\geq \frac{1}{2|z|} \Big| \mathrm{Tr}\Big[(1 \otimes Q_{\max}) \Big(|z| \, |\tilde{\gamma_0}\rangle\langle\gamma_1|^{AB} + |z^*| \, |\gamma_1\rangle\langle\tilde{\gamma_0}|^{AB} \Big) \Big] \Big| \\ &= \frac{1}{2|z|} D_{\mathrm{tr}}(\gamma_+^B, \gamma_-^B). \end{aligned} \tag{5.44}$$

Rearranging this yields

$$D_{\mathrm{tr}}(\gamma_+^B, \gamma_-^B) \leq 2|z| F(\gamma_0^A, \gamma_1^A) = 2|\alpha\beta^*| F(\gamma_0^A, \gamma_1^A). \tag{5.45}$$

□

In essence, the unitary on Bob's side that characterises his trace distance in its variational formula connects it to the fidelity on Alice's side via Uhlmann's theorem, which demands that the fidelity between two states is the maximal overlap between any two purifications. Any two purifications are connected by a local unitary, so Uhlmann's theorem also maximises over a local unitary – just like the trace distance on Bob's side. Hence, it is natural that Bob's trace distance and Alice's fidelity are connected.

We now establish a trade-off between Alice's and Bob's error in discriminating product states under certain structural assumptions.

5.3.10. Theorem. *Consider an arbitrary ensemble of quantum states that contains four states of the form*

$$\begin{aligned} |\psi_0\rangle^{AB} &= |a_0\rangle^A \, |b_0\rangle^B \\ |\psi_1\rangle^{AB} &= |a_1\rangle^A \, |b_1\rangle^B \\ |\psi_2\rangle^{AB} &= |a_2\rangle^A \, (\alpha \, |b_0\rangle + \beta \, |b_1\rangle)^B \\ |\psi_3\rangle^{AB} &= |a_3\rangle^A \, (\alpha \, |b_0\rangle - \beta \, |b_1\rangle)^B, \end{aligned} \tag{5.46}$$

with $\langle a_2|a_3\rangle > 0$. Say Bob makes error $\varepsilon_B^{2,3} \geq 0$ in distinguishing $|\psi_2\rangle$ from $|\psi_3\rangle$. Then Alice makes error

$$\varepsilon_A^{0,1} \geq \frac{1}{2} - \frac{1}{2}\sqrt{1 - |\langle a_0|a_1\rangle|^2} - 2|\alpha\beta^*| \frac{\sqrt{\varepsilon_B^{2,3}(1 - \varepsilon_B^{2,3})}}{|\langle a_2|a_3\rangle|} \tag{5.47}$$

in distinguishing $|\psi_0\rangle$ from $|\psi_1\rangle$.

Proof:
For notational simplicity, we will denote a state ρ_{AB} in registers AB simply by AB. When receiving input $|\psi_k\rangle = |a_k\rangle|b_k\rangle$, Alice and Bob apply isometries mapping registers $A^k \mapsto A_L^k A_C^k$ and $B^k \mapsto B_L^k B_C^k$ on input state $|\psi_k\rangle$, where they, respectively, keep the L register locally and communicate the C register to the other party. After communication, Alice measures $A_L^k \otimes B_C^k$ and Bob measures $A_C^k \otimes B_L^k$. By the Holevo-Helström theorem, an error $\varepsilon_B^{2,3}$ means $D_{\mathrm{tr}}(A_C^2 \otimes B_L^2, A_C^3 \otimes B_L^3) = 1 - 2\varepsilon_B^{2,3}$. The Fuchs-van de Graaf inequality then yields

$$F(A_C^2 \otimes B_L^2, A_C^3 \otimes B_L^3) = F(A_C^2, A_C^3) F(B_L^2, B_L^3) \leq 2\sqrt{\varepsilon_B^{2,3}(1-\varepsilon_B^{2,3})}. \tag{5.48}$$

Using $F(A_C^2, A_C^3) \geq F(|a_2\rangle, |a_3\rangle) = |\langle a_2|a_3\rangle|$ we get

$$F(B_L^2, B_L^3) \leq \frac{2\sqrt{\varepsilon_B^{2,3}(1-\varepsilon_B^{2,3})}}{|\langle a_2|a_3\rangle|}. \tag{5.49}$$

Applying Lemma 5.3.9 we obtain

$$D_{\mathrm{tr}}(B_C^0, B_C^1) \leq 4|\alpha\beta^*| \frac{\sqrt{\varepsilon_B^{2,3}(1-\varepsilon_B^{2,3})}}{|\langle a_2|a_3\rangle|}. \tag{5.50}$$

Note that $D_{\mathrm{tr}}(B_C^0, B_C^1) = D_{\mathrm{tr}}(A_L^0 \otimes B_C^0, A_L^0 \otimes B_C^1)$. If we can somehow convert $A_L^0 \otimes B_C^1$ into $A_L^1 \otimes B_C^1$ we can argue about Alice's error $\varepsilon_A^{0,1}$. We can achieve this by the following trick.

Write $|a_0\rangle = \gamma|a_1\rangle + \delta|a_1^\perp\rangle$. Then, after applying Alice's isometry V_A to $|a_0\rangle\langle a_0| = |\gamma|^2|a_1\rangle\langle a_1| + \gamma\delta^*|a_1\rangle\langle a_1^\perp| + \gamma^*\delta|a_1^\perp\rangle\langle a_1| + |\delta|^2|a_1^\perp\rangle\langle a_1^\perp|$, we see

$$A_L^0 = \mathrm{Tr}_{A_C^0}\left[V_A|a_0\rangle\langle a_0|V_A^\dagger\right] = |\gamma|^2 A_L^1 + \gamma\delta^* A_L^{1,1^\perp} + \gamma^*\delta A_L^{1^\perp,1} + |\delta|^2 A_L^{1^\perp}. \tag{5.51}$$

Let $R^1 = \gamma\delta^* A_L^{1,1^\perp} + \gamma^*\delta A_L^{1^\perp,1} + |\delta|^2 A_L^{1^\perp}$ and let us now add the term

$$\frac{1}{2}\left\| -\left(1-|\gamma|^2\right) A_L^1 \otimes B_C^1 + R^1 \otimes B_C^1 \right\|_1 \tag{5.52}$$

to both sides of (5.50). Then, using the triangle inequality, we get on the left-hand side

$$\begin{aligned} &D_{\mathrm{tr}}(A_L^0 \otimes B_C^0, A_L^0 \otimes B_C^1) + \frac{1}{2}\left\| -\left(1-|\gamma|^2\right) A_L^1 \otimes B_C^1 + R^1 \otimes B_C^1 \right\|_1 \\ &\geq \frac{1}{2}\left\| A_L^0 \otimes B_C^0 - A_L^0 \otimes B_C^1 - \left(1-|\gamma|^2\right) A_L^1 \otimes B_C^1 + R^1 \otimes B_C^1 \right\|_1. \end{aligned} \tag{5.53}$$

We plug in (5.51) for A_L^0 in $A_L^0 \otimes B_C^1$ and observe that many terms inside the norm cancel, as desired. We end up with

$$\begin{aligned} &D_{\mathrm{tr}}(A_L^0 \otimes B_C^0, A_L^0 \otimes B_C^1) + \frac{1}{2}\left\| -\left(1-|\gamma|^2\right) A_L^1 \otimes B_C^1 + R^1 \otimes B_C^1 \right\|_1 \\ &\qquad \geq D_{\mathrm{tr}}(A_L^0 \otimes B_C^0, A_L^1 \otimes B_C^1) = 1 - 2\varepsilon_A^{0,1}. \end{aligned} \tag{5.54}$$

For the right-hand side of (5.50) we can use the monotonicity and invariance under isometries of $\|\cdot\|_1$, to explicitly calculate the term (5.52) we added by undoing the partial trace and isometry. This yields, after a couple lines of calculation,

$$\begin{aligned}\frac{1}{2}\|-(1-|\gamma|^2)A_L^1\otimes B_C^1+R^1\otimes B_C^1\|_1\\ \leq \frac{1}{2}\||a_0\rangle\langle a_0|-|a_1\rangle\langle a_1|\|_1=\sqrt{1-|\langle a_0|a_1\rangle|^2}.\end{aligned}\tag{5.55}$$

Putting this into (5.54) and using (5.50) we arrive at

$$4|\alpha\beta^*|\frac{\sqrt{\varepsilon_B^{2,3}(1-\varepsilon_B^{2,3})}}{|\langle a_2|a_3\rangle|}+\sqrt{1-|\langle a_0|a_1\rangle|^2}\geq 1-2\varepsilon_A^{0,1}.\tag{5.56}$$

Rearranging the terms yields (5.47). □

5.3.11. Remark. The above theorem quantifies the trade-off between Alice's and Bob's errors on some of the states (which translates to an overall error over the whole ensemble). One can also assume a uniform error, i.e. assuming that Alice and Bob make some error $\varepsilon\geq 0$ on any state of the subensemble. Then a similar proof leads to (5.47) as a necessary condition on ε, reading

$$2\varepsilon+4|\alpha\beta^*|\frac{\sqrt{\varepsilon(1-\varepsilon)}}{|\langle a_2|a_3\rangle|}+\sqrt{1-|\langle a_0|a_1\rangle|^2}\geq 1.\tag{5.57}$$

Depending on the input ensemble, this condition might necessitate $\varepsilon>0$. More details can be found in [GALC23].

Theorem 5.3.10, or its uniform version (5.57), allow us to give an error lower bound for LOSQC state discrimination ensembles of the form $\{|\mathcal{K}|^{-1},|\psi_k\rangle^{AB}=|a_k\rangle^A|b_k\rangle^B\}_k$. Note that the derived ε only uses a subensemble of 4 states, but it can straightforwardly be converted to an error over the whole ensemble.

5.3.12. Example. For the BB84 ensemble

$$\begin{aligned}|\psi_0\rangle&=|0\rangle|0\rangle & |\psi_2\rangle&=|1\rangle|+\rangle\\ |\psi_1\rangle&=|0\rangle|1\rangle & |\psi_3\rangle&=|1\rangle|-\rangle,\end{aligned}\tag{5.58}$$

we obtain

$$2\varepsilon+2\sqrt{\varepsilon(1-\varepsilon)}\geq 1,\tag{5.59}$$

which implies $\varepsilon\geq\frac{1}{2}-\frac{1}{2\sqrt{2}}$. Hence, we recover the optimal error bound that can also be achieved [TFKW13].

5.3.13. Example. For the Domino states [BDF+99]

$$\begin{aligned}
|\psi_0\rangle &= |1\rangle\,|1\rangle & |\psi_5\rangle &= |1+2\rangle\,|0\rangle \\
|\psi_1\rangle &= |0\rangle\,|0+1\rangle & |\psi_6\rangle &= |1-2\rangle\,|0\rangle \\
|\psi_2\rangle &= |0\rangle\,|0-1\rangle & |\psi_7\rangle &= |0+1\rangle\,|2\rangle \\
|\psi_3\rangle &= |2\rangle\,|1+2\rangle & |\psi_8\rangle &= |0-1\rangle\,|2\rangle\,, \\
|\psi_4\rangle &= |2\rangle\,|1-2\rangle
\end{aligned}$$

where $|i \pm j\rangle = \frac{1}{\sqrt{2}}(|i\rangle \pm |j\rangle)$, we can use the subensemble $\{|\psi_1\rangle, |\psi_2\rangle, |\psi_0\rangle, |\psi_5\rangle\}$ as the 4 states with the required structure to obtain

$$2\varepsilon + 2\sqrt{2}\sqrt{\varepsilon(1-\varepsilon)} \geq 1, \tag{5.60}$$

which implies $\varepsilon \geq \frac{1}{2} - \frac{1}{\sqrt{6}} \simeq 0.09175$.

5.3.14. Example. For the unextendible product basis called Shifts [BDM+99], giving two registers to Alice and one to Bob, yields the bipartite ensemble

$$\begin{aligned}
|\psi_0\rangle &= |00\rangle\,|0\rangle & |\psi_2\rangle &= |-1\rangle\,|+\rangle \\
|\psi_1\rangle &= |+-\rangle\,|1\rangle & |\psi_3\rangle &= |1+\rangle\,|-\rangle\,.
\end{aligned}$$

We obtain

$$2\varepsilon + 4\sqrt{\varepsilon(1-\varepsilon)} + \frac{\sqrt{3}}{2} \geq 1, \tag{5.61}$$

which implies $\varepsilon \geq \frac{1}{2} - \frac{\sqrt{3}+2\sqrt{17}}{20} \simeq 0.00108$.

Chapter 6

Making Quantum Position Verification Protocols Loss Tolerant

Chapter summary. As noted before, signal loss poses a significant threat to the security of quantum cryptography when the chosen protocol lacks loss-tolerance, and for QPV protocols, even small loss rates can compromise security. The goal is thus to find protocols that remain secure at practically achievable loss rates. In this chapter, we modify the usual structure of QPV 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 based on BB84 states ($\mathrm{QPV}^{f}_{\mathrm{BB84}}$). This adjustment, which involves photon presence detection, a small time delay at the prover, and a commitment to play before proceeding, reduces the relevant protocol 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 feasible. We also examine possible 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. Finally, we discuss experimental aspects and give parameter estimates.

This chapter is based on the following paper:

[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*, 2023. arXiv:2312.12614. *Contributed talk at QIP 2024. Contributed talk at QCRYPT 2024.*

6.1 Introduction

In this chapter, we focus on the design of 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 simultaneously, the quantum information shall arrive slightly before the classical information. The prover confirms that he received 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 $\mathsf{c\text{-}P}$.

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 $\mathrm{QPV}^{f}_{\mathrm{BB84}}$). This implies that the protocol is *state-independent*, in the sense that the attackers can replace the input quantum state with any other quantum state (they can do this if the quantum input travels slowly, for example). Then our main result states that for every such QPV protocol P, its committing version $\mathsf{c\text{-}P}$ 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 responding), we informally state our main result, Theorem 6.3.9, as follows:

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

$$\mathbb{P}[\text{attack } \mathsf{c\text{-}P}_{\eta_V,\eta_P}] \leq \mathbb{P}[\text{attack } \mathsf{P}_{\eta_P}] + (1-2\tilde{c})8\sqrt{\varepsilon} + 2\tilde{c}, \tag{6.1}$$

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 $\mathsf{c\text{-}P}_{\eta_V,\eta_P}$ and only the much smaller loss in the prover laboratory, $1-\eta_P$, matters. And for sufficiently high values of η_P we often have security guarantees, e.g. for $\mathrm{QPV}^{f}_{\mathrm{BB84}}$ [BCS22, ES23]. In theory, for an ideal prover, $\mathsf{c\text{-}P}_{\eta_V,\eta_P}$ 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

$$\mathbb{P}[\text{attack } \mathsf{c\text{-}P}_{\eta_V,\eta_P}] = \mathbb{P}[\text{attack } \mathsf{P}_{\eta_P}], \tag{6.2}$$

as the other direction $\mathbb{P}[\text{attack } \mathsf{P}_{\eta_P}] \leq \mathbb{P}[\text{attack } \mathsf{c\text{-}P}_{\eta_V,\eta_P}]$ is simple to see[1]. The above theorem allows for $\varepsilon \neq 0 \neq \tilde{c}$ in attack strategies to make our argument

[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 $\mathsf{c\text{-}P}_{\eta_V,\eta_P}$.

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.

In [ABB+23] we further prove that the success probability for attacking our protocol decays exponentially with the number of (sequentially repeated) rounds that are run, even if attackers are allowed to use adaptive strategies.

Applying our results to $\mathrm{QPV}^{f}_{\mathrm{BB84}}$, 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).

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 linear-optical 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 (for example, by a polarisation measurement in basis $f(x, y)$). We note that for the committing version of $\mathrm{QPV}^{f}_{\mathrm{BB84}}$, $\mathsf{c}\text{-}\mathrm{QPV}^{f}_{\mathrm{BB84}}$, no active feed-forward for the teleportation corrections is required, as they predictably alter the subsequent 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 shall 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 seems possible already and GHz rate seems 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 this chapter. We argue that with state-of-the-art equipment our protocol can remain within its secure regime, even in practice.[2]

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: attackers with bounded pre-shared entanglement, photon loss (for large distances), and slow quantum information.

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

6.2 QPV with a commitment

One of the major issues in practical quantum cryptography is the transmission loss between the interacting parties. 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, ABSV21] 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 laboratory. We define its *committing* version (or protocol with *commitment*), denoted by $\mathsf{c\text{-}P}_{\eta_V,\eta_P}$, 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 the prover, he is required to commit to play ($c = 1$) or not to play ($c = 0$) the round. Only the $c = 1$ rounds are later analysed 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 fulfils 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 $\mathsf{c\text{-}QPV}^f_{\mathrm{BB84}}$ the protocol with commitment.

6.2.1 The protocol $\mathsf{c\text{-}QPV}^f_{\mathrm{BB84}}$

The *committing* version of $\mathrm{QPV}^f_{\mathrm{BB84}}$ is described as follows. We describe the protocol in its purified form, whereas in practice it might be simpler to implement its prepare-and-measure version, using BB84 states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ as inputs.

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

1. The verifiers draw two n-bit strings $x, y \in \{0,1\}^n$ uniformly at random. $\mathsf{V_A}$ prepares the EPR pair $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ and sends one qubit Q and x to P and $\mathsf{V_B}$ sends y 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 $f(x, y)$[3] as soon as x, y arrive and broadcasts his outcome a to $\mathsf{V_A}$ and $\mathsf{V_B}$. If the photon is lost in the time δ or during the measurement, he sends 'signal loss'.

