Practical Quantum Communication

by

Juan Miguel Arrazola

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Physics - Quantum Information

Waterloo, Ontario, Canada, 2015

This thesis consists of material all of which I authored or co-authored: see Statement of Contributions included in the thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Juan Miguel Arrazola

Statement of Contributions

This thesis is based on work that appears in several published manuscripts, which were the product of a collaborative effort. The specific contributions that I, Juan Miguel Arrazola, have made to these publications are listed below.

Section 3.3 is based on results published in Ref. [7], which was published jointly with Oleg Gittsovich and Norbert Lütkenhaus. The construction of nonlinear witnesses based on the Choi-Jamiolkowski isomorphism is due mainly to OG, while the analytic formula was done jointly by OG and myself while I was a Masters student at the University of Toronto. The proof of the necessary and sufficient conditions for the analytical formula was done by me while I was a PhD student at IQC, with revisions by OG. NL provided supervision for the project.

Chapter 5 is based on results published in Ref. [6], which was published jointly with OG, John Donohue, Jonathan Lavoie, Kevin Resch and NL. JD and JL are responsible for conducting the experiment, writing the description of the experimental setup as well as the corresponding figures. The data analysis procedure and observation 6 were done jointly with OG. All other results are mine. KR and NL provided supervision for the project.

The results presented in Chapter 6 are based on Ref. [9], which was published together with NL. These results are mine, with supervision by NL.

Chapter 7 is based on Ref. [10] which is joint work with NL and [133], which was written together with Feihu Xu, Keijin Wei, Wenyuan Wang, Pablo Palacios-Avila, Chen Feng, Hoi-Kwong Lo and NL. The coherent-state protocol for quantum fingerprinting, in its original version of Ref. [10] and its improvements of Ref. [133] are my work, with inputs from NL. With respect to Ref. [133], FX and KW designed and performed the experiment. The computer algorithm to find the optimal experimental parameters was written jointly by me and PPA. The design of the error-correcting codes was performed jointly with WW and CF. Both WW and CF wrote the computer algorithm to perform the encoding.

Finally, Chapter 8 is based on Ref. [11], written with Petros Wallden and Erika Andersson. The generalization of the P2-WDKA protocol was done mostly by PW, with the security proofs done jointly with me. All other results are mine, with extensive revision and improvements by PW. EA provided supervision for this project.

Abstract

Current communication networks are based on classical physics and classical information-processing. However, for nearly a century, we have known that at its most fundamental level, the universe is governed by the laws of quantum mechanics. With quantum communication, new possibilities arise in our capabilities to transmit and process information which, in many cases, lead to advantages compared to what is classically possible. The entire scope of tasks for which quantum communication can offer improvements has not yet been fully explored, but several quantum protocols are known that can either perform tasks which are impossible with classical resources or can outperform classical protocols. These quantum protocols are well understood from a theoretical point of view, but many of them have never been demonstrated in practice. Thus, in the context of quantum communication, there is a significant gap between theory and experiment that must be removed in order to harness the advantages provided by quantum mechanics in a practical setting.

In this thesis, we develop a series of tools for developing and testing practical quantum communication protocols. Our main technique is a theoretical reformulation of existing quantum communication protocols that converts them into a form in which they can be demonstrated with existing experimental techniques. More precisely, they can be implemented using only coherent states of light and linear optics circuits while still retaining the crucial properties of the original abstract protocols. We use this result to construct practical protocols for the Hidden Matching problem and quantum fingerprinting.

In the case of quantum fingerprinting, we make a thorough analysis of the role played by experimental errors and show that our practical protocol can still be implemented in the presence of these imperfections. In fact, we report a proof of concept experimental demonstration of a quantum fingerprinting system that is capable of transmitting less information than the best known classical protocol for this problem. Our implementation is based on a modified version of a commercial quantum key distribution system using off-the-shelf optical components over telecom wavelengths, and is practical for messages as large as 100 Mbits, even in the presence of experimental imperfections.

Similarly, in the context of cryptography, we propose a multiparty quantum signature protocol that can be implemented from any point-to-point quantum key distribution network, proving its security against forging, repudiation and non-transferability. Crucially, since quantum key distribution is already a practical technology, so is this protocol. However, unlike other tasks in quantum communication, there has not been significant theoretical work on establishing a security model for quantum signature schemes. Consequently, we also constructed a security framework for these schemes and proved several properties that these protocols must satisfy in order to achieve their security goals.

Finally, in addition to proposing new practical protocols, we provide a reliable data analysis technique to verify an important property of many quantum communication protocols: the presence of entanglement. Our technique is based on entanglement witnesses and it does not require the specification of a prior distribution nor the assumption of independent measurements. The technique is suitable to be used with nonlinear entanglement witnesses, which we show can be constructed from any linear witness and evaluated from the same experimental data. We also develop numerical tools necessary to employ this approach in practice, rendering the procedure ready to be applied to current experiments. We demonstrate this by analyzing the data of a photonic experiment generating two-photon states whose entanglement is verified with the use of an accessible nonlinear witness.

Acknowledgements

Nothing I have ever accomplished would have been possible if I had done it all by myself. Throughout my life, I have had the fortune of counting with the support and encouragement of many people who have improved my life immensely. My PhD has been no exception.

I begin by thanking my supervisor Norbert Lütkenhaus. During my time at IQC, he has done so much for me that I am not sure I can do him justice with these words. Norbert has been a magnificent mentor: his knowledge, integrity and guidance have shaped me into a better scientist than I had expected to become. I will always be thankful for his support in my decision to live in Toronto with my wife. I am also thankful for the many opportunities he gave me to present my work in conferences around the world. Norbert is an excellent researcher and an extraordinary person; it has been an honour and a privilege to work alongside him.

Besides Norbert, I would like to thank all of the people I had the fortune to work with: John Donohue, Jonathan Lavoie, Chen Feng, Pablo Palacios-Avila, Kejin Wei, Wenyuan Wang, Shihan Sajeed, Kevin Resch, Erika Andersson, and Hoi-Kwong Lo. In particular, I would like to thank Oleg Gittsovich for sharing his knowledge on entanglement theory and mathematics, Feihu Xu for his hard work and dedication, and Petros Wallden for his help in understanding the security of quantum signature schemes.

I would also like to thank the members of my advisory committee, Kevin Resch, Richard Cleve, Michele Mosca and Marco Piani, for their help and advice. I am particularly grateful to Marco for continuing to give me advice and encouragement even after he left IQC. I would also like to thank Harry Buhrman, Eleni Diamanti, Iordanis Kerenidis, Marcos Curty, Romain Alleaume, Saikat Guha, and Mohsen Razavi for stimulating scientific discussions.

Finally, I would like to thank all the people who have made working as a researcher so enjoyable: Nicolas Quesada, Will Stacey, Koon Tong Goh, Alf Petersson, Agnes Ferenczi, Varun Narasimhachar, Razieh Annabestani, Nathan Killoran, Ryo Namiki, Yanbao Zhang, Patrick Coles, Sumeet Kathri, David Luong, Electra Eleftheriadou, Filippo Miatto, Vadym Kliuchnikov, Alex Valtchev, Sadegh Raeisi, Mike Mazurek, Kent Fisher, Aharon Brodutch, Melissa Floyd, Jodi Szimanski, and Martin Laforest.

Quiero agradecer a mis padres y a mi hermano por apoyarme siempre en mi decisión de convertirme en un científico.

Je remercie Jasmina et Rade Ignjatovic pour leur soutien. Merci d'avoir accuelli un scientifique dans votre famille.

Most importantly, I deeply thank my wife Aleksandra Ignjatovic for giving me the love, the happiness, and the inspiration that make my life fulfilled and give me the strength to surmount even the highest obstacles. Thank you for believing in me in every step of the way, thank you for proofreading every paper I wrote, thank you for all the sacrifices you have made for us, thank you for understanding me even when I am in "physics mode", thank you for making our home the best place to return to, thank you for making me a better person. Thank you, thank you, thank you!

Dedication

To Aleksandra Ignjatovic: my wife, my love, my life, my inspiration, and my best friend. Nothing can stop our love.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

Despite appearances, our universe is entirely governed by the laws of quantum mechanics. Everything is quantum – a simple premise, with profound consequences. When we take this statement seriously, we realize that a mastery of quantum theory is necessary not only to truly understand nature, but also to develop technologies for the betterment of humanity. So far, the role that quantum mechanics has played in new technologies has largely been to explain the classical behaviour of physical systems. For example, the computer that was used to create this thesis contains billions of transistors based on semiconductor devices, the properties of which can only be properly understood with quantum mechanics. However, the operation of the computer is completely classical: it processes classical data and runs classical algorithms.

Nevertheless, we have known for decades that there are tasks that are possible to perform in a world governed by quantum mechanics but are either impossible or believed to be impossible to perform in a classical world [97]. Therefore, there are problems for which quantum mechanics provides an advantage compared to what is classically possible. This raises a series of questions:

1. What is the complete scope of information-processing tasks for which quantum mechanics provides an advantage over the classical case?
2. How can we realize these tasks in practice?
3. Which of these tasks are actually useful?

Answering these questions is important from a fundamental perspective but, most significantly, it can lead to genuine technological breakthroughs. Indeed, if we are able to

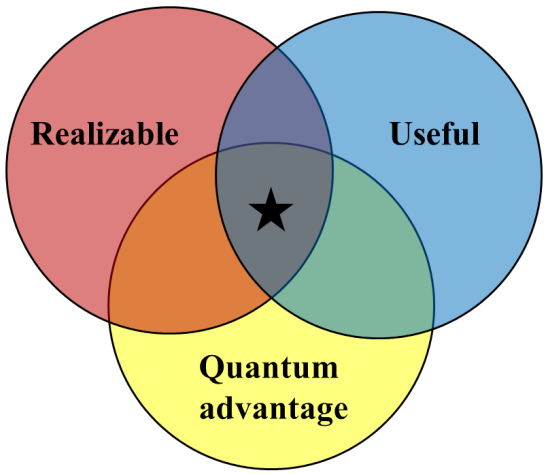


Figure 1.1: An illustration of three different sets of quantum protocols: those that provide a quantum advantage compared to the classical case, those that are useful in practice, and finally, protocols that can be experimentally realized. A significant goal of research in quantum information is to understand and expand the intersection of these three sets.

realize a quantum advantage for useful tasks in practice, we will have entered a new regime of technological capabilities.

Currently, we only have partial answers to these fundamental questions. We know a few examples of tasks for which quantum mechanics provides an advantage, but by no means have we understood all such problems. Similarly, remarkable progress has been made in our ability to control quantum systems, leading to many advances in the experimental demonstration of quantum protocols. However, many challenges remain to scale up many of these protocols and, for other cases, experimental demonstrations have never been achieved. Consequently, significant research efforts are being carried out across the world to theoretically understand all of the advantages which are made possible by quantum mechanics and to experimentally develop the techniques that are necessary to realize them in practice. The ultimate goal is to continue to enlarge the set of protocols that: (i) are useful, (ii) have a quantum advantage and (iii) can be realized in practice, as depicted in Fig. 1.1.

In an experimental setting, when attempting to implement quantum protocols, it is also important to certify that the devices are operating in a regime which cannot be reproduced with purely classical resources. Although there are many different ways of making such

a certification, in many cases it is necessary to demonstrate the presence of entanglement in the physical systems employed. Thus, a crucial component of developing practical quantum protocols is to provide reliable methods to verify that experimental devices are indeed operating in the quantum domain, thus being able to achieve the advantages that are only possible using quantum mechanics.

In this thesis, we present progress towards the goal of developing quantum communication protocols with a quantum advantage that can be experimentally realized. In particular, we focus on quantum protocols in the field of communication complexity and cryptography, and discuss how they can be implemented using available techniques from quantum optics. In chapter 2, we give an overview of the field of quantum communication, focusing on protocols with an advantage over the classical case. In chapter 3 we overview basic concepts in entanglement theory and discuss the role of entanglement in quantum information processing and communication. Additionally, since light is the physical system of choice for realizing communication protocols, in chapter 4 we discuss basic concepts of quantum optics that are necessary to understand the results presented in this thesis.

In chapter 5, we give a reliable data analysis technique for entanglement verification experiments and demonstrate the practicality and properties of this technique by applying it to data generated from an experiment generating entangled states of photonic qubits. Going back specifically to quantum communication, in chapter 6 we introduce a general framework for implementing protocols in quantum communication using standard optical techniques an we apply these techniques to construct new practical protocols in quantum communication. In particular, in chapter 7 we use this framework to build a practical protocol for quantum fingerprinting and we report an experimental demonstration of this protocol which is capable of outperforming the best known classical protocol for this problem. Finally, in chapter 8 we focus on quantum cryptography, outlining a full security framework for quantum signature schemes and introducing a multiparty protocol that can be realized with available experimental techniques.

Chapter 2

Quantum Communication

2.1 Quantum versus classical communication

For centuries, humanity has been concerned with developing methods of transmitting information across large distances. Communication technologies have increased in efficiency and sophistication, to the point that the planet is now intricately connected through the Internet, allowing fast and reliable communication between people located virtually anywhere in the world.

We focus on the simplest communication scenario in which two parties – Alice and Bob – wish to exchange a message. A series of questions arise, for instance:

1. What physical systems should they use in order to transmit these messages?
2. How can they minimize the resources required to communicate?
3. How should they deal with errors affecting their transmission?

In classical communication, answers to such questions are provided within the framework of classical information and classical physics. From an abstract point of view, we model the situation by considering the set X of possible messages $\{1, 2, 3, \ldots, M\}$ that Alice may transmit to Bob. Equivalently, it is customary to view this as the set of n-bit strings, namely $X = \{0, 1\}^n$, where $n = \lceil \log_2 M \rceil$ is the smallest integer larger than $\log_2 M$. Thus, we quantify the size of the set of messages in units of bits.

In order to actually transmit a message $x \in X$, Alice and Bob must encode the message in a physical system with M different distinguishable configurations. For example, they

could choose M different characters written on a piece of paper and transport the paper across the distance separating them. A more modern alternative is to choose two easily distinguishable states of an optical field and use them to encode one bit of information. Larger messages can be constructed by concatenating these single bits to form a larger string. In general, Alice and Bob will choose a physical realization of a classical bit and use that to transmit arbitrary messages across the underlying physical channel. For a particular task at hand, Alice and Bob should then choose the best protocol and physical encodings suitable for their needs.

The crucial point of this scenario is that its mathematical model is based on classical probability and information theory. Similarly, the physical systems used to encode the information are assumed to be describable by classical physics. Consequently, the capabilities of Alice and Bob will be restricted to that which is possible within such a framework. But for nearly a hundred years, we have known that at its most fundamental level, the universe is governed by the laws of quantum mechanics, so it is only natural to ask: Can Alice and Bob use quantum mechanics to their advantage?

Let us re-visit the previous scenario but from a quantum perspective. As before, Alice and Bob wish to transmit a classical message $x \in X$, but now they are allowed to send *quantum* signals to each other. From an abstract point of view, what this means is that Alice and Bob are in general allowed to send superpositions of all M distinguishable states, namely quantum states of the form

$$|\psi\rangle = \sum_{i=1}^{M} \lambda_i |i\rangle, \tag{2.1}$$

where the coefficients λ_i are complex numbers satisfying $\sum_{i=1}^{M} |\lambda_i|^2 = 1$ and $\langle i|j\rangle = \delta_{i,j}$. We can equivalently think of such states as arising from a collection of $n = \lceil \log_2 M \rceil$ qubits, i.e. two-level quantum systems, in which case we would write

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} \lambda_x |x\rangle, \tag{2.2}$$

where $|x\rangle := |x_1\rangle|x_2\rangle \cdots |x_n\rangle$ and x_i is the i-th bit of the string x. To encode these states in physical systems, Alice and Bob can once again choose a system with M distinguishable states, but this time, they must also be able to prepare superpositions of these states.

In a more general setting, Alice can prepare mixed states of the form

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|, \tag{2.3}$$

where $p_i \geq 0$, $\sum_i p_i = 1$ and the states $|\psi_i\rangle$ are quantum states as in Eq. (2.2). On Bob's side, he is allowed to make general measurements, which we describe by a set of positive semi-definite operators $\{E_i\}$ satisfying $\sum_i E_i = \mathbb{1}$.

So how can quantum communication help Alice and Bob? The first thing to notice is that it certainly cannot hurt them! Indeed, they can always go back to the classical case by preparing and transmitting states of the form $|\psi\rangle = |x\rangle$, with Bob measuring in the canonical basis given by all such states $|x\rangle$. By glimpsing at Eq. (2.2), it is natural to wonder whether it is possible to transmit an n-bit classical message using *less* than n-qubits of quantum communication.

To put this formally, suppose that Alice wishes to transmit a classical message $x \in \{0,1\}^n$ which we denote as a classical random variable X whose possible values occur with corresponding probability $p(x)$. To transmit a message x to Bob, Alice prepares a generally mixed state ρ_x and sends it to Bob. Thus, Alice's strategy is uniquely defined by the ensemble

$$\mathcal{E} = \{p(x), \rho_x\}. \tag{2.4}$$

Upon receiving the state from Alice, Bob performs a POVM measurement given by the operators $\{E_y\}$. Thus, Bob associates with his measurement a random variable Y. The joint probability distribution of Alice and Bob's variables is then given by

$$p(x,y) = p(x)\mathrm{Tr}\left(\rho_x E_y\right). \tag{2.5}$$

We can use this joint distribution to calculate the mutual information between X and Y, which is given by

$$I(X:Y) = H(X) + H(Y) - H(X,Y), \tag{2.6}$$

where $H(X) = -\sum_x p(x)\log_2 p(x)$ is the Shannon entropy of the variable X. Informally, the mutual information quantifies the information that Bob learns about X – on average and in the limit of many repetitions – after learning the value of Y. For a formal treatment of the mutual information and its role in quantum communication, see Ref. [130].

Since the correlations of Eq. (2.5) depend on Bob's measurement, in general we should focus on the maximum mutual information that can be achieved when considering all of Bob's measurements on Alice's ensemble. In that case, we refer to the *accessible information*, which is defined as

$$I_{acc}(\mathcal{E}) = \max_{\{E_y\}} I(X:Y). \tag{2.7}$$

If Alice and Bob were to use a quantum strategy in order to transmit n classical bits with less than n qubits, they would require that $I_{acc}(\mathcal{E})$ be larger or equal than n bits and that

the quantum states ρ_x are states of less than n qubits. Although it is difficult in general to compute $I_{acc}(\mathcal{E})$ exactly, the following upper bound was proven by Holevo in Ref. [69]:

Theorem 1. *For a given ensemble $\mathcal{E} = \{p(x), \rho_x\}$ it holds that*

$$I_{acc}(\mathcal{E}) \leq S(\rho) - \sum_x p(x) S(\rho_x) := \chi(\mathcal{E}), \tag{2.8}$$

where $\rho = \sum_x p(x)\rho_x$ and $S(\rho) = -Tr(\rho \log_2 \rho)$ is the Von Neumann entropy.

The function $\chi(\mathcal{E})$ is known as the Holevo quantity.

From this bound, we can straightforwardly show that in order to transmit n bits of information, Alice and Bob must necessarily use states of n qubits. To see this, note that in order to maximize the accessible information, Alice should choose an ensemble that maximizes the Holevo quantity $\chi(\mathcal{E})$. If Alice chooses an ensemble of pure states, it holds that $\chi(\mathcal{E}) = S(\rho)$. Similarly, for a system of n qubits, it holds that $S(\rho) \leq n$ which implies that $I_{acc}(\mathcal{E}) \leq n$. Therefore, n qubits cannot be used to transmit more than n bits of information.

Although this result may seem disheartening, there are still several tasks for which quantum communication can provide an advantage compared to the classical case. For the time being, we can extract a valuable lesson from Holevo's theorem: it is fair to compare bits and qubits when quantifying communication. For example, in section 2.3, we take a look at certain tasks for which it is possible to use less qubits than classical bits. In that case, we can really talk about less information being transmitted, since, in view of Holevo's theorem, this smaller number of qubits is insufficient to transmit the larger number of classical bits required.

Before we take a closer look at tasks for which quantum communication can provide an advantage over the classical case, let us evaluate some of the features of quantum communication that differ from what is classically possible.

1. Non-orthogonality. In classical communication, all possible messages of n-bit strings $x \in \{0,1\}^n$ are perfectly distinguishable, meaning that we can tell them apart perfectly. In the language of quantum mechanics, what this means is that any two different classical states $|x\rangle$ and $|y\rangle$ are *orthogonal*, i.e. $\langle x|y\rangle = 0$ for any $x, y \in \{0,1\}^n$ and $x \neq y$. In quantum mechanics, it is possible to prepare non-orthogonal pure states, i.e. states $|\psi\rangle$ and $|\phi\rangle$ such that $|\langle\psi|\phi\rangle| \neq 0$.

For instance, consider the case of a single bit. Classically, Alice's only two choices are to prepare the states $|0\rangle$ and $|1\rangle$, perhaps with some prior probability. However, quantum

mechanically, any superposition of these two states is also possible. For instance, Alice could prepare the states

$$|\pm\rangle := \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle), \tag{2.9}$$

which are not orthogonal to the states $|0\rangle$ and $|1\rangle$. Fundamentally, it is impossible for Bob to distinguish non-orthogonal states perfectly with a single measurement. For example, suppose that Alice were to send either $|0\rangle$ or $|+\rangle$ to Bob, choosing between both options with equal probability. Then there is no measurement that Bob can make that will allow him to distinguish between these options with unit probability [68].

Additionally, it is important to understand that when Alice sends the state $|+\rangle$, the situation is fundamentally different from the case in which she prepares a classical random bit, i.e. $|0\rangle$ and $|1\rangle$ with probability $\frac{1}{2}$. If Bob measures in the $\{|0\rangle,|1\rangle\}$ basis, the statistics are indeed equal for the state $|+\rangle$ and the classical random bit. But if he measures in the $\{|+\rangle,|-\rangle\}$ basis, the classical random bit will lead to equal probabilities of observing both outcomes while the state $|+\rangle$ leads to a deterministic outcome.

Non-orthogonality leads directly to properties unique to the quantum regime, such as uncertainty relations [128] and no-cloning of unknown quantum states [131], which can be very useful particularly in the context of cryptography. We revisit the role of non-orthogonality in quantum communication in chapter 6.

2. Entanglement. Suppose that Alice holds a four-dimensional system, whose general state can be written as $|\psi\rangle = \sum_{i=1}^{4} \lambda_i |i\rangle$. As before, if we think of this state as being composed of two qubits, we can equivalently write the state as $|\psi\rangle = \sum_{x\in\{0,1\}^2} \lambda_x |x_1\rangle|x_2\rangle$. For example, Alice could prepare the state

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_{A'} + |1\rangle_A|1\rangle_{A'}), \tag{2.10}$$

where we have explicitly labelled each of Alice's qubits as A and A'. So far, we have restricted our attention to the case in which Alice sends Bob all of her quantum systems. But suppose that instead she sent Bob only qubit A'. In that case, they would both share the state

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B), \tag{2.11}$$

where we have made it explicit that the second qubit is in Bob's possession. As we discuss in chapter 3, this is an example of an *entangled* state.

Entanglement allows for stronger correlations between Alice and Bob than what can be achieved with classical random variables. For instance, if Alice and Bob measure the state $|\Phi^+\rangle$ in the $\{|0\rangle, |1\rangle\}$ basis, both of them will always obtain the same outcome. Of course, this would also happen if they instead had prepared $|0\rangle|0\rangle$ or $|1\rangle|1\rangle$ with probability $\frac{1}{2}$. However, for such a classically correlated state, if Alice and Bob measured in the $\{|+\rangle, |-\rangle\}$ basis, they would obtain uncorrelated outcomes. Instead, for the entangled state $|\Phi\rangle$, which can be written as $|\Phi\rangle = \frac{1}{\sqrt{2}}(|+\rangle_A|+\rangle_B + |-\rangle_A|-\rangle_B)$, they will again obtain perfectly correlated outcomes.

Entanglement plays an important role in many quantum communication problems as well as in other areas of quantum information and computation. We discuss such applications more extensively in chapter 3.

3. Quantum Computation. In our simplified model of communication between Alice and Bob, we have only focused on the transmission of signals between them. However, Alice and Bob can also manipulate and process the data they receive. In general, upon receiving a classical message x, they can run an arbitrary classical computation whose input is the message x. Once quantum communication is allowed, the type of computations that Alice and Bob can perform also get upgraded to the quantum domain. As before, this can only help them, since a quantum computer can always simulate a classical one. However, there exist situations where the additional possibilities brought forward by quantum computation will be beneficial for them. We study such scenarios closely in section 2.3.

In summary, despite some limitations, quantum mechanics provides new and exciting possibilities for communication. Our goal in the next sections is to study concrete examples of tasks for which quantum communication provides an advantage compared to the classical case.

2.2 Quantum cryptography

Let us re-examine the previous situation where Alice and Bob want to exchange a message, but this time let us ask a different type of question: How can Alice and Bob communicate in such a way that no other party can learn the content of their messages? In asking this question we are now demanding *security* in the communication. This is precisely the scope of cryptography: the study of secure communication. In the simple example above, Alice and Bob are concerned with preventing a third party from learning the content of their messages, but security can take on different forms. For instance, Alice could be interested in ensuring that no malicious party can modify the message she sends to Bob.

So how can quantum communication help cryptography? Arguably the first person to realize that quantum communication was useful for cryptography was Wiesner, with pioneering work in the 1970's [129]. Although quantum cryptography was initially met with skepticism, several breakthroughs soon followed [18, 52]. In particular, Shor's factoring algorithm [113] – which represented a threat to classical encryption methods – catapulted quantum cryptography into a flourishing and active research field. In the following, we provide a brief overview of some important protocols in quantum cryptography.

2.2.1 Quantum key distribution

Suppose that Alice wants to send Bob an n-bit message $x \in \{0,1\}^n$ in such a way that Bob recovers x perfectly, but no other person can learn anything about x. There is a simple classical protocol – the one-time pad – that allows them to achieve this goal. In the protocol, Alice and Bob must share a secret key k of n-bits drawn uniformly at random from the set $\{0,1\}^n$. In order to secretly transmit any given message x, Alice performs bit-wise modulo 2 addition of the message and key to produce the cryptogram $c = x \oplus k$, which she sends to Bob. To decode the encrypted message, Bob similarly performs addition of the cryptogram and his shared copy of the key to retrieve the message $c \oplus k = x$. Intuitively, since the secret key is completely random, an eavesdropper learns nothing about x from the cryptogram c, allowing Alice and Bob to communicate securely. In this case, we refer to the protocol as being *information-theoretically* secure.

The one-time pad protocol reduces the problem of secrecy in communication to that of distributing secret keys. But how can Alice and Bob manage to share a key that is completely unknown to an adversary? It can be shown that it is impossible to establish a secret key with information-theoretic security when only classical communication is allowed [111, 90]. However, once quantum communication is permitted, secret keys can in fact be distributed with information-theoretic security through the use of insecure quantum channels and authenticated classical channels. *Quantum key distribution* (QKD) is the study of how two remote parties can use quantum communication to establish a shared secret key.

To see how this is possible, we express the ideal scenario of a shared secret key directly in a quantum formalism. If Alice and Bob share a state of the form

$$\rho_{AB} = \frac{1}{2^n} \sum_{k \in \{0,1\}^n} |k\rangle\langle k|_A \otimes |k\rangle\langle k|_B \tag{2.12}$$

then a measurement by each of them in the $\{|k\rangle\}$ basis will result in a shared key drawn uniformly at random from the set of all n-bit strings. This takes care of the requirement

that the keys are identical and random. Additionally, we require that an adversary, Eve, holds no information about the key. This corresponds to the joint state [87]

$$\rho_{ABE}^{\text{ideal}} = \left(\frac{1}{2^n} \sum_{k \in \{0,1\}^n} |k\rangle\langle k|_A \otimes |k\rangle\langle k|_B \right) \otimes \rho_E. \tag{2.13}$$

Therefore, if Alice and Bob can show that they hold a state of the form of Eq. (2.13), they have a guarantee that they can extract a shared secret key from their systems.

Now consider the case where Alice prepares a two-qubit state and sends one of the two qubits to Bob. We assume that she prepares a large number of identical copies of these states. For each of the copies, she independently chooses whether to make a measurement in the $\{|0\rangle,|1\rangle\}$ or $\{|+\rangle,|-\rangle\}$ bases. Remarkably, if every time that they measure in the same basis their measurements are perfectly correlated and every time they measure in a different basis their measurements are completely uncorrelated, it can be proven that the only state that Alice and Bob could share that is compatible with these statistics is the state $|\Phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$ of Eq. 2.11 [87]. Since this state is pure, it must be uncorrelated with the system of an adversary. Overall, if these perfect statistics are observed, the state shared by Alice and Bob state must be given by the ideal state

$$\rho_{ABE} = \left(|\Phi\rangle\langle\Phi|^{\otimes n}\right)_{AB} \otimes \rho_E = \rho_{ABE}^{\text{ideal}}. \tag{2.14}$$

Of course, this certification is only possible because Alice and Bob are assumed to have perfect statistics. In any practical scenario, there will be errors and finite size effects. It is the goal of security proofs of quantum key distribution to demonstrate that even in these imperfect scenarios it is possible for Alice and Bob to safely extract a secret key. Although in this example we have assumed that there is a source of entangled states, it can be shown that for many protocols, this situation is equivalent to one in which Alice selects between a set of non-orthogonal pure states that she sends to Bob, who chooses randomly to measure the signals in different non-orthogonal bases [87].

By now, quantum key distribution is an established technology, with several experimental demonstrations performed over increasingly larger distances and higher rates [108]. Additionally, there has been remarkable progress on the theoretical side by providing increasingly rigorous and general security proofs [121]. Overall, thanks to the unique properties of quantum communication such as entanglement and non-orthogonality, quantum key distribution performs a task that is impossible for separated parties using classical communication only. This constitutes a first example of the advantages that are possible with quantum communication.

2.2.2 Other protocols in quantum cryptography

As discussed before, there is a vast range of security requirements that are important in cryptography. We have already briefly mentioned *secrecy*: messages cannot be known by an adversary, and *integrity*: adversaries cannot tamper the content of these messages. Other commonly studied requirements are *authentication:* an adversary cannot impersonate another person, and *non-repudiation:* a person sending a message cannot later deny having done so. Digital signatures are cryptographic primitives that provide authentication, non-repudiation and transferability of messages and as such, they are widely used to secure electronic communications. In chapter 8, we take a detailed look at how quantum communication can be employed to provide information-theoretic security to signature schemes.

Additionally, it is also important to consider tasks whose end goal is not to transmit messages, but that nevertheless require communication in order to be carried out. A simple example of is Yao's Millionaire's Problem [136]. Here, two rich people want to know who has the largest fortune between them, but without revealing the actual value of their total wealth. More precisely, let Alice's fortune be x and Bob's fortune be y. Their goal is to compute the function

$$f(x,y) = \begin{cases} 1 & \text{if } x \geq y \\ 0 & \text{otherwise} \end{cases} \tag{2.15}$$

without revealing any information about x and y other than the value of $f(x,y)$. This problem constitutes an example of a more general cryptographic task known as *secure function evaluation*, where the goal is to compute the value of any function $f(x,y)$ without revealing additional information about the inputs x and y. Protocols for secure function evaluation can be built from universal primitives, most notably bit commitment and oblivious transfer. Even using quantum communication, it is not possible to perform bit commitment or oblivious transfer with information-theoretic security. However, security can be obtained in a quantum setting by imposing additional constraints on adversaries, such as limiting the amount of quantum memory at their disposal (bounded storage) or the levels of noise in their quantum memories (noisy storage) [127].

Other problems for which quantum communication can provide a cryptographic advantage are blind quantum computing [25], coin tossing [98] and secret sharing [39]. However, it is important to emphasize that quantum cryptography is still a relatively young field: we have most likely only begun to unravel the entire scope of advantages that quantum communication can provide to cryptography.

2.3 Quantum communication complexity

In a cryptographic setting, the difference between quantum and classical communication is *qualitative*: quantum communication permits us to do things which are impossible in a classical world. In this section, we take a look at a different class of problems for which quantum communication can provide a *quantitative* advantage. As mentioned before, Holevo's theorem places a fundamental limit on the savings that quantum communication can provide for the task of direct transmission of a classical message. However, there are situations where Alice and Bob must communicate even though their end goal is not to transmit messages to each other. We already saw an example of such a scenario with the Millionaire's Problem, where Alice and Bob are only interested in learning about the relationship between their private inputs. Can quantum communication help for such problems?

Formally, we consider the case where Alice and Bob respectively receive inputs $x \in \{0,1\}^n$ and $y \in \{0,1\}^n$ and their goal is to collaboratively compute the value of a Boolean function $f(x,y)$. Since in general f depends on both inputs, Alice and Bob must communicate in order to compute the function. *Communication complexity* is the study of the minimum amount of communication – as a function of the input size n – that Alice and Bob must exchange in order to evaluate f [77]. In the usual model, we allow Alice and Bob to have unlimited computational power and focus only on the total amount of communication required to compute f for the *worst-case* inputs x and y. In the deterministic case, Alice and Bob must be able to compute f with probability one, whereas in the randomized case, they have randomness at their disposal and are allowed to compute f with an error probability smaller than ϵ.[1] Usually, the probability of error is taken over randomness in the protocol for the worst-case inputs, but this can be extended to an average error probability over a probability distribution of the inputs.

The communication complexity of a function f, whether classical or quantum, in general depends on the resources that are available to Alice and Bob besides the ability to communicate. In particular, we distinguish between the following cases:

1. *Local randomness:* Alice and Bob are allowed to toss coins locally. The random bits of Alice are independent of those of Bob.

2. *Shared randomness:* Alice and Bob are allowed to toss coins and the random bits generated are shared between them, i.e. they hold the same string of random bits.

[1] In the literature, it is customary to demand an error probability smaller than $\frac{1}{3}$, which can be reduced to an arbitrary ϵ by repeating the protocol and taking the majority vote of the outcomes.

3. *Entanglement:* Alice and Bob share entangled states, usually many copies of the maximally entangled state $|\Phi\rangle$ of Eq. (2.11). These states are available prior to the run of the protocol and are not taken into account when quantifying communication.

In quantifying communication, we count the total number of distinct messages Alice and Bob must be able to transmit in order to carry out the protocol. As usual, we can encode these messages into strings of bits, so we can equivalently refer to the total number of bits exchanged. For a particular protocol P that computes f deterministically, let $S_P(x, y)$ be the total number of bits exchanged on inputs $x, y \in \{0,1\}^n$. The deterministic communication complexity of the protocol P is defined as

$$D(P) := \max_{x,y \in \{0,1\}^n} S_P(x, y). \tag{2.16}$$

Similarly, the deterministic communication complexity of f is defined as

$$D(f) := \min_P D(P). \tag{2.17}$$

In the randomized case, let $S_{P,\epsilon}(x, y)$ be the total number of bits exchanged on inputs x, y for a protocol P that computes f with probability of error smaller than ϵ. We define the randomized communication complexity of P as

$$R_\epsilon(P) := \max_{x,y \in \{0,1\}^n} S_{P,\epsilon}(x, y). \tag{2.18}$$

Finally, the randomized communication complexity of f is defined as

$$R_\epsilon(f) := \min_P R_\epsilon(P). \tag{2.19}$$

The randomized case is usually also referred to as the *bounded-error model* of communication complexity.

Note that Alice and Bob can always compute any function f by simply exchanging their entire inputs. However, in many cases, they can do much better than that. For example, consider the equality function,

$$EQ(x, y) = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{otherwise} \end{cases} \tag{2.20}$$

For this function, it can be proven that $D(f) \geq n$ [77], so the trivial protocol in which Alice sends her entire input to Bob is in fact optimal. However, once randomness is allowed, it

can be proven that $R_\epsilon = O(\log_2 n)$. Thus, they need only to communicate messages much smaller than their entire inputs. Note that Alice and Bob are only interested in learning one bit of information: the value of the function f. Thus, even though f depends on both inputs x, y, it is sometimes possible to send only partial information about the inputs in order to learn the single bit corresponding to the value of f.

In the quantum case, we now allow Alice and Bob to send quantum states to each other. In quantifying communication, we again consider the total number of distinct quantum states that they must be able to transmit in order to carry out the protocol. Formally, we consider the dimension of the Hilbert space spanned by all the possible states in the protocol. For example, if Alice and Bob exchange states of the form

$$|\psi\rangle = \sum_{i=1}^{d} \lambda_i |i\rangle, \tag{2.21}$$

these state span a Hilbert space of dimension d. Notice that this reduces to the classical case when they are only allowed to send states from the orthogonal basis $\{|i\rangle\}$. As before, we can encode these states into a system of $\lceil \log_2 d \rceil$ qubits, so we can equivalently talk about the number of qubits exchanged. In the quantum setting, it is customary to consider only the randomized case. As before, for a particular protocol P that computes f with error probability smaller than ϵ, let $q_{P,\epsilon}(x, y)$ be the total number of qubits exchanged on inputs x, y. The quantum communication complexity of P is defined as

$$Q_\epsilon(P) := \max_{x,y \in \{0,1\}^n} q_{P,\epsilon}(x, y). \tag{2.22}$$

Finally, the quantum communication complexity of f is defined as

$$Q_\epsilon(f) := \min_P Q_\epsilon(P). \tag{2.23}$$

We know that quantum communication can never do worse than classical, but can it really help for communication complexity? At first glance, it would appear that Holevo's theorem once again ruins the party. As it turns out, for specific problems, quantum communication can provide dramatic reductions in communication. The crucial difference compared to the case of direct communication is that Alice and Bob only need to learn a single bit of information, so quantum communication can prove advantageous in allowing them to process and manipulate information in ways that permit an overall reduction in communication. In the following, we take a look at examples of problems for which quantum mechanics can provide exponential reductions in communication complexity compared to the classical case. For a complete review of all such problems, we refer the reader to Ref. [27]. The practical demonstration of these schemes is the main topic of chapters 6 and 7.

2.3.1 Raz's problem

The first example of an exponential separation between classical and quantum communication complexity is due to Raz [102]. In this problem, Alice receives a unit vector $v \in \mathbb{R}^m$ and a decomposition of $\mathbb{R}^m$ into two orthogonal subspaces H_0 and H_1. Bob receives as input an $m \times m$ unitary matrix U. They are given the promise that either $||P_{H_0}Uv||^2 \geq \frac{2}{3}$ or $||P_{H_1}Uv||^2 \geq \frac{2}{3}$, where P_H is the projector on the corresponding subspace. Their job is to determine which of the two cases holds with probability of error smaller than ϵ. Even though the problem in its above formulation has continuous input, we can re-formulate it for discrete inputs by approximating real numbers with $k \log_2 m$ bits, for some constant integer k. In that case, Alice's and Bob's input have size $n = O(m^2 \log_2 m)$ bits.

It was proven in Ref. [102] that any classical protocol for this problem must transmit at least $\Omega(n^{\frac{1}{4}}/\log_2 n)$ bits. However, there exists a simple quantum protocol that requires only $O(\log_2 n)$ qubits. In the protocol, Alice encodes the vector $v = (v_1, v_2, \cdots, v_m)$ into a quantum state

$$|\psi_v\rangle = \sum_{i=1}^{m} v_i |i\rangle \tag{2.24}$$

and sends it to Bob, who applies his unitary transformation U on the state. He then returns the state to Alice, who makes a measurement defined by the two projectors $\{P_{H_0}, P_{H_1}\}$. Because of the promise of the problem, she will obtain the correct answer with probability greater or equal than $\frac{2}{3}$. In order to decrease the error probability to an arbitrary $\epsilon > 0$, they can simply repeat the protocol a constant number of times and take the majority vote of the outcomes. Again, since the states $\{|\psi_v\rangle\}$ sent by Alice span an m-dimensional Hilbert space, we can equivalently think of them as states of $\log_2 m = O(\log_2 n)$ qubits. This is an exponential separation compared to the classical case.

2.3.2 The Hidden Matching problem

In this problem, Alice receives an n-bit string $x \in \{0,1\}^n$ as input, with n an even number. Bob receives a matching $M = \{(i_1, j_1), (i_2, j_2), \ldots, (i_{n/2}, j_{n/2})\}$ on the set of numbers $\{1, 2, \ldots, n\}$, i.e. a partition into $n/2$ pairs. For example, a matching for the case $n = 6$ could be $\{(1,6), (2,5), (3,4)\}$. Only one-way communication from Alice to Bob is permitted and the goal is for Bob to output at least one element of the matching (i, j) and a corresponding bit value b such that $b = x_i \oplus x_j$, where x_i is the i-th bit of the string x. Note that the problem can be easily solved if Bob can communicate with Alice: he only needs to send her an element of the matching, which requires $O(\log_2 n)$ bits of communication.

It has been shown that in the bounded-error model, any classical protocol with shared randomness requires $\Omega(\sqrt{n})$ bits of communication [13]. It was also shown in Ref. [13] that there exists an efficient quantum protocol that uses only $O(\log_2 n)$ qubits of communication and outputs a correct answer with certainty. In this protocol, Alice prepares the state

$$|x\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} (-1)^{x_i} |i\rangle \tag{2.25}$$

and sends it to Bob, who measures it in the basis

$$\{\tfrac{1}{\sqrt{2}}(|i\rangle \pm |j\rangle)\}, \tag{2.26}$$

with $(i, j) \in M$. Since these states form a complete basis, one of these outcomes will always occur, and it will always correspond the correct value because $\frac{1}{\sqrt{2}}(|i\rangle + |j\rangle)$ only occurs if $x_i \oplus x_j = 0$ and similarly, $\frac{1}{\sqrt{2}}(|i\rangle - |j\rangle)$ only occurs if $x_i \oplus x_j = 1$. This allows Bob to give a correct output after performing his measurement.

In chapter 6 we study how this problem can be implemented in a practical setting.

2.3.3 Quantum fingerprinting

Quantum fingerprinting is arguably the most appealing protocol in quantum communication complexity, as it constitutes a natural problem for which quantum mechanics permits an exponential reduction in communication complexity [28]. In the simultaneous message passing model (SMP) [135], Alice and Bob are each given an n-bit string, which we label x and y respectively and they must each send a message to a third party, the referee, whose task is evaluate a given function $f(x, y)$. Alice and Bob do *not* have access to shared randomness and there is only one-way communication to the referee. For quantum fingerprinting, we focus on the equality function $EQ(x, y)$ as in Eq. (2.20) and the goal is for Alice and Bob to send messages to the referee so that he can determine whether their inputs are equal or not with an error probability of at most ϵ.

In this case, it has been proven that any classical protocol must transmit at least $\Omega(\sqrt{n})$ bits of information to the referee [12, 95]. On the other hand, a quantum protocol was specified in Ref. [28] that transmits only $O(\log_2 n)$ qubits of information – an exponential improvement over the classical case.

