Optical Quantum Communication
&
Cryptography with Temporarily Trusted Parties

by

Ashutosh Satyajit Marwah

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Science (MSc)
in
Physics (Quantum Information)

Waterloo, Ontario, Canada, 2019

Author's Declaration

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.

Statement of Contributions

Chapter 3 consists of the work published in the paper, ’Characterization of Gram matrices of multimode coherent states’ [1] and its erratum [2]. The work presented in this chapter was performed by the author and Norbert Lütkenhaus.

The work presented in Chapter 4 was performed by the author and Norbert Lütkenhaus. The work described in Section 4.2.2 was based on code provided by Juan Miguel Arrazola. Dave Touchette helped in proving the results in Section 4.3.2.

Chapter 5 consists of the work performed together by the author, Dave Touchette and Norbert Lütkenhaus. This work is supposed to appear in a publication soon. The contents of this chapter, which are almost the same as the contents of the paper, are co-written by the author and Dave Touchette.

Abstract

The work in this thesis can be divided into three parts. The first two parts deal with optical quantum communication protocols and the third part deals with quantum cryptography. The first part of the thesis is a step towards reformulating quantum protocols in terms of coherent states. Quantum communication protocols are typically formulated in terms of abstract qudit states and operations. This leaves the question of an experimental realization open. Direct translation of these protocols, say into single photons with some d-dimensional degree of freedom, are typically challenging to realize. Multi-mode coherent states, on the other hand, can be easily generated experimentally. Reformulation of protocols in terms of these states has been a successful strategy for implementation of quantum protocols. Quantum key distribution and the quantum fingerprinting protocol have both followed this route. In Chapter 3, we characterize the Gram matrices of multi-mode coherent states in an attempt to understand the class of communication protocols, which can be implemented using these states. We also derive the closure of the Gram matrices, which can be implemented in this way, so that we also characterize those matrices, which can be approximated arbitrarily well using multi-mode coherent states.

In the second part of the thesis, Chapter 4, we describe our collaboration with an experimental group to implement the quantum fingerprinting protocol and examine the tradeoffs between the resources required to implement such protocols. It is seen that it is difficult to implement the quantum fingerprinting protocol experimentally for large input sizes. This leads us to study the tradeoff between the two resources expended during optically implemented simultaneous message passing communication protocols: the duration of the protocol and the energy required to run it. We derive general bounds on the growth of these quantities which are valid for all optical protocols. We also develop tighter bounds for the growth of these resources for protocols implementing quantum fingerprinting with coherent states.

Finally in Chapter 5, we venture into quantum cryptography. We introduce a new setting for two-party cryptography with temporarily trusted third parties. In this setting, in addition to Alice and Bob, there are third parties, which Alice and Bob both trust to be honest during the course of the protocol. However, once the protocol concludes, there is no guarantee over the behaviour of these third parties. It is possible that they collaborate and act adversarially against the honest parties. We implement a variant of bit commitment in this setting, which we call erasable bit commitment. In this primitive, Alice has the choice of either opening or erasing her commitment after the commit phase. The ability to ask for an erasure allows Alice to ask the trusted nodes to erase her commitment in case the trust period is about to expire. However, this ability also makes erasable bit commitment weaker than the standard version of bit commitment. In addition to satisfying the security requirements of bit commitment, our protocol also does not reveal any information about the commitment to the third parties. Lastly, our protocol for this primitive requires a constant number of trusted third parties and can tolerate a small number of dishonest trusted nodes as well as implementation errors.

Acknowledgements

First and foremost, I would like to thank my supervisor, Norbert Lütkenhaus. His door was always open to discuss research questions and even administrative issues. I could always count on him to present me with a better perspective to look at a problem. He has alway encouraged me to pursue my interests and explore different fields. His guidance has undoubtedly helped me become a better researcher. I am grateful to him for everything.

Secondly, I would like to thank Dave Touchette. I owe most of what I know about cryptography and quantum communication to him. He was always ready to discuss and help me with my projects and ideas. Needless to say, I benefitted immensely from his deep insight.

I would also like to thank John Watrous. He was only an email away when I needed suggestions. I rank his course on the 'Theory of Quantum Information' as one of the best courses I have ever taken. It also helped me discover the research direction I wished to pursue. I would also like to thank him along with Thomas Jennewein for serving on my supervisory committee. I also thank Thomas Jennewein for giving me a better perspective on optics. Further, I also thank him and Jon Yard for serving on my thesis defence committee.

I thank Alan Migdall and Joshua Bienfang for giving me the opportunity to perform simulations for their quantum fingerprinting experiment, and for explaining the various obstacles one encounters in such experimental implementations. Discussions with them motivated the resource tradeoff results in Chapter 4.

I would like to thank David Gosset, Benjamin Lovitz, and Jie Lin for interesting discussions. I would also like to thank Benjamin Lovitz for pointing an error in an early version of the proof of Theorem 3.1. I am also grateful to Matthias Kleinmann for independently pointing out an error in an earlier version of Ref. [1], which comprises Chapter 3.

I wholeheartedly thank the administrative staff of IQC and the Physics department, particularly Judy McDonnell, Michelle Roche and Maren Butcher, who shield us from all kinds of bureaucratic processes making our lives way easier and without whom IQC would be submerged under heaps of papers and dust.

Finally, I would like to thank IQC, UW and everyone who makes these institutions possible for offering a rigorous and farsighted Master's program. I also thank the Government and the people of Canada, my home for the last two years. It is indeed a cold country with warmhearted people.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

Quantum physics offers a wide range of possibilities for communication. It allows us to perform tasks which were not possible earlier using classical devices. Such a qualitative *quantum advantage* is typically seen in quantum cryptograhpic protocols like quantum key distribution [4, 5]. Quantitatively, on the other hand, quantum messages can be used to solve distributed communication problems more efficiently [6–9]. Moreover, quantum communication protocols have also proved useful to experimentally demonstrate the benefits of quantum technologies [3, 10, 11]. As quantum networks are established in the near future, it is expected that we will be able to fully exploit the power of quantum communication.

However, there are still several quantum protocols which cannot yet be implemented experimentally. One of the major reasons for this is that protocols are theoretically stated in terms of qudit states, and general unitary and measurment operations. Arbitrary qudit states can possibly have large entanglement between the particles which constitute these qudits. As a result, it is difficult to create and manipulate these states in an experiment. Recently, therefore, there has been an effort to reformulate protocols in terms of quantum states which are easy to create and manipulate. Coherent states are the simplest states of light. Unlike other states of light, no complex or expensive equipment is required to produce these states. All one needs to create these states are lasers and attenuators. Further, they are also very robust to noise. For this reason, several quantum communication protocols have been successfully implemented by reformulating them in terms of coherent states and linear optics [3, 10, 11]. Understanding when and how we can reformulate communication protocol in terms of coherent states and linear optics is, therefore, of paramount importance. In Chapter 3, we take the first step towards developing such an understanding. We work towards understanding the geometry of coherent states by characterizing the *Gram matrices* of coherent states. This allows us to understand when a set of general qudit states used in a protocol can be replaced by a set of coherent states.

While Chapter 3 focusses on trying to make abstract protocols more amenable to experimental implementation, in Chapter 4, we focus on improving the existing optical implementations of quantum communication protocols, specifically the *quantum fingerprinting protocol*. The quantum fingerprinting protocol solves an interesting problem in communication complexity with exponentially lesser communication than what is possible classically. In this problem, Alice and Bob need to send as small messages about their inputs as possible to a Referee, so that he can determine if these inputs are equal or not. We describe our collaboration with experimentalists to implement the quatum fingerprinting protocol in order to beat the classical information leakage bound. During our discussions with the experimental team, we realized that even though the protocol itself is relatively simple, implementing it experimentally for large inputs is difficult. This naturally led us to consider the tradeoffs in the growth of the resources for implementing communication protocols optically. We identify the mean number of photons and the number of modes used as the resources which determine the energy required during the protocol and the time needed to run the protocol. Tradeoff bounds on the growth of these two quantities are proven using simple techniques from communication complexity. Indeed this is yet another testimony to the power and generality of this theory. We further specialize to the case of coherent state quantum fingerprinting protocols, and prove tighter tradeoff bounds for this case. In addition, we show that the coherent state reformulation of the quantum fingerprinting protocol given by Arrazola and Lütkenhaus [12] is almost optimal.

In Chapter 5, we turn our attention to cryptography. Certain cryptographic primitives, like bit commitment, cannot be implemented even in the quantum setting without some assumption, say on the computational capabilities or the memories of the dishonest parties [13]. There are drawbacks to using functionalities built on such assumptions. The computational capabilities of adversaries are continually growing, especially with the advent of quantum technologies. Whereas implementations, based on the assumption of inherent noise in quantum memories, will take a longer and longer time to run as the quality of these memories improves. We introduce a new setting in the quantum regime: *the temporarily trusted party setting* to implement two-party protocols. In two-party cryptographic protocols, the two parties, Alice and Bob, do not trust each other. In the temporarily trusted party setting, in addition to these two parties, there are third parties, which Alice and Bob both trust to be honest during the protocol. However, once the protocol concludes, there is no guarantee over the behaviour of these parties. It is possible that they collaborate and act adversarially. Therefore, we say that these third parties are *temporarily* trusted. We develop a simple protocol for a variant of bit commitment in this setting. In addition to the regular security requirements for bit commitment, our protocol also does not reveal any information about the commitment to the third parties. The protocol is based on BB84 states, which are already easy to implement optically. We believe that these states too can be substituted with coherent states in the protocol.

Chapter 2

Background

2.1 Introduction

In this chapter, we will provide a brief introduction to the topics and results we use throughout this thesis. We assume that the reader is familiar with the basic elements of quantum information like density matrices, quantum channels, measurements, etc. This chapter does not contain any new results and is simply meant to provide the reader with sufficient background to understand the results presented in this thesis and to point them to the right references in case they wish to explore the topic further.

2.2 Basic Notation

In this thesis, vectors will be denoted by alphabets, and should be identified by their spaces. For example, $v \in \mathbb{C}^n$ denotes a vector. We will use kets to denote physical quantum states. We use the term quantum channel for a completely-positive and trace preserving (CPTP) linear map on the set of matrices. For a matrix, P, the notation $P \geq 0$ will be used to indicate that the matrix is positive semidefinite. In Table 2.1, we list the notation for frequently used sets from linear algebra. We provide additional notation in the following sections after introducing the relevant concepts.

Table 2.1: Notation for frequently used sets

$\mathrm{L}(\mathcal{X}, \mathcal{Y})$	The set of linear operators from complex Euclidean space, $\mathcal{X}$ to complex Euclidean space, $\mathcal{Y}$.
$\mathrm{L}(\mathcal{X})$	The set of linear operators from complex Euclidean space, $\mathcal{X}$ to itself.
$\mathrm{U}(\mathcal{X}, \mathcal{Y})$	The set of isometries from complex Euclidean space, $\mathcal{X}$ to complex Euclidean space, $\mathcal{Y}$.
$\mathrm{Herm}(\mathcal{X})$	The set of Hermitian operators in $\mathrm{L}(\mathcal{X})$.
$\mathrm{Pos}(\mathcal{X})$	The set of positive semidefinite operators in $\mathrm{L}(\mathcal{X})$.
$\mathrm{D}(\mathcal{X})$	The set matrices $\rho \in \mathrm{Pos}(\mathcal{X})$ with $\mathrm{Tr}(\rho) = 1$.
$[n]$	The set $\{1, 2, \cdots, n\}$.

2.3 Distance measures

2.3.1 Matrix and channel norms

We use the Schatter p-norms for matrices. For a matrix $X \in L(\mathbb{C}^n, \mathbb{C}^m)$, we define the Schatten p-norm of X to be

$$\|X\|_p := \left(\mathrm{Tr}((X^\dagger X)^{\frac{p}{2}})\right)^{\frac{1}{p}}.$$

These norms are in fact the same as the corresponding vector p-norms on the vector of singular values of X, i.e., $\|X\|_p = \|s(X)\|_p$ where $s(X)$ represents the vector of the singular values of X. In our study, we will be mostly concerned with the 1-norm and the 2-norm. These are

$$\|X\|_1 = \mathrm{Tr}((X^\dagger X)^{\frac{1}{2}}) = \sum_i s_i(X),$$

$$\|X\|_2 = (\mathrm{Tr}(X^\dagger X))^{\frac{1}{2}} = \left(\sum_{i,j} |X_{ij}|^2\right)^{\frac{1}{2}}.$$

The matrix 2-norm is convenient to use as it can be expressed in terms of the matrix elements. The 1-norm or the trace norm is particularly useful for developing security definitions for cryptographic protocols which are well motivated and composable [13–15]. In particular, the trace norm characterizes ones ability to distinguish between two quantum states according to the Holevo-Helstrom theorem.

Theorem 2.1 (Holevo-Helstrom theorem [16, Theorem 3.4])**.** *Let $\rho_1, \rho_2 \in D(\mathbb{C}^n)$ be two quantum states. Suppose ρ_1 and ρ_2 are both prepared with a probability of $1/2$. Then, the probability of successfully determining which state was prepared is at most*

$$\frac{1}{2}\left(1 + \frac{1}{2}\|\rho_1 - \rho_2\|_1\right).$$

Throughout this thesis and particularly in Chapter 5, we use the symbol $\approx$ to compare two quantum states using the trace distance. We say that $\rho_1 \approx_\epsilon \rho_2$ if $1/2\|\rho_1 - \rho_2\|_1 \leq \epsilon$.

We can use these matrix norms to define induced norms on the set of quantum channels. The induced channel norm of a channel $\Phi : L(\mathcal{X}) \to L(\mathcal{Y})$ is given by

$$\|\Phi\|_1 := \max\{\|\Phi(X)\|_1 : X \in L(\mathcal{X}) \text{ such that } \|X\|_1\}.$$

It can be seen from the definition of the induced channel norm that for a channel Φ and a matrix X, we have

$$\|\Phi(X)\|_1 \leq \|\Phi\|_1\|X\|_1.$$

This is a useful identity, especially when coupled with the following theorem.

Theorem 2.2 ([16, Corollary 3.40]). *Let $\Phi : L(\mathcal{X}) \to L(\mathcal{Y})$ be a quantum channel, that is, a completely-positive and trace-preserving map, then it holds that $\|\Phi\|_1 = 1$.*

We see that the trace norm of a quantum state cannot increase under an action by a quantum channel. This is the reason for the composability of security definitions based on the trace norm [14].

2.3.2 Fidelity

The Fidelity function is also useful for quantifying the distance between two quantum states. The fidelity of two quantum states $\rho, \sigma \in D(\mathbb{C}^n)$ is defined as

$$F(\rho, \sigma) := \|\sqrt{\rho}\sqrt{\sigma}\|_1.$$

According to Uhlmann's theorem, the fidelity between two quantum states ρ and σ can also be characterized as the maximum possible overlap of the purifications of these states.

Theorem 2.3 (Uhlmann's theorem [16, Theorem 3.22]). *Let $\rho_A, \sigma_A \in D(\mathbb{C}^n)$. Further, suppose that $|\psi_{AR}\rangle \in \mathbb{C}^n \otimes \mathbb{C}^n$ is a purification of ρ_A, i.e., $\mathrm{Tr}_R(|\psi_{AR}\rangle\langle\psi_{AR}|) = \rho_A$. Then, we have that*

$$F(\rho, \sigma) = \max\{|\langle\psi|\phi\rangle| : |\phi_{AR}\rangle \in \mathbb{C}^n \otimes \mathbb{C}^n \textit{ is a purification of } \sigma\}$$

The fidelity of two quantum states is also closely related to the trace norm between them. This relationship between these two quantities is given by the Fuchs-van de Graaf inequalities.

Theorem 2.4 (Fuchs-van de Graaf inequalities [16, Theorem 3.33])**.** *Let $\rho, \sigma \in D(\mathbb{C}^n)$ be quantum states. For these we have that*

$$1 - \frac{1}{2}\|\rho - \sigma\|_1 \leq F(\rho, \sigma) \leq \sqrt{1 - \frac{1}{4}\|\rho - \sigma\|_1^2}$$

or equivalently,

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

2.4 Quantum information theory

2.4.1 Von-Neumann entropies

Let $\mathcal{X}$ be a Hilbert space. We define the von-Neumann entropy or simply the entropy of a quantum state $\rho \in D(\mathcal{X})$ as

$$H(X)_\rho := \sum_i -\lambda(\rho)_i \log_2(\lambda(\rho)_i)$$

where $\{\lambda(\rho)_i\}_i$ are eigenvalues of the matrix ρ.

Let $\mathcal{X}$ and $\mathcal{Y}$ be two Hilbert spaces. Using the above definition, we can define the mutual information between registers X and Y for a bipartite state $\rho_{XY} \in D(\mathcal{X} \otimes \mathcal{Y})$ as

$$I(X : Y)_\rho := H(X)_\rho + H(Y)_\rho - H(XY)_\rho.$$

Mutual information $I(X : Y)$ can be thought of as a measure of the information contained in the register Y about register X. This description of mutual information is based on Shannon's Noisy Channel Coding Theorem (see for example [17]) and the Entanglement Assisted Classical Capacity Theorem (see [18, 19]).

2.4.2 Min-entropy

Min-entropy is an entropic measure, which is useful for quantifying the adversary's information especially in cryptographic settings. Von-Neumann entropy based measures usually characterize operations in the i.i.d and asymptotic limit. However, min-entropy is a *one-shot* entropy, i.e., it can be used to tightly characterize finite sized tasks without any assumption on the structure of the states. As we will see, in particular, min-entropy can be used to characterize the task of *privacy amplification* for finite sized strings. The precise definitions of min-entropy and smooth min-entropy vary across literature. In this thesis, we follow the definitions given in Ref. [13].

Definition 2.1 (Introduced in Ref. [14])**.** The *min-entropy* of a quantum state ρ_{AB} given B is defined as

$$H_{\min}(A|B)_\rho := -\log_2 \left(\inf\{\mathrm{Tr}(\sigma_B) : \sigma_B \geq 0 \text{ and } \rho_{AB} \leq \mathbb{1}_A \otimes \sigma_B\}\right).$$

Furthermore, since the min-entropy is discontinuous as a function of the state ρ_{AB}, a smoothed version of min-entropy is defined by taking a supremum over all states close to the original.

Definition 2.2 (Introduced in Ref. [14]; we follow the definition in Ref. [13])**.** The *ϵ-smooth min-entropy* of a quantum state ρ_{AB} given B is defined as

$$\begin{aligned} H^\epsilon_{\min}(A|B)_\rho := \sup\{H_{\min}(A|B)_{\bar\rho} \mid \bar\rho_{AB} \geq 0, \\ \frac{1}{2}\|\bar\rho_{AB} - \rho_{AB}\|_1 \leq \mathrm{Tr}(\rho_{AB})\epsilon \\ \text{and } \mathrm{Tr}(\rho_{\bar{AB}}) \leq \mathrm{Tr}(\rho_{AB})\} \end{aligned}$$

To understand min-entropy better, we will focus our attention to the case where an honest party holds the classical register X and the adversary holds a quantum register Q, which might be correlated with X. In other words, the state $\rho_{XQ} = \sum_x p(X = x) |x\rangle\langle x| \otimes \rho^x_Q$ is distributed between the two parties, with the honest party holding classical register X and the adversary holding Q. In such a scenario, a natural way to quantify the information held by the adversary about string X is to calculate the maximum average probability of him being able guess the string in register X. This is given by

$$P_{\text{guess}}(X|Q) := \max_{\{M_x\}_x} \left\{\sum_x p(X = x)\,\mathrm{Tr}(M_x \rho^x_Q)\right\}$$

where the maximum is taken over all sets of possible POVMs $\{M_x\}_x$. Then, it can be shown [20] that in this case the min-entropy of X given Q as

$$H_{\min}(X|Q) := -\log_2(P_{\text{guess}}(X|Q)).$$

We also point out that the smooth min-entropies satisfy the following important properties. For $\epsilon \in [0, 1)$ and quantum states ρ_{AB}, and $\sigma_{AB'} := \Phi_B(\rho_{AB})$ where Φ_B is a channel on the register B, we have

$$H^\epsilon_{\min}(A|B')_\sigma \geq H^\epsilon_{\min}(A|B)_\rho. \tag{2.1}$$

This is called the data processing inequality for min-entropy [21, Theorem 6.2]. As a special case of this inequality, observe that for $\epsilon \in [0, 1)$ and a quantum state ρ_{ABC}

$$H^\epsilon_{\min}(A|B) \geq H^\epsilon_{\min}(A|BC). \tag{2.2}$$

Further, we also have the following chain rule [21, Lemma 6.8]. For $\epsilon \in [0, 1)$ and a quantum state ρ_{ABX}, where X is a classical register, we have

$$H^\epsilon_{\min}(A|BX) \geq H^\epsilon_{\min}(A|B) - \log_2(\dim(X))$$

Lastly, smooth min-entropy is particularly interesting to study since it tightly characterizes the task of privacy amplification. If the smooth min-entropy of a string held by an honest party given the adversary's information is *large*, then the honest participant can use privacy amplification to create a smaller key which is almost decoupled from the adversary. Privacy amplification can be performed by applying a family of two-universal hash functions randomly on the string. A family of functions $\mathrm{Ext} : \{0,1\}^n \otimes \mathcal{R} \to \{0,1\}^\ell$ is said to be two-universal if for every $x \neq x'$, we have $\mathbb{P}r_r[\mathrm{Ext}(x,r) = \mathrm{Ext}(x',r)] \leq 2^{-\ell}$ where $r \in_R \mathcal{R}$ is chosen uniformly at random.

Theorem 2.5 (Privacy amplification theorem [14, 22])**.** *Let* $\mathrm{Ext} : \{0,1\}^n \otimes \mathcal{R} \to \{0,1\}^\ell$ *be a family of two-universal hash functions, and* ρ_{XQ} *a classical-quantum state. Further, suppose* $\rho_{XQR} = \rho_{XQ} \otimes \tau_R$*, where* τ_R *is the completely mixed state, i.e.,* R *is uniformly random. Then, we have that*

$$\rho_{\mathrm{Ext}(X,R)QR} \approx_{\epsilon'} \tau_{\{0,1\}^\ell} \otimes \rho_{QR}$$

where $\epsilon' = 2^{-\frac{1}{2}(H^{\epsilon}_{min}(X|Q)-\ell)-1} + 2\epsilon$

We have once again stated the theorem as it is stated in Ref. [13].

2.5 Background on quantum optics

We only require a few basic concepts from quantum optics for our purpose. We will cover all of these briefly in this section. To begin, the Hilbert space for a single optical mode, $\mathcal{H}$, is a countably infinite dimension Hilbert space. Formally, we identify this Hilbert space with ℓ_2, the set of all square summable sequences. If $\hat{n}$ is the photon number operator on this Hilbert space, then we can let $\{|k\rangle\}_{k=0}^{\infty}$ be the eigenvectors of $\hat{n}$. These form an orthonormal basis for $\mathcal{H}$, and are called the Fock basis. A concrete way to view $\mathcal{H}$ is as

$$\mathcal{H} = \left\{ \sum_{k=0}^{\infty} x_k |k\rangle : \sum_{k=0}^{\infty} |x_k|^2 < \infty \right\}.$$

The photon number operator on this space is given by

$$\hat{n} := \sum_{k=0}^{\infty} k |k\rangle \langle k| .$$

The number operator on the Hilbert space of m-modes $\mathcal{H}^{\otimes m}$ is given by $\hat{N} := \sum_{i=1}^{m} \hat{n}_i$, where $\hat{n}_i := I \otimes \cdots \otimes \hat{n} \otimes \cdots \otimes I$ (the number operator acting on the i^{th} Hilbert space). Since, $\hat{N}$ is Hermitian, it can also be associated with a measurement. Using Eigenvalue decomposition, write $\hat{N}$ as $\hat{N} = \sum_{n=0}^{\infty} n P_n$, where P_n is the projector onto the n-photon subspace, i.e.,

$$P_n = \sum_{(n_1,\cdots,n_m)\in S_n} |n_1, n_2, \cdots, n_m\rangle \langle n_1, n_2, \cdots, n_m|$$

where $S_n := \{(n_1, n_2, \cdots, n_m) : \sum_{i=1}^{m} n_i = n\}$. The measurement corresponding to $\hat{N}$ is the measurement $\{P_n\}_n$. We will also refer to the random variable corresponding to the measurement result in this basis as $\hat{N}$. Thus, the probability of measuring n-photons in the state ρ will be denoted by

$$\mathbb{P}r_\rho[\hat{N} = n] = \mathrm{Tr}(P_n \rho).$$

The mean number of photons of the state is given by

$$\mathbb{E}_\rho[\hat{N}] = \sum_{n=0}^{\infty} n \mathbb{P}r_\rho[\hat{N} = n] = \mathrm{Tr}(\hat{N}\rho).$$

Finally, we note that the Markov inequality for $\hat{N}$ (viewed as a random variable) implies that

$$\mathbb{P}r_\rho[\hat{N} \geq a] \leq \frac{\mathbb{E}_\rho[\hat{N}]}{a}. \tag{2.3}$$

2.5.1 Coherent states

We will be looking at coherent states and their properties for a large part of the thesis, in particular because it is easy to generate them experimentally. One can simply use lasers to create coherent states as laser pulses approximate these states very well. These states also minimize the uncertainty relation between the two phase quadratures of light and are the most classical states of light [23–25].

However, we do not require a lot of background on coherent states. A (single-mode) coherent state can be defined as the eigenstate of the annihilation operator, or simply the state

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \tag{2.4}$$

for $\alpha \in \mathbb{C}$. It should be noted that we will use Greek alphabets inside kets to denote a coherent state. A multi-mode coherent state [26] is simply

$$\bigotimes_{k=1}^{n} |\alpha_k\rangle$$

for $\{\alpha_k\}_{k=1}^{n} \subset \mathbb{C}$. We will use $\mathscr{C}_n$ to denote the set of n-mode coherent states.

$$\mathscr{C}_n := \left\{ e^{i\phi} \bigotimes_{k=1}^{n} |\alpha_k\rangle : \ \forall\ 1 \leq k \leq n,\ \alpha_k \in \mathbb{C},\ \phi \in \mathbb{R} \right\}$$

This notation can be simplified, by using the map

$$\| \cdot \rangle\!\rangle : \mathbb{C}^n \longrightarrow \mathscr{C}_n$$

which takes an amplitude vector, $\alpha = (\alpha_1\ \alpha_2 \cdots \alpha_n)^{\mathrm{T}} \in \mathbb{C}^n$, and creates a multi-mode coherent state using its components, that is,

$$\|\alpha\rangle\rangle := \bigotimes_{k=1}^{n} |\alpha_k\rangle$$

Hence, $\mathscr{C}_n$ can be written as

$$\mathscr{C}_n = \left\{ e^{i\phi} \|\alpha\rangle\rangle : \alpha \in \mathbb{C}^n,\ \phi \in \mathbb{R} \right\}.$$

During Section 3.2, it will be seen that this notation arises naturally. Finally, we note that the inner product between two coherent states is

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

2.6 Communication complexity

Communication complexity is the study of the number of bits two parties need to communicate in order to be able to compute a function on their inputs. There are different models of communication one can consider to quantify the communication complexity of a function. In this thesis, we will mainly deal with the Simultaneous Message Passing (SMP). We will however use results connecting the complexity of a function in the SMP model with the two-party deterministic communication complexity of a function. In this section, we describe these settings and the results we use in this thesis. We point the reader to the books [27, 28] for a more thorough introduction to this subject.

We begin with an overview of classical communication complexity. Consider two parties Alice and Bob who wish to collaborate and compute a function $f : \mathcal{X} \times \mathcal{Y} \to \{0, 1\}$ on their inputs x and y *exactly* using a deterministic protocol Π. The number of bits they need to communicate with each other for this purpose is called the communication cost of the protocol on inputs x and y and denoted by $\mathrm{cost}_{\Pi}(x, y)$. The communication cost of the protocol is given by

$$\mathrm{cost}(\Pi) := \max_{x,y}\{\mathrm{cost}_{\Pi}(x, y)\}.$$

Further, we define the deterministic communication complexity of a function f to be the minimum communication cost for computing f. That is,

$$D(f) := \min_{\pi} \mathrm{cost}\{\Pi\}$$

where the minimization is over all deterministic protocols Π which compute f exactly. The definitions given above can also be extended to randomized protocols which allow for an error $\epsilon \geq 0$ during the protocol. Typically two types of models for randomness are studied in communication complexity: shared randomness and private randomness. In the shared randomness setting, Alice and Bob have access to an arbitrarily long random string, which they can use during the protocol. Whereas in the private randomness setting, Alice and Bob can generate randomness only locally. A randomized protocol Π is said to compute a function f with error at most ϵ, if for every pair of inputs x, y we have

$$\mathbb{P}r_{\Pi}[\Pi(x,y) \neq f(x,y)] \leq \epsilon. \tag{2.5}$$

The communication cost of the protocol is once again defined to be the maximum number of bits which Alice and Bob may be required to communicate during the protocol, and the randomized communication complexity of f is defined as the minimum protocol cost for computing f. We omit the details for randomized protocols here, since knowledge of these will not be required during this thesis.

The Simultaneous Message Passing (SMP) model is a more restricted setting in communication complexity. In the SMP model, there are three parties: Alice, Bob and a Referee. Alice and Bob receive inputs x and y. These inputs are not visible to the Referee. Further, throughout this thesis we consider the model where Alice and Bob have access to private randomness as well. Models where Alice and Bob have access to shared resources like shared randomness (or shared entanglement in the quantum case) are also studied, but we will not require these for the purpose of this thesis. Alice and Bob both send messages to the Referee, so that he is able to compute $f(x,y)$ with high probability. It should be noted that Alice and Bob cannot view each other's messages in this setting. A protocol is said to compute function f with error at most ϵ if it satisfies the condition in Eq. 2.5 for every input x, y. The communication cost of a SMP protocol Π is the maximum number of bits Alice and Bob have to send to the Referee for any input and randomness. The SMP communication complexity of computing a function f with error at most ϵ denoted by $R_{\epsilon}^{||}(f)$ is the minimum communication cost of any SMP protocol which computes f with error at most ϵ.

We can define similar settings in the quantum case as well. In this thesis, however, we will only consider quantum communication protocols in the SMP model. The setting of the model is the same as the classical model above. However, now Alice and Bob can send quantum states as messages to the Referee. In the model that we consider in this thesis, there are no shared resources[1] between any of the parties. Now the communication cost of the protocol is quantified using the maximum number of qubits sent by Alice and Bob during the protocol. Suppose Π is a SMP quantum communication protocol, then we define $\text{cost}_{\Pi}^{Q}(x,y)$ to be the total number of qubits sent by Alice and Bob to the Referee. As before, we define the quantum communication cost of the protocol as

$$\text{cost}_{Q}(\Pi) := \max_{x,y}\{\text{cost}_{\Pi}^{Q}(x,y)\}.$$

[1] For example, one can consider variants of this model where Alice and Bob share entangled states.

The quantum SMP communication complexity of computing f with error at most ϵ denoted by $Q_\epsilon^{||}(f)$ is

$$Q_\epsilon^{||}(f) := \min_{\Pi}\{\mathrm{cost}_Q(\Pi)\}$$

where the minimization takes place over protocols which compute f with error at most ϵ.

We will now state some well known results in communication complexity, which will be used later on in this thesis. The following theorem shows that up to multiplicative factors the communication complexity of function is the same for different errors.

Theorem 2.6 (Confidence Amplification; see for example Ref. [27])**.** *Consider a function $f : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ and $0 < \epsilon < 1/2$. In the classical SMP communication setting, we have that*

$$R_\epsilon^{||}(f) = O(R_{1/3}^{||}(f)\log(1/\epsilon)).$$

This result can easily be proven by having the parties repeat the same protocol many times and by having the Referee output the majority outcome. A similar result is also valid for other randomized settings and protocols. Thus, as long as the error of a protocol is below $1/3$ [2], we can convert it to a protocol with arbitrary non-zero error while keeping the order of the communication the same. Moreover, for this reason it is also sufficient to consider the error to be $1/3$ when studying randomized communication complexity. The next theorem provides a lower bound for the classical SMP communication complexity of a function in terms of its deterministic communication complexity.

Theorem 2.7 (Babai and Kimmel [29])**.** *The classical SMP communication complexity of a function $f : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ satisfies*

$$R_{1/3}^{||}(f) = \Omega(\sqrt{D(f)}).$$

The following lower bound can be proven by observing that any q-qubit quantum state can be specified using $O(q2^q)$ classical bit with exponential precision (see for example Ref. [7, Section 2]).

Theorem 2.8. *For any function $f : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$, the quantum and classical SMP communication complexities are related as follows*

$$Q_\epsilon^{||}(f) = \Omega(\log(R_\epsilon^{||}(f))).$$

[2] In fact, we only need the error to be strictly smaller than $1/2$.

Chapter 3

Characterization of Gram matrices of multi-mode coherent states

3.1 Introduction

It has been shown that the use of quantum resources offers significant qualitative and quantitative advantages over classical communication for several problems. Quantum cryptographic protocols are a prominent example of the qualitative advantage, while numerous protocols demonstrating the quantitative advantage in terms of communication or information complexity have been developed [6–9]. The theoretical description of these protocols is usually given in terms of d-dimensional quantum systems, or qudits. However manipulation and control of these systems still remains a challenge. Due to this reason the question of experimental implementation of these protocols is also left open. The most successfully implemented quantum protocols are ones which have been reformulated in terms of coherent states, which can be produced using lasers, and linear optics. Widely celebrated quantum key distribution [10, 30, 31] and quantum fingerprinting protocols [3, 11, 12] fall in this category, and as always there is a great impetus towards realizing more protocols using these tools [32–34].