4. The verifiers collect (c, a) and $\mathsf{V_A}$ 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 'signal loss' if they both receive 'signal loss' on time. If any of the answers do not arrive on time or are different the verifiers abort.

The sequentially repeated protocol, denoted by $\mathsf{c\text{-}P}^{\mathrm{seq}}_{\eta_V,\eta_P}$, works as follows:

1. The verifiers collect a certain number of rounds r of $\mathsf{c\text{-}P}_{\eta_V,\eta_P}$ that come back with commitments $(c_A, c_B) \neq (0, 0)$. Rounds with $(c_A, c_B) = (0, 0)$ are discarded.

2. If in any round the verifiers see different commits, i.e. $(c_A, c_B) = (0, 1)$ or $(1, 0)$, or different protocol answers, they abort immediately.

3. Otherwise, after reaching the required number of $(c_A, c_B) \neq (0, 0)$ rounds, they do the security analysis as described in Section 6.4 and accept or reject, depending on the score Γ_r of the sample.

6.3 Security of QPV with commitment

Attack model

As discussed in Chapter 3, the most general attack on a 1-dimensional QPV protocol is to place an adversary, who we will call Alice, between $\mathsf{V_A}$ and the position where the prover should be and another adversary, who we will call Bob, between the supposed prover location and $\mathsf{V_B}$. 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 (possibly entangled) quantum state σ_{AB}. Then Alice (A) and Bob (B) intercept the information sent from their closest verifier, make a copy, and broadcast the classical information to their fellow attacker. They also 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.

[3] For more basis choices, the range of f would become $\{0, 1, \ldots, m-1\}$.

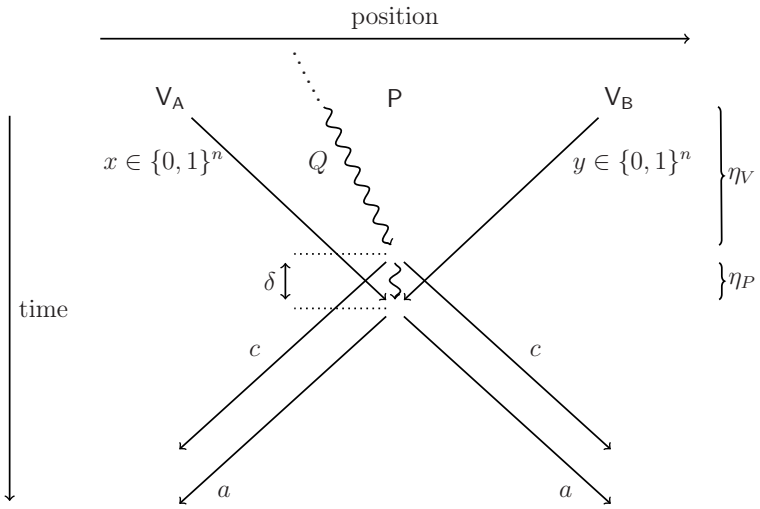


Figure 6.1: Schematic representation of the $\mathsf{c\text{-}QPV}^{f}_{\mathrm{BB84}}$ protocol. Undulated lines represent quantum information, straight lines represent classical information. The slowly traveling quantum system Q originated from $\mathsf{V_A}$ in the past. The novel aspects are the 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.

Denote by $\omega^{(x,y)}$ the quantum state after communication, to which attackers apply the POVM. Fix a partition into systems $AA_{\mathrm{com}}BB_{\mathrm{com}}$, where 'com' denotes the subsystems that are communicated. We can write the attackers two-outcome POVMs as $\{\Pi^{A,(x,y)}_{AB_{\mathrm{com}}}, \mathbb{1} - \Pi^{A,(x,y)}_{AB_{\mathrm{com}}}\}$ and $\{\Pi^{B,(x,y)}_{A_{\mathrm{com}}B}, \mathbb{1} - \Pi^{B,(x,y)}_{A_{\mathrm{com}}B}\}$ 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

$$\mathbb{P}[\text{attack } \mathsf{P}_{\eta_V,\eta_P}] = \frac{1}{2^{2n}} \sum_{x,y} \mathrm{Tr}\Big[\Big(\Pi^{A,(x,y)}_{AB_{\mathrm{com}}} \otimes \Pi^{B,(x,y)}_{BA_{\mathrm{com}}}\Big)\omega^{(x,y)}_{AA_{\mathrm{com}}BB_{\mathrm{com}}}\Big]. \tag{6.3}$$

Our main result will hold for a class of QPV protocols that have the following property, which we call *state-independent*.

6.3.1. Definition. (State-independent protocol). We say that a QPV protocol P is *state-independent* if the protocol remains secure independently of the state σ_{AB} that the attackers pre-share at the start of the protocol [4].

[4] As long as this state does not allow for a perfect attack, for example due to sufficiently

In a general attack on a c-QPV protocol, Alice and Bob act as follows:

1. The attackers prepare a joint (possibly entangled) quantum state σ_{AB}.

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_{AB} 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_{AB} to determine the commitments c_A and c_B. We will write $\mathcal{I}^{xy}_1 = \mathcal{I}^A_{1|x} \otimes \mathcal{I}^B_{1|y}$. To proceed with the protocol, the attackers will use the state post-selected on commitments $c_A = 1$ and $c_B = 1$, denoted by $\tilde{\mathcal{I}}^{xy}_1(\rho) = \mathcal{I}^{xy}_1(\rho)/\operatorname{Tr}[\mathcal{I}^{xy}_1(\rho)]$. Alice can send a share of her state to Bob and vice versa.

4. Upon receiving the information sent by the other party, each attacker locally applies a POVM depending on (x, y) to obtain classical answers which will be sent to $\mathsf{V_A}$ and $\mathsf{V_B}$, 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 6.2. Then the probability that the attackers answer the correct values to the verifiers is given by

$$\mathbb{P}[\text{attack c-P}_{\eta_V,\eta_P}] = \frac{1}{2^{2n}} \sum_{x,y} \operatorname{Tr}\left[\left(\Pi^{A,(x,y)}_{AB_{\text{com}}} \otimes \Pi^{B,(x,y)}_{BA_{\text{com}}}\right)\omega^{\mathcal{I}_1,(x,y)}_{AA_{\text{com}}BB_{\text{com}}}\right]. \tag{6.4}$$

6.3.1 Security proof

The intuition

We move on to prove the security of c-QPV. The idea is to reduce the security of a protocol with commitment $\text{c-P}_{\eta_V,\eta_P}$ 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.

large pre-shared entanglement, of course. In the regime where security can be shown, it is independent of the adversarial input state. For such protocols no property other than the entanglement or dimension of the entangled resource state is relevant for attacks. $\text{QPV}^f_{\text{BB84}}$ is a state-independent protocol, since it remains secure for any σ_{AB} whose dimension is linearly bounded (in n) [BCS22].

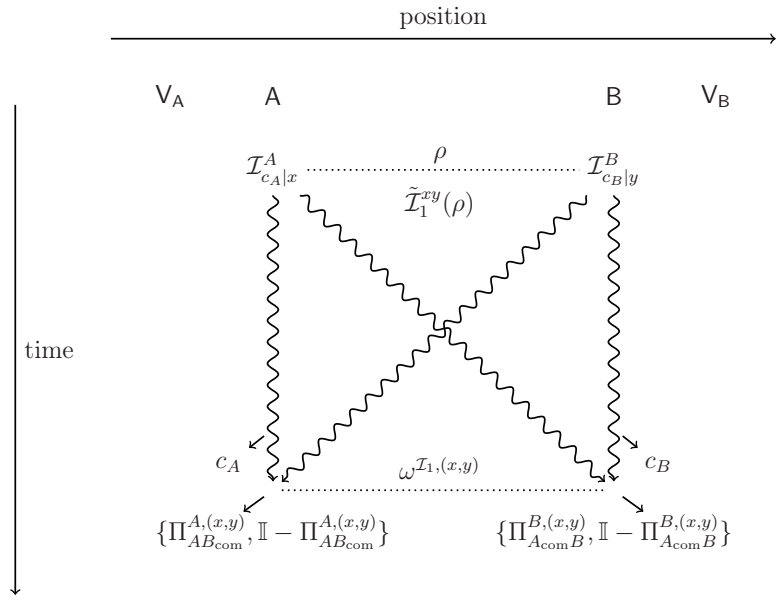


Figure 6.2: Schematic representation of a general attack on a c-QPV protocol, where straight lines represent classical information, and undulated lines represent quantum information, including x and y.

Ideally, both attackers' commitment bits are equal, i.e. $c_A = c_B = c$. Without loss of generality, as Alice and Bob act on separate registers, we may assume that Alice applies her quantum instrument $\{\mathcal{I}^A_{c_A|x}\}_{c_A\in\{0,1\}}$ first. But then her commitment c_A completely fixes Bob's c_B, which he obtains by applying his instrument $\{\mathcal{I}^B_{c_B|y}\}_{c_B\in\{0,1\}}$, for *any* y. Hence, invoking the gentle measurement lemma together with the fact that any quantum instrument can be decomposed into a measurement followed by a quantum channel [Hay16, Lemma 7.2], Bob's measurement (from his instrument) cannot disturb the state after Alice applied her instrument. This means that the post-commitment state is independent of his input y. By the same argument, assuming that Bob applies his instrument first, the post-commitment state is independent of Alice's input x. Both assertions hold simultaneously, thus the post-commitment state is independent of the classical input information (x, y). Note that then, after the commitment, the attackers find themselves in the same situation as for attacking the underlying protocol $\text{QPV}^f_{\text{BB84}}$, since from that moment on they can apply local quantum channels (originating from the quantum instrument decomposition) to the state they hold and make use of one round of simultaneous communication, followed by local measurements producing their final answer – indeed exactly the same setting as

attacking the underlying protocol without a commitment step. We needed to use quantum instruments in the first step, because the extra commitment step allows Alice and Bob to post-select their states depending on the commitment and x at Alice and y at Bob, respectively.

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. We allow them to commit differently with small probability ε, and do not restrict them at all on a small fraction $\tilde{c}$ of all inputs (x, y). Intuitively, if ε is very small relative to the number of rounds played, with high probability the verifiers will not see a round with different commitments. Likewise, if attackers choose to play more risky on the fraction $\tilde{c}$ of inputs (x, y), and $\tilde{c}$ is small, with high probability the verifiers won't see that behaviour. However, in principle, such a relaxation could help the attackers compromise security, so we need to deal with it. By applying a robust version of our gentle measurement argument and carefully keeping track of ε and $\tilde{c}$ we prove that only a linear overhead in terms of $\sqrt{\varepsilon}, \tilde{c}$ is added to the success probability of attackers. We demonstrate that, by running more protocol rounds, we can build confidence that both ε and $\tilde{c}$ are small. Intuitively, if we run many many rounds, but never see different commitments, then with very high probability the ε and $\tilde{c}$ of the attack strategy must be very small. We can further replace $\varepsilon, \tilde{c}$ by a single security parameter k. The verifiers are in control of the overhead by demanding more rounds.

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 6.3.3 does.

The tools

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.

6.3.2. 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*

$$\rho' = \frac{\sqrt{M}\rho\sqrt{M}}{\mathrm{Tr}[M\rho]} \tag{6.5}$$

of measuring M fulfills

$$||\rho - \rho'||_1 \leq 2\sqrt{\varepsilon}. \tag{6.6}$$

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 for convenience.

6.3.3. 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 $\mathcal{E}_i$ such that*

$$\mathcal{I}_i(\rho) = \mathcal{E}_i\Big(\sqrt{M_i}\rho\sqrt{M_i}\Big). \tag{6.7}$$

Proof:
Let $\{K_j\}_j$ be a Kraus decomposition of $\mathcal{I}_i$, whose existence is guaranteed by Lemma 2.1.10. Since

$$\mathrm{Tr}[\mathcal{I}_i(\rho)] = \mathrm{Tr}\left[\sum_j K_j\rho K_j^\dagger\right] = \mathrm{Tr}\left[\rho\sum_j K_j^\dagger K_j\right] = \mathrm{Tr}[\rho M_i], \tag{6.8}$$

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

$$\sum_j\Big(\sqrt{M_i}\Big)^- K_j^\dagger K_j\Big(\sqrt{M_i}\Big)^- = \Big(\sqrt{M_i}\Big)^- M_i\Big(\sqrt{M_i}\Big)^- = P^\dagger P = P. \tag{6.9}$$

Hence, if we add $\mathbb{1} - P$ on both sides, we obtain a full Kraus decomposition $\big\{K_j(\sqrt{M_i})^-, \mathbb{1} - P\big\}_j$ of a map, call it $\mathcal{E}_i$, that adds up to the identity. Thus, by Lemma 2.1.10, $\mathcal{E}_i$ is completely positive and trace preserving, i.e. a quantum channel. Finally, we see that

$$\begin{aligned}\mathcal{E}_i\Big(\sqrt{M_i}\rho\sqrt{M_i}\Big) &= (\mathbb{1}-P)\sqrt{M_i}\rho\sqrt{M_i}(\mathbb{1}-P)\\ &\quad+\sum_j K_j(\sqrt{M_i})^-\sqrt{M_i}\rho\sqrt{M_i}(\sqrt{M_i})^- K_j^\dagger\\ &= \sum_j K_j\rho K_j^\dagger = \mathcal{I}_i(\rho),\end{aligned} \tag{6.10}$$

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 $K_jP = K_j$. This follows via $M_i = \sum_j K_j^\dagger K_j$, implying 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 $K_jP = K_j$. □

Combining the Stinespring dilation with Lemma 6.3.3 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.

6.3.4. 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*

$$\mathcal{I}_i(\rho) = \mathrm{Tr}_E\Big[U_i\Big(\sqrt{M_i}\rho\sqrt{M_i} \otimes |0\rangle\langle 0|_E\Big)U_i^\dagger\Big] \tag{6.11}$$

for all $\rho \in \mathrm{D}(\mathcal{H})$.

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 (6.11) is the unitary corresponding to a Stinespring dilation of the channel $\mathcal{E}_i$ appearing in Lemma 6.3.3. 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 $\{M^x_A, \mathbb{1} - M^x_A\}$ and $\{M^y_B, \mathbb{1} - M^y_B\}$, respectively. Here, the POVM elements M^x_A and M^y_B 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

$$\rho^{xy} := \frac{\left(\sqrt{M^x_A} \otimes \sqrt{M^y_B}\right)\rho\left(\sqrt{M^x_A} \otimes \sqrt{M^y_B}\right)}{\mathrm{Tr}[(M^x_A \otimes M^y_B)\rho]}. \tag{6.12}$$

The observation is now that no two post-commitment states can differ too much from each other by Lemma 6.3.2. 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 input pairs (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.

6.3.5. LEMMA. *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,*

$$\|\rho^{xy} - \rho^{x'y'}\|_1 \leq 8\sqrt{\varepsilon}. \tag{6.13}$$

Proof:
Consider the attackers Alice and Bob performing the most general attack described above and the POVMs $\{M^x_A, \mathbb{1} - M^x_A\}$ and $\{M^y_B, \mathbb{1} - M^y_B\}$ as defined before. We write

$$\rho^{x,(\cdot)} = \frac{(\sqrt{M^x_A} \otimes \mathbb{1}_B)\,\rho\,(\sqrt{M^x_A} \otimes \mathbb{1}_B)}{\mathrm{Tr}[(M^x_A \otimes \mathbb{1}_B)\rho]}, \quad \rho^{(\cdot),y} = \frac{(\mathbb{1}_A \otimes \sqrt{M^y_B})\,\rho\,(\mathbb{1}_A \otimes \sqrt{M^y_B})}{\mathrm{Tr}[(\mathbb{1}_A \otimes M^y_B)\rho]} \tag{6.14}$$

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

$$\mathrm{Tr}\big[((\mathbb{1}_A \otimes (\mathbb{1} - M^y_B))\rho^{x,(\cdot)}\big] \leq \varepsilon, \qquad \mathrm{Tr}\big[((\mathbb{1} - M^x_A) \otimes \mathbb{1}_B)\rho^{(\cdot),y}\big] \leq \varepsilon. \tag{6.15}$$

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

$$\mathrm{Tr}\Big[(\mathbb{1}_A \otimes (\mathbb{1} - M_B^y))\rho^{x',(\cdot)}\Big] \leq \varepsilon, \qquad \mathrm{Tr}\Big[\Big((\mathbb{1} - M_A^{x'}) \otimes \mathbb{1}_B\Big)\rho^{(\cdot),y}\Big] \leq \varepsilon, \tag{6.16}$$

$$\mathrm{Tr}\Big[\Big(\mathbb{1}_A \otimes (\mathbb{1} - M_B^{y'})\Big)\rho^{x',(\cdot)}\Big] \leq \varepsilon, \qquad \mathrm{Tr}\Big[\Big((\mathbb{1} - M_A^{x'}) \otimes \mathbb{1}_B\Big)\rho^{(\cdot),y'}\Big] \leq \varepsilon. \tag{6.17}$$

Therefore, by the gentle measurement lemma, Lemma 6.3.2, we get the following inequalities:

$$\begin{aligned} &\|\rho^{(\cdot),y} - \rho^{xy}\|_1 \leq 2\sqrt{\varepsilon}, \quad \|\rho^{(\cdot),y} - \rho^{x'y}\|_1 \leq 2\sqrt{\varepsilon}, \\ &\|\rho^{x',(\cdot)} - \rho^{x'y}\|_1 \leq 2\sqrt{\varepsilon}, \quad \|\rho^{x',(\cdot)} - \rho^{x'y'}\|_1 \leq 2\sqrt{\varepsilon}, \end{aligned} \tag{6.18}$$

which implies the following

$$\begin{aligned} \|\rho^{x'y'} - \rho^{xy}\|_1 &= \|\rho^{x'y'} - \rho^{x',(\cdot)} + \rho^{x',(\cdot)} - \rho^{x'y} + \rho^{x'y} - \rho^{(\cdot),y} + \rho^{(\cdot),y} - \rho^{xy}\|_1 \\ &\leq \|\rho^{x'y'} - \rho^{x',(\cdot)}\|_1 + \|\rho^{x',(\cdot)} - \rho^{x'y}\|_1 + \|\rho^{x'y} - \rho^{(\cdot),y}\|_1 + \|\rho^{(\cdot),y} - \rho^{xy}\|_1 \\ &\leq 8\sqrt{\varepsilon}, \end{aligned} \tag{6.19}$$

where we used the triangle inequality and (6.18). □

Note that if the probability of answering different commits on the inputs (x, y') instead of (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 6.3.5, we see that all post-commit states are equal, and thus independent of (x, y), so the initial intuition is true. 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 an underlying state-independent protocol (cf. Definition 6.3.1). Thus, the probability of successfully attacking the protocol on rounds in which the attackers commit is equal to the original protocol. This is summarised in the following corollary:

6.3.6. 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* $\mathsf{c\text{-}P}$ *becomes fully loss tolerant against transmission loss. That is,*

$$\mathbb{P}[\text{attack } \mathsf{c\text{-}P}_{\eta_V,\eta_P}] = \mathbb{P}[\text{attack } \mathsf{P}_{\eta_P}]. \tag{6.20}$$

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

However, one can argue that 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 6.3.5 can be pictured as a connection problem on 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 for those x, y, 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) we have $\|\rho^{xy} - \rho^{x'y'}\|_1 \leq 8\sqrt{\varepsilon}$, if there is an edge in the graph that connects either x', y or x, y'. This is represented in Figure 6.3.