This quantum fingerprinting protocol relies on the concept of error-correcting codes. A code can be expressed as a function $E : \{0,1\}^n \to \{0,1\}^m$, where $E(x)$ is the *codeword*

associated with the input x, where $R = \frac{n}{m} < 1$ is the rate of the code. The protocol makes use of codes that have the additional property that the minimum Hamming distance between any two codewords is at least δm, for some $\delta > 0$. More precisely, for the error-correcting code it holds that

$$\min_{x,y \in \{0,1\}^n} h(E(x), E(y)) \geq \delta m \text{ for all } x \neq y \text{ and for all } n, \tag{2.27}$$

where $h(\cdot, \cdot)$ is the Hamming distance. The parameter δ is called the *minimum distance* of the code.

In the protocol, Alice and Bob respectively prepare the fingerprint states

$$|h_x\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} (-1)^{E(x)_i} |i\rangle, \tag{2.28}$$

where $E(x)_i$ is the ith bit of the codeword $E(x)$. This state has dimension m, so it can be associated to a system of $\log_2 m = O(\log_2 n)$ qubits. Upon receiving the states from Alice and Bob, the referee performs a SWAP test on them. In this test, the referee adds an ancilla qubit initialized to the state $|0\rangle$ and applies the transformation

$$(\mathbb{1} \otimes H) \, \text{c-SWAP} \, (\mathbb{1} \otimes H) \, |0\rangle |h_x\rangle |h_y\rangle, \tag{2.29}$$

where H is the Hadamard transform, SWAP is the transformation that exchanges Alice's and Bob's systems, i.e. it performs the transformation $|h_x\rangle|h_y\rangle \to |h_y\rangle|h_x\rangle$, and c-SWAP is a controlled SWAP operation. After applying this transformation, the referee performs a measurement in the computational basis of the ancilla qubit, with corresponding outcomes "0" and "1".

It can be shown that if $x = y$, then $\Pr(1) = 0$, whereas if $x \neq y$, $\Pr(1) \geq \frac{1-(1-\delta)^2}{2}$ [28]. Therefore, the referee can decide whether the states are equal or not by simply checking whether outcome "1" occurs. If the inputs are equal, this will never happen but if the inputs are different, there is a fixed probability for this outcome to occur. The probability of error can then be made arbitrarily small by simply repeating the protocol enough times and checking whether outcome "1" occurs.

In chapter 7, we study a practical protocol for quantum fingerprinting as well as its experimental demonstration.

2.3.4 Conclusion

In this chapter, we have given an overview of quantum communication with a focus on how it can provide advantages compared to classical communication. However, the ex-

amples discussed are by no means exhaustive. Quantum communication is an active field both in theory and experiment, covering additional subtopics such as quantum Shannon theory [130], quantum non-locality [26], quantum repeaters [106], and quantum networks [76]. Globally, there is an interest in building a quantum Internet, to be used to perform tasks beyond what is classically possible. It is a grand challenge not only to develop the technologies required to achieve this goal, but also to acquire a profound theoretical understanding of quantum communication, in particular by identifying how it can improve upon what can be done classically.

Chapter 3

Entanglement Theory

In chapter 2, we made our first encounter with entanglement when we reviewed how entangled states could be used in a cryptographic context. Entanglement, however, plays a much larger role in quantum mechanics and quantum communication. In this chapter, we cover the basic concepts of entanglement theory, with a particular attention on how the entanglement of physical systems can be verified in practice.

3.1 Bipartite entanglement

Previously, we claimed that the state

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$$

was an entangled state of two-qubits, but we did so without even defining what entanglement is! So let us begin with some definitions.

Definition 2. *A pure bipartite state $|\psi_{AB}\rangle \in \mathcal{H}$, with $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$, is called a* product state *if it can be written in the form $|\psi_{AB}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle$ for some $|\psi_A\rangle \in \mathcal{H}_A$ and $|\psi_B\rangle \in \mathcal{H}_B$. Otherwise, the pure state is called* entangled.

Notice that the decomposition of the underlying Hilbert space $\mathcal{H}$ is a crucial part of the definition. In particular, a state may be entangled with respect to some bipartition

but not with respect to another. A family of maximally entangled two-qubit states that will recur in this thesis are the Bell states

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{3.1}$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \tag{3.2}$$

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \tag{3.3}$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \tag{3.4}$$

We can extend the above definition to mixed states to provide the most general definition of entanglement.

Definition 3. *A bipartite state $\rho_{AB} \in \mathcal{D}(\mathcal{H})$, with $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$, is called* separable *if there exists $\{p_i\}$, with $\sum_i p_i = 1$, $p_i > 0$ and local states $\{\rho_A^i\}$, $\{\rho_B^i\}$ such that ρ_{AB} can be written in the form*

$$\rho_{AB} = p_i \sum_i \rho_A^i \otimes \rho_B^i. \tag{3.5}$$

Otherwise, the state is called entangled.

The set of separable states is convex, meaning that for any two separable states ρ_1 and ρ_2 and any $0 \leq p \leq 1$, the state $\rho = p\rho_1 + (1-p)\rho_2$ is also separable. The set of entangled states, however, is not convex.

In general, it is a computationally hard task to determine whether a given state ρ is entangled or not. In section 3.2, we consider different criteria that can be employed in order to determine whether a state is separable or entangled. In this thesis, we focus only on bipartite entanglement, but, naturally, the theory of entanglement extends also to the multipartite case.

3.1.1 Why are we interested in entanglement?

Based on its definition alone, it is not easy to see why entanglement is an important property of physical systems. However, in recent decades and particularly with the advent of quantum information, entanglement has been well established as a useful resource for performing tasks that are not possible using only classical resources.

In the context of quantum computing, it is known that quantum algorithms on pure states that produce only small amounts of entanglement can be simulated efficiently by a classical computer [125]. This implies that in the context of pure-state quantum computation, entanglement is a necessary condition for achieving an exponential speed-up over the classical case. In the case of mixed-state quantum computing, the role of entanglement is not so well understood [79]. Entanglement also plays an important role in one-way quantum computing, where a the quantum computation is performed by appropriate measurements of highly entangled states [101]. In fact, the presence of entanglement is often used as a benchmark for current small-scale quantum computers [2].

In the context of communication, entanglement shared between parties is required to perform quantum teleportation, superdense coding and entanglement swapping [19, 138]. These can in turn be used as building blocks for other tasks such as quantum repeaters and error correction [106, 81]. Entanglement can also be a powerful resource for communication complexity [40]. If Alice and Bob share an unlimited number of maximally entangled two-qubit states – such as the Bell state $|\Phi^+\rangle$ – and they are allowed to communicate classically, this entanglement can be used to realize effective quantum channels via quantum teleportation. Thus, adding shared entanglement to classical communication can lead to exponential savings in communication complexity for the same problems discussed in chapter 2. Additionally, as discussed before, in the context of cryptography, entanglement can be used to perform quantum key distribution as well as other tasks such as oblivious transfer. In particular, it has been shown that entanglement is a necessary condition for the security of quantum key distribution [43]. Finally, entanglement plays a fundamental role in device-independent quantum cryptography, certified randomness generation, and nonlocality [26].

Entanglement also plays an important role in quantum metrology, particularly in schemes that allow quadratic improvements in the precision of estimating an optical phase [61]. Additionally, it is an important aspect of many-body physics, giving new insights to areas such as superconductivity, phase transitions and Bose-Einstein condensates [3]. Overall, entanglement plays a crucial role in quantum physics, quantum information, and quantum technologies [73].

However, despite its usefulness and significance, generating entanglement, controlling it and preserving it in an experimental setting is a daunting task. As such, it is a challenge for experiments claiming to generate entanglement to certify that the physical systems in consideration are indeed entangled. In the following section, we review theoretical methods for certifying the entanglement of quantum states and how these methods can be applied to entanglement verification in experiments.

3.2 Separability criteria

Suppose that you are given a full description of a bipartite quantum state ρ. How can you determine whether the state is entangled or not? Naively, all we have to do is show that the state cannot be expressed in the form of Eq. (3.5). But for large systems, this turns out to be a computationally challenging task. In fact, determining whether a state is separable or not – known as the *separability problem* – is an NP-hard problem in terms of the number of qubits in the system [65]. Therefore, we do not expect there to be efficient algorithms for certifying the entanglement of general states. The situation is even more dire in an experimental setting, where we never have access to the full density matrix of the system, but can only perform a finite number of measurements and make statistical inferences from the data.

Instead, we are often interested in *separability criteria*: conditions that hold for all separable states but are not met by some entangled states. Thus, if we can show that a state does not meet a particular criterion, we are certain it must be entangled. Separability criteria usually lead to methods for entanglement verification that are less computationally demanding than more general solutions, and they are also more accessible to experiments. We now take a look at some important separability criteria.

1. Positive but not completely positive maps [72]. Let $\mathcal{B}(\mathcal{H})$ be the set of all bounded linear operators on a Hilbert space $\mathcal{H}$. A map $\Lambda : \mathcal{B}(\mathcal{H}) \mapsto \mathcal{B}(\mathcal{H}')$ is called a *positive map* if it maps Hermitian operators to Hermitian operators, satisfies $\Lambda(X^\dagger) = \Lambda(X)^\dagger$, and it maps positive operators to positive operators, i.e. $\Lambda(X) \geq 0$ for all $X \geq 0$. A map is called *completely positive* if for any Hilbert space $\mathcal{H}_A$ it holds that the map $\mathbb{1}_A \otimes \Lambda(X)$ is also positive. Intuitively, a completely positive map preserves positivity even when it acts only on a subsystem of a larger physical system. Thus, all physical maps are completely positive. We refer to maps that are positive but not completely positive as PnCP maps.

Theorem 4. *For any PnCP map Λ and any bipartite separable state $\rho \in \mathcal{H}_A \otimes \mathcal{H}_B$ it holds that*

$$(\mathbb{1}_A \otimes \Lambda)(\rho) \geq 0. \tag{3.6}$$

Therefore, if for any PnCP map Λ it holds that $(\mathbb{1}_A \otimes \Lambda)(\rho) \ngeq 0$, we can conclude that the state ρ must be entangled. In fact, it has been shown that a state ρ is separable if and only if $(\mathbb{1}_A \otimes \Lambda)(\rho) \geq 0$ for all PnCP maps [72]. However, characterizing the set of all PnCP maps is as hard as characterizing the set of all entangled states. Therefore, it is usually

desirable to focus on simple PnCP maps that are capable of detecting the entanglement of a wide class of quantum states.

2. PPT criterion [100, 72]. The most celebrated example of a simple PnCP map is the transposition map T. The map $(\mathbb{1} \otimes T)$ is referred to as the *partial transposition*. Its action on a bipartite state

$$\rho = \sum_{i,j} \sum_{kl} \rho_{ij,kl} |i\rangle\langle j| \otimes |k\rangle\langle l| \tag{3.7}$$

is given by

$$(\mathbb{1} \otimes T)(\rho) := \rho^{\Gamma} = \sum_{i,j} \sum_{kl} \rho_{ij,kl} |j\rangle\langle i| \otimes |k\rangle\langle l|. \tag{3.8}$$

States satisfying the condition $\rho^{\Gamma} \geq 0$ are referred to as PPT states. From the PnCP criterion, we know that all separable states are PPT and any state satisfying $\rho^{\Gamma} \ngeq 0$ must be entangled. Famously, the PPT criterion provides a necessary and sufficient condition for entanglement in dimensions 2×2 and 2×3 [72]. Additionally, partial transposition has the highly appreciated property of being efficiently computable.

3. Entanglement witnesses. An important drawback of the two previous criteria is that they require complete knowledge of the quantum state ρ. In experiments, the state is unknown, and all the information that is available is the result of repeated measurements on sequential preparations of a given system. Using techniques from quantum state tomography [99], it is possible to statistically reconstruct the quantum state of a system and then use separability criteria to verify entanglement. However, for systems of large dimension, the number of different measurements that have to be made in order to reconstruct a state quickly increase beyond experimental capabilities. For example, for systems of n-qubits, the required measurement settings to reconstruct a general state will in general increase exponentially with the number of qubits [63]. Consequently, it is desirable to use methods that allow the verification of entanglement without the requirement to perform full tomography.

A widely used approach relies on entanglement witnesses. A linear entanglement witness on a bipartite Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ is a Hermitian operator W, such that

$$\begin{aligned} &\mathrm{Tr}\,(W\rho^s) \geq 0 \quad \forall \rho^s \text{ separable} \\ &\exists \rho \text{ entangled such that } \mathrm{Tr}\,(W\rho) < 0. \end{aligned} \tag{3.9}$$

Therefore, if the expectation value of a witness is negative for a given state, this state must be entangled. We refer to this situation as the state being *detected* by the witness. Geometrically, a linear entanglement witness can be viewed as a hyperplane defined by the set of states such that $\mathrm{Tr}\,(W\rho) = 0$. The existence of entanglement witnesses is guaranteed by the fact that the set of separable states is convex: The hyperplane separation theorem then states that for any entangled state, there must exist a hyperplane separating this state from set of separable states [72]. Thus, for any entangled state, there exists an entanglement witness for which the state has a negative expectation value. However, finding a witness for a particular state is in general a hard problem, since this would imply a solution to the separability problem.

Notice that the expectation value of an entanglement witness corresponds to a *single parameter* of a quantum state ρ. In principle, directly measuring the expectation value of the witness W is sufficient to verify the entanglement of this state; much easier than doing full tomography of ρ. However, a direct measurement of W is difficult to perform experimentally as it generally requires global measurements. Instead, a linear witnesses can be decomposed in terms of a linear combination of local observables $\{A_i \otimes B_i\}$ as

$$W = \sum_{i=1}^{N} c_i A_i \otimes B_i. \tag{3.10}$$

These local observables are then easier to measure experimentally. Then, it suffices to measure the expectation values $\{\mathrm{Tr}\,(\rho A_i \otimes B_i)\}$ in order to determine the expectation value of the witness. In most cases, linear witnesses can be decomposed in terms of a number of local operators that scales favourably with the dimension of the system, thus making the task much easier to perform experimentally than full tomography.

The problem of entanglement detection with a fixed restricted set of measurements corresponding to the eigenvalues of the operators $\{A_i \otimes B_i\}$ has been addressed in Ref. [42]. Investigation of this problem naturally leads to the definition of *verifiable states*. For the given set of restricted measurements a state is called *verifiable* if the outcomes of the measurements are not compatible with the outcomes of the same measurements on any separable state. The set of all linear witnesses which can be constructed from this restricted set of measurements is called the *verification set*. Characterizing the verification set or finding a witness for a given verifiable state is a challenging problem [42], which is in fact as hard as finding an entanglement witness for an arbitrary entangled state [73].

3.2.1 Choi-Jamiołkowski isomorphism

A beautiful connection between entanglement witnesses and PnCP maps can be established through the Choi-Jamiołkowski isomorphism. This relation states that any linear map $\Lambda_W : \mathcal{B}(\mathcal{H}_A) \mapsto \mathcal{B}(\mathcal{H}_B)$ is connected to an operator W acting on a bipartite Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ via the relation

$$\Lambda_W(X) = \mathrm{Tr}_A(W\, X^T \otimes \mathbb{1}_B) \tag{3.11}$$

where, as before, X^T is the transpose of X. The inverse relation, connecting the operator W to the map, is given by

$$W = (\mathbb{1}_{A'} \otimes \Lambda_W)(|\Phi\rangle\langle\Phi|) := \tilde{\Lambda}_W(|\Phi\rangle\langle\Phi|), \tag{3.12}$$

where $\mathbb{1}_{A'}$ is the identity operator on $\mathcal{H}_{A'}$, $\mathcal{H}_{A'} \simeq \mathcal{H}_A$ and $|\Phi\rangle = \sum_i |i\rangle|i\rangle$ is a non-normalized maximally entangled state on $\mathcal{H}_{A'} \otimes \mathcal{H}_A$. Note that the map $\tilde{\Lambda}_W$ maps operators in $\mathcal{B}(\mathcal{H}_{A'} \otimes \mathcal{H}_A)$ to operators in $\mathcal{B}(\mathcal{H}_{A'} \otimes \mathcal{H}_B)$.

It can be shown that Λ_W is a PnCP map if and only if W is an entanglement witness. This profound connection has several important applications in the context of entanglement theory [63]. For our purposes, it suffices to see that the Choi-Jamiołkowski isomorphism provides a method of constructing interesting PnCP maps from entanglement witnesses.

3.3 Nonlinear entanglement witnesses

The entanglement witnesses that we have studied so far are linear, in the sense that their expectation value is a linear function of the quantum state ρ. Linear entanglement witnesses are useful for detecting the entanglement of some states, but for any witness, there are always entangled states that have a positive expectation value and whose entanglement cannot be detected with that witness. However, it is possible to construct nonlinear extensions of any entanglement witness, which detect more states than their linear counterparts.

In order to derive a nonlinear witness on a Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$, we first note that the quantity $\mathrm{Tr}\left(POO^\dagger\right)$ is positive semi-definite for any positive operator P and any operator O. As a consequence, for any decomposition $O = \sum_{i=1}^n c_i B_i$ with free parameters c_i and any set of operators B_i, this condition can be shown to be equivalent [93] to the positive semi-definiteness of the matrix

$$[M(P)]_{i,j} = \mathrm{Tr}\left(PB_iB_j^\dagger\right). \tag{3.13}$$

If we choose B_1 as the projector P_{Φ^+} onto the maximally entangled state $|\Phi^+\rangle$ on $\mathcal{H}_A \otimes \mathcal{H}_{A'}$ and B_2 as some unitary U, for a given entanglement witness W we can construct a 2×2 matrix defined as

$$M(\rho) := M(\tilde{\Lambda}_W^\dagger[\rho]) = \begin{pmatrix} \mathrm{Tr}\left(\tilde{\Lambda}_W^\dagger[\rho]\mathbb{1}\right) & \mathrm{Tr}\left(\tilde{\Lambda}_W^\dagger[\rho]\mathrm{P}_{\Phi^+}U\right) \\ \mathrm{Tr}\left(\tilde{\Lambda}_W^\dagger[\rho]U\mathrm{P}_{\Phi^+}\right)^* & \mathrm{Tr}\left(\tilde{\Lambda}_W^\dagger[\rho]\mathrm{P}_{\Phi^+}\right) \end{pmatrix}, \tag{3.14}$$

where ρ is a bipartite quantum state in $\mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and $\tilde{\Lambda}_W^\dagger$ is the adjoint map of the witness map $\tilde{\Lambda}_W$, which as before is given by

$$\tilde{\Lambda}_W := \mathbb{1}_A \otimes \Lambda_W. \tag{3.15}$$

The adjoint map is defined as the unique map satisfying

$$\mathrm{Tr}\left[\tilde{\Lambda}_W^\dagger(X)Y\right] = \mathrm{Tr}\left[X\tilde{\Lambda}_W(Y)\right] \tag{3.16}$$

for all $X \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and all $Y \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_{A'})$.

Since Λ_W is a PnCP map, $\tilde{\Lambda}_W$ will transform separable states into positive operators, and so will its adjoint $\tilde{\Lambda}^\dagger$, i.e. $\tilde{\Lambda}^\dagger[\rho_s] \geq 0$ for any separable state $\rho_s \in \mathcal{B}(\mathcal{H})$. Therefore, for all separable bipartite states the matrix $M(\rho_s)$ must be positive semi-definite [93]. Moreover, for general bipartite states ρ, failure of the matrix in Eq. (3.14) to be positive is a conclusive proof that the particular ρ must be entangled.

By using the definition of the adjoint map, noting that $\tilde{\Lambda}_W[\mathrm{P}_{\Phi^+}] = W$ and assuming that $\mathrm{Tr}\left(\rho\tilde{\Lambda}_W[\mathbb{1}]\right) \neq 0$, we construct from the determinant of Eq. (3.14) a nonlinear function which improves the entanglement detection of the linear witness [93]:

$$w_1(\rho) = \mathrm{Tr}\left(\rho W\right) - \frac{|\mathrm{Tr}\left(\rho\tilde{\Lambda}_W[\mathrm{P}_{\Phi^+}U]\right)|^2}{\mathrm{Tr}\left(\rho\tilde{\Lambda}_W[\mathbb{1}]\right)}. \tag{3.17}$$

That is, if for some U we have that $w_{NL}(\rho) < 0$, then the state ρ must be entangled. The new criterion (3.17) detects more entangled states because we subtract a strictly positive number from the expectation value of W.

This procedure can be iterated to build consequent improvements to the preceding witness. In Ref. [7], it was shown that, whenever $U^2 = \mathbb{1}$, in the asymptotic limit of

an infinite number of iterations, the expectation value of the nonlinear witness can be expressed in terms of an analytic formula as

$$w_\infty(\rho) := \mathrm{Tr}\,(\rho W) - \varkappa(\rho)|c(\rho)|^2 - \frac{\varkappa(\rho)|d(\rho)|^2}{1-(\varkappa(\rho)|k(\rho)|)^2} \tag{3.18}$$

$$\text{where } k(\rho) = \mathrm{Tr}\left(\rho\tilde{\Lambda}_W[U]\right), \tag{3.19}$$

$$\varkappa^{-1}(\rho) = \mathrm{Tr}\left(\rho\tilde{\Lambda}_W[\mathbb{1}]\right) \tag{3.20}$$

$$c(\rho) = \mathrm{Tr}\left(\rho\tilde{\Lambda}_W[P_{\Phi^+}U]\right), \tag{3.21}$$

$$d(\rho) = \mathrm{Tr}\,(\rho W) - \varkappa c(\rho)k(\rho). \tag{3.22}$$

In general, for a witness W that is decomposed in terms of local observables $\{A_i \otimes B_i\}$, it will not be possible to evaluate the expectation value (3.18) of its nonlinear extension only from the expectation values $\langle A_i \otimes B_i\rangle := \mathrm{Tr}\,(\rho A_i \otimes B_i)$ of the local observables. This of course presents a severe problem, since one of the appealing properties of entanglement witnesses is that they can be evaluated from this small set of expectation values. However, for the right choice of the unitary U, it is indeed possible to construct nonlinear witnesses that can be evaluated from exactly the same measurement data as the original linear ones. They are called *accessible nonlinear witnesses* [7]. In general, any expression is deemed *accessible* if it can be evaluated from the expectation values $\langle A_i \otimes B_i\rangle$.

We now give necessary and sufficient conditions for the expectation value $w_\infty(\rho)$ of Eq. (3.18) to be accessible.

Observation 5. *Let $W = \sum_i c_i A_i \otimes B_i$ be a decomposition of a linear entanglement witness and let the unitary U used in the construction of the nonlinear witness satisfy $U^2 = \mathbb{1}$. Then $w_\infty(\rho)$ is accessible if and only if $k(\rho)$, $\varkappa(\rho)$ and $c(\rho)$ are accessible.*

Proof: First assume that $k(\rho)$, $\varkappa(\rho)$ and $d(\rho)$ are accessible. Then $w_\infty(\rho)$ must be accessible as it is a function of $k(\rho), \varkappa(\rho)$ and $d(\rho)$ only. This finishes the first part of the proof.

Now assume every $w_\infty(\rho)$ is accessible. Define $v_i := \mathrm{Tr}\,(\rho A_i \otimes B_i)$ and $z_j := \mathrm{Tr}\,(\rho Z_j)$ where the set of hermitian operators $\{Z_j\}$ form a basis of the orthogonal complement $V^\perp$ of $V = \mathrm{span}\{A_i \otimes B_i\}_{i=1}^N$. Then a quantity $q(\{v_i\},\{z_i\})$ is accessible if it can be expressed as a function of the variables v_i only. Equivalently, one can say that all derivatives of q with respect to every z_j must vanish for all values of the variables $\{v_i\}$ and $\{z_j\}$.

First note that for $c(\rho) = 0$, we find that $w_\infty(\rho) = w_0(\rho) = \mathrm{Tr}\,(\rho W)$ for all n. In this case, the nonlinear improvements coincide with the expectation value of the linear witness and therefore can be evaluated from the same measurement data. So from now on we can assume that $c(\rho) \neq 0$ whenever necessary.

In general, we can write $c = \sum_i a_i v_i + \sum_j x_j z_j$ and $\varkappa^{-1} = \sum_i b_i v_i + \sum_j y_j z_j$ for some fixed numbers $\{a_i\}, \{x_j\}, \{b_i\}, \{y_j\}$. We want to show that $x_j = y_j = 0$ for all values of j. It is a lengthy but straightforward calculation to show that the condition $\frac{\partial}{\partial z_l} \varkappa |c|^2 = 0$, for any $l = 1, \ldots, dim(V^\perp)$ is equivalent to the system of linear equations

$$\gamma_l |x_l|^2 = 0 \tag{3.23}$$

$$y_l |x_l|^2 = 0 \tag{3.24}$$

$$\beta_l \gamma_l = \alpha_l y_l, \tag{3.25}$$

where

$$\alpha_l = \sum_i \sum_j a_i a_j^* v_i v_j + \sum_i \sum_{j \neq l} (a_i x_j^* + a_i^* x_j) v_i z_j \tag{3.26}$$

$$\beta_l = \sum_i (a_i x_l^* + a_i^* x_l) v_i + \sum_{j \neq l} (x_j x_l^* + x_j^* x_l) z_j \tag{3.27}$$

$$\gamma_l = \sum_i b_i v_i + \sum_{j \neq l} y_j z_j. \tag{3.28}$$

Recall from (3.17) that we always have $\varkappa^{-1} = \gamma_l + y_l z_l \neq 0$ and therefore Eqns. (3.23) and (3.24) imply $|x_l| = 0$ (otherwise both γ_l and y_l must be equal to zero, which would imply $\varkappa^{-1} = 0$). Since this holds for any arbitrary l, it proves that $c = \sum_i a_i v_i$ and therefore it proves that c is accessible. Further, because of $|x_l| = 0$, Eq. (3.27) becomes $\beta_l = 0$ and Eq. (3.26) becomes $\alpha_l = \sum_i \sum_j a_i a_j^* v_i v_j = |c|^2$. Moreover, Eq. (3.25) gives $\alpha_l y_l = 0$. Since $\alpha_l = |c|^2 \neq 0$ it must be that $y_l = 0$ for all values of l. This proves that $\varkappa^{-1} = \sum_i b_i v_i$ and therefore $\varkappa$ is also accessible. Finally, from Eqs. (3.18) and (3.22), it is straightforward to show that $\varkappa |k|$ is accessible and this implies that k is accessible as well. ■

These results tells us that, as long as we choose a unitary U satisfying $U^2 = \mathbb{1}$ as well as the conditions of observation 5, it is always possible to construct a nonlinear extension of a witness W whose expectation value can be easily computed as a function of the same measurement data required for the linear witness W. Moreover, the nonlinear witness is a strict improvement as it always detects the entanglement of more states. In chapter 5, we provide a reliable data analysis technique to evaluate the results of entanglement verification experiments and employ it in an experiment to verify the entanglement of two-qubit states using accessible nonlinear witnesses.

Chapter 4

Quantum Optics

So far, we have studied quantum communication and entanglement theory without a specification of the physical systems that are used to communicate or to generate entanglement. In the context of communication, light is essentially the only carrier of information that is suitable for fast, long distance communication. Similarly, although entanglement has been demonstrated in a large variety of physical systems such as ion traps and superconducting circuits, optical systems also provide a versatile platform for the generation and manipulation of entanglement, leading to many pioneering experiments. In this thesis, we focus on light as the physical system of choice and in this chapter, we give a brief introduction to the canonical quantization of the electromagnetic field, which provides the working framework of quantum optics. From this starting point, we continue by studying important quantum states of the quantized electromagnetic field, as well as basic notions of linear optics and single-photon detection.

4.1 Quantized electromagnetic field

In classical physics, the theory of electromagnetism is elegantly summarized in Maxwell's equations. In the vacuum, i.e. without the presence of charged particles, the electric field

$\mathbf{E}(\mathbf{r}, t)$ and the magnetic field $\mathbf{B}(\mathbf{r}, t)$ obey the equations

$$\nabla \cdot \mathbf{E} = 0 \tag{4.1}$$

$$\nabla \cdot \mathbf{B} = 0 \tag{4.2}$$

$$\nabla \times \mathbf{E} = -\frac{\partial \mathbf{B}}{\partial t} \tag{4.3}$$

$$\nabla \times \mathbf{B} = \frac{1}{c^2}\frac{\partial \mathbf{B}}{\partial t}, \tag{4.4}$$

where c is the speed of light and, for simplicity, we have dropped the explicit dependence on the position vector $\mathbf{r}$ and on time t. All physically allowed configurations of the electric and magnetic fields must obey Maxwell's equations, so the study of electromagnetism is strongly linked to the study of the solutions to these equations. A convenient method of expressing these solutions is to look at the vector and scalar potentials, ϕ and $\mathbf{A}$ respectively, which satisfy

$$\mathbf{B} = \nabla \times \mathbf{A} \tag{4.5}$$

$$\mathbf{E} = -\nabla\phi - \frac{\partial \mathbf{A}}{\partial t}. \tag{4.6}$$

The potentials have *gauge freedom*, meaning that there are transformations that can be applied to them which leave the electric and magnetic fields unaltered. In general, for any function $f(\mathbf{r}, t)$, the transformations

$$\mathbf{A} \to \mathbf{A} + \nabla f \tag{4.7}$$

$$\phi \to \phi - \frac{\partial f}{\partial t} \tag{4.8}$$

are gauge transformations that leave the electric and magnetic fields unchanged. For convenience, we can therefore set $\phi = 0$ and demand that the vector potential satisfy $\nabla \cdot \mathbf{A} = 0$. This is known as the *Coulomb gauge*. In this case, plugging equations (4.5) and (4.6) into equation (4.4), and making use of vector calculus identities, gives the following re-formulation of Maxwell's equations for the vector potential:

$$\nabla^2 \mathbf{A} = \frac{1}{c^2}\frac{\partial^2 \mathbf{A}}{\partial t^2}. \tag{4.9}$$

This is known as the *wave equation*, a famous equation in physics whose solutions have been extensively studied. Any particular solution $\mathbf{A}(\mathbf{r}, t)$ is referred to as an *optical mode*.

For simplicity, we focus on solutions defined on a finite cubic volume of space of length L and volume $V = L^3$. In this case, any solution to the wave equation can be expressed in terms of a Fourier decomposition, i.e. a linear combination of plane wave solutions of the form

$$\mathbf{A}(\mathbf{r}, t) = \sum_{\mathbf{k},p} \left(A_{\mathbf{k},p} e^{-i(\omega_k t - \mathbf{k}\cdot\mathbf{r})} + A^*_{\mathbf{k},p} e^{i(\omega_k t - \mathbf{k}\cdot\mathbf{r})} \right) \hat{\varepsilon}_p, \tag{4.10}$$

where $A_{\mathbf{k},p}$ is the complex amplitude of the field, $\omega_k = c|\mathbf{k}|$, and the *wave vector* is given by $\mathbf{k} = (k_x, k_y, k_z)$, whose components must satisfy

$$k_x = \frac{2\pi n_x}{L} \tag{4.11}$$

$$k_y = \frac{2\pi n_y}{L} \tag{4.12}$$

$$k_z = \frac{2\pi n_z}{L} \tag{4.13}$$

for integer values of n_x, n_y and n_z. Additionally, $\hat{\varepsilon}_p$ is a unit *polarization* vector satisfying

$$\hat{\varepsilon}_p \cdot \mathbf{k} = 0. \tag{4.14}$$

Thus, in three-dimensional space, there are only two linearly independent polarization degrees of freedom, which are perpendicular to the direction of propagation of the given plane wave mode. The sum in Eq. (4.10) is thus taken over all wave vectors $\mathbf{k} = (k_x, k_y, k_z)$ and polarizations $\hat{\varepsilon}_1, \hat{\varepsilon}_2$.

In order to construct a quantum theory of the electromagnetic field, we begin by writing down its Hamiltonian, which can be expressed as [59]

$$H = 2\epsilon_0 V \sum_{\mathbf{k},p} \omega_k^2 A_{\mathbf{k},p} A^*_{\mathbf{k},p}, \tag{4.15}$$

where ϵ_0 is the permittivity of the vacuum. This Hamiltonian can be re-written in more familiar form by expressing the mode amplitudes as

$$A_{\mathbf{k},p} = \frac{1}{\sqrt{4\omega_k^2 \epsilon_0 V}} \left(\omega_k X_{\mathbf{k},p} + i P_{\mathbf{k},p} \right) \tag{4.16}$$

$$A^*_{\mathbf{k},p} = \frac{1}{\sqrt{4\omega_k^2 \epsilon_0 V}} \left(\omega_k X_{\mathbf{k},p} - i P_{\mathbf{k},p} \right) \tag{4.17}$$

in which case the Hamiltonian takes the form

$$H = \frac{1}{2} \left(P^2_{\mathbf{k},p} + \omega_k^2 X^2_{\mathbf{k},p} \right). \tag{4.18}$$

This Hamiltonian is mathematically equivalent to the Hamiltonian of a simple harmonic oscillator of unit mass.

In the canonical quantization approach, we construct a quantum theory of the electromagnetic field by promoting the variables $P_{\mathbf{k},p}$ and $X_{\mathbf{k},p}$ to operators $\hat{p}_{\mathbf{k},p}$ and $\hat{x}_{\mathbf{k},p}$ satisfying the canonical commutation relations

$$[\hat{p}_{\mathbf{k},p}, \hat{p}_{\mathbf{k}',p'}] = [\hat{x}_{\mathbf{k},p}, \hat{x}_{\mathbf{k}',p'}] = 0 \tag{4.19}$$

$$[\hat{x}_{\mathbf{k},p}, \hat{p}_{\mathbf{k}',p'}] = i\hbar\, \delta_{\mathbf{k},\mathbf{k}'}\delta_{p,p'}. \tag{4.20}$$

Finally, by introducing the operators

$$a_{\mathbf{k},p} = \frac{1}{\sqrt{2\hbar\omega_k}}(\omega_k \hat{x}_{\mathbf{k},p} + i\hat{p}_{\mathbf{k},p}) \tag{4.21}$$

$$a^\dagger_{\mathbf{k},p} = \frac{1}{\sqrt{2\hbar\omega_k}}(\omega_k \hat{x}_{\mathbf{k},p} - i\hat{p}_{\mathbf{k},p}) \tag{4.22}$$

we can re-write the Hamiltonian of the single-mode quantized electromagnetic field as

$$H = \hbar\omega_k \left(a^\dagger_{\mathbf{k},p} a_{\mathbf{k},p} + \frac{1}{2}\right) = \hbar\omega_k \left(\hat{n}_{\mathbf{k},p} + \frac{1}{2}\right), \tag{4.23}$$

where we have introduced the *photon number operator* $\hat{n}$. The operators $a^\dagger_{\mathbf{k},p}$ and $a_{\mathbf{k},p}$ are called the *creation* and *annihilation* operators respectively. They satisfy the commutation relations

$$[a_{\mathbf{k},p}, a_{\mathbf{k}',p'}] = [a^\dagger_{\mathbf{k},p}, a^\dagger_{\mathbf{k}',p'}] = 0 \tag{4.24}$$

$$[a_{\mathbf{k},p}, a^\dagger_{\mathbf{k}',p'}] = \delta_{\mathbf{k},\mathbf{k}'}\delta_{p,p'}. \tag{4.25}$$

Finally, we express the quantum vector potential of a plane-wave mode in terms if these operators as

$$\hat{A}_{\mathbf{k},p}(\mathbf{r}, t) = \frac{\hbar}{2\epsilon_0 V \omega_k}\left(a_{\mathbf{k},p} e^{-i(\omega_k t - \mathbf{k}\cdot\mathbf{r})} + a^\dagger_{\mathbf{k},p} e^{i(\omega_k t - \mathbf{k}\cdot\mathbf{r})}\right). \tag{4.26}$$

Therefore, in quantum theory, the vector potential is mathematically described as a vector potential operator that assigns an operator to every space-time coordinate $(\mathbf{r}, t)$. Moreover, from the commutation relations (4.24) and (4.25), we see that distinct optical modes are independent systems, since all operators corresponding to distinct modes commute.

4.2 Quantum states of light

In the previous section, we have studied operators associated to the quantized electromagnetic field such as its Hamiltonian, the vector potential operator and the creation and annihilation operators. In this section, we study instead important *states* of the quantized electromagnetic field. Henceforth, we drop the subscripts labelling the modes and focus on the single-mode case unless otherwise stated.

4.2.1 Fock states

For all physical systems, the eigenstates of the Hamiltonian form a natural and convenient basis. In our case, the eigenstates of the Hamiltonian satisfy the eigenvalue equation

$$\hbar\omega \left(a^\dagger a + \frac{1}{2} \right) |n\rangle = E_n |n\rangle. \tag{4.27}$$

It can be shown [59] that this Hamiltonian has a ground state $|0\rangle$ satisfying

$$a|0\rangle = 0, \tag{4.28}$$

where a is the annihilation operator of the mode. The ground state $|0\rangle$ is referred to as the *vacuum* state of the field. Therefore, from Eq. (4.27), the eigenvalue of the ground state is $\frac{1}{2}\hbar\omega$. Additionally, it can be shown that the action of the creation and annihilation operators on the eigenstates of the Hamiltonian are given by

$$a|n\rangle = \sqrt{n}|n-1\rangle \tag{4.29}$$

$$a^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle. \tag{4.30}$$

Therefore, we can construct the eigenstates and eigenvalues of the Hamiltonian by repeated action of the creation operator on the ground state $|0\rangle$. The result is that there are a countably infinite number of eigenstates $\{|n\rangle\}$ with corresponding eigenvalues

$$E_n = \hbar w \left(n + \frac{1}{2} \right) \quad n = 0, 1, 2, \ldots \tag{4.31}$$

The eigenstates of the Hamiltonian are called *Fock states* and they form a complete basis – the Fock basis – for the Hilbert space associated with an optical mode. In particular, they satisfy the completeness relation

$$\sum_{n=0}^{\infty} |n\rangle\langle n| = \mathbb{1}. \tag{4.32}$$

The physical interpretation of a Fock state $|n\rangle$ is that it corresponds to n fundamental particles called *photons*. For example, the state $|1\rangle$ corresponds to the state of a single photon with energy $\hbar\omega$ and the vacuum $|0\rangle$ corresponds to a state with no photons (hence its name).

Fock states can be expressed in terms of the action of the creation operator on the vacuum as

$$|n\rangle = \frac{a^\dagger}{\sqrt{n!}}|0\rangle. \tag{4.33}$$

Therefore, we can interpret the action of this operator as creating a photon in the mode (hence its name). Similarly, from Eq. (4.29), we can interpret the action of the annihilation operator as removing one photon from the field.

Finally, Fock states can be used to define different kinds of photonic qubits. For example, a simple qubit can be defined by two basis states corresponding to the vacuum $|0\rangle$ and single-photon $|1\rangle$ of a single mode. Alternatively, we can define a qubit in terms of single-photon states across two modes. For instance, let $a_H^\dagger$ and $a_V^\dagger$ be the creation operators corresponding respectively to horizontal and vertical polarizations of a a given optical mode. Then we can define a qubit in terms of the basis states

$$|H\rangle := a_H^\dagger|0\rangle \tag{4.34}$$

$$|V\rangle := a_V^\dagger|0\rangle. \tag{4.35}$$

4.2.2 Coherent states

Fock states are eigenstates of the Hamiltonian and, from Eq. (4.23), also eigenstates of the photon number operator $\hat{n}$. We now consider a different class of states which are eigenstates of the annihilation operator a, namely states $|\alpha\rangle$ satisfying

$$a|\alpha\rangle = \alpha|\alpha\rangle. \tag{4.36}$$

The states $|\alpha\rangle$ are known as *coherent states*. Notice that since a is not a Hermitian operator, the eigenvalues α are in general complex numbers. It can be shown that, in terms of the Fock basis, coherent states can be expressed as

$$|\alpha\rangle = e^{-\frac{1}{2}|\alpha|^2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}}|n\rangle. \tag{4.37}$$

Alternatively, coherent states can be written in terms of the action of the displacement operator on the vacuum

$$|\alpha\rangle = D(\alpha)|0\rangle, \tag{4.38}$$

where the displacement operator is given by [59]

$$D(\alpha) = \exp(\alpha a^\dagger - \alpha^* a). \tag{4.39}$$

The expectation value of the photon number operator for a coherent state $|\alpha\rangle$ satisfies

$$\langle\alpha|\hat{n}|\alpha\rangle := \bar{n} = |\alpha|^2 \tag{4.40}$$

and the probability of observing n photons after measuring a coherent state $|\alpha\rangle$ is given by

$$\Pr(n) = e^{-|\alpha|^2}\frac{|\alpha|^{2n}}{n!}, \tag{4.41}$$

which is a Poissonian probability distribution with mean $\mu = |\alpha|^2$. Finally, the overlap of two coherent states $|\alpha\rangle$ and $|\beta\rangle$ satisfies

$$|\langle\alpha|\beta\rangle| = \exp(-\frac{1}{2}|\alpha - \beta|^2). \tag{4.42}$$

Therefore, all coherent states are non-orthogonal.

For a coherent state $|\alpha\rangle$, where $\alpha = |\alpha|e^{i\theta}$, the expectation value of the electric field operator $\hat{E}(\mathbf{r}, t)$ – which can be derived from the vector potential operator of Eq. (4.26) – is given by

$$\langle\alpha|\hat{E}(\mathbf{r}, t)|\alpha\rangle = 2|\alpha|\left(\frac{\hbar\omega_k}{2\epsilon_0 V}\right)^{\frac{1}{2}}\sin(\omega_k t - \mathbf{k}\cdot\mathbf{r} - \theta). \tag{4.43}$$

Thus, for coherent states, the expectation value for the electric field is a sinusoidal wave, with amplitude proportional to $|\alpha|$ and with phase θ. Thus, the parameter θ is usually referred to as the *phase* of the coherent state.

Coherent states are a good approximation of the quantum states of light produced by a laser and therefore, from a practical point of view, they are relatively easy to prepare and manipulate. This makes them versatile and important states that arise in several applications of quantum optics and quantum communication. In fact, in chapter 6, we show that several protocols in quantum communication can be implemented using only coherent states.