Consider the quantum fingerprinting protocol as an example. The protocol solves the Equality problem in the simultaneous message passing model. Essentially two parties have to check whether the strings they hold are equal or not in the absence of shared randomness and with as little communication as possible. In 2001, Buhrman et al. gave a quantum protocol for this problem [7], which required exponentially less communication than the optimal classical protocol for this task. It was not until 2015 [11] though, that the protocol was implemented experimentally. This implementation became possible after the protocol had been reformulated such that it required only coherent states and linear optics, in a way which also preserved the communication cost [12]. The original protocol mapped the set of n-bit strings, $\{s_i\}_{i=1}^{2^n}$ to qudit states, $\{|\psi_i\rangle\}_{i=1}^{2^n} \subset \mathcal{H}_q$, such that for $i \neq j$, the overlap, $|\langle\psi_i|\psi_j\rangle| \leq \delta$ for some δ, and $\dim(\mathcal{H}_q) = O(n)$.

It should be observed that this is in fact a constraint on the Gram matrix of the vectors. Using this mapping, they showed that one could decide if two strings were equal or unequal by communicating only $O(\log n)$ qubits. Arrazola et al. [12] showed that one could instead choose multi-mode coherent states which satisfy the requirements on the overlap for the protocol. This naturally leads us to ask under what conditions can the vectors forming a Gram matrix be chosen as multi-mode coherent states, so that a protocol implemented by them may be run using coherent states.

This is the question we answer in this chapter. We characterize the set of Gram matrices of coherent states and their closure. Not only will such a characterization help us in reformulating quantum protocols in terms of coherent states, but it will also shed light on the fundamental properties of sets of coherent states, which are the most classical states of light [23–25]. A Gram matrix of a set of quantum states encodes the information about their orientation relative to each other. For this reason, we can very often exchange one set of states with another in a protocol if their Gram matrices are the same, though the measurements also need to be changed correspondingly[1]. Additionally, the set of states attainable by applying physical tranformations on an initial set of states also depends on the Gram matrix of the initial set of states [35, 36]. Therefore, our work also characterizes all the set of states attainable from a set of multi-mode coherent states.

The chapter is organised as follows. In Section 3.2, we completely characterize the set of Gram matrices, which can be constructed using multi-mode coherent states. This result is stated as Theorem 3.1. We provide a test to check if a matrix belongs in this set. We show that the Hadamard exponential of Euclidean distance matrices can be written as a Gram matrix of multi-mode coherent states, which proves that they are positive semidefinite. Moreover in Section 3.3, we derive the closure of this set to characterize the Gram matrices, which can be approximated arbitrarily well using multi-mode coherent states. This characterization is presented in Theorem 3.2.

3.2 Characterization of Gram matrices of multi-mode coherent states

Throughout this Chapter, we will consider general multi-mode coherent states. We choose to study these states due to the relative ease with which one can implement them. A coherent state can simply be thought of as a pulse of laser. On the other hand, we can implement a multi-mode coherent state using a sequence of laser pulses. In this case, the modes are chosen to be the temporal modes. We begin by recalling some notation introduced in Chapter 2. Recall that for

[1] If two sets of vectors have the same Gram matrix, then one can transform one set into the other using an isometry.

an amplitude vector $\alpha \in \mathbb{C}^n$, the corresponding n-mode coherent state is given by

$$\|\alpha\rangle\!\rangle := \bigotimes_{k=1}^{n} |\alpha_k\rangle .$$

We use $\mathscr{C}_n$ to denote the set of n-mode coherent states.

$$\begin{aligned}\mathscr{C}_n &:= \left\{ e^{i\phi} \bigotimes_{k=1}^{n} |\alpha_k\rangle : \; \forall\ 1 \le k \le n,\ \alpha_k \in \mathbb{C},\ \phi \in \mathbb{R} \right\} \\ &= \left\{ e^{i\phi} \|\alpha\rangle\!\rangle : \alpha \in \mathbb{C}^n,\ \phi \in \mathbb{R} \right\} .\end{aligned}$$

The following notation will be used to denote the standard inner product on a Hilbert Space, $\mathcal{H}$.

$$\langle\, \cdot\, ,\, \cdot\, \rangle \;:\; \mathcal{H} \times \mathcal{H} \longrightarrow \mathbb{C}$$

As an example, the inner product between two multi-mode coherent states, $\|\alpha\rangle\!\rangle$ and $\|\beta\rangle\!\rangle$ will be denoted as $\langle \|\alpha\rangle\!\rangle, \|\beta\rangle\!\rangle \rangle$. Finally, we also define a function which takes an n-tuple of vectors and maps them to their Gram matrix.

Definition 3.1. For a Hilbert space, $\mathcal{H}$, we define G to be the function which takes vectors $v_1, v_2, \cdots, v_n \in \mathcal{H}$ and maps them to their Gram matrix.

$$\begin{aligned} &G : \mathcal{H}^n \to \mathrm{Pos}(\mathbb{C}^n) \\ &\left(G\left(v_1, v_2, \cdots, v_n\right)\right)_{ij} := \langle v_i, v_j \rangle \text{ for } 1 \le i, j \le n \end{aligned} \tag{3.1}$$

Given this definition of G, we can introduce the notation,

$$G(S^n) = \{G(v_1, v_2, \cdots, v_n) : v_1, v_2, \cdots, v_n \in S\} .$$

where $S \subset \mathcal{H}$ is a set of vectors.

In this section, we will prove a theorem which characterizes Gram matrices of multi-mode coherent states. Namely, we will answer the question: can we write a Gram matrix P, as $P = G(e^{i\phi_1}\|\alpha_1\rangle\!\rangle, e^{i\phi_2}\|\alpha_2\rangle\!\rangle, \cdots, e^{i\phi_n}\|\alpha_n\rangle\!\rangle)$?

If indeed the matrix P is a gram matrix of multi-mode coherent states, then for every i, j

$$P_{ij} = \left\langle e^{i\phi_i} \bigotimes_{k=1}^{m} |\alpha_{ik}\rangle , e^{i\phi_j} \bigotimes_{k=1}^{m} |\alpha_{jk}\rangle \right\rangle$$

for some given number of modes, $m \in \mathbb{N}$, a set of amplitudes, $\{\alpha_{jk} : j \in [n], k \in [m]\}$ and a set of real phases, $\{\phi_i : i \in [n]\}$. Let us further simplify this:

$$\begin{aligned} P_{ij} &= e^{i(\phi_j - \phi_i)} \prod_{k=1}^{m} \langle |\alpha_{ik}\rangle , |\alpha_{jk}\rangle \rangle \\ &= e^{i(\phi_j - \phi_i)} \prod_{k=1}^{m} \exp\left(-\frac{1}{2} \left(|\alpha_{ik}|^2 + |\alpha_{jk}|^2 - 2\alpha_{ik}^* \alpha_{jk} \right) \right) \\ &= \exp\left(i\left(\phi_j - \phi_i\right) - \frac{1}{2} \sum_{k=1}^{m} \left(|\alpha_{ik}|^2 + |\alpha_{jk}|^2 - 2\alpha_{ik}^* \alpha_{jk} \right) \right) . \end{aligned}$$

Define, the vector, $\alpha_i := (\alpha_{i1}\ \alpha_{i2} \cdots \alpha_{im})^{\mathrm{T}} \in \mathbb{C}^m$, and the vector of phases, $\phi := (\phi_1\ \phi_2 \cdots \phi_n)^{\mathrm{T}} \in \mathbb{R}^n$ for every $i \in [n]$. This naturally gives rise to the notation mentioned earlier for multi-mode coherent states. The inner product can be written as

$$P_{ij} = \exp\left(-\frac{1}{2}\left(\|\alpha_i\|_2^2 + \|\alpha_j\|_2^2 - 2\langle\alpha_i, \alpha_j\rangle\right) + i\left(\phi_j - \phi_i\right)\right) \tag{3.2}$$

or equivalently,

$$P_{ij} = \exp\left(-\frac{1}{2}\|\alpha_i - \alpha_j\|_2^2 + i\left(\mathrm{Im}\{\langle\alpha_i, \alpha_j\rangle\} + (\phi_j - \phi_i)\right)\right). \tag{3.3}$$

For a particular branch of the ln functions Eqs. 3.2 and 3.3 are equivalent to the existence of $\{N_{ij}\}_{i,j} \subset \mathbb{Z}$ for which

$$\begin{aligned}\ln(P_{ij}) - i2\pi N_{ij} = -\frac{1}{2}&\left(\|\alpha_i\|_2^2 + \|\alpha_j\|_2^2 - 2\langle\alpha_i, \alpha_j\rangle\right)\\ &+ i\left(\phi_j - \phi_i\right)\end{aligned} \tag{3.4}$$

or equivalently,

$$\begin{aligned}\ln(P_{ij}) - i2\pi N_{ij} = -\frac{1}{2}&\|\alpha_i - \alpha_j\|_2^2\\ &+ i\left(\mathrm{Im}\{\langle\alpha_i, \alpha_j\rangle\} + (\phi_j - \phi_i)\right)\end{aligned} \tag{3.5}$$

holds for every $i, j \in [n]$.

In the Lemma that follows, we characterize matrices Q which satisfy

$$Q_{ij} = -\frac{1}{2}\left(\|\alpha_i\|_2^2 + \|\alpha_j\|_2^2 - 2\langle\alpha_i, \alpha_j\rangle\right) + i\left(\phi_j - \phi_i\right)$$

for some set of complex vectors $\{\alpha_i\}_i$, and real phases, $\{\phi_i\}_i$. For the statement of this Lemma, we define the vector, $u \in \mathbb{C}^n$ to be the vector of all ones, i.e.,

$$u := (1\ 1 \cdots 1)^T$$

Lemma 3.1. *For a matrix, $Q \in L(\mathbb{C}^n)$, the following are equivalent:*

(I) There exists $m \in \mathbb{N}$, a set of complex vectors $\{\alpha_i : i \in [n]\} \subset \mathbb{C}^m$, and a set of real phases $\{\phi_i : i \in [n]\} \subseteq \mathbb{R}$ such that for $i, j \in [n]$,

$$Q_{ij} = -\frac{1}{2}\left(\|\alpha_i\|_2^2 + \|\alpha_j\|_2^2 - 2\langle\alpha_i, \alpha_j\rangle\right) + i\left(\phi_j - \phi_i\right). \tag{3.6}$$

(II) $Q \in$ Herm$(\mathbb{C}^n)$, $Q_{ii} = 0$ for all $i \in [n]$ and there exists a vector, $x \in \mathbb{C}^n$, such that

$$Q + xu^\dagger + ux^\dagger \geq 0. \tag{3.7}$$

(III) $Q \in$ *Herm*$(\mathbb{C}^n)$, $Q_{ii} = 0$ *for all* $i \in [n]$ *and for every vector,* $s \in \mathbb{C}^n$, *such that* $\langle u, s \rangle = 1$, *it holds that*

$$\left(\mathbb{1} - us^{\dagger}\right) Q \left(\mathbb{1} - su^{\dagger}\right) \geq 0. \tag{3.8}$$

(IV) $Q \in$ *Herm*$(\mathbb{C}^n)$, $Q_{ii} = 0$ *for all* $i \in [n]$ *and there exists a vector,* $s \in \mathbb{C}^n$, *such that* $\langle u, s \rangle = 1$ *and*

$$\left(\mathbb{1} - us^{\dagger}\right) Q \left(\mathbb{1} - su^{\dagger}\right) \geq 0. \tag{3.9}$$

(V) $Q \in$ *Herm*$(\mathbb{C}^n)$, $Q_{ii} = 0$ *for all* $i \in [n]$ *and for every vector,* $y \in \mathbb{C}^n$, *such that* $\langle u, y \rangle = 0$, *it holds that*

$$y^{\dagger} Q y \geq 0. \tag{3.10}$$

Proof. In the characterization presented here, Q behaves similar to a Euclidean distance matrices [37,38]. The equation of the inner products of the vectors in statement I of the Lemma is similar to the equation for an element of a distance matrix. The proofs of these statements are almost the same as the ones given by Gower in Ref. [37] for the characterization of Euclidean distance matrices. It should be noted however that Q here is not a distance matrix, since its entries may be complex. We will prove the statements of the theorem in the order

$$\begin{aligned}
&(\mathrm{I}) \Rightarrow (\mathrm{II}) \Rightarrow (\mathrm{I})\\
&(\mathrm{II}) \Rightarrow (\mathrm{III}) \Rightarrow (\mathrm{IV}) \Rightarrow (\mathrm{II})\\
&(\mathrm{III}) \Rightarrow (\mathrm{V}) \Rightarrow (\mathrm{III}).
\end{aligned}$$

We will prove that statement (I) ⇒ statement (II). It is clear from Eq. 3.6 that Q is Hermitian and that for every $i \in [n]$, $Q_{ii} = 0$. Let H be the Gram matrix of the vectors, $\{\alpha_i\}_{i=1}^{n}$, that is, $H_{ij} := \langle \alpha_i, \alpha_j \rangle$. Then, we have that H is positive semidefinite, since the set of Gram matrices and positive semidefinite matrices is equivalent. We can write Eq. 3.6 as

$$Q_{ij} = i\left(\phi_j - \phi_i\right) - \frac{1}{2}\left(H_{ii} + H_{jj} - 2H_{ij}\right). \tag{3.11}$$

Without loss of generality let, $H = Q + X$ for some X. Then, $H_{ii} = Q_{ii} + X_{ii} = 0 + X_{ii} = X_{ii}$. We substitute this into Eq. 3.11 to derive a consistency equation for X.

$$\begin{aligned}
Q_{ij} &= i\left(\phi_j - \phi_i\right) - \frac{1}{2}\left(X_{ii} + X_{jj} - 2Q_{ij} - 2X_{ij}\right)\\
\Rightarrow X_{ij} &= \left(\frac{1}{2}X_{ii} + i\phi_i\right) + \left(\frac{1}{2}X_{jj} - i\phi_j\right)
\end{aligned}$$

Define $x \in \mathbb{C}^n$, as $x_i := X_{ii}/2 + i\phi_i$ ($X_{ii} = \|\alpha_i\|_2^2 \in \mathbb{R}$, and $\phi_i \in \mathbb{R}$). Then, for $i, j \in [n]$ we may write

$$X_{ij} = x_i + x_j^{*},$$

which is equivalent to

$$X = xu^\dagger + ux^\dagger. \tag{3.12}$$

Therefore, if statement (I) is true, then $H = Q + xu^\dagger + ux^\dagger \geq 0$. Thus statement II is true.

For the converse, statement (II) ⇒ statement (I), assume that $Q \in \text{Herm}(\mathbb{C}^n)$, for every $i \in [n]$ $Q_{ii} = 0$ and that there is a vector, $x \in \mathbb{C}^n$, such that $Q + xu^\dagger + ux^\dagger \geq 0$. Let $H := Q + xu^\dagger + ux^\dagger$. Then, there exists a set of vectors, $\{\alpha_i\}_{i=1}^n$, such that $H_{ij} = \langle \alpha_i, \alpha_j \rangle$, since H is positive semi-definite. We can now show that these amplitude vectors satisfy Eq. 3.6 for an appropriate definition of ϕ. To see this, observe that

$$\begin{aligned} H_{ij} &= Q_{ij} + x_i + x_j^* \\ H_{ii} &= x_i + x_i^*. \end{aligned}$$

Now let's evaluate the following expression.

$$\begin{aligned} \|\alpha_i\|_2^2 + &\|\alpha_j\|_2^2 - 2\langle \alpha_i, \alpha_j \rangle \\ &= H_{ii} + H_{jj} - 2H_{ij} \\ &= x_i + x_i^* + x_j + x_j^* - 2Q_{ij} - 2x_i - 2x_j^* \\ &= -2Q_{ij} - (x_i - x_i^*) + \left(x_j - x_j^*\right) \\ &= -2Q_{ij} - 2i\text{Im}\{x_i\} + 2i\text{Im}\{x_j\} \end{aligned}$$

Define, $\phi \in \mathbb{R}^n$, such that $\phi_i := \text{Im}\{x_i\} \in \mathbb{R}$. Then, the right hand side of Eq. 3.6 is

$$\begin{aligned} &-\frac{1}{2}\left(\|\alpha_i\|_2^2 + \|\alpha_j\|_2^2 - 2\langle \alpha_i, \alpha_j \rangle\right) + i\left(\phi_j - \phi_i\right) \\ &= \left(Q_{ij} + i\text{Im}\{x_i\} - i\text{Im}\{x_j\}\right) + i\left(\text{Im}\{x_j\} - \text{Im}\{x_i\}\right) \\ &= Q_{ij}. \end{aligned}$$

Hence, given statement (II) one can define a set of amplitude vectors, $\{\alpha_i\}_{i=1}^n \subseteq \mathbb{C}^n$, and a vector of phases, $\phi \in \mathbb{R}^n$ such that Eq. 3.6 is satisfied for all $i, j \in [n]$. Therefore, (I) ⇔ (II).

For all the rest of the statements the facts $Q \in \text{Herm}(\mathbb{C}^n)$ and $Q_{ii} = 0$ for every $i \in [n]$ are common. So, we don't need to prove them for each statement. We will assume these and prove the rest of the statements. To see that statement (II) ⇒ statement (III), choose a vector, $s \in \mathbb{C}^n$, such that $\langle u, s \rangle = 1$. We note that for any such choice

$$\begin{aligned} \left(\mathbb{1} - us^\dagger\right)&xu^\dagger\left(\mathbb{1} - su^\dagger\right) \\ &= \left(\mathbb{1} - us^\dagger\right)\left(xu^\dagger - x(u^\dagger s)u^\dagger\right) \\ &= 0. \end{aligned} \tag{3.13}$$

Using the fact that the expression in Eq. 3.13 and its conjugate are zero, we can now show, starting with statement (II), that

$$\begin{aligned}&H := Q + xu^\dagger + ux^\dagger \geq 0\\ &\Rightarrow \left(\mathbb{1} - us^\dagger\right) H \left(\mathbb{1} - su^\dagger\right) \geq 0\\ &\Rightarrow \left(\mathbb{1} - us^\dagger\right) Q \left(\mathbb{1} - su^\dagger\right) \geq 0.\end{aligned}$$

This proves that statement (II) ⇒ statement (III). Statement (III) ⇒ statement (IV) trivially.

For statement (IV) ⇒ statement (II), assume that the vector, $s \in \mathbb{C}^n$ is such that $\langle u, s\rangle = 1$, and

$$\left(\mathbb{1} - us^\dagger\right) Q \left(\mathbb{1} - su^\dagger\right) \geq 0.$$

We can write the above as

$$Q + xu^\dagger + ux^\dagger \geq 0,$$

for the choice, $x := \frac{1}{2}\left(s^\dagger Q s\right) u - Qs$. Hence, we have shown the equivalence of the first four statements.

For statement (III) ⇒ statement (V), we have that $\left(\mathbb{1} - us^\dagger\right) Q \left(\mathbb{1} - su^\dagger\right) \geq 0$ for every $s \in \mathbb{C}^n$ such that $\langle u, s\rangle = 1$ using statement (III). Then, for every vector, $y \in \mathbb{C}^n$, such that, $\langle u, y\rangle = 0$,

$$\begin{aligned}&y^\dagger \left(\mathbb{1} - us^\dagger\right) Q \left(\mathbb{1} - su^\dagger\right) y \geq 0\\ &\Rightarrow y^\dagger Q y \geq 0.\end{aligned}$$

For statement (V) ⇒ statement (III), we assume that for every vector, $y \in \mathbb{C}^n$, such that, $\langle u, y\rangle = 0$,

$$y^\dagger Q y \geq 0.$$

If we choose any vector $s \in \mathbb{C}^n$ such that $\langle u, s\rangle = 1$, and any vector $v \in \mathbb{C}^n$, then we can construct a vector y with $\langle u, y\rangle = 0$ by setting $y = (\mathbb{1} - su^\dagger)v$. Using statement (V) with this choice of vector y then gives

$$\begin{aligned}&v^\dagger \left(\mathbb{1} - us^\dagger\right) Q \left(\mathbb{1} - su^\dagger\right) v \geq 0\\ &\Rightarrow \left(\mathbb{1} - us^\dagger\right) Q \left(\mathbb{1} - su^\dagger\right) \geq 0,\end{aligned}$$

which proves statement (V) ⇒ statement (III).

□

We can use this Lemma to check if a matrix is a Gram matrix of multi-mode coherent states. First, we define the Hadamard logarithm, as

$$(\ln \odot(P))_{ij} := \ln P_{ij}.$$

Using Eq. 3.4 and Lemma 3.1, we have that a matrix P such that $P_{ii} = 1$ for every $i \in [n]$ is Gram matrix of coherent states if and only if there exists a matrix of integers $N \in \mathbb{Z}^{n\times n}$ such that $(\ln\odot(P) - 2\pi i N) \in \text{Herm}(\mathbb{C}^n)$, $2\pi i N_{ii} = \ln 1$ for every $i \in [n]$ and

$$\left(\mathbb{1} - \frac{uu^\dagger}{n}\right)(\ln\odot(P) - 2\pi i N)\left(\mathbb{1} - \frac{uu^\dagger}{n}\right) \geq 0.$$

However, in this form this condition cannot be checked since there are countably infinite choices for the matrix, N. Now, we will show that we only need to check this condition for a finite number of matrices, N. First, we show that if a matrix can be written as a Gram matrix of multi-mode coherent states, then one of the coherent states can be chosen as $\|0\rangle\rangle$.

Lemma 3.2. *If* $P = G(e^{i\phi_1}\|\alpha_1\rangle\rangle, e^{i\phi_2}\|\alpha_2\rangle\rangle, \cdots, e^{i\phi_n}\|\alpha_n\rangle\rangle)$, *then* $P = G(e^{i\phi'_1}\|0\rangle\rangle, e^{i\phi'_2}\|\alpha'_2\rangle\rangle, \cdots, e^{i\phi'_n}\|\alpha'_n\rangle\rangle)$, *where* $\alpha'_i = \alpha_i - \alpha_1$, *and* $\phi'_i = \phi_i - Im\{\langle\alpha_i, \alpha_1\rangle\}$ *for every* $i \in [n]$.

Proof. This can be proven by just plugging in the values given above in Eq. 3.3. □

Our goal is to restrict the values the matrix element N_{ij} can take. We accomplish this by using a complex $\ln$ function mapping to the branch, $[\beta, \beta + 2\pi)$ in the following equation.

$$\begin{aligned}\ln(P_{ij}) = -\frac{1}{2}\|\alpha_i - \alpha_j\|_2^2 \\ + i\left(\text{Im}\{\langle\alpha_i, \alpha_j\rangle\} + (\phi_j - \phi_i) + 2\pi N_{ij}\right)\end{aligned} \tag{3.14}$$

The imaginary part on the left hand side of Eq. 3.14 is restricted to the interval $[\beta, \beta + 2\pi)$. If we can bound the terms in the imaginary part on the right hand side, then we would be able to bound the terms N_{ij} as well. For this purpose, we define the parameter,

$$\delta := \min_{i,j} |P_{ij}|. \tag{3.15}$$

If $\delta = 0$, then we know that $P \notin G(\mathscr{C}_m^n)$, since the inner product between two coherent states cannot be zero (see Eq. 3.2). So, we consider $\delta \neq 0$. If $P \in G(\mathscr{C}_m^n)$, then $P = G(e^{i\phi_1}\|\alpha_1\rangle\rangle, e^{i\phi_2}\|\alpha_2\rangle\rangle, \cdots, e^{i\phi_n}\|\alpha_n\rangle\rangle)$ for some amplitude vectors, $\{\alpha_i\}_{i=1}^n$ with $\alpha_1 = 0$ and real phases, $\{\phi_i\}_{i=1}^n$ (using Lemma 3.2). Moreover, we can assume that for every $i \in [n]$, $\phi_i \in [0, 2\pi)$. Then, for every $i, j \in [n]$ we have that

$$-2\pi \leq \phi_j - \phi_i \leq 2\pi. \tag{3.16}$$

For a matrix $P \in G(\mathscr{C}_m^n)$, we have

$$\begin{aligned}\delta &= \min_{i,j}\{\exp\left(-\frac{1}{2}\|\alpha_i - \alpha_j\|_2^2\right)\} \\ &= \exp\left(-\frac{1}{2}\left(\max_{i,j}\{\|\alpha_i - \alpha_j\|_2\}\right)^2\right).\end{aligned}$$

This implies that

$$\max_{i,j}\{\|\alpha_i - \alpha_j\|_2\} = (-2\ln(\delta))^{1/2}.$$

For every $i \in [n]$, and amplitude vector, α_i in this representation of P, we have

$$\begin{aligned}\|\alpha_i\|_2 &= \|\alpha_i - 0\|_2\\ &= \|\alpha_i - \alpha_1\|_2\\ &\leq \max_{i,j}\{\|\alpha_i - \alpha_j\|_2\} = (-2\ln(\delta))^{1/2}.\end{aligned}$$

Further, we have that for every $i, j \in [n]$

$$\begin{aligned}|\langle\alpha_i, \alpha_j\rangle| &\leq \|\alpha_i\|_2\|\alpha_j\|_2\\ &\leq -2\ln(\delta) = |2\ln(\delta)|.\end{aligned}$$

We will use this to bound the Im$\{\alpha_i, \alpha_j\}$, using

$$|\text{Im}\{\langle\alpha_i, \alpha_j\rangle\}| \leq |\langle\alpha_i, \alpha_j\rangle| \leq |2\ln(\delta)| \tag{3.17}$$

Now, observe that in Eq. 3.14 if we consider the ln function with $[\beta, \beta + 2\pi)$ branch, for every $i, j \in [n]$ we have

$$\begin{aligned}&\beta \leq 2\pi N_{ij} + \text{Im}\{\langle\alpha_i, \alpha_j\rangle\} + (\phi_j - \phi_i)\\ \Rightarrow\ &\beta - \text{Im}\{\langle\alpha_i, \alpha_j\rangle\} - (\phi_j - \phi_i) \leq 2\pi N_{ij}\\ \Rightarrow\ &\beta - |2\ln(\delta)| - 2\pi \leq 2\pi N_{ij},\end{aligned}$$

and,

$$\begin{aligned}&2\pi N_{ij} + \text{Im}\{\langle\alpha_i, \alpha_j\rangle\} + (\phi_j - \phi_i) < \beta + 2\pi\\ \Rightarrow\ &2\pi N_{ij} < \beta + 2\pi - \text{Im}\{\langle\alpha_i, \alpha_j\rangle\} - (\phi_j - \phi_i)\\ \Rightarrow\ &2\pi N_{ij} < \beta + 4\pi + |2\ln(\delta)|,\end{aligned}$$

for which we have used Eqs. 3.16 and 3.17. Thus for every $i, j \in [n]$ we have the following bound:

$$N_{ij} \in \mathbb{Z} \cap \left[\frac{\beta}{2\pi} - \frac{1}{\pi}|\ln(\delta)| - 1, \frac{\beta}{2\pi} + \frac{1}{\pi}|\ln(\delta)| + 2\right). \tag{3.18}$$

To summarize, we have proven that if $P \in G(\mathscr{C}_m^n)$, then there exists an integer matrix $N \in \mathbb{Z}^{n\times n}$ with elements in the range given by Eq. 3.18 and a set of vectors, $\{\alpha_i\}_i$ (where $\alpha_1 = 0$ specifically) and phases, $\{\phi_i\}_i$, such that for every i, j

$$\begin{aligned}\ln(P_{ij}) - i2\pi N_{ij} = -\frac{1}{2}&\left(\|\alpha_i\|_2^2 + \|\alpha_j\|_2^2 - 2\langle\alpha_i, \alpha_j\rangle\right)\\ &+ i\left(\phi_j - \phi_i\right).\end{aligned}$$

Using the characterization of matrix equations of this form given in Lemma 3.1, we have that this is equivalent to $(\ln \odot(P) - 2\pi i N)$ being a Hermitian matrix, $2\pi i N_{ii} = \ln(1)$ for every $i \in [n]$ and

$$\left(\mathbb{1} - \frac{uu^\dagger}{n}\right)(\ln \odot(P) - 2\pi i N)\left(\mathbb{1} - \frac{uu^\dagger}{n}\right) \geq 0.$$

Thus, we have proven the following Theorem, which characterizes the Gram matrices of multi-mode coherent states. Here we consider the $\ln$ function with the branch $[\beta, \beta + 2\pi)$.

Theorem 3.1. *For a matrix, $P \in$ Herm$(\mathbb{C}^n)$ such that $P_{ii} = 1$ for all $i \in [n]$, $P \in G(\mathscr{C}_m^n)$ for some $m \in \mathbb{N}$ if and only if there exists an integer matrix $N \in \mathbb{Z}^{n\times n}$, such that $(\ln \odot(P) - 2\pi i N) \in$ Herm$(\mathbb{C}^n)$, $2\pi i N_{ii} = \ln(1)$ for every $i \in [n]$, and*

$$\left(\mathbb{1} - \frac{uu^\dagger}{n}\right)(\ln \odot(P) - 2\pi i N)\left(\mathbb{1} - \frac{uu^\dagger}{n}\right) \geq 0. \tag{3.19}$$

Further, we can restrict the range of the elements of N to the following:

$$N_{ij} \in \mathbb{Z} \cap \left[\frac{\beta}{2\pi} - \frac{1}{\pi}|\ln(\delta)| - 1, \frac{\beta}{2\pi} + \frac{1}{\pi}|\ln(\delta)| + 2\right) \tag{3.20}$$

for every $i, j \in [n]$, where $\delta := \min_{i,j} |P_{ij}| > 0$.

Note that Eq. 3.19 can be replaced with any of the statements from Lemma 3.1. We have used $s = u/n$ in the statements III and IV of Lemma 3.1 for simplicity. Moreover, for every matrix $P \in$ Herm$(\mathbb{C}^n)$ we only need to check Eq. 3.19 for finitely many matrices, N. However, we need to check the conditions for $\exp(O(n^2))$ number of matrices N, where n is the size of the matrix P. It might be possible to use semidefinite programming and rounding methods to create a more efficient algorithm for this task but we do not pursue this lead here.

In the following corollary, we show that we can restrict the number of modes of the coherent states forming a Gram matrix to the size of the matrix.

Corollary 3.1. *For every $m \in \mathbb{N}$, $G\left(\mathscr{C}_{n+m}^n\right) = G\left(\mathscr{C}_n^n\right)$.*
That is, no more than n-modes are required to represent a Gram matrix of n-vectors.

Proof. A matrix $P \in$ Herm$(\mathbb{C}^n)$ with $P_{ii} = 1$ for every $i \in [n]$ can be written as a Gram matrix of coherent states if and only if there exist complex amplitude vectors, $\{\alpha_i\}_{i=1}^n \subset \mathbb{C}^m$ (where m is the number of modes) and a set of real phases $\{\phi_i\}_{i=1}^n$ such that

$$P_{ij} = \exp\left(-\frac{1}{2}\left(\|\alpha_i\|_2^2 + \|\alpha_j\|_2^2 - 2\langle\alpha_i, \alpha_j\rangle\right) + i\left(\phi_j - \phi_i\right)\right).$$

It is clear from the above equation that the collection of vectors, $\{\alpha_i\}_{i=1}^n$, is isometrically invariant, i.e., if $\{\alpha_i\}_{i=1}^n$ satisfy this equation, then for a $U \in U(\mathbb{C}^m, \mathbb{C}^p)$, the vectors $\{U\alpha_i\}_{i=1}^n$ also satisfy this equation. Therefore, one can simply constrain the vectors, $\{\alpha_i\}_{i=1}^n$, to be in an n-dimensional space (since there are only n vectors), i.e., we can choose the number of modes $m = n$.

□

Corollary 3.1 tells us that one cannot do better by simply increasing the number of modes. With this result in hand, we can see that the set of Gram matrices, which can be constructed using coherent states, is just $G(\mathscr{C}_n^n)$. Therefore, in Section 3.3, where we study the closure of the set of Gram matrices of multi-mode coherent states, we will just consider the set $G(\mathscr{C}_n^n)$.

We will demonstrate our characterization result by using it to show that n multi-mode coherent states, $\{e^{i\phi_i}\|\alpha_i\rangle\!\rangle\}_{i=1}^n$ can be chosen such that for $i \neq j$ the inner product $\langle e^{i\phi_i}\|\alpha_i\rangle\!\rangle, e^{i\phi_j}\|\alpha_j\rangle\!\rangle\rangle = r$ for some $r \in (0,1]$. That is, we can choose acute equiangular multi-mode coherent states.

Example 3.1. *Acute equiangular coherent states*
To show that coherent states with the aforementioned property exist, we show that the Gram matrix, $P \in \mathrm{Herm}(\mathbb{C}^n)$ such that $P_{ii} = 1$ for every $i \in [n]$, and $P_{ij} = r$ (where $r \in (0,1]$) for every $i \neq j \in [n]$, can be constructed using coherent states. For this we choose the $\ln$ function with $[-\pi,\pi)$ branch. Then, $\ln \odot P$ is Hermitian. Moreover, $\ln P_{ii} = 0$ for every $i \in [n]$, and $\ln P_{ij} = \ln(r)$ for every $i \neq j \in [n]$. That is,

$$\ln \odot P = \ln(r) uu^\dagger - \ln(r)\mathbb{1}.$$

Then, we have that

$$\begin{aligned}&\left(\mathbb{1} - \frac{uu^\dagger}{n}\right)(\ln \odot P)\left(\mathbb{1} - \frac{uu^\dagger}{n}\right)\\ &= \ln\left(\frac{1}{r}\right)\left(\mathbb{1} - \frac{uu^\dagger}{n}\right) \geq 0.\end{aligned}$$

Thus, we can choose n coherent states, such that the inner products between any two of these states is equal to some $r \in (0,1]$.