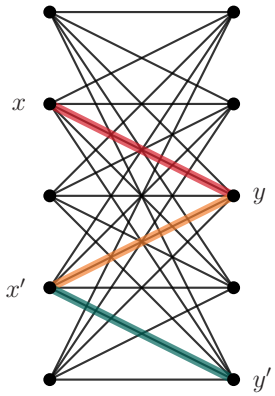


Figure 6.3: Graphical representation of converting the pair (x, y) (red) to (x', y') (green) via (x', y) (orange). Vertices on the left correspond to possible inputs x, on the right to possible inputs y. A connection between two strings means that the probability of committing differently on this input is smaller than ε.

The statement of Lemma 6.3.5 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 enforce to be true for every pair of strings. The verifiers can only check for the rounds

they play whether the commitments are equal, but since 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.

In Figure 6.3, 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 then. 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 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 6.3.5).

6.3.7. Lemma. *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

$$\begin{aligned}\Sigma_\varepsilon &:= \{x, y \mid \mathrm{Tr}\big[(\mathbb{1} \otimes (\mathbb{1} - M_B^y))\rho^{x,(.)}\big] \leq \varepsilon \wedge \mathrm{Tr}\big[(\mathbb{1} - M_A^x) \otimes \mathbb{1})\rho^{(.),y}\big] \leq \varepsilon\} \\ &= \{x, y \mid \mathbb{P}[c_B = 0 \mid c_A = 1, x_A, y_B] \leq \varepsilon \wedge \mathbb{P}[c_A = 0 \mid c_B = 1, x_A, y_B] \leq \varepsilon\},\end{aligned} \tag{6.21}$$

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

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

$$\|\rho^{x_\star y_\star} - \rho^{x' y'}\|_1 \leq 8\sqrt{\varepsilon}. \tag{6.22}$$

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 6.3.7 there is a pair $(x_\star, y_\star)$ from which there are at least $(1-2\tilde{c})2^{2n}$ edges connected in two steps. Applying Lemma 6.3.5 gives the desired statement. □

The proof

We can now patch things together for a full security proof of QPV with commitment. The addition of the commitment round opens up a new possible attack. Attackers can now try to apply some transformation on their state and answer 'no commit' ($c = 0$) when it 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 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 6.3.8.

Then we can bound the probability of success of the protocol with commitment, because the post-commit state can be replaced by a 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 6.3.1 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 $\mathrm{QPV}^f_{\mathrm{BB84}}$.

6.3.9. 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, then, on the rounds the attackers play, the following bound on the probability of attackers answering correctly to* $\mathsf{c\text{-}P}$ *holds:*

$$\mathbb{P}[\text{attack } \mathsf{c\text{-}P}_{\eta_V, \eta_P}] \leq \mathbb{P}[\text{attack } \mathsf{P}_{\eta_P}] + (1-2\tilde{c})8\sqrt{\varepsilon} + 2\tilde{c}. \tag{6.23}$$

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 perform to generate these bits

is a quantum instrument. By Lemma 6.3.3 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 at Alice and y at Bob. We want to upper bound the attack 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 (renormalised) post-instrument state the attackers hold if they both commit to playing:

$$\begin{aligned}\tilde{\mathcal{I}}_1^{xy}(\rho) &= \frac{\mathcal{I}_1^{xy}(\rho)}{\mathrm{Tr}[\mathcal{I}_1^{xy}(\rho)]} = \frac{\mathcal{E}_1^{xy}\Big(\Big(\sqrt{M_A^x}\otimes\sqrt{M_B^y}\Big)\rho\Big(\sqrt{M_B^y}\otimes\sqrt{M_A^x}\Big)\Big)}{\mathrm{Tr}[(M_A^x\otimes M_B^y)\rho]} \\ &= \mathcal{E}_1^{xy}(\rho^{xy}) \\ &= \mathrm{Tr}_E\big[U^{xy}(\rho^{xy}\otimes|0\rangle\langle 0|_E)U^{xy\dagger}\big]. \end{aligned} \tag{6.24}$$

By assumption we have $|\Sigma_\varepsilon^c| \leq \tilde{c}2^{2n}$, so we can invoke Lemma 6.3.8, which says that there must be a reference pair $(x_\star, y_\star) \in \Sigma_\varepsilon$ such that there are at least $(1-2\tilde{c})2^{2n}$ other pairs $(x,y) \in \Sigma_\varepsilon$ fulfilling

$$\|\rho^{x_\star y_\star} - \rho^{xy}\|_1 \leq 8\sqrt{\varepsilon}. \tag{6.25}$$

Combining both results, we get from the data processing inequality for the 1-norm that

$$\begin{aligned}\|\mathcal{E}_1^{xy}(\rho^{xy}) - \mathcal{E}_1^{xy}(\rho^{x_\star y_\star})\|_1 &\leq \|\rho^{xy} - \rho^{x_\star y_\star}\|_1 \\ &\leq 8\sqrt{\varepsilon}. \end{aligned} \tag{6.26}$$

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

$$\Lambda_\varepsilon^{(x,y)} = \Big\{(x',y') \in \Sigma_\varepsilon : \|\rho^{xy} - \rho^{x'y'}\|_1 \leq 8\sqrt{\varepsilon}\Big\}, \tag{6.27}$$

and write $\Lambda_\varepsilon \coloneqq \Lambda_\varepsilon^{(x_\star,y_\star)}$ 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 $AA_{\mathrm{com}}BB_{\mathrm{com}}$, where 'com' denotes the subsystems that are communicated. We can write the attackers two-outcome POVMs as $\{\Pi_{AB_{\mathrm{com}}}^{A,(x,y)}, \mathbb{1}-\Pi_{AB_{\mathrm{com}}}^{A,(x,y)}\}$ and $\{\Pi_{A_{\mathrm{com}}B}^{B,(x,y)}, \mathbb{1}-\Pi_{A_{\mathrm{com}}B}^{B,(x,y)}\}$ respectively, where we 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 notational simplicity, denote the final operation of the attackers by $\Pi_{AB_{\mathrm{com}}}^{A,(x,y)} \otimes \Pi_{A_{\mathrm{com}}B}^{B,(x,y)} = \Pi^{xy}$. Then

$$
\begin{aligned}
\mathbb{P}[\text{attack } \mathsf{c\text{-}P}_{\eta_V,\eta_P}] &= \frac{1}{2^{2n}} \sum_{(x,y)} \operatorname{Tr}\left[\Pi^{xy} \tilde{\mathcal{I}}_1^{xy}(\rho)\right] \\
&= \frac{1}{2^{2n}} \sum_{(x,y)\in\Lambda_\varepsilon} \operatorname{Tr}[\Pi^{xy} \mathcal{E}_1^{xy}(\rho^{xy})] + \frac{1}{2^{2n}} \sum_{(x,y)\in\Lambda_\varepsilon^c} \operatorname{Tr}[\Pi^{xy} \mathcal{E}_1^{xy}(\rho^{xy})] \\
&\leq \frac{1}{2^{2n}} \sum_{(x,y)\in\Lambda_\varepsilon} \operatorname{Tr}[\Pi^{xy}(\mathcal{E}_1^{xy}(\rho^{xy}) - \mathcal{E}_1^{xy}(\rho^{x_\star y_\star}) + \mathcal{E}_1^{xy}(\rho^{x_\star y_\star}))] + \frac{|\Lambda_\varepsilon^c|}{2^{2n}} \\
&= \frac{1}{2^{2n}} \sum_{(x,y)\in\Lambda_\varepsilon} \operatorname{Tr}[\Pi^{xy}(\mathcal{E}_1^{xy}(\rho^{xy}) - \mathcal{E}_1^{xy}(\rho^{x_\star y_\star}))] + \frac{1}{2^{2n}} \sum_{(x,y)\in\Lambda_\varepsilon} \operatorname{Tr}[\Pi^{xy} \mathcal{E}_1^{xy}(\rho^{x_\star y_\star}))] + \frac{|\Lambda_\varepsilon^c|}{2^{2n}} \\
&\leq \frac{1}{2^{2n}} \sum_{(x,y)\in\Lambda_\varepsilon} \|\Pi^{xy}\|_\infty \|\mathcal{E}_1^{xy}(\rho^{xy}) - \mathcal{E}_1^{xy}(\rho^{x_\star y_\star})\|_1 + \frac{1}{2^{2n}} \sum_{(x,y)\in\Lambda_\varepsilon} \operatorname{Tr}[\Pi^{xy} \mathcal{E}_1^{xy}(\rho^{x_\star y_\star}))] + \frac{|\Lambda_\varepsilon^c|}{2^{2n}} \\
&\leq \frac{|\Lambda_\varepsilon|}{2^{2n}} 8\sqrt{\varepsilon} + \frac{|\Lambda_\varepsilon^c|}{2^{2n}} + \frac{1}{2^{2n}} \sum_{(x,y)\in\Lambda_\varepsilon} \operatorname{Tr}[\Pi^{xy} \mathcal{E}_1^{xy}(\rho^{x_\star y_\star}))] \\
&\leq \frac{|\Lambda_\varepsilon^c|}{2^{2n}} (1 - 8\sqrt{\varepsilon}) + 8\sqrt{\varepsilon} + \mathbb{P}[\text{attack } \mathsf{P}_{\eta_P}] \\
&\leq \mathbb{P}[\text{attack } \mathsf{P}_{\eta_P}] + (1 - 2\tilde{c}) 8\sqrt{\varepsilon} + 2\tilde{c}, \qquad (6.28)
\end{aligned}
$$

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

We can estimate ε and $\tilde{c}$ to show that, with increasing numbers of rounds, $\mathbb{P}[\text{attack } \mathsf{c\text{-}P}_{\eta_V,\eta_P}]$ becomes ever closer to $\mathbb{P}[\text{attack } \mathsf{P}_{\eta_P}]$. This should follow from getting better and better estimates of ε when verifiers keep seeing only equal commitments.

6.3.10. Remark. Theorem 6.3.9, applied to the ideal setting of $\varepsilon = 0 = \tilde{c}$ and $\eta_P = 1$, shows that state-independent protocols, in particular $\text{QPV}_{\text{BB84}}^f$, can be made *fully loss-tolerant* against transmission loss by adding a commitment step.

6.3.2 Parameter estimation

Non-adaptive strategies

However, as we have noted before, we cannot really set $\varepsilon = 0$, since a small ε might help the attackers, while remaining undetected 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 confident that the probability of one party not committing given that the other party commits is small. Hence, we want to estimate the conditional probabilities:

$$\mathbb{P}[c_A = 0 | c_B = 1] = \frac{1}{2^{2n}} \sum_{x,y} \mathbb{P}[c_A = 0 | c_B = 1, x_A, y_B], \tag{6.29}$$

$$\mathbb{P}[c_B = 0 | c_A = 1] = \frac{1}{2^{2n}} \sum_{x,y} \mathbb{P}[c_B = 0 | c_A = 1, x_A, y_B]. \tag{6.30}$$

These probabilities should be small. Suppose we want to upper bound the maximum conditional probability of the two in (6.29), (6.30) by some value $\alpha > 0$ of our choice by running more and more rounds and checking the sample for rounds with different commitments. In particular, that will mean $\varepsilon \leq \alpha$. Then we can do the following. We keep playing until we get r/α 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 the attack strategy is non-adaptive. If we detect different commit bits in one of these rounds, we immediately abort, because an honest prover would never send these. But if the probability of answering different commit bits would be greater than α, the probability of answering equal commit bits consistently would be smaller than $(1-\alpha)^{\frac{r}{\alpha}}$.

We will now lower bound the probability to detect attackers due to differing commits. Suppose the maximum of the two probabilities (6.29), (6.30) 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

$$\mathbb{P}[\text{detect attackers} \,|\, \text{commits} \neq (0,0)] = \mathbb{P}[\exists j \text{ with } C^j_{\text{diff}} \,|\, \forall i \; C^i_{\neq 0}]. \tag{6.31}$$

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

we can write

$$\begin{aligned}
\mathbb{P}[\text{detect attackers} \,|\, \text{commits} \neq (0,0)] &= 1 - \mathbb{P}[\forall i \; C^i_{\text{eq}} \,|\, \forall i \; C^i_{\neq 0}] \\
&= 1 - \prod_{i=1}^{r/\alpha} \mathbb{P}[C^i_{(1,1)} \,|\, C^i_{\neq 0}] = 1 - \prod_{i=1}^{r/\alpha} \big(1 - \mathbb{P}[C^i_{\text{diff}} \,|\, C^i_{\neq 0}]\big) \\
&\geq 1 - \prod_{i=1}^{r/\alpha} \big(1 - \max\{\mathbb{P}[c^i_B = 0 \,|\, c^i_A = 1], \mathbb{P}[c^i_A = 0 \,|\, c^i_B = 1]\}\big) \\
&\geq 1 - \prod_{i=1}^{r/\alpha} (1 - \alpha) = 1 - (1-\alpha)^{r/\alpha} \\
&\geq 1 - e^{-\alpha r/\alpha} = 1 - e^{-r}. \qquad (6.32)
\end{aligned}$$

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

$$\mathbb{P}[C^i_{\text{diff}} \,|\, c^i_A = 1] = \frac{\mathbb{P}[(c^i_A, c^i_B) = (1,0)]}{\mathbb{P}[(c^i_A, c^i_B) = (1,0)] + \mathbb{P}[(c^i_A, c^i_B) = (1,1)]}, \qquad (6.33)$$

$$\mathbb{P}[C^i_{\text{diff}} \,|\, C^i_{\neq 0}] = \frac{\mathbb{P}[(c^i_A, c^i_B) = (1,0)] + \mathbb{P}[(c^i_A, c^i_B) = (0,1)]}{1 - \mathbb{P}[(c^i_A, c^i_B) = (0,0)]}. \qquad (6.34)$$

Writing $a = \mathbb{P}[(c^i_A, c^i_B) = (0,0)], b = \mathbb{P}[(c^i_A, c^i_B) = (0,1)], c = \mathbb{P}[(c^i_A, c^i_B) = (1,0)]$ and $d = \mathbb{P}[(c^i_A, c^i_B) = (1,1)]$ one can restate these probabilities as $\frac{c}{c+d}$ and $\frac{c+b}{1-a}$, respectively, and verify that $\frac{c}{c+d} \leq \frac{c+b}{1-a}$ given that $a+b+c+d = 1$. Thus,

$$\mathbb{P}[C^i_{\text{diff}} \,|\, C^i_{\neq 0}] \geq \mathbb{P}[C^i_{\text{diff}} \,|\, c^i_A = 1] = \mathbb{P}[c^i_B = 0 \,|\, c^i_A = 1]. \qquad (6.35)$$

The case $c^i_B = 1$ works the same way. Hence,

$$\mathbb{P}[C^i_{\text{diff}} \,|\, C^i_{\neq 0}] \geq \max\{\mathbb{P}[c^i_B = 0 \,|\, c^i_A = 1], \mathbb{P}[c^i_A = 0 \,|\, c^i_B = 1]\}. \qquad (6.36)$$

From (6.32) we see that if the probability to commit differently was higher than α we would detect attackers in the r/α committed rounds with a probability exponentially close to 1 in r. If we pick $r = 20$ for example, we would 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 r/α rounds, we can say with very high probability that the probabilities in (6.29), (6.30) 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 6.3.9.

