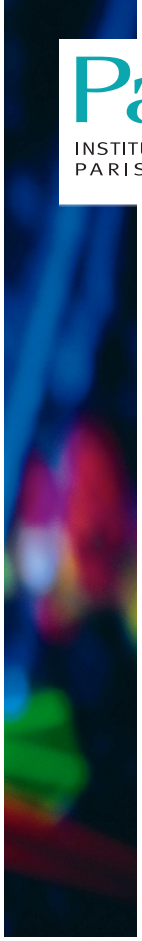

ParisTech
INSTITUT DES SCIENCES ET TECHNOLOGIES
PARIS INSTITUTE OF TECHNOLOGY

TELECOM ParisTech

2018-ENST-0055

EDITE - ED 130

Doctorat ParisTech

T H È S E

pour obtenir le grade de docteur délivré par

TELECOM ParisTech

Spécialité «Information Quantique »

Design, analysis and implementation of advanced quantum communication protocols

THÈSE

Directeur de thèse : **Eleni DIAMANTI**
Co-encadrement de la thèse : **Iordanis KERENIDIS**

Jury

M. Antonio ACÍN, Professeur, ICFO, Institut des Sciences Photoniques	Rapporteur
M. Nobert LÜTKENHAUS, Professeur, IQC, Université de Waterloo	Rapporteur
M. David ELKOUSS, Professeur associé, QuTech, TUDelft	Examinateur
Mme. Elham KASHEFI, Directrice de Recherche, LIP6, Sorbonne Université	Examinatrice
M. Iordanis KERENIDIS, Directeur de Recherche, IRIF, Université Paris 7	Directuer de thèse
Mme. Eleni DIAMANTI, Chargée de Recherche, LIP6, Sorbonne Université	Directrice de thèse

TELECOM ParisTech

École de l'Institut Mines-Télécom - membre de ParisTech

46 rue Barrault 75013 Paris - (+33) 1 45 81 77 77 - www.telecom-paristech.fr

Acknowledgment

The best place to work is where you can be your best. I have been so privileged to have the supportive set of people around me at work and outside, who have guided me, enjoyed my success as if their own, pulled me up when I was down. In short, they have been a cherished part of my PhD journey in Paris.

I would start by thanking my PhD supervisors Eleni Diamanti and Iordanis Kerenidis, who have been the best mentors one could ask for. Their constant support and patience, while letting me figure out the research path, has been instrumental in making me a better scientist than what I had imagined to become. In short, it has been a privilege to work alongside two exceptional researchers and human beings.

I am thankful to the QI LIP6 permanent researchers Frédéric Grosshans, Damian Markham and Elham Kashefi for their constant support and countless technical, non-technical discussions during my PhD. In particular, Frédéric Grosshans who has helped me develop the quantum money scheme through numerous discussions. I would also like to thank all the QI LIP6 past and present researchers: Ulysse, Mathieu, Anu, Luis, Marc, Shane, Tom, Shouvik, Luka, Pierre-Emmanuel, Victor, Simon, Federico, Andrea, Léo, Raja, Shraddha, Rawad, Francesco and everyone else who have been very good q(quantum)-colleagues and friends. I would specially thank Ulysse, who is one of the most motivated young researchers I have come across, and with whom, countless discussions have resulted in new scheme on optical swap with coherent states. Also, Luis, who, has been a constant source of knowledge and wisdom. And Mathieu and Anu, who have been my closest annoying set of colleagues and friends.

I am thankful to Nobert Lütkenhaus for his insightful discussions regarding the areas I have worked in my thesis. I am also thankful to Lim Ci Wen Charles for inviting me to visit CQT, Singapore to spend two wonderful weeks of research time there.

I want to thank Elham Kashefi, Nobert Lütkenhaus, Antonio Ać in and David Elkouss for kindly agreeing to be the jury members for my thesis.