We can also use our characterization to prove that the Hadamard exponential of a Euclidean distance matrices is positive semidefinite. We will formulate this result as Corollary 3.2. A matrix, $D \in \mathrm{L}(\mathbb{R}^n)$ is a Euclidean distance matrix if there exist vectors, $\{\alpha_i\}_{i=1}^n \subset \mathbb{R}^n$, such that for $i,j \in [n]$

$$D_{ij} = -\frac{1}{2}\|\alpha_i - \alpha_j\|_2^2.$$

In Ref. [37] it has been proven that a matrix is a Euclidean distance matrix if and only if

$$\left(\mathbb{1} - \frac{uu^\dagger}{n}\right) D \left(\mathbb{1} - \frac{uu^\dagger}{n}\right) \geq 0. \tag{3.21}$$

Lastly, we define the Hadamard exponential of a matrix, X as the component wise exponential of a matrix. That is,

$$(\exp \odot(X))_{ij} := \exp(X_{ij}).$$

Corollary 3.2. *The Hadamard exponential of a Euclidean distance matrix, D is positive semidefinite. That is*

$$\exp\odot(D)\geq 0. \tag{3.22}$$

Proof. Let $P := \exp\odot(D)$. Since, D is a Euclidean distance matrix, it is a real matrix and $P_{ij} > 0$ for every i, j. If we choose the $\ln$ function to be the lnarithm with the branch $[-\pi, \pi)$, then $\ln\odot(P) = D$. Using this fact, we have

$$\begin{aligned}
&\left(\mathbb{1}-\frac{uu^\dagger}{n}\right)D\left(\mathbb{1}-\frac{uu^\dagger}{n}\right)\geq 0\\
\Rightarrow&\left(\mathbb{1}-\frac{uu^\dagger}{n}\right)(\ln\odot(P))\left(\mathbb{1}-\frac{uu^\dagger}{n}\right)\geq 0\\
\Rightarrow&\, P\in G(\mathscr{C}_n^n)\\
\Rightarrow&\, P\geq 0\\
\Rightarrow&\, \exp\odot(D)\geq 0,
\end{aligned}$$

where we have used Theorem 3.1 in the third step and the fact that Gram matrices are positive semidefinite in the fourth step. □

One can, in principle use Theorem 3.1 to not only check if a given square matrix, $P \in \mathrm{L}(\mathbb{C}^n)$ (such that $P_{ii} = 1$ for every $i \in [n]$) can be represented as a Gram matrix of coherent states or not, but also to find a set of coherent states, $\{e^{i\phi_i}\|\alpha_i\rangle\!\rangle\}_i$ such that $P = G(e^{i\phi_1}\|\alpha_1\rangle\!\rangle, \cdots, e^{i\phi_n}\|\alpha_n\rangle\!\rangle)$. One can use the following algorithm for example. Choose $\ln$ to be the logarithm with the branch $[-\pi, \pi)$. For the given matrix P, calculate $\delta := \min_{i,j}|P_{ij}|$. Let

$$\begin{aligned}
\mathcal{F} :=\{&N\in\mathbb{Z}^{n\times n}:\\
&N_{ij}\in\mathbb{Z}\cap\left[-\frac{3}{2}-\frac{1}{\pi}|\ln(\delta)|,\frac{3}{2}+\frac{1}{\pi}|\ln(\delta)|\right)\\
&\text{for every } i\neq j\in[n],\ 2\pi i N_{ii}=\ln(1)\\
&\text{for every } i\in[n] \text{ and}\\
&(\ln\odot(P)-2\pi i N)\in\mathrm{Herm}(\mathbb{C}^n)\}.
\end{aligned}$$

be the set of possible integer matrices. Note that this set is finite. For every $N \in \mathcal{F}$ do the following:

1. Let $X := (\mathbb{1} - ue_1^\dagger)(\ln\odot(P) - 2\pi i N)(\mathbb{1} - e_1u^\dagger)$.
2. Check if X is positive semidefinite or not.

(a) If it is positive semidefinite, then Theorem 3.1 (we are using an alternate but equivalent version of the condition in Eq. 3.19 for convenience) guarantees that you can write your matrix as a Gram matrix of multi-mode coherent states. Moreover, these coherent states can be found by using the columns of $X^{1/2}$ (this can be seen through the proof of Lemma 3.1). If

$$X^{1/2} = (\alpha_1 \ \alpha_2 \cdots \alpha_n)$$

where $\alpha_i \in \mathbb{C}^n$ for each $i \in [n]$, then we have $P = G(e^{i\phi_1}\|\alpha_1\rangle\!\rangle, e^{i\phi_2}\|\alpha_2\rangle\!\rangle, \cdots, e^{i\phi_n}\|\alpha_n\rangle\!\rangle)$ for $\phi_i := -\text{Im}\{\ln P_{i1}\}$ for each $i \in [n]$.

(b) If it is not positive semidefinite, move to the next integer matrix in $\mathcal{F}$.

Finally, if X is not positive semidefinite for any of the integer matrices $N \in \mathcal{F}$, then $P \notin G(\mathscr{C}_n^n)$.

Remark: If we replace e_1 with u/n in the above algorithm, then X and $X^{1/2}$ will have rank at most $(n-1)$, which means that one could in fact choose vectors in $\mathbb{C}^{n-1}$ to satisfy Eq. 3.2. Thus, we can choose $(n-1)-$mode coherent states to construct any matrix in $G(\mathscr{C}_n^n)$ or, $G(\mathscr{C}_n^n) = G(\mathscr{C}_{n-1}^n)$. One can also see this through Lemma 3.2, which allows us to reduce the rank of the amplitude vectors by at least 1. We state this result as Corollary 3.3, a slightly strengthened form of Corollary 3.1.

Corollary 3.3. *For $n, m \in \mathbb{N}$ and $n \geq 2$, $G\left(\mathscr{C}_{n-1+m}^n\right) = G\left(\mathscr{C}_{n-1}^n\right)$.*

However, we will continue to use $G\left(\mathscr{C}_n^n\right)$ to represent the Gram matrices of n multi-mode coherent states for notational convenience.

Since, it seems hard to decide if a Gram matrix P lies in $G(\mathscr{C}_n^n)$ or not, we provide two Corollaries, which would be helpful in deciding this question in certain cases. Both of these rely on the fact that it is easy to check if a matrix is a Euclidean distance matrix (EDM) (see Eq. 3.21).

Corollary 3.4. *If $P \in G(\mathscr{C}_n^n)$, then the matrix $R := [\ln(|P_{ij}|)]_{ij}$ is a Euclidean distance matrix ($\ln$ function considered here is the real logarithm function).*

Proof. If $P \in G(\mathscr{C}_n^n)$, then for every $i, j \in [n]$

$$\ln(|P_{ij}|) = -\frac{1}{2}\|\alpha_i - \alpha_j\|_2^2 \tag{3.23}$$

for some complex vectors, $\{\alpha_k\}_{k=1}^n \subset \mathbb{C}^n$. Define, a $2n$- dimensional vector $\beta_i := (\text{Re}\{\alpha_i\}, \text{Im}\{\alpha_i\})$ for every $i \in [n]$. These vectors would also satisy Eq. 3.23. Further these can be rotated into a n-dimensional space using an orthogonal matrix, which would leave the distance between these vectors invariant. Hence, the matrix R would be an EDM. □

One may wonder if the converse also holds in Corollary 3.4, i.e., given that for a Gram matrix P, the matrix $R := [\ln(|P_{ij}|)]_{ij}$ is a Euclidean distance matrix, does this imply $P \in G(\mathscr{C}_n^n)$? This is seen not to be the case. A counterexample is the Gram matrix of three equiangular vectors in two dimensions,

$$P = \begin{pmatrix} 1 & -0.5 & -0.5 \\ -0.5 & 1 & -0.5 \\ -0.5 & -0.5 & 1 \end{pmatrix}.$$

The matrix $R := [\ln(|P_{ij}|)]_{ij}$ in this case is an EDM, but one can use the algorithm based on Theorem 3.1 to show that $P \notin G(\mathscr{C}_n^n)$. However, the converse does hold when all the elements of the Gram matrix P are real and positive.

Corollary 3.5. *If $P \in Herm(\mathbb{C}^n)$ and $P_{ij} \in \mathbb{R}$ and $P_{ij} > 0$ for every $i, j \in [n]$, then $P \in G(\mathscr{C}_n^n)$ if an only if $\ln \odot P$ is a Euclidean distance matrix ($\ln$ function considered here is the real logarithm function).*

Proof. The fact that if $P \in G(\mathscr{C}_n^n)$ then $\ln \odot P$ is a Euclidean distance matrix can be seen using Corollary 3.4 in this case. For the other direction, since $\ln \odot P$ is an EDM, we can choose vectors $\{\alpha_i\}_{i=1}^n \subset \mathbb{R}^n$ such that for every $i, j \in [n]$

$$\begin{aligned} \ln P_{ij} &= -\frac{1}{2}\|\alpha_i - \alpha_j\|_2^2 \\ \Leftrightarrow P_{ij} &= \exp\left(-\frac{1}{2}\|\alpha_i - \alpha_j\|_2^2\right), \end{aligned}$$

which implies that $P = G(\|\alpha_1\rangle\rangle, \cdots, \|\alpha_n\rangle\rangle)$ using the fact that α_i are real vectors and Eq. 3.3. □

We can also connect our work to the coherent state mapping presented in Ref. [39]. We will assume that the entries of the Gram matrix, P are close to 1 (and $P_{ii} = 1$ for all $i \in [n]$). That is, the angles between the vectors forming the Gram matrix are small. In order to recreate this Gram matrix using multi-mode coherent states, we need to find amplitude vectors, $\{\alpha_i\}_{i=1}^n \subset \mathbb{C}^n$, a phase vector, $\phi \in \mathbb{R}^n$ and an integer matrix such that Eq. 3.19 is satisfied. We choose the $[-\pi, \pi)$ branch of the $\ln$ function. Further, for convenience we assume that no element of P lies on the negative real axis. In this case, $\ln \odot P$ is Hermitian, with zero diagonal. We will choose, $\{\alpha_i\}_{i=1}^n \subset \mathbb{C}^n$, such that $\|\alpha_i\|_2 = 1$ for all $i \in [n]$, $\phi = 0$, and $N = 0$. For these choice, we need $\{\alpha_i\}_{i=1}^n$ satisfying

$$\begin{aligned} \ln(P_{ij}) &= -\frac{1}{2}\left(\|\alpha_i\|_2^2 + \|\alpha_j\|_2^2 - 2\langle\alpha_i, \alpha_j\rangle\right) + i\left(\phi_j - \phi_i\right) \\ &= -\frac{1}{2}\left(2 - 2\langle\alpha_i, \alpha_j\rangle\right). \end{aligned}$$

Using the assumption that the entries of P are close to 1,

$$\begin{aligned} P_{ij} - 1 + O((P_{ij} - 1)^2) &= -1 + \langle\alpha_i, \alpha_j\rangle \\ \Rightarrow P_{ij} &\approx \langle\alpha_i, \alpha_j\rangle. \end{aligned}$$

Thus, the problem of finding coherent states in this case reduces to finding unit vectors forming the Gram matrix, P. This can be done easily by choosing $\{\alpha_i\}_{i=1}^n$ to be the columns of B for any B such that $P = B^\dagger B$. Ref. [39] studies exactly this mapping of qudit states ($\{\alpha_i\}_i$) to multi-mode coherent states ($\{\|\alpha_i\rangle\!\rangle\}_i$). Our results show that this is indeed well motivated.

3.3 Closure of the set of Gram matrices of multi-mode coherent states

The set of Gram matrices of n multi-mode coherent states, $G(\mathscr{C}_n^n)$ is not closed. For example, one may construct Gram matrices arbitrarily close to the identity matrix using coherent states, but the identity matrix itself cannot be constructed, since the inner products between any two coherent states is never zero. In this section, we will characterize the closure of $G(\mathscr{C}_n^n)$, which we will represent as $G(\overline{\mathscr{C}_n^n})$. This set consists of the Gram matrices which can be approximated arbitrarily well using Gram matrices of coherent states. Experimentally $G(\overline{\mathscr{C}_n^n})$ is more relevant than $G(\mathscr{C}_n^n)$. One expects that block diagonal Gram matrices, where each of the blocks is a Gram matrix of coherent states, would lie in $G(\overline{\mathscr{C}_n^n})$. Each block could be realized by the set of corresponding coherent states, and one could displace the amplitudes between the sets relative to each other with a sufficiently large amplitude vector to achieve this. In fact, we will show that all the matrices in $G(\overline{\mathscr{C}_n^n})$ can be put into such a block diagonal form. To prove this, we will require two intermediate results, Lemmas 3.3 and 3.4. Lemma 3.3 relates the distance between the amplitude vectors of two coherent states with their inner-product with each other and a third coherent state. Lemma 3.4 shows that if a Gram matrix with non-zero entries belongs in $G(\overline{\mathscr{C}_n^n})$, then it also belongs in $G(\mathscr{C}_n^n)$. Together these two will allow us to characterize $G(\overline{\mathscr{C}_n^n})$.

Lemma 3.3. *If $\|\alpha\rangle\!\rangle, \|\beta\rangle\!\rangle, \|\gamma\rangle\!\rangle \in \mathscr{C}_n$, are such that $|\langle\|\alpha\rangle\!\rangle, \|\beta\rangle\!\rangle\rangle| = p_{\alpha\beta}$ and $|\langle\|\alpha\rangle\!\rangle, \|\gamma\rangle\!\rangle\rangle| = p_{\alpha\gamma}$, then*

$$\begin{aligned}(-2\ln p_{\alpha\gamma})^{1/2} + (-2\ln p_{\alpha\beta})^{1/2} &\geq \|\beta - \gamma\|_2 \\ &\geq \left|(-2\ln p_{\alpha\gamma})^{1/2} - (-2\ln p_{\alpha\beta})^{1/2}\right|. \end{aligned} \tag{3.24}$$

Proof. From Eq. 3.3, the following can be deduced:

$$\begin{aligned}\|\alpha - \beta\|_2 &= (-2\ln(p_{\alpha\beta}))^{1/2} \\ \|\alpha - \gamma\|_2 &= (-2\ln(p_{\alpha\gamma}))^{1/2}.\end{aligned}$$

To establish the lower bound, we use the triangle inequality in the following manner.

$$\begin{aligned}\|\gamma - \beta\|_2 &= \|\,(\gamma - \alpha) - (\beta - \alpha)\,\|_2 \\ &\geq |\|\gamma - \alpha\|_2 - \|\beta - \alpha\|_2| \\ &\geq |\,(-2\ln p_{\alpha\gamma})^{1/2} - (-2\ln p_{\alpha\beta})^{1/2}\,|\end{aligned}$$

We use the triangle inequality again to establish the upper bound.

$$\begin{aligned}\|\gamma - \beta\|_2 &\leq \|\gamma - \alpha\|_2 + \|\beta - \alpha\|_2 \\ &= (-2\ln p_{\alpha\gamma})^{1/2} + (-2\ln p_{\alpha\beta})^{1/2}\end{aligned}$$

□

Before we go on further, we would like to point out that if $P \in G(\mathscr{C}_n^n)$, then $P_{ij} \neq 0$ for all $i, j \in [n]$. This can be seen from Eq. 3.2. In the lemma that follows, we prove that if a matrix with non-zero entries belongs in $\overline{G(\mathscr{C}_n^n)}$, then it also belongs in $G(\mathscr{C}_n^n)$.

Lemma 3.4. *For $P \in L(\mathbb{C}^n)$ such that $P_{ii} = 1$ for all $i \in [n]$, if $P_{ij} \neq 0$ for all $i, j \in [n]$, then $P \in \overline{G(\mathscr{C}_n^n)}$ if and only if $P \in G(\mathscr{C}_n^n)$.*

Proof. $P \in G(\mathscr{C}_n^n)$ implies $P \in \overline{G(\mathscr{C}_n^n)}$ is trivial. For the other direction, we have that, if $P \in \overline{G(\mathscr{C}_n^n)}$, then there exists a sequence, $\{P_k\}_{k=1}^{\infty} \subseteq G(\mathscr{C}_n^n)$ such that $\lim_k P_k = P$ under the 2-norm (where the 2-norm, $\|\cdot\|_2$ is defined as $\|X\|_2 = (\mathrm{Tr}(X^\dagger X))^{1/2}$; all norms are equivalent in a finite dimensional space [40], so we can choose the 2-norm without loss of generality). Firstly, observe that $P \in \mathrm{Pos}(\mathbb{C}^n)$ and that $P_{ii} = 1$ for all $i \in [n]$, since these sets are closed. Moreover, this implies the existence of integer matrices, $\{N_k\}_{k=1}^{\infty} \subset \mathbb{Z}^{n\times n}$, for which each $(\ln \odot(P_k) - 2\pi i N_k) \in \mathrm{Herm}(\mathbb{C}^n)$, $2\pi i (N_k)_{ii} = \ln(1)$ for every i and such that for all $y \in \mathbb{C}^n$, $\langle u, y\rangle = 0$ (we are using an alternate characterization of Theorem 3.1; see Lemma 3.1, Statement V)

$$y^\dagger(\ln \odot(P_k) - 2\pi i N_k)y \geq 0.$$

Further, we can assume that for all i, j:

$$(N_k)_{ij} \in \mathbb{Z} \cap \left[\frac{\beta}{2\pi} - \frac{1}{\pi}|\ln(\delta_k)| - 1, \frac{\beta}{2\pi} + \frac{1}{\pi}|\ln(\delta_k)| + 2\right)$$

where $\delta_k := \min_{i,j} |(P_k)_{ij}|$, and the branch of the function $\ln$ is chosen such that it is continuous at P_{ij} for every $i, j \in [n]$. Before we proceed further, we show that for sufficiently large k we can restrict the choice of matrices, N_k to a finite set.

Claim: For the sequence, $\{P_k\}_{k=1}^{\infty}$ and integer matrices $\{N_k\}_{k=1}^{\infty}$ as described above, there exists $M \in \mathbb{N}$, such that for all $k \geq M$ and for all $i, j \in [n]$, we have

$$(N_k)_{ij} \in \mathbb{Z} \cap \left[\frac{\beta}{2\pi} - \frac{1}{\pi}|\ln(\frac{\delta}{2})| - 1, \frac{\beta}{2\pi} + \frac{1}{\pi}|\ln(\frac{\delta}{2})| + 2\right),$$

where $\delta := \min_{i,j} |P_{ij}|$. This essentially says that the range of elements of N_k can be made independent of k.

Proof of claim: Since, $\delta \neq 0$ and the elements $(P_k)_{ij} \to P_{ij}$ for every $i, j \in [n]$, we can choose M such that for all $k \geq M$ and $i, j \in [n]$

$$\begin{aligned} &| \, |(P_k)_{ij}| - |P_{ij}| \, | < \frac{\delta}{2} \\ \Rightarrow \; & |P_{ij}| - \frac{\delta}{2} < |(P_k)_{ij}| \\ \Rightarrow \; & \delta - \frac{\delta}{2} < |(P_k)_{ij}| \\ \Rightarrow \; & \frac{\delta}{2} < |(P_k)_{ij}|. \end{aligned}$$

Since, this is true for all $i, j \in [n]$, for every $k \geq M$ we have

$$\frac{\delta}{2} < \min_{i,j} |(P_k)_{ij}| = \delta_k.$$

Using the fact that $|\ln(x)|$ is decreasing for $x \in (0, 1]$, we see that

$$\left[\frac{\beta}{2\pi} - \frac{1}{\pi}|\ln(\delta_k)| - 1, \frac{\beta}{2\pi} + \frac{1}{\pi}|\ln(\delta_k)| + 2\right)$$

is a subset of

$$\left[\frac{\beta}{2\pi} - \frac{1}{\pi}|\ln(\frac{\delta}{2})| - 1, \frac{\beta}{2\pi} + \frac{1}{\pi}|\ln(\frac{\delta}{2})| + 2\right).$$

This proves the claim for M as chosen above. ■

Now, we only consider the infinite sequence of matrices, $\{P_k : k \geq M\}$, where M is the number as defined in the claim above. Observe that the integer matrix corresponding to each of these matrices, N_k, is chosen from the finite set of matrices,

$$\begin{aligned} \mathcal{F} :=& \{N \in \mathbb{Z}^{n \times n} | \text{ for all } i, j \in [n] : \\ & \frac{\beta}{2\pi} - \frac{1}{\pi}|\ln(\frac{\delta}{2})| - 1 \leq N_{ij} < \frac{\beta}{2\pi} + \frac{1}{\pi}|\ln(\frac{\delta}{2})| + 2\}. \end{aligned}$$

We can write

$$\mathcal{F} = \{K_1, K_2, \cdots, K_l\}$$

for some $l \in \mathbb{N}$ to emphasize the fact that its finite. Since, this set is finite and the sequence $(N_k)_k$ is infinite, there exists a $p \in [l]$ such that $N_k = K_p$ for infinitely many k. Define $K := K_p$ for convenience. We choose a subsequence of $\{P_k : k \geq M\}$, $\{P_{k_t}\}_{t=1}^{\infty}$ such that $N_{k_t} = K$ for all $t \geq 1$. Also, as this is a subsequence of $\{P_k\}_k$, $P_{k_t} \to P$. Now, observe that for every $y \in \mathbb{C}^n$ such that $\langle u, y \rangle = 0$ and for all $t \geq 1$,

$$y^\dagger(\ln \odot(P_{k_t}) - 2\pi i K)y \geq 0.$$

This implies that for such a vector, y,

$$\begin{aligned}
&\lim_{t\to\infty} y^\dagger(\ln\odot(P_{k_t}) - 2\pi i K)y \geq 0\\
&\Rightarrow\ y^\dagger(\ln\odot(\lim_{t\to\infty}(P_{k_t})) - 2\pi i K)y \geq 0\\
&\Rightarrow\ y^\dagger(\ln\odot(P) - 2\pi i K)y \geq 0,
\end{aligned}$$

where we have used the fact that K is a constant and the functions– $f_y(X) = y^\dagger X y$, and $f(X) = \ln\odot X$ are continuous. The $\ln\odot X$ function is continuous because we chose the branch of the $\ln$ function such that no element of P lay on the branch cut. Further, $2\pi i(K)_{ii} = \ln(1)$ for every i, since $K = N_k$ for some k, and $\ln\odot(P) - 2\pi i K = \lim_{t\to\infty}(\ln\odot(P_{k_t}) - 2\pi i K) \in \text{Herm}(\mathbb{C}^n)$, because the set of Hermitian matrices is closed. Using an equivalent characterization of Theorem 3.1, this proves our claim. □

We need one final notion to characterize $\overline{G(\mathscr{C}_n^n)}$. Observe that if

$$\begin{aligned}
&G(v_1,\cdots,v_n) \in G(\mathscr{C}_n^n), \text{ then}\\
&G(v_{\pi^{-1}(1)},\cdots,v_{\pi^{-1}(n)}) = P_\pi G(v_1,\cdots,v_n)P_\pi^\dagger \in G(\mathscr{C}_n^n),
\end{aligned} \tag{3.25}$$

for any permutation π (where P_π represents the permutation matrix associated with π). If one can construct a Gram matrix, Q using coherent states, then all one needs to do to construct the Gram matrix, $P_\pi Q P_\pi^\dagger$ is to permute the order of the coherent states forming Q by π. Therefore, $Q \in G(\mathscr{C}_n^n)$ is equivalent to $P_\pi Q P_\pi^\dagger \in G(\mathscr{C}_n^n)$. In fact, because of the isometric invariance [16] of the 2-norm, $Q \in \overline{G(\mathscr{C}_n^n)}$ is equivalent to $P_\pi Q P_\pi^\dagger \in \overline{G(\mathscr{C}_n^n)}$. We can use this fact to simplify our analysis of matrices in $\overline{G(\mathscr{C}_n^n)}$. In the rest of the chapter, we will refer to a Gram matrix of the form, $Q' = G(v_{\pi^{-1}(1)}, v_{\pi^{-1}(2)},\cdots,v_{\pi^{-1}(n)})$ as a rearrangement of the vectors forming the Gram matrix, $Q = G(v_1, v_2,\cdots,v_n)$.

Theorem 3.2. *A matrix, $P \in L(\mathbb{C}^n)$, is a member of $\overline{G(\mathscr{C}_n^n)}$ if and only if P can be written as*

$$P_\pi P P_\pi^\dagger = \bigoplus_{i=1}^{m} P_i = \begin{pmatrix} P_1 & & & \\ & P_2 & & \\ & & \ddots & \\ & & & P_m \end{pmatrix} \tag{3.26}$$

where, $\bigoplus_{i=1}^m P_i$ represents a direct sum of matrices, $\{P_i\}_{i=1}^m$ and for each $i \in [m]$, $P_i \in G(\mathscr{C}_{n_i}^{n_i})$ for some $n_i \in \mathbb{N}$, and P_π is a permutation matrix.

In other words, $P \in \overline{G(\mathscr{C}_n^n)}$ if and only if up to a rearrangement of the vectors forming it, P can be written as a block-diagonal matrix where each block is a Gram matrix that can be realized by multi-mode coherent states.

Proof. We will first prove that if $P \in \overline{G(\mathscr{C}_n^n)}$, then it has the aforementioned block diagonal form. This will be done in two steps. In the first step, we will establish two properties of elements of such a matrix, P. In the second step, which primarily relies on linear algebra, we will show that these two properties suffice to prove that the matrix, P, has the required block diagonal structure.

Step 1: For a $P \in \overline{G(\mathscr{C}_n^n)}$, and indices $i, k \in [n]$ such that $P_{ik} \neq 0$ we will prove that, if $j \in [n]$ such that $P_{ij} = 0$, then $P_{kj} = 0$ and if $j \in [n]$ such that $P_{ij} \neq 0$, then $P_{kj} \neq 0$. The idea is that if two multi-mode coherent states have a non-zero inner product then their amplitude vectors have to be a finite distance away from each other, but if their inner product approaches zero then the distance between these vectors has to grow infinitely large.

We will first show that if $P_{ik} \neq 0$ and $j \in [n]$ such that $P_{ij} = 0$, then $P_{kj} = P_{jk} = 0$. To prove this pick a sequence, $\{P_u\}_{u=1}^{\infty} \subseteq G(\mathscr{C}_n^n)$ such that,

$$\lim_{u \to \infty} P_u = P.$$

Here, we once again consider the 2-norm without any loss of generality. Observe that this is equivalent to

$$\lim_{u \to \infty} (P_u)_{ab} = P_{ab}$$

for all $a, b \in [n]$. Since, $P_u \in G(\mathscr{C}_n^n)$, there exist multi-mode coherent states, $\{e^{i\phi_{ui}} \| \alpha_i^u \rangle\!\rangle\}_{i=1}^n \subseteq \mathscr{C}_n$, such that $(P_u)_{ab} = \left\langle e^{i\phi_{ua}} \| \alpha_a^u \rangle\!\rangle, e^{i\phi_{ub}} \| \alpha_b^u \rangle\!\rangle \right\rangle$ for all $a, b \in [n]$. Using Lemma 3.3, we have,

$$\begin{aligned}
\left(-2 \ln |(P_u)_{jk}|\right)^{1/2} &= \|\alpha_k^u - \alpha_j^u\|_2 \\
&\geq \left(-2 \ln |(P_u)_{ij}|\right)^{1/2} - \left(-2 \ln |(P_u)_{ik}|\right)^{1/2}.
\end{aligned}$$

Taking the limit, $u \to \infty$, we have

$$\begin{aligned}
\lim_{u \to \infty} \left(-2 \ln |(P_u)_{jk}|\right)^{1/2} &\geq \left(-2 \ln \lim_{u \to \infty} |(P_u)_{ij}|\right)^{1/2} \\
&\quad - \left(-2 \ln \lim_{u \to \infty} |(P_u)_{ik}|\right)^{1/2} \\
&\geq \left(-2 \ln \lim_{u \to \infty} |(P_u)_{ij}|\right)^{1/2} \\
&\quad - \left(-2 \ln |P_{ik}|\right)^{1/2},
\end{aligned}$$

where we have used the continuity of $|\cdot|$, $\ln(\cdot)$, and $(\cdot)^{1/2}$ functions. The limit on the RHS tends to ∞ since $\lim_{u \to \infty} |(P_u)_{ij}| = |P_{ij}| = 0$ and $P_{ik} \neq 0$, therefore

$$\begin{aligned}
&\left(-2 \ln \lim_{u \to \infty} |(P_u)_{jk}|\right)^{1/2} = \infty \\
&\Rightarrow \lim_{u \to \infty} |(P_u)_{jk}| = |P_{jk}| = 0.
\end{aligned}$$

Hence, for $P_{ik} \neq 0$, and for every $j \in [n]$ such that $P_{ij} = 0$,

$$P_{kj} = P_{jk} = 0. \tag{3.27}$$

since, P is Hermitian.

Now, we will prove that given $P_{ik} \neq 0$, if for $j \in [n]$ $P_{ij} \neq 0$, then $P_{kj} \neq 0$. For j such that $P_{ij} \neq 0$, using the upper bound given in Lemma 3.3, we have

$$\begin{aligned}\left(-2\ln\left|\left(P_u\right)_{jk}\right|\right)^{1/2} &= \|\alpha_k^u - \alpha_j^u\|_2 \\ &\leq \left(-2\ln\left(|(P_u)_{ki}|\right)\right)^{1/2} + \left(-2\ln\left(|(P_u)_{ij}|\right)\right)^{1/2}.\end{aligned}$$

Taking the limit, $u \to \infty$, we have

$$\begin{aligned}\lim_{u\to\infty}\left(-2\ln\left|\left(P_u\right)_{jk}\right|\right)^{1/2} &\leq \lim_{u\to\infty}\left(-2\ln\left(|(P_u)_{ki}|\right)\right)^{1/2} \\ &\qquad + \lim_{u\to\infty}\left(-2\ln\left(|(P_u)_{ij}|\right)\right)^{1/2} \\ &\leq \left(-2\ln|P_{ki}|\right)^{1/2} \\ &\qquad + \left(-2\ln|P_{ij}|\right)^{1/2} =: M < \infty\end{aligned}$$

where we have defined M to be the upper bound. This gives us

$$|P_{jk}| \geq \exp\left(-\frac{1}{2}M^2\right) > 0.$$

Therefore, for $P_{ik} \neq 0$ and $j \in [n]$ such that $P_{ij} \neq 0$, we have

$$P_{jk} = P_{kj}^* \neq 0. \tag{3.28}$$

Therefore, we have proven that for any $n \in \mathbb{N}$, a matrix, $P \in \overline{G(\mathscr{C}_n^n)}$, and i, j, and $k \in [n]$ Eq. 3.27 and Eq. 3.28 hold. These two properties are sufficient to establish the block diagonal structure of P.

Step 2: We will use induction on the size of the Gram matrices to prove the statement that if $P \in \overline{G(\mathscr{C}_n^n)}$, then P has the block diagonal form given in Eq. 3.26, up to a rearrangement of the vectors forming it. First observe that since the sets, $\{X \in \mathrm{L}(\mathbb{C}^n) : X_{ii} = 1 \text{ for all } i \in [n]\}$ and $\mathrm{Pos}(\mathbb{C}^n)$ are closed, P will belong in these sets. The induction hypothesis is clearly true for $n = 1$ as $P = (1)$ is the only Gram matrix in this case and $P = G(\|0\rangle\rangle)$. We assume that our hypothesis is true for all $p \leq n$. For $P \in \overline{G(\mathscr{C}_{n+1}^{n+1})}$, P can always be put into the form

$$P = \begin{pmatrix} P' & x \\ x^\dagger & 1 \end{pmatrix}$$

where $x \in \mathbb{C}^n$. It can be shown that $P' \in \overline{G(\mathscr{C}_n^n)}$. Since, P is positive semidefinite, we can write $P = G(v_1, v_2, \cdots, v_{n+1})$ for vectors, $\{v_i\}_{i=1}^{n+1}$. Then, $P' = G(v_1, v_2, \cdots, v_n)$. By the induction hypothesis, there exists a permutation, π such that

$$P_\pi P' P_\pi^\dagger = G(v_{\pi^{-1}(1)}, \cdots, v_{\pi^{-1}(n)}) = \begin{pmatrix} P_1' & & & \\ & P_2' & & \\ & & \ddots & \\ & & & P_m' \end{pmatrix} \tag{3.29}$$

where for every $i \in [m]$, $P_i' \in G(\mathscr{C}_{n_i}^{n_i})$ for some n_i. We can transform P as

$$P \longrightarrow \begin{pmatrix} P_\pi & 0 \\ 0 & 1 \end{pmatrix} P \begin{pmatrix} P_\pi^\dagger & 0 \\ 0 & 1 \end{pmatrix}$$

and prove our claim for this matrix without loss of generality. So, from now on we will assume that P is block diagonal in the first $n \times n$ entries.

If for every $i \in [n]$, $P_{(n+1)i} = 0$, then our matrix is already in the required block diagonal form. So, we will assume that there exists $i \in [n]$ such that $P_{(n+1)i} \neq 0$. Observe that the block structure of the first $n \times n$ entries divides the vectors forming the Gram matrix into orthogonal subspaces. So, we may associate a subspace with each Gram matrix, P_l' (Eq. 3.29). Further assume without loss of generality that the vector, v_i (where $P = G(v_1, v_2, \cdots, v_{n+1})$) is in the subspace associated with the Gram matrix, P_m' (if not one can always permute the vectors forming P such that this is true). Then using the fact that for all j such that $P_{ij} = 0$, $P_{(n+1)j} = 0$ (Eq. 3.27), one can see that P also has a block diagonal form if one includes the $(n+1)^{\text{th}}$ row and column in P_m' (See Fig. 3.1 for a schematic representation of this fact). We will call this new last block P_m. All the other blocks remain the same.

Furthermore, for every $l \in [m-1]$, $P_l' \in G(\mathscr{C}_{n_l}^{n_l})$, and if we prove that the new block, P_m belongs in $G(\mathscr{C}_{n_m+1}^{n_m+1})$ then we would be done. Observe that $P_m' \in G(\mathscr{C}_{n_m}^{n_m})$, which means that $(P_m')_{uv} \neq 0$ for all $u, v \in [n_m]$. In addition, using Eq. 3.28, we can show that for all $u, v \in [n_m + 1]$, $(P_m)_{uv} \neq 0$. Moreover, $P_m \in \overline{G(\mathscr{C}_{n_m+1}^{n_m+1})}$. Using Lemma 3.4, these two imply that $P_m \in G(\mathscr{C}_{n_m+1}^{n_m+1})$. Therefore, if $P \in \overline{G(\mathscr{C}_n^n)}$, then P has the block diagonal form given in Eq. 3.26, up to a rearrangement of the vectors forming it.