4.3 Linear optics

Besides studying important quantum states of light, we are also interested in studying transformations on these states. A simple class corresponds to *linear optics* transformations, which preserve the total photon number of an optical field. A simple example corresponds to the transformation performed by a *phase-shifter*, which transforms the creation operator as

$$a^\dagger \to e^{i\theta} a^\dagger. \tag{4.44}$$

Since any state can be expressed in terms of the Fock basis and any Fock state can be expressed in terms of creation operator, we can use Eq. (4.44) to calculate the action of a phase-shifter on an arbitrary state. For example, a coherent state can be written as

$$|\alpha\rangle = e^{-\frac{1}{2}|\alpha|^2} \sum_{n=0}^{\infty} \frac{\alpha^n}{n!} (a^\dagger)^n |0\rangle, \tag{4.45}$$

which, by the action of a phase-shifter is transformed to

$$\begin{aligned} & e^{-\frac{1}{2}|\alpha|^2} \sum_{n=0}^{\infty} \frac{\alpha^n}{n!} (e^{i\theta} a^\dagger)^n |0\rangle \\ =& e^{-\frac{1}{2}|\alpha|^2} \sum_{n=0}^{\infty} \frac{(\alpha e^{i\theta})^n}{n!} (a^\dagger)^n |0\rangle = |e^{i\theta}\alpha\rangle. \end{aligned} \tag{4.46}$$

Thus, the phase-shifter changes the phase of the coherent state by θ. Physically, a phase-shifter is implemented by introducing a slab of material with a different index of refraction.

General linear optics transformations couple many modes. For example, the action of a *beam splitter* is to transform the creation operators of two different input modes, $a^\dagger_{in}$ and $b^\dagger_{in}$, into the output operators $a^\dagger_{out}$ and $b^\dagger_{out}$ as

$$a^\dagger_{out} = \cos\theta a^\dagger_{in} + ie^{-i\varphi} \sin\theta b^\dagger_{in} \tag{4.47}$$

$$b^\dagger_{out} = ie^{i\varphi} \sin\theta + a^\dagger_{in} \cos\theta b^\dagger_{in}. \tag{4.48}$$

Notice that this relation can equivalently be written in matrix notation as

$$\begin{pmatrix} a^\dagger_{out} \\ b^\dagger_{out} \end{pmatrix} = \begin{pmatrix} \cos\theta & ie^{-i\varphi}\sin\theta \\ ie^{i\varphi}\sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} a^\dagger_{in} \\ b^\dagger_{in} \end{pmatrix}. \tag{4.49}$$

Thus, we can view the action of the beam-splitter as a unitary transformation of the creation operators of the two modes. For example, suppose that we set $\cos\theta = \sin\theta = \frac{1}{\sqrt{2}}$ and $e^{i\varphi} = i$, then the unitary corresponding to the action of the beam-splitter is given by

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}. \tag{4.50}$$

Suppose we have as an input to this beam-splitter a single-photon state $a_{in}^\dagger|0\rangle$. We can calculate the action of the beam-splitter on this state by inverting Eq. (4.49) to express $a_{in}^\dagger$ in terms of the output modes, giving

$$\begin{aligned} a_{in}^\dagger|0\rangle &= \frac{1}{\sqrt{2}}(a_{out}^\dagger - b_{out}^\dagger)|0\rangle \\ &= \frac{1}{\sqrt{2}}(|1,0\rangle - |0,1\rangle). \end{aligned} \tag{4.51}$$

Notice that the beam splitter creates entanglement across the modes, as the output state is mathematically equivalent to a Bell state $|\Psi^-\rangle$. Moreover, the single photon is 'split' equally, in the sense that the probability of observing a photon in either of the two output modes is equal to $\frac{1}{2}$. In general, the parameters $t = \cos^2\theta$ and $r = \sin^2\theta$ are respectively referred to as the *transmittance* and *reflectance* of the beam-splitter. A 50:50 beam-splitter is one for which $r = t = \frac{1}{2}$.

A general linear optics transformation acts on N input modes and transforms them into N output modes. A device performing such a transformation is usually referred to as an N-port *interferometer*. Mathematically, the action of an interferometer can be described by an $N \times N$ unitary transformation U relating the annihilation operators of the input modes $\{a_1, a_2, \ldots, a_N\}$ to the annihilation operators of the output modes $\{a'_1, a'_2, \ldots, a'_N\}$ as

$$a_i = \sum_{j=1}^{N} U_{j,i} a'_j. \tag{4.52}$$

Notably, it has been shown that for any $N \times N$ unitary, there exists an interferometer performing that transformation. Moreover, the interferometer can be implemented using only beam-splitters and phase-shifters [103]. Therefore, although still challenging to implement, general linear optics transformations can be performed in practice, specially if the number of modes is not too large, c.f. [29].

4.3.1 Single-photon detection

Having discussed important quantum states and transformations of optical fields, we now briefly describe a class of measurements on optical fields. A basis for the Hilbert space corresponding to a system of N optical modes can be built from the tensor product of the Fock bases of the individual modes:

$$|n_1, n_2, \ldots, n_N\rangle := |n_1\rangle \otimes |n_2\rangle \otimes \cdots \otimes |n_N\rangle, \tag{4.53}$$

where n_i is the occupation number of the i-th mde, i.e. the number of photons in the mode. We have already made use of this basis when describing the output of a single-photon entering a 50:50 beam-splitter in Eq. (4.51).

In order to make a measurement in this basis, it suffices to make a measurement in the Fock basis of each mode. Devices that can perform such a measurement are called *single-photon number-resolving detectors*. Currently, state-of-the-art detectors can resolve between a few different photon numbers. For instance, transition edge sensors can distinguish up to 8 photons clearly [82]. However, for many applications, it is sufficient to use simpler detectors without number-resolving properties. These detectors are called *single-photon threshold detectors* and they are able to distinguish only between the vacuum and all other Fock states, effectively coarse-graining all non-zero photon numbers into one single outcome. Mathematically, the POVM performed by these detectors is a two-outcome measurement given by the operators $\{|0\rangle\langle 0|, \mathbb{1} - |0\rangle\langle 0|\}$.

4.4 Conclusion

Optical systems provide a rich and versatile platform for the implementation of protocols in quantum communication. The theory of the quantized electromagnetic field has been well understood for decades, but only recently are we unravelling the methods of manipulating optical systems in order to perform quantum communication tasks. In chapter 5, we study a reliable method of analyzing the data from entanglement verification experiments and apply the technique to real experimental data produced from measurements on a system of entangled photonic qubits. In chapters 6 and 7, we explore how new quantum communication protocols with a quantum advantage can be implemented using only coherent states and linear optics transformations.

Chapter 5

Reliable Entanglement Verification

In chapter 3, we have explored how entanglement witnesses can be used to verify the entanglement of physical systems. The expectation value of these witnesses – whether linear or nonlinear – is evaluated from experimental data corresponding to the expectation values of local observables, which are estimated from repeated measurements of a physical system. The data obtained from these measurements is necessarily finite and therefore the claim that entanglement was present can never be issued with certainty. More precisely, there will always be a non-zero probability that the data was produced from a separable state, regardless of what the data may be. Therefore, in any entanglement verification experiment, we are forced to provide statistical statements that quantify our confidence that entanglement was indeed present. Naturally, the procedure that leads to these statements should have a clear interpretation, should not rely on unwarranted assumptions about state preparation and be readily implementable in practice [123].

The most widely used approach consists of computing the standard deviation of measured quantities and using these as error bars to specify the uncertainty of the reported values [63]. However, there are several conceptual issues with this approach [22, 21] and is known to be inadequate to deal with nonlinear expressions [51]. This strongly asks for better alternatives and consequently other approaches have been recently suggested (see e.g. [23]).

In this chapter, we apply the work of Christandl and Renner on quantum state tomography [37] to formulate a reliable method for analyzing the data of entanglement verification experiments. As shown in Ref. [37], the method in principle does not rely on the specification of a prior distribution of prepared states nor on the assumption that they are independent and identically distributed. Additionally, it is suitable for experiments

performing arbitrary quantum measurements and the final statements have a clear and well-defined operational interpretation. The approach relies on the concept of *confidence regions*: regions of state space that contain the true state with high probability [37].

Applying this method requires the specification of a region of state space for all possible measurement outcomes, an issue that is not dealt with directly in Ref. [37]. In the work presented in this chapter, we provide a recipe to assign confidence regions to data obtained from entanglement verification experiments that rely on entanglement witnesses. This assignment requires the evaluation of a non-trivial inequality for which we specifically develop numerical techniques to efficiently calculate it, rendering the entire method ready to be applied to current experiments. We demonstrate this fact by experimentally producing a family of photonic two-qubit states whose entanglement is verified by an accessible nonlinear witness (ANLW) [7].

The remainder of this chapter is organized as follows. For the sake of completeness, we first briefly outline the framework introduced in Ref. [37] and summarize some of its main results. We then proceed to illustrate the data analysis procedure that we build and elucidate the numerical tools that we develop to perform the necessary calculations. Finally, we describe the experimental setup and analyze the results with our technique.

The results presented in this chapter have been published in Ref. [6].

5.1 Confidence regions

We provide an overview of the main results of Ref. [37] and direct the reader to this work for further details. We begin by considering a collection of $n + k$ quantum systems described by a state ρ^{n+k}, each system associated with a Hilbert space $\mathcal{H}$ of dimension d. The measurement is performed only on a randomly selected subset of n systems and is described by a general POVM consisting of a set $\{B_i\}$ of positive operators satisfying $\sum_i B_i = \mathbb{1}_{\mathcal{H}}^{\otimes n}$. In the case of independent measurements of each of the systems, each element B_i will be a tensor product of n positive operators acting on a single copy of the state. However, it must be clear that the formalism does not require this assumption: one should always think of this POVM as an arbitrary, generally collective measurement on $\mathcal{H}^{\otimes n}$. The role of the remaining k systems is to make it operationally clear what we mean by verifying entanglement: the goal of the entanglement verification procedure is to make predictions about the state of these remaining systems. More precisely, we want to know if these systems belong to regions of state space that contain only entangled states. We refer to n as the *number of runs* of the experiment, producing n systems which are

then measured and the outcomes analyzed to build the predictions. Finally, note that instead of selecting the n systems at random, we can alternatively imagine an equivalent situation where the $n+k$ systems are permuted at random and the first n are selected for measurements.

Consider an experiment in which the predictions are made only for a subset of k' subsystems, with $k' < k$. It was noted in Ref. [37] that in the limit of $k \to \infty$, the reduced state of the $n+k'$ subsystems $\rho^{n+k'} = \mathrm{Tr}_{k-k'}(\rho^{n+k})$ can always be described by a permutationally-invariant state of the form $\int P(\sigma)\sigma^{\otimes(n+k')}d\sigma$ [35]. This corresponds to the usual independent and identically distributed (i.i.d) case in which many copies of a true state σ are prepared according to some initial probability distribution $P(\sigma)$. Thus, in the scenario of an experiment that can in principle be repeated an arbitrary number of times ($k \to \infty$) and predictions are made on a sample of k' states, the above result in fact provides a justification of the i.i.d. assumption that is common in the literature. For convenience, we adopt this point of view but remind the reader that the i.i.d. assumption is not necessary for the validity of the upcoming results [37].

The data analysis procedure we employ is a mapping that assigns a particular region of state space to every possible measurement outcome. Crucially, this mapping must be specified before the experiment is carried out. The regions are deemed *confidence regions* if they contain the true state σ with high, user-specified probability. More precisely, for all i, denote by $R(B_i)$ the region assigned to outcome B_i. This region will be a subset of the space of density matrices $\mathcal{D}(\mathcal{H})$ associated to $\mathcal{H}$. The assignment of regions is deemed one that produces confidence regions with confidence level $1-\epsilon$ if it holds that

$$\mathrm{Prob}_{B_i}\left[\sigma \in R(B_i)\right] \geq 1-\epsilon, \quad \forall\sigma, \tag{5.1}$$

where $\mathrm{Prob}_{B_i}\left[\sigma \in R(B_i)\right]$ is the expected probability of success with respect to the distribution $\mathrm{Tr}\left(\sigma^{\otimes n}B_i\right)$ of the measurement outcomes B_i. In this picture, statistical statements take the following form: "We have applied a procedure that, with probability at least $1-\epsilon$, assigns a region containing the prepared state σ". It is important to emphasize that this probability refers to the success of the procedure before any measurements are carried out: in the end, the original input state σ is either definitely contained in the assigned region or not. The quantity $1-\epsilon$ should thus be interpreted as the confidence level of the statement that the state is contained in the assigned region. This statement is valid for all possible states and outcomes and does not depend on extra assumptions about state preparation nor on the prior distribution $P(\sigma)$. This fact makes the procedure reliable and robust even in the cryptographic scenario in which σ might have been chosen maliciously [37].

A main result of Ref. [37] was to provide a criteria to determine whether a given mapping from outcomes to regions succeeds in constructing confidence regions. This result

is summarized as follows. Firstly, for each measurement outcome define the function

$$\mu_i(\sigma) = \frac{1}{\mathcal{N}} \mathrm{Tr}\left(\sigma^{\otimes n} B_i\right) = \frac{1}{\mathcal{N}} \mathcal{L}_i(\sigma), \tag{5.2}$$

where

$$\mathcal{N} = \int_{\mathcal{D}(\mathcal{H})} \mathcal{L}_i(\sigma) d\sigma$$

is a normalization constant. The function $\mathrm{Tr}\left(\sigma^{\otimes n} B_i\right)$ is usually referred to as the *likelihood function*, so that $\mu_i(\sigma)$ is simply its normalized version. Furthermore, let $\{\Gamma_i\}$ be a collection of subsets of $\mathcal{D}(\mathcal{H})$, where the number of these regions is equal to the number of POVM elements $\{B_i\}$. For each set Γ_i define the enlarged set

$$\Gamma_i^\delta = \{\sigma : \exists \sigma' \in \Gamma_i \text{ such that } F(\sigma, \sigma') \geq \sqrt{1-\delta^2}\}, \tag{5.3}$$

where $F(\sigma, \sigma') = \mathrm{Tr}\left(\sqrt{\sqrt{\sigma}\sigma'\sqrt{\sigma}}\right)$ is the fidelity and

$$\delta^2 = \frac{2}{n}\left[\ln\frac{2}{\epsilon} + (d^2-1)\ln n\right]. \tag{5.4}$$

If for all possible outcomes B_i it holds that

$$\int_{\Gamma_i} \mu_i(\sigma) d\sigma \geq 1 - \frac{\epsilon}{c_{n,d}} \tag{5.5}$$

with

$$c_{n,d} = 2n^{(d^2-1)/2}, \tag{5.6}$$

then the assigned regions Γ_i^δ are confidence regions with confidence level $1-\epsilon$ (Corollary 1, [37]). In equation (5.5), $d\sigma$ is the Hilbert-Schmidt measure: the flat measure on the set of density matrices of dimension d induced from the Haar measure on the set of pure states of dimension $d \times d$ [140]. It must be noted that the polynomial factor $2n^{(d^2-1)/2}$ [36] is an improvement on the term appearing in Ref. [37].

The above condition (5.5) can be more conveniently cast by referring directly to the quantity $1 - \int_{\Gamma_i} \mu_i(\sigma) d\sigma$ and making a direct comparison with the term $\epsilon/c_{n,d}$. This can be achieved by instead integrating over the complement regions $\overline{\Gamma_i} = \{\sigma : \sigma \notin \Gamma_i\}$. Therefore we define

$$\begin{aligned} \epsilon_2(B_i, \Gamma_i) &:= \int_{\overline{\Gamma_i}} \mu_i(\sigma) d\sigma \\ &= \frac{\int_{\overline{\Gamma_i}} \mathcal{L}_i(\sigma) d\sigma}{\int_{\mathcal{D}(\mathcal{H})} \mathcal{L}_i(\sigma) d\sigma}. \end{aligned} \tag{5.7}$$

For convenience, we drop the explicit dependence on B_i and Γ_i from $\epsilon_2(B_i, \Gamma_i)$ whenever it is not necessary, while keeping in mind that its value will depend on the measurement outcome and the region assigned to it. Condition (5.5) can then be more conveniently cast as

$$\epsilon_2 \cdot c_{n,d} \leq \epsilon. \tag{5.8}$$

In summary, the assigned regions $\{\Gamma_i\}$ determine whether criteria (5.8) is satisfied for some fixed value of ϵ and whenever it is, the enlarged regions Γ_i^δ constitute confidence regions. It is these latter regions that we assign to each individual outcome in our data analysis procedure.

It is very important to note the role played by the polynomial factor $c_{n,d}$ and the enlarging parameter δ. Because the dimension of the Hilbert space d is fixed for a given experiment and typically large, the factor $c_{n,d}$ of Eq. (5.6) will be a high-order polynomial in the number of runs n. Satisfying condition (5.8) will require ϵ_2 to be much smaller than the value of the parameter ϵ that quantifies the confidence of the procedure. This can be problematic for small n but will play only a minor role for larger values because ϵ_2 decreases exponentially in n whenever the maximum of the function $\mu_i(\sigma)$ is contained in the region Γ_i [37].

On the other hand, as will be seen later in this chapter, the size of the complement region $\overline{\Gamma_i}$ increases as δ grows larger, implying that large values of δ result in larger values of ϵ_2. In particular, whenever $\delta \geq 1$ (which can occur for sufficiently low n) it will hold that the region $\overline{\Gamma_i}$ will be equal to the entire state space $\mathcal{D}(\mathcal{H})$ and consequently $\epsilon_2 = 1$. Thus, for a fixed confidence level, the value of n for which $\delta = 1$ sets a lower limit on the number of runs of the experiment that are required to verify the presence of entanglement. This is illustrated in Fig. 5.1. These features indicate that in this framework, it is usually necessary to accumulate large amounts of data in order to reliably report the presence of entanglement.

We have in hand a method to verify whether a set of prescribed regions are in fact confidence regions. The question then remains of how to choose these regions in the first place, an issue that is not addressed in Ref. [37]. Although the results of Christandl and Renner were originally targeted at quantum state tomography, we instead apply these results in the context of entanglement verification. We now describe a procedure for entanglement verification that fully specifies how to assign confidence regions in terms of entanglement witnesses.

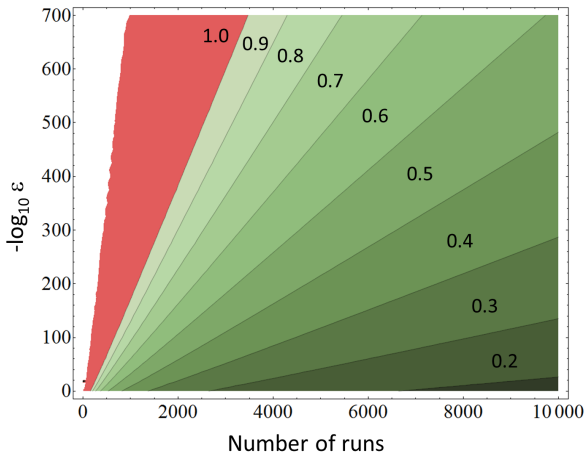


Figure 5.1: Contour plot of δ as a function of the confidence and number of runs n. The red region to the left represents the case when $\delta > 1$, illustrating a lower bound on the number of runs that must be performed to achieve a certain value of ϵ, quantified by the quantity $-\log_{10}\epsilon$. In practice, even larger values of n will be required to meet a desired confidence.

5.2 Entanglement verification procedure

The goal of an entanglement verification experiment is to determine whether a prepared state is entangled or not with the highest possible certainty. In the language of confidence regions this translates to the task of deciding with the highest level of confidence possible whether the prepared state lies in a region consisting only of entangled states.

The starting point of our procedure is the specification of an entanglement witness W and a POVM $\{B_i\}$ whose possible outcomes are sufficient to determine the expectation value of W. In our description, $w(\sigma)$ refers to the expectation value of a linear or nonlinear witness, such as those described in chapter 3. Recall that in order to verify entanglement whenever it is present, we need to assign confidence regions that contain only entangled states. For this purpose, we define

$$\Gamma_W^\delta := \{\sigma : w(\sigma) < 0\} \tag{5.9}$$

as the set of detected states. From the definition of an entanglement witness, Γ_W^δ contains only entangled states. Our goal will be to report Γ_W^δ as the confidence region whenever possible. Going back to definition (5.3), notice that the set Γ_i^δ is defined for a fixed Γ_i. But

in our picture, we are interested in always reporting regions that contain only entangled states. Therefore, we alternatively choose to fix the reported region Γ_W^δ and construct the smaller regions implicitly. From (5.3), it can be directly seen that if Γ_W^δ is fixed, its corresponding subregion Γ_W is defined by

$$\Gamma_W := \{\sigma : \max_{\sigma' \in \overline{\Gamma_W^\delta}} F(\sigma, \sigma') < \sqrt{1-\delta^2}\}. \tag{5.10}$$

We are now ready to specify the mapping from outcomes to regions that constitutes the data analysis procedure for reliable entanglement verification.

Data analysis procedure. To construct confidence regions with confidence level $1-\epsilon$ in an entanglement verification experiment, apply the following rule to assign a region to each outcome B_i:

1. Fix ϵ.
2. For each possible measurement outcome B_i, compute $\epsilon_2(B_i, \Gamma_W) = \int_{\overline{\Gamma_W}} \mu_i(\sigma) d\sigma$.
3. If condition (5.8) holds, i.e. if $\epsilon_2 \cdot c_{n,d} \leq \epsilon$, assign the set of detected states Γ_W^δ. Otherwise, assign the entire state space $\mathcal{D}(\mathcal{H})$.

Therefore, we assign only two possible regions: the set of detected states Γ_W or the entire state space $\mathcal{D}(\mathcal{H})$. Note that the entire state space is trivially a confidence region for any given confidence level, so that our assignment indeed produces confidence regions. However, assigning the entire state space must be interpreted as the statement that for the given confidence level, it is not possible to certify that the set of detected states contains the true state.

Even though the procedure is now completely specified, we are still faced with the difficulty of calculating ϵ_2. As a first step, we note that it is preferable to find a simpler way to characterize the set Γ_W. One way to do this is to find a subset of Γ_W that can be more easily described. We now show that such a subregion can always be found in terms of a bound on the expectation value of a linear entanglement witness.

Observation 6. *Let W be an entanglement witness and let the number $\alpha > 0$ satisfy $\alpha > 2||W||_\infty \delta$. Then the set $\Gamma_\alpha = \{\sigma : Tr(\sigma W) < -\alpha\}$ is a subregion of Γ_W.*

Proof: In order to prove the claim we only need to show that $F^2(\sigma,\sigma') < 1-\delta^2$ whenever $\mathrm{Tr}\,(\sigma W) < -\alpha$ and $\mathrm{Tr}\,(\sigma' W) > 0$. We begin by considering the following general inequality:

$$\begin{aligned} |\mathrm{Tr}\,[(\sigma'-\sigma)W]\,| &= |\langle W, \sigma'-\sigma\rangle| \\ &\leq ||W||_\infty ||\sigma'-\sigma||_1 \\ &\leq 2||W||_\infty \sqrt{1-F^2(\sigma,\sigma')} \end{aligned} \tag{5.11}$$

where we have used *Hölder's inequality*

$$|\langle \sigma, W\rangle| \leq ||\sigma||_1 ||W||_\infty \tag{5.12}$$

and the *Fuchs-van de Graaf inequality* [56]

$$||\sigma'-\sigma||_1 \leq 2\sqrt{1-F^2(\sigma,\sigma')}. \tag{5.13}$$

Now let $\mathrm{Tr}\,(\sigma W) = -\alpha$ and $\mathrm{Tr}\,(\sigma' W) = \beta$ for some $\alpha, \beta > 0$. Inserting into (5.11) and rearranging we get

$$F^2(\sigma,\sigma') \leq 1 - \left(\frac{\beta+\alpha}{2||W||_\infty}\right)^2.$$

We want to find a condition on α such that $F^2(\sigma,\sigma') < 1-\delta^2$ for any β. This will occur whenever

$$\begin{aligned} 1 - \left(\frac{\beta+\alpha}{2||W||_\infty}\right)^2 &< 1-\delta^2 \\ \Rightarrow \alpha &> 2||W||_\infty \delta - \beta. \end{aligned}$$

Since this inequality must hold for all β, we can restrict ourselves to the worst case scenario of $\beta = 0$ to obtain

$$\alpha > 2||W||_\infty \delta \tag{5.14}$$

as desired. ■

This result is illustrated in Fig. 5.2. Unfortunately, obtaining a similar and useful result for nonlinear witnesses is difficult: the value of the nonlinear witness may differ greatly for two states even if their fidelity is high.

Note that because $\Gamma_\alpha \subseteq \Gamma_W$, it holds that

$$\int_{\overline{\Gamma_\alpha}} \mathcal{L}_i(\sigma) d\sigma \geq \int_{\overline{\Gamma_W}} \mathcal{L}_i(\sigma) d\sigma \quad \forall i, \tag{5.15}$$

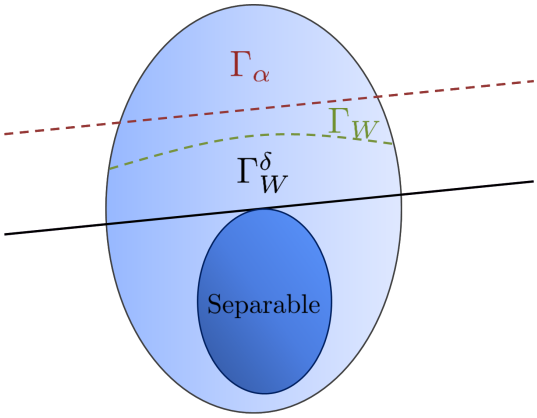


Figure 5.2: The region Γ_W^δ is fixed as the set of states detected by a linear entanglement witness W. This region can be seen as the set of states *above* the black line. Fixing Γ_W^δ implicitly defines a region Γ_W that determines if criteria (5.8) is satisfied. This region is located above the dashed green line labelled Γ_W. The required numerical efforts are greatly simplified by realizing that the set of states Γ_α above the dashed red line constitute a subregion of Γ_W as in Observation 6.

since $\mathcal{L}_i(\sigma) \geq 0$. Therefore if condition (5.8) is satisfied when integrating over $\overline{\Gamma_\alpha}$, it will always be satisfied for the integral over $\overline{\Gamma_W}$.

Typically, it is possible to assign the set of detected states as a confidence region for very high confidence levels i.e. with $\epsilon \ll 1$. Therefore, from now on we quantify the confidence level of the procedure by the more appropriate quantity

$$C = -\log_{10} \epsilon, \tag{5.16}$$

which we refer to as the *confidence* of the entanglement verification procedure. We further define this quantity to be zero whenever the assigned region is the entire state space $\mathcal{D}(\mathcal{H})$. Thus, higher values of the confidence result in higher certainty that the state is contained in the set of detected states.

From the description of the data analysis procedure, it should be clear that the crucial step is the computation of ϵ_2: a highly non-trivial task that requires the normalization of the likelihood function as well as its integral over the implicitly defined set Γ_W. In the following section, we construct and illustrate a series of tools developed to numerically evaluate an upper bound on ϵ_2, ensuring a method to verify condition (5.8). We note that

other numerical techniques for evaluating integrals of likelihood functions have recently been developed in Refs. [110, 109].

5.3 Numerical tools

There are several difficulties in calculating ϵ_2. An analytical approach is essentially intractable owing primarily to the high dimensionality of parameter space and the non-trivial geometry of the space of positive semi-definite operators [17]. Moreover, the region of integration $\overline{\Gamma_W}$ is not known in closed form but can only be cast as a black-box i.e. we can only ask whether a state lies in this region or not. Finally, we require any approximation of ϵ_2 to provide an upper bound on its value in order to ensure that the inequality $\epsilon_2 \leq c_{n,d}\epsilon$ is always satisfied.

Fortunately, high-dimensional integration over black-box constraints can be handled with the use of Monte Carlo techniques. Most of these techniques are well summarized in [47]. In the Monte Carlo approach, the mean value of the integrand is approximated by the average value of samples randomly drawn from the region of integration, which in conjunction with knowledge of the hyper-volume of the integration region can be used to calculate the value of the integral. Importantly, the number of samples can be chosen independently of the underlying dimension and any constraint can be straightforwardly incorporated by checking whether a sample point lies within the constraint region.

More specifically, the simplest version of a Monte Carlo technique to approximate a general integral of the form $\int_R f(\sigma)d\sigma$ involves a random sequence of N density operators $\{\sigma_1, \sigma_2, \ldots, \sigma_N\}$ uniformly sampled inside the region R according to the measure $d\sigma$. By definition, the average $\langle f \rangle_R$ of a function over a region R satisfies

$$\int_R f(\sigma)d\sigma = \langle f \rangle_R \cdot V_R, \tag{5.17}$$

where $V_R = \int_R d\sigma$ is the hyper-volume of the integration region. The goal in Monte Carlo integration is to approximate the average of the function from the random sample. Namely, we approximate the value of the integral as

$$\int_R f(\sigma)d\sigma \approx \left[\frac{1}{N}\sum_{j=1}^{N} f(\sigma_j)\right] \cdot V_R, \tag{5.18}$$

while keeping in mind that all sampled states lie in the integration region. Convergence to the true value of the integral is guaranteed as $N \to \infty$ due to the law of large numbers

[47]. A main drawback of this approach is that convergence can be extremely slow for highly-peaked functions such as $\mathcal{L}_i(\sigma)$, since only very rarely will a state be drawn from the region surrounding the maximum of the function. This is particularly troublesome for our purposes because an error in the calculation of ϵ_2 can lead to wrong conclusions about the confidence of the procedure. For this reason, we now introduce an approach that can be easily and efficiently implemented and provides an upper bound on ϵ_2.

We first note that such a bound can be achieved by introducing a lower bound on the normalization constant $\mathcal{N}$. Since the likelihood function is strictly positive, this can always be achieved by integrating over a subregion R of $\mathcal{D}(\mathcal{H})$, i.e.

$$\epsilon_2 \leq \frac{\int_{\overline{\Gamma_W}} \mathcal{L}_i(\sigma) d\sigma}{\int_R \mathcal{L}_i(\sigma) d\sigma}. \tag{5.19}$$

We can use this fact to our advantage by restricting R to be a region around the maximum of $\mathcal{L}_i(\sigma)$. Note that this maximum is unique and is in general achieved for a convex set of states [23]. Ideally, this region should be chosen to satisfy $\int_R \mathcal{L}_i(\sigma) d\sigma \approx \int_{\mathcal{D}(\mathcal{H})} \mathcal{L}_i(\sigma) d\sigma$ in order to provide a tight bound, but this is not necessary as the bound is guaranteed to hold for any R. Additionally, because the likelihood function is more flat around the maximum and R is much smaller than $\mathcal{D}(\mathcal{H})$, drawing random states within R will greatly improve the convergence of a Monte Carlo integration.

We now illustrate how this region R can be constructed from a hyper-rectangle in parameter space. Following the convention of [139], we begin by parametrizing any state $\sigma \in \mathcal{D}(\mathcal{H})$ in terms of the real-valued Bloch vector $\tau = (\tau_1, \tau_2, \ldots, \tau_{d^2-1})$ as

$$\sigma(\tau) = \frac{1}{d}\mathbb{1} + \sum_{j=1}^{d^2-1} \tau_j \hat{\lambda_j}, \tag{5.20}$$

where the operators $\{\hat{\lambda_j}\}$ are an orthogonal set of traceless Hermitian generators of $SU(d)$ satisfying $\mathrm{Tr}\left(\hat{\lambda_j}^2\right) = 1$. Any operator written in such a form is immediately Hermitian and of unit trace but may be non-positive for some vectors τ. Thus, it will be important to keep in mind that not all possible vectors yield valid density matrices. With this parametrization, the likelihood function will be a function of the Bloch vector $\mathcal{L}_i(\sigma) = \mathcal{L}_i(\tau_1, \tau_2, \ldots, \tau_{d^2-1})$. Our goal will be to define a region around the maximum that contains only valid states for which the value of the likelihood function is sufficiently large.

Construction of integration regions. To construct a region R to be used in an approximation of the normalization of the likelihood function, perform the following:

1. Calculate the maximum value of the likelihood function $\mathcal{L}_i^{\max}$ and find a vector $\tau^* = (\tau_1^*, \tau_2^*, \ldots, \tau_{d^2-1}^*)$ for which this maximum is attained.

2. Find, for all j, the lowest possible quantities $x_j^{\pm} > 0$ such that $\mathcal{L}_i(\tau_1^*, \tau_2^*, \ldots, \tau_j^* \pm x_j^{\pm}, \ldots, \tau_{d^2-1}^*) = \mathcal{L}_i^{\max}/\eta$ for some fixed number $\eta > 0$. If no such values can be found for some j, let $x_j^{\pm} = \infty$.

3. Find, for all j, the highest possible quantities $y_j^{\pm} > 0$ such that $\sigma(\tau_1^*, \tau_2^*, \ldots, \tau_j^* \pm y_j^{\pm}, \ldots, \tau_{d^2-1}^*)$ is still a valid density matrix.

4. Define $r_j^{\pm} = \min\{x_j^{\pm}, y_j^{\pm}\}$. Then the integration region R is equal to all the valid density matrices within the hyper-rectangle r defined by $r = \{\tau : \tau_j^* - r_j^- \leq \tau_j \leq \tau_j^* + r_j^+, \forall j\}$.

This construction is illustrated in Fig. 5.3. Note that the task of maximizing the likelihood function can be performed efficiently and is routine in the context of quantum state tomography. A good choice of η will in general depend on each individual problem, but it should be chosen to be large enough to include only regions that contribute significantly to the integral.

Once the hyper-rectangle has been constructed, it is straightforward to perform the Monte Carlo integration by sampling uniformly within the rectangle, while keeping only operators in that sample that are valid density matrices. Let these sampled states form the set $\{\sigma_1, \sigma_2, \ldots, \sigma_N\}$. The target integral is then given by

$$\begin{aligned} \int_R \mathcal{L}_i(\sigma) d\sigma &\approx \left[\frac{1}{N} \sum_{j=1}^{N} \mathcal{L}_i(\sigma_j) \right] \cdot V_R \\ &= \langle \mathcal{L}_i \rangle_R \cdot V_R. \end{aligned} \tag{5.21}$$

Because typical values of the likelihood function are extremely small, it is preferable to work with the logarithm of the function and use the identity

$$\log(a+b) = \log[\exp(\log a - \log b) + 1] + \log b \tag{5.22}$$

to add the values of $\mathcal{L}_i(\sigma_j)$ at each step of the algorithm and determine $\langle \mathcal{L}_i \rangle_R$ as in equation (5.21).

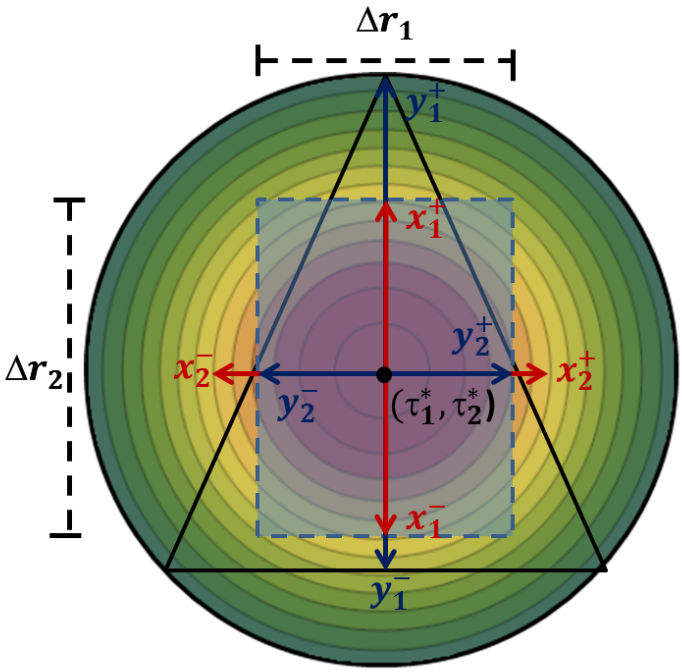


Figure 5.3: Construction of integration regions. We imagine a two-dimensional section of parameter space characterized by the variables τ_1 and τ_2. Only the region inside the triangle contains valid density matrices and contours of $\mathcal{L}_i(\sigma)$ are shown in the background. To construct the integration region we do the following: 1. Find the maximum of the function and a state for which it occurs, in this case (τ_1^*, τ_2^*). 2. From this maximum, find the displacements $x_1^\pm$ and $x_2^\pm$ such that the value of the function is decreased by a specified amount, in this case corresponding to the 6th contour line. 3. Find the displacements $y_1^\pm$ and $y_2^\pm$ that define the points where the boundary of valid states is met. 4. By choosing the minimum of these quantities in each direction, we construct a rectangle (dashed) and the integration region is the intersection of this rectangle with the space of valid density matrices.

In order to calculate V_R, we use the fact that the Hilbert-Schmidt metric on the space of quantum states generates the Hilbert-Schmidt measure [139]. The Hilbert-Schmidt distance between two density matrices is given by

$$D_{HS}(\sigma_1, \sigma_2) = ||\sigma_1 - \sigma_2||_2 = \sqrt{\mathrm{Tr}\left[(\sigma_1 - \sigma_2)^2\right]}. \tag{5.23}$$

This correspondence between metric and measure implies that the volume of the hyper-rectangle r can be found in the usual sense as the product of the length of its sides with respect to the Hilbert-Schmidt metric. More specifically, let $\sigma_j^{\pm} = \sigma(\tau_1^*, \ldots, \tau_j^* \pm r_j^{\pm}, \ldots, \tau_{d^2-1}^*)$. Then the length Δr_j of the jth side of r is given simply by

$$\begin{aligned} \Delta r_j &= D_{HS}(\sigma_j^+, \sigma_j^-) \\ &= ||r_j^+ \hat{\lambda}_j + r_j^- \hat{\lambda}_j||_2 = r_j^+ + r_j^-, \end{aligned} \tag{5.24}$$

where we have used the fact that the operators $\hat{\lambda}_j$ are normalized with respect to the Hilbert-Schmidt inner product. The hyper-volume V_r of r is then given by

$$V_r = \prod_{j=1}^{d^2-1} \Delta r_j. \tag{5.25}$$

This correspondence is also useful in generating a random sample, as one needs only to obtain a random number within the intervals $[\tau_j^* - r_j^-, \tau_j^* + r_j^+]$. Because not all operators in r are valid density matrices, V_r is in general larger than the hyper-volume V_R of the integration region R. However, one can estimate R from knowledge of the fraction f of the randomly drawn operators that are valid density matrices. The relationship between these quantities is

$$V_R \approx f \cdot \prod_{j=1}^{d^2-1} \Delta r_j, \tag{5.26}$$

which can finally be inserted in (5.21) to provide the numerical calculation of the target integral

$$\int_R \mathcal{L}_i(\sigma) d\sigma \approx \left[\frac{1}{N} \sum_{j=1}^{N} \mathcal{L}_i(\sigma_j)\right] \cdot f \cdot \prod_{k=1}^{d^2-1} \Delta r_k. \tag{5.27}$$

To calculate f, it is sufficient to verify how many of the drawn operators are valid density operators and divide this number by the total number of randomly drawn operators.

One could imagine that a similar technique could be used to calculate the integral $\int_{\overline{\Gamma_W}} \mathcal{L}_i(\sigma) d\sigma$ appearing in the definition of ϵ_2. Unfortunately, this would greatly increase the computational efforts in the construction of R since one must additionally ensure that each of the drawn samples lie in $\overline{\Gamma_W}$. Additionally, in this case, restricting the integration region results in an incorrect lower bound on ϵ_2. Instead, we can construct an upper bound on this integral via the maximum of the likelihood function as

$$\begin{aligned} \int_{\overline{\Gamma_W}} \mathcal{L}_i(\sigma) d\sigma &= \langle \mathcal{L}_i \rangle_{\overline{\Gamma_W}} \cdot V_{\overline{\Gamma_W}} \\ &\leq \left(\max_{\sigma \in \overline{\Gamma_W}} \mathcal{L}_i(\sigma) \right) \cdot V_{\mathcal{D}(\mathcal{H})}, \end{aligned} \tag{5.28}$$

where $V_{\mathcal{D}(\mathcal{H})}$ is the Hilbert-Schmidt hyper-volume of the entire state space. This volume was calculated explicitly in [139] for Hilbert spaces of arbitrary dimension. We can then combine this result with our previous bound on the normalization constant to provide an overall upper bound on ϵ_2. Since this value will be typically very small and in order to make a direct comparison with the confidence, we henceforth refer to the logarithm of ϵ_2 for which we now have the inequality

$$\log_{10} \epsilon_2 \leq \log_{10} \left(\frac{\max_{\sigma \in \overline{\Gamma_W}} \mathcal{L}_i(\sigma)}{\langle \mathcal{L}_i \rangle_R} \frac{V_{\mathcal{D}(\mathcal{H})}}{V_R} \right). \tag{5.29}$$

Of course, the average of the likelihood function over $\overline{\Gamma_W}$ will generally be much smaller than the maximum over this region, making the bound very loose. However, in practice this is not a problem because the above bound on ϵ_2 is dominated by the much larger differences between the global maximum of the function and its maximum over $\overline{\Gamma_W}$. More specifically, for experiments with a large number of runs (large n), it will typically hold that

$$|\log_{10} \left(\frac{\max_{\sigma \in \overline{\Gamma_W}} \mathcal{L}_i(\sigma)}{\langle \mathcal{L}_i \rangle_R} \right)| \gg |\log_{10} \left(\frac{\langle \mathcal{L}_i \rangle_{\overline{\Gamma_W}}}{\max_{\sigma \in \overline{\Gamma_W}} \mathcal{L}_i(\sigma)} \right)|, \tag{5.30}$$

so that

$$\begin{aligned} &\log_{10} \left(\frac{\langle \mathcal{L}_i \rangle_{\overline{\Gamma_W}}}{\langle \mathcal{L}_i \rangle_R} \right) = \\ &\log_{10} \left(\frac{\max_{\sigma \in \overline{\Gamma_W}} \mathcal{L}_i(\sigma)}{\langle \mathcal{L}_i \rangle_R} \frac{\langle \mathcal{L}_i \rangle_{\overline{\Gamma_W}}}{\max_{\sigma \in \overline{\Gamma_W}} \mathcal{L}_i(\sigma)} \right) \\ &\approx \frac{\max_{\sigma \in \overline{\Gamma_W}} \mathcal{L}_i(\sigma)}{\langle \mathcal{L}_i \rangle_R} \end{aligned} \tag{5.31}$$

and the value for $\log_{10}\epsilon_2$ is not altered significantly by the loose bound.

The final quantity we must be able to calculate is the maximum of the likelihood function over $\overline{\Gamma_W}$. This again is a non-trivial global optimization problem involving a black-box constraint. As in the case of integration, the particular features of this problem impede the usual techniques and strongly ask for a Monte Carlo approach. To handle the optimization in the general case, we employ an adaptation to the quantum scenario of a simulated annealing algorithm (SA) based on the Metropolis-Hastings algorithm outlined in [21].