Outside work, I am grateful to have my closest set of friends, specially Adel, Mylou, Yozajandi, Danilo, Antoinette, Maxime, Caroline, Kaushik, Dalia, Praveer, Mainak, Aakanksha, Nilesh, Venkat, Kate, Vamsi, Subethaa for making my stay in Paris extremely enjoyable and being a family away from family for me. Special thanks to Adel for countless discussions

on navigating life in a foreign country, and his excellent cooking skills. And, to Mylou for being my first teacher to help with the French language. I am also grateful to my friends back in India, Raja, Mukul, Shalabh, Shubham, Rahul who have been there for me whenever I needed them.

And last but definitely not the least, I express special thanks to my family members who have been a pillar in my life and have supported me in all the ventures I have undertaken. Without their constant support and guidance, I would not be where I am today.

Merci Thank you Dhanyawaad

To my parents

Abstract

In this thesis we focus on designing protocols for quantum information processing tasks that can be implemented with current photonic technologies. We start by providing the first example of a communication model and a distributed task for which there exists a realistic quantum protocol asymptotically more efficient than any classical protocol, both in terms of communication and information resources. To this end, we extend the recently proposed coherent state mapping for quantum communication protocols, study the use of coherent state fingerprints over multiple channels and show their role in the design of an efficient quantum protocol for estimating the Euclidean distance between two real vectors within a constant factor.

In the second part of the thesis, we propose a new problem in one-way communication model, Sampling Matching problem, for which there exists an exponential gap between a realistic quantum protocol and any randomized classical protocol within bounded error. We implement this problem using attenuated coherent states and linear optics, and show an advantage in using quantum resources from very low input sizes to the problem. This new proposal is a far simplified alternative to the previous problems in one-way communication model due to it requiring $\mathcal{O}(1)$ linear optical elements for implementation. This facilitates the implementation of the quantum protocol for arbitrarily large input sizes.

Then we introduce a private-key quantum money-scheme with the verification protocol based on the Sampling Matching scheme. We look at the scheme when the Bank prepares notes as single photon superposition states. The features of our scheme include single-round classical interaction with the Bank, linear note re-usability, robustness against experimental imperfection, and an unconditional security against an adversary trying to forge the Bank note. We then follow up this work by proposing a practical quantum money-scheme when the Bank prepares notes as attenuated coherent states. This is an experimentally motivated framework which utilises the advantage offered by the Sampling Matching verification protocol that it requires only $\mathcal{O}(1)$ linear optical elements for implementation.

Finally we introduce a programmable device whose input states control the the measurement operation. In particular, our device is the generalised Sylvester-Hadamard operation to discriminate two unknown coherent states in the setting of a single copy of one state (*test* state), and $M-1$ copies of the other state (*reference* state). Our distinguishing scheme involves M linear optics components (50/50 beam splitters), and $M-1$ single photon threshold detectors. We show that our setting strictly improves the soundness in discriminating two coherent states compared to the setting when one is provided only a single copy of the two states.

Contents

1 Introduction

1.1 A Brief History of Quantum Mechanics

Towards the end of the nineteenth century, classical physics, characterised by Newtonian laws of mechanics, Maxwell's theory of electromagnetism, and Boltzmann's theory on statistical mechanics, were deemed successful enough to explain most relevant physical phenomena. Some physical phenomena which were still unexplained by these theories, were considered marginal, or exceptions in the behaviour of nature. One such major absurdity was the famous *ultraviolet catastrophe*, the classical theory prediction that a perfect black body emits infinite intensity radiation at high ultraviolet frequencies, which was not true in the experiments conducted in those times. This motivated Max Planck (1848-1947), regarded as one of the founding fathers of quantum theory, to hypothesise that the radiating energy must be discretised packets, which he termed *quanta* [Pla13]. This brought in the first wave of revolution towards quantum mechanics.

Planck's theory became widely accepted when Albert Einstein (1875-1955) provided an explanation of the *photo-electric effect* using the discretised packets of energy (*photons*), the phenomenon where applying an electromagnetic radiation beyond the threshold energy on a metallic surface produces a current in the metal. Subsequently, in the decades from 1920 to 1940, thanks to the works of Neils Bohr, Louis De Broglie, Erwin Schrödinger, Werner Heisenberg, Paul Dirac, Wolfgang Pauli and others, a major development took place into formulating quantum mechanics from the initial quantum theory.