We will prove the converse of the statement by construction. We will present a construction for Gram matrices with 2 blocks, which can be generalised to m blocks easily. Suppose, we have $P_1 \in G(\mathscr{C}_{n_1}^{n_1})$ and $P_2 \in G(\mathscr{C}_{n_2}^{n_2})$, then we wish to prove that

$$P = \begin{pmatrix} P_1 & \\ & P_2 \end{pmatrix} \in G(\mathscr{C}_n^n)$$

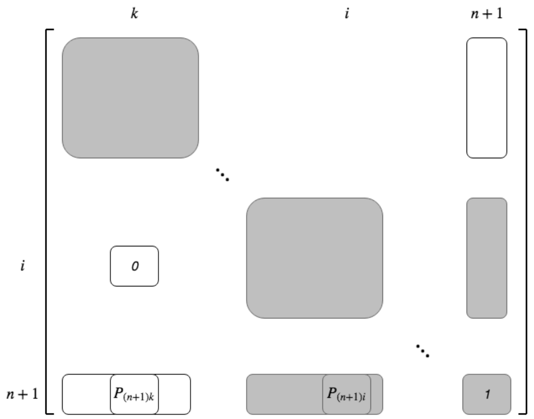


Figure 3.1: In this figure, we schematically represent the matrix, $P \in \overline{G(\mathscr{C}_{n+1}^{n+1})}$, which is diagonal in its first $n \times n$ entries. We consider the case where $P_{(n+1)i} \neq 0$. The facts proved in Step 1 of the proof show that the zero (white) and non-zero (gray) terms in the i^{th}-row (column) coincide with zero and non-zero terms respectively in the $(n+1)^{\text{th}}$-row (column).

for $n = n_1 + n_2$.
For $i = 1, 2$ let the multi-mode coherent states, $\left\{e^{i\phi_{ij}} \| \alpha_j^i \rangle\!\rangle\right\}_{j=1}^{n_i}$ be such that

$$(P_i)_{uv} = \left\langle e^{i\phi_{iu}} \| \alpha_u^i \rangle\!\rangle, e^{i\phi_{iv}} \| \alpha_v^i \rangle\!\rangle \right\rangle .$$

There are at least two ways in which this can be accomplished. One way would be to put both the sets of amplitude vectors into the same space, say $\mathcal{X} = \mathbb{C}^{n'}$ for $n' = \max\{n_1, n_2\}$, and to displace one of the sets by a large amplitude vector, $A \in \mathcal{X}$. This way the inner products of the coherent states belonging to the same set of states remains invariant for appropriately defined phases, but the inner product of the coherent states belonging to different sets would tend to zero as the norm of the vector, A, tends to ∞. The second way, which we present here, is similar but it puts the amplitude vectors in different subspaces, and makes the distance between these subspaces go to ∞.

We will define multi-mode coherent states $\{e^{i\Phi_j} \| \beta_j(A) \rangle\!\rangle\}_{j=1}^{n}$ dependent on a parameter, $A \in \mathbb{R}$, such that their Gram matrix will approach P as $A \to \infty$. Define,

$$n := n_1 + n_2$$

and,

$$\begin{aligned} &\{\beta_j(A)\}_{j=1}^{n} \subset (\mathbb{C}^{n_1} \oplus \mathbb{C}^{n_2}) \oplus (\mathbb{C} \oplus \mathbb{C}) \\ &\{\Phi_j\}_{j=1}^{n} \subset \mathbb{R} \end{aligned}$$

such that for each $j \in [n]$,

$$\beta_j(A) := \begin{cases} \alpha_j^1 \oplus 0 \oplus A \oplus 0 & j \leq n_1 \\ 0 \oplus \alpha_{j'}^2 \oplus 0 \oplus A & j' = j - n_1 > 0 \end{cases}$$
$$\Phi_j := \begin{cases} \phi_{1j} & j \leq n_1 \\ \phi_{2j'} & j' = j - n_1 > 0 \end{cases}$$

Given these, one can check that the following hold for $u, v \in [n_1]$

$$\begin{aligned} &\|\beta_u(A) - \beta_v(A)\|_2^2 = \|\alpha_u^1 - \alpha_v^1\|_2^2 \\ &\text{Im}\left\{\langle \beta_u(A), \beta_v(A)\rangle\right\} = \text{Im}\left\{\langle \alpha_u^1, \alpha_v^1\rangle\right\} \\ &\Phi_u - \Phi_v = \phi_{1u} - \phi_{1v}, \end{aligned}$$

whic imply that,

$$\langle e^{i\Phi_u}\|\beta_u(A)\rangle\rangle, e^{i\Phi_v}\|\beta_v(A)\rangle\rangle\rangle = \langle e^{i\phi_{1u}}\|\alpha_u^1\rangle\rangle, e^{i\phi_{1v}}\|\alpha_v^1\rangle\rangle\rangle.$$

Similar relations hold for the case when $u, v > n_1$, although one needs to replace u with $u' = u - n_1$ and v with $v' = v - n_1$ on the RHS of these equations. For $u \leq n_1$ and $v > n_1$, we have

$$\begin{aligned} &\|\beta_u(A) - \beta_v(A)\|_2^2 = \|\alpha_u^1\|_2^2 + \|\alpha_{v'}^2\|_2^2 + 2A^2 \geq 2A^2 \\ &\Rightarrow |\langle e^{i\Phi_u}\|\beta_u(A)\rangle\rangle, e^{i\Phi_v}\|\beta_v(A)\rangle\rangle\rangle| \leq \exp(-A^2). \end{aligned} \tag{3.30}$$

The matrix, $P(A) = G(e^{i\Phi_1}\|\beta_1(A)\rangle\rangle, \cdots, e^{i\Phi_n}\|\beta_n(A)\rangle\rangle)$ is a member of $G\left(\mathscr{C}_{n+2}^n\right)$ and also of $G\left(\mathscr{C}_n^n\right)$ (by Corollary 3.1) for every $A \in \mathbb{R}$. For this family of matrices, we have that

$$\lim_{A\to\infty} P(A) = \begin{pmatrix} P_1 & \\ & P_2 \end{pmatrix} \in \overline{G\left(\mathscr{C}_n^n\right)}.$$

This together with the observation that $P \in \overline{G(\mathscr{C}_n^n)} \Leftrightarrow P_\pi P P_\pi^\dagger \in \overline{G(\mathscr{C}_n^n)}$ for a permutation matrix, P_π, completes our proof.

□

We have proven here that an $n \times n$ Gram matrix can be approximated arbitrarily well using Gram matrices of multi-mode coherent states if and only it can be put into the form of Eq. 3.26. Moreover, we have also shown that if this is the case then we can approximate it using at most $n-$mode coherent states. During the proof of the converse of the theorem, we also suggest a way to construct such matrices, which would potentially require only $\max_i\{n_i\}$ number of modes (here n_i are the dimensions of the block diagonal matrices in Eq. 3.26). Secondly, one may wish to understand the energy requirements for approximating a Gram matrix up to an error, ϵ, using coherent states. In the proof for the converse presented here, the overlap between the states of two blocks decreases exponentially fast in the number of additional photons (Eq.

3.30). Therefore, we would only require $O(\log(1/\epsilon))$ additional photons to approximate a block diagonal Gram matrix.

We use this characterization of the closure of $G(\mathscr{C}_n^n)$ to show that one cannot arbitrarily approximate Gram matrices of mutually unbiased bases using multi-mode coherent states. Recall that two orthonormal sets of vectors, $\{|e_i\rangle\}_{i=1}^n$ and $\{|f_i\rangle\}_{i=1}^n$ are said to be mutally unbiased [41] if for every $i, j \in [n]$

$$|\langle |e_i\rangle , |f_j\rangle\rangle|^2 = \frac{1}{n}. \tag{3.31}$$

In standard literature, these sets are bases of $\mathbb{C}^n$. However, we relax this condition here and consider these to be sets of vectors in the infinite dimensional Fock space.

Example 3.2. *Gram matrices of mutually unbiased bases cannot be arbitrarily approximated using multi-mode coherent states*
Consider two mutually unbiased sets of vectors, $\mathcal{E} = \{|e_i\rangle\}_{i=1}^n$ and $\mathcal{F} = \{|f_i\rangle\}_{i=1}^n$ in the Fock space. $\mathcal{E}$ and $\mathcal{F}$ are orthonormal sets satisfying Eq. 3.31. For these vectors, define $P := G(|e_1\rangle , |e_2\rangle , \cdots , |e_n\rangle , |f_1\rangle , |f_2\rangle , \cdots , |f_n\rangle)$. Suppose, $P \in \overline{G(\mathscr{C}_{2n}^{2n})}$, then using the fact that $P_{ki} \neq 0$ and $P_{ji} \neq 0$ implies $P_{kj} \neq 0$ for such matrices (equivalent to Eq. 3.28 in Theorem 3.2), we have that since $P_{1(n+1)} = \langle |e_1\rangle , |f_1\rangle\rangle \neq 0$ and $P_{2(n+1)} = \langle |e_2\rangle , |f_1\rangle\rangle \neq 0$, $P_{12} = \langle |e_1\rangle , |e_2\rangle\rangle \neq 0$, which is a contradiction. Hence, $P \notin \overline{G(\mathscr{C}_{2n}^{2n})}$.

3.4 Conclusion

In this chapter, we successfully characterized the set of Gram matrices of multi-mode coherent states and its closure. We provided tests to check if a Gram matrix belongs to either of these sets. We proved that no more than $(n-1)$-modes are required to represent a Gram matrix of n-vectors. These results will hopefully serve as a toolbox for formulating quantum protocols in terms of coherent states, and facilitate their experimental implementation. They also add to our theoretical knowledge of coherent states, and completely describe sets of states attainable from them. We also expect our results to be beneficial towards understanding the kind of quantum resources a communication protocol requires.

Chapter 4

Optical quantum fingerprinting

4.1 Introduction

Quantum communication allows for exponential savings as compared to classical communication. This fact was demonstrated by Buhrman et al. [7] who gave a protocol requiring only $O(\log n)$ quantum communication for the Equality problem in the simultaneous message passing (SMP) model. This is exponentially smaller than the communication lower bound of $\Omega(\sqrt{n})$ for classical protocols solving the problem in the same model. Their protocol is referred to as the quantum fingerprinting protocol. Furthermore, this protocol is not merely a theoretical curiousity. It has been demonstrated experimentally in regimes where it requires lesser communication than any possible classical protocol. These experimental realizations were made possible by the reformulation of the protocol in terms of coherent states and linear optics.

This chapter will mainly deal with optical protocols in the simultaneous message passing (SMP) setting. We refer the reader to Section 2.6 for a description of this setting and the known results. This chapter consists of two parts. In the first part, we discuss our collaboration with experimentalists to demonstrate a quantum advantage in terms of *information loss* during the protocol. This is a much more difficult task compared to what has been previously done. The challenges encountered in the implementation of this experiment motivated us to look at the growth of resources in general protocols to solve the Equality problem. In the second part of the chapter, we study the tradeoff between the two resources expended during optically implemented SMP communication protocols: the duration of the protocol and the energy required to run it. We derive general bounds on the growth of these quantities which are valid for all optical protocols. Then, we develop tighter bounds for the growth of these resources for protocols implementing quantum fingerprinting with coherent states.

4.2 Experimental quantum fingerprinting

In this section, we describe our work with an experimental collaboration to implement the quantum fingerprinting protocol. The goal of the experiment is to beat the classical information leakage bound for the Equality problem. We helped the group to determine the correct parameter range for the experiment, as well as to figure out the optimal way to conduct the experiment. We describe the results used for this purpose, and the challenges faced during the experiment. This will lead us into a theoretical analysis of the growth of the resources required to conduct the experiment, which we shall cover in the next section.

4.2.1 Coherent state quantum fingerprinting protocol

We first recall the coherent state quantum fingerprinting (QFP) protocol given by Arrazola et al. in Ref. [12]. Let $E : \{0,1\}^n \to \{0,1\}^m$ be a classical error correcting code (ECC), such that for strings $x \neq y$, $h(E(x), E(y)) \geq \delta m$ (where h is the Hamming distance) for some $\delta > 0$ and $m = O(n)$. That is, the error correcting code guarantees us that the encodings for two different strings will differ for at least δ fraction of the strings. For a string $x \in \{0,1\}^n$, define the amplitude vector $\alpha_x \in \mathbb{C}^m$ as

$$(\alpha_x)_i := (-1)^{E(x)_i} \sqrt{\frac{\mu}{m}} \tag{4.1}$$

for every $i \in [m]$. The quantum fingerprinting protocol requires Alice and Bob to map their strings x and y to quantum states $|\psi_x\rangle$ and $|\psi_y\rangle$ such that whenever $x \neq y$, $|\langle\psi_x|\psi_y\rangle| < \gamma$ for some $\gamma < 1$. These amplitude vectors have been chosen such that the states $\{\|\alpha_x\rangle\rangle\}_{x\in\{0,1\}^n}$ satisfy this criterion. For $x \neq y$, we have $|\langle\|\alpha_x\rangle\rangle, \|\alpha_y\rangle\rangle\rangle| \leq e^{-2\mu\delta} < 1$. Now, we describe the quantum fingerprinting protocol which is based on these states.

Coherent state quantum fingerprinting protocol [12]:

1. Suppose Alice's input is x and Bob's input is y. Then, they prepare the states $\|\alpha_x\rangle\rangle$ and $\|\alpha_y\rangle\rangle$ for the amplitudes defined above in Eq. 4.1 and send them to the Referee.
2. The Referee performs an interference measurement on the two states he receives: the optical states are passed through a balanced beam splitter and the number of photons at the dark port is measured using a CCD detector [1].
3. If the number of photons measured is greater than a certain predetermined threshold μ_{th} the Referee concludes that the strings were different.

[1] The protocol given in Ref. [12] uses single photon detectors instead of CCD detectors

If the states received by the Referee in the above protocol are the same, then ideally he should not observe any photons in the dark port. However, due to experimental imperfections a certain threshold μ_{th} is set depending on the experimental parameters. The aforementioned description of the states $\{\|\alpha_x\rangle\rangle\}_x$ using Eq. 4.1 is only a particular example of possible fingerprinting states for the strings. If a quantum fingerprinting protocol uses coherent states as fingerprinting states, then we refer to it as *a coherent state QFP* protocol, while we refer to the above protocol as *the coherent state QFP* protocol.

4.2.2 Experimental QFP to beat the classical information leakage bound

The aim of our experiment is to implement the coherent state quantum fingerprinting protocol given in Ref. [12], and to beat the classical information leakage bound for the equality problem [34]. This protocol has been previously implemented in two different experiments [3, 11]. The experiment by Xu et al. [11] demonstrated that the coherent state QFP protocol required lesser communication than the best known classical protocol. Guan et al. [3] went a step further and showed that this protocol requires lesser communication than any possible classical protocol. Both these experiments focus on the communication complexity of the problem. They use the communication cost or the number of qubits required to perform the protocols as a measure of communication. For protocols, which use states in infinite dimensional Hilbert spaces like coherent states, the equivalent number of qubits, which would be required to approximate these states (using a tool like Theorem 4.2) are used to determine the communication cost of the protocols. In our experiment, we look at the information complexity of the problem instead. In Ref. [42], a measure of information transmission based on quantum Shannon theory called *quantum information leakage* was provided for this problem and it was theoretically shown the quantum protocol required exponentially lesser communication than the classical protocols. The aim of our experiment is to show that the coherent state QFP protocol can be used to provably beat the information leakage bound for classical protocol. As it turns out, it is much more difficult to do so. Our analysis reveals that the experiment has to be conducted for string lengths, which are almost two orders of magnitude larger than what the previous experiments did.

In the following subsection, we present the relevant definitions of quantum and classical information leakage in the SMP model. We also give the bounds for information leakage in the classical and the quantum settings. In the second subsection, we discuss the experiment and the techniques used to estimate the experimental parameters.

4.2.2.1 Information leakage for the equality problem

We begin by first defining the classical information leakage of a protocol in the SMP model. Intuitively, the information leakage of the protocol is the information leaked to the Referee by Alice and Bob about their inputs. This notion is formalised by considering the mutual information between Alice and Bob's messages, and their inputs.

Consider the protocol Π to compute the function f in the SMP model with error ϵ. Let the random variable X represent Alice's input, and Y represent Bob's input. Let R_R represent the private randomness of the Referee. Finally, suppose that M_A and M_B are the random variables representing messages sent by Alice and Bob to the Referee during the protocol Π. We then define the information leakage of the protocol as follows.

Definition 4.1 ([34]). The information leakage of the protocol Π on the input distribution $p \in P(X \times Y)$ is defined to be

$$\mathrm{IL}(\Pi, p) \coloneqq I(XY : M_A M_B R_R)$$

and the information leakage of the protocol Π is defined as

$$\mathrm{IL}(\Pi) \coloneqq \max_{p \in P(X \times Y)} \mathrm{IL}(\Pi, p).$$

The information leakage for computing f with error ϵ is defined as

$$\mathrm{IL}(f, \epsilon) \coloneqq \inf_{\Pi} \{\mathrm{IL}(\Pi)\}$$

where the infimum is over SMP protocols which compute f with error ϵ.

From early work [43] in the field of classical communication complexity, it is known that the information leakage of the Equality problem is at least $\Omega(\sqrt{n})$. Since, the quantum fingerprinting protocol given by Buhrman et al. uses only $O(\log n)$ qubits, the information leakage of such protocols is also bounded above by $O(\log n)$ (for coherent state protocol this is formally presented below). However, the classical lower bound proven in [43] is very weak, and it would be difficult to violate it experimentally. For this reason, Arrazola and Touchette proved a stronger lower bound in their paper [34], and it is this bound which we use in our experiment to determine the required string length. We state this bound as Theorem 4.1.

Theorem 4.1 ([34]). *For every $n \in \mathbb{N}$, $\epsilon > 0$, $\delta_1 > 0$ and $\delta_2 > 0$ satisfying $\epsilon + \delta_1 + \delta_2 < 0.5$, we have the following lower bound*

$$\mathrm{IL}(\mathrm{Eq}_n, \epsilon) \geq \delta_1 (2\sqrt{g_3(\epsilon + \delta_1 + \delta_2) n} - g_3(\epsilon + \delta_1 + \delta_2) - g_2(n, n, \delta_2) - 10) - g_1(2n) \tag{4.2}$$

with $g_1(x) = 2\log(x+1) + 10$, $g_2(x, y, z) = 2\log(\frac{2(x+y)}{z^2 \log(e)} + 1) + 2$ and $g_3(x) = 2\log(e)(0.5 - x)^2$.

Following the definition of information leakage for protocols in the classical SMP setting, we can define the *quantum information leakage* of a protocol in the quantum SMP setting. Suppose during a SMP protocol Π, Alice sends the quantum state σ_x^A to the Referee on input x and Bob sends the state η_y^B on input y. Further, suppose that p is the joint distribution over the inputs. In this case, the joint state of Alice, Bob and the Referee during the protocol is

$$\rho_{XYAB} \coloneqq \sum_{x,y} p(x,y) \left|x\right\rangle\left\langle x\right|^X \otimes \left|y\right\rangle\left\langle y\right|^Y \otimes \sigma_x^A \otimes \eta_y^B. \tag{4.3}$$

For this protocol, we define the quantum information leakage as follows.

Definition 4.2 ([42]). Given a quantum SMP protocol as described above, we define the quantum information leakage as

$$\mathrm{QIL}(\Pi) = \max_{p \in P(X \times Y)} I(XY : AB)_\rho \tag{4.4}$$

where ρ is the state described in Eq. 4.3.

In Ref. [12], Arrazola and Lütkenhaus show that one can arbitrarily approximate the coherent states $\{\|\alpha_x\rangle\!\rangle\}_x$ with constant mean photon number by quantum states living in a $O(\log(n))$ dimension Hilbert space. Their argument can be also extended to include coherent states with mean photon number below a certain value. This would be helpful later on. We state their result with this modification as Theorem 4.2.

Theorem 4.2 ([12]). *Let $\{\|\alpha_x\rangle\!\rangle\}_{x\in\{0,1\}^n}$ be a set of m-mode coherent states such that for every x, $\|\alpha_x\|_2^2 \leq \mu$. Then, for every $\epsilon > 0$, there exist a collection of states $\{|\Psi_x\rangle\}_{x\in\{0,1\}^n} \subset \mathcal{H}_d$ where $\log(\dim(\mathcal{H}_d)) = O(\mu \log(m))$ such that*

$$\|\,\|\alpha_x\rangle\!\rangle\langle\!\langle\alpha_x\| - |\Psi_x\rangle\langle\Psi_x|\,\|_1 \leq \epsilon$$

for every $x \in \{0,1\}^n$. In particular, if $m = O(n)$, then $\log(\dim(\mathcal{H}_d)) = O(\mu \log(n))$.

Proof. We provide a proof of this theorem in the Appendix A.2. □

This result can be used to prove an upper bound of $O(\log n)$ on the quantum information leakage of the coherent state QFP protocol. Suppose in such a protocol, Alice and Bob map their strings to the multimode coherent states $\{\|\alpha_x\rangle\!\rangle\}_x$ with constant mean photon number μ. Then, for $\epsilon > 0$, we can choose a Hilbert space $\mathcal{H}_d$ which contains states approximating $\{\|\alpha_x\rangle\!\rangle\}_x$ as above. By using a continuity bound for entropy (the Fannes-Audenaert inequality), the following upper bound for the quantum information leakage of such protocols was proven in Ref. [42]

$$\mathrm{QIL}(\Pi^{(n)}_{\text{CS-QFP}}) \leq \log(\dim(\mathcal{H}_d)) + 2n\sqrt{2\epsilon} + H_2(\sqrt{2\epsilon}) \tag{4.5}$$

where we use $\Pi^{(n)}_{\text{CS-QFP}}$ to denote any family of coherent state fingerprinting protocols with constant mean photon number, and $H_2(x) = -x\log(x) - (1-x)\log(1-x)$ is the binary entropy function. Strictly speaking, this bound does not show that the information leakage is bounded by $O(\log n)$, since the right hand side grows linearly in n. However, this bound is numerically easy to use. Further, since ϵ is arbitrary one can optimize over ϵ. This makes the growth of the bound

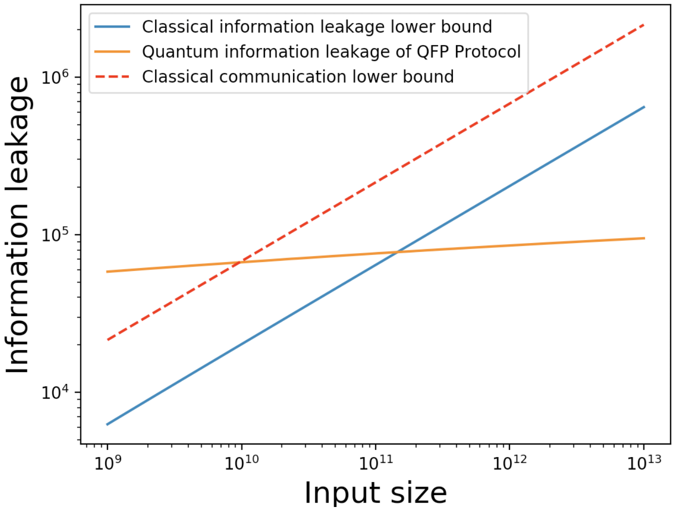


Figure 4.1: We plot the information leakage lower bound for classical protocols and the upper bound on the information leakage for the coherent state quantum fingerprinting protocol. We also plot the communication lower bound for classical protocols which was beaten by [3]. It can be seen that the information leakage lower bound is much smaller than the communication lower bound. The information leakage in the coherent state QFP protocol is seen to be lower than the lower bound on the information leakage of any classical protocol for $n \gtrsim 10^{11}$. It is possible that for smaller input sizes than this value there exist classical protocols with information leakage lower than this specific QFP protocol.

close to logarithmic numerically. Nevertheless, for the sake of completeness we point the reader to Ref. [42] which proves that the information leakage is actually bounded above by $O(\log n)$.

The bound in Eq. 4.5 allows us to calculate the quantum information leakage using the experimental parameters. Eqns. 4.2 and 4.5 are used to numerically calculate the string length at which the experiment should run to beat the classical information leakage bound. From Fig. 4.1, it can be seen that we need to go to string lengths of the order of 10^{11} to accomplish this task.

4.2.2.2 Estimation of experimental parameters

Our experiment follows almost the same protocol as the one given in Ref. [12], except for the fact that we use CCD detectors instead of single photon detectors. In Ref. [12], Arrazola and Lütkenhaus analyze the protocol for the case where the Referee makes an intereference measurement using a beam splitter and a single photon detector. In our experiment, the Referee makes an interference measurment by using a beam splitter and a CCD detector, which counts the total number of photons in each run of the protocol unlike the single photon detector which only measures the presence or absence of photons for each mode and gives a count of these. The protocol in Ref. [12] does not require the time resolution of single photon counting. Hence, bucket detectors like CCD detectors are sufficient to conduct the protocol. We chose CCD detectors for the experiment because they do not suffer from dark counts like single photon detectors. It is seen that dark count probability significantly deteriorates the performance of the experiment and increases the time required to conduct the experiment [11]. Dark counts affect the probability of whether a click is measured or not in each mode (number of modes $m \sim 10^{11}$). Whereas, the noise in CCD detectors can be modelled as a constant readout noise independent of the number of temporal modes. This leads to a higher error probability in the protocol if one uses single photon detectors instead of CCD detectors.

Recall that in the coherent state QFP protocol, Alice and Bob map their strings x and y to coherent states $\|\alpha_x\rangle\!\rangle$ and $\|\alpha_y\rangle\!\rangle$, where the amplitudes are given by Eq. 4.1. A subclass of random linear codes with Toeplitz generator matrices was used as the error correcting code following Ref. [11]. These codes are effcient to compute and have a high rate (approach the Gilbert-Varshamov rate bound asymptotically). These codes could be used to set the fraction of differences between different codewords δ to be anything in $(0, 1/2)$. The Referee passes the optical states he receives through a beam splitter and measures the dark port using a CCD detector. A balanced beam splitter transforms coherent states as $|\alpha\rangle|\beta\rangle \longrightarrow |(\alpha+\beta)/\sqrt{2}\rangle_L |(\alpha-\beta)/\sqrt{2}\rangle_D$, where L represents the light mode and D the dark mode.

In order to theoretically model the system and comment on its performance we also need to take experimental imperfections into account. Non-unity transmission efficiency η_T and quantum efficiency of the CCD camera η_Q have the effect of scaling the amplitude of the coherent state incident on the CCD detector. A non-unity visibility ν of the beam splitters leads to a mixing of the light and dark modes. Finally, we model the noise in the CCD detector as a constant readout noise r. If we consider these imperfections, then we are guaranteed that the CCD detector at the dark port sees a multimode coherent state with an average number of photons greater than

$$\mu_{\text{neq}} = 2\mu\eta_T\eta_Q\left((1-\nu)(1-\delta)+\delta\nu\right)+r$$

for unequal strings. On the other hand, for equal strings the dark port sees a multimode coherent state with an average number of photons equal to

$$\mu_{\text{eq}} = 2\mu\eta_T\eta_Q\left(1-\nu\right)+r.$$

Thus, the Referee's task reduces to discriminating between two Poisson distributions with mean values μ_{eq} and μ_{neq}. The error of discriminating these distributions is also the error of the protocol. Ref. [12] demonstrates a theoretical method for bounding this error. In our work, however, we calculate the error numerically.

Using these relations, we helped the experimental team figure out the acceptable range of experimental parameters like the various efficiencies and the visibility of the interferometer. Once these parameters were decided, we optimized the protocol parameters like δ and the protocol error for the experiment.

It is seen that in order to beat the classical information leakage bound, we need to go up to string lengths of 10^{11}, which when encoded with the ECC are about 4×10^{11} bits long. Hence, at a transmission rate of about 2 GHz the experiment takes 200 seconds. It is extremely difficult to ensure the stability of the experiment for such long durations. Therefore, in the next section we study if the time required for the QFP experiment can be reduced. The time required by our experiment depends on the number of modes in the signals sent by Alice and Bob. We study the dependence of the number of modes on the problem size for general optical protocols. We also examine if the growth of the number of modes can be traded off with the energy required during the protocol (mean photon number of the signals).

4.3 Tradeoff between resources for optical quantum fingerprinting

In this section, we will study the tradeoff between the number of modes and the mean number of photons required to run an optical quantum SMP protocol to compute the Equality function. Both of these are resources we invest while computing any function optically. The time required for Alice and Bob to run the protocol depends on the number of temporal modes in the signals they have to send to the Referee. Whereas, the mean photon number of the signals is directly proportional to the energy required to run the protocol. Therefore, we are essentially studying the tradeoff relation between the time required to run the protocol and the energy required during the protocol.

First, in Subsection 4.3.2, we study this problem in a general context. We develop a general bound on the growth of the number of modes and the mean number of photons with respect to the problem length for any optical protocol computing a function f. Then, in Subsection 4.3.3, we develop similar bounds for coherent state QFP protocols. We show that the number of modes increases almost linearly with the problem size for such protocols and hence the time required for Arrazola and Lütkenhaus' QFP protocol is optimal upto a constant factor.

4.3.1 Intermediate results

We begin by proving some intermediate results. These would be helpful for proving general tradeoff bounds in Section 4.3.2.

Lemma 4.1 (Winter's gentle measurement lemma [16, Corollary 3.15])**.** *Let $\mathcal{H}$ be a Hilbert space, $\rho \in D(\mathcal{H})$ be a density operators and $P \in Pos(\mathcal{H})$ a positive operator satisfying $P \leq \mathbb{1}$*

and $\operatorname{Tr}(P\rho) > 0$*. Then, we have*

$$F\left(\rho, \frac{\sqrt{P}\rho\sqrt{P}}{\operatorname{Tr}(P\rho)}\right) \geq \sqrt{\operatorname{Tr}(P,\rho)}.$$

Lemma 4.2. *Let P be a projector and $\rho \in D(\mathcal{H})$ be a density matrix in the Hilbert space $\mathcal{H}$, such that $\operatorname{Tr}(P\rho) \geq 1 - \delta$ for $\delta \in (0,1)$. Then, we have that*

$$\frac{1}{2}\left\|\rho - \frac{P\rho P}{\operatorname{Tr}(P\rho P)}\right\|_1 \leq \sqrt{2\delta} \tag{4.6}$$

Proof. As a result of Lemma 4.1, we have

$$F\left(\rho, \frac{P\rho P}{\operatorname{Tr}(P\rho)}\right) \geq \sqrt{\operatorname{Tr}(P,\rho)} \geq \sqrt{1-\delta}.$$

Using the Fuchs-van de Graaf inequality (Theorem 2.4), the trace distance

$$\begin{aligned}\left\|\rho - \frac{P\rho P}{\operatorname{Tr}(P\rho P)}\right\|_1 &\leq 2\sqrt{1 - F(\rho,\sigma)^2}\\ &\leq 2\sqrt{1-(1-\delta)^2}\\ &= 2\sqrt{2\delta - \delta^2}\\ &\leq 2\sqrt{2\delta}\end{aligned}$$

□

Lemma 4.3. *Suppose in a quantum simultaneous message passing (SMP) protocol to compute the function f with error at most ϵ, Alice and Bob send the quantum states ρ_x and σ_y on inputs x and y. If ρ'_x and σ'_y are quantum states such that $1/2\|\rho_x - \rho'_x\|_1 \leq \delta$ and $1/2\|\sigma_y - \sigma'_y\|_1 \leq \delta$ for all x and y, then the states used in the actual protocol can be replaced by these to create a SMP protocol with error at most $\epsilon + 2\delta$.*

Proof. Suppose that on inputs x and y, Alice and Bob send the quantum state ρ_x and σ_y to the referee, who applies Φ_{ref} (quantum-classical CPTP map) to the joint state to compute $f(x,y)$. For such a protocol, we have that for every x, y

$$\frac{1}{2}\|\Phi_{\text{ref}}(\rho_x \otimes \sigma_y) - |f(x,y)\rangle\langle f(x,y)|\,\|_1 \leq \epsilon,$$

which is equivalent to saying that for inputs the error probability is less than ϵ. Now, if we replace the states used by Alice and Bob by ρ'_x and σ'_y such that $1/2\|\rho_x - \rho'_x\|_1 \le \delta$ and $1/2\|\sigma_y - \sigma'_y\|_1 \le \delta$ for all x and y, then we have that for every x and y

$$\begin{aligned}
&\frac{1}{2}\|\Phi_{\text{ref}}(\rho'_x \otimes \sigma'_y) - |f(x,y)\rangle\langle f(x,y)|\,\|_1 \\
&\qquad \le \frac{1}{2}\|\Phi_{\text{ref}}(\rho_x \otimes \sigma_y) - |f(x,y)\rangle\langle f(x,y)|\,\|_1 + \frac{1}{2}\|\Phi_{\text{ref}}(\rho_x \otimes \sigma_y) - \Phi_{\text{ref}}(\rho'_x \otimes \sigma'_y)\|_1 \\
&\qquad \le \epsilon + \frac{1}{2}\|\Phi_{\text{ref}}(\rho_x \otimes \sigma_y) - \Phi_{\text{ref}}(\rho'_x \otimes \sigma_y)\|_1 + \frac{1}{2}\|\Phi_{\text{ref}}(\rho'_x \otimes \sigma_y) - \Phi_{\text{ref}}(\rho'_x \otimes \sigma'_y)\|_1 \\
&\qquad \le \epsilon + 2\delta
\end{aligned}$$

where we have used the fact that for all $\rho \in D(\mathcal{H})$, $\|\rho\|_1 = 1$ and for all CPTP maps Φ, $\|\Phi\|_1 \le 1$ (Theorem 2.2). □

4.3.2 Tradeoff between the mean photon number and the number of modes for optical SMP protocols

Now, we will study the tradeoff between the number of modes and the mean photon number for a family of optical SMP protocols computing a function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. Let $\{\Pi_n\}_{n=1}^{\infty}$ be a family of SMP protocols, which computes the function $f(x,y)$ with error at most $1/10$. The exact value of error is not relevant, since the communication cost for fixed error rates are equal up to multiplicative factors (Theorem 2.6). The protocol Π_n can be used to compute the function $f(x,y)$ when x and y are n-bit strings. We suppose that these protocols are implemented optically. That is, the states sent by Alice and Bob while running Π_n are part of a $m(n)$-mode Hilbert space $\mathcal{H}^{\otimes m(n)}$, where $\mathcal{H}$ is the single mode Fock space. Note that the states used depend on the problem parameter n, and hence the number of modes $m = m(n)$ too. We will call the states sent by Alice and Bob on inputs x and y during protocol Π_n, $\rho_x^{(n)}$ and $\sigma_y^{(n)}$. Further, we define the maximum mean number of photons $\mu(n)$, which Alice or Bob may have to send during Π_n as

$$\mu(n) := \max\left\{\{\operatorname{Tr}(\hat{N}\rho_x^{(n)}) : x \in \{0,1\}^n\} \cup \{\operatorname{Tr}(\hat{N}\sigma_y^{(n)}) : y \in \{0,1\}^n\}\right\}. \tag{4.7}$$

For notational convenience, we will drop the explicit dependence of $\mu(n)$ and $m(n)$ on n and denote the number of modes and the maximum mean photon number by m and μ.