The SA algorithm is based on a biased random walk that preferentially moves to states with higher values of the objective function while still accepting moves to lower values with a probability governed by a global "temperature" parameter. This last feature prevents the algorithm from being confined in local maxima. Unfortunately, this same feature makes the convergence slow, usually requiring many steps to reach close proximity to the maximum. For each step, one must additionally make the costly verification that the states lie in the region of integration $\overline{\Gamma_W}$, so it must be understood that run times are usually long. A detailed description of the algorithm is included in Appendix A.

One drawback of the SA algorithm is that due to its stochastic nature, independent runs of the algorithm will generally yield different values. Moreover, by construction, these values cannot be larger than the global maximum. In order to address this issue, one should estimate the numerical error by performing many independent runs of the algorithm and collecting statistics of the sample values. The usual choice is to calculate the standard deviation of the values [47] and take this as the error. It is then important to ensure that condition (5.8) is satisfied well within this error.

Nevertheless, we are still interested in obtaining a more efficient method to solve the maximization problem. We can achieve this for the case of linear witnesses by noting that for the subregion Γ_α of Γ_W, it holds that

$$\max_{\sigma\in\overline{\Gamma_\alpha}} \mathcal{L}_i(\sigma) \geq \max_{\sigma\in\overline{\Gamma_W}} \mathcal{L}_i(\sigma) \tag{5.32}$$

since in that case $\overline{\Gamma_W}$ is a subregion of $\overline{\Gamma_\alpha}$. Therefore, we can provide a final expression for the bound on ϵ_2 as

$$\log_{10}\epsilon_2 \leq \log_{10}\left(\frac{\max_{\sigma\in\overline{\Gamma_\alpha}} \mathcal{L}_i(\sigma)}{\langle\mathcal{L}_i\rangle_R}\frac{V_{\mathcal{D}(\mathcal{H})}}{V_R}\right) \tag{5.33}$$

where Γ_α is defined as in observation 6. This expression has the enormous advantage that because the constraint over Γ_α is convex and $\mathcal{L}_i(\sigma)$ is log-convex, the maximization of $\mathcal{L}_i(\sigma)$

over this region can be calculated with vastly greater efficiency using standard methods in convex optimization.

We are additionally interested in reporting the highest possible confidence level, which corresponds to the case in which the equality $\epsilon_2 \cdot c_{n,d} = \epsilon$ holds. The value of ϵ_2 depends on the region Γ_W which in turn implicitly depends on ϵ through the definition of the enlarging parameter δ, so that the above equality is in principle an equation to be solved for ϵ. Unfortunately, there is no clear method of how to solve the equation directly, primarily because of the difficulty of calculating ϵ_2 itself. Instead, to achieve the highest possible confidence level, one must iteratively adapt the chosen value of ϵ until $\epsilon_2 \cdot c_{n,d} \approx \epsilon$ while still satisfying the inequality (5.8).

With these tools in hand it is now possible to apply the reliable entanglement verification procedure for both linear and nonlinear witnesses. We now proceed to demonstrate the features of the method by applying the technique to data obtained from an experiment generating a family of entangled two-photon states. The entanglement of these states is verified with the use of an accessible nonlinear witness.

5.4 Experiment

To apply our entanglement verification procedure to real experimental data, we aimed to produce photon pairs in the maximally entangled states $|\Phi^\phi\rangle = \frac{1}{\sqrt{2}}\left(|HH\rangle + e^{i\phi}|VV\rangle\right)$, where $|H\rangle$ and $|V\rangle$ are defined respectively as single-photon states of polarization parallel and perpendicular to the optical table. A frequency doubled titanium-sapphire laser (80 MHz, 790 nm) was used to pump a pair of orthogonally oriented 1 mm β-Barium borate (BBO) crystals, as seen in Fig. 5.4. By pumping with diagonal polarization $|D\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle + |V\rangle\right)$, the pump may produce photon pairs via type-I noncollinear spontaneous parametric down-conversion (SPDC) in either the first or second crystal [78]. Bismuth borate, α-BBO, and quartz crystals were used to ensure that each path was spatially and temporally indistinguishable, and the photon pairs were filtered using bandpass filters with a centre wavelength of 790 nm and a bandwidth FWHM of 3 nm. The single photon signal was measured with avalanche photodiodes (APDs) and coincidences were recorded within a 3 ns window.

Single photons were detected at a rate of approximately 200 kHz in each arm, with a coincidence rate of approximately 35 kHz. A quarter-wave plate was tilted to introduce an arbitrary phase shift between horizontally and vertically polarized components, allowing control over the phase ϕ. This setup constitutes part of the setup used for the experiment

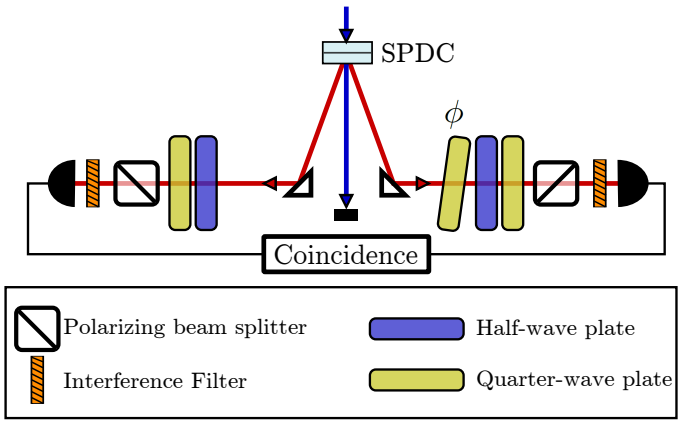


Figure 5.4: Experimental setup for producing $|\Phi^{\phi}\rangle = \frac{1}{\sqrt{2}}\left(|HH\rangle + e^{i\phi}|VV\rangle\right)$ polarization states. Photon pairs are generated via type-I noncollinear SPDC in a pair of orthogonally oriented BBO crystals and analyzed with wave plates and polarizing beamsplitters. The phase ϕ is adjusted by tilting a quarter-wave plate.

reported in [80]. The two-photon state was prepared for six values of ϕ, corresponding to a waveplate tilt range of twelve degrees and transforming the state from $|\Phi^-\rangle$ to $|\Phi^+\rangle$.

Projective measurements were taken in three bases, corresponding to the eigenbases of the operators $\{\sigma_x \otimes \sigma_x, \sigma_y \otimes \sigma_y, \sigma_z \otimes \sigma_z\}$. We refer to the elements of these bases as $|x_i\rangle\langle x_i|$, $|y_i\rangle\langle y_i|$ and $|z_i\rangle\langle z_i|$ respectively. For example, the eigenbasis of $\sigma_z \otimes \sigma_z$ is given by $|z_1\rangle = |HH\rangle, |z_2\rangle = |HV\rangle, |z_3\rangle = |VH\rangle, |z_4\rangle = |VV\rangle$, and similarly for the other bases. To verify the entanglement of these states, an accessible nonlinear witness was constructed from the linear witness

$$W = (1/4)(\mathbb{1} + \sigma_x \otimes \sigma_x - \sigma_y \otimes \sigma_y + \sigma_z \otimes \sigma_z). \tag{5.34}$$

Following the results presented in chapter 3, the expectation value $w_\infty(\sigma)$ of the nonlinear witness for a state σ can be expressed as

$$w_\infty(\sigma) = \mathrm{Tr}\,(\rho W) - |c|^2 - \frac{|d|^2}{1-|k|^2}, \tag{5.35}$$

where

$$\begin{aligned} c &= \mathrm{Tr}\left[\sigma(|\psi^-\rangle\langle\psi^-|U)^\Gamma\right] \\ k &= \mathrm{Tr}\left(\sigma U^\Gamma\right) \\ d &= \mathrm{Tr}\,(\sigma W) - ck, \end{aligned}$$

$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle)$ and the superscript Γ denotes partial transposition. By choosing $U = \sigma_z \otimes \sigma_z$, this expectation value can be computed from the expectation value of the aforementioned operators and the nonlinear witness is *accessible* [7]. An accessible nonlinear witness was chosen because, unlike its linear counterpart, it detects these entangled states for most values of ϕ.

In this experiment, all measurements are independent so that each element of the POVM $\{B_i\}$ is a tensor product of the operators corresponding to possible individual outcomes. The likelihood function takes the form

$$\mathcal{L}_i(\sigma) = \prod_{j=1}^{4} \mathrm{Tr}\left(\sigma|x_j\rangle\langle x_j|\right)^{n_x^j} \cdot \mathrm{Tr}\left(\sigma|y_j\rangle\langle y_j|\right)^{n_y^j} \cdot \mathrm{Tr}\left(\sigma|z_j\rangle\langle z_j|\right)^{n_z^j}, \tag{5.36}$$

where n_x^j is the number of times outcome $|x_j\rangle\langle x_j|$ is obtained and similar definitions hold for the other operators, so that the total number of measurement outcomes is $n = \sum_{j=1}^{4} n_x^j + n_y^j + n_z^j$. Note that in this case the measurement outcome B_i is fully specified by the numbers $\{n_x^j, n_y^j, n_z^j\}$. In the experiment, six states were prepared corresponding to six different values of the parameter ϕ. The measurement outcomes for each case are summarized in Fig. 5.5.

We have calculated the confidence as in equation (5.16) for the six preparations of the entire experiment. These results are illustrated in Table 5.1. We can report very high confidences for almost all states, with the exception of state 4 for which condition (5.8) cannot be satisfied for any value of ϵ. This is not entirely surprising as this state presents the weakest correlations in the $\{|x_j\rangle\langle x_j|\}$ and $\{|y_j\rangle\langle y_j|\}$ bases leading to a value of the nonlinear witness that is closest to zero, as seen in Table 5.1. Thus, the outcomes for this case most closely resemble the ones that could be obtained from a separable state. This again is evidence that only large data which are clearly inconsistent with separable states can lead to the reliable statements obtained from our procedure.

Additionally, we are interested in understanding how the maximum achievable confidence depends on the total number of runs of an experiment. It is also important to gain insight on the cost of using the bound of observation 6 for linear witnesses. For this purpose, samples of different size were randomly selected from the outcomes of experiment (6) in Fig. 5.5. That is, from the entire set of observations in this experiment (shown in Fig. 5.5), we randomly selected a subset of all the data and interpreted it as arising from an experiment with a fewer number of runs (counts). The confidence was calculated for each of them using both regions Γ_W and Γ_α, this latter being possible because this state is also detected by the linear witness. The obtained values using these two different methods is portrayed in Fig. 5.7 and Table 5.2.

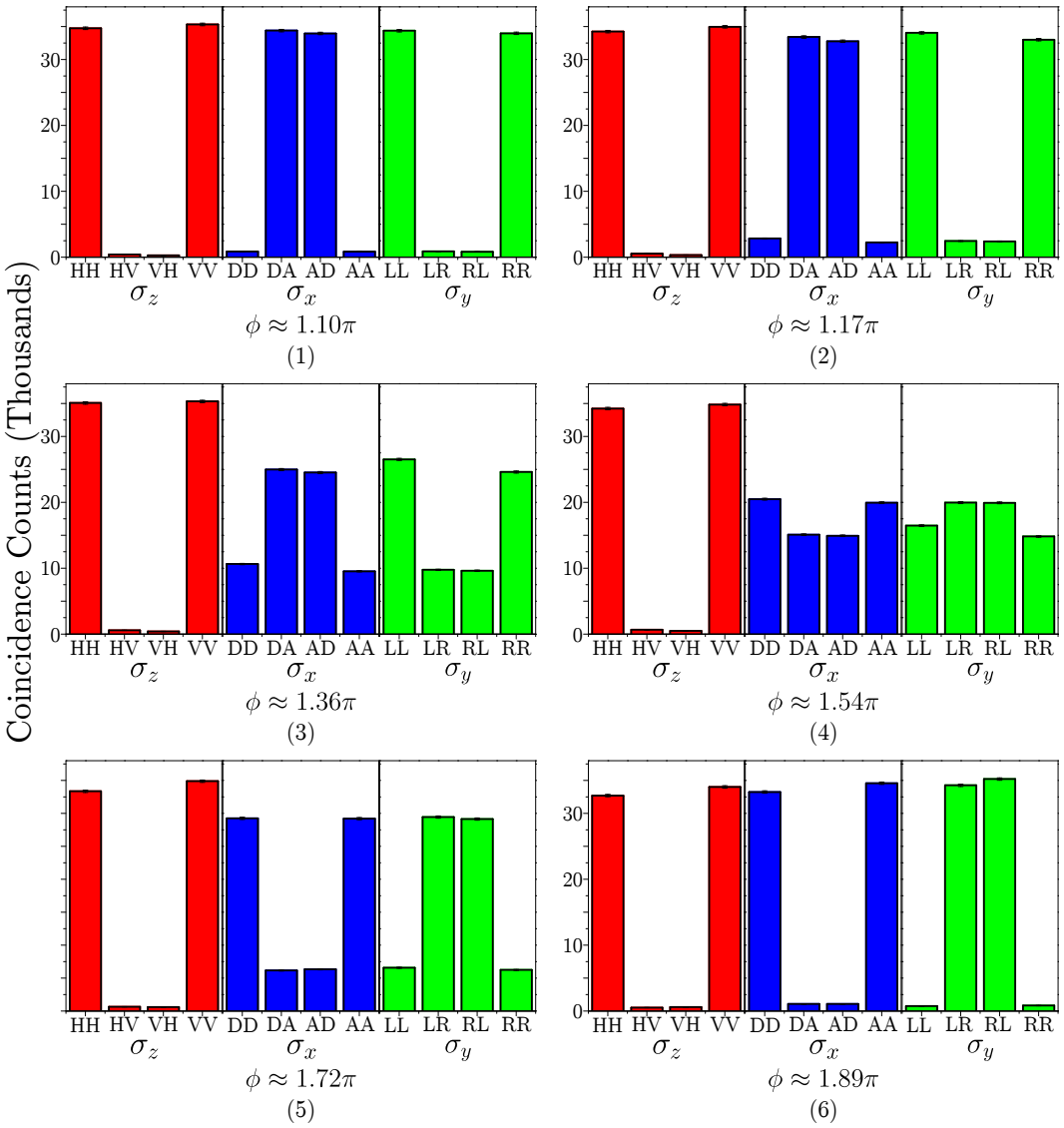


Figure 5.5: Results of projective measurements on six states of the form $\frac{1}{\sqrt{2}}\left(|HH\rangle + e^{i\phi}|VV\rangle\right)$, corresponding to the eigenbases of the operators $\{\sigma_x \otimes \sigma_x, \sigma_y \otimes \sigma_y, \sigma_z \otimes \sigma_z\}$. The approximate value of the phase is included for each case. 1 s of data was taken per measurement.

State	Approximate phase	Confidence	w_∞
1	1.10π	5150	-23.0
2	1.17π	2050	-15.2
3	1.36π	410	-3.4
4	1.54π	0	-0.3
5	1.72π	1819	-5.8
6	1.89π	4980	-13.6

Table 5.1: Calculation of the confidence and value of the nonlinear witness for all prepared states in the experiment. The total number of counts obtained in each case was roughly 35,000.

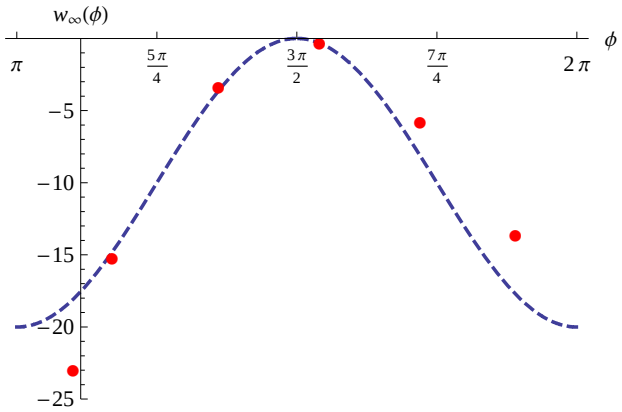


Figure 5.6: Value of the nonlinear witness $w_\infty(\phi)$ for the six states prepared in the experiment (dots). The value of the nonlinear witness for the family of states $\sigma(\phi) = (1-p)|\Phi^\phi\rangle\langle\Phi^\phi| + \frac{p}{4}\mathbb{1}$ with $p = 1/42$ is shown in the background (dashed). This curve is included only to illustrate the values of ϕ for which it is difficult to verify entanglement and should not be interpreted as a fit to the data. The value of p was chosen to adjust the scaling to the recorded values.

Total counts	Confidence (Γ_α)	Confidence (Γ_W)
1500	0	0
3000	18	24
6000	165	200
15000	300	315
30000	660	700
60000	1378	1500

Table 5.2: Calculation of the confidence for samples of different size from the outcomes of experiment 6 based on Γ_W and Γ_α.

The results indicate that, as a percentage of the total confidence, the loss introduced by considering Γ_α is small. It is also clear that a large number of runs are necessary in order to report a non-zero confidence, in accordance to our understanding of the role of the enlarging parameter δ. To estimate the numerical error present in the SA algorithm, we performed 20 independent runs of the algorithm for the data of state 1 and found the error to be 1.85%. In all calculations it was ensured that condition (5.8) was satisfied by at least ten times this numerical error. In the construction of the integration regions a value of $\eta = 10^5$ was chosen for all cases. Finally, the CVX package for specifying and solving convex programs [44] was used to numerically calculate the global maximum of the likelihood function, as well as its maximum over Γ_α.

5.5 Conclusion

In this chapter, we have applied the work of Christandl and Renner in Ref. [37] to the case of entanglement verification. Through the concept of confidence regions, we have provided a procedure to make reliable and efficient statistical statements quantifying the confidence level of having entanglement present in a physical system. These statements have a clear operational interpretation and in principle do not require the specification of a prior distribution nor the assumption of independent measurements or i.i.d. sources. We have shown that this method can be applied in practice by developing specific numerical tools designed to calculate all necessary quantities. For the particular case of experiments relying on linear entanglement witnesses, we have shown that the procedure can be implemented efficiently using only plain Monte Carlo integration and convex optimization methods. The procedure is ready to be applied to current experiments as we demonstrated

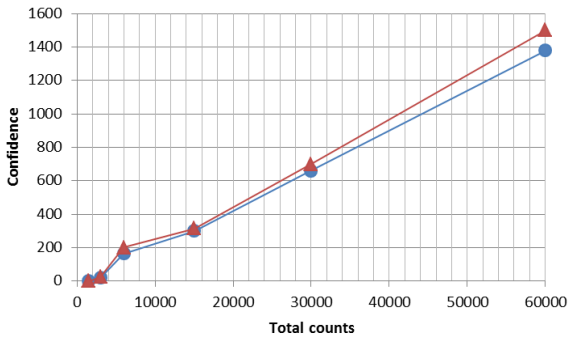


Figure 5.7: Confidence for random samples of different size, quantified by the total number of counts. The confidences were calculated for Γ_W (triangles) and Γ_α (dots). These results illustrate that the bound introduced by considering the subregion Γ_α is small and is not an impediment to reach a very large confidence. In the case of 1500 total counts, the confidence is zero, consistent with our understanding that a large number of outcomes are needed in order to reliably report entanglement with our technique. Moreover, the data shows that the confidence is roughly linear in the number of outcomes.

by applying the technique to data obtained from an experiment generating entangled two-photon states. However, the procedure has a significant drawback, which is that large amounts of data are necessary in order for the size of the confidence regions to be small enough to be able to verify entanglement. However, this is very likely to an issue arising from the proof techniques of Ref. [37], which in principle can be improved to construct confidence regions that converge faster to the actual state.

It is important to note that this work assumes that there are no systematic errors in the measurements performed. In any real experiment, there will always be discrepancy between the intended measurement and the one actually performed, no matter how small this discrepancy is. These systematic errors can in principle lead to incorrect statements and a method to incorporate it in the framework should be pursued. Numerical techniques also invariably involve errors and these should also be clearly incorporated in the framework. Future research may lead to improved algorithms, such as has been done in Refs. [110, 109]. Finally, let us note that it is often desirable to quantify the amount of entanglement present as opposed to just verifying it. Our technique can in principle be applied to such cases by reporting regions that contain states with at least a certain amount of entanglement.

Chapter 6

Quantum Communication with Coherent States and Linear Optics

In the previous chapter, we studied techniques to verify the entanglement of physical systems. As we saw before, these investigations are motivated by the fact that entanglement plays a crucial role in several tasks in quantum computation and quantum communication. However, there are great experimental challenges associated with controlling large quantum systems and generating states of such systems that exhibit large amounts of entanglement. Consequently, the difficulty of generating highly entangled states of large systems places severe barriers to our current capabilities of experimentally realizing several interesting protocols. The situation is even more dire in quantum communication, where we are effectively restricted to using light as the carrier of information, without an option of employing the advantages of other physical systems. Therefore, if we are serious about our goal of demonstrating protocols with a quantum advantage – such as those discussed in chapter 2 – we must understand the extent to which we can deploy quantum protocols with available techniques.

In terms of experimental implementations, only quantum key distribution (QKD) has been routinely demonstrated and deployed over increasingly complex networks and large distances [117, 107]. This is possible largely due to the fact that, fundamentally, QKD can be carried out with sequences of independent signals and measurements [108]. Important progress has been made in implementing other quantum communication protocols [16, 132, 96, 38, 86, 83, 41, 20, 98], but there remain several examples of quantum improvements that have never been realized experimentally. This is largely due to the fact that, in their abstract formulation, these protocols require the preparation and transmission of complex quantum states as well as performing sophisticated operation on them, making

them difficult to implement. Notably, in the case of quantum communication complexity, only a few proof-of-principle implementations have been reported [137, 122, 71].

Confronted with this challenges we face two alternatives: We can either strive to improve current technology or we can flip the issue around and ask: Can protocols in quantum communication be adapted to a form that makes them ready to be deployed with available techniques? To adopt the latter strategy is to push for a theoretical reformulation that converts previously intractable protocols into a form that, while conserving their relevant features, eliminates the obstacles affecting their implementation. This is precisely the road that has already been successfully followed for QKD.

In this chapter, we describe an abstract mapping that converts quantum communication protocols that use pure states of multiple qubits, unitary operations, and projective measurements into another class of protocols that use only a sequence of coherent states, linear optics operations, and measurements with single-photon threshold detectors. The new class of protocols requires a number of optical modes equal to the dimension of the original states, but the total number of photons can be chosen independently from the dimension and is typically very small. The protocols obtained from the mapping share important properties with the original ones, meaning that they can also fulfil the goal that the original protocols where intended to achieve. Overall, the mapping is suitable for its application to protocols that originally require a moderate number of qubits, but are still hard to implement with usual methods.

In the remainder of this chapter, we describe the mapping in detail and discuss the various properties of the coherent-state protocols. We proceed by examining how the mapping can be applied to construct protocols in quantum communication complexity and describe a protocol for the hidden matching problem which can be realized with technology that is within current reach. The results presented in this chapter have been published in Refs. [9] and [8].

6.1 Coherent-state protocols

We consider a wide class of quantum communication protocols that require only three basic operations: the preparation of pure states of a fixed dimension, unitary transformations on these states, and projective measurements on a canonical basis. The simplest form of a protocol in this class is one in which Alice prepares a state $|\psi\rangle$ and sends it to Bob, who then applies a unitary transformation U_B to that state, followed by a projective measurement on the canonical basis. More complex protocols can be constructed by increasing the number

of these basic operations as well as the number of parties. Even though these protocols generally involve states of some arbitrary dimension d, it is common to think of them as corresponding to a system of $O(\log_2 d)$ qubits. Hence, we refer to them as *qubit protocols*.

An *exact* implementation of such protocols can be achieved without the use of actual physical qubits by instead considering a single photon in a linear combination of optical modes. Any pure state $|\psi\rangle = \sum_{k=1}^{d} \lambda_k |k\rangle$, with $\sum_{k=1}^{d} |\lambda_k|^2 = 1$, can be equally thought of as the state of a single photon in a linear combination of d modes

$$a_\psi^\dagger |0\rangle = \sum_{k=1}^{d} \lambda_k b_k^\dagger |0\rangle, \tag{6.1}$$

where $a_\psi^\dagger = \sum_{k=1}^{d} \lambda_k b_k^\dagger$ for a collection of creation operators $\{b_1^\dagger, b_2^\dagger, \ldots, b_d^\dagger\}$ corresponding to d optical modes.

In this picture, unitary operations correspond exactly to linear optics transformations [103], and measurements in the canonical basis are equivalent to a photon counting measurement in each of the modes. Note that the quantum information is encoded by photons residing in linear combinations of modes.

From a practical perspective, the issue with implementing qubit protocols in terms of a single photon in a linear combination of modes is that the experimental preparation of these states presents daunting challenges. Instead, we are interested in an adaptation of this formulation of qubit protocols into another that is more readily implementable in practice. As discussed in Ref. [89], as an alternative to a single photon we can consider a single coherent state in a linear combination of modes. In that case, instead of the state of Eq. (6.1), we have

$$D_{a_\psi}(\alpha)|0\rangle = \bigotimes_{k=1}^{d} |\alpha\, \lambda_k\rangle_k, \tag{6.2}$$

where $D_{a_\psi}(\alpha) = \exp(\alpha a_\psi^\dagger - \alpha^* a_\psi)$ is the displacement operator. Once again, the quantum information is encoded in the mode structure, but we have a coherent state instead of the single-photon of Eq. (6.1) as the quantum state of light. Remarkably, this state is equivalent to a tensor product of coherent states over d optical modes.

With this idea in mind, we now outline a method for converting qubit protocols into another class of protocols that, although seemingly disparate, actually retain the essential properties of the original ones. We call these *coherent-state protocols* since they can be implemented by using only coherent states of light and linear optics operations. The recipe for constructing coherent-state protocols is specified by the following rules:

Coherent-state mapping

1. The original Hilbert space $\mathcal{H}$ of dimension d with canonical basis $\{|1\rangle, |2\rangle, \ldots, |d\rangle\}$ is mapped to a set of d orthogonal optical modes with corresponding annihilation operators $\{b_1, b_2, \ldots, b_d\}$:
$$|k\rangle \longrightarrow b_k. \tag{6.3}$$

2. A state $|\psi\rangle = \sum_{k=1}^{d} \lambda_k |k\rangle$ is mapped to a coherent state with parameter α in the mode $a_\psi = \sum_{k=1}^{d} \lambda_k b_k$:
$$|\psi\rangle \longrightarrow |\alpha, \psi\rangle := \bigotimes_{k=1}^{d} |\alpha\, \lambda_k\rangle_k,$$
where $|\alpha\, \lambda_k\rangle_k$ is a coherent state with parameter $\alpha\, \lambda_k$ in the k-th mode. The value of the amplitude α can be chosen freely as a parameter of the mapping, independently of the dimension d, but remains fixed.

3. A unitary operation U acting on a state in $\mathcal{H}$ is mapped into linear optics transformation corresponding to the same unitary operator U acting on the modes $\{b_1, b_2, \ldots, b_d\}$. Thus, the transformation of a state is linked to a transformation of the modes as:
$$|\psi'\rangle = U|\psi\rangle \longrightarrow b_k = \sum_l U_{kl} b'_l. \tag{6.4}$$
This linear optics network has the effect of transforming the coherent state $|\alpha, \psi\rangle = \bigotimes_{k=1}^{d} |\alpha\, \lambda_k\rangle_k$ to the state
$$|\alpha, \psi'\rangle = \bigotimes_{k=1}^{d} |\alpha\, \lambda'_k\rangle_k, \tag{6.5}$$
where $\lambda'_k = \sum_l U_{kl} \lambda_l$. This is the same state obtained from applying the mapping directly to the output state $|\psi'\rangle$ of the original protocol.

4. A projective measurement in the canonical basis $\{|1\rangle, |2\rangle, \ldots, |d\rangle\}$ is mapped into a two-outcome measurement in each of the modes with single-photon threshold detectors:
$$\{|1\rangle\langle 1|, |2\rangle\langle 2|, \ldots, |d\rangle\langle d|\} \longrightarrow \left\{ \bigotimes_{k=1}^{d} F_{\mathrm{c}}^{k} \right\}, \tag{6.6}$$
where $c =$ "click", "no-click", $F^k_{\text{no-click}} = |0\rangle\langle 0|$ is a projection onto the vacuum state of the modes, $F^k_{\text{click}} = \sum_{n=1}^{\infty} |n\rangle_k \langle n|_k$, and $|n\rangle_k$ is a state with n photons in the $k-$th

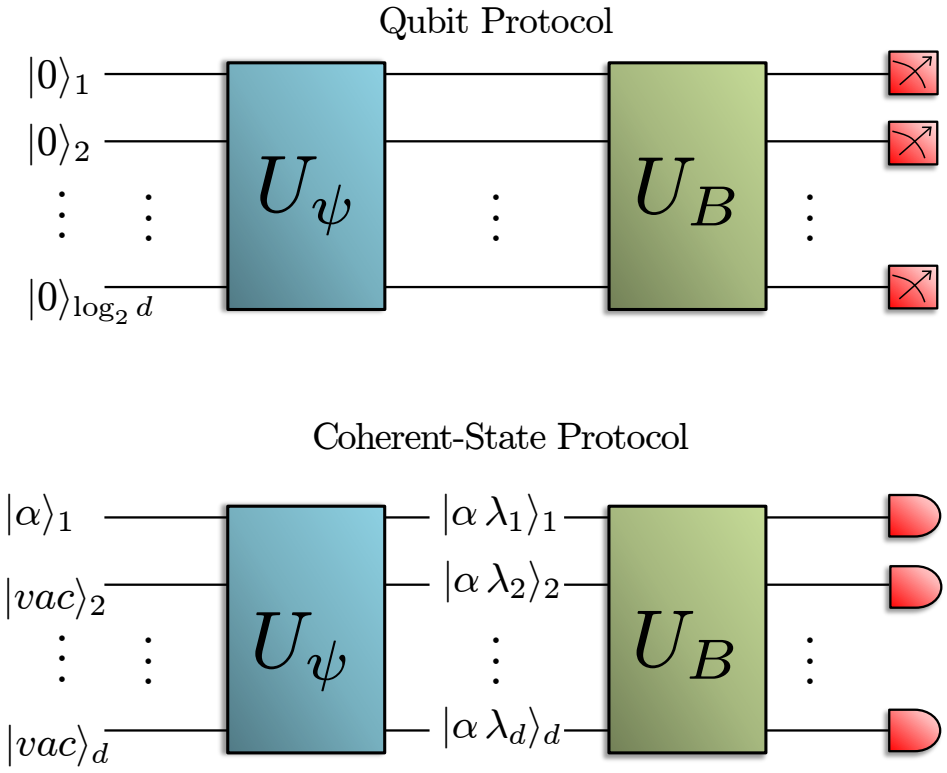


Figure 6.1: In a simple qubit protocol, Alice prepares a state $|\psi\rangle = \sum_{k=1}^{d} \lambda_k |k\rangle$ of $\log_2 d$ qubits by applying a unitary transformation U_ψ on an inital state $|\bar{0}\rangle := |0\rangle^{\otimes \log_2 d}$. She sends the state to Bob, who applies a unitary transformation U_B and measures the resulting state in the computational basis. In the equivalent coherent-state protocol, the initial state corresponds to a coherent state in a single mode and the vacuum on the others. The state $|\alpha, \psi_x\rangle = \bigotimes_{k=1}^{d} |\alpha\,\lambda_k\rangle_k$ is prepared by applying the transformation U_ψ to the optical modes. This state is sent to Bob, who applies the transformation U_B and consequently measures each mode for the presence of photons with threshold single-photon detectors.

mode. As such, an outcome in a coherent-state protocol corresponds to a pattern of clicks across the modes.

Since any qubit protocol can be constructed from the basic operations of state preparation, unitary transformations, and projective measurements, the above instructions are sufficient to construct the coherent-state version of any qubit protocol. However, as there are 2^d possible outcomes compared to the d possible outcomes of the qubit protocol, the interpretation of the outcomes in the coherent-state protocol is not immediately provided by the mapping. Nevertheless, as will be discussed later, the statistics closely resemble those of the original protocol and they can be thought of as arising from several independent runs of the original qubit protocol. As an illustration, a simple qubit protocol and its coherent-state counterpart are depicted in Fig. 6.1.

An immediate appealing property of coherent-state protocols is that their implementation faces much lesser obstacles than their qubit counterparts. Indeed, the fundamental challenge of a quantum-optical implementation of qubit protocols lies in the difficulty of generating entangled states of many qubits and performing global unitary transformations on them. On the other hand, coherent-state protocols face significantly less daunting obstacles. The experimental generation of coherent states is a commonplace task and the construction of linear-optical circuits can, in principle, be realized with simple devices such as beam splitters and phase-shifters [103], though experimental challenges may remain depending on the required unitary operation. Moreover, the platforms for linear optics experiments continue to improve at a fast rate, most notably with the development of integrated optics [120, 29].

As we have mentioned already, an advantage of coherent-state protocols is that they employ a coherent state in a linear combination of modes, which is equivalent to a tensor product of individual coherent states across the various modes. However, qubit protocols usually require high amounts of entanglement. This seems to indicate that the 'quantumness' of the original qubit protocol has been lost through the mapping. Nevertheless, it is important to realize that this is not the case, as coherent-state protocols showcase a truly quantum property: non-orthogonality. Given two states $|\alpha, \psi\rangle = \bigotimes_{k=1}^{d} |\alpha\, \lambda_k\rangle_k$ and $|\alpha, \varphi\rangle = \bigotimes_{k=1}^{d} |\alpha\, \nu_k\rangle_k$, with $d \gg |\alpha|^2$, the amplitude of the individual coherent states will typically satisfy $|\alpha\, \lambda_k| \sim |\frac{\alpha}{\sqrt{d}}| \ll 1$. Therefore, the inner product of the individual states obeys

$$|\langle \alpha\, \nu_k | \alpha\, \lambda_k \rangle|^2 = e^{-|\alpha(\lambda_k - \nu_k)|^2} \approx 1, \tag{6.7}$$

and so the individual states are typically highly non-orthogonal.

In fact, it can be useful to intuitively think of the coherent-state mapping as an exchange between entanglement and non-orthogonality, since an implementation of qubit protocols with actual physical qubits usually requires entanglement amongst the qubits.

In coherent-state protocols, the average photon number—$|\alpha|^2$—is a parameter that can be chosen independently of the dimension of the states of the original qubit protocol. This is to be put in contrast with any quantum protocol that encodes a qubit in the degrees of freedom of a photon, which inevitably requires a number of photons that scales with the dimension of the states. Hence, coherent-state protocols offer an intrinsic saving in the number of photons required for their implementation. The drawback, of course, is that the required number of optical modes is equal to the dimension of the states in the original protocol. This implies that the mapping will lead to practical protocols only if the dimension of the original states is comparable to the number of modes that can be efficiently manipulated with existing technologies.

Fortunately, current laser sources can operate with clock rates above 1GHz [48], permitting the generation of a very large number of modes per second. This makes it possible in practice to apply the mapping to quantum communication protocols involving states of a moderate number of qubits. As we discuss in section 6.2, there are many qubit protocols to which we can apply the mapping that require only a modest number of qubits but still currently escape the grasp of direct implementations. From a theoretical perspective, the relationship between these two types of protocols may provide an insight into the trade-offs between different resources in quantum communication, as well as into the interplay between entanglement and non-orthogonality in quantum mechanics.

Now that we have specified how to construct coherent-state protocols, our goal is to understand their properties. We pay special attention to their resemblance to qubit protocols, but also concentrate on understanding the features that may provide an advantage over their qubit counterparts or find applications in quantum communication.

6.1.1 Transmitted information

We are often interested in quantifying the amount of transmitted information that takes place in a quantum protocol. Informally, this is done by counting the number of qubits that are employed. But what happens if a protocol uses physical systems that are manifestly *not* qubits? As discussed in chapter 2, we quantify the transmitted information in terms of the smallest number of qubits that would be required, in principle, to replicate the performance of the protocol. More precisely, if a quantum protocol uses states in a Hilbert space of dimension d, this space can be associated with a system of $O(\log_2 d)$ qubits. Therefore,

the amount of communication C in a quantum protocol is generally given by

$$Q = \log_2[\dim(\mathcal{H})], \tag{6.8}$$

where $\mathcal{H}$ is the smallest Hilbert space containing all states of the protocol, which can be a significantly smaller than the entire Hilbert space associated with the physical systems. Moreover, Holevo's theorem [69] guarantees that no more than $O(\log_2 d)$ classical bits of information could be transmitted, on average, by a quantum protocol that uses states in a Hilbert space of dimension d.

By quantifying the amount of communication carefully, we gain a better understanding of the different physical resources that are required to transmit a certain amount of information. For example, the fact that the same amount of information can be transmitted by a single photon in n optical modes, at most n photons in a single mode or $\log_2 n$ polarization qubits, is understood because the smallest Hilbert space containing all possible states in each of the three cases has the same dimension.

Quantifying the amount of transmitted information in qubit protocols is straightforward. For coherent-state protocols obtained from the mapping, even though the *actual* Hilbert space associated with all possible signal states is large (distinct coherent states are linearly independent), they effectively occupy a small Hilbert space, as is expressed in the following theorem:

Theorem 7. *[10] Let $|\alpha, \psi\rangle$ be a state with parameter α obtained using the coherent-state mapping from a state $|\psi\rangle$ of dimension d. Then for any $\epsilon > 0$, there exists a Hilbert space $\mathcal{H}_\alpha$ such that*

$$\begin{aligned} &\langle \alpha, \psi | P_{\mathcal{H}_\alpha} | \alpha, \psi \rangle \geq 1 - \epsilon, \\ &\log_2[dim(\mathcal{H}_\alpha)] = O(|\alpha|^2 \log_2(|\alpha|^2 + d)), \end{aligned}$$

and where $P_{\mathcal{H}_\alpha}$ is the projector onto $\mathcal{H}_\alpha$.

Proof: For a given $\Delta > 0$, we choose $\mathcal{H}_\alpha$ to be the subspace spanned by the set of Fock states $\{|n_1, n_2 \ldots n_d\rangle\}$ over d modes whose total photon number $n = \sum_{k=1}^{d} n_k$ satisfies $|n - |\alpha|^2| \leq \Delta$. In other words, this is the space of states whose total photon number is close to $|\alpha|^2$.

The dimension of the Hilbert space spanned by states of n photons is equal to the the number of distinct ways in which n photons can be distributed into the d different modes. Since the photons are indistinguishable, this quantity is given by the binomial

factor $\binom{n+d-1}{d-1}$ [112]. In the case of $\mathcal{H}_\alpha$, there are 2Δ different possible values of n, the largest being $n = |\alpha|^2 + \Delta$. Thus, the dimension $dim(\mathcal{H}_\alpha)$ of this subspace satisfies

$$dim(\mathcal{H}_\alpha) \leq 2\Delta \binom{|\alpha|^2 + \Delta + d - 1}{d-1}, \tag{6.9}$$

which gives

$$\begin{aligned} \log_2[dim(\mathcal{H}_\alpha)] \leq & \log_2 \left[2\Delta \binom{|\alpha|^2 + \Delta + d - 1}{d-1} \right] \\ \leq & (|\alpha|^2 + \Delta) \log_2 \left[(|\alpha|^2 + \Delta + d - 1) \right] + \log_2(2\Delta), \end{aligned} \tag{6.10}$$

which is $O(|\alpha|^2 \log_2(d + |\alpha|^2))$ for any fixed ϵ.

Now notice that the number $\langle \alpha, \psi | P_{\mathcal{H}_\alpha} | \alpha, \psi \rangle$ is equal to the probability of performing a photon number measurement on $|\alpha, \psi\rangle$ and obtaining a value n satisfying $|n - |\alpha|^2| \leq \Delta$. Since any coherent state $|\alpha, \psi\rangle$ has a Poissonian photon number distribution with mean $|\alpha|^2$, independently of $|\psi\rangle$, we can use the properties of this distribution to calculate the probability that the measured number of photons lies within the desired range. This probability satisfies [54]

$$P(|n - |\alpha|^2| \geq \Delta) \leq 2e^{-|\alpha|^2} \left(\frac{e|\alpha|^2}{|\alpha|^2 + \Delta} \right)^{|\alpha|^2 + \Delta} \tag{6.11}$$

which can be made equal to any $\epsilon > 0$ by choosing Δ accordingly while keeping α fixed. ■

Therefore, the fact that the mean photon number $|\alpha|^2$ is fixed in coherent-state protocols leads to the states involved effectively occupying a Hilbert space of dimension that is comparable to that of the original one. This implies that the asymptotic behaviour of the amount of transmitted information is the same for both classes of protocols. In fact, Eq. (6.9) provides a precise bound on the transmitted information. Moreover, the effectively unused sections of the entire Hilbert space can still be used, in principle, for other purposes such as the transmission of additional classical or quantum information through multiplexing schemes. A method for achieving this in practice is a line for future research.

It is important to note that this correspondence in the transmitted information is not exactly mirrored in terms of the expenditure of physical resources. A coherent-state protocol obtained from the mapping employs d modes but a number of photons that is tunable and independent of this dimension. This is to be put in contrast with any quantum protocol that encodes a qubit in the degrees of freedom of a single photon, which employs $O(\log_2 d)$ optical modes and $O(\log_2 d)$ photons.

6.1.2 Outcome probabilities

In qubit protocols, the probability of obtaining an outcome k upon a measurement of a state $|\psi\rangle = \sum_{k=1}^{d} \lambda_k |k\rangle$ is given by

$$p_k = |\langle k|\psi\rangle|^2 = |\lambda_k|^2, \tag{6.12}$$

with $\sum_{k=1}^{d} p_k = 1$. For coherent-state protocols, the situation is different since we are performing independent measurements on each of the modes. In this case, the individual detector clicks are not mutually exclusive: We can have many clicks across the various modes, or even no clicks at all.

Nevertheless, for the state $|\alpha, \psi\rangle$, the probability distribution of the number of photons in each mode is equivalent to the one obtained from many repetitions of a measurement on the single-photon state $|\psi\rangle = \alpha_\psi^\dagger |0\rangle$ of Eq. (6.1), where the number of repetitions is drawn from a Poisson distribution with mean $\mu = |\alpha|^2$.

To see this, first note that the state $|\alpha, \psi\rangle$ can be written as

$$\begin{aligned} |\alpha, \psi\rangle &= D_{a_\psi}(\alpha)|0\rangle \\ &= e^{-\frac{1}{2}|\alpha|^2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle_{a_\psi}. \end{aligned} \tag{6.13}$$

The state of n photons in mode α_ψ is itself given by

$$|n\rangle_{a_\psi} = \frac{1}{\sqrt{n!}} (\alpha_\psi^\dagger)^n |0\rangle = \frac{1}{\sqrt{n!}} \left(\sum_{k=1}^{d} \lambda_k b_k^\dagger \right)^n |0\rangle. \tag{6.14}$$

For this state, the probability of obtaining $n_1, n_2, \ldots, n_d$ photons in each of the modes $b_1, b_2, \ldots, b_d$, with $\sum_k n_k = n$, is given by

$$\Pr(n_1, \ldots, n_d) = \frac{n!}{n_1! \ldots n_d!} |\lambda_1|^{2n_1} \ldots |\lambda_d|^{2n_d}, \tag{6.15}$$

which, from the multinomial theorem, is exactly equal to that obtained from n measurements of the single-photon state $|\psi\rangle = \alpha_\psi^\dagger |0\rangle$. Since the number of photons n in the state $|\alpha, \psi\rangle$ are Poissonian distributed with mean $\mu = |\alpha|^2$, this proves the claim.