Quantum mechanics as a theory has some remarkable conceptual differences as compared to the existing classical mechanics. Some of these concepts include:

(i) *Randomness*: Quantum mechanics has randomness as a fundamental element of the theory. This is in contrast with classical mechanics models, under which the evolution of a system is deterministic. The evolution of a quantum mechanical state is not deterministic, and starting from exact same conditions, one may end up with different

results. Note that this is not due to the imprecision of the measurement device, but rather an intrinsic property of quantum mechanics.

(ii) *Uncertainty*: Another feature of quantum mechanics is that a measurement technique interferes with the system, thus changing its state. This is due to Heisenberg's uncertainty principle, which states that the measurement of one conjugate quantity of the quantum mechanical state with a certain accuracy inhibits the measurement of the other conjugate quantity with the same accuracy. In classical mechanics, all the variables are non-conjugate, and thus can be independently measured to arbitrary precision.

(iii) *Wave-particle duality*: In classical wave theory, a wave is the result of coherent displacement of multiple particles. Some examples include sound waves, ocean waves, electric and magnetic waves. However, quantum theory also exhibits this interference, or in other words, even the discretised particles exhibit wave-like phenomena. This forms the fundamental wave-particle duality in quantum mechanics. It was exhibited in the version of Young's double slit experiment [CM91].

(iv) *Superposition*: This feature of quantum mechanics states that for any two distinct quantum states, ϕ and ψ, any linear combination of these states $\alpha\phi + \beta\psi$ is also an accepted quantum state. This is one of the major properties of quantum mechanics that provides advantages in information processing and computation over classical mechanics.

(v) *Entanglement*: The most striking and counter-intuitive feature of quantum mechanics is entanglement. This feature has no analogue in classical mechanics. Entanglement refers to the correlations among two or more quantum states, which are stronger than any achievable classical correlations. This term was first coined by Schrödinger. Later Einstein, Podolsky, and Rosen presented an apparent paradox that included entanglement. This was famously called the EPR paradox which stated that entanglement poses a threat to the completeness property of quantum mechanics, and thus it must be explained by a classical hidden variable theory. This was resolved by John Bell in 1964, who constructed an inequality, the Bell inequality, and proved an upper bound on it using the classical "local hidden-variable theory". He then showed that entangled states of two particles violate this inequality, thus proving that there is no classical hidden variable theory which explains entanglement [Bel01].

Richard Feynman was first to suggest that quantum mechanics could be used to produce information systems that could be much more powerful than classical computers [Fey82]. In his words,

> "*Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look easy*" [Fey82]

Around the same time, Charles Bennett and Gilles Brassard explored the ideas of secure communication on channels via quantum mechanics. This was the first quantum cryptographic protocol providing unconditional security in secure communications [BB14]. Subsequently, there have been enormous applications of quantum mechanics in four major areas: *quantum computation*, *quantum communication*, *quantum simulation* and, *quantum sensing and metrology*.

In the major part of the thesis, we focus on *quantum communication*. Specifically our goal is to investigate the models where protocols based on quantum mechanics offer an improvement in efficiency and security of information transfer in communication links, compared to the classical communications. Subsequently in the last part, we focus on *quantum computations*, where we construct an optimal unitary machine to distinguish two non-orthogonal quantum states.

1.2 From Classical to Quantum Information

All practically information tasks today are realised using integrated chips consisting of semi-conductor devices and fibre optics. The basic components in these devices, electrons in semi-conducting devices and photons in optical fibres, obey quantum mechanics instead of classical mechanics. However, for current technologies, it is important that these devices do not operate in the regime where quantum effects are prominent. Let us understand what happens when these devices start showing quantum effects. In traditional information sciences, the input-output current/voltage relation is given by classical mechanics. Thus, a certain input should produce a certain deterministic output after passing through these devices. However, when these devices start operating at the few electron/photon regime, then the inherent uncertainty principle of quantum mechanics starts to dominate which can result in the input-output relation being a quantum superposition, instead of fixed values as predicted by classical mechanics. Engineers have sought for alternative ways to get around this issue. However this has resulted in the device not achieving its optimal performance. The only way to harness the optimal performance in these miniaturised devices is by considering quantum effects i.e. describing the input-output relation using quantum mechanics.