Our strategy will be to use the fact that the maximum mean photon number is μ to find a projector P, which has high overlap with the states $\rho_x^{(n)}$ and $\sigma_y^{(n)}$ used in the protocol. The rank or the dimension of this projector will be shown to depend only on m and μ. We will use it to transform the given protocol into another protocol, where Alice and Bob send the finite dimensional states $P\rho_x^{(n)}P/\operatorname{Tr}(P\rho_x^{(n)})$ and $P\sigma_y^{(n)}P/\operatorname{Tr}(P\sigma_y^{(n)})$ on inputs x and y. This protocol would require the communication of only $O(\log(\operatorname{rank}(P)))$ qubits, which has to satisfy the known lower bounds for the SMP communication complexity of f.

Consider a fixed value of n. For any state $\rho^{(n)} \in \{\rho_x^{(n)} : x \in \{0,1\}^n\} \cup \{\sigma_y^{(n)} : y \in \{0,1\}^n\}$ sent by Alice or Bob during Π_n, using the Markov inequality (Eq. 2.3) we have that

$$\begin{aligned} \mathbb{P}r_{\rho^{(n)}}[N \geq \mu/\delta] &\leq \delta \frac{\mathbb{E}_{\rho^{(n)}}[N]}{\mu} \leq \delta \\ \Rightarrow \mathbb{P}r_{\rho^{(n)}}[N < \mu/\delta] &\geq 1 - \delta. \end{aligned} \tag{4.8}$$

Define, $P := \sum_{(n_1,\cdots,n_m)\in S_{<\mu/\delta}} |n_1,\cdots,n_m\rangle\langle n_1,\cdots,n_m|$ where $S_{<\mu/\delta} := \{(n_1,n_2,\cdots,n_m) : \sum_{i=1}^m n_i < \mu/\delta\}$. We can rewrite Eq. 4.8 as

$$\mathrm{Tr}(P\rho^{(n)}) \geq 1 - \delta. \tag{4.9}$$

Now, using Lemma 4.2, we have that for every x, y

$$\begin{aligned} \frac{1}{2}\left\| \rho_x^{(n)} - \frac{P\rho_x^{(n)}P}{\mathrm{Tr}(P\rho_x^{(n)}P)} \right\|_1 &\leq \sqrt{2\delta} \\ \frac{1}{2}\left\| \sigma_y^{(n)} - \frac{P\sigma_y^{(n)}P}{\mathrm{Tr}(P\sigma_y^{(n)}P)} \right\|_1 &\leq \sqrt{2\delta}. \end{aligned}$$

Using Lemma 4.3, we can create a SMP protocol for f with error at most $1/10 + 2\sqrt{2\delta}$, which uses the states $\{P\rho_x^{(n)}P/\mathrm{Tr}(P\rho_x^{(n)}) : x \in \{0,1\}^n\} \cup \{P\sigma_y^{(n)}P/\mathrm{Tr}(P\sigma_y^{(n)}) : y \in \{0,1\}^n\}$. This protocol requires the communication of only $O(\log(\mathrm{rank}(P)))$ qubits. Further, the rank of the projector P can be estimated as follows.

The rank of the projector is equal to $|S_{<\mu/\delta}|$ which is equal to the number of non-negative integer solutions of the equation

$$\sum_{i=1}^m n_i < \frac{\mu}{\delta}.$$

If we introduce a slack variable s, this is equal to the number of non-negative integer solutions of

$$\sum_{i=1}^m n_i + s = \lfloor \frac{\mu}{\delta} \rfloor$$

which is equal to

$$\binom{a+m}{m}$$

where $a = \lfloor \mu/\delta \rfloor$ using standard combinatorics. Further, using Lemma A.1, this expression can be bounded by $(1+m)^a$ and $(1+a)^m$. Thus, we have that

$$\log(\text{rank}(P)) \leq \min\left\{\frac{\mu}{\delta}\log(1+m), m\log(1+\frac{\mu}{\delta})\right\} \tag{4.10}$$

We can choose $\delta = 10^{-4}$, so that the error of the protocol is smaller than $1/3$. Then, we can simply use the lower bounds corresponding to an error of $1/3$. This does not affect the asymptotic bounds we are working towards as the asymptotic communication cost for communication protocols does not depend on the error. Thus, moving forward we can ignore the dependence of the upper bound on δ. Recall that the SMP communication cost for quantum protocols for function f is lower bounded by $\Omega(\log(R^{||}_{1/3}(f)))$, where $R^{||}_{1/3}(f)$ is the SMP communication complexity for computing f with error at most $1/3$ (Theorem 2.8). Further, the classical private SMP communication complexity is lower bounded by $\Omega(\sqrt{D(f)})$, where $D(f)$ is the deterministic communication complexity of f (Theorem 2.7). Thus, the number of qubits q used by any quantum protocol is lower bounded by $\Omega(\log(D(f)))$. For any family of optical quantum SMP protocols for f, the following bounds holds true

$$\mu\log(m) = \Omega(\log(D(f))) \tag{4.11}$$

$$m\log(\mu) = \Omega(\log(D(f))). \tag{4.12}$$

In particular, if the maximum mean number of photons for a family of quantum fingerprinting protocol is constant, then we have that

$$\log(m) = \Omega(\log(n))$$

These bounds show that in a *weak* sense the QFP protocol given by Arrazola and Lütkenhaus is optimal. We use the phrase *weak*, because these bounds do not rule out the possibility of a family of optical protocols with constant mean photon number and sublinear growth of m in n. In the next section, we will show that these bounds can be made tighter for the implementations of the quantum fingerprinting protocol given in Ref. [7] which use coherent states.

4.3.3 Tradeoff bounds for the QFP protocol implemented using coherent states

In this section, we only consider the protocol for the Equality function given in Ref. [7] (referred to as *the Quantum Fingerprinting (QFP) protocol* here on). While our earlier results were valid for all possible optical protocols to solve the Equality problem in the SMP model, the results in this section will focus only on implementations of the QFP protocol which use multimode coherent states. Recall that in the QFP protocol, Alice and Bob both map their strings x and y to pure states $|\psi_x\rangle$ and $|\psi_y\rangle$ which satisfy $|\langle\psi_x|\psi_y\rangle| \leq \delta$ for some $\delta > 0$. The referee then uses an appropriate test to check if the states $|\psi_x\rangle = |\psi_y\rangle$ or not. In the following, we specifically consider an implementation of this protocol where the states prepared by Alice and Bob are constrained to be multimode coherent states, whereas the Referee is allowed to use any measurement to solve the problem. Alice and Bob in this setting can be thought of as resource limited 'clients' to an all powerful 'server', the Referee.

Consider a family of QFP protocols $\{\text{QFP}_n\}$ which can be used to solve the Equality problem in the SMP setting when x and y are n-bit strings. Suppose that the coherent state implementation of this family of QFP protocols uses the multimode coherent states $\{\|\alpha_x^{(n)}\rangle\!\rangle\}_{x\in\{0,1\}^n}$. We define the number of modes m and maximum average photon number μ as in the previous section. We also define the parameter $\delta(n)$ to be the maximum overlap between any two of these states,

$$\delta(n) := \max_{x\neq y}\{|\langle\|\alpha_x^{(n)}\rangle\!\rangle, \|\alpha_y^{(n)}\rangle\!\rangle\rangle|\}. \tag{4.13}$$

By the requirements of the protocol, we have that $\delta(n) < 1$ for every n. We further note that practically $\delta(n) \leq 1 - \epsilon_{\text{exp}}$ for every n for some constant parameter $\epsilon_{\text{exp}} > 0$, since experimentally it would not be possible to distinguish or prepare states with fidelity arbitrarily close to unity[2]. One can also think of this restriction as a consequence of the experimental precision of preparation of the states. In our discussion moving forward, we once again drop the dependence of the maximum overlap on n and simply refer to it as δ for the sake of clarity. Using Eq. 3.3, we see that Eq. 4.13 further implies that the amplitude vectors, $\{\alpha_x^{(n)}\}_{x\in\{0,1\}^n} \subset \mathbb{C}^m$ are such that for every $x \neq y$

$$\|\alpha_x^{(n)} - \alpha_y^{(n)}\|_2 \geq \delta' \tag{4.14}$$

where we define $\delta' := (2\ln(1/\delta))^{1/2}$ (note that δ' too depends on n). We also have that for every $x \in \{0,1\}^n$, $\|\alpha_x^{(n)}\|_2 \leq \sqrt{\mu}$ since the mean number of photons of $\|\alpha_x^{(n)}\rangle\!\rangle$ is equal to $\|\alpha_x^{(n)}\|_2^2$. Using these we can bound the number of modes m with the help of a sphere packing argument. Let $A := \sqrt{\mu} + \delta'/2$. Observe that

$$\bigcup_{x\in S} B(\alpha_x^{(n)}, \frac{\delta'}{2}) \subset B(0, A)$$

where $B(x,r) := \{y \in \mathbb{C}^m : \|y - x\|_2 < r\}$. In fact this is a disjoint union as can be seen from Eq. 4.14. Using the fact that $\mathbb{C}^m$ is equivalent to $\mathbb{R}^{2m}$ for the purpose of integration, we have that

$$\begin{aligned}
&\text{vol}\left(\bigcup_{x\in S} B(\alpha_x^{(n)}, \frac{\delta'}{2})\right) \leq \text{vol}\left(B(0,A)\right) \\
&\Rightarrow 2^n \left(\frac{\delta'}{2}\right)^{2m} \leq A^{2m} \\
&\Rightarrow \frac{n}{2} \leq m \log_2\left(\frac{2A}{\delta'}\right) \\
&\Rightarrow \frac{n}{2} \leq m \log_2\left(\frac{2A}{(2\ln(1/\delta))^{1/2}}\right).
\end{aligned} \tag{4.15}$$

[2] We essentially require that $\sup_{n\geq 1} \delta(n) < 1$.

where we used the fact that the sets are disjoint in the second step. We can also eliminate δ in the above equation by using the fact that $\delta \leq 1 - \epsilon_{\text{exp}}$ for a fixed ϵ_{exp} and that the equation above is increasing in δ. We then get

$$\frac{n}{2} \leq m \log_2 \left(1 + \sqrt{\frac{\mu}{2\ln(1/(1-\epsilon_{\text{exp}}))}}\right). \tag{4.16}$$

or that $m\log(\mu) = \Omega(n)$ *practically*. It should be observed that this is substantially stronger than the general bound presented earlier (Eq. 4.11). If we suppose that $m = O(n^c)$ for $0 < c < 1$, then the mean photon number satisfies $\mu \geq 2^{\Omega(n^{1-c})}$, i.e., the mean photon number would increase exponentially in n^{1-c}, which would be very undesirable experimentally. Finally, in the case of a family of quantum protocols with constant mean number of photons, we have that

$$m = \Omega(n)$$

assuming the aforementioned experimental limitations. Let us define the rate of a coherent state QFP protocol to be the ratio n/m. For the purpose of comparison with current protocols, we will try to use the bound above to propose a practical coherent state QFP protocol with a high rate. Observe that if we assume that our class of coherent state QFP protocols satisfies $\delta(n) \leq \epsilon$ for some constant $\epsilon < 1$, then the above bound is again valid, i.e.,

$$\frac{n}{m} \leq 2\log_2 \left(1 + \sqrt{\frac{\mu}{2\ln(1/\epsilon)}}\right). \tag{4.17}$$

In Appendix A.3, we show that for such a class of protocols the Referee can also use the interference measurement described in Section 4.2.2.2 and solve the Equality problem with an error at most ϵ. If we use amplitude vectors which optimally pack the sphere while being at least $(2\ln(1/\epsilon))^{1/2}$ distance apart, then we can reach the bound on the rate on the right hand side of Eq. 4.17. Moreover, our protocol would have an error at most ϵ. Using Theorem 4.2 and the argument following it, we can also show that the information leakage for such a protocol would also be logarithmic. For $\mu = 10^3$ and $\epsilon = 0.01$, the bound on the right hand side of Eq. 4.17 is 7, whereas the rate of the coherent state QFP protocol[3] is typically around 0.3. Thus, if we are able to use these states, then we can improve the rate of coherent state QFP protocol by a factor of about 20.

More generally, let us consider $\mu = 10^3$ and $\epsilon_{\text{exp}} = 10^{-6}$ in Eq. 4.16, which is a very generous experimental limitation. This is equivalent to assuming that we can experimentally prepare two states ρ, σ accurately as long as the fidelity satisfies $F(\rho, \sigma) \leq 1 - 10^{-6}$. Even in this case we get an upper bound of 29 on the rate. Taken together these results allow us to narrow down the maximum rate of coherent state QFP protocols to within a factor of about 4.

[3] Assuming $\delta \approx 0.2$ in the QFP protocol and using the Gilbert-Varshamov bound.

4.4 Conclusion

In this chapter, we discussed quantum fingerprinting using coherent states. We described the tools and results we used for the experiment on quantum fingerprinting. We saw that in order to beat the classical information leakage bound the experiment needs to run at string lengths of the order of 10^{11}, which is very difficult experimentally. Motivated by this we studied the tradeoff between the growth of the number of modes and the mean number of photons required to solve the Equality problem optically. We developed lower bounds for the growth of these resources for general problems and protocols. For fixed photon number protocols to solve the Equality problem, we saw that the number of modes m grew as $\log(m) = \Omega(\log(n))$. We strengthened this bound to $m = \Omega(n)$ for fixed photon number coherent state quantum fingerprinting protocols, which are based on the protocol given in Ref. [7]. We hope that our work can be used as a guide for the construction of better optical protocols.

Chapter 5

Erasable Bit Commitment with Temporarily Trusted Parties

5.1 Introduction

5.1.1 Background

It is well known that unconditional bit commitment between two parties cannot be implemented classically or even by utilizing quantum resources [44–48]. Several different relaxations on the security requirements of bit commitment have been studied in the past. In the classical setting, the most notable of these are settings which require bit commitment to either be statistically binding and computationally hiding, or computationally binding and statistically hiding. On the other hand, in the quantum setting unconditionally secure bit commitment can be implemented if one assumes that the adversaries have small or noisy quantum memories (see, e.g., [13,49–51] and reference therein).

Another possible way of implementing bit commitment is to use a trusted third party, who is honest during the protocol. (See [52] for a variant where the trusted party only helps to initialize the protocol.) To commit to a bit b, Alice and Bob first share a secret key k. Then, Alice sends $(b \oplus k)$ to the third party (through a private channel), who stores the bit until the open phase. During the open phase, Alice simply asks the trusted party to reveal the bit $(b \oplus k)$ to Bob, who is able to extract b from it. Since, the third party is honest, he does not reveal the bit to Bob (Hiding for Bob) and he also does not change the value of the bit after the commit phase (Binding for Alice). Furthermore, the protocol is even hiding for the trusted party, as he cannot determine b unless someone tells him k.

Suppose, however, that Alice decides to abandon the commitment instead of opening it. If it is the case that Alice can trust the third party *forever*, Alice's commitment remains a secret from Bob for all future times. This case, though, is improbable. It is possible that the third party becomes an adversary to Alice and colludes with Bob after the conclusion of the protocol. If Bob and the third party get together after the protocol, then they can figure out the value of the bit Alice was committed to.

5.1.2 Simple protocol for erasable bit commitment from temporary quantum trust

In fact, due to the no-go theorem for classical bit commitment no classical protocol which is binding for Alice can satisfy a hiding property for both Bob and the trusted party together once the protocol is over. On the other hand, one can use quantum mechanics to create a protocol, which only requires Alice and Bob to temporarily trust the third party during the course of the protocol. The basic idea of this protocol, implementing a primitive which we term *erasable bit commitment* (EBC), can be explained by modifying the aforementioned classical protocol.

First, Alice and Bob share secret bits θ and k. In order to commit to bit b, Alice sends the state $H^\theta \left|b \oplus k\right\rangle$ (where H is the Hadamard gate) to the third party in order to commit to b. To open the commitment, Alice asks the third party to forward the state to Bob, who can invert the Hadamard depending on the value of the secret bit θ, and open b. Furthermore, in case Alice decides to abandon the commitment, she can ask for an ”erasure”, that is, ask the third party to send her the state back. In this case, once the protocol is over, even if the trusted party and Bob get together, they will not be able to figure out Alice's commitment. The secret bits Bob shared with Alice were not correlated with Alice's commitment. Whereas, since the third party honestly returned the quantum state back to Alice, he too would not have any information about Alice's commitment. Unlike the classical setting, this primitive is possible in the quantum setting due to the no-cloning theorem.

Note that if the trust time is limited, the possibility for Alice to ask for an erasure at the end of the trust period is necessary. In fact, it could happen that the condition for Alice to issue the open command is not met during the trust period. In such a case, she needs to be able to abort given that the end of the trust period is looming! The erasure command allows her to abort while still ensuring that her data is not revealed to Bob or the third party in the future, even if she can no longer trust the third party anymore. Additionally, the erasure command is announced publically so that Bob knows that Alice has abandoned her commitment and may not be committed to a classical value anymore.

The chapter is organised as follows. We begin by introducing the temporarily trusted party setting in the next section. Then, we describe the erasable bit commitment primitive and the security requirements for such a primtive. Following this we present a robust protocol for this primitive based on BB84 states and prove its security informally. In Section 5.6, we state our claims concerning additional security guarantees. The conclusion discusses how our protocol avoids the no-go results for quantum bit commitment and also compare our protocol to other variants on quantum bit commitment. In the Appendix, we describe our channel noise model, prove the impossibility of classical protocols for erasable bit commitment in a trusted party setting and then formally state definitions and provide security proofs.

5.2 Temporarily trusted party setting

In this section, we describe the temporarily trusted party setting, which we use to implement erasable bit commitment. As stated earlier, the idea is to try to use trusted third parties to implement protocols which cannot be implemented in a two party setting. Further, we do not wish to trust the parties for eternity, we would like to trust them only temporarily for the duration of the protocol. In this section, we formally define what we mean when we use the term *trust*. We also wish to allow for a certain number of dishonest or corrupted trusted parties. We state the trust guarantee in the presence of such parties as well.

5.2.1 Quantum honest-but-curious parties

We would like our trusted parties to behave in a manner which is indistinguishable from an honest party to an external observer. We call such behaviour *quantum-honest-but-curious* behaviour. In particular, the input-output behaviour of quantum honest-but-curious parties is consistent with that of honest participants during the protocol. However, these parties may try to gather as much information as possible during the protocol. We base our definition of $\delta-$honest-but-curious parties on the definition of specious adversaries given by [53]. The definition considered by Ref. [53] is suited for the case of two parties where at most one of those can be honest-but-curious. We generalize this definition to a setting with p number of parties.

Similar to the previous definition, we define a party to be honest-but-curious if at each step of the protocol it can prove to an external auditor that it has been following the protocol honestly. Specifically, at any stage during the protocol the honest-but-curious party should be able to apply a local map to its state to make its behaviour indistinguishable from that of an honest party. Further, we also require that the party announces any deviations from the protocol publicly. This behaviour is encapsulated in the following definition.

Definition 5.1 (δ-honest-but-curious party)**.** Consider a k-step protocol between the parties $(P_n)_{n=1}^p$. Let $\rho_{P_1 \ldots P_p}$ be an initial state distributed between these parties and $\rho_{P'_1 \ldots P'_p R}$ an extension of this state to some reference system R. In the following, we say that the parties follow a strategy $(P'_n)_{n=1}^p$ if at step j of the protocol the joint state of all the parties is $\Phi^{(j)}_{P'_1 \ldots P'_p}(\rho)$. Further, we denote the honest strategy of party P_n by P_n and a general (possibly adversarial) strategy by P'_n.

For a k-step protocol between the parties $(P_n)_{n=1}^{p}$, the party P_i (and equivalently the strategy of P_i) is said to be δ−honest-but-curious if

1. For every strategy of the other parties $P'_{\bar{i}} \coloneqq (P'_n)_{n \neq i}$, every initial state $\rho_{P_i P_{\bar{i}} R}$ and for every step in the protocol $j \in [k]$, there exists a local CPTP map $\mathcal{T}_j$ such that
$$((\mathcal{T}_j)_{P'_i} \otimes I_{P'_{\bar{i}}})\ \Phi^{(j)}_{P'_i P'_{\bar{i}}}(\rho_{P_i P_{\bar{i}} R}) \approx_\delta \Phi^{(j)}_{P_i P'_{\bar{i}}}(\rho_{P_i P_{\bar{i}} R}) \tag{5.1}$$
where $\Phi^{(j)}_{P_i P'_{\bar{i}}}$ ($\Phi^{(j)}_{P'_i P'_{\bar{i}}}$) is the map applied on the initial state after step j if party P_i follows the protocol honestly (dishonestly) and the other parties follow $P'_{\bar{i}}$.

2. The party P_i publicly announces if it receives any input or message from any party which deviates from the protocol, in particular if party P_i expects to receive an n-dimensional quantum state and receives something lying outside of that space, it publicly announces the deviation.

It should be noted at this point that the second requirement above precludes the possibility of the honest-but-curious nodes communicating and collaborating during a protocol. This is different from the definition of classical specious adversaries considered by Ref. [53], who allow the specious adversaries to collaborate freely. In the scenario considered in Ref. [53], this was reasonable since they only considered specious adversaries. In our setting, however, we consider both honest-but-curious adversaries and dishonest adversaries. We cannot expect the participants to know beforehand which parties are honest-but-curious and which ones are dishonest. Therefore, we further require that the honest-but-curious nodes do not interact with other parties unless they are required to do so according to the protocol. This assumption, though, can be lifted in our protocol, as we will show in our additional security claim of 'Expungement on successful runs' (Sec. 5.6.2).

In Appendix B.3.3.1, we show that if a quantum honest-but-curious party is given a quantum state at some point during a protocol, and is asked to return it at a later point in the protocol, we can be certain that the state returned by him was *almost* the same as the one given to him earlier up to tensoring of a fixed state. Specifically, suppose that the honest-but-curious party T is given a state ρ_{TR} during the protocol, and is asked to send his share to party P at a later point. Then, the state $\rho'_{RPT'}$ (where T' is a memory held by T) sent by T satisfies

$$\rho'_{PRT'} \approx_{O(\sqrt{\delta})} (I_R \otimes I_{T \to P})\rho_{RT} \otimes \tau_{T'}.$$

for some fixed state τ. (See Lemma B.2 for formal statement). We see that in this scenario the honest-but-curious party is forced to be almost honest in this scenario. In this chapter, we will therefore assume that the honest-but-curious nodes act completely honestly during the protocol for simplicity, since we will only be dealing with the action of honest-but-curious parties in scenarios like this. Formally, this corresponds to assuming $\delta = 0$ or assuming the parties to be perfectly-honest-but-curious. This does not lead to loss of generality and the security arguments remain almost the same. A more careful analysis of the behaviour of such parties during our protocol is provided in the Appendix B.3.3. Lastly, since the memory of the honest-but-curious parties after giving away the state ρ_{RT} is almost decoupled from that state, we say that the honest-but-curious party *forgets* the state he received.

5.2.2 Temporarily trusted party setting

In addition to the usual two parties, Alice and Bob, involved in a bit commitment protocol, there are also additional trusted third parties $\mathcal{T}_1, \ldots, \mathcal{T}_m$ involved in the temporarily trusted party settings we consider. For the purpose of this chapter, we refer to all the additional trusted third parties $\mathcal{T}_1, \ldots, \mathcal{T}_m$ as trusted parties or trusted nodes. Alice and Bob both trust that out of these m trusted parties at least $(m - t)$ will act quantum honest-but-curiously for the duration of the protocol. In the context of the definition of honest-but-curious above, in our setting the parties are $(A, B, \mathcal{T}_1, \cdots, \mathcal{T}_m)$, and there exists a subset $E \subset [m]$ such that $|E| \leq t$ and for all $j \notin E$ the party $\mathcal{T}_j$ is quantum honest-but-curious. Further, the EBC protocol is a two step protocol as will be seen later. The rest of the third parties (at most t in number) can behave dishonestly during the protocol and even collaborate with the cheating party. We use the term 'adversaries' during the protocol to denote the cheating party (dishonest Alice or dishonest Bob) along with the dishonest trusted nodes.

Further, this trust assumption is *temporary* or time-limited: after the end of the regular duration of the protocol, Alice and Bob do not have any guarantee about the behaviour of the third parties. They can no longer assume that the $\mathcal{T}_i$'s behave honestly. These parties could act adversarially after the end of the protocol and even collaborate with a dishonest Alice or a dishonest Bob.

5.3 Erasable bit commitment in a setting with temporarily trusted parties

Erasable bit commitment (EBC) is a protocol between two parties, Alice and Bob, in a setting with m additional trusted parties, at most t of which are dishonest and adversarial during the protocol. The protocol has two phases: a commit phase, followed by one of either an open or an erase phase. During the commit phase, Alice inputs a string s and Bob receives a message notifying him that Alice has completed the commit phase. At the end of this stage, she is committed to this string, that is, if the commitment is 'opened' then Bob will receive s or reject the commitment. Moreover, the commitment is hidden from Alice's adversaries (Bob and dishonest nodes collaborating with him) at this stage. After the commit phase, Alice can choose to open or erase the commitment. In case of an open, Bob receives the string s, the string Alice was committed to. Further, in this case, even if all the trusted parties get together after the protocol they cannot determine s. In case Alice chooses to erase, then once the protocol is over, even if Bob and all the trusted parties collaborate they cannot ascertain the value of s.

In the rest of the chapter, we consider a randomized version of erasable bit commitment. Randomized EBC is essentially the same as above except now Alice does not have any input during the commit stage. Instead of choosing the string for her commitment as above, Alice receives a random string c at the end of the commit phase, which is called as her commitment. This randomized EBC can easily be converted into a EBC like above by asking Alice to send $s \oplus c$ to Bob after the commit phase (See Ref. [13]).

Thus, in the randomized EBC protocol (referred to as EBC here on) Alice and Bob do not have any inputs during the commit phase. Alice inputs an "open" or "erase" bit at some point after the commit phase into the protocol. In addition to the commitment c mentioned above, Alice and Bob also receive flags F_A and F_B (let $F = F_A = F_B$) notifying them if Alice called for an erase ($F = \text{erase}$), or if the open was successful ($F = \text{success}$) or if the open failed ($F = \text{failure}$). In general if Alice is dishonest, Bob may not receive the same string as Alice. So, we call Bob's output $\hat{c}$. To summarize, the outputs of the protocol for Alice and Bob are as follows:

- Alice outputs a string $c \in \{0,1\}^\ell$ at the end of the commit phase, and a flag $F_A \in \{\text{success}, \text{failure}, \text{erase}\}$ at the end of either the open or erase phase;
- Bob outputs a string $\hat{c} \in \{0,1\}^\ell$ as well as a flag $F_B \in \{\text{success}, \text{failure}, \text{erase}\}$ at the end of either the open or erase phase.

5.3.1 Security requirements for erasable bit commitment:

Given m trusted nodes $(\mathcal{T}_i)_{i=1}^m$ of which at least $(m - t)$ act quantum honest-but-curiously for the duration of the protocol, an erasable bit commitment protocol satisfies the following security requirements:

1. Correctness: If both Alice and Bob are honest and Alice receives c during the commit phase, then, in the case of open, Bob accepts the commitment ($F = \text{success}$) and $\hat{c} = c$.
2. Binding: If Bob is honest, then, after the commit phase, there exists a classical variable $\tilde{C}$ such that Alice is commited to $\tilde{C}$, i.e. during the open phase, either Bob accepts the commitment ($F_B = \text{success}$) and receives an output $\hat{C}$ such that $\hat{C} = \tilde{C}$, or Bob rejects the commitment ($F_B = \text{failure}$). (This guarantee only makes sense in the case that the open protocol is run after the commit protocol; if an erase protocol is run instead, then Alice does not have to be committed to a classical value anymore.)
3. Hiding:

(a) *Commit:* If Alice is honest and she receives the output c during the commit phase, then, after the commit phase and before the open or erase phase, Bob and the dishonest trusted nodes together can only extract negligible information about c, i.e., their joint state is almost decoupled from Alice's commitment.

(b) *Open:* If Alice and Bob are honest and Alice's commitment is c, then, after an open phase, the $\mathcal{T}_i$'s together can only extract negligible information about c, i.e., their joint state is almost decoupled from Alice's commitment.

(c) *Erase:* If Alice is honest and she receives the output c during the commit phase, then, after the erase phase, Bob and the $\mathcal{T}_i$'s together can only extract negligible information about c, i.e., their joint state is almost decoupled from Alice's commitment.

We give more formal security definitions based on the security definitions for bit commitment given in Ref. [13] in Appendix B.3. One can easily check that the simple protocol given in Section 5.1.2 satisfies these requirements (if we consider $m = 1$, $t = 0$ and $\delta = 0$).

Lastly, it should be noted that the binding condition for EBC is weaker than the corresponding binding condition for bit commitment. In EBC, Alice is only committed to a classical value if the commitment is *opened*. This makes EBC a weaker primitive than bit commitment. For example, we cannot use a general EBC protocol instead of bit commitment to implement oblivious transfer (OT) using the protocol given in Ref. [54]. If we attempt to do so in a straightforward fashion, then the OT protocol, hence created, could possibly be susceptible to a superposition attack by Bob. However, we should note that even though EBC is weaker than bit commitment, it cannot be implemented quantum mecahnically in the two-party setting without additional assumptions. The no-go theorem for two-party quantum bit commitment [44, 45] precludes the possibility of a protocol which is both hiding and binding after the commit phase, as EBC is.

5.4 Robust Protocol for EBC based on BB84 states

In this section, we will develop a protocol for EBC using BB84 states which is robust to noise and a small non-zero number of dishonest trusted nodes. This will be done by modifying the simple protocol presented in Section 5.1.2. We use tools like privacy amplification and classical error correcting codes for this purpose. Before we proceed further, however, we describe our channel assumptions and our noise model.

5.4.1 Channel assumptions

We assume that the communication between the participants is done over secure (private and authenticated) channels between each pair of participants. We assume that the classical channels are noiseless, but we allow the quantum channels to be noisy. The fact that the quantum channels are noisy somewhat complicates the authentication part of the security guarantee: we cannot simply guarantee that the state output by the channel will be the state which was input. For simplicity, we assume the following, weaker, authentication guarantee with a simple model of adversarial noise: if the quantum channel in one direction between a pair of participants is used n times at some timestep, then at least $(1-\gamma)n$ of these transmissions will be transmitted perfectly, while the other at most γn transmissions might be arbitrarily corrupted by the adversary. Note that this is sufficient to model some random noise, for example, depolarizing noise, except with negligible probability.

Also note that we could use a shared secret key between sender and receiver together with variants of various quantum cryptography techniques, e.g., that of the trap authentication scheme [55], to obtain guarantees that with high probability, the actual channel acts as a superposition over such type of bounded noise channels (in the sense of the adversarial channels of [56]). We leave a detailed analysis of how to implement such a variant of our guarantee in practical settings and the proof of security of our scheme in such settings for future work. Also note that we do not assume any minimal noise level on the channels; guarantees on minimal noise level can be sufficient to allow one to implement cryptographic primitives like bit commitment (see, e.g., Ref. [57]).

We do not have any synchronicity assumptions; time-stamping can be achieved, for example, by broadcasting (with potential abort if some participant is dishonest) end-of-time-step signals.

5.4.2 High-level description

We consider a setting with m trusted third parties, at most t of which can be dishonest. To understand the tools and the structure of the robust protocol, we try to extend the simple protocol presented in Section 5.1.2 in a straightforward fashion. Imagine that Alice wishes to commit to the string $x \in \{0,1\}^k$ (this can be selected randomly to perform randomized EBC). To commit to x, during the commit phase, Alice randomly selects a basis $\theta \in_R \{0,1\}^k$ and a key $v \in \{0,1\}^k$, and distributes the state $|\psi\rangle = H^\theta |x \oplus v\rangle$ to the m-trusted parties, giving k/m qubits to each party. Further, she sends θ and v to Bob. In case Alice chooses to open, the trusted parties simply forward their shares to Bob and in case she chooses to erase, they send their states back to Alice. If everyone is honest during the protocol and there is no noise, then the string decoded by Bob, $\hat{x}$, is the same as x. However, if some qubits sent to Bob are corrupted by the dishonest trusted nodes or noise then $\hat{x} \neq x$. In order to circumvent this problem, we have Alice first encode her string x as $y = \mathrm{Enc}(x)$ using a pre-agreed $[n,k,d]$-classical error correcting code (ECC) with appropriate parameters and then sends it to the trusted parties. Not only would this allow the protocol to be robust to noise, it will also help ensure that the protocol is binding for Alice by making sure that Alice and the adversarial nodes cannot change the commitment "too much". Further, if in such a protocol t trusted parties collaborate with Bob, then they would know y for tn/m positions. This would provide Bob with some partial information about Alice's commitment x. Therefore, we require Alice to use privacy amplification (PA) to extract a shorter commitment $c = \mathrm{Ext}(x, r)$, which would be almost decoupled from her adversaries' share using a randomness extractor Ext. Here $r \in_R \mathcal{R}$ is picked by Alice before the commit phase and sent to Bob during the commit phase. In the next section, we will show how we can choose the right parameters to ensure that the other security requirements are also met.