Whenever possible, we will not use photon-number resolving detectors in protocols obtained from coherent-state mapping, but threshold detectors that give clicks or no clicks. Note that while the statistics of photon counts is directly derived from the Poissonian

distribution of repetitions of the single-photon protocol, this does not hold for the statistics of clicks of the threshold detectors.

However, for most states, the coefficients λ_k will typically be very small, so that the mean number of photons $|\alpha\,\lambda_k|^2$ will also be small provided α is not too large. Then it is unlikely that more than one photon will be present in each mode, and the number-resolving properties of the detectors are not necessary.

For example, with threshold detectors, the probability of obtaining a click on the k-th mode after a measurement of a state $|\alpha,\psi\rangle = \bigotimes_{k=1}^{d} |\alpha\,\lambda_k\rangle_k$ is given by

$$p_{\alpha,k} = 1 - \exp(-|\alpha\,\lambda_k|^2), \tag{6.16}$$

which for $|\alpha\,\lambda_k| \ll 1$ gives

$$p_{\alpha,k} \approx |\alpha\,\lambda_k|^2. \tag{6.17}$$

If we choose $|\alpha|^2 = 1$, we recover a behaviour very similar to that of the qubit protocol: Only one click is expected to occur and it does so with a probability that is essentially identical to that of the original protocol.

In any case, the multiple-photon property of a coherent-state protocol constitutes a potential advantage over its qubit counterpart. The expected number of clicks can be controlled by modifying α appropriately, and a larger number of clicks will give rise to more information gained per measurement.

6.1.3 State overlap

All of the physically-relevant information of a set of quantum states $\{|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_N\rangle\}$ is contained in its Gram matrix, which is defined as

$$G_{i,j} = \langle\psi_i|\psi_j\rangle. \tag{6.18}$$

Thus, for quantum communication protocols defined over a set of possible signal states, it is natural to ask how the overlap between states behaves under a coherent-state mapping. The answer is provided by the following observation.

Observation 8. *Let $|\psi\rangle = \sum_k \lambda_k|k\rangle$ and $|\varphi\rangle = \sum_k \nu_k|k\rangle$ be two arbitrary states with overlap $\langle\psi|\varphi\rangle = \delta$. Then the overlap of their coherent-state versions satisfies*

$$\delta_\alpha := \langle\psi,\alpha|\varphi,\alpha\rangle = \exp\left[|\alpha|^2(\delta-1)\right]. \tag{6.19}$$

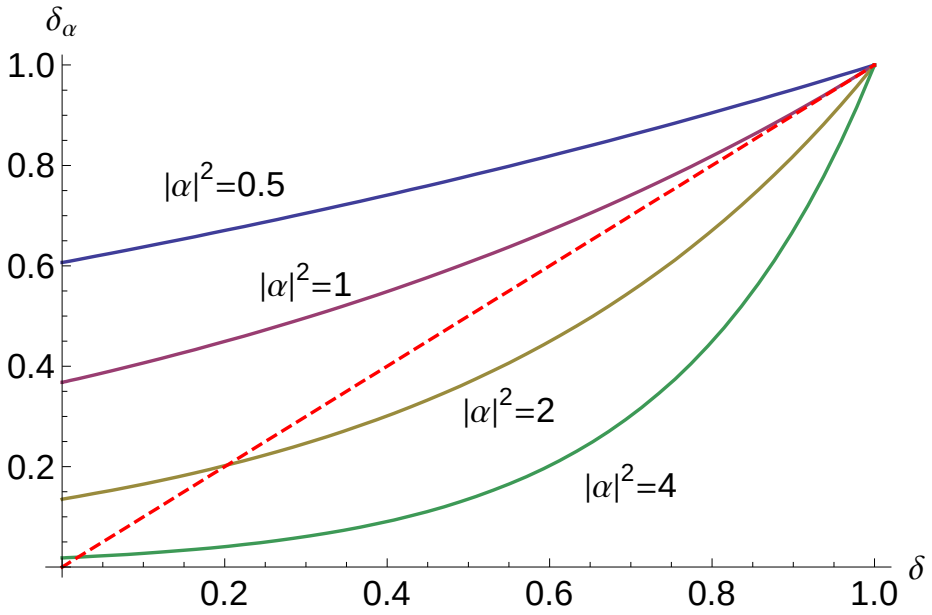


Figure 6.2: Overlaps of states in coherent-state protocols for different values of the mean photon number $|\alpha|^2$ and choosing real values of δ (implying real values of δ_α). For $|\alpha|^2 < 1$, the overlap δ_α is larger than the original overlap δ. For $|\alpha|^2 \approx 1$, both the original and coherent-state overlaps are close to each other when δ is close to 1 and when $|\alpha|^2$ is large, δ_α can be made smaller than almost any value of the original overlap. In fact, in the limit $\alpha \to \infty$, any two states become orthogonal, while in the limit $\alpha \to 0$ any two states are mapped to the vacuum and thus have unit overlap. Finally, for any $\delta \neq 0$ there exists a value of α such that $\delta = \delta_\alpha$.

Proof: The overlap of the coherent-state versions is given by

$$\begin{aligned}
\langle \psi, \alpha | \varphi, \alpha \rangle &= \prod_k \langle \alpha\, \lambda_k | \alpha\, \nu_k \rangle \\
&= \prod_k \exp\left[-\tfrac{|\alpha|^2}{2} (|\lambda_k|^2 + |\nu_k|^2 - 2\lambda_k^* \nu_k) \right] \\
&= \exp\left[-\tfrac{|\alpha|^2}{2} \sum_k (|\lambda_k|^2 + |\nu_k|^2 - 2\lambda_k^* \nu_k) \right] \\
&= \exp\left[|\alpha|^2 (\langle \psi | \varphi \rangle - 1) \right] \\
&= \exp\left[|\alpha|^2 (\delta - 1) \right],
\end{aligned}$$

where we have used the relations $\sum_k |\lambda_k|^2 = \sum_k |\nu_k|^2 = 1$ and $\langle \psi | \varphi \rangle = \sum_k \lambda_k^* \nu_k$. ■

Once again, there is an added richness in coherent-state protocols, since the overlaps may be adapted by varying the value of the parameter α. For example, in many quantum communication protocols, all overlaps between pairs of states are real numbers, and consequently so are those of their coherent-state versions. In that case, the parameter α can be chosen to increase or decrease the overlap, or to match the exact overlap for a given pair of states. This is illustrated in Fig. 6.2.

Now that we have outlined the properties of coherent-state protocols, we continue by describing how these techniques can be applied in the construction of protocols in quantum communication complexity.

6.2 Quantum communication complexity

As mentioned in chapter 2, communication complexity is the study of the amount of communication that is required to perform distributed information-processing tasks. This corresponds to the scenario in which two parties, Alice and Bob, respectively receive inputs $x \in \{0,1\}^n$ and $y \in \{0,1\}^n$ and their goal is to collaboratively compute the value of a Boolean function $f(x,y)$ with as little communication as possible [135]. As discussed in chapter 2, it has been proven that there exist various problems for which the use of quantum resources offer exponential savings in communication compared to their classical counterparts. However, the field of experimental quantum communication complexity remains largely unexplored, largely due to the difficulty of implementing these protocols using standard approaches. In this section, our goal is to employ the mapping to construct protocols that can be implemented using only coherent states and linear optics.

We focus on the bounded-error model in which Alice and Bob have randomness at their disposal and only need to determine the value of the function $f(x, y)$ with probability greater or equal to $1 - \epsilon$ (with $\epsilon < \frac{1}{2}$) even for the worst-case values of x and y. They can send quantum states to each other, apply unitary transformations on these states, and make measurements in the same way as the quantum communication protocols discussed before. Since they are only interested in learning the value of the function, their final measurement can always be thought of as a projective measurement onto two orthogonal subspaces H_0 and H_1, corresponding to $f(x, y) = 0$ and $f(x, y) = 1$ respectively.

In a coherent-state version of this model, the crucial difference lies in the measurement stage, where the subspaces H_0 and H_1 are mapped onto sets of modes S_0 and S_1, where many clicks can occur. In this case, in order to decide between both values of $f(x, y)$, the strategy is to count the number of clicks that occur in each set of modes. If there are more clicks in the set S_0 than in the set S_1, the output of the protocol is $f(x, y) = 0$, and vice versa. In this way we map the large number of possible click patterns in the coherent-state protocol to the two outcomes of interest.

We now provide conditions such that, if the original protocol had success probability larger than $1-\epsilon$, its coherent-state version, using threshold detectors, will also have success probability larger than $1 - \epsilon$. Let C_b be the random variable corresponding to the number of clicks observed in the set of modes S_b, with $b = 0, 1$. The distribution of C_b is known as a Poisson-binomial distribution and its expectation value is given by

$$\mathbb{E}(C_b) = \sum_{k \in S_b} p_{\alpha,k} := \mu_b. \tag{6.20}$$

This distribution can be difficult to work with in its exact form, so it is usual to approximate it by a Poisson distribution with the same mean. This approximation can be made precise through the following result:

Theorem 9. *[14] Let C_b be a Poisson-binomial random variable with mean μ_b. Similarly, let L_b be a Poisson random variable with the same mean μ_b. Then, for any set A, it holds that*

$$|\Pr(C_b \in A) - \Pr(L_b \in A)| \leq \min(1, \mu_b^{-1})\tau_b, \tag{6.21}$$

where $\tau_b := \sum_{k \in S_b} (p_{\alpha,k})^2$ and $p_{\alpha,k}$ is the probability of obtaining a click on the k-th mode.

We can use this fact to show that, under certain conditions, a coherent-state version of a bounded-error qubit protocol also gives the correct value of the function with bounded error.

Theorem 10. *Let a qubit protocol for communication complexity have a probability of success $P_s \geq 1-\epsilon$. Then the corresponding coherent-state protocol has a probability of success $P_\alpha > 1-\epsilon$ if there exists a mean photon number $\mu = |\alpha|^2$ such that*

$$2e^{-P_s\mu}(2eP_s\mu)^{\mu/2} + \max_{\mu_0,\mu_1}\{\min(1,\mu_b^{-1})\}\tau \leq \epsilon \tag{6.22}$$

where μ_b is the expected number of clicks in the set of modes S_b and $\tau = \sum_k (p_{\alpha,k})^2$.

Proof. Without loss of generality, we take $f(x,y) = 0$ to correspond to the correct value of the function. We can bound the success probability as

$$\begin{aligned} P_\alpha &= \Pr(C_0 > C_1) \\ &\geq \Pr(C_0 > \tfrac{\mu}{2}) \Pr(C_1 < \tfrac{\mu}{2}) \\ &= (1 - \Pr(C_0 < \tfrac{\mu}{2}))(1 - \Pr(C_1 > \tfrac{\mu}{2})). \end{aligned}$$

From Theorem 9 we can also write

$$\begin{aligned} \Pr(C_0 < \tfrac{\mu}{2}) &\leq \Pr(L_0 < \tfrac{\mu}{2}) + \min(1,\mu_0^{-1})\tau_0 \\ &\leq e^{-\mu_0}\left(\frac{2e\mu_0}{\mu}\right)^{\mu/2} + \min(1,\mu_0^{-1})\tau_0, \end{aligned}$$

where we have bounded the Poisson distribution as in Eq. (6.11). Similarly we have

$$\Pr(C_1 > \tfrac{\mu}{2}) \leq e^{-\mu_1}\left(\frac{2e\mu_1}{\mu}\right)^{\mu/2} + \min(1,\mu_1^{-1})\tau_1.$$

Putting these together we get

$$\begin{aligned} P_\alpha \geq & \left(1 - e^{-\mu_0}\left(\frac{2e\mu_0}{\mu}\right)^{\mu/2} - \min(1,\mu_0^{-1})\tau_0\right) \times \\ & \left(1 - e^{-\mu_1}\left(\frac{2e\mu_1}{\mu}\right)^{\mu/2} - \min(1,\mu_1^{-1})\tau_1\right) \\ >& 1 - e^{-\mu_0}\left(\frac{2e\mu_0}{\mu}\right)^{\mu/2} - e^{-\mu_1}\left(\frac{2e\mu_1}{\mu}\right)^{\mu/2} \\ & - \min(1,\mu_0^{-1})\tau_0 - \min(1,\mu_1^{-1})\tau_1 \\ \geq& 1 - e^{-P_s\mu}(2eP_s\mu)^{\mu/2} - e^{-(1-P_s)\mu}(2e(1-P_s)\mu)^{\mu/2} \\ & - \max_{\mu_0,\mu_1}\{\min(1,\mu_b^{-1})\}\tau, \end{aligned}$$

where $\tau = \tau_0 + \tau_1 = \sum_k (p_{\alpha,k})^2$ and we have used the fact that

$$P_s\mu = \sum_{k \in S_0} |\alpha|^2 p_k > \sum_{k \in S_0} (1 - e^{-|\alpha|^2 p_k}) = \mu_0 \tag{6.23}$$

and similarly $(1-P_s)\mu > \mu_1$. Whenever $P_s > 1/2$, it holds that $e^{-P_s\mu} P_s > e^{-(1-P_s)\mu}(1-P_s)$ so we can finally write

$$P_\alpha > 1 - 2e^{-P_s\mu}(2eP_s\mu)^{\mu/2} - \max_{\mu_0,\mu_1}\{\min(1, \mu_b^{-1})\}\tau. \tag{6.24}$$

From this expression it is clear that whenever condition (6.22) holds, $P_\alpha > 1-\epsilon$ as desired. ■

Notice that the quantity $2e^{-P_s\mu}(2eP_s\mu)^{\mu/2}$ can be made arbitrarily small for any $P_s > 1-\epsilon$ by choosing a large enough value of $\mu = |\alpha|^2$. However, large values of μ result in higher values of the individual click probabilities $\{p_{\alpha,k}\}$, and consequently larger values of $\tau = \sum_k (p_{\alpha,k})^2$, making it harder for the quantity $\max_{\mu_0,\mu_1}\{\min(1, \mu_b^{-1})\}\tau$ to be small. Therefore, condition (6.22) will only be satisfied when the original probabilities $\{p_i\}$ are very small, as this results in a small τ even when μ is large. Of course, whenever the communicated states lie in a Hilbert space of large dimension, we expect the outcome probabilities to be small and the coherent-state protocol to function adequately.

We are interested in applying the coherent-state mapping to known protocols in quantum communication complexity. We now discuss how the mapping can be used to construct a protocol for the Hidden Matching problem.

6.2.1 The Hidden Matching problem

Recall from chapter 2 that in this communication complexity problem, Alice receives an n-bit string $x \in \{0,1\}^n$ as input, with n an even number. Bob receives a matching $M = \{(i_1, j_1), (i_2, j_2), \ldots, (i_{n/2}, j_{n/2})\}$ on the set of numbers $\{1, 2, \ldots, n\}$, i.e. a partition into $n/2$ pairs. Only one-way communication from Alice to Bob is permitted and the goal is for Bob to output at least one element of the matching (i, j) and a corresponding bit value v such that $v = x_i \oplus x_j$, where x_i is the i-th bit of the string x.

It has been shown that in the bounded-error model, any classical protocol requires $\Omega(\sqrt{n})$ bits of communication [13]. It was also shown in Ref. [13] that there exists an

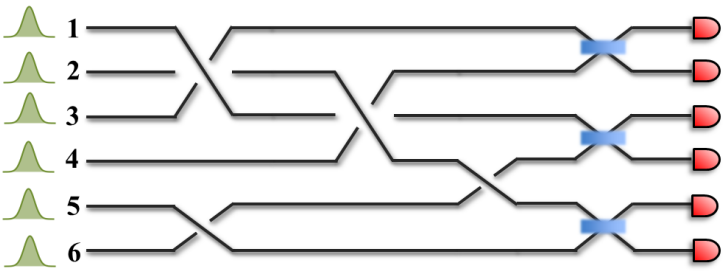


Figure 6.3: An example of an implementation of a coherent-state protocol for the Hidden Matching problem. Alice receives a string of six bits and Bob receives the matching $(1,6),(2,5),(3,4)$. Alice encodes her input values in the phases of six coherent states in different modes and sends them to Bob. His measurement consists of a circuit in which the modes are permuted in accordance with the matching and then interefere pairwise in three balanced beamsplitters. Bob can output a correct solution to the problem based on the detectors that click.

efficient quantum protocol that uses only $O(\log_2 n)$ qubits of communication and outputs a correct answer with certainty. In this protocol, Alice prepares the state

$$|x\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} (-1)^{x_i} |i\rangle \tag{6.25}$$

and sends it to Bob, who measures it in the basis

$$\{\tfrac{1}{\sqrt{2}}(|i\rangle \pm |j\rangle)\}, \tag{6.26}$$

with $(i,j) \in M$. Since these states form a complete basis, one of these outcomes will always occur, and it will always correspond the correct value since $\frac{1}{\sqrt{2}}(|i\rangle + |j\rangle)$ only occurs if $x_i \oplus x_j = 0$ and similarly, $\frac{1}{\sqrt{2}}(|i\rangle - |j\rangle)$ only occurs if $x_i \oplus x_j = 1$. This allows Bob to give a correct output after performing his measurement. Note that Bob's measurement basis is constructed from the canonical basis by applying a Hadamard transformation to the subspaces $\{|i\rangle, |j\rangle\}$, with $(i,j) \in M$.

To construct a coherent-state protocol for the Hidden Matching problem, we just have to apply the rules of the mapping.

Hidden Matching Protocol

1. Alice prepares the state
$$|\alpha, x\rangle = \bigotimes_{i=1}^{n} |(-1)^{x_i} \tfrac{\alpha}{\sqrt{n}}\rangle \tag{6.27}$$
according to her input x and sends it to Bob.

2. Bob permutes the modes according to the matching M and interferes all pairs of modes $\{b_i, b_j\}$, with $(i, j) \in M$, in a balanced beam-splitter. The detectors in the output ports of the beam-splitters are labelled '0' and '1'.

3. If detector $v = 0, 1$ clicks, corresponding to the modes (b_i, b_j), Bob outputs v and (i, j).

The protocol is illustrated in Fig. 6.3. Note that the linear-optical equivalent of a Hadamard gate is a balanced beam-splitter, which explains the form of Bob's measurement in step 2. Additionally, if the incoming states to the input ports of the beam splitter are

$$|(-1)^{x_i} \tfrac{\alpha}{\sqrt{n}}\rangle \otimes |(-1)^{x_j} \tfrac{\alpha}{\sqrt{n}}\rangle, \tag{6.28}$$

the output states will be

$$|\left(1 + (-1)^{x_i \oplus x_j}\right) \tfrac{\alpha}{\sqrt{n}}\rangle \otimes |\left(1 - (-1)^{x_i \oplus x_j}\right) \tfrac{\alpha}{\sqrt{n}}\rangle. \tag{6.29}$$

For each possible value of $x_i \oplus x_j$, one of the output states will be a vacuum while the other is a coherent state with non-zero amplitude. Therefore, we can associate a value $v = 0, 1$ to each of the output detectors so that whenever a click occurs, the correct value of $x_i \oplus x_j$ can be inferred with certainty. Even if there are many clicks, they will always correspond to a correct value. The only issue that can arise is that no-clicks occur and the probability that this happens is given by

$$P_{\text{no-click}} = e^{-|\alpha|^2}, \tag{6.30}$$

which can be made arbitrarily small by choosing α appropriately. Moreover, Theorem 7 guarantees that the amount of information that is transmitted in the coherent-state protocol is $O(\log_2 n)$ and an exponential separation in communication complexity is maintained.

6.3 Conclusions

In this chapter, we have outlined a general framework for encoding quantum communication protocols involving pure states, unitary transformations, and projective measurements, into another set of protocols that employs a coherent state of light in a linear combination of modes, linear optics transformations, and measurements with single-photon threshold detectors. This provides a general method for mapping protocols in quantum communication into a form in which they can be implemented with current technology.

From a theoretical perspective, the coherent-state mapping can be thought of as a tool for understanding fundamental aspects about quantum communication and information. For example, the mapping provides us with a connection between two intrinsically quantum properties: entanglement and non-orthogonality. Additionally, the mapping can be also applied in reverse: obtaining qubit protocols from coherent-state protocols. This provides a connection between the interferometry of coherent states with single photon detectors, and abstract quantum communication protocols using qubits. Besides being of fundamental interest, this may serve as a theoretical test bed for proving results regarding qubit protocols, in the same way as many other dualities have been useful in both physics and mathematics.

The remarkable advantages of the coherent-state protocols obtained from the mapping come at the price of a number of optical modes that is equal to the dimension of the original states in the qubit protocol. For practical purposes, this implies that they are suited for protocols that originally do not require a very large number of qubits. But as we have seen, there exists a regime in which the mapping leads to practical protocols whose implementation was previously inaccessible. As such, we expect that our results will pave the way for the experimental demonstration of a wide range of protocols in quantum communication.

In the following chapter, we apply the results of this chapter to construct a practical protocol for an important problem in quantum communication complexity: quantum fingerprinting. We also report a proof of concept experimental demonstration of this protocol.

Chapter 7

Quantum Fingerprinting with Coherent States

In this chapter, we take a close look at a quantum fingerprinting protocol that can be built form the results of chapter 6. As opposed to the protocols previously discussed, in this case we make an in-depth analysis of the role of experimental imperfections and report a proof of concept experimental demonstration of quantum fingerprinting capable of transmitting less information than the best known classical protocol for this problem. The results presented in this chapter have been published in Refs. [10] and [133].

For the sake of clarity, we briefly summarize the discussion on quantum fingerprinting problem of chapter 2. In this problem, Alice and Bob are each given an n-bit string, which we label x and y respectively. They must each send a message to a third party, the referee, whose task is to decide whether the inputs x and y are equal or not with an error probability of at most ϵ. Alice and Bob do *not* have access to shared randomness and there is only one-way communication to the referee. In this case, it has been proven that any classical protocol for this problem must transmit at least $\Omega(\sqrt{n})$ bits of information to the referee [12, 95]. On the other hand, a quantum protocol was specified in Ref. [28] that transmits only $O(\log_2 n)$ qubits of information.

In this protocol, for each possible input x, Alice prepares the fingerprint states

$$|h_x\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} (-1)^{E(x)_i} |i\rangle, \tag{7.1}$$

where $E(x)_i$ is the ith bit of a codeword $E(x)$. Bob does the same his input y and they send the states to the referee, who performs a SWAP test of the signals. The referee can

decide whether the states are equal or not by simply checking whether outcome "1" occurs. If the inputs are equal, this will never happen but if the inputs are different, there is a fixed probability with which it will. The probability of error can be made arbitrarily small by simply repeating the protocol enough times.

7.1 Coherent-state quantum fingerprinting protocol

How can we implement this abstract quantum fingerprinting protocol in practice? An approach to implementing the fingerprint states of Eq. (7.1) is to decompose the underlying Hilbert space as a tensor product of Hilbert spaces of smaller dimension as done in Refs. [71, 49, 46]. For example, we could have a collection of $O(\log_2 n)$ two-level systems, such as photons in the polarization degree of freedom. As noted already in Ref. [71], a serious drawback of this strategy is that most fingerprint states must be highly entangled [92, 91]. As a result, even for low input sizes, the experimental requirements greatly exceed that which is possible to achieve with current technology. For this reason, the implementations of [71, 49] are restricted to one single qubit transmission and within a few meters, without a practical possibility of scaling them to demonstrate a reduction in the transmitted information.

Alternatively, we can consider the underlying Hilbert space as arising directly from a single $m-$dimensional physical system, such as a single photon distributed over m orthogonal optical modes, as has been considered in Refs. [89, 57]. However, as discussed already in chapter 6, these states are also very challenging to create and transmit. Instead, we will apply the mapping of chapter 6 to create a practical protocol that is robust to experimental imperfections. This protocol was first introduced in Ref. [10]. Following the rules of the mapping, the states of Eq. (7.1) are mapped to a sequence of coherent states given by

$$|\alpha, x\rangle = \bigotimes_{i=1}^{m} |(-1)^{E(x)_i} \tfrac{\alpha}{\sqrt{m}}\rangle_i. \tag{7.2}$$

Here $E(x)_i$ is the i-th bit of the codeword and α is a complex amplitude. Notice that all the coherent states have the same amplitude, but their individual phases depend on the particular codeword, which in turn is determined by the input x. The total mean photon number in the entire sequence is $\mu := |\alpha|^2$.

Since the fingerprinting states are coherent states instead of single-photon states, a perfect two-photon interference is not required [70]. All we need is a measurement by the referee that allows her to verify whether the relative phases of the incoming pulses are

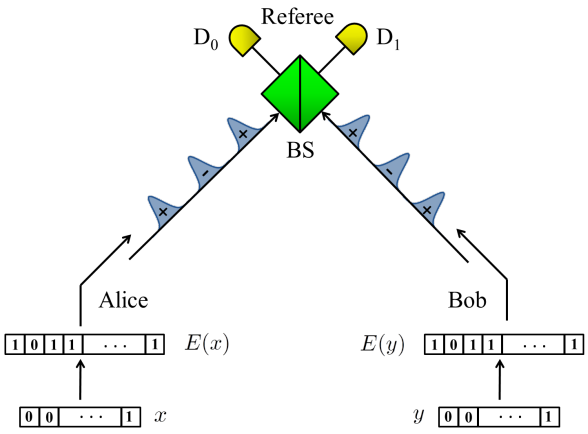


Figure 7.1: A schematic illustration of the quantum fingerprinting protocol. Alice and Bob receive inputs x and y, respectively, which they feed to an error-correcting code to produce the codewords $E(x)$ and $E(y)$. Using these codewords, they modulate the phases of a sequence of coherent pulses that they send to the referee. The incoming signals interfere at a beam-splitter (BS) and photons are detected in the output using single-photon detectors D_0 and D_1. In an ideal implementation, detector D_1 fires only when the inputs to Alice and Bob are different.

equal or different. A way of achieving this consists of a phase interferometer in which the individual pulses enter a balanced beam splitter, and whenever there is a click in the output detectors, it is unambiguously revealed whether their phases are the same or not [5].

Indeed, in our scheme, Bob does the same as Alice for his input y, and they both send their sequence of states to the referee, who interferes the individual states in a balanced beam-splitter. The referee checks for clicks at the outputs of the phase interferometer using single-photon detectors, which we label "D_0" and "D_1". In the ideal case, a click in detector D_1 will never happen if the phases of the incoming states are equal, i.e. if $E(x)_i \oplus E(y)_i = 0$. However, it is possible for a click in detector D_1 to occur if the phases are different, i.e. if $E(x)_i \oplus E(y)_i = 1$. Thus, if $x \neq y$, we expect a number of clicks in D_1 that is proportional to the total mean number of photons and the Hamming distance between the codewords. This allows the referee to distinguish between equal and different inputs by simply checking for clicks in detector D_1.

Let $D_{1,E}$ and $D_{1,D}$ be random variables corresponding to the number of clicks in detector D_1 for the case of equal and worst-case different inputs, respectively. The probability

distributions for these variables can be well approximated by binomial distributions $D_{1,E} \sim \text{Bin}(m, p_E)$ and $D_{1,D} \sim \text{Bin}(m, p_D)$ given by

$$\Pr(D_{1,E} = k) = \binom{m}{k} p_E^k (1 - p_E)^{m-k} \tag{7.3}$$

$$\Pr(D_{1,D} = k) = \binom{m}{k} p_D^k (1 - p_D)^{m-k}, \tag{7.4}$$

where m is the number of modes and p_E, p_D are the probabilities of observing a click in each mode for the case of equal and worst-case inputs respectively. These probabilities are given by [10]:

$$p_E = (1 - e^{-\frac{2(1-\nu)\mu}{m}}) + p_{dark} \tag{7.5}$$

$$p_D = \delta(1 - e^{-\frac{2\nu\mu}{m}}) + (1 - \delta)(1 - e^{-\frac{2(1-\nu)\mu}{m}}) + p_{dark}. \tag{7.6}$$

Here ν is the interference visibility – which quantifies the contrast of the interferometer – and p_{dark}, the dark count probability, is the probability that a detector will fire even when no incident photons from the signals are present. As before, μ is the total mean photon number in the signals and δ is the minimum distance of the error-correcting code.

The referee sets a threshold value $D_{1,th}$ such that, if the number of clicks is smaller or equal than $D_{1,th}$, she will conclude that the inputs are equal. Otherwise, she concludes that they are different. Note that – unlike the ideal case – in the presence of imperfections, an error can occur even when the inputs are equal. In our protocol, the value of $D_{1,th}$ is chosen in such a way that an error is equally likely to occur in both cases, so that the probability of error is given by

$$\Pr(\text{error}) = \Pr(D_{1,E} > D_{1,th}) = \Pr(D_{1,D} \leq D_{1,th}), \tag{7.7}$$

which can be calculated directly from the distributions of $D_{1,E}$ and $D_{1,D}$. This is illustrated in Fig. 7.2.

In the regime in which dark counts are negligible and $\mu \ll m$, we can approximate Eqs. (7.5) and (7.6) as

$$p_E \approx \frac{2(1-\nu)\mu}{m} \tag{7.8}$$

$$p_D \approx \delta \left(\frac{2\nu\mu}{m} \right) + (1 - \delta) \left(\frac{2(1-\nu)\mu}{m} \right). \tag{7.9}$$

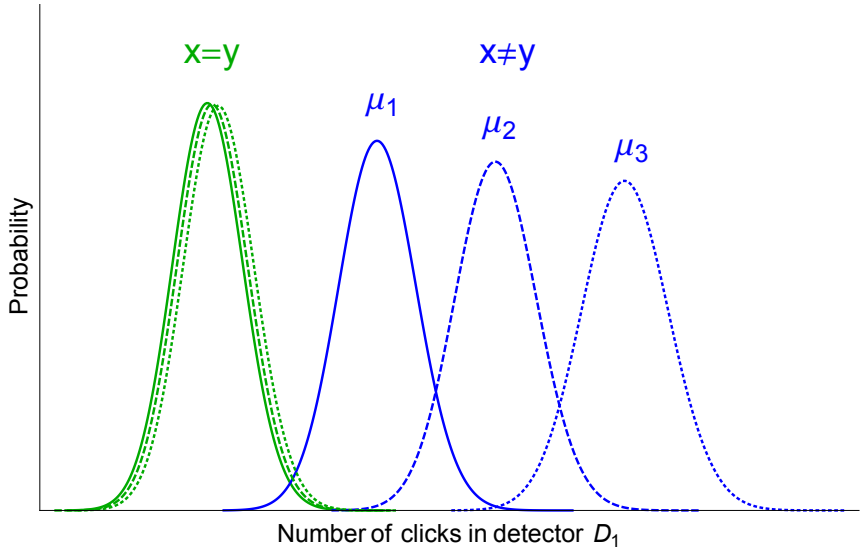


Figure 7.2: An illustration of the probability distributions for the number of clicks in detector D_1 for equal inputs ($x = y$) and worst-case different inputs ($x \neq y$). The distributions are shown for three different total mean photons numbers: μ_1 (solid), μ_2 (dashed) and μ_3 (dotted), with $\mu_1 < \mu_2 < \mu_3$. The distributions for equal inputs (green) are dominated by dark counts, so they are largely unaffected by changes in μ. On the other hand, for the worst-case different inputs (blue), the mean value of the distributions depends strongly on μ. Therefore, the error in distinguishing both distributions can be controlled by choosing μ appropriately.

In this case, the average number of clicks in detector D_1 for equal and worst-case different inputs satisfy

$$\langle D_{1,E} \rangle = mp_E \approx 2(1-\nu)\mu \tag{7.10}$$
$$\langle D_{1,D} \rangle = mp_D \approx [2\delta\nu + 2(1-\delta)(1-\nu)]\mu. \tag{7.11}$$

Thus, the difference between these two averages $\langle D_{1,D} \rangle - \langle D_{1,E} \rangle = 2\delta\mu(2\nu - 1)$ can be made as large as desired by choosing μ accordingly, independently of m and consequently of the input size n. A larger difference in these averages is leads to a smaller probability of error. Therefore, any error probability can be achieved by fixing μ appropriately. In the regime where dark counts are negligible, μ depends only on the error probability, whereas when dark counts are significant, we must increase μ as a function of the input size. In general, the protocol determines an appropriate vale of the total mean photon number μ for each input size n by finding the smallest value of μ such that the probability of error – as given in Eq. (7.7) – is smaller than the desired error probability of the protocol.

In summary, the coherent-state quantum fingerprinting protocol is given by the following set of rules:

Coherent-state protocol

1. For the given input size n, all parties calculate the threshold value D_{th} such that $\Pr(D_{1,E} > D_{1,th}) = \Pr(D_{1,D} \leq D_{1,th})$.

2. For the given input size n and D_{th} obtained in the previous step, Alice and Bob calculate the smallest value of $\mu = |\alpha|^2$ such that $\Pr(\text{error}) < \epsilon$, where $\Pr(\text{error})$ is given by Eq. (7.7) and ϵ is the target error probability of the protocol.

3. Alice applies an error-correcting code to her input x to produce the codeword $E(x)$. She then prepares the state $|\alpha, x\rangle = \bigotimes_{i=1}^{m} |(-1)^{E(x)_i} \frac{\alpha}{\sqrt{m}}\rangle_i$.

4. Bob does the same as Alice for his input y and they each send their states to the referee.

5. The referee interferes the signals in a balanced beam splitter and counts the number of clicks observed in detector D_1. If this number is smaller than D_{th}, he concludes that the inputs are equal. Otherwise, he concludes that the inputs are different.

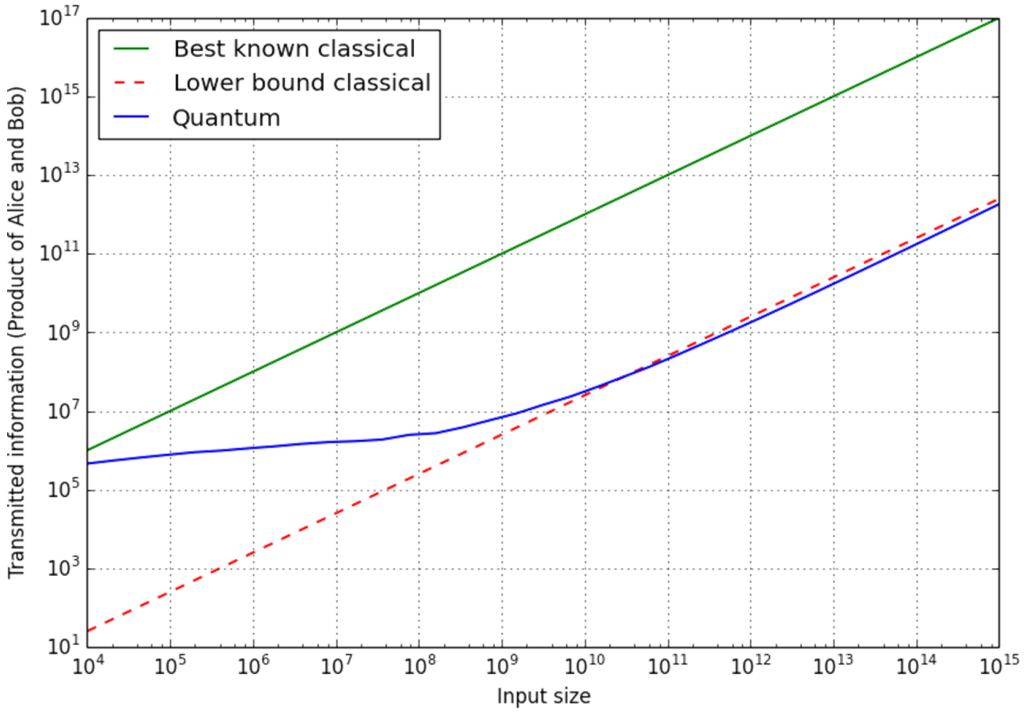


Figure 7.3: Logarithmic plot of the transmitted information in the quantum fingerprinting protocol compared to the best-known classical protocol and the classical lower bound of Ref. [12]. For illustration, we have chosen parameters $\eta = 0.85$, $p_{dark} = 10^{-9}$ – which can be achieved using the detectors of Ref. [88] – and a visibility of $\nu = 99\%$. The target error probability is 1%. As can be seen in the plot, dark counts become significant for input sizes greater than 10^9 and the logarithmic scaling of the transmitted information is lost. Nevertheless, the quantum protocol can outperform the classical one by more than two orders of magnitude.

As noted before, in the regime in which dark counts are negligible, the total mean photon number is fixed and independent of the input size n. From Eq. (6.10), the transmitted information Q in the protocol satisfies

$$Q \leq (\mu + \Delta) \log_2 [(\mu + \Delta + m - 1)] + \log_2(2\Delta) \tag{7.12}$$
$$= O(\mu \log_2 n). \tag{7.13}$$

For fixed μ, this gives an exponential separation in communication complexity compared to the classical case. It is in this sense that the protocol provides an advantage compared to the classical case. In the regime where dark counts become significant – namely when $p_D \approx p_{dark}$ – it no longer becomes possible to attain the desired error probability with fixed μ. Therefore, dark counts pose a limit to the maximum input size for which the logarithmic scaling of the transmitted information can be maintained. For fixed total mean photon number μ and codeword size m, we can always use Eq. (7.12) to bound the transmitted information in the protocol.

Finally, we note that in any implementation of the protocol there will be some loss captured by the combined effect of limited detector efficiency and channel loss. We quantify this with the single parameter $\eta < 1$. As shown in Ref. [10], the effect of loss can be compensated by adjusting the total mean photon number accordingly: $\mu \to \mu/\eta$. Thus, the protocol is robust to loss. An illustration of the transmitted information of the protocol as a function of input size is shown in Fig. 7.3, where we compare our quantum protocol with the best-known classical protocol for this problem [12].

7.2 Error-correcting code

In quantum fingerprinting, an error-correcting code (ECC) is used to amplify the Hamming distance between the inputs of Alice and Bob. Even if these inputs are originally very close to each other – for example if they differ in a single position – after applying the ECC, the resulting codewords will have a much larger Hamming distance. In the worst-case scenario, this distance is given by the minimum distance of the code. Note, however, that no error-correction actually takes place in the quantum fingerprinting protocol – we just use the properties of error-correcting codes to increase the distance between the inputs.

The quantum fingerprinting protocol of Ref. [28] used Justesen codes as an example to illustrate the properties of the protocol. However, these codes are not optimal for quantum fingerprinting. In this section, we construct more efficient codes based on random Toeplitz matrices that significantly relax the requirements on the experimental devices and lead

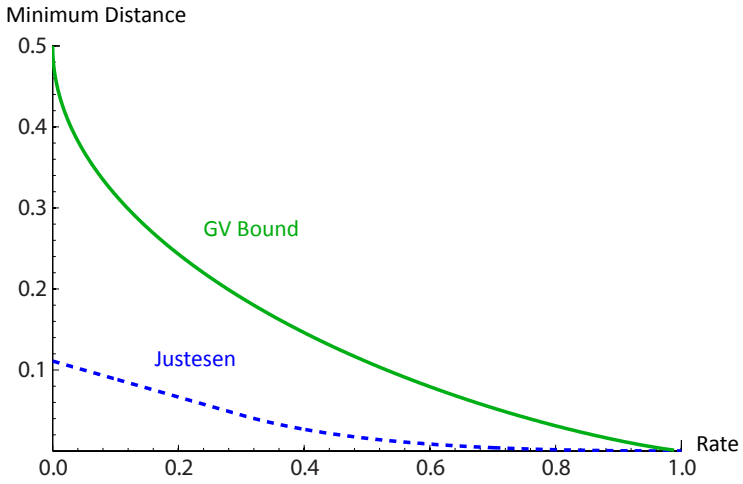


Figure 7.4: The Gilbert-Varshamov bound compared to the distance-rate relationship achieved by Justesen codes suggested in Refs. [10, 28]. For various rates, a code satisfying the GV bound – like the one we use in our protocol – achieves a minimum distance that is more than three times the value for Justesen codes.

to a faster implementation of the protocol. Due to their probabilistic construction, these codes are not guaranteed to have the desired minimum-distance, but do achieve it with exponentially high probability (See Appendix B for details). Therefore, by using these codes, we can only claim that with exponentially high probability, we are using codes with the required properties to attain the desired error probability.

An ECC with a high rate and a large minimum distance is desired, since a higher rates leads to lower transmitted information and larger tolerance for dark counts, while a larger minimum distance leads to smaller error probability for fixed mean photon number. Fundamentally, there is an inherent trade-off between the rate and distance of ECCs. In particular, the Gilbert-Varshamov (GV) bound [60, 124] states that there exists some binary linear code whose rate R and minimum distance δ satisfy the relation

$$R \geq 1 - H_2(\delta), \tag{7.14}$$

where $H_2(\cdot)$ is the binary entropy function. Using a binary linear code that approaches this bound would constitute a significant improvement over the codes suggested in previous protocols [10, 28]. This is clearly illustrated in Fig. 7.4.

It is well known in coding theory that random linear codes (RLCs) can asymptotically approach the GV bound with encoding complexity $O(n^2)$ [15]. However, in quantum

fingerprinting, the input size n is typically very large (e.g. $n = 10^8$), thus making the encoding time prohibitively high. In order to reduce this encoding complexity, we make use of a subclass of RLCs whose generator matrices are Toeplitz matrices. A Toeplitz matrix is a matrix in which each descending diagonal from left to right is constant. An $n \times m$ Toeplitz matrix is completely determined by the $n + m - 1$ elements on its first row and column. This structure implies that only $O(n \log n)$ time for encoding is required for this subclass of RLCs [53]. Additionally, these codes also asymptotically approach the GV bound (see Appendix B for a proof). By using this family of codes, we are able to reduce the encoding times by several orders of magnitude, making them suitable for practical applications.

The exponential separation between quantum and classical communication complexity for the equality function only holds if Alice and Bob do not have access to shared randomness that is generated in each run of the protocol [12]. However, even though the generator matrices of our RLCs are randomly constructed, once they have been created they remain fixed for all future instances of the protocol. This ensures that no new randomness is generated in each run of the protocol, as required to satisfy the conditions of the exponential separation. In particular, Alice and Bob can store the generator matrices in memory and use them to encode their inputs in exactly the same way as if they had been generated deterministically.