We also need to control the dependence on $\tilde{c}$ (which comes from $|\Sigma^c_\alpha| \leq \tilde{c} 2^{2n}$), which we will argue now. Intuitively, if the set Σ^c_α 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 would look at $\Sigma^c_{2\alpha}$ for example, we expect the set to be much smaller than Σ^c_α.

We can make this intuition precise. Suppose that we play $k\frac{20}{\alpha}$ 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^c_α. In the worst case, all the values in this set are very close to α and, for the average to be $\frac{\alpha}{k}$, we see that the maximal size is $|\Sigma^c_\alpha| \leq \frac{2}{k}2^{2n}$. 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 $|\Sigma^c_\alpha|/2$ pairs (x, y) in Σ^c_α or $\mathbb{P}[c_B = 0|c_A = 1, x, y] \geq \alpha$ for at least $|\Sigma^c_\alpha|/2$ pairs (x, y) in Σ^c_α. Let us assume without loss of generality that we are in the former case. Thus, we can estimate

$$\begin{aligned}\frac{\alpha}{k} &\geq \frac{1}{2^{2n}}\sum_{x,y}\mathbb{P}[c_A = 0|c_B = 1, x, y] \geq \frac{1}{2^{2n}}\sum_{(x,y)\in\Sigma^c_\alpha}\mathbb{P}[c_A = 0|c_B = 1, x, y] \\ &\geq \frac{1}{2^{2n}}\frac{|\Sigma^c_\alpha|}{2}\alpha. \end{aligned} \tag{6.37}$$

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 $\frac{1}{16k^2}$, for a new security parameter k, 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 6.3.9 we get the following corollary for the attack probability on a *single round* of the protocol.

6.3.11. Corollary. *Consider a QPV protocol* P*, with the properties described as in Theorem 6.3.9 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 of* $\mathsf{c\text{-}P}$ *depending only on* k*:*

$$\begin{aligned}\mathbb{P}[\text{attack } \mathsf{c\text{-}P}_{\eta_V,\eta_P}] &\leq \mathbb{P}[\text{attack } \mathsf{P}_{\eta_P}] + \left(1 - \frac{4}{k}\right)8\sqrt{\alpha} + \frac{4}{k} \\ &\leq \mathbb{P}[\text{attack } \mathsf{P}_{\eta_P}] + \frac{6}{k} \end{aligned} \tag{6.38}$$

Thus, by running more rounds of the protocol with commitment, we can still get the attack success probability to be arbitrary close to the one on the

underlying protocol, even when allowing attackers $\varepsilon \neq 0 \neq \tilde{c}$. Each round the verifiers play gives a better bound on 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. In general, they could use adaptive strategies, adjusting them each round to how they responded before. We will now provide a bound for this most general scenario. The statement of Theorem 6.3.9 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 from the previous rounds. This may change the underlying probabilities of events. However, the proof already considers arbitrary distributions of commitments, so we can just 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 cannot change the probability of successfully attacking the protocol. Therefore, we get the following corollary on the probability of attacking a specific round i.

6.3.12. Corollary. *Consider a QPV protocol* P*, with the properties described as in Theorem 6.3.9 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, 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:*

$$\mathbb{P}[\text{attack } \mathsf{c\text{-}P}_{\eta_V,\eta_P}] \leq \mathbb{P}[\text{attack } \mathsf{P}_{\eta_P}] + (1-2\tilde{c}_i)8\sqrt{\varepsilon_i} + 2\tilde{c}_i. \tag{6.39}$$

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

$$\mathbb{P}[A_1, \ldots, A_n] = \mathbb{P}[A_1]\mathbb{P}[A_2 \,|\, A_1] \cdots \mathbb{P}[A_n \,|\, A_1, \ldots, A_{n-1}], \tag{6.40}$$

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

$$\begin{aligned}\mathbb{P}[\text{detect attackers} \,|\, \text{commits} \neq (0,0)] &= 1 - \mathbb{P}[\forall i \; C^i_{\text{eq}} \,|\, \forall i \; C^i_{\neq 0}] \\ &= 1 - \mathbb{P}[\forall i \; C^i_{(1,1)} \,|\, \forall i \; C^i_{\neq 0}].\end{aligned} \tag{6.41}$$

Explicitly, (6.41) reads

$$\mathbb{P}[\text{detect attackers} \,|\, \text{commits} \neq (0,0)] = 1 - \mathbb{P}[C^1_{(1,1)}, \ldots, C^r_{(1,1)} \,|\, C^1_{\neq 0}, \ldots, C^r_{\neq 0}] \tag{6.42}$$

After using (6.40) and noting that $C^i_{(1,1)} \cap C^i_{\neq 0} = C^i_{(1,1)}$ for any i, this can be rewritten as

$$\begin{aligned}
&\mathbb{P}[\text{detect attackers} \,|\, \text{commits} \neq (0,0)] \\
&\quad = 1 - \prod_{i=1}^{r} \mathbb{P}\Big[C^i_{(1,1)} \,\Big|\, C^1_{(1,1)}, \ldots, C^{i-1}_{(1,1)}, C^i_{\neq 0}, \ldots, C^r_{\neq 0}\Big] \\
&\quad = 1 - \prod_{i=1}^{r} \Big(1 - \mathbb{P}\Big[C^i_{\text{diff}} \,\Big|\, C^1_{(1,1)}, \ldots, C^{i-1}_{(1,1)}, C^i_{\neq 0}, \ldots, C^r_{\neq 0}\Big]\Big).
\end{aligned} \tag{6.43}$$

We can then consider the equations analogous to (6.33), (6.34), but with all the extra events for rounds $1, \ldots, i-1, i+1, \ldots, r$ in the conditioning. Again, labelling these probabilities analogously with a_i, b_i, c_i, d_i (cf. (6.33), (6.34)) we obtain the inequality $\frac{c_i}{c_i+d_i} \leq \frac{c_i+b_i}{p_i-a_i}$, where now

$$p_i = \mathbb{P}\Big[C^1_{(1,1)}, \ldots, C^{i-1}_{(1,1)}, C^i_{\text{any}}, C^{i+1}_{\neq 0}, \ldots, C^r_{\neq 0}\Big], \tag{6.44}$$

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

$$\begin{aligned}
&\mathbb{P}[C^i_{\text{diff}} \,|\, C^1_{(1,1)}, \ldots, C^{i-1}_{(1,1)}, C^i_{\neq 0}, \ldots, C^r_{\neq 0}] \\
&\quad \geq \mathbb{P}\Big[C^i_{\text{diff}} \,\Big|\, C^1_{(1,1)}, \ldots, C^{i-1}_{(1,1)}, \{c^i_A = 1\}, C^{i+1}_{\neq 0}, \ldots, C^r_{\neq 0}\Big] \\
&\quad = \mathbb{P}\Big[c^i_B = 0 \,\Big|\, C^1_{(1,1)}, \ldots, C^{i-1}_{(1,1)}, \{c^i_A = 1\}, C^{i+1}_{\neq 0}, \ldots, C^r_{\neq 0}\Big].
\end{aligned} \tag{6.45}$$

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

$$\begin{aligned}
&\mathbb{P}[\text{detect attackers} \,|\, \text{ commits} \neq (0,0)] \geq \\
&1 - \prod_{i=1}^{r} \Big(1 - \max\big\{\mathbb{P}[c^i_B = 0 \,|\, C^1_{(1,1)}, \ldots, C^{i-1}_{(1,1)}, \{c^i_A = 1\}, C^{i+1}_{\neq 0}, \ldots, C^r_{\neq 0}], \\
&\qquad\qquad \mathbb{P}[c^i_A = 0 \,|\, C^1_{(1,1)}, \ldots, C^{i-1}_{(1,1)}, \{c^i_B = 1\}, C^{i+1}_{\neq 0}, \ldots, C^r_{\neq 0}]\big\}\Big).
\end{aligned} \tag{6.46}$$

Define ε_i as the maximum in (6.46). 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 required number r of non-$(0,0)$ commitment rounds.

Now there are two cases. Either the probability in (6.46) is $\geq 1-\delta$ for 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

$$1 - \prod_{i=1}^{r}(1-\varepsilon_i) \leq 1-\delta. \tag{6.47}$$

We can rewrite this condition as

$$0 < \delta \leq \prod_{i=1}^{r}(1-\varepsilon_i) \leq e^{-\sum_{i=1}^{r}\varepsilon_i}. \tag{6.48}$$

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.

6.3.13. 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 $\mathcal{R} \subset \{\varepsilon_1, \ldots, \varepsilon_r\}$ of size $|\mathcal{R}| = qr$ such that for all $\varepsilon_j \in \mathcal{R}$ we have $\varepsilon_j \leq \frac{\alpha}{(1-q)r}$.*

Proof:
Assume 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 $\varepsilon_i \in \mathcal{R}$. Therefore, a similar argument can be run as in the proof for Corollary 6.3.11 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 6.3.12 that

$$\begin{aligned}\mathbb{P}[&\text{attack } \mathsf{c\text{-}P}_{\eta_V,\eta_P} \text{ in round } i \in \mathcal{R}] \\ &\leq \mathbb{P}[\text{attack } \mathsf{P}_{\eta_P}] + \left(1-\frac{4}{k}\right)8\sqrt{\frac{\ln(1/\delta)}{(1-q)r}} + \frac{4}{k},\end{aligned} \tag{6.49}$$

while kr rounds are run (similar to Corollary 6.3.11). 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

$$\begin{aligned}\mathbb{P}[\text{attack } \mathsf{c\text{-}P}_{\eta_V,\eta_P} \text{ in round } i \in \mathcal{R}] &\leq \mathbb{P}[\text{attack } \mathsf{P}_{\eta_P}] + \left(1-\frac{4}{k}\right)8\sqrt{\frac{20}{r/k}} + \frac{4}{k} \\ &\leq \mathbb{P}[\text{attack } \mathsf{P}_{\eta_P}] + \frac{6}{k}, \end{aligned} \tag{6.50}$$

to obtain a similar bound as in Corollary 6.3.11, 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 can choose k, which will determine the number of rounds they have to run to guarantee (6.50) 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 summarise our findings in the following corollary.

6.3.14. Corollary. *Consider a QPV protocol* P*, with the properties described as in Theorem 6.3.9 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*

$$\mathbb{P}[\text{attack } \mathsf{c\text{-}P}^{\text{seq}}_{\eta_V,\eta_P} \text{ in round } i] \leq \mathbb{P}[\text{attack } \mathsf{P}_{\eta_P}] + \frac{6}{k} \tag{6.51}$$

for all i *with* $\varepsilon_i \in \mathcal{R}$*.*

6.4 Sequential repetition

For QPV protocols P with the properties mentioned in Theorem 6.3.9 and security under sequential repetition, we can extend the results of the previous section to prove security for sequential repetition of its committing version $\mathsf{c\text{-}P}$. Using techniques also used in [ES23], which utilises Azuma's inequality [Azu67], one can show that the attack success probability of $\mathsf{P}^{\text{seq}}_{\eta_V,\eta_P}$ exponentially decays in the number of rounds. Here we will just briefly summarise the results. For a detailed treatment and proof we refer to [ABB+23]. We introduce nomenclature for the different security settings studied: **S1** for the ideal setting with $\varepsilon = \tilde{c} = 0$, **S2** for non-adaptive strategies and **S3** for adaptive strategies. The bounds in this section apply to the case when attackers are not caught due to a different commitment, as mentioned in Corollaries 6.3.11 and 6.3.14.

No loss at the prover

First, for the case of perfect transmission in the prover's laboratory ($\eta_P = 1$) Table 6.1 summarises our findings. In scenario **S1** this is obtained by simply upper bounding the probability that attackers get every round correct via the bounds obtained in the previous section. In scenarios **S2** and **S3** we can define a random variable Γ_r representing a 'score' over the r rounds run, giving different points for correct, wrong and 'signal loss' answers. The expected score per round is μ and δ describes a threshold parameter for how far from the expected score the returned sample is allowed to be. Then a standard Chernoff bound allows us to lower bound the probability that the honest party achieves the threshold, while Azuma's inequality allows us to upper bound the probability that attackers achieve the threshold (provided their single-round success probability is smaller than $1 - p_{\text{err}}$).

	$p_{\text{err}} = 0$	$p_{\text{err}} > 0$
Honest prover	1	$1 - e^{-r\delta^2\mu^2}$
Attackers **S1**	$(\mathbb{P}[\text{attack P}])^r$	$e^{-\frac{r}{2}((1-\mathbb{P}[\text{attack P}]-p_{\text{err}})(1-\delta))^2}$
Attackers **S2**	$\left(\mathbb{P}[\text{attack P}] + 24\sqrt[3]{\frac{5}{r}}\right)^r$	$e^{-\frac{r}{2}\left((1-\mathbb{P}[\text{attack P}]-24\sqrt[3]{\frac{5}{r}}-p_{\text{err}})(1-\delta)\right)^2}$
Attackers **S3**	$\left(\mathbb{P}[\text{attack P}] + 12\sqrt[4]{\frac{20}{r}}\right)^{\left(1-2\sqrt[4]{\frac{20}{r}}\right)r}$	$e^{-\frac{r}{2}\left((1-\mathbb{P}[\text{attack P}]-12\sqrt[4]{\frac{20}{r}})(1-\delta)-\sqrt[4]{\frac{320}{r}}\right)^2}$

Table 6.1: Overview over the lower bounds for the honest prover's probability of answering always correctly (when $p_{\text{err}} = 0$) and achieving the threshold (when $p_{\text{err}} > 0$), i.e. $\Pr[\Gamma_r > r\mu(1-\delta)]$, versus the upper bounds of their counterparts for the attackers in the security models **S1**, **S2**, and **S3**, after r sequential repetitions of $\mathsf{c\text{-}P}_{\eta_V,\eta_P}$ with $\eta_P = 1$, i.e. no loss at the prover. Note that with increasing r, the honest success probability gets arbitrarily close to 1, while the upper bounds on the one of attackers get suppressed.

Lossy prover

A similar argument can be made for the most general and practically relevant scenario of a prover with $p_{\text{err}} > 0$ and $\eta_P < 1$, taking into account that there is another 'signal loss' answer and single round security is only provided on a large subset of all rounds as per Theorem 6.3.14.

For security models **S1** and **S2** (with $r = 320k^3$) we obtain an upper bound

of

$$\Pr\left[\tilde{\Gamma}_r^{\text{att}} \geq r\tilde{\mu}(1-\delta)\right] \leq e^{-\frac{r}{2}(\tilde{\mu}(1-\delta))^2}, \tag{6.52}$$

and for security model **S3** (with $r = 320k^4$) we get

$$\Pr\left[\tilde{\Gamma}_r^{\text{att}} \geq r\tilde{\mu}(1-\delta)\right] \leq e^{-\frac{r}{2}\left(\tilde{\mu}(1-\delta)-\frac{1}{k}\right)^2}, \tag{6.53}$$

for the probability that attackers achieve the threshold successfully. This holds as long as η_P is sufficiently high not to allow for a simple lossy guessing attack, as mentioned in Section 3.2.1, and p_{err} is sufficiently low so that the honest success probability in a single round is strictly larger than the corresponding attack upper bounds. For more details, see [ABB+23].

6.5 c-QPV$^f_{\text{BB84}}$ as a practical QPV protocol

Our result makes the practically interesting protocol QPV$^f_{\text{BB84}}$ a strong candidate for an implementation of QPV by running its version c-QPV$^f_{\text{BB84}}$ with commitment instead.

QPV$^f_{\text{BB84}}$, and its extensions encoding the qubit Q in m bases, can be attacked if the transmission of the protocol is $\eta_V\eta_P \leq 1/m$, by Alice guessing the basis and claiming 'signal loss' whenever the guess was wrong. Previously, the high transmission loss between the verifiers and the prover would make this condition always true in practice, making the protocol insecure. Our main result, Theorem 6.3.9, removes this problem, as for c-QPV$^f_{\text{BB84}}$ this transmission loss $1-\eta_V$ becomes irrelevant for the security of the protocol and only the loss in the prover's laboratory $1-\eta_P$, which should be much smaller, matters. If one assumes there's no loss in the prover's laboratory, security is recovered applying the upper bound of $\mathbb{P}[\text{attack QPV}^f_{\text{BB84}}]$ in [BCS22], which also includes errors from the prover. In addition, considering loss in the prover's laboratory, security is recovered by applying the upper bounds on $\mathbb{P}[\text{attack QPV}^f_{\text{BB84}}]$ in [ES23], but now for arbitrary large distances. These bounds hold as long as the attackers cannot share a quantum state of larger dimension than $\Omega(n)$ at the beginning of each round. Notice that since the time delay δ is small, m can remain small[5].

All this makes c-QPV$^f_{\text{BB84}}$ a protocol that is experimentally feasible to implement, that can be made loss-tolerant enough for practice, that is robust against slow quantum communication, and that inherits the desirable trade-off between the resources of the honest parties and the attackers for an attack. Importantly, the latter lower bound is in the classical input size. Since sending classical information is easy from the point of view of verifiers and the honest prover, we can set the attacking requirements so high that it becomes practically infeasible

[5]If the loss during time δ is below 50%, QPV$^f_{\text{BB84}}$ with $m = 2$ already provides security.

to attack the protocol with current technology. In the foreseeable future, it is not possible to store and manipulate the amount of qubits needed to attack the protocol successfully.