We describe the structure of our protocol before we discuss our parameter choices. Fix an error correcting code with encoding map Enc and minimum distance d, and the randomness extractor Ext. Our protocol has the following structure:

Commit: Alice randomly selects a $x \in_R \{0,1\}^k$, $z \in_R \{0,1\}^n$, $\theta \in_R \{0,1\}^n$ and $r \in_R \mathcal{R}$. She outputs the random commitment $c = \mathrm{Ext}(x, r)$. Let $y := \mathrm{Enc}(x)$ and $u := y \oplus z$. She then distributes the qubits of $|\psi\rangle := H^\theta |u\rangle$ equally between the trusted nodes and privately sends the classical information (θ, z, r) to Bob.

Open: Alice publicly announces 'open' and sends x to Bob privately. The trusted parties forward their shares of $|\psi\rangle$ to Bob. Bob measures $|\psi\rangle$ in θ basis and checks if the outcome agrees with x.

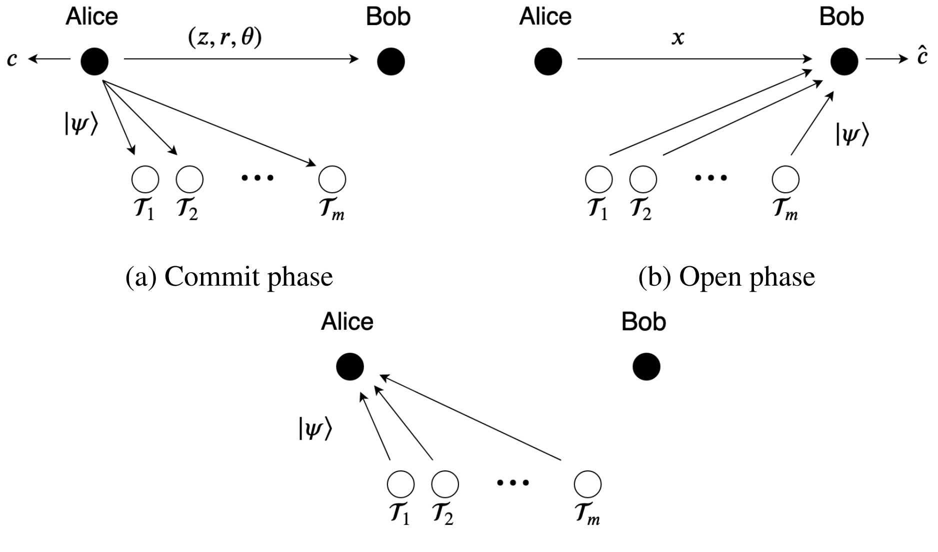
Erase: Alice publicly announces 'erase'. During the erase phase, the trusted nodes send their shares of $|\psi\rangle$ back to Alice.

We have added an extra step above, which we did not discuss earlier. Specifically, we xor the encoding of x with a random string z. This does not affect the discussion above and will be useful to prove an additional security property for the protocol (specifically the 'Expungement on successful runs' property proved in Sec. 5.6.2).

5.4.3 Choice of parameters

Consider the protocol given in the structure above. Let's start by looking at the case when both Alice and Bob are honest, and t of the trusted nodes act adversarially. We also account for at most γn of the transmissions being corrupted by the adversaries according to the channel model. Suppose $\tilde{\psi}$ is the state forwarded to Bob by the trusted parties. Let $\hat{u}$ be the string measured by Bob when he measures $\tilde{\psi}$ in the θ basis and let $\hat{y} := \hat{u} \oplus z$. Since there are at most t dishonest trusted nodes, we have that $h(y, \hat{y}) \le (t/m + \gamma)n$. So, if Alice encodes k randomly chosen bits x into $y = \mathrm{Enc}(x)$ using a $[n, k, d]$ ECC with minimum distance d satisfying $d > 2(t/m + \gamma)n$, then y is the only codeword satisfying $h(y, \hat{y}) \le (t/m + \gamma)n$ and Bob can agree with Alice's x despite t of the trusted nodes being active adversaries.

Next, we consider the case when Alice collaborates with these t adversary $\mathcal{T}_i$'s. In this scenario, is the protocol binding or could Alice hope to change her commitment during the



(a) Commit phase

(b) Open phase

(c) Erase phase

Figure 5.1: The structure of the protocol is depicted here. During the commit phase, Alice sends $|\psi\rangle$ to the trusted parties and (z, r, θ) to Bob. In case Alice chooses to open, the quantum state is forwarded to Bob. Whereas, in case of an erase, it is returned back to Alice.

open phase after the commit phase? Suppose that the minimum distance of the ECC is $d = 2tn/m + 1$. Then, it is possible that Alice could pick $\tilde{y}$ such that there exist x_1 and x_2 and corresponding codewords $y_1 = \mathrm{Enc}(x_1)$ and $y_2 = \mathrm{Enc}(x_2)$ satisfying $h(\tilde{y}, y_1) = tn/m$ and $h(\tilde{y}, y_2) = tn/m + 1$. Alice could then collaborate with the t adversarial trusted nodes to make Bob decode either x_1 or x_2 at the open phase. In order to avoid this, we require an ECC with a minimum distance $d > 4(t/m + \gamma)n$, and only have Bob accept the commitment if $\hat{y}$ is within a distance $(t/m + \gamma)n$ of an actual codeword. Otherwise, Bob outputs ”failure” because he is convinced that Alice did not provide a valid commitment. In this way, we can ensure that Alice cannot change the value of the commitment that she opens after the commit phase.

Finally, we look at the hiding properties of the protocol. First, observe that after the commit phase Bob and the adversarial trusted nodes have access to at most $(t/m + \gamma)n$ information about y. Depending on the ECC, this might reveal at most $(t/m + \gamma)n$ bits of information about x. Hence, we want to ensure that privacy amplification is applied such that $(t/m + \gamma)n$ bits of information about x reveal almost no information about Alice's commitment which is $c = \mathrm{Ext}(x, r)$. For this purpose, we would like the parameter k of the ECC to be large enough compared to $(t/m + \gamma)n$, so that the output length ℓ of the randomness extractor used during privacy amplification is $\Theta(n)$ and we can get exponential security in n. Therefore, we choose $k = \Theta(n)$, and $\ell = \Theta(n)$ such that $k - (t/m + \gamma)n - \ell = \Omega(n)$.

In this way, the information held by the adversary is essentially decoupled from Alice's commitment c after the commit phase, as well as after the protocol in both the case of an open and an erase. After the protocol, the $(m - t)$ honest-but-curious trusted nodes completely forget the quantum states they held and hence any information about x. As a result, they have no information about c either at the end of the protocol. Furthermore, the information held by the adversaries in both the case of an open and an erase is lesser than $(t/m + \gamma)n$. Thus, even if all the trusted parties and adversaries get together they would be almost decoupled from Alice's commitment.

5.4.4 Protocol

Given a security parameter n, Alice and Bob agree on an [n, k, d] ECC with encoding map $\mathrm{Enc} : \{0,1\}^k \to \{0,1\}^n$, as well as a randomness extractor $\mathrm{Ext} : \{0,1\}^k \times \mathcal{R} \to \{0,1\}^\ell$ for some ℓ which we will now define.

Let γ be the tolerable noise level. We consider a setting with m temporarily trusted nodes at most t of which act dishonestly during the protocol. As discussed above, we fix the various parameters for ECC and PA as follows. For some parameters $\delta_c > 0$ and $\delta' > 0$:

- $k = (\frac{t}{m} + \gamma + \delta_c + \delta')n$
- $\ell = \delta_c n$
- $d = 4(\frac{t}{m} + \gamma)$ n + 1

Existence of ECC and PA schemes with these parameters: It should be noted that $(t/m + \gamma)$ should be *small* to allow for the existence of ECC with the above parameters. For example, we can use the Gilbert Varshamov bound [58] to prove that such codes exist for parameters (t, m, γ) for which

$$\frac{t}{m} + \gamma < 1 - H_2\left(4\left(\frac{t}{m} + \gamma\right)\right)$$

for large enough n (here $H_2(\cdot)$ is the binary entropy function). This is inequality is satisfied as long as $t/m + \gamma \leq 0.083$. The existence of PA schemes follows from the privacy amplification theorem (see, e.g., Ref. [22] for an early version robust to quantum side information).

The three phases of the protocol are as follows.

Commit phase

1. Alice randomly picks $x \in_R \{0,1\}^k$, $z \in_R \{0,1\}^n$, $r \in_R \mathcal{R}$, $\theta \in_R \{0,1\}^n$.
2. Alice computes $c = \mathrm{Ext}(x, r)$, $y = \mathrm{Enc}(x)$, $u = y \oplus z$.

3. Alice sends z, r, θ to Bob, who acknowledges reception through broadcast.

4. Alice prepares $|\psi\rangle = H^{\theta} |u\rangle$.

5. Alice distributes the qubits of $|\psi\rangle$ evenly between $\mathcal{T}_1 \ldots \mathcal{T}_m$ (sends n/m qubits to each trusted party).

6. $\mathcal{T}_1 \ldots \mathcal{T}_m$ verify that ψ is in span $\{|0\rangle, |1\rangle\}^n$, and all acknowledge reception through broadcast.

7. Alice outputs $c \in \{0, 1\}^{\ell}$.

Open phase

1. On input ”open”, Alice broadcasts ”open” and sends x to Bob.

2. $\mathcal{T}_1 \ldots \mathcal{T}_m$ send ψ to Bob.

3. Bob measures $H^{\theta}(\psi)$ in computational basis, gets outcome $\hat{u}$.

4. Bob decodes $\hat{y} = \hat{u} \oplus z$.

5. Bob computes $y' = \mathrm{Enc}(x)$ and $h = h(\hat{y}, y')$.

6. If $h > (\frac{t}{m} + \gamma)n$, Bob outputs $\hat{c} = 0^{\ell}$ and $F_B = \mathrm{failure}$, else output $\hat{c} = \mathrm{Ext}(x, r)$ and $F_B = \mathrm{success}$. Bob broadcasts F_B and Alice outputs $F_A = F_B$.

Erase phase

1. On input ”erase”, Alice broadcasts ”erase”.

2. $\mathcal{T}_1 \ldots \mathcal{T}_m$ send ψ back to Alice.

3. Alice measures $H^{\theta}(\psi)$ in computational basis, gets outcome $\hat{u}$.

4. Alice computes $\hat{y} = \hat{u} \oplus z$ and $h = h(\hat{y}, y)$.

5. If $h > (\frac{t}{m} + \gamma)n$, Alice outputs $F_A = \mathrm{failure}$, else she output $F_A = \mathrm{erase}$.

6. Alice broadcasts F_B and Bob outputs $F_B = F_A$ and $\hat{c} = 0^{\ell}$.

5.5 Security of the protocol

We now informally prove that our protocol satisfies the security requirements given in Section 5.3.1. Throughout we assume that we are in a setting with m temporarily trusted third parties $\mathcal{T}_i$'s out of which at most t can be dishonest during the protocol, and that γ is the acceptable rate of noise for the quantum channels. After the completion of the protocol, the trusted parties may bring the information they gathered during the protocol together and collaborate with the adversaries. Once again, we point the reader to Appendix B.3.3 for formal security definitions and their proofs.

5.5.1 Correctness: Dishonest trusted nodes cannot change the commitment

Claim 1. *For honest Alice and honest Bob, the protocol is correct: If Alice outputs c during the commit phase, then Bob outputs $\hat{c} = c$ and $F_B = \text{success}$ during the open phase..*

Suppose Alice follows the protocol honestly and prepares (x, r, z, θ) and $|\psi\rangle$ as required by the protocol. Then, her output is $c = \text{Ext}(x, r)$. Since, at least $(m - t)$ of the trusted nodes are honest-but-curious during the protocol, the $\hat{y}$ measured by Bob satisfies $h(y, \hat{y}) \leq (t/m + \gamma)n$ as the adversarial trusted nodes only have access to at most $(t/m + \gamma)n$ qubits. Thus, Bob accepts Alice's x and outputs $\hat{c}$ which is equal to c.

5.5.2 Binding for Alice after the commit phase

Claim 2. *For an honest Bob, the protocol is binding for Alice after the execution of the commit phase: After the commit phase, there exists a classical variable $\tilde{C}$ such that Alice is commited to $\tilde{C}$, i.e. during the open phase, with high probability, either Bob accepts the commitment ($F_B = \text{success}$) and receives an output $\hat{C}$ such that $\hat{C} = \tilde{C}$, or Bob rejects the commitment ($F_B = \text{failure}$). (As before this guarantee only makes sense in the case that the open protocol is run after the commit protocol.)*

Suppose Alice sends some $\tilde{\rho}$ to the trusted nodes and (θ, r, z) to Bob. Once they are handed over to the trusted nodes, all the qubits of $\tilde{\rho}$, except for at most $(t/m + \gamma)n$ qubits which are controlled by the dishonest $\mathcal{T}_i$'s and adversarial noise, remain unchanged. Therefore, if we can show that Alice can't change her commitment by modifying any set of $(t/m + \gamma)n$ qubits we will be done. This is achieved by using a classical ECC with distance $d > 4(t/m + \gamma)n$ and having Bob reject the received message $\hat{y}$ when there is no codeword in a $(t/m + \gamma)n$ ball around $\hat{y}$.

The fact that Alice is committed to a classical variable $\tilde{C}$ after the commit phase if the commitment were to be opened can be seen by using a simulator based argument. Fundamentally, if the open phase were to be conducted right after the commit phase then Bob would measure a random variable $\tilde{Y}$ when he measures $\tilde{\rho}$ in the θ basis and xors the output with z. He could then use $\tilde{Y}$ to figure out Alice's commitment $\tilde{C}$. It will be shown that once Alice commits to a particular instance of this random variable, she cannot change it during the open phase. A formal simulator based argument for this is given in Appendix B.3.3.4.

After the commit phase, we define $\tilde{Y}$ as above. Let us consider a particular instance of this random variable $\tilde{y}$. Let $\bar{y}$ be a codeword at a distance less than or equal to $2(t/m+\gamma)n$ away from $\tilde{y}$. Note that there exists at most one such $\bar{y}$ since the minimum distance d satisfies $d = 4(t/m+\gamma)n+1$. If there is no such $\bar{y}$, then even after modifying $(t/m+\gamma)n$ positions of $\tilde{y}$ the distance from any codeword is still greater than $(t/m+\gamma)n$ and Bob rejects any x Alice tries to open, so let us focus on the case where there exists a unique such $\bar{y}$. We will show that in this instance Bob either accepts the commitment corresponding to $\bar{y}$ or the protocol ends in failure. Let $\hat{y}$ be as defined in the protocol. Alice's actions can either bring $\hat{y}$ closer to $\bar{y}$ or take it away from it. If her actions manage to get $\hat{y}$ within a distance of $(t/m+\gamma)n$ from $\bar{y}$, then the commitment corresponding to $\bar{y}$ would be accepted by Bob. On the other hand, no matter how she modifies her string, she cannot come within a distance of $(t/m+\gamma)n$ of some other codeword y', since the distance between y' and $\tilde{y}$ would be greater than $2(t/m+\gamma)n$ and she only has access to $(t/m+\gamma)n$ qubits. Since for every instance of $\tilde{Y}$ Alice cannot change her commitment after the commit phase, the protocol is binding.

5.5.3 Hiding for the adversaries after the commit phase

Claim 3. *The protocol is hiding for honest Alice after commit: If Alice is honest and she receives the output c during the commit phase, then, after the commit phase and before the open or erase phase, Bob and the dishonest trusted nodes together can only extract negligible information about c, i.e., their joint state is almost decoupled from Alice's commitment.*

Let E be the set of dishonest trusted parties and $\bar{E}$ the set of honest-but-curious nodes. Together the adversaries have access to at most $(t/m+\gamma)n$ qubits of $|\psi\rangle$, z and θ. Let's say the adversaries' qubits are in the quantum memory T_E. Further, suppose that these qubits encode the string y_E (the string y corresponding to the positions of the qubits held by E). Then, we have

$$\begin{aligned}
\mathrm{H}_{\min}(X|T_E, Z, \Theta) &= \mathrm{H}_{\min}(Y|T_E, Z, \Theta) \\
&\geq \mathrm{H}_{\min}(Y|Y_E, Z, \Theta) \\
&= \mathrm{H}_{\min}(Y|Y_E) \\
&\geq \mathrm{H}_{\min}(Y) - |Y_E| \\
&= \mathrm{H}_{\min}(X) - |Y_E| \\
&\geq k - (\frac{t}{m} + \gamma) \\
&= (\delta_c + \delta')n.
\end{aligned}$$

The first equality follows since $Y = \mathrm{Enc}(X)$ and Enc is a deterministic one-to-one function, the inequality on the second line is a result of applying the data processing inequality, the equality in the third line follows from the fact that Z, Θ are independent of Y and the inequality in the fourth line follows from the chain rule for min-entropy ($|Y_E|$ is the length of the string Y_E).

Since $\ell = \delta_c n$, $\mathrm{H}_{\min}(X|T_E, Z, \Theta) - \ell \geq \delta' n$ and by PA theorem, it holds that for any set of adversaries with access limited to these many qubits, the quantum memory T_E is almost independant of the output c of Alice's randomized commitment, even if one is given z and θ. Hence, the claim holds true.

5.5.4 Hiding for all trusted parties and Bob together after the erase phase

Claim 4. *The protocol is hiding for honest Alice after the erase phase: If Alice is honest and she receives the output* c *during the commit phase, then, after the erase phase, Bob and the* $\mathcal{T}_i$*'s together can only extract negligible information about* c*, i.e., their joint state is almost decoupled from Alice's commitment.*

At the end of the erase phase, once again all the parties together have at most $(t/m + \gamma)n$ qubits of $|\psi\rangle$. The rest of the qubits are completely forgotten by the $(m - t)$ quantum honest-but-curious nodes, and the content of their register $T_{\bar{E}}$ is independent of x. Further, Bob does not get any additional information during the erase phase. Therefore, similar to above, we get

$$\mathrm{H}_{\min}(X|T_E, T_{\bar{E}}, Z, \Theta) \geq (\delta_c + \delta')n$$

and the hiding property holds for the $\mathcal{T}_i$'s and Bob after the erase phase.

5.5.5 Hiding for all the trusted parties together after the open phase

Claim 5. *The protocol is hiding for honest Alice and honest Bob after an open phase: If Alice and Bob are honest and Alice's commitment is* c*, then, after an open phase, the* $\mathcal{T}_i$*'s together can only extract negligible information about* c*, i.e., their joint state is almost decoupled from Alice's commitment.*

The information held by all the trusted nodes in this case is lesser than their information in the case of an erase. The claim follows easily by following the argument in Section 5.5.4.

5.6 Additional security properties

5.6.1 Decoupling of honest-but-curious nodes during the protocol

Our protocol satisfies a stronger hiding property than one given in Section 5.3.1. In addition to being hiding for Bob and the dishonest trusted nodes during the commit stage, the protocol is also hiding for the honest-but-curious trusted nodes in the sense that the qubits they hold locally are also approximately decoupled from Alice's commitment. A similar strong security definition was used by Ref. [53] for their protocols on secure evaluation of unitaries against honest-but-curious adversaries. In particular, their security definition demands that at any point in the protocol the state held by the honest-but-curious party can be reproduced by applying a quantum channel on the honest-but-curious party's share of the initial or final state. This definition ensures that the honest-but-curious party never has access to more information than it needs to. It is based on a definition given in Ref. [59] for statistical zero knowledge proofs. However, we feel that this definition is too strong for our purposes, since in the quantum domain one can force the honest-but-curious parties to 'forget' quantum information. So, it is possible that at some point in a protocol a honest-but-curious party holds too much information in its quantum state, but the protocol is such that at a later point the party is forced to return the information and hence 'forgets' it. This is the behaviour that we try to encapsulate in our security definition of erasable bit commitment in a setting with temporarily trusted parties. We only insist that at the end of the protocol, the state held by the honest-but-curious nodes are completely decoupled from the commitment. Nevertheless, as mentioned earlier, the protocol presented in this chapter satisfies the following stronger security requirement used by Ref. [53].

Claim 6. *For an honest Alice, the protocol is locally hiding for all the honest-but-curious nodes: the local quantum state of the honest-but-curious nodes is almost decoupled from Alice's output* c *throughout the protocol.*

This can be proven using the same argument as that of hiding for adveraries (Sec. 5.5.3). After the commit phase, an honest-but-curious node $\mathcal{T}_i$ for $i \in \bar{E}$ has access to only n/m qubits in his quantum memory $T_{\bar{E}_i}$. Therefore, we once again have the following min-entropy guarantee

$$\begin{aligned} \mathrm{H}_{\min}(X|T_{\bar{E}_i}) &\geq \mathrm{H}_{\min}(X) - \log(|T_{\bar{E}_i}|) \\ &\geq (\delta_c + \delta')n. \end{aligned}$$

5.6.2 Expungement on successful runs

In this section, we show that our protocol has an additional property whenever it is successful, namely that it guarantees that the commitment is indeed 'expunged' from the memories of the trusted nodes, or that the trusted nodes indeed 'forget' about the commitment. In order to prove this, we only need to assume that the trusted nodes did not collaborate with Bob. We do not even need to assume that the trusted nodes acted honestly. The assumption that Bob does not collaborate with the trusted nodes is necessary, since he knows the choice of basis θ, and given the basis, the trusted parties could measure $|\psi\rangle$ without disturbing it. In a sense, all we need to implement our protocol are three sets of parties which do not communicate with each other unless required by the protocol; this is similar to the type of assumptions used in relativistic bit commitment and we further explore the link between our setting and that of relativistic bit commitment in the conclusion. Hence, it seems that the trust assumption required by our protocol is fairly weak. Further, this security claim also allows us to move closer to the definition of honest-but-curious parties in multi-party protocols given in Ref. [53], which permits such parties to communicate and collaborate with each other.

5.6.2.1 Expungement after the erase phase

Claim 7. *For an honest Alice and* $F_A = \text{erase}$*, if Bob does not collaborate with the trusted parties during the execution of the protocol, then the protocol is hiding for all the trusted parties and Bob together after the execution of an erase phase, even if the trusted parties collaborate and act arbitrarily during the protocol.*

The setup for this is similar to one for QKD, with Alice after the erase phase acting as ”QKD-Bob”. Since, we assume that Bob does not collaborate with the trusted parties, they must handle $|\psi\rangle = H^\theta |u\rangle$ and return it to Alice without knowing anything about θ or u. Upon receiving ψ back, Alice measures it according to θ and only accepts if the measured error rate is at most γ. This is indeed similar to a QKD setup, and standard methods [60–62] allow us to show that, even if θ is revealed, in the case of an accepted run,

$$\mathrm{H}^{\epsilon}_{\min}(U|T\Theta) \geq n(1 - H_2(\gamma + \mu_\epsilon)) - \delta_\epsilon, \tag{5.2}$$

for parameters μ_ϵ, δ_ϵ, and T the memory held by the trusted parties after the erase phase. This is not quite sufficient for our purposes, since we want to make sure that the min-entropy about x is high even if, after the protocol, B and the $\mathcal{T}_i$'s get together, i.e., we want to prove that $\mathrm{H}^{\epsilon'}_{\min}(X|T\Theta Z)$ is large. Using among other tools chain rules for smooth min-entropy [63], we show precisely this in the Appendix B.5.2.

Note that we could even allow for Bob and a small set $\mathcal{T}_E$ of the trusted nodes such that $E \subset [m]$ and $|E| \leq t$ to collaborate with Bob, as long as the remaining $(m - t)$ trusted nodes do not interact with $\mathcal{T}_E$ and Bob.

5.6.2.2 Expungement after the open phase

Claim 8. *For honest Alice and honest Bob, and* $F_A = F_B = \mathit{success}$ *after the execution of an open, the protocol is hiding for all the trusted nodes even if they collaborate and act arbitrarily during the protocol.*

The argument follows similarly as for the previous claim, now with Bob acting as ”QKD-Bob”, except that the adversary has even less information since we assume Alice and Bob are both honest.

5.7 Conclusion

5.7.1 Avoiding quantum no-go results

In this work, we introduced a new primitive, erasable bit commitment, as well as a new paradigm, that of temporary quantum trust. The temporary trust assumption allows us to avoid no-go results for quantum bit commitment: if Bob and the trusted nodes were to put their information together right after the commit phase, they would be able to extract the value of Alice's commitment. Hence, the protocol is not hiding against a coalition of Bob and all the trusted nodes. In fact, no protocol which is hiding for both Bob and the trusted nodes can be binding for Alice according to the no-go theorem for quantum bit commitment. As already noted, our robust protocol, which makes use of a constant number of trusted nodes, is even robust against a coalition of Bob and a small constant fraction of trusted nodes, as long as the other trusted nodes are indeed acting honest-but-curiously and do not communicate with Bob during the execution period. Note that for security against a dishonest Alice, we cannot guarantee that she is still committed to a classical value at the end of an erase phase. Hence, this primitive is weaker than a standard two-party bit commitment whenever an erase rather than an open might be required.

5.7.2 Comparison to other variants on quantum bit commitment

5.7.2.1 Bounded and noisy quantum storage model:

In the bounded and noisy quantum storage model [13, 51, 64], security of bit commitment is ensured by assuming that the parties do not have access to perfect quantum memory. This assumption allows for the implementation of the stronger, regular version of bit commitment. In our protocol, for the duration of the trust period, the trusted node must maintain Alice's commitment in memory, but they do not need to further manipulate it. In some sense, the requirements here are complementary to those in the noisy storage model. In the noisy storage model, an honest Alice waits for a long enough period for the content of a dishonest Bob's quantum memory to decay sufficiently before announcing her basis. Here, the temporary trust period must be sufficiently short to prevent the contents of the trusted nodes' quantum memories from decaying too much before they are transmitted to Bob. Hence, as progress in physical implementations allows for better and better quantum memory and the power of the noisy storage model decreases, our model allows for longer trust period if so desired. We believe that efforts towards the physical implementation of this protocol could be an interesting stepping stone towards more complicated multi-node protocols.

5.7.2.2 Relativistic bit commitment:

In relativistic quantum bit commitment [65–68], Alice and Bob are split into various nodes at different locations, and the security of the scheme follows from the impossibility of communication between these nodes which is enforced from relativistic constraints. Hence, Alice has to have complete trust into all of the nodes which are corresponding to her, and similarly for Bob. Contrary to our temporary trust setting, there is no need for nodes which are trusted by both parties. However, the mutual trust between all nodes associated to Alice is usually assumed to be everlasting rather than time-limited as in our setting, and similarly for Bob. Similar to our protocol, relativistic bit commitment is also weaker than bit commitment in the case where the commitment is not opened.

It would be interesting to see if our protocol can be modified to fit the relativistic framework, by splitting the temporarily trusted nodes into nodes which are temporarily trusted by Alice and nodes which are temporarily trusted by Bob, while keeping only a single main Alice node and a single main Bob node.

5.7.2.3 Cheat-sensitive bit commitment:

In cheat-sensitive bit commitment [69–71], it is possible that a dishonest party is able to cheat with a non-trivial probability, but it can be caught cheating by the honest party with a non-zero probability too. We prove something similar in one of our additional security claims. We showed that if Bob does not communicate with the trusted nodes, then the trusted nodes cannot cheat without getting caught with high probability. It might be possible to create stronger versions of cheat-sensitive bit commitment in our trusted party setting.

Chapter 6

Conclusion and Outlook

In this thesis, we studied optical communication protocols and cryptography with temporarily trusted parties. We took the first steps towards reformulating quantum communication protocols in terms of coherent states and understanding the resource tradeoffs for optical protocols. In Chapter 3, we characterized the Gram matrices of coherent states in an attempt to understand when it is possible to switch the qudit states used in a communication protocol with coherent states. However, our work leaves several unanswered questions. An important one of these is to determine if we can efficiently classify matrices as Gram matrices of coherent states or not. The algorithm given in Section 3.2 for this task requires $\exp(O(n^2))$ time. It might be possible to solve this task more efficiently by using semidefinite programming and rounding methods. Furthermore, our numerical work suggests that there is considerable redundancy between the conditions our current algorithm checks. We also showed that mutually unbiased bases (MUBs) do not lie in the closure of the set of Gram matrices of coherent states. Another question we leave open is to determine how well one can approximate MUBs using coherent states. This might also be an interesting question from the viewpoint of cryptography and specifically quantum key distribution since MUBs are maximally incompatible, that is, they maximize the entropic uncertainty relations [72].

This leads to an interesting direction for future work: studying finite approximations of Gram matrices using Gram matrices of coherent states. How far is a matrix from the closure of the set of Gram matrices of coherent states, if it does not lie in this set? Also, which coherent states could be used to best approximate this matrix? Another interesting direction would be to extend our characterization to squeezed states and Gaussian states, which are also easy to create experimentally. Understanding the class of protocols which can be implemented using these different sets of states would also shed light on the kind of quantum resources required to implement these protocols. It would help us understand how different states of light can be used to perform different communication tasks. This is equivalent to studying the kinds of communication resources different states of light constitute. Numerous studies have explored such resource theories in optics [73–75]. It would further be interesting to see if this line of work can be connected with these existing resource theories. Our work only considers the reformulation of the quantum states used in communication protocols. In order to implement a protocol, the measurements and operations used during the protocol also need to be easy to implement. Future work in this area should also look in this direction.

Lastly, the Gram matrices of a set of states encodes the information about these states relative to each other. A characterization of Gram matrices can be used as tool for solving other problems as well. The state discrimination problem for pure states can be completely characterized in terms of their Gram matrix. It might be possible to use our characterization to derive analytical solutions or bounds for the state discrimination problem for coherent states. Similarly, Gram matrices also play an important role in the proof of the partial results given in Ref. [76] towards lower bounds on stabilizer ranks. It might be possible to extend such ideas to the field of continuous-variable quantum computation using our characterization.

In Chapter 4, we turned our attention to improving the implementation of quantum communication protocols. We discussed our collaboration with with an experimental group to implement the quantum fingerprinting protocol with the objective of beating the classical information leakage bound. We also studied the bounds on the growth of the mean photon number and the number of modes of a protocol for optical quantum commmunication protocols in the simultaneous message passing model. Firstly, it would be interesting to see if we can generalize our bounds to protocols in more general and interesting communication models (for example, to two party interactive communication protocols). Further, it is also not clear at this point if these are the tightest possible lower bounds for these resources in this model. It would be interesting to see if one can come up with tighter tradeoff bounds for communication protocols which use only coherent states and Gaussian states.

We further developed tighter tradeoff relations for coherent state quantum fingerprinting (QFP) protocols. We showed that the coherent state protocol given in Ref. [12] is almost optimal and can only be improved by at most a constant factor. We also suggested a protocol to improve the rate of coherent state QFP protocols by about 20. It would be interesting to see if the suggested protocol can be implemented experimentally. As stated earlier, squeezed states and Gaussian states are also easy to implement. Whether or not one can use squeezed states (or other easy-to-implement states) to make the QFP protocol faster still remains an open question.

Finally, in Chapter 5, we introduced the temporarily trusted party setting and gave a protocol for erasable bit commitment (EBC) in this setting. Our EBC protocol used BB84 states. We believe that these can be replaced with coherent states in a straighforward fashion to make implementation more robust. However, further work needs to be carried out to show this. In order to make the protocol more experimentally viable, it should be determined if the protocol can be modified so that it does not require the use of quantum memories (as is the case with the noisy storage protocols [13]). Quantum memories are very lossy and difficult to create. It would indeed be very difficult to demonstrate a protocol, like ours, with a large number of quantum memories.

It would also be interesting to further study the applications of the erasable bit commitment primitive. Bit commitment can be used to implement several interesting protocols like coin flipping and secure evaluation of unitaries against specious adversaries [53]. It is also not clear if the standard *stronger* version of bit commitment can be implemented in the trusted party setting. More generally, we also need to further study the temporarily trusted setting and determine if other interesting cryptographic primitives are also possible in this setting. Further work is also needed to understand the absolute limits of this setting. For example to determine the minimum number of trusted parties required to implement EBC. Another interesting direction for future research would be to relate the temporarily trusted setting and the relativistic setting [65, 68]. In particular, is there a way to implement bit commitment, with the help of relativistic constraints, such that some subset of the temporarily trusted parties is only trusted by Alice and the others are only trusted by Bob.

References

[1] Ashutosh S. Marwah and Norbert Lütkenhaus. Characterization of gram matrices of multimode coherent states. *Phys. Rev. A*, 99:012346, Jan 2019.

[2] Ashutosh S. Marwah and Norbert Lütkenhaus. Erratum: Characterization of gram matrices of multimode coherent states [phys. rev. a 99, 012346 (2019)]. *Phys. Rev. A*, 99:049903, Apr 2019.

[3] Jian-Yu Guan, Feihu Xu, Hua-Lei Yin, Yuan Li, Wei-Jun Zhang, Si-Jing Chen, Xiao-Yan Yang, Li Li, Li-Xing You, Teng-Yun Chen, Zhen Wang, Qiang Zhang, and Jian-Wei Pan. Observation of quantum fingerprinting beating the classical limit. *Phys. Rev. Lett.*, 116:240502, Jun 2016.

[4] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7 – 11, 2014. Theoretical Aspects of Quantum Cryptography celebrating 30 years of BB84.

[5] Artur K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67:661–663, Aug 1991.