For the experiment reported in the next section, an encoder program written in C++ was built and tested, demonstrating the feasibility of this subclass of RLCs. The free Fast-Fourier Transform library FFTW was used to accelerate multiplications with Toeplitz matrices [55] and the random numbers to construct the matrices were generated from a quantum random number generator [134]. The results from an optimized encoder are shown in Table 7.1. As we can see, our encoder is practical, can be run on any common lab PC, and finishes the encoding in an acceptable time frame for input sizes as large as $n = 3 \times 10^8$. Faster encoding times could be obtained by using dedicated hardware.

7.3 Experiment

One of the main goals of the results outlined in chapter 6 was to establish a technique to construct practical quantum communication protocols. In this section, we will make the practicality of quantum fingerprinting explicit by reporting on a proof of concept experimental demonstration of the coherent-state protocol introduced in this chapter. Unlike the previous quantum fingerprinting experiments of Refs. [71, 49], which demonstrated an increase in the success probability for a small and fixed amount of transmitted information,

n (bit)	m (bit)	Time (s)	Memory (Mbit)
10^6	5×10^6	6	52
10^7	5×10^7	106	733
3×10^7	1.5×10^8	181	1654
3×10^8	1.5×10^9	4831	10000

Table 7.1: The performance of the encoder for different input sizes, using a computer with a quad-core i7-4770 @3.4GHz CPU and 16GB RAM. Running times are acceptable for experimental applications for input sizes as large as $n = 3 \times 10^8$.

our experiment was capable of running for input sizes as large as 100 Megabits, achieving a reduction in the transmitted information compared to the best-known classical protocol. This experiment has been reported in Ref. [133].

This proof of concept quantum fingerprinting protocol was demonstrated using a plug&play scheme [116], initially designed for quantum key distribution (QKD). The advantage of the plug&play system with respect to other viable systems is that it offers a particularly robust and stable implementation. This allows us to perform reliable experiments with highly attenuated coherent states for long time durations. A disadvantage is that, in this setup, Bob must be located very close to the referee. The protocol was implemented on top of two commercial systems, namely ID-500 and Clavis2, manufactured by ID Quantique [1]. The experimental setup is shown in Fig. 7.5.

Since the operating conditions of the protocol are significantly different from those of standard QKD, using a commercial QKD equipment for the implementation requires several important modifications to the system. First, two single-photon detectors with low dark count rates were installed. Indeed, as can be deduced from Eqs. (7.5) and (7.6), lower dark count rates permit the operation of the system at lower mean photon numbers, which lead to a reduction in the transmitted information. Fortunately, our error correction codes improve the tolerance of the protocol to dark counts, which permits us to use commercial detectors. Two commercial free-running InGaAs avalanche photodiodes – ID220 [1] were employed. The dark count rate per 1 ns detection gate for this detectors is about $(3.5 \pm 0.2) \times 10^{-6}$ and the corresponding quantum efficiency is about 20%. The detections are recorded by a high-precision time interval analyzer (TIA, PicoQuant HydraHarp 400). The system was run at a repetition rate of 5 MHz with the detector dead time set at 10μs. This means that after a click occurred, the following 50 pulses are blocked before the detector is active again. This is not a problem in our experiment because the mean photon number in each pulse is extremely low, therefore the expected number of undetected photons as a

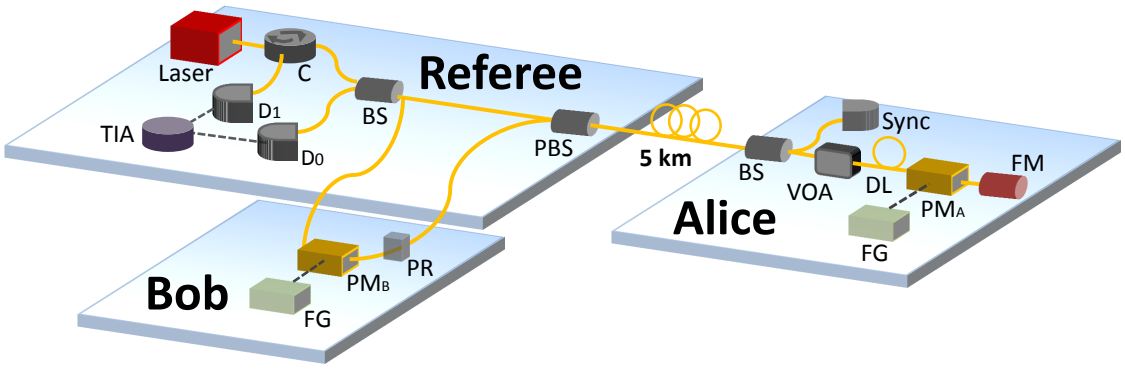


Figure 7.5: Experimental setup for quantum fingerprinting. The laser source at the referee's setup emits photon pulses which are separated at a 50:50 beam-splitter (BS) into two pulses, the signal pulse and the reference pulse. The signal pulse passes through Bob's phase modulator (PM) and then through a polarization rotator (PR) which rotates the pulses' polarization by 90°. The pulses are then recombined at a polarization beam splitter (PBS) where they exit through the same port and travel to Alice through the 5 kms fiber. After passing through Alice's BS, the reference (forward) pulse is split into two pulses, where one is used as a synchronization (Sync) and the other one continuous travelling. Similarly, the signal (backward) pulse is split into two. Then, Alice uses her phase modulator (PM) to set the phase of the signal pulse only, according to her codeword $E(x)$. Once the reference and the signal pulses are reflected back by the Faraday mirror (FM), she attenuates them to the desired photon level by using the variable optical attenuator (VOA). When the two pulses return in the direction of the referee, because of Alice's FM, the reference pulse will travel through Bob, who uses his PM to modulate the pulse according to his codeword $E(y)$. Both Alice and Bob use two external function generators (FG) to control the PMs. Finally, the two pulses arrive simultaneously at the BS, where they interfere and are detected by two detectors D_0 and D_1. The detection events are recorded by a time interval analyzer (TIA).

result of this effect is negligible compared to other sources of error (see Appendix B for details).

Additionally, new functionalities and control signals were added to the system. On one hand, the VOA inside Alice was used to reduce the mean photon number per pulse down to suitable numbers. These values – in the order of 10^{-5} per pulse – were in fact four orders of magnitude lower than those typically used for QKD. Hence, several calibration processes of the system are required, which imposes particular care in the synchronization of the phase modulation and attenuation signals. On the other hand, commercial QKD

η_{AR}	η_{BR}	η_{det}	p_{dark}	ν
3 dB (2.36 dB)	1.5 dB (1 dB)	20.0%	$(3.5 \pm 0.2) \times 10^{-6}$	$(99 \pm 0.5)\%$

Table 7.2: Parameters measured in the implementations. The overall loss between the output of Alice's VOA and the input to the referee's detectors is given by the parameter η_{AR}. Similarly, η_{BR} defines the overall loss between the output of Bob's PM and the referee's detectors. Both η_{AR} and η_{BR} are carefully characterized in ID-500 (Clavis2). The other parameters are the detector's quantum efficiency η_{det}, dark count rate per pulse p_{dark} for each detector, and system visibility ν, which are nearly the same for ID-500 and Clavis2.

systems like Clavis2 have an internal random number generator to set the phase modulations, which does not allow us to modulate the phases according to the pre-generated codewords. This difficulty was solved by using two external function generators (FG, Agilent 88250A) loaded with the codewords to control Alice's and Bob's phase modulator. This requires precise synchronization and calibration procedures to guarantee correct phase modulations. Finally, high interference visibility of about $(99 \pm 0.5)\%$ was observed after careful calibration.

In the implementation on ID-500, the random numbers controlling the phase modulations are accessible to the users. The codewords were used to replace those random numbers directly. However, after testing for an input data size of $n = 1.42 \times 10^8$ on ID-500, an unexpected hardware problem made ID-500 unavailable for further experiments. To further test the feasibility of the protocol for different input sizes, we switched to Clavis2 for measurements. In the implementation on Clavis2, since each function generator has a small memory, for simplicity we load a frame of about 430 random numbers to each function generator and reuse these random numbers. This allows us to create binary sequences with the desired distance δ that can be used to test the performance of the system. All the above modifications led to the development of a practical system that is capable of performing quantum fingerprinting.

7.3.1 Experimental results

The quantum fingerprinting experiment over a standard telecom fiber of 5 km between Alice and the referee. The overall loss between the output of Alice's VOA and the input of the referee's detector D_1 – which includes the losses of quantum channel, PBS, BS and the circulator – is about 3 dB (2.36 dB) for ID-500 (Clavis2). The channel between Bob and the referee is about a few meters, and its overall loss including Bob's channel, the BS and

the circulator, is about 1.5 dB (1 dB). We summarize all system parameters in Table 7.2. Based on these parameters, for a given input size n, we use our model of the protocol to optimize the photon number μ in order to achieve a desired error probability ϵ.

Because there is loss in the channels and the detectors are not perfectly efficient, Alice and Bob must use higher mean photon numbers compared to the case with no channel loss and perfect detectors. As implied by Eq. (7.13), this also leads to an increase in the transmitted information, which we take into account in our calculations of the transmitted information. In particular, if Alice and Bob experience different amounts of loss, they must choose a different mean photon number when preparing their signals, ensuring that the amplitude of their pulses is equal when they interfere in the referee's beam splitter.

In the experiment, the detection events registered on D_0 and D_1 in conjunction with the known experimental conditions in the system can be used to characterize the photon numbers sent out by Alice and Bob, the dark count probability, and the visibility of the interferometer. From the characterization of these parameters, we find that there is a good agreement with our model of the system. The main source of uncertainty is due to an imperfect matching between the observed mean photon numbers and those pre-calibrated from the VOA. This uncertainty is determined by the fluctuations of several devices, such as laser power, VOA, and detector efficiency. The detailed values of this uncertainty are shown in Appendix B.

The quantum fingerprinting protocol was tested over several values of the input size n. For each n, we record the detection counts on D_1 for two types of input data: equal inputs $E(x) = E(y)$, and the worst-case different inputs, i.e. those for which the codewords $E(x) \neq E(y)$ have a distance equal to the minimum distance δ. For our experiment, we minimize the transmitted information by choosing an optimal value of $\delta = 0.22$ for the minimum distance. From the threshold value $D_{1,th}$ that is pre-calculated from our model, the referee can distinguish between equal and different inputs. The upper bound Q on the quantum information Alice and Bob is calculated from their respective mean photon numbers μ_A and μ_B, as well as the codeword length m.

In Fig. 7.6, we show the transmitted information as a function of the input size n for a target error probability of $\epsilon = 5 \times 10^{-5}$. The error probability was calculated from our theoretical model of the experiment. Within experimental uncertainty, the worst-case values of the mean photon number, visibility, and dark count probability were used to reconstruct the probability distributions of clicks in detector D_1. These distributions, in turn, were used to calculate the error probability from Eq. (7.7). Since our theoretical model is only an approximation, the error probability should also be understood as approximate. Future implementations should improve on this by treating the system as a black-box, using the

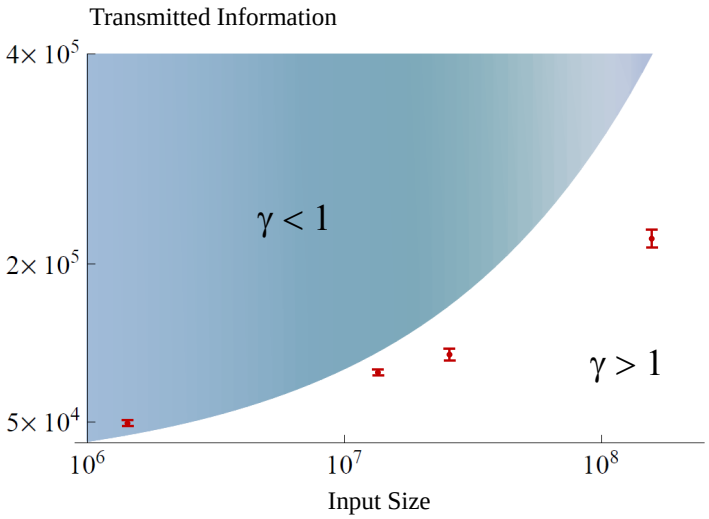


Figure 7.6: Log-inear plot of the transmitted information in the protocol. The blue area indicates the region where the classical protocol transmits less information than the protocol, while the red point shows our experimental results. The error bars correspond to one standard deviation. For large n, our results are strictly better than the best known classical protocol for a range of practical values of the input size.

data directly to make statistical inferences about the error probability, without relying on an approximate model of the system. The blue area in Fig. 7.6 indicates the region where the best known classical protocol of Ref. [12] transmits less information than our quantum protocol. For this target error probability, the classical protocol requires the transmission of $16\sqrt{n}$ bits. The red points show our experimental results, where the data point for the largest n is obtained from ID-500 and the other three data points are obtained from Clavis2. Note that Clavis2 and ID-500 have almost the same optics and functionality [1]. We use the same measurement and processing method for the data obtained from these two systems, and show the experimental results together in one figure instead of two. The error bars come from the uncertainty in the estimation of the mean photon number μ. For large n, our experimental results are strictly better than those of the classical protocol for a wide range of practical values of the input size.

To obtain further insight into the results, we define the *quantum advantage* γ as the ratio between the transmitted classical information C of the best-known classical protocol

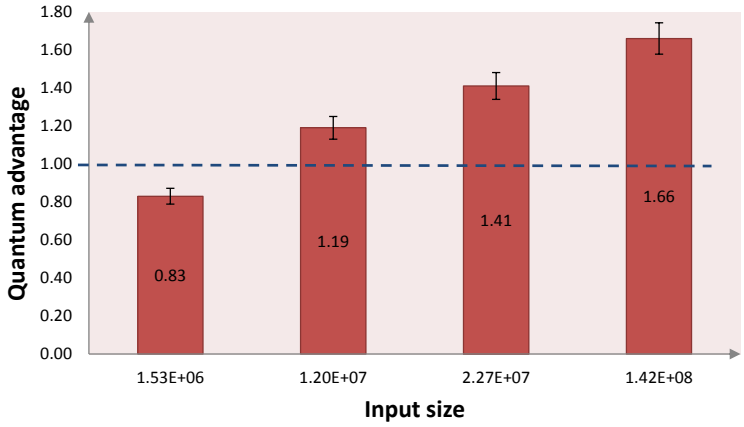


Figure 7.7: The quantum advantage γ between the transmitted classical information and the upper bound on the transmitted quantum information. For the three large input sizes, the ratio is well above 1. The quantum advantage was as large as $\gamma = 1.66$, which implies that the transmitted information in the classical protocol was 66% larger than in the quantum case.

[12] and the upper bound Q on the transmitted quantum information:

$$\gamma = \frac{C}{Q}. \tag{7.15}$$

A value $\gamma > 1$ for a given error probability ϵ implies that less information is transmitted in the quantum case than in the classical one. This allows us to use the quantum advantage as a figure of merit to assess the performance of our quantum fingerprinting implementation. In Fig. 7.7, we show the experimental results for γ as a function of different input sizes. For the three largest input sizes, the ratio is well above 1, and the classical protocol transmitted as much as 66% more information than the quantum protocol. For the smallest input size, no quantum improvement was obtained.

7.4 Discussion

Based on the protocol of Ref. [10], we have experimentally demonstrated a proof of concept quantum fingerprinting system that is capable of transmitting less information than the best known classical protocol for this problem. Our experimental test of this system

indicates that its operation is consistent with our model of the devices and hence also with achieving the desired error probability. Moreover, we have operated our system in a parameter regime in which the information transmitted in the protocol is up to 66% lower than the best known classical protocol. This constitutes the first time that a quantum fingerprinting protocol has been carried out that is capable of achieving this reduction in the transmitted information.

In communication complexity, it is assumed that the parties have unlimited computational power. However, from a practical perspective, it may not always be possible to ignore these computational requirements. In fact, even though the running time during communication of our experiment scales linearly with the input size, the total running time of the protocol is dominated by the time required to run the error-correcting code – which is a crucial component of the protocol. For instance, at a repetition rate of 5MHz, it takes 5 minutes to run the communication for an output size of $m = 1.5 \times 10^9$. On the other hand, even with the use of RLCs with quasi-linear encoding complexity, more than one hour is needed to run the encoding algorithm, as seen in Table 7.1. Even if dedicated hardware is used to improve the encoding speeds, the encoding complexity is quasi-linear in the input size, while the transmission times scales linearly. Therefore, the practical advantages of quantum fingerprinting, in terms of reductions in resource expenditures, will likely be found in a reduction of the number of photons used. This is a major property that the protocol possesses. Indeed, for the largest input size that was tested in the experiment, $n = 1.42 \times 10^8$, a total mean photon number of only $\mu \approx 7 \times 10^3$ was used (see Appendix B). Even further reductions would occur with better detectors. Overall, it is remarkable that quantum fingerprinting with coherent states can be realized while revealing only a very small amount of information to the referee – a feature of the protocol that may have important applications to fields such as cryptography [58] and information complexity [31], where this extremely small leakage of information plays a fundamental role.

In the implementation, a reference pulse is transmitted between the two participants for a share of synchronization and phase reference. In practice, one can overcome this by using a system where each of Alice and Bob holds a frequency-locked laser source separately. A common phase reference can be established before the start of the protocol or the referee can employ phase-locking techniques to interfere the two pulses from Alice and Bob. Indeed, a potential method for such an implementation is to use the techniques that have been recently developed in the field of QKD [104, 84, 119]. This configuration, unlike the plug&play scheme, can also permit Bob to be situated at a large distance from the referee.

In this quantum fingerprinting protocol, the maximum reduction in the transmitted information depends crucially on the dark count probability and the overall loss in the

system. Thus, the results of the experiment can be directly improved by using detectors with higher efficiency and lower dark counts. This can lead to a quantum fingerprinting protocol that, with the use of available technology [88], transmits several orders of magnitudes less information than the best known classical protocol for large input sizes, as was shown in Fig. 7.3. Even though there is no proof that the best known classical protocol is optimal, a lower bound for the classical transmitted information was proven in Ref. [12]. This lower bound states that, for any classical protocol with error probability smaller than 0.01, Alice and Bob must send at least $\frac{\sqrt{n}}{20}$ bits of information. This is roughly two orders of magnitude smaller than the transmitted information of the best known classical protocol. By using state-of-the-art detectors, it should be possible to demonstrate a quantum fingerprinting protocol capable of beating this classical lower bound. Achieving this would constitute a significant milestone for experimental quantum communication complexity.

It is an appealing and useful property of this quantum fingerprinting protocol that we can achieve a quantum advantage without the need for entanglement, single-photon sources or squeezing. So where does the improvement come from? As mentioned in chapter 6, one way of understanding this is to view the quantum advantage as arising from the non-orthogonality of weak coherent states and the quantum mechanical properties of single-photon detectors. In the protocol, the weak coherent states have a very low mean photon number, on the order of 10^{-5}. This means that the two possible states that are sent in each mode, $|+\frac{\alpha}{\sqrt{m}}\rangle$ and $|-\frac{\alpha}{\sqrt{m}}\rangle$, are highly non-orthogonal and difficult to distinguish. Therefore, very little information can be learnt by looking at each pulse. This is essentially the reason why the transmitted information is very low – exponentially less than in the classical case. On the other hand, after the coherent states interfere in the beam-splitter, a click in the single-photon detector unambiguously provides valuable information to the referee: she now knows whether the phases of the coherent states are equal or not. The referee uses this information to determine whether the inputs to Alice and Bob are equal, even if very little information was sent to her. This unambiguous information is only possible because the detectors respond quantum mechanically to the incoming light field.

Finally, we emphasize a unique property of this protocol: no time-resolution is required from the detectors. In order to make her decision, the referee only needs to count the number of clicks that occur in detector D_1. It does not matter when the clicks happen, all that matters is how may of them occur. This property implies that alternative detector technologies and modulation techniques could be employed in the protocol. For example, slow detectors with low dark count rates and high efficiency, such as those employed in CCD cameras, can potentially provide significant improvements on the performance of the protocol compared to the use of traditional detectors. Moreover, this implies that the repetition rate of the protocol is limited only by the modulation of the signals, which can

be performed at rates well above 1 GHz.

Chapter 8

Multiparty Quantum Signature Schemes

The results presented in the previous two chapters provide new examples of practical quantum communication protocols, which were made possible by new methods of encoding abstract protocols into physical systems. The focus was made on using coherent states and linear optics, which was motivated from a desire to design protocols that could be implemented in practice with available techniques. In this chapter, our goal is to build practical protocols for quantum signature schemes. However, in this case, we take a different approach than in previous chapters: instead of providing a specific physical implementation of these protocols, we reduce the experimental difficulty of implementing quantum signature schemes (QSSs) to that of carrying out quantum key distribution (QKD) in a point-to-point network.

However, unlike the case of other tasks in quantum communication, there has not been significant theoretical work on establishing a security model for quantum signature schemes. In the absence of such a model, it is unclear what are the precise security goals of these schemes nor what are the requirements for achieving those goals. Consequently, before being able to construct practical quantum signature schemes, it is crucial to first outline a security framework for these schemes and to provide an understanding of their required properties. More specifically, in this chapter, we provide a security framework suitable for quantum signature schemes involving an arbitrary number of participants.

The rest of this chapter is organized as follows. In section 8.1, we generalize the security definitions of Swanson and Stinson [118] so that they can apply also to the quantum case and introduce a formal definition of transferability based on different verification levels. We

also present a characterization of the general structure of QSS protocols and in section 8.2 we introduce rigorous definitions of security. Additionally, in section 8.3 we prove several properties that QSS protocols must satisfy in order to achieve their security goals. Thus, as opposed to what occurred in other chapters, in this case we spend considerable efforts on purely mathematical aspects of quantum signature schemes before developing practical protocols. Finally, in section 8.4 we make use of our results to generalize a quantum protocol of Wallden et. al [126] to the multiparty case and prove its security against forging, repudiation and non-transferability. As mentioned before, this protocol can be implemented from any point-to-point quantum key distribution network and therefore is ready to be experimentally demonstrated. The results presented in this chapter appear in Ref. [11].

8.1 Classical and quantum signature schemes

Digital signatures are important cryptographic building-blocks that are widely used to provide security in electronic communications. They achieve three main cryptographic goals: authentication, non-repudiation, and transferability. These properties make them suitable for securing important tasks such as financial transactions, software updates, and legal contracts, forming a fundamental building block for network security. The digital signatures schemes that are in use today, which are based on public-key cryptography, derive their security from unproven computational assumptions, and most of them – notably those based on the RSA algorithm or on elliptic curves – can be broken in the presence of a quantum computer [34].

Consequently, from both a practical and fundamental perspective, there has been interest in studying digital signature protocols that do not rely on computational assumptions, but instead offer information-theoretic security. These schemes were first introduced by Chaum and Roijakkers [32] and are known as *unconditionally secure signature* (USS) schemes. Besides the proposal of Chaum and Roijakkers, several other USS protocols have been suggested [24, 66, 67, 74, 75, 105, 114, 115, 126], most of them based on removing standard trust assumptions from message authentication codes (MACs). However, all known classical USS protocols proposed so far rely on the assumption of either a trusted arbiter or authenticated broadcast channels. Crucially, they also require the use of secure channels, which are impossible to realize with information-theoretic security using classical communication only [111, 90].

However, once quantum communication is allowed, it becomes possible to construct digital signature schemes whose information-theoretic security is based on fundamental principles of quantum mechanics. These are known as quantum signatures schemes (QSS). The first QSS protocol was proposed by Gottesman and Chuang [62], who introduced the main ideas for bringing digital signatures into the quantum world. As discussed before, although influential from a fundamental point of view, their scheme requires the preparation of complex quantum states, performing quantum computations on these states and storing them in quantum memories, making the protocol highly impractical. This is also an issue of other protocols that appeared shortly after [94, 85].

In recent years, new QSS protocols have been proposed that do not require a quantum memory and which can be realized with standard quantum-optical techniques [126, 50, 9]. Some of these protocols have also been demonstrated experimentally [38, 41], thus establishing their viability as a practical technology. Nevertheless, these schemes have not been generalized to more than three participants, and their security goals have not been formally defined. Overall, a security framework for quantum signatures schemes that includes rigorous definitions of security suitable for multiparty protocols has not yet been proposed. In the absence of such a framework, it is not clear how to design secure and practical multiparty protocols, nor what are the concrete advantages of quantum signatures schemes compared to their classical counterparts. In order to build such a framework, we start with some definitions.

8.2 Definitions for QSS protocols

A QSS protocol is carried out by a set of participants and is divided into two stages: the *distribution* stage and the *messaging* stage. The distribution stage is a communication stage, where the parties may exchange quantum and classical signals according to the rules of the protocol. Although in principle they could store the received quantum states in a quantum memory, we focus on more practical protocols in which the participants perform measurements on the states and store the outcomes in a classical memory. The participants may also process their data and communicate classically with each other. Overall, each participant is left with a set of rules to sign a message and to verify signatures. These rules generally depend on their measurement outcomes and the classical communication. At the end of the distribution stage, the parties decide whether to continue to the messaging stage or to abort the protocol. In the messaging stage, one of the participants—the signer—signs a message by attaching a classical string—the signature—to the message. When a participant receives a signed message, they verify its validity according to the rules of the

protocol.

A QSS protocol must achieve authenticity, non-repudiation, and transferability as its main security goals. Informally, these goals can be defined as follows:

1. Authentication: Except with negligible probability, an adversary cannot create a message and signature pair that is accepted by another participant, i.e. a signature cannot be forged.

2. Non-repudiation: Except with negligible probability, a signer cannot later deny having signed a message that has been accepted by an honest recipient.

3. Transferability: A recipient that accepts a signed message can be confident that, except with negligible probability, the signature will also be accepted by other participants.

In order to satisfy non-repudiation and transferability, each recipient must have a method of determining whether other participants will also agree on the validity of a signature. This is straightforward in classical public-key schemes, since every recipient applies the same rule to verify a signature. However, as we discuss later, in an information-theoretic scenario, every recipient must have a different rule for verifying a signed message. Thus, a security model for QSS schemes must deal carefully with the notion of non-repudiation and the transferability of signatures.

We now generalize the work of Swanson and Stinson [118] in the context of USS schemes to construct formal definitions that are also suitable for quantum signature schemes and allow different levels of verification. This will permit us to formalize the structure of general QSS protocols, provide rigorous security definitions, and illustrate properties they must possess in order to be secure.

Definition 11. *A QSS protocol* $\mathcal{Q}$ *is an ordered set* $\{\mathcal{P}, X, \Sigma, L, \text{Gen}, \text{Sign}, \text{Ver}\}$ *where:*

- *The set* $\mathcal{P} = \{P_0, P_1, \ldots, P_{N-1}\}$*, is the set of* N *different participants involved in the protocol. We fix* P_0 *to be the signer, and* P_i *are the possible recipients, with* $i \in \{1, \cdots, N-1\}$*.* X *is the set of possible messages and* Σ *is the set of possible signatures.*

- Gen *is the generation algorithm that gives rise to the functions* Sign *and* Ver *that are used to generate a signature and verify its validity. More precisely, the generation algorithm specifies the instructions for the quantum and classical communication that*

takes place in the distribution stage of the protocol. Additionally, the generation algorithm instructs how to construct the functions Sign *and* Ver *based on the data obtained during the distribution stage. The generation algorithm includes the option of outputting an instruction to abort the protocol.*

- *The signature function* Sign *is a deterministic function* $X \to \Sigma$ *that takes a message* x *and outputs a signature* $\sigma \in \Sigma$*.*

- $L = \{-1, 0, 1, \ldots, l_{\max}\}$ *is the set of possible verification levels of a signed message. A verification level* l *corresponds to the minimum number of times that a signed message can be transferred sequentially to other recipients. The role of the verification level* $l = -1$ *is to prevent repudiation. For a given protocol, the maximum number of sequential transfers that can be guaranteed is denoted by* $l_{\max} \leq N - 1$*.*

- *The verification function* Ver *is a deterministic function* $X \times \Sigma \times \mathcal{P} \times L \to \{\text{True}, \text{False}\}$ *that takes a message* x*, a signature* σ*, a participant* P_i *and a level* l*, and gives a truth value depending on whether participant* P_i *accepts the signature as valid at the verification level* l*. We denote a verification function with a fixed participant* P_i *and level* l *as* $\text{Ver}_{i,l}(x, \sigma) := \text{Ver}(x, \sigma, i, l)$*.*

In general, the generation algorithm will involve randomness in the construction of the signing and verification functions. The randomness may be generated locally by each participant or it can also arise from the intrinsic randomness of quantum measurements. Therefore, even though the signing and verification functions are deterministic functions, they are randomly generated. An illustration of the distribution stage for a generic QSS protocol can be seen in Fig. 8.1.

The verification levels are a method of determining whether a signature can be transferred sequentially among participants. As an illustration, consider a protocol involving a signer Alice, a recipient Bob, and a bank. Other participants may be involved as well. Bob receives a payment from Alice which is signed using a QSS protocol, and Bob wants to transfer this signed message to the bank. For Bob, it does not suffice to verify that the signature comes from Alice – he also needs a guarantee that when he transfers the signed message to the bank, they will be able to validate it. Now suppose that the bank also requires the ability to transfer the message to another participant, otherwise they don't accept the message. Then Bob needs a guarantee that it can be transferred *twice* in sequence, from himself to the bank and from the bank to another participant. In general, Bob may require that a signed message can be transferred many times in sequence. This guarantee is provided by the verification levels: With high probability, a signature that is

verified at level l can be transferred l times in sequence. A signature that is verified at level $l = 0$ is certified to have come from the signer, but does not have a guarantee that it can be transferred to other participants. The role of the verification level $l = -1$ is to prevent repudiation, as will be explained in section 8.2.

We now introduce additional useful definitions, which are inspired from Ref. [118] and generalized to allow different levels of verification. Since QSS protocols have different verification functions for each participant as well as different levels of verification, it is important to carefully specify what it means for a particular signature to be valid.

Definition 12. *A signature σ on a message x is* authentic *if $\sigma = \mathrm{Sign}(x)$.*

Definition 13. *A signature σ on a message x is* valid *if $\mathrm{Ver}_{(i,0)}(x, \sigma) = \mathrm{True}$ for all $i \in \{1, \cdots, N-1\}$.*

Thus, a valid signature is simply one for which all participants can verify that it originates from the intended signer. Crucially, a valid signature does not need to be authentic, a possibility not originally considered in Ref. [118].

It is important that a QSS protocol works properly when all parties are honest, which leads to the following definition.

Definition 14. *A QSS protocol $\mathcal{Q}$ is* correct *if authentic signatures pass the verification function of all participants at all verification levels, i.e. if $\mathrm{Ver}_{(i,l)}(x, \mathrm{Sign}(x)) = \mathrm{True}$ for all x, i, l.*

Definition 15. *A signature σ on a message x is i-*acceptable *if $\mathrm{Ver}_{(i,0)}(x, \sigma) = \mathrm{True}$.*

Note that, as opposed to a valid signature, an i-acceptable signature may not pass the verification functions of participants other than P_i. Therefore, an i-acceptable signature may not be a valid signature. As discussed before, the participants may additionally be interested in the transferability of the signature. This motivates the following definitions.

Definition 16. *A signature σ on a message x is l-*transferable *if $\mathrm{Ver}_{(i,l)}(x, \sigma) = \mathrm{True}$ for all $i \in \{1, \cdots, N-1\}$ and there exists j such that $\mathrm{Ver}_{(j,l+1)}(x, \sigma) = \mathrm{False}$. For $l = l_{\max}$, the function $\mathrm{Ver}_{(j,l_{\max}+1)}(x, \sigma)$ is not defined and we assume by convention that it is always* False.

The above definition means that a signature is l-transferable if l is the largest level for which this signature will pass the verification test of all participants.

Definition 17. *A signature σ on a message x is (i, l)-*transferable *if $\mathrm{Ver}_{(i,l)}(x, \sigma) = \mathrm{True}$ and $\mathrm{Ver}_{(i,l+1)}(x, \sigma) = \mathrm{False}$.*

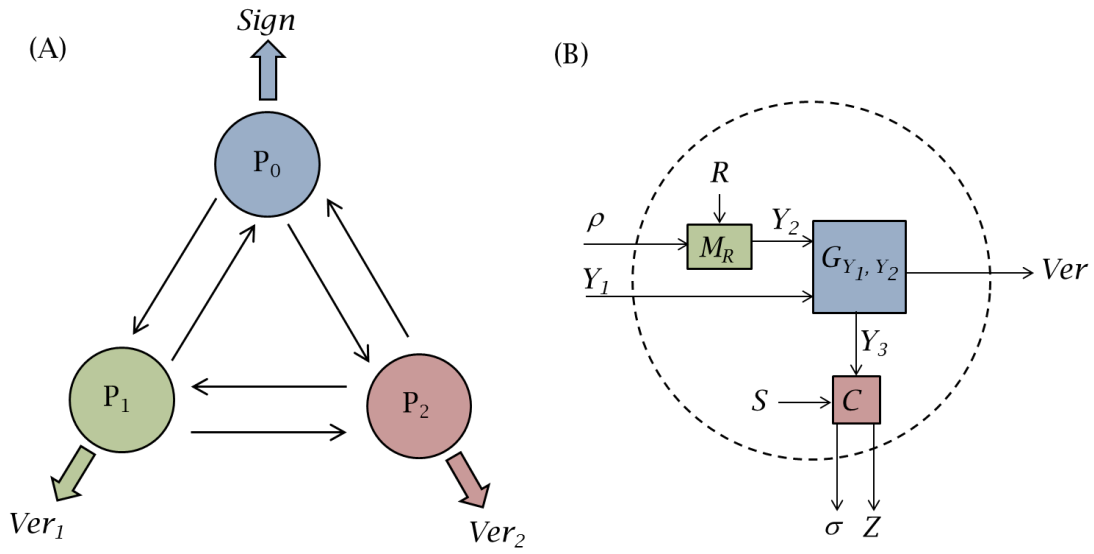


Figure 8.1: (A) Schematic portrayal of a possible generation algorithm in the distribution stage of a QSS protocol with three participants. The three parties exchange messages over classical and quantum channels. At the end of their communication, the signer has a specification of the signing algorithm, and the recipients have a specification of their respective verification functions. (B) An example of a generation algorithm for one of the recipients. From their perspective, they receive a quantum state ρ and a classical message Y_1 from the other participants. A measurement M_R that depends on a random variable R is carried out on the quantum state, and the outcome Y_2, together with the classical data Y_1, is fed to an algorithm G_{Y_1,Y_2}. This program outputs data Y_3 that, together with another possibly random variable S, is fed to a second algorithm C that determines the quantum and classical messages sent to the other participants. After several iterations of these steps, the program G_{Y_1,Y_2} outputs the verification function.

Thus, an (i, l)-transferable signature will pass the verification test of participant i at level l, but not at any other higher level. As opposed to an l-transferable signature, it may not pass the verification functions of other participants.

8.2.1 Dispute resolution

In traditional digital signature schemes based on public-key cryptography, there is a public verification function to test the validity of a signature. If a person denies having signed a message, the recipient who initially verified the signature can show it to other honest parties – a judge for example – who will use the same public verification function to certify its validity and therefore reject the signer's claims.

However, as we show in section 8.3, in a QSS scheme each participant has a different verification function, which makes it possible in principle that two or more participants will disagree on the validity of a signature. This presents a problem particularly for non-repudiation. Suppose that Alice signs a contract and sends it to Bob. The signature passes Bob's verification function at level $l = 0$ and he is convinced that the message comes from Alice. Later, Alice attempts to repudiate by denying that she signed the contract. Bob knows that the other participants have different verification functions than his own, so what can he do to prevent Alice from repudiating? The solution is to incorporate a dispute resolution method: a mechanism to handle the event of a disagreement on the validity of a signature. Based on Ref. [118], we formally define such a method as follows:

Definition 18. *A dispute resolution method* DR *for a QSS scheme* $\mathcal{Q}$ *is a procedure invoked whenever there is a disagreement on whether a signature* σ *on a message* x *is a valid signature originating from the signer* P_0*. The participant invoking the dispute resolution can be anyone, including the signer* P_0*. The procedure consists of an algorithm* DR *that takes as input a message-signature pair* (x, σ) *and outputs a value* {Valid, Invalid} *together with the rules:*

1. *If* $\mathrm{DR}(x, \sigma)$ *outputs* Valid*, then all users must accept* (x, σ) *as a valid signature for* x*.*

2. *If* $\mathrm{DR}(x, \sigma)$ *outputs* Invalid*, then all users must reject* (x, σ) *as a valid signature for* x*.*

Defining a particular dispute resolution method constitutes a crucial part of specifying a QSS protocol. Whether a protocol is secure against repudiation will in general depend on

the choice of dispute resolution. But what are the concrete possibilities that we can choose from? A simple strategy is to designate a trusted participant to be in charge of deciding the validity of a signature whenever the dispute resolution method is invoked. This participant, who may have access to more information about the protocol than others, serves as an arbiter who has the final word whenever there is a dispute. An obvious drawback of this choice is the necessity of trust: If the arbiter behaves dishonestly, perhaps due to being blackmailed to do so, the entire security of the protocol is compromised. Instead, we focus on a *majority vote* dispute resolution method.

Definition 19. *When the validity of a message-signature pair* (x, σ) *is invoked, a majority vote dispute resolution method* $\mathrm{MV}(x, \sigma)$ *is defined by the following rule:*

1. $\mathrm{MV}(x, \sigma) = \text{Valid}$ *if* $\mathrm{Ver}_{(i,-1)}(x, \sigma) = \text{True}$ *for more than half of the users.*
2. $\mathrm{MV}(x, \sigma) = \text{Invalid}$ *otherwise,*

where $\mathrm{Ver}_{(i,-1)}$ *is the verification function at level* $l = -1$.

The need for a verification level $l = -1$ can be understood as a mechanism to prevent repudiation from Alice, and it is only relevant when DR is invoked. Intuitively, $\mathrm{Ver}_{(i,-1)}$ should be chosen such that it is infeasible to produce a signature that passes the verification function of one participant at level $l = 0$, but does not pass the verification function of the majority of participants at level $l = -1$. This will be formalized in section 8.3.

The majority vote dispute resolution method was implicitly used in the protocols of [126, 50] when discussing security against repudiation. The obvious advantage of the majority vote method is that we do not need to trust any fixed participant, but instead assume only that at least *most* of them are honest. However, we emphasize that the security definitions of the following section do not depend on a particular choice of DR.

Note that a dispute resolution method can be used by any participant to convince others of the validity of a signature, even when the signature is only verified at level $l = 0$. If the protocol is secure against repudiation – as will be formally defined in the next section – no person other than the signer will be able to create a signature that is deemed valid by the dispute resolution method. Therefore, if DR is invoked and outputs"Valid", everyone is already convinced that the signature must have come from the signer. This means that the verification levels serve the specific purpose of providing the participants with an assurance that other people will sequentially verify a transferred signature *without the need to invoke dispute resolution.* This is desirable because carrying out dispute resolution may be expensive and should only be invoked under special circumstances.

Finally, we also consider the case in which a participant is dishonest about the level at which he verifies a signature. For instance, suppose that Bob wants to transfer a payment signed by Alice to a store. The store only accepts signatures that they can transfer to a bank, so Bob needs an assurance that Alice's signature can be transferred twice in sequence. Bob verifies the signature at level $l = 2$ and sends it to the store. The store, however, is dishonest, and lies to Bob by claiming that they verified the signature only at level $l = 0$, even though Bob knows that they should have verified it at least at level $l = 1$. If the protocol is secure against repudiation, Bob can invoke dispute resolution to make everyone, including the bank, agree on the validity of the signature. But he has no method of penalizing the bank for its dishonesty. For this reason, we define an additional dispute resolution method for the verification level of a signature.

Definition 20. *A transferability dispute resolution method at level l,* TDR*, for a QSS scheme $\mathcal{Q}$ consists of an algorithm* DR_{l} *that takes as input a message-signature pair (x, σ) and verification level l and outputs* $\{l-$transferable, not $l-$transferable$\}$ *together with the rules:*

1. *If* $\mathrm{DR}_{\mathrm{l}}(x, \sigma, l)$ *outputs* $l-$transferable*, then all users must accept (x, σ) as an l-transferable signature for x.*
2. *If* $\mathrm{DR}_{\mathrm{l}}(x, \sigma, l)$ *outputs* not l-transferable*, then all users must reject (x, σ) as an l-transferable signature for x.*

For this form of dispute resolution method, we can also use a majority vote method defined as before.

Definition 21. *A majority vote transferability dispute resolution method at level l,* $\mathrm{MV}(x, \sigma, l)$*, is defined by the following rule:*

1. $\mathrm{MV}(x, \sigma, l) = l-$transferable *if* $\mathrm{Ver}_{(i,l-1)}(x, \sigma) = \mathrm{True}$ *for more than half of the users.*
2. $\mathrm{MV}(x, \sigma, l) =$ not $l-$transferable *otherwise.*

If the protocol offers transferability – as will be formally defined in section 8.2.2 – any participant that verifies a signature at level l has a guarantee that, with high probability, any other participant will verify the signature at level at least $l - 1$. Therefore, if the majority of participants are honest, a majority vote will indeed deem the signature that was verified at level l by an honest participant as an $(l - 1)$-transferable signature. This form of dispute resolution can serve as a deterrent for dishonest behaviour. In our previous example, the store is discouraged from lying to Bob as they know that a transferability dispute resolution can be used to detect their dishonesty, for which they can be penalized.

8.2.2 Security definitions

Previously, we informally introduced the security goals of QSS schemes. We are now in a position to define them rigorously. The first thing to consider is that more than one of the participants can be malevolent, so in general we must look at coalitions of participants that attack the scheme. In an attempt at repudiation, the coalition must include the signer, whereas a coalition aiming to forge a signature does not include the signer. Formally, we define successful cases of repudiation and forging as follows:

Definition 22. *Given a QSS protocol $\mathcal{Q}$ and a coalition $C \subset \mathcal{P}$ of malevolent participants – including the signer P_0 – that output a message-signature pair (x, σ), we define* repudiation *to be the function:*

$$Rep_C(\mathcal{Q}, DR, \sigma, x) = \begin{cases} 1 & \text{if } (\sigma, x) \text{ is } i\text{-acceptable for some } i \notin C \\ & \text{and } \mathrm{DR}(\sigma, x) = \text{Invalid} \\ 0 & \text{otherwise} \end{cases} \tag{8.1}$$

Thus, a coalition succeeds at repudiation if they can produce a signature that passes the verification test of one of the honest participants at level $l = 0$, but when a DR is invoked, it will be decided that the signature is invalid. According to this definition, a malevolent signer may be able to repudiate with respect to some dispute resolution method, but not other methods.