6.6 QPV with commitment in practice

For the protocol with commitment, the honest prover needs a device detecting the presence of the input quantum state[6] without destroying it, i.e. a photon 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.

Transmission in the prover laboratory

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

$$\begin{aligned}\eta_P &= \mathbb{P}[\text{photon measured} \,|\, \text{presence detected}] \\ &= \frac{\mathbb{P}[\text{photon measured} \wedge \text{presence detected}]}{\mathbb{P}[\text{presence detected}]}.\end{aligned} \tag{6.54}$$

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

(i) 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*

(ii) (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 (6.54) as[7]

$$\eta_P = \frac{(\eta_{\text{meas}} + p_{\text{dc}})\eta_V \eta_{\text{det}}^{\text{QND}} + p_{\text{dc}} p_{\text{dc}}^{\text{QND}}}{\eta_V \eta_{\text{det}}^{\text{QND}} + p_{\text{dc}}^{\text{QND}}}. \tag{6.55}$$

[6] We will focus on photonic qubits.

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

Notice that

$$\text{if } \eta_V \ll p_{\text{dc}}^{\text{QND}}: \qquad \eta_P \sim p_{\text{dc}}. \tag{6.56}$$

If the probability that a photon enters the presence detector (η_V) is much smaller than the dark count rate $p_{\text{dc}}^{\text{QND}}$ then most photon presence detection events, and thus $c = 1$ commitments, will be due to dark counts! Then the (e.g. polarisation) 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 $\eta_P \to p_{\text{dc}}$ as expected. Single photon detectors routinely achieve $p_{\text{dc}} \sim 10^{-7}$ or similar per detection window [Had09]. For such small η_P the usual lossy attack of guessing the prover's 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 $\eta_V \ll p_{\text{dc}}^{\text{QND}}$.

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

$$\texttt{SNR}_{\text{QND}}(\gamma) = \frac{\eta_V \eta_{\text{det}}^{\text{QND}}}{\eta_V \eta_{\text{det}}^{\text{QND}} + p_{\text{dc}}^{\text{QND}}} = \frac{\gamma \eta_{\text{det}}^{\text{QND}}}{\gamma \eta_{\text{det}}^{\text{QND}} + 1}. \tag{6.57}$$

We have already argued that in the case $\eta_V \ll p_{\text{dc}}^{\text{QND}}$ our proposal cannot be used. Let us therefore focus on the case where η_V is at least the order of magnitude of $p_{\text{dc}}^{\text{QND}}$, corresponding to $\gamma \geq 1$. Then, using that p_{dc} is usually negligibly small compared to the other quantities, we can simplify η_P to

$$\eta_P \sim \texttt{SNR}_{\text{QND}}(\gamma) \eta_{\text{meas}}. \tag{6.58}$$

The condition that the input transmission must be greater than $p_{\text{dc}}^{\text{QND}}$ 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 fibres reads $\eta = 10^{-\alpha L/10}$ [SJ09], where α is the attenuation of the fibre in dB/km and L is the length of the fibre in km. A standard value for current optical fibres is $\alpha = 0.2\,\text{dB/km}$ [SJ09], with the most sophisticated ones achieving $\alpha = 0.14\,\text{dB/km}$ [HTS+18]. We can solve for L and insert η_V in terms of the presence detection dark count rate to obtain

$$L = -\frac{10}{\alpha} \log_{10}(\eta_V) = -\frac{10}{\alpha} \log_{10}\left(\gamma p_{\text{dc}}^{\text{QND}}\right). \tag{6.59}$$

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 polarisation state, generating EPR pairs, fast low-loss 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:

(i) Single photon generation: MHz, in principle up to GHz [MSSM20],

(ii) Polarisation modulation: up to GHz [LLX+19],

(iii) EPR state generation: up to GHz, depending on pump laser power [LVSL18, APS+21],

(iv) Switching: up to THz [CHW+17],

(v) Single photon detector count rate: up to GHz [Had09].

Therefore, we expect our protocol can run at least at MHz rate and possibly at GHz rate with top equipment, albeit we acknowledge that it may be challenging to run all these processes at high rates simultaneously or with high transmission. 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 required to reach the number of rounds stated in Corollary 6.3.14.

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 $t_{\text{c-P}}$ in seconds is therefore

$$t_{\text{c-P}} = \frac{320k^4}{p_{\text{commit}}\nu}. \tag{6.60}$$

Given a choice of security parameter k, a probability to commit p_{commit} from the prover[8] 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 6.3.14.

6.6.1 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

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

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

$$\begin{aligned} \text{Photon in output mode given heralding } (\eta_{\text{surv}}): &\sim 25\text{-}55\%, \\ \text{Dark count rate } (p_{\text{dc}}^{\text{QND}}): &\sim 3\%, \\ \text{Fidelity of photon in output mode:} &\sim 96\%. \end{aligned} \tag{6.61}$$

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.

Even though this technology is currently not usable 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.

6.6.2 Simplified presence detection with a 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[9] 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 6.4 [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 η_V. This will jeopardise security only if it makes

[9] We will define which click patterns count as successful further in Figure 6.4.

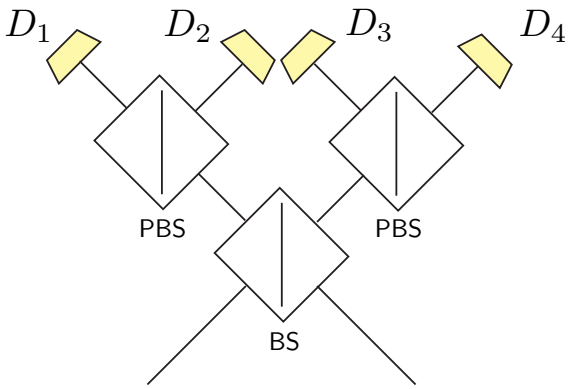


Figure 6.4: Schematically a partial Bell measurement can be implemented via a 50/50 beam splitter (BS), two polarisation beam splitters (PBS) and four single photon detectors (D_i). An input state $|\Psi_-\rangle$ triggers one detector in each arm (D_1, D_3 or D_2, D_4), $|\Psi_+\rangle$ triggers two 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.

η_V so small that dark counts take over. Moreover, it may be that the teleportation corrections don't 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$^f_{\text{BB84}}$ for example. So then only a partial, linear-optical BSM and (very short) storage of the other EPR qubit would be required experimentally. The BSM setup also has the beneficial property that it has no false positives in the ideal case. So detecting *some* incoming photons with certainty is a much easier task than detecting all photons that come in. In practice, what matters is the dark count rate of the QND measurement, as this does introduce false positives and subsequently introduces errors in the prover's final measurement.

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

$$\eta_P \sim \mathtt{SNR}_{\mathrm{QND}}(\gamma)\eta_{\mathrm{meas}} \leq \frac{\gamma\eta_{\mathrm{det}}^3}{\gamma\eta_{\mathrm{det}}^2+1}. \tag{6.62}$$

Easy-to-use single photon detectors have detection efficiencies of up to 20-65% [Had09], and the most sophisticated detectors reach up to 98%[10] [RNN+20]. In reality, there will also be losses pre-measurement, making the true value in (6.62) 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 (6.62) and secure c-QPV becomes possible if this value is large enough to prevent lossy attacks.

With regard to the distance L between the verifiers and the prover, we can use (6.59) to obtain an estimate of what kinds of distances become possible for QPV with our proposal. As mentioned, with this setup $p_{\mathrm{dc}}^{\mathrm{QND}} \sim p_{\mathrm{dc}} \sim 10^{-7}$. Moreover, η_V should be at least one (preferably more) order of magnitude larger than $p_{\mathrm{dc}}^{\mathrm{QND}}$ to obtain a decent signal-to-noise ratio, so say $\gamma \gtrsim 10$. This yields via (6.59) that

$$L \lesssim 400\,\mathrm{km} \tag{6.63}$$

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

6.6.1. Remark. c-QPV makes a class of previously not loss-tolerant QPV protocols, with $\mathrm{QPV}_{\mathrm{BB84}}^{f}$ as a prime example, loss-tolerant even in practice as long as both the signal-to-noise ratio of the photon presence detection $\mathtt{SNR}_{\mathrm{QND}}$ and the efficiency of the prover measurement η_{meas} are sufficiently high such that η_P is high enough to prevent lossy attacks[11]. The signal-to-noise ratio $\mathtt{SNR}_{\mathrm{QND}}$ depends on the transmission η_V between the verifiers and the prover, the dark count rate $p_{\mathrm{dc}}^{\mathrm{QND}}$, and the detection efficiency $\eta_{\mathrm{det}}^{\mathrm{QND}}$. This ultimately limits the maximal distance between the verifiers and the prover[12]. The experimental requirements of our proposal in the prover laboratory are as follows:

(i) The prover needs to be able to generate an EPR pair on demand.

(ii) Photon presence detection, e.g. via a partial linear-optical BSM (like the scheme in Figure 6.4).

(iii) A short delay loop, so the prover can store the teleported qubit until the classical information x, y arrives. This time delay should be as short as possible.

(iv) 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 $f(x, y)$.

[10] Note that detection efficiencies always depend on the wavelength of the photons used.
[11] For example as studied in [ES23] for $\mathrm{QPV}_{\mathrm{BB84}}^{f}$, which carries over to our c-$\mathrm{QPV}_{\mathrm{BB84}}^{f}$.
[12] To much larger distances than previously possible for QPV, however.

The verifiers need to be able to generate and modulate single-photon states (e.g. polarisation) with high frequency. All requirements are in principle practically feasible, or within reach, with state-of-the-art equipment.

6.7 Discussion

The three major roadblocks for practically implementable and secure QPV are: entangled attackers, slow honest quantum communication, and signal loss. In addition, the honest protocol must be feasible experimentally. So far, no QPV protocol has been able to deal with all of these issues. The work in this chapter presents the first such protocol: c-QPV$^{f}_{\mathrm{BB84}}$. 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 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. c-QPV$^{f}_{\mathrm{BB84}}$ 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 analysing 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. We argue that all the experimental requirements are, in principle, feasible and that our protocol can be run at reasonably high rates. These properties taken together make c-QPV$^{f}_{\mathrm{BB84}}$ the first QPV protocol that can successfully address all the main practical issues of QPV. Our result is not limited to QPV$^{f}_{\mathrm{BB84}}$ per se, but can be applied to any state-independent QPV protocol (loosely speaking, protocols that are of the same structure as QPV$^{f}_{\mathrm{BB84}}$).

Chapter 7

Quantum Position Verification with Continuous Variables

Chapter summary. In this chapter we study quantum position verification with continuous-variable quantum states. In contrast to existing discrete protocols, we present and analyse a protocol that utilises coherent states and its properties. Compared to discrete-variable photonic states, coherent states offer practical advantages since they can be efficiently prepared and manipulated with current technology. We prove security of the protocol against any unentangled attackers via entropic uncertainty relations, showing that the adversary has more uncertainty than the honest prover about the correct response as long as the noise in the quantum channel is below a certain threshold. Additionally, we show that attackers who pre-share one continuous-variable EPR pair can break the protocol.

This chapter is based on the following paper:

[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*, 2023. arXiv:2308.04166

7.1 Introduction

Almost all previously studied QPV protocols have in common that they contain only finite-dimensional quantum systems. The study of QPV using continuous-variable (CV) quantum information was first mentioned in [QS15], in which a general attack was shown in the transmission regime $t \leq 1/2$, but the security of the protocol was not further analysed. Moreover, [LXS+16] studied a practical implementation of QPV_{Bell} using decoy states.

A well-known example of CV quantum information is the quantised harmonic

oscillator, which is usually described by continuous variables such as position and momentum. CV quantum systems are particularly relevant for quantum communication and quantum-limited detection and imaging techniques because they provide a quantum description of the propagating electromagnetic field. Important CV states are the eigenstates of the annihilation operator, the so-called coherent states, and their quadrature squeezed counterparts known as squeezed coherent states. The main appearance of CV quantum states in a quantum communication protocol was the CV variant of quantum key distribution (CV-QKD).

We extend the ideas of finite-dimensional QPV protocols, and more formally analyse a QPV protocol very similar to the one mentioned in [QS15]. We provide a general proof of security against attackers who do not have access to entanglement, taking into account attenuation and excess noise in the quantum channel. We also show that the attackers can break the scheme if they pre-share one pair of maximally entangled modes.

In the finite-dimensional case, often the job of the prover is to complete a task *correctly*, and attackers are detected by a suspiciously high error rate. This property of QPV protocols changes in the continuous setting, where even the honest prover's answers are drawn from a probability distribution. Therefore, the verifiers' job is to distinguish an honest sample from an adversarial one.

Although the generalisation of QPV to CV is interesting in itself, the motivation here is practical. CV systems are much simpler to handle in practice and leverage several decades of experience in coherent optical communication technology. One particular advantage is that no true single-photon preparation or detection is necessary. Clean creation and detection of single photons is still expensive and technically challenging, especially if photon number resolution is desired. In contrast, homodyne and heterodyne measurements are easy to implement and a lot of existing infrastructure is geared towards handling light at low-loss telecom wavelengths (1310nm, 1550nm), whereas an ideal single photon source in these wavelength bands still has to be discovered and frequency up-conversion is challenging and introduces new losses and errors.

7.2 The protocol $\mathrm{QPV}_{\mathrm{coh}}$

7.2.1 Prepare-and-measure version

Consider two spatially separated verifiers V_0 and V_1, and a prover P somewhere in between them. Let $\mathcal{A}$ be a publicly known set of angles in $[0, 2\pi)$ such that $\alpha \in \mathcal{A} \implies \alpha + \pi/2 \in \mathcal{A}$. Let σ be a publicly known parameter with $\sigma \gg 1$. A single round of the protocol $\mathrm{QPV}_{\mathrm{coh}}$ consists of the following steps:

1. The verifiers draw a random $\theta \in \mathcal{A}$ and two random variables $(r, r^{\perp})$ from the Gaussian distribution $\mathcal{N}_{0,\sigma^2}$. Verifier V_0 prepares a coherent state $|\psi\rangle$

with quadratures $(x_0, p_0) = (r\cos\theta + r^{\perp}\sin\theta,\ r\sin\theta - r^{\perp}\cos\theta)$. Then $\mathsf{V_0}$ sends $|\psi\rangle$ to the prover, and $\mathsf{V_1}$ sends θ to the prover.

2. The prover receives θ and $|\psi\rangle$ and performs a homodyne measurement on $|\psi\rangle$ in the θ direction, resulting in a value $r' \in \mathbb{R}$. The prover sends r' to both verifiers.

After n rounds, the verifiers have received a sample of responses, which we denote as $(r'_i)_{i=1}^n$. The verifiers check whether all prover responses arrived at the correct time, and whether the reported values $(r'_i)_{i=1}^n$ satisfy

$$\frac{1}{n}\sum_{i=1}^{n}\frac{\left(r'_i - r_i\sqrt{t}\right)^2}{\frac{1}{2}+u} < \gamma \qquad \text{with } \gamma \coloneqq 1 + \frac{2}{\sqrt{n}}\sqrt{\ln\frac{1}{\varepsilon_{\mathrm{hon}}}} + \frac{2}{n}\ln\frac{1}{\varepsilon_{\mathrm{hon}}}. \tag{7.1}$$

Here $\varepsilon_{\mathrm{hon}}$ is an upper bound on the honest prover's failure probability, see Section 7.2.3. The $\varepsilon_{\mathrm{hon}}$ is a protocol parameter and can be set to a desired value. The verifiers *reject* if not all these checks are satisfied. We refer to the sum in (7.1) as the *score*.

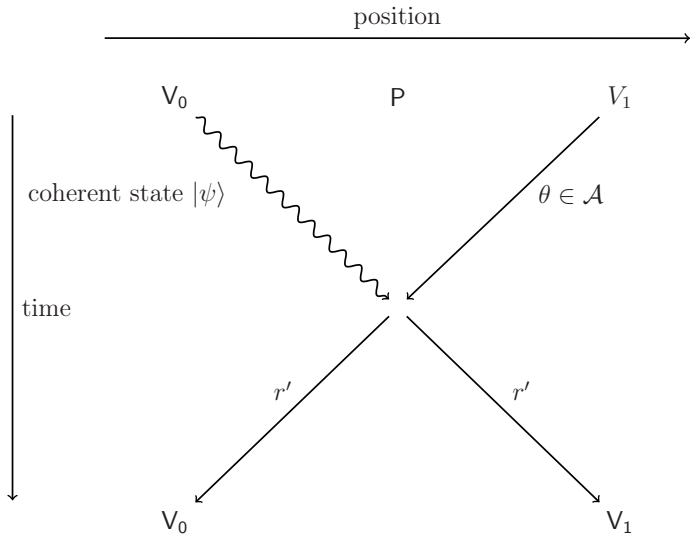


Figure 7.1: Schematic representation of the protocol $\mathrm{QPV}_{\mathrm{coh}}$. Undulated lines represent quantum information, straight lines represent classical information.

7.2.2 Entanglement based version

In security proofs for qubit-based schemes, it is customary to reformulate a protocol into an EPR based form. The act of one party (the verifier $\mathsf{V_0}$ in our case)

preparing and sending a qubit state in a particular basis b is equivalent to V_0 preparing a two-qubit EPR pair and then measuring one of the qubits in the basis b while the other qubit is sent. The act of measuring can also be postponed. This has the advantage that in the security analysis the basis choice can be delayed and it is then possible to base security on the properties of entangled states.