[6] Harry Buhrman, Richard Cleve, and Avi Wigderson. Quantum vs. classical communication and computation. In *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*, STOC '98, pages 63–68, New York, NY, USA, 1998. ACM.

[7] Harry Buhrman, Richard Cleve, John Watrous, and Ronald de Wolf. Quantum fingerprinting. *Phys. Rev. Lett.*, 87:167902, Sep 2001.

[8] 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*, STOC '04, pages 128–137, New York, NY, USA, 2004. ACM.

[9] Dmitry Gavinsky, Julia Kempe, Iordanis Kerenidis, Ran Raz, and Ronald de Wolf. Exponential separations for one-way quantum communication complexity, with applications to cryptography. In *Proceedings of the Thirty-ninth Annual ACM Symposium on Theory of Computing*, STOC '07, pages 516–525, New York, NY, USA, 2007. ACM.

[10] Frédéric Grosshans, Gilles Van Assche, Jérôme Wenger, Rosa Brouri, Nicolas J. Cerf, and Philippe Grangier. Quantum key distribution using gaussian-modulated coherent states. *Nature*, 421, 01 2003.

[11] Feihu Xu, Juan Miguel Arrazola, Kejin Wei, Wenyuan Wang, Pablo Palacios-Avila, Chen Feng, Shihan Sajeed, Norbert Lütkenhaus, and Hoi-Kwong Lo. Experimental quantum fingerprinting with weak coherent pulses. *Nature Communications*, 6:8735 EP –, 10 2015.

[12] 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.

[13] Robert Konig, Stephanie Wehner, and Jürg Wullschleger. Unconditional security from noisy quantum storage. *IEEE Transactions on Information Theory*, 58(3):1962–1984, 2012.

[14] Renato Renner. *Security of Quantum Key Distribution*. PhD thesis, -, Dec 2005.

[15] Michael Ben-Or, Michał Horodecki, Debbie W. Leung, Dominic Mayers, and Jonathan Oppenheim. The universal composable security of quantum key distribution. In Joe Kilian, editor, *Theory of Cryptography*, pages 386–406, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg.

[16] John Watrous. *The Theory of Quantum Information*. Cambridge University Press, 2018.

[17] Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory (Wiley Series in Telecommunications and Signal Processing)*. Wiley-Interscience, New York, NY, USA, 2006.

[18] Charles H. Bennett, Peter W. Shor, John A. Smolin, and Ashish V. Thapliyal. Entanglement-assisted classical capacity of noisy quantum channels. *Phys. Rev. Lett.*, 83:3081–3084, Oct 1999.

[19] Mark M. Wilde. *Quantum Information Theory*. Cambridge University Press, 2013.

[20] Robert König, Renato Renner, and Christian Schaffner. The operational meaning of min- and max-entropy. *IEEE Trans. Inf. Theor.*, 55(9):4337–4347, September 2009.

[21] Marco Tomamichel. Quantum Information Processing with Finite Resources - Mathematical Foundations. *arXiv e-prints*, page arXiv:1504.00233, Apr 2015.

[22] Renato Renner and Robert König. Universally composable privacy amplification against quantum adversaries. In Joe Kilian, editor, *Theory of Cryptography*, pages 407–425, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg.

[23] Christopher Gerry and Peter Knight. *Introductory Quantum Optics*. Cambridge University Press, 2004.

[24] Mark Hillery. Classical pure states are coherent states. *Physics Letters A*, 111(8):409 – 411, 1985.

[25] R.L. Hudson. When is the wigner quasi-probability density non-negative? *Reports on Mathematical Physics*, 6(2):249 – 252, 1974.

[26] Werner Vogel and Dirk-Gunnar Welsch. *Quantum Optics*. John Wiley & Sons, 2006.

[27] Eyal Kushilevitz and Noam Nisan. *Communication Complexity*. Cambridge University Press, 1996.

[28] Anup Rao and Amir Yehudayoff. *Communication Complexity: and Applications*. Cambridge University Press, 2019.

[29] L. Babai and P. G. Kimmel. Randomized simultaneous messages: solution of a problem of yao in communication complexity. In *Proceedings of Computational Complexity. Twelfth Annual IEEE Conference*, pages 239–246, June 1997.

[30] Frédéric Grosshans and Philippe Grangier. Continuous variable quantum cryptography using coherent states. *Physical review letters*, 88:057902, 2002.

[31] Ch. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs. Continuous variable quantum cryptography: Beating the 3 db loss limit. *Phys. Rev. Lett.*, 89:167901, Sep 2002.

[32] Ryan Amiri and Juan Miguel Arrazola. Quantum money with nearly optimal error tolerance. *Phys. Rev. A*, 95:062334, Jun 2017.

[33] Jian-Yu Guan, Juan Miguel Arrazola, Ryan Amiri, Weijun Zhang, Hao Li, Lixing You, Zhen Wang, Qiang Zhang, and Jian-Wei Pan. Experimental preparation and verification of quantum money. *Phys. Rev. A*, 97:032338, Mar 2018.

[34] Juan Miguel Arrazola and Dave Touchette. Quantum advantage on information leakage for equality. *CoRR*, abs/1607.07516, 2016.

[35] Anthony Chefles, Richard Jozsa, and Andreas Winter. On the existence of physical transformations between sets of quatum states. *International Journal of Quantum Information*, 02(01):11–21, 2004.

[36] Anthony Chefles. Deterministic quantum state transformations. *Physics Letters A*, 270(1):14 – 19, 2000.

[37] J.C. Gower. Euclidean distance geometry. *Math. Scientist*, 7:1–14, 1982.

[38] Jon Dattorro. *Convex Optimisation and Euclidean Distance Geometry*. Meboo Publishing USA, 2017.

[39] Juan Miguel Arrazola and Norbert Lütkenhaus. Quantum communication with coherent states and linear optics. *Phys. Rev. A*, 90:042335, Oct 2014.

[40] Béla Bollobás. *Linear Analysis: An Introductory Course*. Cambridge University Press, 2 edition, 1999.

[41] Ingemar Bengtsson. Three ways to look at mutually unbiased bases. *AIP Conference Proceedings*, 889(1):40–51, 2007.

[42] Benjamin Lovitz and Norbert Lütkenhaus. Families of quantum fingerprinting protocols. *Phys. Rev. A*, 97:032340, Mar 2018.

[43] A. Chakrabarti, Yaoyun Shi, A. Wirth, and A. Yao. Informational complexity and the direct sum problem for simultaneous message complexity. In *Proceedings 42nd IEEE Symposium on Foundations of Computer Science*, pages 270–278, Oct 2001.

[44] Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical review letters*, 78(17):3414, 1997.

[45] Hoi-Kwong Lo and Hoi Fung Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78(17):3410, 1997.

[46] Gilles Brassard, Claude Crépeau, Dominic Mayers, and Louis Salvail. A brief review on the impossibility of quantum bit commitment. *arXiv e-prints*, pages quant–ph/9712023, Dec 1997.

[47] Giacomo Mauro D'Ariano, Dennis Kretschmann, Dirk Schlingemann, and Reinhard F. Werner. Reexamination of quantum bit commitment: The possible and the impossible. *Phys. Rev. A*, 76:032328, Sep 2007.

[48] Severin Winkler, Marco Tomamichel, Stefan Hengl, and Renato Renner. Impossibility of growing quantum bit commitments. *Phys. Rev. Lett.*, 107:090502, Aug 2011.

[49] Ivan B Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. Cryptography in the bounded-quantum-storage model. *SIAM Journal on Computing*, 37(6):1865–1890, 2008.

[50] Ivan B Damgård, Serge Fehr, Renato Renner, Louis Salvail, and Christian Schaffner. A tight high-order entropic quantum uncertainty relation with applications. In *Annual International Cryptology Conference*, pages 360–378. Springer, 2007.

[51] Stephanie Wehner, Christian Schaffner, and Barbara M Terhal. Cryptography from noisy storage. *Physical Review Letters*, 100(22):220502, 2008.

[52] Ronald Rivest. Unconditionally secure commitment and oblivious transfer schemes using private channels and a trusted initializer. *Unpublished manuscript*, 1999.

[53] Frédéric Dupuis, Jesper Buus Nielsen, and Louis Salvail. Secure two-party quantum evaluation of unitaries against specious adversaries. In *Annual Cryptology Conference*, pages 685–706. Springer, 2010.

[54] Claude Crépeau. Quantum oblivious transfer. *Journal of Modern Optics*, 41(12):2445–2454, 1994.

[55] Anne Broadbent, Gus Gutoski, and Douglas Stebila. Quantum one-time programs. In *Annual Cryptology Conference*, pages 344–360. Springer, 2013.

[56] Debbie Leung and Graeme Smith. Communicating over adversarial quantum channels using quantum list codes. *IEEE transactions on information theory*, 54(2):883–887, 2008.

[57] Claude Crépeau. Efficient cryptographic protocols based on noisy channels. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 306–317. Springer, 1997.

[58] Florence Jessie MacWilliams and Neil James Alexander Sloane. *The theory of error-correcting codes*, volume 16. Elsevier, 1977.

[59] J. Watrous. Limits on the power of quantum statistical zero-knowledge. In *The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002. Proceedings.*, pages 459–468, Nov 2002.

[60] Marco Tomamichel and Renato Renner. Uncertainty relation for smooth entropies. *Physical review letters*, 106(11):110506, 2011.

[61] Marco Tomamichel, Charles Ci Wen Lim, Nicolas Gisin, and Renato Renner. Tight finite-key analysis for quantum cryptography. *Nature communications*, 3:634, 2012.

[62] Niek J Bouman and Serge Fehr. Sampling in a quantum population, and applications. In *Annual Cryptology Conference*, pages 724–741. Springer, 2010.

[63] Alexander Vitanov, Frederic Dupuis, Marco Tomamichel, and Renato Renner. Chain rules for smooth min-and max-entropies. *IEEE Transactions on Information Theory*, 59(5):2603–2612, 2013.

[64] Ivan B. Damgard, Serge Fehr, Louis Salvail, and Christian Schaffner. Cryptography in the bounded quantum-storage model. In *Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science*, FOCS '05, pages 449–458, Washington, DC, USA, 2005. IEEE Computer Society.

[65] Adrian Kent. Unconditionally secure bit commitment. *Phys. Rev. Lett.*, 83:1447–1450, Aug 1999.

[66] Adrian Kent. Unconditionally secure bit commitment with flying qudits. *New Journal of Physics*, 13(11):113015, nov 2011.

[67] Adrian Kent. Unconditionally secure bit commitment by transmitting measurement outcomes. *Phys. Rev. Lett.*, 109:130501, Sep 2012.

[68] J. Kaniewski, M. Tomamichel, E. Hnggi, and S. Wehner. Secure bit commitment from relativistic constraints. *IEEE Transactions on Information Theory*, 59(7):4687–4699, July 2013.

[69] Lucien Hardy and Adrian Kent. Cheat sensitive quantum bit commitment. *Phys. Rev. Lett.*, 92:157901, Apr 2004.

[70] Harry Buhrman, Matthias Christandl, Patrick Hayden, Hoi-Kwong Lo, and Stephanie Wehner. Possibility, impossibility, and cheat sensitivity of quantum-bit string commitment. *Phys. Rev. A*, 78:022316, Aug 2008.

[71] Guang Ping He. Security bound of cheat sensitive quantum bit commitment. *Scientific Reports*, 5:9398 EP –, 03 2015.

[72] Patrick J. Coles, Mario Berta, Marco Tomamichel, and Stephanie Wehner. Entropic uncertainty relations and their applications. *Rev. Mod. Phys.*, 89:015002, Feb 2017.

[73] Ludovico Lami, Bartosz Regula, Xin Wang, Rosanna Nichols, Andreas Winter, and Gerardo Adesso. Gaussian quantum resource theories. *Phys. Rev. A*, 98:022335, Aug 2018.

[74] Ryuji Takagi and Quntao Zhuang. Convex resource theory of non-gaussianity. *Phys. Rev. A*, 97:062337, Jun 2018.

[75] Benjamin Yadin, Felix C. Binder, Jayne Thompson, Varun Narasimhachar, Mile Gu, and M. S. Kim. Operational resource theory of continuous-variable nonclassicality. *Phys. Rev. X*, 8:041038, Dec 2018.

[76] Sergey Bravyi, Dan Browne, Padraic Calpin, Earl Campbell, David Gosset, and Mark Howard. Simulation of quantum circuits by low-rank stabilizer decompositions. *arXiv e-prints*, page arXiv:1808.00128, Jul 2018.

[77] M. Franceschetti, O. Dousse, D. N. C. Tse, and P. Thiran. Closing the gap in the capacity of wireless networks via percolation theory. *IEEE Transactions on Information Theory*, 53(3):1009–1018, March 2007.

[78] Frédéric Dupuis, Mario Berta, Jürg Wullschleger, and Renato Renner. One-shot decoupling. *Communications in Mathematical Physics*, 328(1):251–284, 2014.

APPENDICES

Appendix A

Known results used for Chapter 4

A.1 A simple combinatorial inequality

Lemma A.1. *For* $n, m \in \mathbb{N}$ *we have*

$$\binom{n+m}{m} \leq (1+m)^n.$$

Proof. Observe that

$$\begin{aligned}\binom{n+m}{m} &= \frac{(n+m)!}{m!\,n!} \\ &= \frac{m+n}{n} \cdot \frac{m+n-1}{n-1} \cdots \frac{m+1}{1} \\ &\leq (1+m)^n.\end{aligned}$$

□

A.2 Proof of Theorem 4.2

To prove the theorem, we use the Chernoff bound, which we state here for completeness.

Theorem A.1 (Chernoff Bound)**.** *For a random variable, X, the following bound holds*

$$P(X \geq a) \leq \inf_{t \geq 0} \left\{ \frac{\mathbb{E}[e^{tX}]}{e^{ta}} \right\}. \tag{A.1}$$

The $\mathbb{E}[e^{tX}]$ term is the moment generating function of the random variable, X. For the Poisson distribution, $X \sim \text{Poi}(\lambda)$, this is,

$$\mathbb{E}[e^{tX}] = \exp\left(\lambda(\exp(t) - 1)\right).$$

In this case, the bound given in Theorem A.1 can be evaluated to [77]

$$\mathbb{P}r(X \geq a) \leq e^{-\lambda}\left(\frac{e\lambda}{a}\right)^{a} \tag{A.2}$$

Proof of Theorem 4.2. For a parameter $\Delta \geq 0$, we define

$$\begin{aligned}\mathcal{F}_\Delta &:= \{|n_1\rangle|n_2\rangle\cdots|n_m\rangle : \sum_{i=1}^{m} n_i \leq \mu + \Delta\}\\ \mathcal{V}_\Delta &:= \text{span}\{\mathcal{F}_\Delta\}.\end{aligned}$$

We will show that for an appropriate value of Δ, $\mathcal{V}_\Delta$ is the required Hilbert space. Let P_Δ be the projector onto $\mathcal{V}_\Delta$. Recall that $\hat{N}$ is the total number operator and for a multimode coherent state the measurement of this operator is distributed as a Poissonian. Observe that,

$$\begin{aligned}\|P_\Delta\|\alpha_x\rangle\!\rangle - \|\alpha_x\rangle\!\rangle\|_2^2 &= \mathbb{P}r_{\|\alpha_x\rangle\!\rangle}\left(\hat{N} > \mu + \Delta\right)\\ &\leq e^{-\|\alpha_x\|_2^2}\left(\frac{e\|\alpha_x\|_2^2}{\mu + \Delta}\right)^{\mu+\Delta}\\ &\leq \left(\frac{e\mu}{\mu + \Delta}\right)^{\mu+\Delta}\end{aligned}$$

For $\epsilon > 0$, if we set $\Delta = (2e - 1)\mu + \log(4/\epsilon^2)$, we have that

$$\frac{e\mu}{\mu + \Delta} \leq \frac{1}{2}$$

and

$$\left(\frac{1}{2}\right)^{\mu+\Delta} \leq \frac{\epsilon^2}{4}.$$

In particular, we get

$$\|P_\Delta\|\alpha_x\rangle\!\rangle - \|\alpha_x\rangle\!\rangle\|_2 \leq \frac{\epsilon}{2}$$

Thus, if set $|\psi_x\rangle := P_\Delta\|\alpha_x\rangle\!\rangle / \|P_\Delta\|\alpha_x\rangle\!\rangle\|_2$, then, for every x we have

$$\|\,\|\alpha_x\rangle\!\rangle\langle\!\langle\alpha_x\| - |\Psi_x\rangle\langle\Psi_x|\,\|_1 \leq \epsilon$$

using the Fuchs- van de Graaf inequality.

Now, we show that for the value of Δ chosen above (for ϵ), $\log(\dim(\mathcal{V}_\Delta)) = |\mathcal{F}_\Delta| = O(\mu \log m)$. Observe that $\Delta = O(\mu)$. We now bound the cardinality of $\mathcal{F}_\Delta$. Observe that the number of positive integer solutions to

$$\sum_{i=1}^{m} n_i \leq \mu + \Delta$$

is lesser than,

$$\binom{K_\Delta + m}{m}$$

where, $K_\Delta := \lceil \mu + \Delta \rceil$. Therefore, using Lemma A.1, we have

$$|\mathcal{F}_\Delta| \leq \binom{K_\Delta + m}{m} \leq (1+m)^{K_\Delta}.$$

Thus, the dimension of the Hilbert space $\mathcal{V}_\Delta$ satisfies

$$\begin{aligned} \log(\dim(\mathcal{V}_\Delta)) = &\leq K_\Delta \log(1+m) \\ &\leq (\mu + \Delta + 1)\log(1+m) = O(\mu \log(m)). \end{aligned} \tag{A.3}$$

□

A.3 Interference measurement for general coherent state QFP protocols

Suppose, that Alice and Bob use the set of coherent states $\{\|\alpha_x\rangle\!\rangle\}_x$ satisfying $|\langle \|\alpha_x\rangle\!\rangle, \|\alpha_y\rangle\!\rangle\rangle| < \delta$ for $x \neq y$ as fingerprinting states. In this subsection, we show that the Referee can use the interference measurement described in Section 4.2.2.2 to determine if $x = y$ with error δ. Consider $x, y \in \{0,1\}^n$ and the corresponding fingerprinting states $\|\alpha_x\rangle\!\rangle = \otimes_{i=1}^m |\alpha_{xi}\rangle$ and $\|\alpha_y\rangle\!\rangle = \otimes_{i=1}^m |\alpha_{yi}\rangle$. Recall once again that a balanced beam splitter transforms the coherent states as $|\alpha\rangle|\beta\rangle \longrightarrow |(\alpha+\beta)/\sqrt{2}\rangle_+ |(\alpha-\beta)/\sqrt{2}\rangle_-$. Average number of photons seen by a CCD detector at the dark port are

$$\sum_{i=1}^{m} \frac{1}{2}|\alpha_{xi} - \alpha_{yi}|^2 = \frac{1}{2}\|\alpha_x - \alpha_y\|_2^2.$$

This would be zero for the case when $x = y$. To discriminate $x \neq y$ from this case, we calculate the probability of observing photons at the dark port when $x \neq y$.

$$\begin{aligned} P(N=0) &= \exp\left(-\frac{1}{2}\|\alpha_x - \alpha_y\|_2^2\right) = |\langle \|\alpha_x\rangle\!\rangle, \|\alpha_y\rangle\!\rangle\rangle| \\ P(N \neq 0) &= 1 - P(N=0) \\ &= 1 - |\langle \|\alpha_x\rangle\!\rangle, \|\alpha_y\rangle\!\rangle\rangle| \\ &\geq 1 - \delta \end{aligned}$$

Since this is true for all $x \neq y$, in this case δ is also the error of our protocol.

Appendix B

Formal proofs for the results presented in Chapter 5

B.1 Channel Model

As stated in the main body, we study quantum channels with the following authentication guarantee: if the quantum channel in one direction between a pair of participants is used n times in a given timestep, then at least $(1-\epsilon)n$ of these transmission will be transmitted perfectly, while the other at most ϵn transmission might be arbitrarily corrupted by the adversary.

We now argue that this is sufficient to model some random noise, e.g., depolarizing noise, except with negligeable probability.

As a model for random channel noise, we use a depolarizing qubit channel, which takes as input a qubit ρ and outputs $(1-\epsilon)\rho + \epsilon\frac{\mathbb{I}}{2}$ for some parameter ϵ. Note that for any ρ, $\frac{\mathbb{I}}{2} = \frac{1}{4}(\rho + X\rho X + Y\rho Y + Z\rho Z)$. This is a very general noise model, in particular it is a stronger form of noise than erasure noise, since we can always further decay an erasure channel into a depolarizing channel by outputting $\frac{\mathbb{I}}{2}$ whenever there is an erasure flag. Moreover, if we apply n idenpendent depolarizing channels to n qubits, then, except with probability negligeable in n, the output of these channel is a combination of at least $(1-\frac{3\epsilon}{4}+\delta)n$ perfectly transmitted qubits plus Pauli errors on the remaining qubits, for some small constant δ. We can then denote $\gamma = 1-\frac{3\epsilon}{4}+\delta$ the fraction of perfectly transmitted qubits, except with negligeable probability in n.

B.2 No-go for classical EBC protocols

In this section, we will show that EBC cannot be implemented classically. The proof of this fact is similar to the proof that unconditionally secure bit commitment cannot be implemented classically. In particular, we show that if the protocol is statistically hiding for Bob and the trusted parties after an erasure phase, then the protocol is not binding for Alice.

We assume that all the trusted nodes are honest but curious and that there is no dishonest adversarial node (this is sufficient to prove the result). Moreover, we assume that each party keeps a copy of their message transcripts, since they are allowed to be honest-but-curious. Let $b \in \{0,1\}$ be Alice's input. The transcripts after each phase of the protocol for honest Alice and Bob are given by:

Commit: $\mathcal{M}_b^c := (AB_b^c, AT_b^c, BT_b^c, TT_b^c)$

Open: $\mathcal{M}_b^c\mathcal{M}_b^o := (AB_b^c AB_b^o, AT_b^c AT_b^o, BT_b^c BT_b^o, TT_b^c TT_b^o)$

Erase: $\mathcal{M}_b^c\mathcal{M}_b^e := (AB_b^c AB_b^e, AT_b^c AT_b^e, BT_b^c BT_b^e, TT_b^c TT_b^e)$.

where the random variable XY_b^{ph} represents the transcript of communication between party X and party Y during the phase ph of the protocol given that Alice's commitment is b. The transcript of communication between all the trusted parties and Alice is written as AT for the sake of simplicity. Similarly, BT represents the transcripts between Bob and all of the trusted nodes and TT the transcripts between all of the trusted nodes. Further, let R_B be the private randomness used by Bob and R_T be the private randomness used by all the trusted parties. As we aim to show that Alice can cheat, we assume that Bob follows the honest strategy throughout the protocol.

If Bob and the trusted parties get together after an erasure, then all the transcripts would be available to them. The requirement that the protocol be hiding for Bob and the trusted parties after an erasure implies that

$$\begin{aligned} &\mathcal{M}_0^c\mathcal{M}_0^e R_B R_T \approx_\epsilon \mathcal{M}_1^c\mathcal{M}_1^e R_B R_T \\ &\Rightarrow \mathcal{M}_0^c R_B R_T \approx_\epsilon \mathcal{M}_1^c R_B R_T \end{aligned}$$

using the monotonicity under partial trace. We will now show that a dishonest Alice can use this to cheat. First, she runs the commit phase for $b = 0$. Now, if she wishes to open a 0, she simply runs the open phase honestly. On the other hand, if she wishes to open a 1, then all she has to do is to run the open phase for 1. In this case, we have

$$\begin{aligned} &\mathcal{M}_0^c R_B R_T \approx_\epsilon \mathcal{M}_1^c R_B R_T \\ &\Rightarrow \mathcal{M}_0^c\bar{\mathcal{M}}_1^o R_B R_T \approx_\epsilon \mathcal{M}_1^c\mathcal{M}_1^o R_B R_T \end{aligned}$$

where $\bar{\mathcal{M}}_1^o$ denotes the transcripts produced during the open phase by a dishonest Alice following our procedure. The approximate equality in the second step follows once again from the monotonicity of the trace distance. The right hand side in the second equation above opens $b = 1$ due to correctness with high probability ($> 1 - \epsilon$). Thus, except with probability 2ϵ, Alice is able to open a 1 even though she committed to 0.

B.3 Proof of Security for the Erasable Bit Commitment protocol

B.3.1 High-level description

Our definitions are direct adaptation of those of Ref. [13] in the two-party setting to the temporarily trusted setting we study here. There, informally, the bit commitment scheme consist of commit and open primitives between two parties, Alice and Bob. First, Alice and Bob execute the commit primitive, where Alice has input $x \in \{0,1\}^\ell$ and Bob has no input. As output, Bob receives a notification that Alice has chosen an input $x \in \{0,1\}^\ell$. Afterwards, they may execute the open protocol, during which Bob either accepts or rejects. If both parties are honest, Bob always accepts and receives the value x. If Alice is dishonest, however, we still demand that Bob either outputs the correct value of x or rejects (binding). If Bob is dishonest, he should not be able to gain any information about x before the open protocol is executed (hiding).

Here, for our erasable bit commitment scheme, Alice and Bob use help from temporarily trusted nodes $\mathcal{T}_1, \ldots, \mathcal{T}_m$ in order to implement the commit and open primitives. We assume that, except for at most t of these nodes which might collaborate adversarially, perhaps with a dishonest Alice or Bob, all these temporarily trusted nodes act (quantum) honest-but-curiously during the protocol, without collaborating with any other nodes during the execution of the protocol. After the execution of the protocol, the trust assumption is lifted: all the temporarily trusted nodes $\mathcal{T}_1, \ldots, \mathcal{T}_m$ and the dishonest party might gather the data they accumulated during the protocol and act adversarially against the honest parties. In order to complete the execution of the protocol (and lift the corresponding trust assumption) after a commit phase which will not be opened, we add a phase to complement the open phase, which we call an erase phase. This phase forces the temporarily trusted nodes to forget about the commitment before we end the protocol and lift the trust assumption.

As is standard to simplify security definitions and protocols achieving such security, and as is done in Ref. [13], we make use of a randomized version of a commitment. Instead of inputting her own string x, Alice now receives a random string c at the end of the commit phase. Note that if Alice wants to commit to a value x of her choice, she may simply send the XOR of her value with the commitment $x \oplus c$ to Bob at the end of the commit protocol.

B.3.2 Formal definitions for erasable bit commitment

To give a more formal definition, we also provide direct adaptation of the definitions of Ref. [13] to the current setting with temporarily trusted nodes. Note that we may write the commit, open and erase protocols as CPTPMs C_{ABT}, O_{ABT} and E_{ABT}, respectively, consisting of the local actions of honest Alice, Bob and the temporarily trusted nodes on registers $T = T_1 \ldots T_m$, together with any operations they may perform on messages that are exchanged.

When all parties are honest, the output of the commit protocol will be a state $C_{ABT}(\rho_{in}) = \rho_{CABT}$ for some fixed input state ρ_{in}, where $C \in \{0,1\}^\ell$ is the classical output of Alice, and A, B and T are the internal states of Alice, Bob and the temporarily trusted nodes, respectively. If Alice and some nodes $\mathcal{T}_E$, for $E \subseteq [m]$ and $|E| \leq t$, are dishonest and collaborate, then they might not follow the protocol, and we use $C_{A'BT'_E T_{\bar{E}}}$ to denote the resulting map, where $\bar{E} := [m] \setminus E$. Note that $C_{A'BT'_E T_{\bar{E}}}$ might not have output C, hence we simply write $\rho_{A'BT'_E T_{\bar{E}}}$ for the resulting output state, where $A'T'_E$ denote the registers of the dishonest Alice and $\mathcal{T}_E$. Similarly, we use $C_{AB'T'_E T_{\bar{E}}}$ to denote the CPTPM corresponding to the case where Bob and $\mathcal{T}_E$ are dishonest, and write $\rho_{CAB'T'_E T_{\bar{E}}}$ for the resulting output state, where $B'T'_E$ denote the registers of the dishonest Bob and $\mathcal{T}_E$. The case of both Alice and Bob honest but dishonest $\mathcal{T}_E$ is similar.

The open protocol can be described similarly. If all parties are honest, the map O_{ABT} creates the state $\eta_{C\tilde{C}F} := (I_C \otimes O_{ABT})(\rho_{CABT})$, where $\tilde{C} \in \{0,1\}^\ell$ and $F \in \{\text{success}, \text{failure}\}$ is the classical output of Bob. Again, if Alice and $\mathcal{T}_E$ are dishonest, we use $O_{A'BT'_E T_{\bar{E}}}$ to denote the resulting map with output $\eta_{A'T'_E T_{\bar{E}}\tilde{C}F}$. Similarly, we use $O_{CAB'T'_E}$ to denote the CPTPM corresponding to the case where Bob and $\mathcal{T}_E$ are dishonest, and write $\eta_{CB'T'_E}$ for the resulting output state. In the case of both Alice and Bob honest but dishonest $\mathcal{T}_E$, we use $O_{CABT'_E T_{\bar{E}}}$ to denote the CPTPM corresponding to the case $\mathcal{T}_E$ are dishonest, and write $\eta_{C\tilde{C}FT'_E T_{\bar{E}}}$ for the resulting output state also considering the memory content of the quantum honest-but-curious nodes in $\mathcal{T}_{\bar{E}}$.

The erase protocol can also be described similarly. If all parties are honest, the map E_{ABT} creates the state $\zeta_{CF} := (I_C \otimes E_{ABT})(\rho_{CABT})$, where $F = \text{erase}$ is the classical output of Bob. Again, if Alice and $\mathcal{T}_E$ are dishonest, we use $E_{A'BT'_E T_{\bar{E}}}$ to denote the resulting map with output $\zeta_{A'T'_E F}$. Similarly, we use $E_{CAB'T'_E T_{\bar{E}}}$ to denote the CPTPM corresponding to the case where Bob and $\mathcal{T}_E$ are dishonest, and write $\zeta_{CB'T'_E T_{\bar{E}}}$ for the resulting output state also considering the memory content of the quantum honest-but-curious nodes in $\mathcal{T}_{\bar{E}}$. The case of both Alice and Bob honest but dishonest $\mathcal{T}_E$ is similar.

The security definitions for EBC as defined here are direct adaptations of the definitions in Ref. [13], which are themselves a generalization of the ones in Ref. [50], to our setting.

Definition B.1. An (ℓ, ϵ) randomized erasable string commitment scheme is a protocol between Alice, Bob and temporarily trusted nodes $\mathcal{T}_1, \ldots, \mathcal{T}_m$ satisfying the following properties:

Correctness:

Open: If both Alice and Bob are honest, the set of dishonest $\mathcal{T}_i$, $E \subset [m]$ is such that $|E| \leq t$, and the rest of the $\mathcal{T}_i$ are quantum honest-but-curious then, after the open protocol, the ideal state σ_{CCFT} is defined such that

1. The distribution of C is uniform, Bob accepts the commitment and the $\mathcal{T}_i$'s learn nothing about c:

$$\sigma_{CFT} = \tau_{\{0,1\}^\ell} \otimes |\text{success}\rangle\langle\text{success}| \otimes \sigma_T.$$

2. The joint state $\eta_{C\tilde{C}FT}$ created by the real protocol is ϵ-close to the ideal state

$$\eta_{C\tilde{C}FT} \approx_\epsilon \sigma_{CCFT}.$$

Erase: If both Alice and Bob are honest, $|E| \leq t$ and the rest of the $\mathcal{T}_i$ are quantum honest-but-curious, then after the erase protocol, the ideal state $\sigma_{C\tilde{C}FT}$ is defined such that

1. The distribution of C is uniform, that of $\tilde{C}$ is constant, Bob outputs an erasure flag and the $\mathcal{T}_i$'s learn nothing about c:

$$\sigma_{C\tilde{C}FT} = \tau_{\{0,1\}^\ell} \otimes |0\rangle\langle 0| \otimes |erase\rangle\langle erase| \otimes \sigma_T$$

2. The joint state $\zeta_{C\tilde{C}FT}$ created by the real protocol is ϵ-close to the ideal state

$$\zeta_{C\tilde{C}FT} \approx_\epsilon \sigma_{CCFT}.$$

Security for Alice (ϵ-hiding):

Commit: If Alice is honest, $|E| \leq t$ and $\mathcal{T}_{\bar{E}}$ are quantum honest-but-curious, then for any joint state $\rho_{CB'T'_ET_{\bar{E}}}$ created by the commit protocol, the Bob and the adversarial nodes do not learn C:

$$\rho_{CB'T'_E} \approx_\epsilon \tau_{\{0,1\}^\ell} \otimes \rho_{B'T'_E}$$

Erase: If Alice is honest, $|E| \leq t$ and $\mathcal{T}_{\bar{E}}$ are quantum honest-but-curious, then for any joint state $\zeta_{CB'T'_ET_{\bar{E}}}$ created by the erase protocol, the adversaries together with the honest-but-curious nodes do not learn C:

$$\zeta_{CB'T'_ET_{\bar{E}}} \approx_\epsilon \tau_{\{0,1\}^\ell} \otimes \zeta_{B'T'_ET_{\bar{E}}}.$$

Security for Bob (ϵ-binding):

If Bob is honest, $|E| \leq t$ and $\mathcal{T}_{\bar{E}}$ are quantum honest-but-curious then there exists an ideal state $\sigma_{\tilde{C}A'BT'_ET_{\bar{E}}}$ where $\tilde{C}$ is a classical register such that for all open maps $O_{A'BT'_ET_{\bar{E}} \to A'\hat{C}FT'_ET_{\bar{E}}}$

1. Bob almost never accepts $\hat{C} \neq \tilde{C}$:

$$\text{For } \sigma^O_{\tilde{C}A'\hat{C}FT'_ET_{\bar{E}}} = (I_{\tilde{C}} \otimes O)(\sigma_{\tilde{C}A'BT'_ET_{\bar{E}}}), \text{we have}$$
$$\Pr[\hat{C} \neq \tilde{C} \text{ and } F = \text{success }] \leq \epsilon.$$

2. If the open map is applied to the real committed state, the joint state produced $\eta_{A'\hat{C}FT'_ET_{\bar{E}}} := O(\rho_{A'BT'_ET_{\bar{E}}})$ is ϵ-close to the ideal state

$$\eta_{A'\hat{C}FT'_ET_{\bar{E}}} \approx_\epsilon \sigma^O_{A'\hat{C}FT'_ET_{\bar{E}}}.$$

B.3.3 Security proofs

B.3.3.1 Intermediate results

We will prove some Lemmas, which will act as intermediaries to prove security. In particular, we will analyze the actions of the honest-but-curious nodes in the protocol.