Definition 23. *Given a QSS protocol $\mathcal{Q}$ and a coalition of malevolent parties $C \subset \mathcal{P}$ – not including the signer P_0 – that output a message-signature pair (x, σ), we define* forging *to be the function:*

$$Forg_C(\mathcal{Q}, \sigma, x) = \begin{cases} 1 & \text{if } (\sigma, x) \text{ is } i\text{-acceptable for some } i \notin C \\ 0 & \text{otherwise} \end{cases} \tag{8.2}$$

A successful forgery therefore only requires the coalition to create a signature that passes the verification test of *one* honest participant at level $l = 0$. Note that we could have additionally asked that the signature be deemed valid by the DR method, but that would constitute a more difficult task for the attackers.

Definition 24. *Given a QSS protocol $\mathcal{Q}$, a coalition of malevolent parties $C \subset \mathcal{P}$ – including the signer P_0 – that output a message-signature pair (x, σ), and a verification level l, we define* non-transferability *to be the function:*

$$NonTrans_C(\mathcal{Q},\sigma,x,l) = \begin{cases} 1 & \text{if } \mathrm{Ver}_{(i,l)}(\sigma,x) = \text{True for some } i \notin C \text{ and} \\ & \mathrm{Ver}_{(j,l')}(\sigma,x) = \text{False for some} \\ & 0 \le l' < l \text{ and some } j \ne i,\ j \notin C \\ 0 & \text{otherwise} \end{cases} \tag{8.3}$$

Therefore, a message-signature pair will be non-transferable at level l if the coalition can produce a signature that at least one honest participant verifies at level l, but some other honest participant does not verify at a lower level. Thus, if the signature is non-transferable, there exists a sequence of participants such that, as the signature is transferred in the order of the sequence, at least one of them will not agree that he can transfer the signature to the remaining participants.

We can now state the main security definitions for QSS protocols:

Definition 25. *Given a coalition $C \subset \mathcal{P}$, a QSS protocol $\mathcal{Q}$ is called* ϵ-secure against forging *if, using their optimal strategy, the probability that the coalition outputs a message-signature pair (x,σ) constituting a successful forgery satisfies*

$$\Pr[Forg_C(\mathcal{Q},\sigma,x) = 1] \le \epsilon, \tag{8.4}$$

where the probability is taken over any randomness in the generation algorithm and the optimal forging strategy.

Definition 26. *Given a coalition $C \subset \mathcal{P}$ and a dispute resolution method* DR*, a QSS protocol $\mathcal{Q}$ is called* ϵ-secure against repudiation *if, using their optimal strategy, the probability that the coalition outputs a message-signature pair (x,σ) constituting successful repudiation satisfies*

$$\Pr[Rep_C(\mathcal{Q},\sigma,x) = 1] \le \epsilon, \tag{8.5}$$

where the probability is taken over any randomness in the generation algorithm and the optimal repudiation strategy.

Definition 27. *Given a coalition $C \subset \mathcal{P}$, a QSS protocol $\mathcal{Q}$ is called* ϵ-transferable *at level l if, using their optimal strategy, the probability that the coalition outputs a non-transferable message-signature pair (x,σ) at level l satisfies*

$$\Pr[NonTrans_C(\mathcal{Q}, \sigma, x, l) = 1] \leq \epsilon, \tag{8.6}$$

where the probability is taken over any randomness in the generation algorithm and the optimal cheating strategy.

Note that the notion of transferability only makes sense between honest participants. As discussed before, even if the protocol is ϵ-transferable, if a participant transfers a signed message to a dishonest participant, the dishonest person can always deny that they have an assurance of being able to transfer it further. In that case, a transferability dispute resolution method can be invoked at level l. Finally, we must clarify that the security definitions we have provided here can in principle be adapted or relaxed, depending on the particular scope of the protocol.

8.3 Properties of QSS protocols.

In this section, we examine several required properties of QSS protocols. Understanding these properties is important for several reasons. First, they serve as guiding principles for the construction of new protocols. Additionally, from a fundamental point of view, it provides insight on the precise characteristics of QSS protocols that give rise to their security. Finally, delineating these properties allows us to construct a coherent picture of the practical challenges to building these protocols as well as their advantages and limitations compared to classical schemes. In the remainder of this section, we list several of these properties and whenever relevant, prove that they are required for the security of QSS protocols.

Observation 28. *In any secure QSS protocol, all classical communication must be authenticated.*

First, authentication is necessary as a guarantee that the participants of the protocol are who they are supposed to be. Otherwise, it would be possible for unauthorized outsiders to participate and compromise the security of the protocol, for example during dispute resolution. Moreover, just as with quantum key distribution, without authentication any QSS protocol is subject to a man-in-the-middle-attack, where an attacker impersonates the participants to each other, thus rendering the entire scheme insecure. Information-theoretic authentication requires shared secret keys, so the above observation implies that any secure QSS protocol requires small shared secret keys between the participants [30].

Since the verification level of a signature corresponds to the maximum number of times a signature can be transferred, a signature that is verified at a given level should also be verified at all lower levels.

Observation 29. $\mathrm{Ver}_{(i,l)}(x,\sigma) = \mathrm{True} \Rightarrow Ver_{(i,l')}(x,\sigma) = \mathrm{True}$ *for all* $l' < l$.

We have mentioned before that in an information-theoretic scenario, it is necessary that each participant has a different verification function. We are now in a position to show this explicitly, following a result of Ref. [118].

Observation 30. *[118] For any QSS protocol that is* ϵ*-secure against forging, it most hold that*

$$\Pr\left(\mathrm{Ver}_{(i,l)} \neq \mathrm{Ver}_{(j,l)}\right) \geq 1 - \epsilon \tag{8.7}$$

for all l *and for all* $i \neq j$.

Proof. Since we are concerned with information-theoretic security, participant P_i can always conduct an exhaustive search for a message-signature pair such that $\mathrm{Ver}_{(i,l)}(x,\sigma) = \mathrm{True}$. However, if $\mathrm{Ver}_{(i,l)} = \mathrm{Ver}_{(j,l)}$, participant P_i will also have produced a message-signature pair that passes the verification function of participant P_j. From observation 29, if participant P_i can produce such a signature, he can also produce a signature such that $\mathrm{Ver}_{(j,0)}(x,\sigma) = \mathrm{True}$, which constitutes successful forging. Therefore, the verification functions must be different at all levels to guarantee security against forging. If the protocol is ϵ-secure against forging, the verification functions must be different with probability greater than $1 - \epsilon$. ■

Corollary 1. *A secure QSS protocol with a finite number of possible signatures can only exist for a finite number of participants.*

Proof. For a given verification level l and message x, a verification function for participant P_i is equivalent to the specification of a subset $S \subset \Sigma$ of signatures such that $\mathrm{Ver}_{(i,l)}(x,\sigma) = \mathrm{True}$. Since the possible number of signatures is a finite set, so is the number of verification functions. From Observation 30, in any secure protocol, every participant must have a different verification function with high probability, and since there is only a finite number of these functions, there can only be a finite number of participants. ■

In principle, one could add new participants to a protocol by performing further communications between the new participant and the original ones. Essentially, in order to

construct a protocol with $N+1$ participants from a protocol with N participants, the new participant could interact with all others in exactly the same way as if he had participated directly in a protocol with $N+1$ participants. This interaction could happen at a later time than the original distribution stage.

Observation 31. *The generation algorithm of a secure QSS protocol must randomly generate the verification and signing functions.*

Proof. If all functions are generated deterministically, the specification of the protocol is sufficient for every participant to know the signing function and all the verification functions. However, if a participant knows the signing algorithm, forging is trivial since he can produce authentic signatures. Similarly, if a participant knows the verification function of another person, he can conduct an exhaustive search to find a message-signature pair that is validated by the other participant, which constitutes a successful forgery. Finally, if a signer knows the verification function of the other participants, she can conduct an exhaustive search to find a signature that is accepted by one of them at level l, but rejected by everyone else at level $l-1$, which allows her to repudiate or break transferability. Thus, a secure protocol requires a randomized generation algorithm. ■

The randomness in the protocol may be produced locally by each participant or it may arise from the intrinsic randomness of performing measurements on quantum systems. Overall, from the point of view of each participant, the generation algorithm must induce a probability distribution over the possible signing functions as well as the possible verification functions. Therefore, the security of a QSS protocol depends crucially on the difficulty of guessing the functions of other participants. We can formalize this requirement with the following observations.

Observation 32. *For a given message x, let S_C be the set of signatures that pass the verification functions at level $l=0$ of all members of a coalition C. Similarly, let S_i be the set of signatures that pass the verification function at level $l=0$ of a participant P_i outside of the coalition. Then, for any QSS protocol that is ϵ-secure against forging, it must hold that*

$$\frac{|S_i \cap S_C|}{|S_C|} \leq \epsilon \text{ for all } i \notin C, \tag{8.8}$$

where $|S|$ is the size of the set S and $|S_i \cap S_C|$ is the intersection between S_i and S_C.

Proof. Let (x, σ_c) be a message-signature pair drawn uniformly at random from S_C. If this signature passes the verification function at level $l=0$ of a participant outside of the coalition, it will constitute a successful forgery. The probability that this happens is given

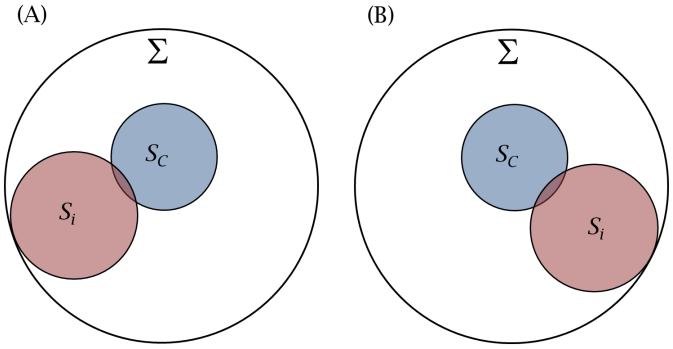


Figure 8.2: S_C is the set of signatures that pass the verification functions at level $l = 0$ of all members of a coalition C. S_i is the set of signatures that pass the verification function at level $l = 0$ of a participant P_i outside of a coalition. If the protocol is secure against repudiation, the intersection $S_C \cap S_i$ must be small compared to S_C. Moreover, the coalition should ignore what the verification functions of the other participants are. For example, even though S_C is the same in both cases, if the protocol is secure against forging, the coalition cannot be able to distinguish whether they are in situation (A) or (B).

by $\frac{|S_i \cap S_C|}{|S_C|}$, which must be smaller than ϵ in order for the protocol to be ϵ-secure against forging. ■

An illustration of the above property can be seen in Figure 8.2. Notice that if a protocol is correct, authentic signatures are verified by all participants. Therefore, for correct protocols it holds that $S_C \cap S_i \neq \emptyset$. Similarly to the above, we can provide a condition for security against repudiation.

Observation 33. *For a given message x, let S_i be the set of signatures that pass the verification function at level $l = 0$ of a participant P_i outside of a coalition C, and let Σ be the set of all possible signatures for this message. Then, for any QSS protocol that is ϵ-secure against forging and ϵ'-secure against repudiation with a majority vote dispute resolution, it must hold that*

$$\frac{|S_i|}{|\Sigma|} \leq \frac{\epsilon'}{1-\epsilon}. \tag{8.9}$$

Proof. Let σ_r be a signature drawn uniformly at random from the set Σ of possible

signatures. The probability that the signer can repudiate with this signature is given by

$$\begin{aligned}\Pr(Rep) &= \Pr[\mathrm{Ver}_{(i,0)}(x,\sigma_r) = \text{True AND } \mathrm{MV}(x,\sigma_r) = \text{Invalid}] \\ &= \Pr[\mathrm{MV}(x,\sigma_r) = \text{Invalid}|\mathrm{Ver}_{(i,0)}(x,\sigma_r) = \text{True}]\Pr[\mathrm{Ver}_{(i,0)}(x,\sigma_r) = \text{True}]. \end{aligned} \tag{8.10}$$

If σ_r is drawn uniformly at random from Σ, conditioning on σ_r passing the verification function of participant P_i induces a uniform distribution over the set S_i. From observation 32, if the protocol is ϵ-secure against forging, the probability that a signature drawn uniformly at random from S_i passes the verification function of another honest participant must be smaller or equal to ϵ. Consequently, the probability that a signature drawn randomly from S_i passes the verification function of the *majority* of participants must also be smaller than ϵ, so we have that

$$\Pr[\mathrm{MV}(x,\sigma_r) = \text{Valid}|\mathrm{Ver}_{(i,0)}(x,\sigma_r) = \text{True}] \leq \epsilon$$

and therefore

$$\begin{aligned}\Pr[\mathrm{MV}(x,\sigma_r) = \text{Invalid}|\mathrm{Ver}_{(i,0)}(x,\sigma_r) = \text{True}] &= 1 - Pr[\mathrm{MV}(x,\sigma_r) = \text{Valid}|\mathrm{Ver}_{(i,0)}(x,\sigma_r) = \text{True}] \\ &\geq 1-\epsilon. \end{aligned} \tag{8.11}$$

If the protocol is ϵ'-secure against repudiation it must hold that $\Pr(rep) \leq \epsilon'$, which, using Eqs. (8.10) and (8.11) gives us

$$\begin{aligned}\epsilon' \geq \Pr(rep) &\geq (1-\epsilon)\Pr[\mathrm{Ver}_{(i,0)}(x,\sigma_r) = \text{True}] \\ &\geq (1-\epsilon)\frac{|S_i|}{|\Sigma|} \\ \Rightarrow \frac{|\mathrm{Ver}_{(i,0)}|}{|\Sigma|} &\leq \frac{\epsilon'}{1-\epsilon},\end{aligned}$$

where we have used the fact that $\Pr[\mathrm{Ver}_{(i,0)}(x,\sigma_r) = \text{True}] = \frac{|S_i|}{|\Sigma|}$. ■

The size of the sets that pass the verification functions at different levels also plays an important role in permitting transferability. In fact, for a special class of QSS protocols, such as the QSS of Refs. [126, 50, 9], it is possible to provide conditions for these sets in order to achieve transferability and security against repudiation. These protocols, which we call *bit-mismatch* protocols, have the following properties. The set of possible signatures Σ is the set of all binary strings of n bits, i.e. $\Sigma = \{0,1\}^K$. For each possible message x, recipient P_i is given a random subset of positions p_i^x of size K of the integers $\{1,2,\ldots,n\}$. The recipient also receives verification bits v_i^x. Upon receiving a signature σ, a recipient

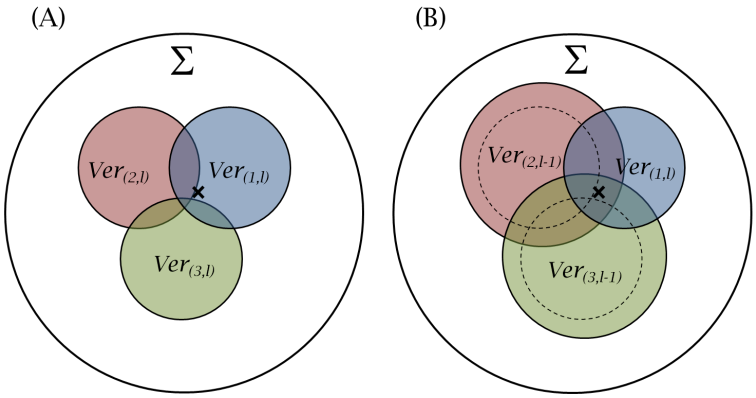


Figure 8.3: For a given verification level l, a signer may produce a signature that, with non-negligible probability, passses the verification function at level l of participant P_1, but not of the other two participants at this same level. Such a signature is illustrated by a cross in the figure. Since more signatures are accepted at lower levels, when the other participants verify that same signature at level $l-1$, it now passes the verification function of all participants. This feature prevents repudiation and permits transferability.

collects the bits of σ at the positions corresponding to p_i^x to form a shorter string which we call σ_i. The verification functions are then given by:

$$\mathrm{Ver}_{(i,l)}(x,\sigma) = \begin{cases} \text{True} & \text{if } h(\sigma_i, v_i^x) \leq s_l K \\ \text{False} & \text{otherwise} \end{cases} \tag{8.12}$$

for some $s_l \in [0, \frac{1}{2})$ which depends on the verification level l and where $h(v_i^x, \sigma_i)$ is the Hamming distance between v_i^x and σ_i.

Observation 34. *For any correct bit-mismatch protocol that is transferable and is secure against repudiation with a majority vote dispute resolution method, it must hold that* $s_l > s_{l-1}$ *for all* l.

Proof. Consider a cheating strategy from the signer in which she randomly flips each bit of the authentic signature $\mathrm{Sign}(x)$ with probability p, leading to an altered signature σ'. For each participant, the choice of p induces a corresponding probability $q_{i,l}(p)$ that the altered signature will pass their verification function at level l. Since the protocol is correct, authentic signatures pass the verification functions of all participants at all levels, which implies that $q_{i,l}(0) = 1$ and $q_{i,l}(1) = 0$ for all l. The induced probability $q_{i,l}(p)$ is

a continuous function of p[1], which implies that there must exist a value p_l^* such that, for some non-negligible $\delta > 0$, it holds that

$$\frac{1}{2} - \delta < q_{i,l}(p_l^*) < \frac{1}{2} \tag{8.13}$$

for all participants P_i.

Now consider the case $l = 0$ and assume that $s_0 \leq s_{-1}$. By choosing p_0^* for her cheating strategy, the signer can create a signature that a given participant accepts with a non-negligible probability greater than $\frac{1}{2} - \delta$ and smaller than $\frac{1}{2}$, according to Eq. (8.13). Moreover, since $s_0 \leq s_{-1}$, Eq. (8.13) implies that the probability that any other participant accepts the signature at level $l = -1$ must be smaller than $\frac{1}{2}$. In that case, with non-negligible probability, the majority of participants will reject the signature during dispute resolution, where they check the signature at level $l = -1$. Therefore, such a protocol cannot be secure against repudiation.

Similarly, for the case $l > 0$, a dishonest signer can choose p_l^* for her cheating strategy and have any given participant accept a signature at this level with probability at least $\frac{1}{2} - \delta$. If $s_l \leq s_{l-1}$, when the participant that accepts the signature at level l transfers it to another person, the new participant will reject the signature at level $l - 1$ with non-negligible probability greater than $\frac{1}{2}$. Thus, such a protocol cannot offer transferability. ■

Intuitively, the above proof states that the size of the set of signatures that pass the verification functions at a given level must increase for lower verification levels. This is illustrated in Fig. 8.3.

In the next section, we use the security framework and properties developed so far to generalize the protocol P2-WDKA introduced in Ref. [126] to the case of many participants. We provide a full security proof against forging, repudiation and non-transferability.

8.4 Generalized P2-WDKA protocol

This protocol, which is a generalization of the protocol P2 of Ref. [126], is a classical protocol where the role of quantum communication is exclusively to realize secure channels

[1]This probability distribution can be shown to be equal to the sum of two cumulative binomial distributions, which are continuous functions.

using quantum key distribution (QKD). Since QKD is a practical technology, this makes our protocol practical. Moreover, this allows us to use existing security proofs for QKD to deal with attacks on the quantum communication, which is generally a very challenging task.

In the protocol, we have $N+1$ participants given by the set $\mathcal{P} = \{P_0, \cdots, P_N\}$. The set of possible messages is $X = \{x_1, \ldots, x_M\}$, where there are M different possible messages. Additionally, $\Sigma = \{0,1\}^K$ is the set of possible signatures, where $K = nN$ is the length of the total signature and n is an integer that depends on the required security parameters and is divisible by N.

As in any cryptographic protocol, we make some trust assumptions. In particular, we assume that the number of honest participants is at least h, with $h > \frac{N+1}{2}$. We can then define the fraction of dishonest participants as $d_f = 1 - h/N$. The maximum verification level $l_{\max}$ is determined by the allowed fraction of dishonest participants:

$$(l_{\max} + 1)d_f < \frac{1}{2}. \tag{8.14}$$

The reason for this restriction will become clear later. The distribution stage of the protocol, which gives rise to the generation algorithm, proceeds as follows:

1. All the participants use QKD links in order to establish pairwise secret keys. Each recipient needs to share a secret key of nM bits with the signer P_0 and a secret key of $2\frac{nM}{N}(1 + \lceil \log_2 n \rceil)$ bits with each of the other recipients.

2. For each possible message $x \in X$, the signer selects a string σ^x of $K = nN$ bits uniformly at random and divides it into N sections $\{\sigma_1^x, \sigma_2^x, \ldots, \sigma_N^x\}$. The signer sends σ_i^x to participant P_i over a secure channel using their shared secret keys.

3. For every possible message, each recipient randomly divides the set $\{1, 2, \ldots, n\}$ into N disjoint subsets $\{p_{i,1}^x, p_{i,2}^x, \ldots, p_{i,N}^x\}$ and uses the bit values of σ_i^x at the randomly chosen positions $p_{i,j}^x$ to form the string $v_{i,j}^x$.

4. For all $i \neq j$, each participant P_i transmits the string $v_{i,j}^x$ and the positions $p_{i,j}^x$ to participant P_j over a secure channel using their shared secret keys. Participant P_i keeps $v_{i,i}^x$ and $p_{i,i}$ to herself.

5. Each participant P_j defines a test for a section σ_i^x as follows. First, they form a shorter string $\sigma_{i,j}^x$ from σ_i^x by keeping only the bits corresponding to the positions $p_{i,j}^x$. The test is then defined as

$$T^x_{i,j,l}(\sigma^x_i) = \begin{cases} 1 & \text{if } h(\sigma^x_{i,j}, v^x_{i,j}) < s_l \frac{n}{N} \\ 0 & \text{otherwise} \end{cases} \tag{8.15}$$

where $h(\sigma^x_{i,j}, v^x_{i,j})$ is the Hamming distance between $\sigma^x_{i,j}$ and $v^x_{i,j}$ and s_l is a fraction defined by the protocol. These fractions satisfy

$$\frac{1}{2} > s_{-1} > s_0 > s_1 > \cdots > s_{l_{\max}}. \tag{8.16}$$

6. The verification function is defined as

$$\text{Ver}_{(i,l)}(x, \sigma) = \begin{cases} \text{True} & \text{if } \sum_{j=1}^n T^x_{j,i,l}(\sigma^x_j) > N f_l \\ \text{False} & \text{otherwise} \end{cases} \tag{8.17}$$

where f_l is a threshold fraction given by

$$f_l = \frac{1}{2} + (l+1)d_f. \tag{8.18}$$

7. The signature function is given by $\text{Sign}(x) = \sigma_x$.

8. Majority vote is the dispute resolution method.

For clarity, the main steps of the distribution stage are illustrated in Fig. 8.4

The verification function, in words, accepts at level l if there are more than a fraction f_l of the sections $\{\sigma^x_1, \sigma^x_2, \ldots, \sigma^x_N\}$ that pass the test of the ith participant. This choice of the fraction f_l is made in order to satisfy a few constraints. First, we need the protocol for $l = -1$ to still require more than half of the tests to succeed i.e. $f_{-1} > \frac{1}{2}$. Second, we want the difference of the thresholds between two levels to exceed the fraction of dishonest participants i.e. $f_l - f_{l-1} > d_f$. Finally, by noting that $f_l \leq 1$ for all l, we determine the maximum value that l can take and this results in Eq. (8.14).

In the protocol, there are two different types of thresholds, s_l and f_l, both depending on the verification level l. The first threshold, s_l, determines whether a given part of the signature passes the test or not, by checking the number of mismatches at this part. The second threshold, f_l, determines how many parts of the signature need to pass the test in order for the signature to be accepted at that level.

An example of why different fractions for each verification level are needed is as follows. Assume that one recipient, P_1 for example, is a "spy" of an adversarial sender P_0, i.e.

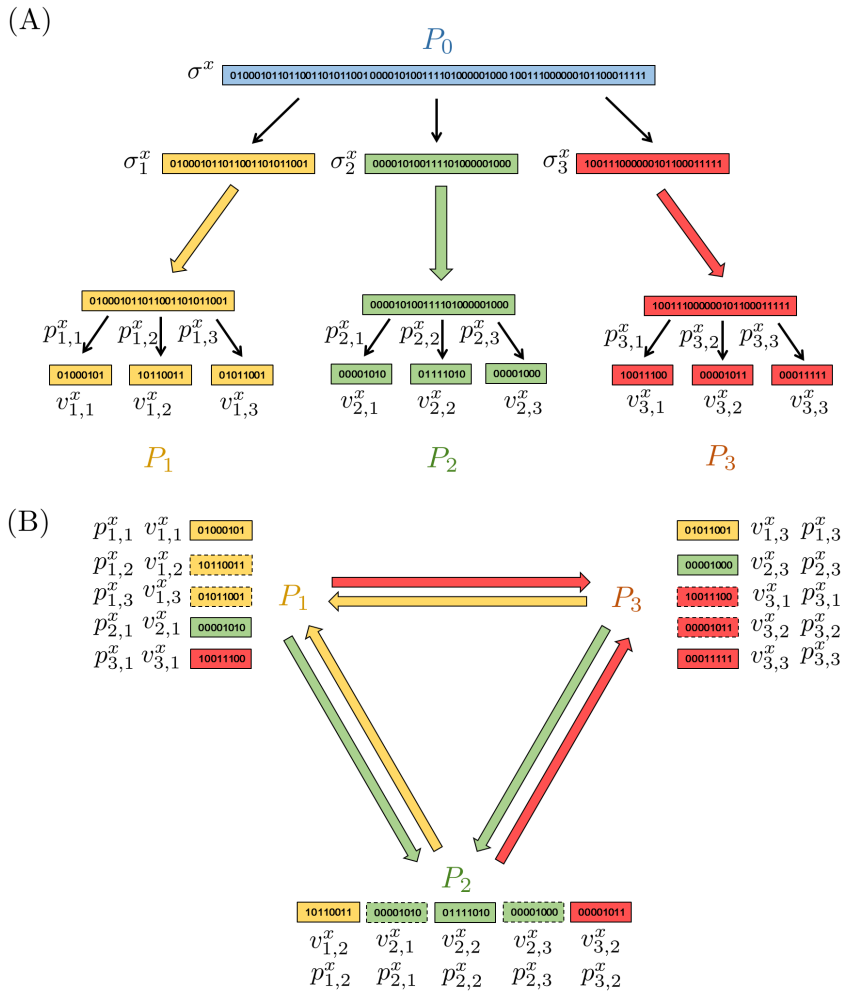


Figure 8.4: Illustration of the protocol with four participants. In part (A), the sender divides a randomly generated string σ^x into three sections $\sigma_1^x, \sigma_2^x, \sigma_3^x$ and sends one of them to the other participants over a secure channel, using a secret key previously generated using quantum key distribution. Secure channels are portrayed with solid coloured arrows. The other participants divide the sections they receive to produce the strings $v_{i,j}^x$ alongside the corresponding positions $p_{i,j}^x$. In (B), the participants exchange the sections $v_{i,j}^x$ of the signature and the positions $p_{i,j}^x$ over secure channels. In the end, every participant keeps their original sections plus one additional section from each of the other participants, which they use for their verification functions. The sections in dashed boxes are known by the corresponding participant but are not used in the verification functions.

colludes with her in order to make two honest recipients P_2 and P_3 disagree on the validity of a signature. The spy can tell the sender the elements $(v^x_{1,2}, p_{1,2})$ and $(v^x_{1,3}, p_{1,3})$. The sender can then use this information to send a signature σ' that differs from the ideal signature σ only by flipping all the bit values at the positions determined by $p_{1,3}$. Recipient P_2 would accept the message, since he finds no errors. However, P_3 will find that *all* the bits of $v_{1,3}$ wrong, which will make his test fail. In general, if $d_f n$ dishonest participants exist, and if all of them are spies, two honest participants can differ by at most $d_f n$ tests. From Eq. (8.18), choosing $f_l - f_{l-1} = d_f$ allows the protocol to remain secure against this type of attack.

We now proceed to prove the security of this protocol. In the following, for simplicity, we drop the superscript labelling the message x from $v^x_{i,j}$, $p^x_{i,j}$ and $T^x_{(i,j,l)}$, and we refer to participants by their index only, i.e. as i instead of P_i.

8.4.1 Security proofs:

We separately address the security of this protocol against forging, repudiation and non-transferability. Our main concern will be to prove that all cheating probabilities decrease exponentially fast in the protocol parameters, without worrying significantly about the tightness of the bounds we introduce in the security proofs.

We begin by noticing that the value of n must be chosen depending on other parameters and on the level of security. In particular, we want the probabilities for forging, non-transferability, and repudiation to decrease exponentially fast with n. However, the number of participants N also enters the security expressions. To make sure that all the cheating probabilities go to zero even when the number of participants is very large, in general we require that

$$n \geq \alpha N^{1+\delta} \tag{8.19}$$

where $\alpha \gg 1$ is a large positive constant and δ a small positive constant.

Forging. Intuitively, security against forging can be understood as follows. In order to forge, a coalition C needs to output a message-signature pair (x, σ) that is i-acceptable for some $i \notin C$. Recall that a signature σ is i-acceptable if $\mathrm{Ver}_{(i,0)}(x, \sigma) = \mathrm{True}$ and the verification function will be passed if more than $N f_0$ tests are passed. The coalition can always pass the $N d_f$ tests arising form its members, but they must also pass additional tests corresponding to honest participants. However, since the positions $p_{i,j}$ and the sections

$v_{i,j}$ of these tests were exchanged through secure channels, they are completely unknown to the coalition. This prevents them from passing these tests and therefore from forging a message. Below is a formal proof of this fact.

In general, according to our definitions, we consider forging successful if the coalition can deceive *any* honest participant, and not a fixed one. Here, for simplicity, we restrict attention to trying to deceive a fixed participant, and we prove that this probability decays exponentially fast with the parameter n. At the end, we extend this to the general case where the target is not a fixed participant. Therefore, for now, we fix the recipient that the coalition wants to deceive to be i.

The coalition knows the pairs $(v_{j,i}, p_{j,i})$ for all $j \in C$, so they can use this knowledge to trivially pass Nd_f tests. It follows that in order to forge, the coalition must pass at least $N(f_0 - d_f) = \frac{N}{2}$ tests out of the $N(1 - d_f)$ tests that they do not have access to. The first step to compute the probability that they can do this is to calculate the probability of passing a single test $T_{j,i,0}$ for $j \notin C$.

1. We denote by p_t the probability to pass a test at level $l = 0$ for a coalition with no access to the pair $(v_{i,j}, p_{i,j})$. Because the strings $(v_{i,j}, p_{i,j})$ were transferred over secure channels by honest recipients, they are completely unknown to the coalition and hence the probability of guessing correctly a single bit of $v_{i,j}$ is exactly $\frac{1}{2}$. In order to pass the test, the coalition needs to guess at least a fraction s_0 of bits out of a total of $\frac{n}{N}$ bits. The probability that they can achieve this can be bounded using Hoeffding's inequality as

$$p_t \leq \exp\left[-2\left(\frac{1}{2} - s_0\right)^2 \frac{n}{N}\right], \tag{8.20}$$

   which decays exponentially with the number $\frac{n}{N}$ provided that $s_0 < \frac{1}{2}$. Note that, from Eq. (8.19), this term decays exponentially even for $N \to \infty$.

2. We now give a bound for the probability of forging against a *fixed* participant. This can be obtained by computing the probability of passing at least one of the unknown $N(1 - d_f)$ tests, which is given by

$$\begin{aligned} \Pr(\text{FixedForge}) &< 1 - (1 - p_t)^{N(1-d_f)} \approx N(1 - d_f)p_t \\ &\leq (1 - d_f)N \exp\left[-2\left(\frac{1}{2} - s_0\right)^2 \frac{n}{N}\right], \end{aligned} \tag{8.21}$$

where we have used the fact that $p_t \ll 1$ in the approximation. Again, this probability goes to zero exponentially fast in the parameter n. Note also that, by Eq. (8.19), this expression goes to zero even for the case $N \to \infty$, as the term with p_t goes exponentially fast to zero while the other term grows only linearly in N.

3. We have now computed the probability to deceive a fixed participant i. The total number of honest participants is $N(1-d_f)$ and for successful forging we require that any one of them is deceived. We therefore obtain

$$\begin{aligned} \Pr(\text{Forge}) &= 1 - (1 - \Pr(\text{FixedForge}))^{N(1-d_f)} \\ &\lesssim N^2(1-d_f)^2 \exp\left[-2\left(\frac{1}{2} - s_0\right)^2 \frac{n}{N}\right]. \end{aligned} \tag{8.22}$$

Once again, this probability decreases exponentially fast with n.

Transferability. In order to break the transferability of the protocol, a coalition C must generate a message-signature pair (x, σ) that is accepted by an honest recipient i at level l but rejected by another honest recipient j at a level $l' < l$. As usual, the coalition can make recipients disagree on those tests that arise from its members, but in order to break transferability, they will also have to make them disagree for at least some tests corresponding to other honest participants. Intuitively, this is hard for the coalition because the positions and verifications bits of these tests were transmitted over secure channels, so they are completely unknown to the coalition. Moreover, as explained in observation 34, the difference between the thresholds s_l and s'_l makes it difficult for a test to be passed at level l but not at level l'. In the following, we give a formal proof of security against non-transferability.

To provide an upper bound, we consider the maximum number of dishonest participants, i.e. Nd_f. For simplicity, we fix the participants whom the coalition is trying to deceive to be i and j, while all the other honest participants are labelled with the index k. In general, according to our definitions, transferability fails if the coalition forms a signature that is not transferable for *at least one* pair of honest participants i, j. Therefore, we should take into account all possible pairs of honest participants. Here, we first focus on the case of a fixed pair of participants, and we give at the end the more general expressions. The members of the coalition C are labelled with the index c.

1. First, we compute $p_{m_{l,l'}}$, which is the probability that the kth test $T_{k,i,l}$ of an honest recipient i at level l is accepted *and* the test $T_{k,j,l'}$ of another honest recipient j at a level $l' < l$ is rejected. Since the sender is in the coalition, they know the values of all the sections $v_{i,j}$, but they are completely ignorant of the positions $p_{k,i}$ and $p_{k,j}$, since participants k, i and j are all honest. As in observation 34, the coalition can decide to send signatures in such a way that they introduce an average fraction of mistakes p_e compared to the ideal signature that was used to generate the verification algorithms. Thus, the average fraction of mistakes is under their control. Since the protocol is symmetric for all participants, this average fraction of mistakes will be the same for all honest participants and in particular for both i and j.

   To compute a bound on the joint probability of i accepting at level l and j rejecting at level l' we consider

$$\begin{aligned} p_{m_{l,l'}} &= \Pr\left(i \text{ accepts at level } l \text{ AND } j \text{ rejects at level } l'\right) \\ &\leq \min\{\Pr\left(i \text{ accepts at level } l\right), \Pr\left(j \text{ rejects at level } l'\right)\}. \end{aligned} \tag{8.23}$$

   The probability of passing the test at level l with an average error p_e can be bounded using Hoeffding's inequalities to be below $\exp\left[-2(p_e - s_l)^2 \frac{n}{N}\right]$. This is the case since the expected number of mistakes are $\frac{n}{N} p_e$ while the mistakes that are tolerated for acceptance are $\frac{n}{N} s_l$. Similarly, the probability of failing the test at level l' with average errors p_e can be bounded to be smaller than $\exp\left[-2(s_{l'} - p_e)^2 \frac{n}{N}\right]$.

   In order to maximize their chances of successful cheating, the coalition must choose a value of p_e satisfying

$$s_l < p_e < s_{l'}. \tag{8.24}$$

   Since in the bound of Eq. (8.23) we are taking the minimum over both cases, the best choice for the coalition is to have both probabilities coincide. This is achieved by using a fraction of errors $p_e = (s_l + s_{l'})/2$ and in that case we obtain the bound

$$p_{m_{l,l'}} \leq \exp\left(-\frac{(s_{l'} - s_l)^2}{2} \frac{n}{N}\right) \tag{8.25}$$

   which decays exponentially with $\frac{n}{N}$ and it also depends on the difference $(s_{l'} - s_l)$.

2. In order for the coalition to successfully cheat, the number of tests that pass for the ith recipient must be at least $Nf_l + 1$. Out of those tests we can assume that Nd_f were due to the coalition, but there are still $N(f_l - d_f) + 1$ tests that the coalition does not have access to. In order for the non-transferability to be successful, at least one of these $N(f_l - d_f) + 1$ tests should fail for participant j at level l'. We

can bound the probability that the participants disagree on at least one of these tests by considering the probability that they agree on *all of them*, which is given by $(1 - p_{m_{l,l'}})^{N(f_l - d_f)+1}$. Therefore, the probability for non-transferability of two fixed participants can be bounded as

$$\begin{aligned}\Pr(\text{FixedNonTrans}) &\leq 1 - (1 - p_{m_{l,l'}})^{N(f_l - d_f)+1} \\ &\approx [N(f_l - d_f) + 1]\, p_{m_{l,l'}} \\ &\leq [N(f_l - d_f) + 1] \exp\left(-\frac{(s_{l'} - s_l)^2}{2}\frac{n}{N}\right) + O(p^2_{m_{l,l'}}). \end{aligned} \tag{8.26}$$

This goes to zero exponentially with $\frac{n}{N}$. Note that the first term scales linearly in N, but $p_{m_{l,l'}}$ decays exponentially with $\frac{n}{N}$, therefore with the choice of Eq. (8.19) this probability also vanishes at all limits of interest.

3. Finally, we should consider the general case, where the participants i, j are not fixed. Again, we can see that, because the probability for fixed parties decays exponentially in the parameter n, the protocol remains secure. The number of honest pairs of participants is $[N(1 - d_f)][N(1 - d_f) - 1]/2 := N_p$, so we obtain

$$\begin{aligned}\Pr(\text{NonTrans}) &= 1 - (1 - \Pr(\text{FixedNonTrans}))^{N_p} \\ &\approx O(N^3) \exp\left(-\frac{(s_{l'} - s_l)^2}{2}\frac{n}{N}\right). \end{aligned} \tag{8.27}$$

$$\tag{8.28}$$

Repudiation. In order to repudiate, a coalition that includes the signer P_0 must generate an i-acceptable signature for some honest participant, where invoking the dispute resolution DR results in "Invalid". This means that the coalition wants to make any participant accept a signature at level $l = 0$, but then have the majority of participants reject the same signature at level $l = -1$. Intuitively, this must be difficult for the coalition for the same reason that breaking transferability was hard: it is not possible to have a participant accpet a message at level l while having another participant reject the message at a lower level l'.

Formally, we can reduce the problem of proving security against repudiation to the special case of non-transferability from level $l = 0$ to level $l = -1$ in the following three steps.

1. We first find the probability of non-transferability for a fixed pair of participants, i.e. from a fixed honest participant i at level $l = 0$ to another fixed honest participant

j at level $l = -1$. We denote this probability by p_1 and, as found before, it can be bounded by

$$p_1 \lesssim [N(f_0 - d_f) + 1]\, p_{m_{0,-1}} \leq \left(\frac{N}{2} + 1\right) \exp\left(-\frac{(s_{-1} - s_0)^2}{2}\frac{n}{N}\right), \tag{8.29}$$

where we have used the fact that $(f_0 - d_f) = \frac{1}{2}$ from Eq. (8.18). As before, this decreases exponentially fast in n.

2. The second step is to note the following. For a fixed recipient i to accept at $l = 0$, it means that at least $Nf_0+1 = N(\frac{1}{2}+d_f)+1$ of the N tests must pass. Out of these, $\frac{N}{2}+1$ must have come from honest participants. Now, each of those honest participants that sent i a part that passed his tests also sent the other honest participants sections which, with probability $1 - p_1$, pass their tests at level $l = -1$. For a message to be declared invalid in the dispute resolution DR, half of the participants have to reject. However, at least $\frac{N}{2} + 1$ are unlikely to reject, since the probability that they do reject is p_1, which can be made arbitrarily small. In other words, for the DR to give Invalid, at least one of the honest participants needs to fail the transferability for a fixed pair of participants.

3. It is now clear that if no fixed pair of honest participants i, j fails the transferability for levels $l = 0$ to $l = -1$, then the coalition cannot repudiate. This leads to the following bound for the probability of repudiation,

$$\begin{aligned} \Pr(\text{Rep}) &\leq 1 - (1 - p_1)^{N_p} \approx N_p p_1 + O(p_1^2) \\ &\leq O(N^3) \exp\left(-\frac{(s_{-1} - s_0)^2}{2}\frac{n}{N}\right), \end{aligned} \tag{8.30}$$

where N_p as before is the number of honest pairs $[N(1 - d_f)][N(1 - d_f) - 1]/2$ and p_1 decays exponentially with $\frac{n}{N}$.

We have seen that all security parameters, from Eqs. (8.21), (8.26) and (8.30), go to zero exponentially fast with $\frac{n}{N}$, provided correct choices of s_l and f_l are made. As stressed before, by Eq. (8.19), we also know that these parameters go to zero even if the number of participants N goes to infinity.

Secure channels from QKD. Security proofs for QKD rely on the assumption that the parties wishing to exchange a secret key behave honestly during the execution of

the protocol. In the context of our multiparty protocol for quantum signature schemes, this assumption does not hold, since some of the participants performing QKD may be dishonest. However, we can show that this does not present a problem for the security of our protocol in three steps. Similar arguments are made in [4].

Step 1: Only honest-dishonest QKD links may be affected. The first observation is that dishonest behaviour during QKD may only be an issue when the QKD link connects an honest participant with a dishonest one. For two honest participants, standard QKD security proofs apply, so we are not concerned with this scenario. For the case of two dishonest participants, since all members of the coalition have access to the same information – as is assumed in our security definitions – it is irrelevant whether they behave honestly during QKD. Similarly, honest participants do not eavesdrop on dishonest participants, so there are no consequences to the security of the protocol.

In the following two steps we show that for the case of an honest and a dishonest participant using QKD to establish a shared secret key, *any* adversarial behaviour during the QKD stage of the protocol is equivalent to a dishonest behaviour in subsequent parts of the protocol. Therefore, we can assume that the participants were honest during the QKD stage but dishonest at later stages of the protocol, a situation we have already included in our security proofs.

Step 2: No gain from leaking information. At the end of a QKD protocol, an honest participant P_i holds a key register X which, in the ideal case, is identical to the string Y of a dishonest participant P_c and is completely unknown to any other party. This means that any dishonest behaviour by participant P_c can only lead to two possible outcomes: (i) The registers X and Y are not identical, or (ii) X is correlated with the register of another party. Since we assume that all dishonest participants are in coalition, all of them have perfect knowledge of the register Y, so there is no need to eavesdrop information about this string. They of course benefit from knowledge of X, but they can have perfect knowledge of X simply if P_c behaves honestly during QKD. Therefore, leakage of information does not help the adversarial coalition.