We will do an analogous reformulation for CV states. We tune the squeezing parameter ζ such that $\sinh\zeta = \sigma$, as explained in Chapter 2. Preparing a coherent state with Gaussian distributed displacements $x_0, p_0 \sim \mathcal{N}_{0,\sigma^2}$ is equivalent to preparing a two-mode squeezed state with squeezing parameter ζ and then performing a heterodyne $(\hat{x}, \hat{p})$ measurement on one mode, with measurement outcome $\frac{(x_0,-p_0)}{\sqrt{2}\tanh\zeta}$.

In our particular case, the verifier V_0 prepares the two-mode squeezed state ρ_{V_0P} and performs the heterodyne measurement with quadratures rotated by the angle θ on the V_0 subsystem. The measurement outcomes are $r/(\sqrt{2}\tanh\zeta)$ and $-r^\perp/(\sqrt{2}\tanh\zeta)$, resulting in displacement $(r, r^\perp)$ in the state sent to the prover (subsystem P). The prover then performs a homodyne measurement under angle θ to recover r, similar to the prepare-and-measure scheme.

In the security analysis later, we will explicitly write V_0's heterodyne measurement as a double-homodyne measurement. First, V_0 mixes its own mode with the vacuum using a beam splitter, resulting in a two-mode state. On one of these modes, V_0 then performs a homodyne measurement in the θ direction, on the other mode in the $\theta + \frac{\pi}{2}$ direction.

7.2.3 Honest prover

Success probability

We show that the honest prover has a failure probability smaller than ε_{hon}.

7.2.1. Lemma. (Equ. (4.3) in [LM00]) *Let X be a χ^2_n distributed random variable. It holds that*

$$\mathbb{P}[X - n \geq 2\sqrt{na} + 2a] \leq e^{-a}. \tag{7.2}$$

In round i, the honest prover performs a homodyne measurement under an angle θ_i, on a coherent state that has displacement r_i in the θ_i direction (and displacement $r_i^\perp$ in the $\theta_i + \frac{\pi}{2}$ direction). The measurement outcome R_i' is Gaussian-distributed with mean r_i and variance $1/2$ (shot noise). The (unnormalised) score random variable $Z = \sum_{i=1}^n (R_i' - r_i\sqrt{t})^2/(\frac{1}{2} + u)$ then is χ^2_n distributed. The probability that the honest prover fails to pass verification is given by

$$\mathbb{P}[Z \geq n\gamma] = \mathbb{P}\left[Z \geq n + 2\sqrt{n \ln\frac{1}{\varepsilon_{\text{hon}}}} + 2\ln\frac{1}{\varepsilon_{\text{hon}}}\right]. \tag{7.3}$$

By Lemma 7.2.1 this is upper bounded by ε_{hon}.

A posteriori distribution and entropy of R conditioned on measurement

We determine how much uncertainty the honest prover has about the displacements r_i, given the measurement outcomes r'_i. For notational brevity, we omit the round index i. We write the probability density for R as f_R. Since r' is the result of a measurement under angle θ, conditioning on θ is implicit and will be omitted from the notation.

The prover's posterior distribution of R, given r', is

$$f_{R|R'}(r|r') = \frac{f_{RR'}(r,r')}{f_{R'}(r')} = \frac{f_R(r) f_{R'|R}(r'|r)}{f_{R'}(r')}. \tag{7.4}$$

Using $f_R = \mathcal{N}_{0,\sigma^2}$, $f_{R'|R}(r'|r) = \mathcal{N}_{r\sqrt{t},\frac{1}{2}+u}(r')$ and $f_{R'} = \mathcal{N}_{0,t\sigma^2+\frac{1}{2}+u}$ we get, after some algebra,

$$\begin{aligned} f_{R|R'}(r|r') &= \mathcal{N}_{M,\Sigma^2}(r) \\ \text{with } \Sigma^2 &\coloneqq \left(\frac{1}{\sigma^2} + \frac{t}{1/2+u}\right)^{-1}, \\ \text{and } M &\coloneqq \frac{r'}{\sqrt{t}} \cdot \frac{1}{1+\frac{1/2+u}{t\sigma^2}}. \end{aligned} \tag{7.5}$$

For $t\sigma^2 \gg 1$, this tends to a Gaussian distribution centred at $r'/\sqrt{t}$, with variance $(\frac{1}{2}+u)/t$. From the Gaussian probability density function $\mathcal{N}_{M,\Sigma^2}(r)$ we directly obtain the differential entropy of R given R',

$$h(R|R') = \frac{1}{2}\log 2\pi e\Sigma^2. \tag{7.6}$$

7.3 Security against LOSQC attackers

In this section, we show security against LOSQC attackers, i.e. general unentangled attackers, by lower bounding their uncertainty higher than the prover's. This is captured by the following theorem.

7.3.1. Theorem. *For at least one attacker E participating in an LOSQC attack, the differential entropy of R, given side information held by E, follows the inequality*

$$h(R|E) \geq \frac{1}{2}\log\frac{4\pi}{1+\sigma^{-2}}, \tag{7.7}$$

where σ is the same as defined in Section 7.2.2. Furthermore, this attacker's response r' satisfies the inequality

$$\mathbb{E}\big[(R-r')^2\big] \geq \frac{2}{e}\cdot\frac{1}{1+\sigma^{-2}}. \tag{7.8}$$

Proof:
In the entanglement-based protocol, the verifiers perform a heterodyne measurement. This is achieved by mixing one half of the TMS state with vacuum (denoted by O) and then performing a homodyne measurement per mode, in orthogonal directions θ and $\theta + \frac{\pi}{2}$, so

$$\rho_{VP} \xrightarrow[\text{with } O]{\text{mixing}} \rho_{\bar{V}\bar{O}P}, \tag{7.9}$$

where the bar represents the modes after mixing. Here, P is the subsystem sent to the prover and $\bar{V}$ is the subsystem to which the θ measurement will be applied.

In general, Alice performs a quantum operation on the mode P and any local auxiliary modes she has. We call the subsystem that Alice keeps A, and the one she sends to Bob B. The resulting state after communication is $\rho_{\bar{V}\bar{O}AB}$. We are interested in the tripartite state $\rho_{\bar{V}AB}$ at this stage. The result of a homodyne measurement on $\bar{V}$ under angle θ is denoted as $U_\theta \in \mathbb{R}$, and we define $\bar{\theta} = \theta + \frac{\pi}{2}$. Lemma 2.3.7 gives

$$\forall \theta \in \mathcal{A} \qquad h(U_\theta|A) + h(U_{\bar{\theta}}|B) \geq \log 2\pi. \tag{7.10}$$

Averaging over θ, and using the fact that averaging over $\bar{\theta}$ is the same as averaging over θ, gives

$$\mathbb{E}_{\theta\in\mathcal{A}} h(U_\theta|A) + \mathbb{E}_{\theta\in\mathcal{A}} h(U_{\bar{\theta}}|B) = \mathbb{E}_{\theta\in\mathcal{A}} h(U_\theta|A) + \mathbb{E}_{\theta\in\mathcal{A}} h(U_\theta|B) \geq \log 2\pi. \tag{7.11}$$

The last expression can be written as

$$h(U|A\Theta) + h(U|B\Theta) \geq \log 2\pi, \tag{7.12}$$

where the angle Θ is now represented as a random variable. It follows that

$$\max\left\{h(U|A\Theta),\ h(U|B\Theta)\right\} \geq \frac{1}{2}\log 2\pi. \tag{7.13}$$

Finally, we note that $R = U\sqrt{2}\tanh\zeta$ (with $\sinh\zeta = \sigma$) and use Lemma 2.3.3 to conclude

$$h(R|E) \geq \frac{1}{2}\log 2\pi + \frac{1}{2}\log\frac{2}{1+\sigma^{-2}} = \frac{1}{2}\log\frac{4\pi}{1+\sigma^{-2}}. \tag{7.14}$$

Here, we have set $\max\left\{h(R|A\Theta),\ h(R|B\Theta)\right\} = h(R|E)$. The result for $\mathbb{E}[(R-r')^2]$ follows directly from the Fano inequality (Theorem 2.3.8). □

7.3.1 Comparison between LOSQC attackers and honest prover

Recall that $\sigma \gg 1$. The protocol works only if the attackers have more ignorance about the value R than the honest prover. Note that we assume that the attackers

are powerful and have access to an ideal channel ($t = 1, u = 0$). For $\sigma \to \infty$, the difference between their entropies (7.7) and (7.6) satisfies

$$h(R|E) - h(R|R') \geq \frac{1}{2} \log\left(\frac{4}{e} \cdot \frac{t}{1+2u}\right). \tag{7.15}$$

The argument of the logarithm needs to be larger than 1. This is the case when

$$t > \frac{e}{4} \approx 0.680 \quad \text{and} \quad u \leq \frac{t \cdot 4/e - 1}{2}. \tag{7.16}$$

Note that Fano's inequality applied to the honest prover's entropy (7.6) would yield the expression $\mathbb{E}\left[(\sqrt{t}R - r')^2\right] \approx \Sigma^2$ (as $\sqrt{t}R|R'$ is Gaussian with mean r' in the large σ limit), with $\Sigma^2 \approx (1/2 + u)/t$. On the other hand, the expected error of the attacker is lower bound by $2/e \approx 0.74$, which is strictly greater than $(1/2 + u)/t$ for certain parameter ranges, as depicted in Figure 7.2. This proves security of the protocol against a general LOSQC attacks in these parameter ranges.

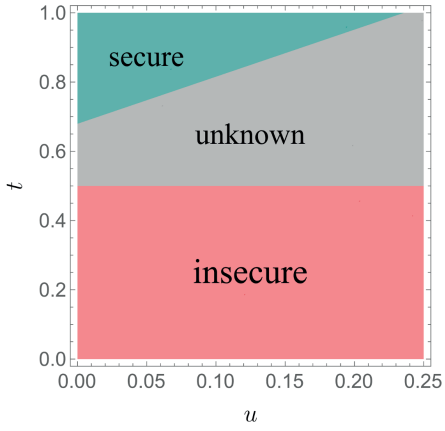


Figure 7.2: Security of the proposed CV-QPV protocol QPV_{coh}. For $t \leq 1/2$ it is insecure (red), as shown in [QS15]. For values in the green region, we prove security (for LOSQC attacks). No conclusions can be drawn about the grey region from our results. The axes denote the transmission t and excess noise u.

So as long as equation (7.15) is positive, i.e.

$$\frac{t}{1+2u} > \frac{e}{4}, \tag{7.17}$$

there's a finite gap between the attacker and the honest entropy about R. Then an attack fails if the score is greater than γ (cf. Section 7.2.1). To estimate the

number of (independent) rounds n we have to run for the attack success probability to become vanishingly small, we cannot assume a specific attack distribution and we have to assume that the attackers have access to an ideal channel. We know that

$$\mathbb{E}\big[(R-r')^2\big] \geq \frac{2}{e}, \tag{7.18}$$

and $\mathbb{E}\big[(\sqrt{t}R-r')^2\big] \geq 2/e$ for any transmission t. The probability that the attackers' score falls below the threshold γ is at most the probability that the score differs from $\mathbb{E}\big[(\sqrt{t}R-r')^2\big]/(1/2+u)$ by more than the difference $\Delta \coloneqq (2/e)/(1/2+u)-\gamma$[1]. Thus, we can use the Chebyshev inequality for the random variable of the score to get

$$\mathbb{P}\left[\left|\frac{1}{n}\sum_{i=1}^{n}\frac{(\sqrt{t}R_i-r_i')^2}{1/2+u}-\frac{\mathbb{E}(\sqrt{t}R-r')^2}{1/2+u}\right|\geq\Delta\right]\leq\frac{\tilde{\sigma}^2}{n\Delta^2}=O\left(\frac{1}{n\Delta^2}\right), \tag{7.19}$$

where $\tilde{\sigma}^2=\mathbb{V}\left[\frac{\left(\sqrt{t}R-r'\right)^2}{1/2+u}\right]$ is the variance of the random variable it contains. If we set $n\Delta^2=\Omega\big(\frac{1}{\varepsilon_{\text{att}}}\big)$, where ε_{att} is the threshold we accept for the attack success probability as a parameter of the protocol, then we get

$$\mathbb{P}\left[\frac{1}{n}\sum_{i=1}^{n}\frac{(\sqrt{t}R_i-r_i')^2}{1/2+u}\leq\gamma\right]\leq O(\varepsilon_{\text{att}}), \tag{7.20}$$

using that the probability on the left hand side is upper bounded by the probability in (7.19). The required number of rounds n can be obtained by first setting the tolerated ε_{att} and then solving $n\Delta^2=\Omega\big(\frac{1}{\varepsilon_{\text{att}}}\big)$ for n. Then we accept the honest prover with probability at least $1-\varepsilon_{\text{hon}}$, while accepting attackers with probability at most ε_{att} after n i.i.d. rounds.

7.4 Entanglement attack

Our protocol can be attacked if Alice and Bob pre-share just one CV EPR pair. The entanglement attack proceeds as follows:

1. Alice and Bob pre-share an ideal EPR pair.

2. Alice teleports $|\psi\rangle$ to Bob. She forwards the measured displacement (d_x, d_p) to Bob.

[1] In the regime where $\Delta > 0$, which is the case for $u \lesssim 2/e - 1/2 \approx 0.24$ for sufficiently large n where $\gamma \approx 1$. This value can also be observed in Figure 7.2 at $t = 1$.

3. Bob intercepts θ and immediately performs a homodyne measurement under angle θ on his own half of the EPR pair, obtaining outcome $\mu \in \mathbb{R}$. He forwards θ, μ to Alice.

4. Alice receives θ, μ. She computes $r' = \mu - d_x \cos\theta - d_p \sin\theta$ and sends r' to V_0.

5. Bob receives d_x, d_p. He computes $r' = \mu - d_x \cos\theta - d_p \sin\theta$ and sends r' to V_1.

The state $|\psi\rangle$ is a coherent state with displacement (x_0, p_0). The effect of the teleportation is that Bob's half of the EPR pair becomes a coherent state with displacement $(x_0 + d_x, p_0 + d_p)$. Bob's homodyne measurement commutes with the displacement induced by teleportation: the undoing of the displacement can be done *after* Bob's measurement. The noise in r' with respect to r is just shot noise, exactly as for the honest prover. Other noises originating from loss or excess noise can just be simulated by the attacker.

Hence, in the case of an ideal pre-shared EPR pair, the responses from the attackers are statistically indistinguishable from honest prover responses.

7.5 Discussion

The security analysis of CV-QPV differs from the usual discrete variable case, since the honest prover now responds with a sample from a probability distribution. Thus, to prove security (in the setting without pre-shared entanglement), we needed to show that an attack necessarily produces a different distribution than the honest one and that the verifiers can distinguish these distributions. We have shown that this can be done using an entropic uncertainty relation for the differential entropy together with a continuum version of the Fano inequality. We included attenuation and excess noise in the honest channel and showed security for a small range of parameters. We further showed that the considered CV-QPV protocol is broken if one CV EPR pair is pre-shared between the attackers.

Since continuous-variable systems have some practical advantages over discrete ones, we hope that this work may spur interest into the further study of QPV in the context of continuous variables, and we hope our techniques can be useful there.

We have also extended this protocol to the case where the classical information θ is computed via a function $f(x, y)$ taking inputs x, y from both verifiers, similar to the discrete variable $\mathrm{QPV}^{f}_{\mathrm{BB84}}$ protocol [BCS22], studied entanglement attacks on it and further generalised results from discrete variable QPV to CV-QPV. The results can be found in [AEFR+24].

More generally, one may ask how far results on QPV for discrete variable protocols generalise or naturally carry over to the CV setting. For example,

can the recent formulation of CV port-based teleportation [PBP23] be used to immediately reformalise the general attack on discrete variable QPV [BK11] in the CV setting? Do the known attacks, which scale with properties of circuit decompositions of the prover's unitary [Spe16a, DC22b], naturally generalise, for example, to CV equivalents of T-count or T-depth?

Bibliography

[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*, 2023. arXiv:2312.12614.

[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. doi:10.22331/q-2024-06-27-1387.

[ABSV21] Rene Allerstorfer, Harry Buhrman, Florian Speelman, and Philip Verduyn Lunel. Towards practical and error-robust quantum position verification. *arXiv preprint*, 2021. arXiv:2106.12911.

[ABSV22] 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*, 2022. arXiv:2311.00677.

[ACCM24] Vahid Asadi, Richard Cleve, Eric Culf, and Alex May. Linear gate bounds against natural functions for position-verification. *arXiv preprint*, 2024. arXiv:2402.18648.

[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*, 2023. arXiv:2309.16655.

[ACH+24] Harriet Apel, Toby Cubitt, Patrick Hayden, Tamara Kohler, and David Pérez-García. Security of position-based quantum cryptogra-

phy limits Hamiltonian simulation via holography. *arXiv preprint*, 2024. arXiv:2401.09058.

[ACM24] Vahid Asadi, Eric Culf, and Alex May. Rank lower bounds on non-local quantum computation. *arXiv preprint*, 2024. arXiv:2402.18647.

[AEFR+24] Rene Allerstorfer, Llorenç Escolà-Farràs, Arpan Akash Ray, Boris Škorić, and Florian Speelman. Continuous-variable quantum position verification secure against entangled attackers. *arXiv preprint*, 2024. arXiv:2404.14261.

[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*, 2023. arXiv:2308.04166.

[AGLL24] Prabhanjan Ananth, Vipul Goyal, Jiahui Liu, and Qipeng Liu. Unclonable secret sharing. *arXiv preprint*, 2024. arXiv:2406.11008.