Lemma B.1 (Corollary to Uhlmann's Theorem)**.** *Suppose that $\rho, \rho' \in D(\mathcal{X})$ such that $1/2\|\rho - \rho'\|_1 < \epsilon$. Then, there exist purifications of ρ and ρ', $|\psi\rangle$ and $|\psi'\rangle$ in $\mathcal{X} \otimes \mathcal{X}$ respectively such that*

$$|\psi\rangle\langle\psi| \approx_{\sqrt{2\epsilon}} |\psi'\rangle\langle\psi'| \tag{B.1}$$

Proof. Using the Fuchs-van de Graaf inequality (Theorem 2.4) we have that

$$F(\rho, \rho') \geq 1 - \frac{1}{2}\|\rho - \rho'\|_1 > 1 - \epsilon.$$

Further using Uhlmann's theorem (Theorem 2.3) we have that there exist purifications $|\psi\rangle$ and $|\psi'\rangle$ in $\mathcal{X} \otimes \mathcal{X}$ of ρ and ρ' such that

$$F(\rho, \rho') = |\langle\psi|\psi'\rangle|,$$

which implies that

$$|\langle\psi|\psi'\rangle| > 1 - \epsilon.$$

Now using the fact ([16, Eq. 1.186]) that

$$\frac{1}{2}\| |\psi\rangle\langle\psi| - |\psi'\rangle\langle\psi'| \|_1 = \sqrt{1 - |\langle\psi|\psi'\rangle|^2}$$

we have

$$\frac{1}{2}\| |\psi\rangle\langle\psi| - |\psi'\rangle\langle\psi'| \|_1 < \sqrt{2\epsilon}.$$

□

In the following Lemma, we consider the action of an honest-but-curious node in the erasable bit commitment protocol in a general fashion. We suppose that Alice sends the T part of the state ρ_{RT} to the party T. The R part of the state may be arbitrarily distributed between the rest of parties. For example, in the real protocol the register $R = (A, \bar{T})$, where $\bar{T}$ represents all the trusted nodes other than the node T. Then, we consider the cases of 'Open' and 'Erase' and show that the state held by T after these are almost decoupled from the state that Alice gave him. In particular, we assume that after the announcement of 'Open' (or 'Erase'), T applies the map $\Phi^O_{T\to BT'}$ (or $\Phi^E_{T\to AT'}$) to his part of ρ_{RT} and sends the B (or A) share of the state to Bob (or Alice).

Similarly, the rest of the parties apply an arbitrary channel, Φ_R to the register R. This channel can be arbitrary since the behaviour of T should appear honest irrespective of the strategies of the other parties by definition. We then show that

$$(\Phi_R \otimes \Phi^O_{T\to BT'})(\rho_{RT}) \approx_{O(\sqrt{\delta})} (\Phi_R \otimes I_{T\to B})(\rho_{RT}) \otimes \tilde{\sigma}_{T'}$$
$$(\Phi_R \otimes \Phi^E_{T\to AT'})(\rho_{RT}) \approx_{O(\sqrt{\delta})} (\Phi_R \otimes I_{T\to A})(\rho_{RT}) \otimes \tilde{\omega}_{T'}$$

where $\tilde{\sigma}_{T'}$ and $\tilde{\omega}_{T'}$ are fixed states.

Lemma B.2. *Let T be a $\delta-$honest-but-curious node in the erasable bit commitment protocol. Suppose that during the commit stage of the protocol, Alice sends the T substate of the state ρ_{RT} to the party T. The R part of the state is distributed arbitrarily between the parties other than T. Further, suppose that in the case of an 'Open', T applies the channel $\Phi^O_{T\to BT'}$ to his state T. Then, there exists a state $\tilde{\sigma}_{T'}$ such that for every state ρ_{RT} distributed by Alice during the commit stage and every channel Φ_R applied on R during the open phase, the state $\eta_{RBT'} := (\Phi_R \otimes \Phi^O_{T\to BT'})(\rho_{RT})$ (where the B part is given to Bob by T and the T' part is held by T) produced during the open phase is such that*

$$\eta_{RBT'} \approx_{5\sqrt{2\delta}} (\Phi_R \otimes I_{T\to B})(\rho_{RT}) \otimes \tilde{\sigma}_{T'}.$$

Similarly, suppose that in the case of an 'Erase', T applies the channel $\Phi^E_{T\to AT'}$ to his state T. Then, there exists a state $\tilde{\omega}_{T'}$ such that for every state ρ_{RT} distributed by Alice during the commit stage and every channel Φ_R applied on R during the erase phase, the state $\zeta_{RAT'} := (\Phi_R \otimes \Phi^E_{T\to AT'})(\rho_{RT})$ (where the A part is given back to Alice by T and the T' part is held by T) produced during the erase phase is such that

$$\zeta_{RAT'} \approx_{5\sqrt{2\delta}} (\Phi_R \otimes I_{T\to A})(\rho_{RT}) \otimes \tilde{\omega}_{T'}.$$

Proof. The proof of this Lemma follows the same argument as the proof of the Rushing Lemma in (Lemma 6.2 in [53]). We will prove this Lemma only for the case of an 'Open'. The case of an 'Erase' follows similarly. Note that due to convexity of the trace norm, it suffices to prove this Lemma for pure states. Further, it is also sufficient to consider isometric channels Φ_R for an arbitrary register R, since one can use the Stinespring representation to write a general channel as an isometric channel composed with the partial trace (see for example [16, Sec. 2.2.2]) and the trace distance decreases under a partial trace operation.

Suppose that after the announcement of 'Open', the trusted node T applies the map $\Phi^O_{T\to BT'}$ and the isometric channel Φ_R is applied to the register R by the other parties. Choose and fix a state $\rho^{(1)}_{RT} := |\psi^{(1)}_{RT}\rangle \langle\psi^{(1)}_{RT}|$. We then define the state

$$\eta^{(1)}_{RBT'} = (\Phi_R \otimes \Phi^O_{T\to BT'})(\rho^{(1)}_{RT}).$$

Since T is δ-honest-but-curious in the case of an open, there exists a channel $\mathcal{T}_{T'}$ such that

$$\begin{aligned}(I_{RB} \otimes \mathcal{T}_{T'})(\eta^{(1)}_{RBT'}) &\approx_{\delta} (\Phi_R \otimes I_{T\to B})(\rho^{(1)}_{RT}) \\ \Rightarrow\ \eta^{(1)}_{RB} &\approx_{\delta} (\Phi_R \otimes I_{T\to B})(\rho^{(1)}_{RT}).\end{aligned}$$

Now, we use Lemma B.1 and the fact that $(\Phi_R \otimes I_{T\to B})(\rho^{(1)}_{RT})$ is a pure state to show that there exists a state $\sigma'_{T''}$ and a purification $\eta^{(1)}_{RBT''}$ of $\eta^{(1)}_{RB}$ such that

$$\eta^{(1)}_{RBT''} \approx_{\sqrt{2\delta}} (\Phi_R \otimes I_{T\to B})(\rho^{(1)}_{RT}) \otimes {\sigma'}_{T''}.$$

Further, since $\eta^{(1)}_{RBT''}$ is a purification of $\eta^{(1)}_{RB}$ and has the same partial state as $\eta^{(1)}_{RBT'}$ on registers R and B, there exists a quantum channel $\Omega_{T''\to T'}$ acting only on T'' transforming $\eta^{(1)}_{RBT''}$ into $\eta^{(1)}_{RBT'}$ ([16, Proposition 2.29]). Thus, we have

$$\eta^{(1)}_{RBT'} \approx_{\sqrt{2\delta}} (\Phi_R \otimes I_{T\to B})(\rho^{(1)}_{RT}) \otimes \tilde{\sigma}_{T'} \tag{B.2}$$

where $\tilde{\sigma}_{T'} = \Omega_{T''\to T'}({\sigma'}_{T''})$.

We claim that this state $\tilde{\sigma}_{T'}$ is the required state. Consider the state $\rho = |\psi_{RT}\rangle\langle\psi_{RT}|$. Now, let $|\psi'_{R'RT}\rangle := 1/\sqrt{2}(|1_{R'}\rangle|\psi_{RT}\rangle + |2_{R'}\rangle|\psi^{(1)}_{RT}\rangle)$ where $|1_{R'}\rangle$ and $|2_{R'}\rangle$ are orthonormal states. Define the states

$$\begin{aligned}\eta_{RBT'} &:= (\Phi_R \otimes \Phi^{O}_{T\to BT'})(|\psi_{RT}\rangle\langle\psi_{RT}|) \\ \eta'_{R'RBT'} &:= (I_{R'} \otimes \Phi_R \otimes \Phi^{O}_{T\to BT'})(|\psi'_{R'RT}\rangle\langle\psi'_{R'RT}|).\end{aligned}$$

Since, the node is δ-honest-but-curious irrespective of the strategy of the other parties, we once again have

$$\eta'_{R'RB} \approx_{\delta} (\Phi_R \otimes I_{T\to B})(|\psi'_{R'RT}\rangle\langle\psi'_{R'RT}|)$$

where we have omitted the identity map on R' for brevity. Arguing as before, we see that there exists a state $\sigma''_{T'}$ such that

$$\eta'_{R'RBT'} \approx_{\sqrt{2\delta}} (\Phi_R \otimes I_{T\to B})(|\psi'_{R'RT}\rangle\langle\psi'_{R'RT}|) \otimes \sigma''_{T'}.$$

If we now apply the channel of the measurement in the $\{|1_{R'}\rangle\langle 1_{R'}|, |2_{R'}\rangle\langle 2_{R'}|\}$ to both the sides of the above equation we get

$$\eta_{RBT'} \approx_{2\sqrt{2\delta}} (\Phi_R \otimes I_{(T\to B)})(|\psi_{RT}\rangle\langle\psi_{RT}|) \otimes \sigma''_{T'} \tag{B.3}$$

$$\eta^{(1)}_{RBT'} \approx_{2\sqrt{2\delta}} (\Phi_R \otimes I_{(T\to B)})(|\psi^{(1)}_{RT}\rangle\langle\psi^{(1)}_{RT}|) \otimes \sigma''_{T'} \tag{B.4}$$

Combining Eq. B.2 and Eq. B.4, we get

$$\sigma''_{T'} \approx_{3\sqrt{2\delta}} \tilde{\sigma}_{T'}.$$

Using this we can show that

$$\eta_{RBT'} \approx_{5\sqrt{2\delta}} (\Phi_R \otimes I_{(T\to B)})(|\psi_{RT}\rangle\langle\psi_{RT}|) \otimes \tilde{\sigma}_{T'}$$

which proves our claim since $|\psi_{RT}\rangle$ was arbitrary. □

In the next Lemma, we consider the action of all the honest temporarily trusted nodes together during the protocol. This Lemma will be useful while proving the various security definitions. Let E be the set of adversarial trusted nodes $(\mathcal{T}_i)$. We assume that at least one of Alice and Bob is honest. This assumption is satisfied by the hypotheses of our security requirements. Under this assumption, during the commit stage Alice distributes the state $\rho_{A'B_C T_{\bar{E}} T_E}$, where the register $B_C = (\Theta, Z, R)$ and is held by Bob. Apart from this restriction, we do not place any other restrictions on the behaviour of these parties. Alice, Bob and the adversarial trusted nodes $\mathcal{T}_E$ follow an arbitrary (possibly dishonest) strategy during the protocol and the trusted nodes $\mathcal{T}_{\bar{E}}$ act honest-but-curiously. Under these conditions, we show that the trusted nodes act almost honestly upto storing some fixed state in their memories.

Lemma B.3. *Consider the erasable bit commitment protocol. Let E be the set of adversarial trusted nodes $(\mathcal{T}_i)$. We assume that one of the parties Alice or Bob is honest. Suppose that during the commit stage, (possibly dishonest) Alice prepares and distributes the state $\rho_{A'B_C T_{\bar{E}} T_E}$, where the register $B_C = (\Theta, Z, R)$ and is held by Bob. Let $\Phi^O_{AB_C T_E}$ be the channel applied by Alice, Bob and the adversarial nodes in case of an 'Open'. Similarly, let $\Phi^E_{AB_C T_E}$ be the channel applied by Alice, Bob and the adversarial nodes in case of an 'Erase'. Then, in case of an 'Open', the state received by Bob $\eta_{AT'_{\bar{E}} T'_E B_C B}$ (where $T'_{\bar{E}}$ and T'_E are registers held by $\mathcal{T}_{\bar{E}}$ and $\mathcal{T}_E$ after an 'Open') satisfies*

$$\eta_{A'T'_{\bar{E}} T'_E B_C B} \approx_{m\sqrt{2\delta}} \left(I_{T_{\bar{E}} \to B_{\bar{E}}} \otimes \Phi^O_{AB_C T_E}\right)\left(\rho_{A'B_C T_{\bar{E}} T_E}\right) \otimes \tilde{\sigma}_{T_{\bar{E}}}.$$

for some fixed state $\tilde{\sigma}_{T_{\bar{E}}}$. In the case of an 'Erase', the state $\zeta_{A'T'_{\bar{E}} T'_E B_C}$ received back by Alice satisfies (where $T'_{\bar{E}}$ and T'_E are registers held by $\mathcal{T}_{\bar{E}}$ and $\mathcal{T}_E$ after an 'Erase')

$$\zeta_{A'T'_{\bar{E}} T'_E B_C} \approx_{m\sqrt{2\delta}} \left(I_{T_{\bar{E}} \to A_{\bar{E}}} \otimes \Phi^E_{AB_C T_E}\right)\left(\rho_{A'B_C T_{\bar{E}} T_E}\right) \otimes \tilde{\omega}_{T_{\bar{E}}}.$$

for some fixed state $\tilde{\omega}_{T_{\bar{E}}}$.

Proof. Once again, we will prove the statement for the case of an 'Open'. The proof for an 'Erase' follows similarly. Suppose, that in case of an 'Open', each honest-but-curious node T_i for $i \in \bar{E}$ applies the channel $\Phi_{T_i} := \Phi^O_{T_i \to B_i T'_i}$ and the other parties apply the channel $\Phi^O_{AB_C T_E}$ collectively to their states. Thus,

$$\eta_{A'T'_{\bar{E}} T'_E B_C B} = \left(\left(\bigotimes_{i \in \bar{E}} \Phi_{T_i}\right) \otimes \Phi^O_{AB_C T_E}\right)\left(\rho_{A'B_C T_{\bar{E}} T_E}\right)$$

Now using Lemma B.2, we know that there exist fixed states $\tilde{\sigma}_{T_i}$ for $i \in \bar{E}$ for which

$$\begin{aligned}
\eta_{A'T'_{\bar{E}} T'_E \Theta B} &\approx_{5\sqrt{2\delta}} \left(I_{T_{\bar{E}_1} \to B_{\bar{E}_1}} \otimes \left(\bigotimes_{i \in \bar{E}; i \neq \bar{E}_1} \Phi_{T_i}\right) \otimes \Phi^O_{AB_C T_E}\right)\left(\rho_{A'B_C T_{\bar{E}} T_E}\right) \otimes \tilde{\sigma}_{T_{\bar{E}_1}} \\
&\approx_{5|\bar{E}|\sqrt{2\delta}} \left(I_{T_{\bar{E}} \to B_{\bar{E}}} \otimes \Phi^O_{AB_C T_E}\right)\left(\rho_{A'B_C T_{\bar{E}} T_E}\right) \otimes \bigotimes_{i \in \bar{E}} \tilde{\sigma}_{T'_i} \\
&\approx_{5m\sqrt{2\delta}} \left(I_{T_{\bar{E}} \to B_{\bar{E}}} \otimes \Phi^O_{AB_C T_E}\right)\left(\rho_{A'B_C T_{\bar{E}} T_E}\right) \otimes \bigotimes_{i \in \bar{E}} \tilde{\sigma}_{T'_i}
\end{aligned}$$

where the second step is the result of repeating the first step multiple times, and in the third step we use the fact that $|\bar{E}| \leq m$. Hence, the Lemma is true for $\tilde{\sigma}_{T_{\bar{E}}} := \otimes_{i \in \bar{E}} \tilde{\sigma}_{T'_i}$ □

B.3.3.2 Correctness for honest Alice and Bob

Correctness for Open:

Proof. If Alice is honest, then she generates the state

$$\rho_{X\Theta ZT} := \sum_{x,\theta,z} 2^{-(2n+k)} \left|x\right\rangle\left\langle x\right| \otimes \left|\theta\right\rangle\left\langle\theta\right| \otimes \left|z\right\rangle\left\langle z\right| \otimes H^{\theta}\left|\mathrm{Enc}(x)\oplus z\right\rangle\left\langle\mathrm{Enc}(x)\oplus z\right| H^{\theta}$$

and sends θ, z to Bob, and the registers $T = (T_i)$ to the trusted nodes. Let E be the set of adversaries. Suppose, that in case of an open each honest-but-curious node T_i for $i \in \bar{E}$ applies the channel $\Phi_{T_i} := \Phi_{T_i \to B_i T_i'}$ and the adversarial nodes apply the channel $\Phi_{T_E} := \Phi_{T_E \to B_E T_E'}$ collectively to their states. Let $\eta_{X\Theta BT'_{\bar{E}}T'_E}$ be the real state of the protocol after the trusted nodes forwards their shares to Bob, that is

$$\eta_{X\Theta ZBT'_{\bar{E}}T'_E} = \left(\left(\bigotimes_{i\in\bar{E}} \Phi_{T_i}\right) \otimes \Phi_{T_E}\right)\left(\rho_{X\Theta ZT}\right)$$

Further, we suppose that Alice and Bob shared a random $r \in \mathcal{R}$ for privacy amplification during the commit phase. By Lemma B.3 we know that

$$\eta_{X\Theta ZBT'_{\bar{E}}T'_E} \approx_{5m\sqrt{2\delta}} \left(I_{T_{\bar{E}}\to B_{\bar{E}}} \otimes \Phi_{T_E}\right)\left(\rho_{X\Theta ZT}\right) \otimes \tilde{\sigma}_{T'_{\bar{E}}}. \tag{B.5}$$

for some fixed state $\tilde{\sigma}_{T'_{\bar{E}}}$. For this strategy of the trusted nodes we define the ideal state σ_{CCFT} to simply be the state

$$\sigma_{CCFT} := \sum_{c} 2^{-l} \left|cc\right\rangle\left\langle cc\right| \otimes \left|\text{success}\right\rangle\left\langle\text{success}\right| \otimes \sigma_T$$

for σ_T defined as

$$\sigma_T := \tilde{\sigma}_{T'_{\bar{E}}} \otimes \eta_{T'_E}$$

where $\eta_{T'_E}$ is the partial state held by the nodes T_E at the end of the 'Open' stage in the real protocol. This ideal state satisfies the security requirements given in B.1. Further, if we apply the decoding map to both sides of Eq. B.5, we see that Bob is able to recover $\hat{X} = X$ with high probability since $|E| \leq t$ and the channel error rate is γ. Now observe that

$$H_{\min}^{5m\sqrt{2\delta}}(X|T'_{\bar{E}}T'_E)_\eta \geq (\delta_c + \delta')n$$

by using Eq. B.5 and an argument similar to the one given in Sec. 5.5.5. By privacy amplification ($\ell = \delta_c n$), we can show that the distance between the ideal state and the real state is at most

$$\epsilon' = 2^{-\frac{\delta' n}{2}-1} + 5m\sqrt{2\delta}.$$

□

Correctness for Erase: Following the same arguments as above one can prove the correctness of Erase in our protocol.

B.3.3.3 Security for honest Alice

The hiding properties of the protocol during the commit stage were proven in Section 5.5.3.

Further, the proof of security for Alice after an erase follows the argument as the proof for correctness of an Erase. The only difference being that the adversaries in this case have access to Θ as well. The arguments given in Section 5.5.4 handle this too.

B.3.3.4 Security for honest Bob

Proof. We now formally prove security for honest Bob. We use a simulator argument similar to that used in Ref. [13] (proof of Theorem III.5) to define the ideal state $\sigma_{\tilde{C}A'BT'_E T_{\bar{E}}}$. We show that Alice is committed to $\tilde{C}$ after the commit phase, i.e. she cannot open something different than $\tilde{C}$ except with negligible probability.

Suppose that during the commit phase of the real protocol, Alice sends the T part of the state $\rho_{A'T}$ to the trusted nodes and θ and r to Bob. Also, let Φ_{T_i} be the channel applied by the honest-but-curious node $i \in \bar{E}$. First, for the honest-but-curious party $i \in \bar{E}$, we let the state $\tilde{\sigma}_{T_i}$ be the state shown to exist in Lemma 2, such that for every initial state $\rho_{AT_{\bar{i}}T_i}$ and every channel $\Phi_{AT_{\bar{i}}}$ applied to the registers held by all the other parties

$$(\Phi_{AT_{\bar{i}}} \otimes \Phi_{T_i})(\rho_{AT_{\bar{i}}T_i}) \approx_{5\sqrt{2\delta}} (\Phi_{AT_{\bar{i}}} \otimes I_{T_i \to B_i})(\rho_{AT_{\bar{i}}T_i}) \otimes \tilde{\sigma}_{T'_i}.$$

Now, we show the existence of the ideal state $\sigma_{\tilde{C}A'BT'_E T_{\bar{E}}}$ algorithmically by making Alice and the $\mathcal{T}_i$'s interact with a simulator. Imagine a protocol Π_{sim} where instead of sending the quantum states to the trusted parties during the commit stage, Alice sends the shares of the honest-but-curious parties $\rho_{T_{\bar{E}}}$ to a simulator and the share of the adversaries to the adversaries. Alice also shares θ and r with the simulator. The simulator measures $\rho_{T_{\bar{E}}}$ in the θ basis to get $\bar{y}_{\bar{E}}$. Define $\bar{y} := (\bar{y}_{\bar{E}}\ 0_E)$ and let $\tilde{y}$ be the codeword closest to $\bar{y}$. Further, let $\tilde{x} := \text{Dec}(\tilde{y})$ and $\tilde{c} := \text{Ext}(\tilde{x}, r)$. Then, it re-encodes $\bar{y}_{\bar{E}}$ in the θ basis (as $H^\theta \left|\bar{y}_{\bar{E}}\right\rangle$) and sends it to the honest-but-curious parties $\bar{E}$. Further, in this protocol, we assume that in the case of an 'Open', the honest-but-curious nodes $i \in \bar{E}, T_i$ apply the channel $\Phi^{(\text{id})}_{T_i}$ which we define as $\Phi^{(\text{id})}_{T_i}(\rho) = \rho \otimes \tilde{\sigma}_{T_i}$ for every state ρ. Finally, Alice and the adversaries T_E apply whatever channel they apply during the commit stage in the real protocol. To prepare the ideal state $\sigma_{\tilde{C}A'BT'_E T_{\bar{E}}}$, the parties follow the above protocol. The register $\tilde{C}$ simply contains the string $\tilde{c}$.

We now prove that for any strategy of Alice and the adversaries after the commit stage on the ideal state defined above, Bob opens the string $\tilde{c}$ during a successful open. Suppose, Bob measures the state, he receives during the open stage, in the θ basis and gets the outcome $\hat{y}$. Since, the $T_{\bar{E}}$ do not change or disturb their states during Π_{sim}, the Hamming distance (h) between $\hat{y}$

and $\bar{y}$ satisfies

$$\begin{aligned} h(\hat{y},\bar{y}) &\leq |E|\frac{n}{m} + \gamma n \\ &\leq \left(\frac{t}{m} + \gamma\right)n = \frac{d-1}{4}. \end{aligned}$$

with high probability. Further, we have that $h(\hat{y},\tilde{y}) \leq h(\hat{y},\bar{y}) + h(\bar{y},\tilde{y}) \leq 3(d-1)/4$. For any codeword y' such that $y' \neq \tilde{y}$, we have that

$$\begin{aligned} h(\hat{y},y') &\geq h(\tilde{y},y') - h(\tilde{y},\hat{y}) \\ &\geq d - \frac{3(d-1)}{4} > \frac{d-1}{4}. \end{aligned}$$

Since, Bob discards the commitment in case the Hamming distance between the measured string and the nearest codeword is more than $(d-1)/4$, the adveraries cannot change the commitment after the commit stage. Hence, the ideal state defined above satisfies the security definition.

Now, we will prove that the real state produced during the protocol is close to the ideal one after the open map is applied. Since, the action of the trusted nodes and the simulator in Π_{sim} commutes, this protocol would produce the same state as a protocol where the simulator is between the trusted nodes and Bob. Then, observe that in Π_{sim}, since the simulator encodes the string $\bar{y}_{\bar{E}}$ in the θ basis and Bob measures this in the θ basis, we can simply remove this re-encoding and measurement step from the modified protocol. The protocol constructed this way, though, is exactly the original protocol, except for the fact that the honest-but-curious nodes instead of applying the maps Φ_{T_i}, apply $\Phi^{(\text{id})}_{T_i}$. Using Lemma B.3, we can prove that the state of this protocol is $5m\sqrt{2\delta}$ close to the real state. □

B.4 Decoupling of honest-but-curious nodes during the protocol

In addition to satisfying the hiding property for Bob's and the adversarial nodes, our protocol satisfies the following hiding condition for the honest-but-curious nodes.

Definition B.2 (Hiding for the honest-but-curious nodes)**.** If Alice is honest, $|E| \leq t$ and $\mathcal{T}_{\bar{E}}$ are quantum honest-but-curious, then for any joint state $\rho_{CB'T'_ET_{\bar{E}}}$ created by the commit protocol, the honest-but-curious nodes do not learn C, or equivalently, they are completely decoupled from C:

$$\forall i \in \bar{E} : \rho_{CT_i} \approx_\epsilon \tau_{\{0,1\}^l} \otimes \rho_{T_i}$$

The proof of that our protocol satisfies this property was given in Sec. 5.6.1.

B.5 Definitions and proofs for the expungement property

B.5.1 Definition of the expungement property

Definition B.3. An (ℓ, ϵ) randomized erasable string commitment scheme is said to satisfy the *expungement on success* property if it satisfies the following properties:

Open: If both Alice and Bob are honest and $F_A = F_B = \mathrm{success}$ after the open protocol, then there exists an ideal state σ_{CCFT} satisfying the following

1. The distribution of C is uniform and the $\mathcal{T}_i$'s learn nothng about c:

$$\sigma_{CFT} = \tau_{\{0,1\}^\ell} \otimes |\mathrm{success}\rangle\langle\mathrm{success}| \otimes \sigma_T.$$

2. The joint state $\eta_{C\tilde{C}FT}$ created by the real protocol is ϵ-close to the ideal state

$$\eta_{C\tilde{C}FT} \approx_\epsilon \sigma_{CCFT}.$$

Erase: If Alice is honest, Bob does not collaborate with the trusted nodes during the protocol and $F_A = erase$ after the erase protocol, then the joint state $\zeta_{CB'T}$ created by the erase protocol satisfies the following:

$$\zeta_{CB'T} \approx_\epsilon \tau_{\{0,1\}^\ell} \otimes \zeta_{B'T}.$$

B.5.2 Proof of the expungement property

We only prove min-entropy bounds on the relevant states. These are sufficient to prove the required statements. However, depending on the noise parameters it might be necessary to change the some of the protocol parameters to achieve security as above. In order to complete the proof that our robust protocol satisfies the expungement property, we first list the properties of min-entropy that we will use, and then derive the desired min-entropy bound. We denote by E the register of the adversarial trusted node who keeps information about X, by $\psi_{TXYZU\theta}$ the state prepared by Alice and by $\rho_{EXYZU\theta} = \mathcal{N}_{T\to E}(\psi_{TXYZU\theta})$ the state after the adversary acted on T and kept register E.

B.5.2.1 Preliminaries for min-entropy bound

We have $x \in_R \{0,1\}^k$, $z \in_R \{0,1\}^n$, $\theta \in_R \{0,1\}^n$.

Also, $y = \mathrm{Enc}(x)$, $u = y \oplus z$, $y = u \oplus z$ and $|\psi\rangle = H^\theta |u\rangle$.

Hence, $\psi^u_{TZ} = \psi^u_T \otimes \rho^u_Z$ and then $\rho^u_{EZ} = \mathcal{N}_{T\to E}(\psi^u_{TZ}) = \mathcal{N}_{T\to E}(\psi^u_T) \otimes \rho^u_Z = \rho^u_E \otimes \rho^u_Z$ with $\rho^u_Z = \mathrm{Enc}(\tau_X)$, and then

$$\mathrm{H}_{\min}(Z|UE) = \mathrm{H}_{\min}(Z|U). \tag{B.6}$$

Then,

$$\mathrm{H}_{\min}(Z|U) = \mathrm{H}_{\max}(Z|U) = \mathrm{H}_{\min}(U|Z) = k, \tag{B.7}$$

since $\mathrm{H}_{\min}(Z|U) = \mathrm{H}_{\min}(Y|U) = \mathrm{H}_{\min}(Y) = \mathrm{H}_{\min}(X) = k$, and similarly for $\mathrm{H}_{\max}(Z|U)$ and $\mathrm{H}_{\min}(U|Z)$.

For smooth entropies, we also have that

$$\mathrm{H}^{\epsilon}_{\min}(X|EZ) = \mathrm{H}^{\epsilon}_{\min}(Y|EZ) = \mathrm{H}^{\epsilon}_{\min}(U|EZ), \tag{B.8}$$

in which the last equality follows from [78, Lemma A.7].

We also make use of the following chain rules for smooth entropies (these are special cases of the inequalities proven in [63]), with $f_\epsilon = \log(\frac{1}{1-\sqrt{1-\epsilon^2}})$,

$$\mathrm{H}^{2\epsilon}_{\min}(AB|C) \geq \mathrm{H}_{\min}(A|BC) + \mathrm{H}^{\epsilon}_{\min}(B|C) - f_\epsilon, \tag{B.9}$$

$$\mathrm{H}^{\epsilon}_{\max}(AB|C) \leq \mathrm{H}_{\max}(A|BC) + \mathrm{H}_{\max}(B|C) + f_\epsilon, \tag{B.10}$$

$$\mathrm{H}^{2\epsilon}_{\min}(AB|C) \leq \mathrm{H}^{7\epsilon}_{\min}(A|BC) + \mathrm{H}^{2\epsilon}_{\max}(B|C) + 2f_\epsilon, \tag{B.11}$$

$$\mathrm{H}^{\epsilon}_{\max}(AB|C) \geq \mathrm{H}_{\min}(A|BC) + \mathrm{H}^{2\epsilon}_{\max}(B|C) - 2f_\epsilon. \tag{B.12}$$

We use the fact that the smooth entropies satisfy a data processing inequality,

$$\mathrm{H}^{\epsilon}_{\max}(Z|E) \leq \mathrm{H}^{\epsilon}_{\max}(Z). \tag{B.13}$$

Finally, we use the following bound from uncertainty relation/sampling, for some parameters μ_ϵ and δ_ϵ, and for γ the tolerable noise rate,

$$\mathrm{H}^{\epsilon}_{\min}(U|E) \geq n(1 - H_2(\gamma + \mu_\epsilon)) - \delta_\epsilon. \tag{B.14}$$

B.5.2.2 Deriving the min-entropy bound

We can now prove the desired bound on $\mathrm{H}_{\min}^{7\epsilon}(X|EZ)$,

$$\begin{aligned}
k - \mathrm{H}_{\min}^{7\epsilon}(X|EZ) &= \mathrm{H}_{\min}(U|Z) - \mathrm{H}_{\min}^{7\epsilon}(U|EZ) && \text{by } (B.7) \text{ and } (B.8)\\
&\leq \mathrm{H}_{\max}^{\epsilon}(UZ) - \mathrm{H}_{\max}^{2\epsilon}(Z) + 2f_\epsilon && \text{by } (B.12)\\
&\quad - \mathrm{H}_{\min}^{2\epsilon}(UZ|E) + \mathrm{H}_{\max}^{2\epsilon}(Z|E) + 2f_\epsilon && \text{by } (B.11)\\
&\leq \mathrm{H}_{\max}^{\epsilon}(UZ) - \mathrm{H}_{\min}^{2\epsilon}(UZ|E) + 4f_\epsilon && \text{by } (B.13)\\
&\leq \mathrm{H}_{\max}(U) + \mathrm{H}_{\max}(Z|U) + f_\epsilon && \text{by } (B.10)\\
&\quad - \mathrm{H}_{\min}^{\epsilon}(U|E) - \mathrm{H}_{\min}(Z|UE) + f_\epsilon + 4f_\epsilon && \text{by } (B.9)\\
&= n + \mathrm{H}_{\max}(Z|U) + 6f_\epsilon\\
&\quad - \mathrm{H}_{\min}^{\epsilon}(U|E) - \mathrm{H}_{\min}(Z|U) && \text{by } (B.6)\\
&= n - \mathrm{H}_{\min}^{\epsilon}(U|E) + 6f_\epsilon && \text{by } (B.7)\\
&\leq n - n(1 - H_2(\gamma + \mu_\epsilon)) + \delta_\epsilon + 6f_\epsilon && \text{by } (B.14)\\
&= n(H_2(\gamma + \mu_\epsilon)) + \delta_\epsilon + 6f_\epsilon.
\end{aligned}$$

Rearranging terms, we get

$$\mathrm{H}_{\min}^{7\epsilon}(X|EZ) \geq k - n(H_2(\gamma + \mu_\epsilon)) - \delta_\epsilon - 6f_\epsilon. \tag{B.15}$$