Quantum information science differs from the classical analogue, not only in a sense that it provides an accurate understanding of information processing behaviour in the regime mentioned above, but also because it introduces the possibility of performing tasks that are impossible in the classical world. This has triggered a major interest in quantum information science, to find tasks for which it is possible to prove the superiority of quantum information compared to classical information, and to demonstrate this advantage experimentally.

An area where this has been illustrated, for instance, is *in nonlocal games*, where experiments have confirmed the violation of Bell inequalities that correspond to better-than-classical strategies for the Clauser-Horne-Shimony-Holt (CHSH) and other Bayesian

type games [HBD+15, TBZG98, MMM+08, AWB+09, PKL+15]. This area prominently harnesses the power of entanglement, which has no analogue in classical theory.

Another prominent example is *quantum cryptography*, where many protocols have been demonstrated to be unconditionally secure, compared to computational security provided in the classical world. Prominent examples include quantum key distribution [JKJL+13, LBGP+07, SBPC+09, LME+09], device-independent quantum cryptography [ABG+07, MPA11, GBHA10], digital signatures [DCK+16], coin flipping [PJL+14], and quantum money [BOV+18, GAA+18].

Unlike the above mentioned areas, the task of implementing most *quantum algorithms* has been extremely challenging with current technologies, with the exception of non-universal boson sampling machines that have been realised for small inputs [TDH+13, COR+13, SVB+14], IQP circuits [FH16, BMS17, BGK17, GWD17, BVHS+18] or random quantum circuits [AC16, BIS+18]. Another recent proposal deals with the power of quantum interactive proofs for verifying NP-complete problems with small proofs [ABD+08, ADK17]. The reason for this difficulty is that quantum algorithms require a large number of fault tolerant qubits to demonstrate an advantage over the classical algorithms, which has been hard to achieve.

With an emphasis on engineering, there has been considerable progress made in the last decade to improve the technology that meets the requirement. The best push in this regard has been the efforts towards engineering of a 72-qubit quantum computing device by Google. This implementation is based on superconducting quantum bits [CW08]. Research in superconducting based architecture is also being conducted by Microsoft, IBM, Rigetti, and Intel, among others.

The other major push is by the D-Wave computing based on quantum annealing, which claims to have of the order of thousands of logical qubits [IMV]. However, D-Wave is not a universal quantum computer and is very specific to solving optimisation based problems.

Several other architectures have been proposed for quantum computing. These include the *trapped ion based quantum computer* [KMW02], the *quantum dot computer* [LD98], the *nuclear magnetic resonance* [VSB+01], the *linear optical quantum computer*[KMN+07], the *diamond-based quantum computer* [Hol07], among others.

There is another area in quantum information which does not involve finding tasks to demonstrate quantum advantage, but rather focuses on accessing data once we have a functioning quantum computer. The task of *verification* of the result of a quantum computer, to make sure it is doing what it claims it's doing, is an important field of study, especially when there has much progress of late into the development of a quantum computer. The first such works in this regard include the verifier possessing a bounded quantum computer, and verifying the quantum computation of an all powerful user [BFK09, GKK17, KDK15]. This has been dramatically improved in [Mah18], where it is sufficient for a classical verifier to verify the computation of an all powerful user. This result utilises the cryptographic primitive based on *learning with errors*, which has been secure against any quantum adversarial

proposition until now.