Step 3: No gain from imperfect keys. Similarly, if there are mismatches between the registers X and Y, any message which is transmitted secretly by using a one-time pad with either register X or Y will be received with errors in all positions in which X and Y differ. However, if Y is used by P_c to transmit a message to the honest participant P_i, the situation is exactly equivalent to one in which they have identical secret keys, but P_c decided to introduce errors in the message sent to P_i. Similarly, if P_i is the one sending the message, the situation is equivalent to the keys being identical but participant P_c introducing errors after receiving the message. In fact, since in order to cheat, the

coalition needs to know the verification function of the honest participants, their optimal strategy is to be honest during the QKD stage and have a perfect copy of the other participants' secret keys. Therefore, in a quantum signature scheme, the security of QKD is only relevant in order to protect honest participants who want to establish a secret key. It is precisely in this regime that standard QKD proofs apply.

8.5 Discussion

In this chapter, we have provided a full security framework for quantum signature schemes, generalizing the security definitions of Swanson and Stinson [118] to allow for quantum schemes and different levels of verification. Additionally, we have proved several properties that QSS protocols must satisfy in order to achieve their security goals. Together, these results form a powerful set of tools to be employed in the understanding and development of improved QSS protocols in a general setting.

In fact, we have done just that by using our security framework to generalize the P2-WDKA protocol of Wallden et. al [126] to the multiparty case. This protocol is secure against forging, repudiation and non-transferability, relying on minimal security assumptions. Crucially, the quantum-mechanical features responsible for the security of the protocol can be completely outsourced to quantum key distribution (QKD), where a vast literature of sophisticated security proofs already exists. This is not only extremely helpful in dealing with the security proofs of the protocol, it also takes care of its practicality: since this protocol can be implemented from any point-to-point QKD network, our protocol is already a practical. This makes experimental demonstrations in the short-term future a real and exciting possibility. Moreover, this feature also addresses the issue of authentication in quantum signature schemes: we can simply use QKD to generate new secret keys to be used in the authentication of future instances of a signature protocol.

As a consequence of our results and those of Ref. [126], the status of unconditionally secure signature schemes should be considered analogous to that of secure communication, where a classical protocol – the one time-pad – already exists and can guarantee information-theoretic security at the expense of shared secret keys. Quantum communication can then be used to establish these secret keys via unsecured quantum channels. Similarly, for signature schemes, there exist classical protocols – like our generalized P2-WDKA protocol – that provide information-theoretic security at the expense of shared secret keys. Remarkably, even in this setting where parties can be dishonest, quantum key distribution can be used to establish the secret keys. Overall, we can now understand

unconditionally secure signature schemes as a possible practical application of quantum key distribution.

Future work should focus on optimizing these classical protocols, most importantly in reducing the length of the secret keys that need to be exchanged as a function of the message size. Additionally, it is important to continue to study protocols where quantum communication can be used to construct quantum signature schemes without the need to distil a secret key, as those schemes could potentially possess additional advantages. Finally, the results presented in this chapter lead to an interesting question: are there other yet undiscovered applications of quantum key distribution besides secret communication using a one-time pad?

Chapter 9

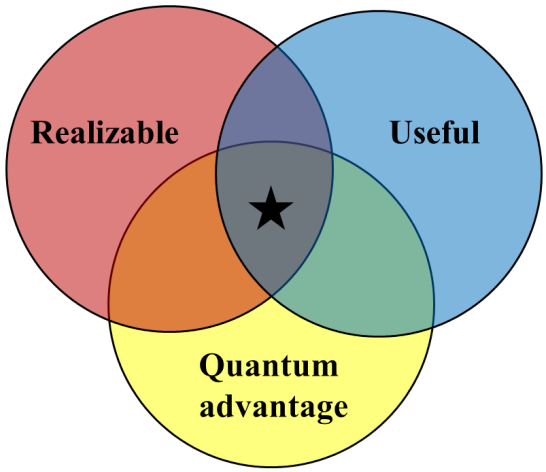
Conclusion

What will the communication networks of the future look like? What role will quantum mechanics play in these networks? These are intriguing questions, the answers to which we currently ignore. However, as it has been discussed extensively in this thesis, quantum communication allows new possibilities that are simply not accessible with classical resources. Moreover, as we continue to improve the devices used to perform classical communication, it is very likely that in reaching their ultimate levels of performance, it will be necessary to harness quantum effects. Even though nobody can predict the future, it would indeed be very surprising if, several decades from today, quantum mechanics does not play a significant role in the way that we transmit and process information. Nevertheless, it remains a challenge to actually build practical quantum communication networks and to fully understand their advantages compared to the classical case.

In this thesis, we have reported various advances towards this goal, most notably by specifying a series of practical quantum communication protocols that can be realized with current technology. In the context of quantum communication complexity, these results pave the way for experimental demonstrations of the exponential advantages that are possible using quantum communication. The strategy that we used was to provide a theoretical reformulation of existing protocols that allowed them to be realized with current experimental techniques. Although this strategy proved to be successful, it is important to understand that, in order to harness all of the potential of quantum communication, it will ultimately be necessary to improve our ability to manipulate quantum systems, effectively giving rise to new technological capabilities.

The results presented in this thesis can be interpreted as a relocation of protocols with a quantum advantage which were previously believed to be experimentally intractable into

the set of protocols that can be experimentally realized. The usefulness of these protocols is currently unclear, but the insights developed are likely to be helpful to develop new practical protocols. Overall, we can view the results of this thesis as part of the many advances that will be required in order to reshape the way that humanity transmits and processes information.



APPENDICES

Appendix A

Simulated Annealing Algorithm

Here we fully describe the simulated annealing (SA) algorithm. The algorithm is based on a biased random walk in state space that preferentially selects states with a higher value of the likelihood function at each new step of the iteration. However, it also accepts jumps to states with lower values with a probability that depends on a global parameter T, usually referred to as the temperature because of its similarity with the physical temperature in the annealing process of metallurgy.

Below is a full enumeration of all the steps of the algorithm to calculate the maximum value of the likelihood function $\mathcal{L}(\sigma)$ over the set Γ_W. A graphical illustration of how the maximum value of the function is reached as the algorithm progresses is found in Fig. A.1. The random walk here described is based upon the quantum adaptation of the Metropolis-Hastings algorithm depicted in [21].

Simulated annealing algorithm:

1. Select an initial value T_0 for the temperature T as well as for the "step size" Δ.

2. Generate a $d \times d-$dimensional random state $|\psi\rangle$ according to the Haar measure, where d is the dimension of the underlying Hilbert space $\mathcal{H}$. Trace out one of the subsystems to obtain the state σ_0. If $\sigma_0 \in \overline{\Gamma_W}$ continue to the next step, repeat otherwise.

3. Randomly choose a 2×2 Hermitian matrix H_{kl} in the following way. Pick two integers k, l randomly from the set $\{1, 2, \ldots, d\}$. If $k < l \rightarrow H_{kl} = |k\rangle\langle l| + |l\rangle\langle k|$, similarly if

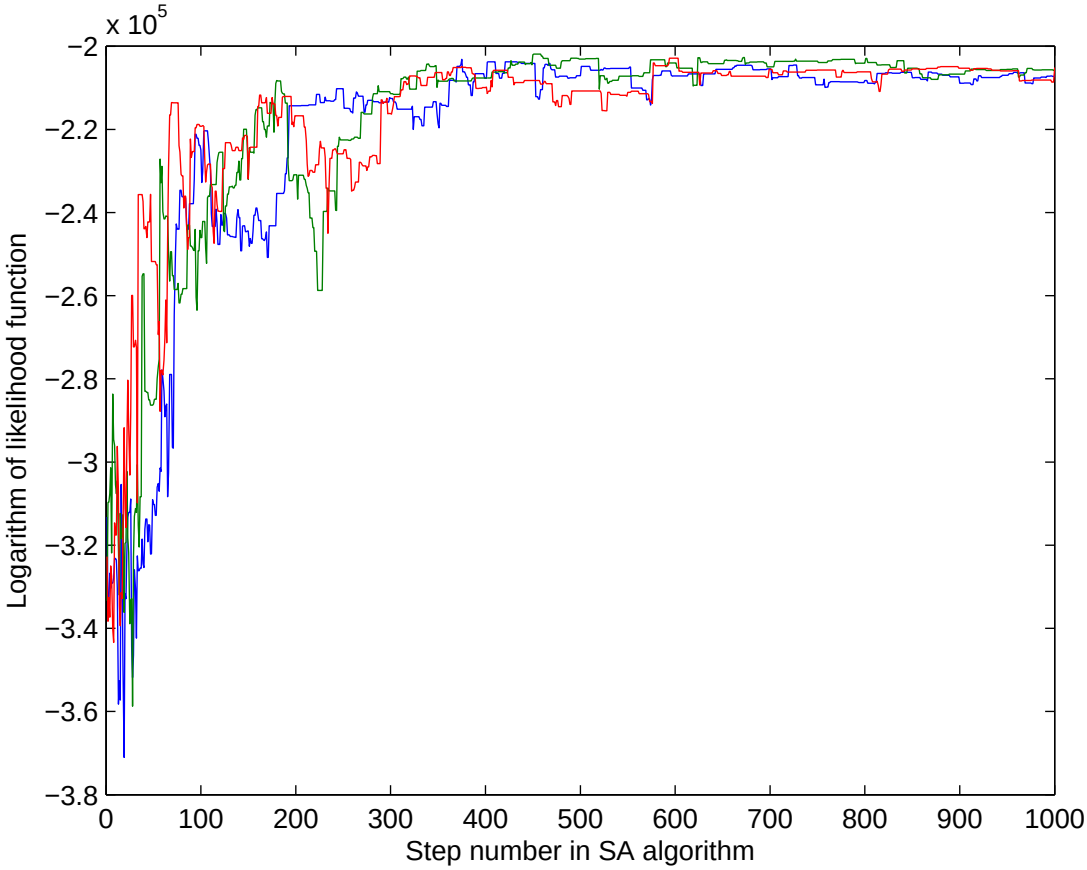


Figure A.1: Three independent runs of the same simulated annealing algorithm for the data of experiment 1. Although all parameters are identical in each case, the output is slightly different in each case due to the stochastic nature of the algorithm.

$k > l \rightarrow H_{kl} = -i|k\rangle\langle l| + i|l\rangle\langle k|$ and finally if $k = l \rightarrow H_{kl} = |k\rangle\langle k| - |k+1\rangle\langle k+1|$ (set $k+1 = 1$ if $k = d$).

4. Pick a distance δ by sampling from a Gaussian distribution with mean 0 and standard deviation Δ.

5. Compute the state $|\psi'\rangle = \exp(iH_{kl}\delta)|\psi\rangle$. Trace out one of the subsystems of $|\psi'\rangle$ to obtain the state σ_0'.

6. If $\sigma_0' \notin \overline{\Gamma_W}$, repeat steps 2 to 5, continue otherwise.

7. Evaluate the ratio $R = \log\left(\mathcal{L}(\sigma_0')/\mathcal{L}(\sigma_0)\right)$. If $R > 0$ $(\mathcal{L}(\sigma_0') > \mathcal{L}(\sigma_0))$, let $\sigma_1 = \sigma_0'$. Otherwise, flip a coin with bias $p = \exp\{-|\log(\mathcal{L}(\sigma_0)) - \log(\mathcal{L}(\sigma_0'))|/T\}$. If "1" is obtained (which happens with probability p), again let $\sigma_1 = \sigma_0'$, otherwise $\sigma_1 = \sigma_0$.

8. Repeat steps 2-6 N times to generate a set $\{\sigma_1, \sigma_2, \ldots, \sigma_N\}$ corresponding to N steps of the random walk. For each step, adapt the temperature via the cooling rule $T(s) = T_0/s$ where s is the step of the walk. The maximum value of $\mathcal{L}(\sigma)$ over this set is the output of the algorithm.

The performance of the algorithm depends strongly on the value of Δ and this value must be adapted throughout each step of the walk in order to maintain a fixed average acceptance ratio, i.e. the fraction of times we jump to a new state. Various values for these ratios are suggested [33]. Similarly, the choice of initial temperature is crucial. Its role is to prevent the algorithm from being stuck in local maxima by allowing it to escape such cases in the initial stages of the algorithm. The temperature is then reduced to ensure that convergence to the maximum is attained. Therefore, the choice of initial temperature and cooling rule is essential and varies for different cases. In practice, they must be chosen for each particular problem based mostly on experience.

Finally, in order to check whether a new state belongs in $\overline{\Gamma_W}$, it is necessary to determine the maximum fidelity of this state with any state in this set. For this purpose, we exploit the fact that the fidelity function is concave in both its arguments and that the restriction $\rho \in \overline{\Gamma_W^\delta}$ is convex for both linear and nonlinear witnesses. These properties allow us to employ the highly efficient tools of convex optimization to solve the maximization problem. Concretely, for a given state σ, we verify membership in $\overline{\Gamma_W}$ by solving the problem

$$\begin{aligned} &\text{maximize} && F(\sigma, \sigma') \\ &\text{subject to} && \sigma' \in \overline{\Gamma_W^\delta} \end{aligned}$$

where σ' must be forced to be a density operator. The state σ is a member of $\overline{\Gamma_W}$ if the solution to this problem is larger than $\sqrt{1-\delta^2}$. In our case, the CVX package for specifying and solving convex programs [44] was used to numerically solve the problem.

Appendix B

Quantum Fingerprinting – Additional Information

B.1 Error probability of the error-correcting code

Let G be a random $n \times m$ Toeplitz matrix over $\mathbb{F}_2$. There are two failure events associated with G: the minimum distance δ being not as large as promised (which results in less-than-expected worst case performance) and the matrix G being not full rank (which can cause two different inputs to be mapped to the same output, leading to a minimum distance of $\delta = 0$). We will show that, for any fixed rate R less than $1 - H_2(\delta)$, the probabilities of both failure events decreases exponentially with the output size m and can thus be neglected for sufficiently large m.

Theorem 35. *[64] Let $G \in \mathbb{F}_2^{n \times m}$ be a Toeplitz matrix chosen uniformly at random. Let $\delta_{\min}(G)$ be the minimum distance of the linear code with G as generator matrix. Then, for any $\delta \in (0, 1/2)$,*

$$\Pr(\delta_{\min}(G) \leq \delta) \leq 2^{-m(1-H_2(\delta)-R)}.$$

In particular, if $R = 1 - H_2(\delta) - \epsilon$, for some $\epsilon > 0$, then

$$\Pr(\delta_{\min}(G) \leq \delta) \leq 2^{-\epsilon m}.$$

The above theorem guarantees that, if we sacrifice an arbitrarily small quantity ϵ of the rate with respect to the Gilbert-Varshamov bound (i.e., we set $R = 1 - H_2(\delta) - \epsilon$),

the probability of obtaining an incorrect minimum distance decreases exponentially with the output size. For example, for a value of $m = 10^7$ and $\epsilon = 10^{-3}$, this probability is less than 10^{-10^4}.

Theorem 36. *Let $G \in \mathbb{F}_2^{n\times m}$ be a Toeplitz matrix chosen uniformly at random. Then,*

$$\Pr(G \textit{ is not full rank}) = 2^{-1}2^{-m(1-R)}.$$

Theorem 36 is an immediate consequence of Theorem 1 in [45]. Once again, this probability decreases exponentially with the output size m.

B.2 Detailed experimental results

In Table B.1, we report the complete results of our experiment. The dominating source of uncertainty is the uncertainty in the total mean photon number of the signals. This uncertainty is due to the summation of the fluctuations of several devices, such as laser power, VOA, and varying loss in the channel. For each input size n, we perform a calibration process to determine μ. In this process, with a proper value of VOA selected from our numerical optimization, the referee sends out around $10^7 \sim 10^8$ pulses to Alice and Bob. From the total detection counts on D_0 and D_1 and the pre-calibrated losses (Table 7.2), we estimate the μ. We repeat this calibration process a few rounds and obtain the mean value and the standard deviation for μ. These results are shown in the second column of Table B.1. For all tested cases, the uncertainty in mean photon number was below 4%.

From our model of the protocol, we use the uncertainty in the mean photon number to directly calculate an uncertainty for the quantum transmitted information as well as for the error probability of the protocol. As it can be seen from Table B.1, all error probabilities are compatible with the system operating below the target value of $\epsilon = 5\times 10^{-5}$. Additionally, we have included the average values observed for the number of clicks in detector D_1 for equal and different inputs, as well as the threshold values used by the referee.

Finally, we estimate the effect of detector dead times in our experiment as follows. For each input size, we can calculate the probability p that an individual pulse leads to a click in detector D_1. In our setup, after a click occurs, the following 50 pulses are blocked by the detector and cannot be registered. The probability p' that a click occurs for these 50 pulses is given by $p' = 1 - (1-p)^{50} \approx 50p$. This number is very small whenever p is small, as is the case in our experiment. For instance, for an input size of $n = 1.42 \times 10^8$,

the expected number of blocked clicks is approximately 0.1% of the total expected clicks. Therefore, this effect is negligible compared to fluctuations in the mean photon number, which is of the order of 4%.

n	1.53×10^6	1.20×10^7	2.27×10^7	1.42×10^8
μ_A	1914±68	3295±118	3670±131	7120±254
$D_{1,E}$	22	277	830	1939
$D_{1,D}$	131	318	954	2224
$D_{1,th}$	49	302	902	2110
Q	47689±1703	93152±3326	108129±3860	229713±8201
γ	0.83±0.02	1.19±0.05	1.41±0.05	1.66±0.06
ϵ	$(1.6 \pm 0.9) \times 10^{-9}$	$(2.3 \pm 1.4) \times 10^{-7}$	$(6.6 \pm 3.7) \times 10^{-6}$	$(2.9 \pm 1.3) \times 10^{-5}$

Table B.1: Detailed experimental results. The parameter μ_A is the mean photon number used by Alice. For the clicks in detector D_1 we report the observed averages for the case of equal inputs $D_{1,E}$, different inputs $D_{1,D}$ and the threshold value used by the referee $D_{1,th}$. As before, Q is the upper bound on the quantum transmitted information, γ is the quantum advantage and ϵ the error probability of the protocol.

References

[1] IDQuantique, Geneva, http://www.idquantique.com.

[2] Tameem Albash, Itay Hen, Federico M Spedalieri, and Daniel A Lidar. Reexamination of the evidence for entanglement in the d-wave processor. *arXiv preprint arXiv:1506.03539*, 2015.

[3] Luigi Amico, Rosario Fazio, Andreas Osterloh, and Vlatko Vedral. Entanglement in many-body systems. *Reviews of Modern Physics*, 80(2):517, 2008.

[4] Ryan Amiri, Petros Wallden, Adrian Kent, and Erika Andersson. Secure quantum signatures using insecure quantum channels. In preparation.

[5] Erika Andersson, Marcos Curty, and Igor Jex. Experimentally realizable quantum comparison of coherent states and its applications. *Phys. Rev. A*, 74:022304, Aug 2006.

[6] Juan Miguel Arrazola, Oleg Gittsovich, John Matthew Donohue, Jonathan Lavoie, Kevin J. Resch, and Norbert Lütkenhaus. Reliable entanglement verification. *Phys. Rev. A*, 87:062331, Jun 2013.

[7] Juan Miguel Arrazola, Oleg Gittsovich, and Norbert Lütkenhaus. Accessible nonlinear entanglement witnesses. *Phys. Rev. A*, 85:062327, Jun 2012.

[8] Juan Miguel Arrazola and Norbert Lütkenhaus. Quantum communication complexity with coherent states and linear optics. In *9th Conference on the Theory of Quantum Computation, Communication and Cryptography*, page 36, 2014.

[9] Juan Miguel Arrazola and Norbert Lütkenhaus. Quantum communication with coherent states and linear optics. *Phys. Rev. A*, 90(4):042335, 2014.

[10] Juan Miguel Arrazola and Norbert Lütkenhaus. Quantum fingerprinting with coherent states and a constant mean number of photons. *Phys. Rev. A*, 89:062305, Jun 2014.

[11] Juan Miguel Arrazola, Petros Wallden, and Erika Andersson. Multiparty quantum signature schemes. *arXiv preprint arXiv:1505.07509*, 2015.

[12] László Babai and Peter G Kimmel. Randomized simultaneous messages: Solution of a problem of yao in communication complexity. In *Proceedings of the 12th Annual IEEE Conference on Computational Complexity*, pages 239–246. IEEE, IEE, Los Alamitos, California, 1997.

[13] Ziv Bar-Yossef, T. S. Jayram, and Iordanis Kerenidis. Exponential separation of quantum and classical one-way communication complexity. In *Proceedings of the Thirty-Sixth Annual ACM Symposium on Theory of Computing*, pages 128–137, 2004.

[14] Andrew D Barbour, Lars Holst, and Svante Janson. *Poisson approximation*. Clarendon press Oxford, 1992.

[15] Alexander Barg and GD Forney. Random codes: Minimum distances and error exponents. *IEEE Transactions on Information Theory*, 48(9):2568–2573, 2002.

[16] FE Becerra, J Fan, G Baumgartner, J Goldhar, JT Kosloski, and A Migdall. Experimental demonstration of a receiver beating the standard quantum limit for multiple nonorthogonal state discrimination. *Nature Photonics*, 7(2):147–152, 2013.

[17] Bengtsson and Życzkowski. *Geometry of Quantum States*. Cambridge University Press, 2006.

[18] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India*, pages 175–179, New York, Dec 1984. IEEE.

[19] C. H. Bennett, G. Brassard, C. Jozsa, R. Crépeau, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dualclassical and einstein- podolsky-rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, 1993.

[20] Guido Berlín, Gilles Brassard, Félix Bussiéres, Nicolas Godbout, Joshua A Slater, and Wolfgang Tittel. Experimental loss-tolerant quantum coin flipping. *Nature communications*, 2:561, 2011.

[21] Robin Blume-Kohout. Optimal, reliable estimation of quantum states. *New J. Phys.*, 12:043034, 2010.

[22] Robin Blume-Kohout. Robust error bars for quantum state tomography. e-print arXiv:1202.5270, 2012.

[23] Robin Blume-Kohout, Jun O. S. Yin, and S. J. van Enk. Entanglement verification with finite data. *Phys. Rev. Lett.*, 105:170501, Oct 2010.

[24] Ernest F Brickell and Doug R Stinson. Authentication codes with multiple arbiters. In *Advances in Cryptology*, pages 51–55. Springer, 1988.

[25] Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi. Universal blind quantum computation. In *FOCS'09. 50th Annual IEEE Symposium on Foundations of Computer Science, 2009.*, pages 517–526. IEEE, 2009.

[26] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. *Reviews of Modern Physics*, 86(2):419, 2014.

[27] Harry Buhrman, Richard Cleve, Serge Massar, and Ronald de Wolf. Nonlocality and communication complexity. *Rev. Mod. Phys.*, 82:665–698, Mar 2010.

[28] Harry Buhrman, Richard Cleve, John Watrous, and Ronald de Wolf. Quantum fingerprinting. *Phys. Rev. Lett.*, 87:167902, Sep 2001.

[29] Jacques Carolan, Chris Harrold, Chris Sparrow, Enrique Martín-López, Nicholas J Russell, Joshua W Silverstone, Peter J Shadbolt, Nobuyuki Matsuda, Manabu Oguma, Mikitaka Itoh, et al. Universal linear optics. *arXiv preprint arXiv:1505.01182*, 2015.

[30] J. L. Carter and M. N. Wegman. Universal classes of hash functions. *J. Comp. Syst. Sci.*, 18:143–154, 1979.

[31] Amit Chakrabarti, Yaoyun Shi, Anthony Wirth, and Andrew Yao. Informational complexity and the direct sum problem for simultaneous message complexity. In *Foundations of Computer Science, 2001. Proceedings. 42nd IEEE Symposium on*, pages 270–278. IEEE, 2001.

[32] David Chaum and Sandra Roijakkers. Unconditionally-secure digital signatures. *Advances in Cryptology*, pages 206–214, 1991.

[33] S. Chib and E. Greenberg. *The American Statistician*, 49:327, 1995.

[34] Andrew M Childs and Wim Van Dam. Quantum algorithms for algebraic problems. *Reviews of Modern Physics*, 82(1):1, 2010.

[35] Giulio Chiribella. On quantum estimation, quantum cloning and finite quantum de finetti theorems. *Theory of Quantum Computation, Communication, and Cryptography Lecture Notes in Computer Science*, 6519:9–25, 2011.

[36] Matthias Christandl. Private communication, 2012.

[37] Matthias Christandl and Renato Renner. Reliable quantum state tomography. *Phys. Rev. Lett.*, 109:120403, Sep 2012.

[38] Patrick J Clarke, Robert J Collins, Vedran Dunjko, Erika Andersson, John Jeffers, and Gerald S Buller. Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light. *Nature communications*, 3:1174, 2012.

[39] R. Cleve, D. Gottesman, and H.-K. Lo. How to share a quantum secret. *Phys. Rev. Lett.*, 83(3):648–651, 1999.

[40] Richard Cleve and Harry Buhrman. Substituting quantum entanglement for communication. *Physical Review A*, 56(2):1201, 1997.

[41] Robert J Collins, Ross J Donaldson, Vedran Dunjko, Petros Wallden, Patrick J Clarke, Erika Andersson, John Jeffers, and Gerald S Buller. Realization of quantum digital signatures without the requirement of quantum memory. *Phys. Rev. Lett.*, 113(4):040502, 2014.

[42] M. Curty, O. Gühne, M. Lewenstein, and N. Lütkenhaus. Detecting two-party quantum correlations in quantum key distribution protocols. *Phys. Rev. A*, 71:022306, 2005.

[43] M. Curty, M. Lewenstein, and N. Lütkenhaus. Entanglement as precondition for secure quantum key distribution. *Phys. Rev. Lett.*, 92:217903, 2004.

[44] Inc. CVX Research. CVX: Matlab software for disciplined convex programming, version 2.0. http://cvxr.com/cvx, August 2012.

[45] D Daykin. Distribution of bordered persymmetric matrices in a finite field. *J. Reine Angew. Math.(Crelles J.)*, 203:47–54, 1960.

[46] J. Niel de Beaudrap. One-qubit fingerprinting schemes. *Phys. Rev. A*, 69:022307, Feb 2004.

[47] Zdravko I. Botev Dirk P. Kroese, Thomas Taimre. *Handbook of Monte Carlo Methods*. John Wiley & Sons, 2011.

[48] AR Dixon, ZL Yuan, JF Dynes, AW Sharpe, and AJ Shields. Gigahertz decoy quantum key distribution with 1 mbit/s secure key rate. *Optics express*, 16(23):18790–18979, 2008.

[49] Jiangfeng Du, Ping Zou, Xinhua Peng, Daniel KL Oi, LC Kwek, CH Oh, and Artur Ekert. Experimental quantum multimeter and one-qubit fingerprinting. *Phys. Rev. A*, 74(4):042319, 2006.

[50] Vedran Dunjko, Petros Wallden, and Erika Andersson. Quantum digital signatures without quantum memory. *Phys. Rev. Lett.*, 112(4):040502, 2014.

[51] W.T. Eadie, D. Drijard, F.E. James, M. Roos, and B. Sadoulet. *Statistical Methods in Experimental Physics*. North-Holland Publishing Co., 1971.

[52] A. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67(6):661–663, 1991.

[53] Ioannis Z Emiris and Victor Y Pan. Applications of fft and structured matrices. In *Algorithms and theory of computation handbook*, pages 18–18. Chapman & Hall/CRC, 2010.

[54] Massimo Franceschetti, Olivier Dousse, David Tse, and Patrick Thiran. Closing the gap in the capacity of wireless networks via percolation theory. *Information Theory, IEEE Transactions on*, 53(3):1009–1018, 2007.

[55] Matteo Frigo and Steven G Johnson. The design and implementation of fftw3. *Proceedings of the IEEE*, 93(2):216–231, 2005.

[56] C.A. Fuchs and J. Van De Graaf. Cryptographic distinguishability measures for quantum-mechanical states. *Information Theory, IEEE Transactions on*, 45(4):1216–1227, 1999.

[57] Juan Carlos Garcia-Escartin and Pedro Chamorro-Posada. Swap test and hong-ou-mandel effect are equivalent. *Phys. Rev. A*, 87(5):052330, 2013.

[58] Dmitry Gavinsky and Tsuyoshi Ito. Quantum fingerprints that keep secrets. *Quantum Information & Computation*, 13(7-8):583–606, 2013.

[59] Christopher Gerry and Peter Knight. *Introductory quantum optics*. Cambridge university press, 2005.

[60] Edgar N Gilbert. A comparison of signalling alphabets. *Bell System Technical Journal*, 31(3):504–522, 1952.

[61] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Advances in quantum metrology. *Nature Photonics*, 5(4):222–229, 2011.

[62] Daniel Gottesman and Isaac Chuang. Quantum digital signatures. *arXiv preprint quant-ph/0105032*, 2001.

[63] O. Gühne and G. Tóth. Entanglement detection. *Physics Reports*, 474:1, 2009.

[64] Venkatesan Guruswami, Atri Rudra, and Madhu Sudan. *Essential Coding Theory*. University of Buffalo, 2014.

[65] L. Gurvits. Annual acm symposium on theory of computing. In *Proceedings of the thirty-fifth ACM Symposium on thory of computing, San Diego, CA*, page 10, San Diego, CA, USA, 2003.

[66] Goichiro Hanaoka, Junji Shikata, Yuliang Zheng, and Hideki Imai. Unconditionally secure digital signature schemes admitting transferability. In *Advances in Cryptology*, pages 130–142. Springer, 2000.

[67] Goichiro Hanaoka, Junji Shikata, Yuliang Zheng, and Hideki Imai. Efficient and unconditionally secure digital signatures and a security analysis of a multireceiver authentication code. In *Public Key Cryptography*, pages 64–79. Springer, 2002.

[68] C. W. Helstrom. *Quantum detection and estimation theory*. Academic Press, New York, 1976.

[69] Alexander Semenovich Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problemy Peredachi Informatsii*, 9(3):3–11, 1973.

[70] CK Hong, ZY Ou, and Leonard Mandel. Measurement of subpicosecond time intervals between two photons by interference. *Phys. Rev. Lett.*, 59(18):2044, 1987.

[71] Rolf T. Horn, S. A. Babichev, Karl-Peter Marzlin, A. I. Lvovsky, and Barry C. Sanders. Single-qubit optical quantum fingerprinting. *Phys. Rev. Lett.*, 95:150502, Oct 2005.

[72] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of mixed states: necessary and sufficient conditions. *Phys. Lett. A*, 223:1–8, 1996.

[73] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Rev. Mod. Phys.*, 81:865–942, Jun 2009.

[74] Thomas Johansson. On the construction of perfect authentication codes that permit arbitration. In *Advances in Cryptology*, pages 343–354. Springer, 1994.

[75] Thomas Johansson. Further results on asymmetric authentication schemes. *Information and Computation*, 151(1):100–133, 1999.

[76] H Jeff Kimble. The quantum internet. *Nature*, 453(7198):1023–1030, 2008.

[77] E. Kushilevitz and N. Nisan. *Communication Complexity*. Cambridge University Press, 2006.

[78] Paul G. Kwiat, Edo Waks, Andrew G. White, Ian Appelbaum, and Philippe H. Eberhard. Ultrabright source of polarization-entangled photons. *Phys. Rev. A*, 60:R773–R776, Aug 1999.

[79] BP Lanyon, M Barbieri, MP Almeida, and AG White. Experimental quantum computing without entanglement. *Physical review letters*, 101(20):200501, 2008.

[80] Jonathan Lavoie, Rainer Kaltenbaek, Marco Piani, and Kevin J. Resch. Experimental bound entanglement in a Four-Photon state. *Phys. Rev. Lett.*, 105(13):130501, 2010.

[81] Daniel A Lidar and Todd A Brun. *Quantum error correction*. Cambridge University Press, 2013.

[82] Adriana E Lita, Aaron J Miller, and Sae Woo Nam. Counting near-infrared single-photons with 95% efficiency. *Optics express*, 16(5):3032–3040, 2008.

[83] Yang Liu, Yuan Cao, Marcos Curty, Sheng-Kai Liao, Jian Wang, Ke Cui, Yu-Huai Li, Ze-Hong Lin, Qi-Chao Sun, Dong-Dong Li, et al. Experimental unconditionally secure bit commitment. *Phys. Rev. Lett.*, 112(1):010504, 2014.

[84] Yang Liu, Teng-Yun Chen, Liu-Jun Wang, Hao Liang, Guo-Liang Shentu, Jian Wang, Ke Cui, Hua-Lei Yin, Nai-Le Liu, Li Li, et al. Experimental measurement-device-independent quantum key distribution. *Phys. Rev. Lett.*, 111(13):130502, 2013.

[85] Xin Lu and Dengguo Feng. Quantum digital signature based on quantum one-way functions. In *Advanced Communication Technology, 2005, ICACT 2005. The 7th International Conference on*, volume 1, pages 514–517. IEEE, 2005.

[86] Tommaso Lunghi, J Kaniewski, Félix Bussières, Raphaël Houlmann, M Tomamichel, A Kent, Nicolas Gisin, S Wehner, and Hugo Zbinden. Experimental bit commitment based on quantum communication and special relativity. *Phys. Rev. Lett.*, 111(18):180504, 2013.

[87] Norbert Lütkenhaus. Quantum key distribution. In *Quantum Information and Coherence*, pages 107–146. Springer, 2014.

[88] F Marsili, VB Verma, JA Stern, S Harrington, AE Lita, T Gerrits, I Vayshenker, B Baek, MD Shaw, RP Mirin, et al. Detecting single infrared photons with 93% system efficiency. *Nature Photonics*, 7(3):210–214, 2013.

[89] Serge Massar. Quantum fingerprinting with a single particle. *Phys. Rev. A*, 71(1):012310, 2005.

[90] Ueli M Maurer. Secret key agreement by public discussion from common information. *Information Theory, IEEE Transactions on*, 39(3):733–742, 1993.

[91] Caterina E. Mora and Hans J. Briegel. Algorithmic complexity and entanglement of quantum states. *Phys. Rev. Lett.*, 95:200503, Nov 2005.

[92] Caterina E. Mora, Hans J. Briegel, and Barbara Kraus. Quantum kolmogorov complexity and its applications. *International Journal of Quantum Information*, 05(05):729–750, 2007.

[93] Tobias Moroder, Otfried Gühne, and Norbert Lütkenhaus. Iterations of nonlinear entanglement witnesses. *Phys. Rev. A*, 78(3):032326, 2008.

[94] Jörn Müller-Quade. Quantum pseudosignatures. *Journal of Modern Optics*, 49(8):1269–1276, 2002.

[95] Ilan Newman and Mario Szegedy. Public vs. private coin flips in one round communication games. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 561–570, 1996.

[96] Nelly Huei Ying Ng, Siddarth K Joshi, Chia Chen Ming, Christian Kurtsiefer, and Stephanie Wehner. Experimental implementation of bit commitment in the noisy-storage model. *Nature communications*, 3:1326, 2012.

[97] M. A. Nielsen and I. L Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[98] Anna Pappa, Paul Jouguet, Thomas Lawson, André Chailloux, Matthieu Legré, Patrick Trinkler, Iordanis Kerenidis, and Eleni Diamanti. Experimental plug and play quantum coin flipping. *Nature communications*, 5:3717, 2014.

[99] Matteo Paris and Jaroslav Rehacek. *Quantum state estimation*, volume 649. Springer Science & Business Media, 2004.

[100] A. Peres. Separability criterion for density matrices. *Phys. Rev. Lett.*, 77:1413, 1996.

[101] R. Raussendorf and H. J. Briegel. A one-way quantum computer. *Phys. Rev. Lett.*, 86:5188, 2001.

[102] Ran Raz. Exponential separation of quantum and classical communication complexity. In *Proceedings of the Thirty-First Annual ACM Symposium on Theory of Computing*, pages 358–367, 1999.

[103] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani. Experimental realization of any discrete unitary operator. *Phys. Rev. Lett.*, 73:58–61, 1994.

[104] Allison Rubenok, Joshua A Slater, Philip Chan, Itzel Lucio-Martinez, and Wolfgang Tittel. Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks. *Phys. Rev. Lett.*, 111(13):130501, 2013.

[105] Reihaneh Safavi-Naini, Luke McAven, and Moti Yung. General group authentication codes and their relation to unconditionally-secure signatures. In *Public Key Cryptography*, pages 231–247. Springer, 2004.

[106] Nicolas Sangouard, Christoph Simon, Hugues De Riedmatten, and Nicolas Gisin. Quantum repeaters based on atomic ensembles and linear optics. *Reviews of Modern Physics*, 83(1):33, 2011.

[107] M Sasaki, M Fujiwara, H Ishizuka, W Klaus, K Wakui, M Takeoka, S Miki, T Yamashita, Z Wang, A Tanaka, et al. Field test of quantum key distribution in the tokyo qkd network. *Optics Express*, 19(11):10387–10409, 2011.

[108] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81(3):1301, 2009.

[109] Yi-Lin Seah, Jiangwei Shang, Hui Khoon Ng, David John Nott, and Berthold-Georg Englert. Monte carlo integration over regions in the quantum state space. ii. *arXiv preprint arXiv:1407.7806*, 2014.

[110] Jiangwei Shang, Yi-Lin Seah, Hui Khoon Ng, David John Nott, and Berthold-Georg Englert. Monte carlo integration over regions in the quantum state space. i. *arXiv preprint arXiv:1407.7805*, 2014.

[111] Claude E Shannon. Communication theory of secrecy systems*. *Bell system technical journal*, 28(4):656–715, 1949.

[112] R. Sheldon. *A First Course In Probability, 6/E*. Pearson Education, 2002.

[113] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM journal on computing*, 26(5):1484–1509, 1997.

[114] Gustavus J Simmons. Message authentication with arbitration of transmitter/receiver disputes. In *Advances in Cryptology*, pages 151–165. Springer, 1988.

[115] Gustavus J Simmons. A cartesian product construction for unconditionally secure authentication codes that permit arbitration. *Journal of Cryptology*, 2(2):77–104, 1990.

[116] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden. Quantum key distribution over 67 km with a plug&play system. *New J. Phys.*, 4:41, 2002.

[117] Damien Stucki, Nino Walenta, Fabien Vannel, Robert Thomas Thew, Nicolas Gisin, Hugo Zbinden, S Gray, CR Towery, and S Ten. High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres. *New J. Phys.*, 11(7):075003, 2009.

[118] Colleen M Swanson and Douglas R Stinson. Unconditionally secure signature schemes revisited. *Information Theoretic Security*, pages 100–116, 2011.

[119] Zhiyuan Tang, Zhongfa Liao, Feihu Xu, Bing Qi, Li Qian, and Hoi-Kwong Lo. Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. *Phys. Rev. Lett.*, 112(19):190503, 2014.

[120] Sébastien Tanzilli, Anthony Martin, Florian Kaiser, Marc P De Micheli, Olivier Alibart, and Daniel B Ostrowsky. On the genesis and evolution of integrated quantum optics. *Laser & Photonics Reviews*, 6(1):115–143, 2012.

[121] Marco Tomamichel, Charles Ci Wen Lim, Nicolas Gisin, and Renato Renner. Tight finite-key analysis for quantum cryptography. *Nature communications*, 3:634, 2012.

[122] Pavel Trojek, Christian Schmid, Mohamed Bourennane, Caslav Brukner, Marek Zukowski, and Harald Weinfurter. Experimental quantum communication complexity. *Phys. Rev. A*, 72:050305, Nov 2005.

[123] S. J. van Enk, N Lütkenhaus, and H. J. Kimble. On experimental procedures for entanglement verification. *Phys. Rev. A*, 75:052318, 2007.

[124] RR Varshamov. Estimate of the number of signals in error correcting codes. In *Dokl. Akad. Nauk SSSR*, volume 117, pages 739–741, 1957.

[125] Guifré Vidal. Efficient classical simulation of slightly entangled quantum computations. *Phys. Rev. Lett.*, 91:147902, Oct 2003.

[126] Petros Wallden, Vedran Dunjko, Adrian Kent, and Erika Andersson. Quantum digital signatures with quantum-key-distribution components. *Phys. Rev. A*, 91:042304, Apr 2015.

[127] Stephanie Wehner. Cryptography in a quantum world. *arXiv preprint arXiv:0806.3483*, 2008.

[128] Stephanie Wehner and Andreas Winter. Entropic uncertainty relationsa survey. *New Journal of Physics*, 12(2):025009, 2010.

[129] S. Wiesner. Conjugate coding. *Sigact News*, 15:78, 1983.

[130] Mark M Wilde. *Quantum information theory*. Cambridge University Press, 2013.

[131] W.K. Wootters and W.H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802, 1982.

[132] Guo-Yong Xiang, Brendon Lloyd Higgins, DW Berry, Howard Mark Wiseman, and GJ Pryde. Entanglement-enhanced measurement of a completely unknown optical phase. *Nature Photonics*, 5(1):43–47, 2011.

[133] Feihu Xu, Juan Miguel Arrazola, Kejin Wei, Wenyuan Wang, Pablo Palacios-Avila, Chen Feng, Shihan Sajeed, Hoi-Kwong Lo, et al. Experimental quantum fingerprinting. *arXiv preprint arXiv:1503.05499*, 2015.

[134] Feihu Xu, Bing Qi, Xiongfeng Ma, He Xu, Haoxuan Zheng, and Hoi-Kwong Lo. Ultrafast quantum random number generation based on quantum phase fluctuations. *Optics express*, 20(11):12366–12377, 2012.

[135] Andrew Chi-Chih Yao. Some complexity questions related to distributive computing (preliminary report). In *Proceedings of the 11th Annual ACM Symposium on Theory of Computing*, pages 209–213, 1979.

[136] Andrew Chi-Chih Yao. Protocols for secure computations. In *FOCS*, volume 82, pages 160–164, 1982.

[137] Jun Zhang, Xiao-Hui Bao, Teng-Yun Chen, Tao Yang, Adán Cabello, and Jian-Wei Pan. Experimental quantum "guess my number" protocol using multiphoton entanglement. *Phys. Rev. A*, 75:022302, Feb 2007.

[138] M. Zukowski, A. Zeilinger, M.A. Horne, and A.K. Ekert. "event-ready-detectors" bell experiment via entanglement swapping. *Phys. Rev. Lett.*, 71:4287–4290, 1993.

[139] Karol Zyczkowski, Paweł Horodecki, Anna Sanpera, and Maciej Lewenstein. Volume of the set of separable states. *Phys. Rev. A*, 58:883–892, Aug 1998.

[140] Karol Zyczkowski and Hans-Jürgen Sommers. Induced measures in the space of mixed quantum states. *J. Phys. A: Math. Gen.*, 34:7111, 2001.