[ApS20] MOSEK ApS. Mosek optimizer API for Python. *Software Package*, Version 9, 2020.

[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. doi:10.1063/5.0023103.

[Azu67] Kazuoki Azuma. Weighted sums of certain dependent random variables. *Tohoku Mathematical Journal*, 19(3), 1967. doi:10.2748/tmj/1178243286.

[BB84] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Proc. IEEE Int. Conf. on Computers, Systems, and Signal Process (Bangalore)*, 1984. doi:10.1016/j.tcs.2014.05.025.

[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*, 70:1895–1899, 1993. doi:10.1103/PhysRevLett.70.1895.

[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. doi:10.1137/130913687.

[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. doi:10.1038/s41567-022-01577-0.

[BCWdW01] Harry Buhrman, Richard Cleve, John Watrous, and Ronald de Wolf. Quantum fingerprinting. *Physical Review Letters*, 87(16):167902, 2001. doi:10.1103/PhysRevLett.87.167902.

[BDF+99] Charles H. Bennett, David P. DiVincenzo, Christopher A. Fuchs, Tal Mor, Eric Rains, Peter W. Shor, John A. Smolin, and William K. Wootters. Quantum nonlocality without entanglement. *Physical Review A*, 59:1070–1091, 1999. doi:10.1103/PhysRevA.59.1070.

[BDM+99] Charles H. Bennett, David P. DiVincenzo, Tal Mor, Peter W. Shor, John A. Smolin, and Barbara M. Terhal. Unextendible product bases and bound entanglement. *Physical Review Letters*, 82(26):5385, 1999. doi:10.1103/PhysRevLett.82.5385.

[BDSW96] Charles H. Bennett, David P. DiVincenzo, John A. Smolin, and William K. Wootters. Mixed-state entanglement and quantum error correction. *Physical Review A*, 54:3824–3851, 1996. doi:10.1103/PhysRevA.54.3824.

[Bel64] John S. Bell. On the Einstein Podolsky Rosen paradox. *Physics Physique Fizika*, 1(3):195, 1964. doi:10.1103/PhysicsPhysiqueFizika.1.195.

[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. doi:10.1145/2422436.2422455.

[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. doi:10.1088/1367-2630/13/9/093036.

[BKMS06] Raymond G. Beausoleil, Adrian Kent, William J. Munro, and Timothy P. Spiller. Tagging systems, US patent 7075438, 2006.

[BM95] Samuel L. Braunstein and A. Mann. Measurement of the Bell operator and quantum teleportation. *Physical Review A*, 51:R1727–R1730, 1995. doi:10.1103/PhysRevA.51.R1727.

[Bro16] Anne Broadbent. Popescu-Rohrlich correlations imply efficient instantaneous nonlocal quantum computation. *Physical Review A*, 94(2):022318, 2016. doi:10.1103/PhysRevA.94.022318.

[CBTW17] Patrick J. Coles, Mario Berta, Marco Tomamichel, and Stephanie Wehner. Entropic uncertainty relations and their applications. *Reviews of Modern Physics*, 89(1):015002, 2017. doi:10.1103/RevModPhys.89.015002.

[CCJP10] S. R. Clark, A. J. Connor, D. Jaksch, and S. Popescu. Entanglement consumption of instantaneous nonlocal quantum measurements. *New Journal of Physics*, 12(8):083034, 2010. doi:10.1088/1367-2630/12/8/083034.

[CDP11] Giulio Chiribella, Giacomo Mauro D'Ariano, and Paolo Perinotti. Informational derivation of quantum theory. *Physical Review A*, 84(1):012311, 2011. doi:10.1103/PhysRevA.84.012311.

[CGMO09] Nishanth Chandran, Vipul Goyal, Ryan Moriarty, and Rafail Ostrovsky. Position-based cryptography. In *Advances in Cryptology – CRYPTO 2009*, pages 391–407, 2009. doi:10.1007/978-3-642-03356-8_23.

[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. doi:10.1103/PhysRevA.103.023705.

[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. doi:10.1002/adom.201600665.

[CKPG23] George Cowperthwaite, Adrian Kent, and Damian Pitalua-Garcia. Towards practical quantum position verification. *arXiv preprint*, 2023. arXiv:2309.10070.

[CL01] John Calsamiglia and Norbert Lütkenhaus. Maximum efficiency of a linear-optical Bell-state analyzer. *Applied Physics B*, 72(1):67–71, 2001. doi:10.1007/s003400000484.

[CL15] Kaushik Chakraborty and Anthony Leverrier. Practical position-based quantum cryptography. *Physical Review A*, 92(5), 2015. doi:10.1103/PhysRevA.92.052304.

[CLM+14] Eric Chitambar, Debbie Leung, Laura Mančinska, Maris Ozols, and Andreas Winter. Everything you always wanted to know about LOCC (but were afraid to ask). *Communications in Mathematical Physics*, 328(1):303–326, 2014. doi:10.1007/s00220-014-1953-9.

[CLM+21] Matthias Christandl, Felix Leditzky, Christian Majenz, Graeme Smith, Florian Speelman, and Michael Walter. Asymptotic performance of port-based teleportation. *Communications in Mathematical Physics*, 381:379–451, 2021. doi:10.1007/s00220-020-03884-0.

[CM23] Joy Cree and Alex May. Code-routing: A new attack on position verification. *Quantum*, 7:1079, 2023. doi:10.22331/q-2023-08-09-1079.

[CNN24] CNN News. Finance worker pays out $25 million after video call with deepfake 'chief financial officer', 2024. Accessed: 29.06.2024. URL: https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html.

[Cos13] Alessandro Cosentino. PPT-indistinguishable states via semidefinite programming. *Physical Review A*, 87(1):012321, 2013. doi:10.1103/PhysRevA.87.012321.

[Cov99] Thomas M. Cover. *Elements of information theory*. John Wiley & Sons, 1999.

[CŚ06] Benoît Collins and Piotr Śniady. Integration with respect to the haar measure on unitary, orthogonal and symplectic group. *Communications in Mathematical Physics*, 264(3):773–795, 2006. doi:10.1007/s00220-006-1554-3.

[CW04] Matthias Christandl and Andreas Winter. 'Squashed entanglement': An additive entanglement measure. *Journal of Mathematical Physics*, 45(3):829–840, 2004. doi:10.1063/1.1643788.

[DC22a] Kfir Dolev and Sam Cree. Holography as a resource for non-local quantum computation. *arXiv preprint*, 2022. arXiv:2210.13500.

[DC22b] Kfir Dolev and Sam Cree. Non-local computation of quantum circuits with small light cones. *arXiv preprint*, 2022. arXiv:2203.10106.

[Del19] Delmic. Time-resolved cathodoluminescence: Reveal emission lifetime dynamics, 2019. Accessed: 29.04.2024. URL: https://tinyurl.com/mr4xc7jw.

[Dol19] Kfir Dolev. Constraining the doability of relativistic quantum tasks. *arXiv preprint*, 2019. arXiv:1909.05403.

[DS21] Siddhartha Das and George Siopsis. Practically secure quantum position verification. *New Journal of Physics*, 23(6):063069, 2021. doi:10.1088/1367-2630/ac0755.

[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. doi:10.1098/rspa.2004.1372.

[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. doi:10.1103/PhysRevLett.131.140802.

[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, 2021. doi:10.1364/oe.423142.

[FBT+14] Fabian Furrer, Mario Berta, Marco Tomamichel, Volkher B. Scholz, and Matthias Christandl. Position-momentum uncertainty relations in the presence of quantum memory. *Journal of Mathematical Physics*, 55(12), 2014. doi:10.1063/1.4903989.

[FTH23] Jiani Fei, Sydney Timmerman, and Patrick Hayden. Efficient quantum algorithm for port-based teleportation. *arXiv preprint*, 2023. arXiv:2310.01637.

[GALC23] Ian George, Rene Allerstorfer, Philip Verduyn Lunel, and Eric Chitambar. Time-constrained local quantum state discrimination. *arXiv preprint*, 2023. arXiv:2311.00677.

[GBO23] Dmitry Grinko, Adam Burchardt, and Maris Ozols. Efficient quantum circuits for port-based teleportation. *arXiv preprint*, 2023. arXiv:2312.03188.

[GC20] Alvin Gonzales and Eric Chitambar. Bounds on Instantaneous Nonlocal Quantum Computation. *IEEE Transactions on Information Theory*, 66(5):2951–2963, 2020. doi:10.1109/TIT.2019.2950190.

[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, 2013. doi:10.1103/PhysRevA.87.052330.

[GLW16] Fei Gao, Bin Liu, and QiaoYan Wen. Quantum position verification in bounded-attack-frequency model. *SCIENCE CHINA Physics, Mechanics & Astronomy*, 59:1–11, 2016. doi:10.1007/s11433-016-0234-0.

[GPS07] Raul Garcia-Patron Sanchez. *Quantum information with optical continuous variables: from Bell tests to key distribution*. PhD thesis, Université libre de Bruxelles, 2007.

[Had09] Robert H. Hadfield. Single-photon detectors for optical quantum information applications. *Nature Photonics*, 3(12):696–705, 2009. doi:10.1038/nphoton.2009.230.

[Har01] Lucien Hardy. Quantum theory from five reasonable axioms. *arXiv preprint*, 2001. arXiv:quant-ph/0101012.

[Har11] Lucien Hardy. Reformulating and reconstructing quantum theory. *arXiv preprint*, 2011. arXiv:1104.2066.

[Hay16] Masahito Hayashi. *Quantum information theory*. Springer, 2016. doi:10.1007/978-3-662-49725-8.

[HBD+15] Bas Hensen, Hannes Bernien, Anaïs E. Dréau, Andreas Reiserer, Norbert Kalb, Machiel S. Blok, Just Ruitenberg, Raymond F. L. Vermeulen, Raymond N. Schouten, Carlos Abellán, et al. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526(7575):682–686, 2015. doi:10.1038/nature15759.

[HHH99] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. General teleportation channel, singlet fraction, and quasidistillation. *Physical Review A*, 60:1888–1898, 1999. doi:10.1103/PhysRevA.60.1888.

[HOM87] C. K. Hong, Z. Y. Ou, and L. Mandel. Measurement of subpicosecond time intervals between two photons by interference. *Physical Review Letters*, 59:2044–2046, 1987. doi:10.1103/PhysRevLett.59.2044.

[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.

[IH08] Satoshi Ishizaka and Tohya Hiroshima. Asymptotic teleportation scheme as a universal programmable quantum processor. *Physical review letters*, 101(24):240501, 2008. doi:10.1103/PhysRevLett.101.240501.

[IH09] Satoshi Ishizaka and Tohya Hiroshima. Quantum teleportation scheme by selecting one of multiple output ports. *Physical Review A*, 79:042306, 2009. doi:10.1103/PhysRevA.79.042306.

[JAC04] Igor Jex, Erika Andersson, and Anthony Chefles. Comparing the states of many quantum systems. *Journal of Modern Optics*, 51(4):505–523, 2004. doi:10.1080/09500340408238064.

[JKPP22] Marius Junge, Aleksander M. Kubicki, Carlos Palazuelos, and David Pérez-García. Geometry of banach spaces: A new route towards position based cryptography. *Communications in Mathematical Physics*, 394(2):625–678, 2022. doi:10.1007/s00220-022-04407-9.

[Ken11] Adrian Kent. Quantum tagging for tags containing secret classical data. *Physical Review A*, 84:022335, 2011. doi:10.1103/PhysRevA.84.022335.

[Ken12] Adrian Kent. Quantum tasks in Minkowski space. *Classical and Quantum Gravity*, 29(22):224013, 2012. doi:10.1088/0264-9381/29/22/224013.

[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(1):012326, 2011. doi:10.1103/PhysRevA.84.012326.

[Kra71] Karl Kraus. General state changes in quantum theory. *Annals of Physics*, 64(2):311–335, 1971. doi:10.1016/0003-4916(71)90108-4.

[KRS09] Robert König, Renato Renner, and Christian Schaffner. The operational meaning of min-and max-entropy. *IEEE Transactions on Information theory*, 55(9):4337–4347, 2009. doi:10.1109/tit.2009.2025545.

[KWW12] Robert König, Stephanie Wehner, and Jürg Wullschleger. Unconditional security from noisy quantum storage. *IEEE Transactions*

on Information Theory, 58(3):1962–1984, 2012. doi:10.1109/TIT.2011.2177772.

[Lan91] Rolf Landauer. Information is physical. *Physics Today*, 44(5):23–29, 1991. doi:10.1063/1.881299.

[LL11] Hoi Kwan Lau and Hoi Kwong Lo. Insecurity of position-based quantum cryptography protocols against entanglement attacks. *Physical Review A*, 83(1):012322, 2011. doi:10.1103/PhysRevA.83.012322.

[LLQ22] Jiahui Liu, Qipeng Liu, and Luowen Qian. Beating classical impossibility of position verification. In *13th Innovations in Theoretical Computer Science Conference (ITCS 2022)*, volume 215 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 100:1–100:11. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2022. doi:10.4230/LIPIcs.ITCS.2022.100.

[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. doi:10.1364/OL.44.005262.

[LM00] Beatrice Laurent and Pascal Massart. Adaptive estimation of a quadratic functional by model selection. *Annals of statistics*, pages 1302–1338, 2000. doi:10.1214/aos/1015957395.

[Lou00] R. Loudon. *The Quantum Theory of Light*. OUP Oxford, 2000. doi:10.1093/oso/9780198501770.001.0001.

[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. doi:10.1063/1.5046962.

[LVW17] Tianren Liu, Vinod Vaikuntanathan, and Hoeteck Wee. Conditional disclosure of secrets via non-linear reconstruction. In *Advances in Cryptology – CRYPTO 2017*, pages 758–790, 2017. doi:10.1007/978-3-319-63688-7_25.

[LXS+16] Charles C. W. 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*, 94(3):032315, 2016. doi:10.1103/PhysRevA.94.032315.

[MA24] Carl A. Miller and Yusuf Alnawakhtha. Perfect cheating is impossible for single-qubit position verification. *arXiv preprint*, 2024. arXiv:2406.20022.

[Mal10a] Robert A. Malaney. Location-dependent communications using quantum entanglement. *Physical Review A*, 81:042319, 2010. doi:10.1103/PhysRevA.81.042319.

[Mal10b] Robert A. Malaney. Quantum location verification in noisy channels. In *IEEE Global Telecommunications Conference GLOBECOM 2010*, pages 1–6, 2010. doi:10.1109/GLOCOM.2010.5684009.

[May19] Alex May. Quantum tasks in holography. *Journal of High Energy Physics*, 2019(10):1–39, 2019. doi:10.1007/JHEP10(2019)233.

[May22] Alex May. Complexity and entanglement in non-local computation and holography. *Quantum*, 6:864, 2022. doi:10.22331/q-2022-11-28-864.

[MMAPG13] Lluís Masanes, Markus P. Müller, Remigiusz Augusiak, and David Pérez-García. Existence of an information unit as a postulate of quantum theory. *Proceedings of the National Academy of Sciences*, 110(41):16373–16377, 2013. doi:10.1073/pnas.1304884110.

[MMWZ96] Markus Michler, Klaus Mattle, Harald Weinfurter, and Anton Zeilinger. Interferometric Bell-state analysis. *Physical Review A*, 53(3):R1209, 1996. doi:10.1103/PhysRevA.53.R1209.

[MPFB13] Alan Migdall, Sergey V. Polyakov, Jingyun Fan, and Joshua C. Bienfang. *Single-photon generation and detection: Physics and applications*. Academic Press, 2013.

[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. doi:10.1007/JHEP08(2020)132.

[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. doi:10.1063/5.0003320.

[MW16] Ashley Montanaro and Ronald de Wolf. *A Survey of Quantum Property Testing*. Theory of Computing Library, 2016. doi:10.4086/toc.gs.2016.007.

[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. doi:10.1038/s41586-021-03290-z.

[Ngu23] Quynh T. Nguyen. The mixed Schur transform: Efficient quantum circuit and applications. *arXiv preprint*, 2023. arXiv:2310.01613.

[OCCG20] Andrea Olivo, Ulysse Chabaud, André Chailloux, and Frédéric Grosshans. Breaking simple quantum position verification protocols with little entanglement. *arXiv preprint*, 2020. arXiv:2007.15808.

[OHM87] Z. Y. Ou, C. K. Hong, and L. Mandel. Relation between input and output states for a beam splitter. *Optics communications*, 63(2):118–122, 1987. doi:10.1016/0030-4018(87)90271-9.

[PBP23] Jason L. Pereira, Leonardo Banchi, and Stefano Pirandola. Continuous variable port-based teleportation. *Journal of Physics A: Mathematical and Theoretical*, 57(1):015305, 2023. doi:10.1088/1751-8121/ad0ce2.

[PM11] Zbigniew Puchała and Jarosław Adam Miszczak. Symbolic integration with respect to the haar measure on the unitary group. *arXiv preprint*, 2011. arXiv:1109.4244.

[PR94] Sandu Popescu and Daniel Rohrlich. Quantum nonlocality as an axiom. *Foundations of Physics*, 24(3):379–385, 1994. doi:10.1007/BF02058098.

[PV07] Martin B. Plenio and Shashank Virmani. An introduction to entanglement measures. *Quantum Information and Computation*, 7:1–51, 2007. doi:10.26421/QIC7.1-2-1.

[QS15] Bing Qi and George Siopsis. Loss-tolerant position-based quantum cryptography. *Physical Review A*, 91(4):042337, 2015. doi:10.1103/PhysRevA.91.042337.

[RB01] Robert Raussendorf and Hans J. Briegel. A one-way quantum computer. *Physical Review Letters*, 86:5188–5191, 2001. doi:10.1103/PhysRevLett.86.5188.

[RG15] Jérémy Ribeiro and Frédéric Grosshans. A tight lower bound for the BB84-states quantum-position-verification protocol. *arXiv preprint*, 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. doi:10.1364/OPTICA.400751.

[SIGA05] Valerio Scarani, Sofyan Iblisdir, Nicolas Gisin, and Antonio Acín. Quantum cloning. *Reviews of Modern Physics*, 77:1225–1256, 2005. doi:10.1103/RevModPhys.77.1225.

[SJ09] John M. Senior and M. Yousif Jamro. *Optical fiber communications: principles and practice*. Pearson Education, 2009. doi:10.1063/1.2820238.

[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 für Informatik, 2016. doi:10.4230/LIPIcs.TQC.2016.9.

[Spe16b] Florian Speelman. *Position-based quantum cryptography and catalytic computation*. PhD thesis, University of Amsterdam, Amsterdam, 2016. OCLC: 964061686. URL: https://eprints.illc.uva.nl/id/eprint/2138/.

[Sti55] W. Forrest Stinespring. Positive functions on C*-algebras. *Proceedings of the American Mathematical Society*, 6(2):211–216, 1955. doi:10.2307/2032342.

[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. doi:10.1088/1367-2630/15/10/103002.

[TFVM20] Rahul Trivedi, Kevin A. Fischer, Jelena Vučković, and Kai Müller. Generation of non-classical light using semiconductor quantum dots. *Advanced Quantum Technologies*, 3(1):1900007, 2020. doi:10.1002/qute.201900007.

[TL17] Marco Tomamichel and Anthony Leverrier. A largely self-contained and complete security proof for quantum key distribution. *Quantum*, 1:14, 2017. doi:10.22331/q-2017-07-14-14.

[Tom15] Marco Tomamichel. *Quantum information processing with finite resources: mathematical foundations*. Springer, 2015. doi:10.1007/978-3-319-21891-5_2.

[Unr14] Dominique Unruh. Quantum position verification in the random oracle model. In *Advances in Cryptology – CRYPTO 2014*, pages 1–18, 2014. doi:10.1007/978-3-662-44381-1_1.

[Vai94] Lev Vaidman. Teleportation of quantum states. *Physical Review A*, 49(2):1473, 1994. doi:10.1103/PhysRevA.49.1473.

[Vai03] Lev Vaidman. Instantaneous measurement of nonlocal variables. *Physical Review Letters*, 90:010402, 2003. doi:10.1103/PhysRevLett.90.010402.

[Wat18] John Watrous. *The Theory of Quantum Information*, page 418. Cambridge University Press, 2018. doi:10.1017/9781316848142.

[Wei78] Don Weingarten. Asymptotic behavior of group integrals in the limit of infinite rank. *Journal of Mathematical Physics*, 19(5):999–1001, 1978. doi:10.1063/1.523807.

[Wei94] Harald Weinfurter. Experimental Bell-state analysis. *Europhysics Letters*, 25(8):559, 1994. doi:10.1209/0295-5075/25/8/001.

[Wig32] Eugene Wigner. On the quantum correction for thermodynamic equilibrium. *Physical Review*, 40(5):749, 1932. doi:10.1103/PhysRev.40.749.

[Win99] Andreas Winter. *Coding theorems of quantum information theory*. PhD thesis, Bielefeld University, 1999. arXiv:quant-ph/9907077.

[WZ82] William K. Wootters and Wojciech Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982. doi:10.1038/299802a0.

[YGC12] Li Yu, Robert B. Griffiths, and Scott M. Cohen. Fast protocols for local implementation of bipartite nonlocal unitaries. *Physical Review A*, 85(1):012304, 2012. doi:10.1103/PhysRevA.85.012304.

Abstract

Position-based Quantum Cryptography: From Theory towards Practice. With the possible advent of large-scale fault-tolerant quantum computers in the next decades, one has to think about the implications very carefully. One of the most influential task such quantum computers are capable of is breaking currently widely used asymmetric encryption schemes. So for classical cryptographers, quantum computers provide a headache. On the other hand, quantum physics enables new quantum cryptographic protocols that may be able to provide very strong levels of security. For example, quantum key distribution (QKD) in theory gives unconditional and everlasting security (up to certain thresholds on noise) and could therefore make critical processes unhackable, even for quantum computers.

This thesis deals with such a new quantum-enabled cryptographic primitive: position-based quantum cryptography (PBQC), and in particular quantum position verification (QPV). A comprehensive literature review of the field is provided in Chapter 3. Whether these types of protocols can achieve a similar security standard as QKD in practice is still open and beyond the scope of this thesis, even though much of the research on QPV is motivated by finding such a secure protocol. If one thinks about actually implementing a QPV protocol, or PBQC, it is also essential to consider practical aspects, like signal errors and losses, and check whether the protocol can deal with those or whether it is broken. These were the main guides in the research of this thesis: better understanding attacks on QPV, thinking about the practicality of QPV protocols and designing QPV protocols accordingly. More fundamentally, this led us to study the interplay between non-locality and interaction in the setting of QPV.

First, regarding practicality, we focus on designing and analysing loss-tolerant QPV protocols, mainly thinking about linear-optical hardware for implementations. A detailed study of a practically versatile QPV protocol is given in Chapter 4. There, we introduce a new QPV protocol based on the SWAP test, or, more experimentally speaking, on Hong-Ou-Mandel interference which turns out

to be experimentally feasible and flexible. We study it theoretically, establishing full loss tolerance, security against unentangled attackers and parallel repetition. On the negative side, we also provide an efficient entanglement attack. Moreover, we provide a detailed experimental study, modelling imperfections from source to detection to see whether realistic noisy honest statistics still retain security against unentangled attackers, who can take advantage of some of those imperfections. The bottom line we found was that $\mathrm{QPV}_{\mathrm{SWAP}}$ is robust to a level of errors that can be achieved with current technology. However, this protocol can still be efficiently attacked and is not yet the end of the story.

In Chapter 6 we provide a solution to the last major practical issue of QPV – signal loss. A minor modification of the standard structure of QPV, namely introducing a small time delay and a commitment to play from the honest prover, allows us to provably make the transmission loss between the verifiers and the honest party irrelevant for security. Our proof holds in the robust and most general adversarial setting. The idea is to reduce the security of the protocol with commitment to the underlying one without it. This holds if the underlying QPV protocol is state-independent. In particular, it is true for $\mathrm{QPV}^{f}_{\mathrm{BB84}}$, a protocol that can deal with the other two major issues of QPV – slow quantum communication and attackers with bounded pre-shared entanglement – but is not loss tolerant. The corresponding protocol with commitment, $\mathsf{c}\text{-}\mathrm{QPV}^{f}_{\mathrm{BB84}}$, becomes loss tolerant due to our results in Chapter 6 and thus constitutes the first practically feasible QPV protocol that can deal with all major issues QPV faces for security. We further study experimental aspects of a real implementation and propose a partial linear-optical Bell measurement as the required partial quantum non-demolition measurement.

Chapter 7 generalises the well known $\mathrm{QPV}_{\mathrm{BB84}}$ protocol to the continuous variable setting. Continuous variable quantum states are simpler to handle and much existing telecommunication infrastructure could be reused for them. We show security against unentangled attackers for a parameter regime of attenuation and excess noise, and provide an entanglement attack.

Finally, regarding studying attacks on QPV, we focus on the difference between quantum and classical communication in Chapter 5. First, we prove a new bound on unentangled attacks on $\mathrm{QPV}_{\mathrm{Bell}}$, or in other words, how well one can distinguish Bell states with local operations and one round of simultaneous quantum communication. In general, it is a priori not clear whether quantum communication can give any advantage in the constrained setting of QPV attacks. However, a separation was first shown for an entangled input ensemble in a co-authored paper. In Chapter 5 we study the particular task of discriminating an ensemble of quantum states in the two different settings. We characterise perfect discrimination in each scenario and construct ensembles that are discriminable with quantum communication, but not locally, from quantum secret sharing schemes. Moreover, we show an advantage of quantum communication even for a concrete separable input ensemble. Lastly, we identify a certain structure that leads to a

necessary condition on the error of the state discrimination, which in turn yields non-zero error lower bounds for certain concrete product state ensembles like the domino states. This structure is related to the structure of the BB84 states and, loosely speaking, any state ensemble that contains four states that look like a generalisation of the BB84 states is subject to the necessary condition on the state discrimination error that we derive.

Samenvatting

Positionele Quantum Cryptografie: van Theorie naar Praktijk. Met de mogelijke komst van grootschalige fout-tolerante quantumcomputers in de komende decennia moeten we zeer zorgvuldig nadenken over de implicaties. Een van de meest invloedrijke taken die zulke quantumcomputers kunnen uitvoeren, is het kraken van de motoestanddiscriminatiefoutymmetrische encryptieschema's. Voor klassieke cryptografen zorgen quantumcomputers dus voor hoofdbrekens. Aan de andere kant maakt de quantumfysica nieuwe quantumcryptografische protocollen mogelijk die zeer sterke beveiligingsniveaus kunnen bieden. Bijvoorbeeld, quantum key distribution (QKD) biedt in theorie onvoorwaardelijke en blijvende veiligheid (tot bepaalde drempels op ruis) en zou daarom kritische processen onvervalsbaar kunnen maken, zelfs voor quantumcomputers.

Dit proefschrift behandelt een nieuw quantum-gebaseerde cryptografische primitief: positiebased quantumcryptografie (PBQC), en in het bijzonder quantumpositieverificatie (QPV). Een uitgebreid literatuuroverzicht van het vakgebied wordt gegeven in Hoofdstuk 3. Of deze soorten protocollen in de praktijk een vergelijkbare veiligheidsstandaard als QKD kunnen bereiken, is nog onduidelijk en valt buiten het domein van dit proefschrift, hoewel veel van het onderzoek naar QPV wordt gemotiveerd door het vinden van zo'n veilig protocol. Als men nadenkt over de daadwerkelijke implementatie van een QPV-protocol, of PBQC, is het ook essentieel om praktische aspecten te overwegen, zoals signaalfouten en -verliezen, en te controleren of het protocol daarmee om kan gaan of dat het daardoor wordt doorbroken. Dit zijn de belangrijkste leidraden in het onderzoek van dit proefschrift: een beter begrip krijgen van aanvallen op QPV, nadenken over de praktische toepasbaarheid van QPV-protocollen en het ontwerpen van zulke QPV-protocollen. Meer fundamenteel leidde dit ons ertoe om de wisselwerking tussen non-localiteit en interactie in de context van QPV te bestuderen.

Allereerst richten we ons, met betrekking tot de praktische toepasbaarheid, op het ontwerpen en analyseren van verlies-tolerante QPV-protocollen, waarbij we voornamelijk denken aan lineair-optische hardware voor implementaties. Een

gedetailleerde studie van een praktisch veelzijdig QPV-protocol wordt gegeven in Hoofdstuk 4. Daar introduceren we een nieuw QPV-protocol gebaseerd op de SWAP-test, of, meer experimenteel gesproken, op Hong-Ou-Mandel-interferentie, wat experimenteel gezien zeer eenvoudig en flexibel is. We bestuderen het theoretisch, waarbij we volledige verlies-tolerantie, veiligheid tegen niet-verstrengelde aanvallers en parallelle herhaling vaststellen. Aan de negatieve kant presenteren we ook een efficiënte verstrengelingsaanval. Bovendien bieden we een gedetailleerde experimentele studie, waarbij we onvolkomenheden van bron tot detectie modelleren om te zien of realistische, ruisachtige eerlijke statistieken nog steeds veiligheid bieden tegen niet-verstrengelde aanvallers, die voordeel kunnen halen uit enkele van die onvolkomenheden. Het belangrijkste resultaat dat we vonden was dat $\mathrm{QPV}_{\mathrm{SWAP}}$ robuust is tegen een niveau van fouten dat met de huidige technologie kan worden bereikt. Dit protocol kan echter nog steeds efficiënt worden aangevallen en is nog niet het einde van het verhaal.

In Hoofdstuk 6 bieden we een oplossing voor het laatste grote praktische probleem van QPV: signaalverlies. Een kleine aanpassing van de standaardstructuur van QPV, namelijk het introduceren van een kleine tijdsvertraging en een toezegging om eerlijk te spelen van de eerlijke prover, stelt ons in staat om aantoonbaar het transmissieverlies tussen de verifiers en de eerlijke partij irrelevant te maken voor de beveiliging. Ons bewijs houdt stand in de robuuste en meest algemene vijandige omgeving. Het idee is om de veiligheid van het protocol met toezegging te reduceren tot die van het onderliggende protocol zonder toezegging. Dit is het geval als het onderliggende QPV-protocol staatsonafhankelijk is. In het bijzonder geldt dit voor $\mathrm{QPV}^{f}_{\mathrm{BB84}}$, een protocol dat de andere twee grote problemen van QPV kan oplossen – trage quantumcommunicatie en aanvallers met begrensde vooraf gedeelde verstrengeling – maar niet verlies-tolerant is. Het overeenkomstige protocol met toezegging, $\mathsf{c}\text{-}\mathrm{QPV}^{f}_{\mathrm{BB84}}$, wordt verlies-tolerant dankzij onze resultaten in Hoofdstuk 6 en vormt daarmee het eerste praktisch haalbare QPV-protocol dat alle belangrijke problemen voor beveiliging kan oplossen. We bestuderen verder experimentele aspecten van een daadwerkelijke implementatie en stellen een gedeeltelijke lineair-optische Bell-meting voor als de vereiste gedeeltelijke quantum non-demolition meting.

Hoofdstuk 7 generaliseert het welbekende $\mathrm{QPV}_{\mathrm{BB84}}$ protocol naar het continue variabelen-scenario. Quantumtoestanden met continue variabelen zijn eenvoudiger te hanteren en veel bestaande telecommunicatie-infrastructuur kan voor hen worden hergebruikt. We tonen aan dat er veiligheid is tegen niet-verstrengelde aanvallers voor een parameterregime van verzwakking en overtollige ruis, en we bieden een verstrengelingsaanval.

Ten slotte, wat betreft het bestuderen van aanvallen op QPV, richten we ons op het verschil tussen quantum- en klassieke communicatie in Hoofdstuk 5. Eerst bewijzen we een nieuwe grens op niet-verstrengelde aanvallen op $\mathrm{QPV}_{\mathrm{Bell}}$, of met andere woorden, hoe goed men Bell-toestanden kan onderscheiden met lokale operaties en één ronde van gelijktijdige quantumcommunicatie. Over het

algemeen is het niet direct duidelijk of quantumcommunicatie enig voordeel kan bieden in de gecreëerde setting van QPV-aanvallen. Een scheiding werd echter eerst aangetoond voor een verstrengeld input-ensemble in een co-auteur artikel. In Hoofdstuk 5 bestuderen we de specifieke taak van het onderscheiden van een ensemble van quantumtoestanden in de twee verschillende settings. We karakteriseren perfecte toestanddiscriminatie in elk scenario en construeren ensembles die met quantumcommunicatie onderscheidbaar zijn, maar niet lokaal, vanuit quantumgeheimdelingsschema's. Bovendien tonen we een voordeel van quantumcommunicatie, zelfs voor een concreet scheidbaar input-ensemble. Ten slotte identificeren we een bepaalde structuur die leidt tot een noodzakelijke voorwaarde voor de fout van de toestanddiscriminatie, wat op zijn beurt niet-nul foutondergrenzen oplevert voor bepaalde concrete producttoestandensembles zoals de domino-toestanden. Deze structuur is gerelateerd aan de structuur van de BB84-toestanden en, grofweg gesproken, is elke toestandsensemble die vier toestanden bevat die eruitzien als een generalisatie van de BB84-toestanden onderworpen aan de noodzakelijke voorwaarde voor de toestanddiscriminatiefout die we afleiden.

Titles in the ILLC Dissertation Series:

ILLC DS-2018-12: **Julia Ilin**
Filtration Revisited: Lattices of Stable Non-Classical Logics

ILLC DS-2018-13: **Jeroen Zuiddam**
Algebraic complexity, asymptotic spectra and entanglement polytopes

ILLC DS-2019-01: **Carlos Vaquero**
What Makes A Performer Unique? Idiosyncrasies and commonalities in expressive music performance

ILLC DS-2019-02: **Jort Bergfeld**
Quantum logics for expressing and proving the correctness of quantum programs

ILLC DS-2019-03: **András Gilyén**
Quantum Singular Value Transformation & Its Algorithmic Applications

ILLC DS-2019-04: **Lorenzo Galeotti**
The theory of the generalised real numbers and other topics in logic

ILLC DS-2019-05: **Nadine Theiler**
Taking a unified perspective: Resolutions and highlighting in the semantics of attitudes and particles

ILLC DS-2019-06: **Peter T.S. van der Gulik**
Considerations in Evolutionary Biochemistry

ILLC DS-2019-07: **Frederik Möllerström Lauridsen**
Cuts and Completions: Algebraic aspects of structural proof theory

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-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-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-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

ILLC DS-2024-08: **Philip Verduyn Lunel**
Quantum Position Verification: Loss-tolerant Protocols and Fundamental Limits