Another important task involves distinguishing two non-orthogonal quantum states. Contrary to classical computing where two classical strings can be checked bit-wise, quantum states can be superposition states that do not allow us to have access to each element of the superposition simultaneously. Simulating a quantum state classically requires an exponential amount of resources and is thus deemed infeasible. Several works including demonstration of the optimal distinguishing operation has been shown by [ACMT+07, BCJ03, CDM+18].

1.3 Quantum Communication

Quantum communication is a field of applied physics that comes under the domain of quantum information tasks. Its most interesting applications include performing efficient communications, and by this we mean performing tasks with optimal time and information resources. This comes under *quantum communication complexity*, an ideal resource model for proving quantum superiority involving two or more parties, each receiving an input and with the goal of jointly performing a distributed task on a communication channel with minimum possible resources. There has been a lot of work towards proving that quantum resources lead to exponential asymptotic savings compared to classical resources [BCWDW01, BCW98, Raz99, BYJK04, GKK+07, Gav16, RK11].

The second application involves performing secure communications, a task of protecting information channels against an eavesdropper by means of *quantum cryptography*. We have already mentioned some of the theoretical and experimental progress made in this domain. In this thesis we focus on the idea of developing money-scheme based on quantum states. This was also the first quantum cryptographic primitive proposed in the 1980s by Stephen Wiesner [Wie83], whose idea was to prepare an unforgeable money scheme based on the bank notes being quantum states. The security of the bank notes was based on the no-cloning property of quantum mechanics [WZ82]. Several other schemes on quantum money have been proposed since then [PYJ+12, AC12, FGH+12, Gav12, GK15, MP16, AA17]. Contrary to existing classical money schemes which are based on computational assumptions, like RSA [RSA78], the schemes for quantum money are based on the inherent property of nature, and thus provide unconditional security against the note forger as long as quantum mechanics is not violated. These money schemes have been difficult to implement until recently (recent proposals are proof-of-principle implementations), due to the fact that they necessitate the creation of a large number of quantum states and storing them in a memory. However, these implementations do seem plausible in the near future with major advances being made in the development of quantum memory to store the money states [JSC+04, LST09, FL02, NVG+14].

We look at these two applications in detail in the section below.

1.3.1 Efficiency in Communication

Efficiency of communication is an important factor in understanding the optimal performance of a communication protocol. This is studied in great deal in *quantum communication complexity*. The basic assumption in this field is that all the communicating parties are honest i.e. they perform the given task as required and do not deviate in order to obtain individual gains. There is also no eavesdropper in the communication channel.

The basic setting involves two or more parties performing a distributed task across the communication channel. Multiple communication models have been constructed in this setting: one-way model, two-way interactive model and, simultaneous message passing model. Under these models, one can study the class of problems with the objective of solving the distributed task either deterministically, or randomly (the task can be computed with an error probability). The efficiency is then defined as the minimum communication resources required to solve the task. This is discussed in detail in Chapter 2.

1.3.2 Security in Communication

Security is the primary application of communication links in the real world, where the objective is to perform secure communications even in the presence of an eavesdropper trying to gain access to the secret information being communicated. Informally, we call a system *secure*, if only a legitimate user can gain access to the message. This was first studied by Claude Shannon in 1949 [Sha49]. He described two levels of security, information-theoretic and computational security.

(i) *Information-theoretic security*: A system is called perfectly secure if the eavesdropper cannot gain any information about the secret even if they have unlimited computational power. This security notion is also called perfect security. The most common example of an information theoretically secure system is *one-time* padding. This is an encryption technique that cannot be cracked, but requires the use of a one-time pre-shared key which is the same size as, or longer than, the message being sent. However, this security comes at a price: a long secret key which cannot be reused. Hence, there has been considerable interest in finding cryptographic schemes which require a shorter keys that can be reused. Quantum mechanics, by virtue of the no-cloning property, is an ideal platform for achieving information theoretic security.

(ii) *Computational security*: A system is called computationally secure if an eavesdropper with limited resources cannot get any information about the secret. Generally, in order to break this security, one needs to solve a computationally hard problem, which cannot be solved in polynomial time with limited resources. A famous example of this is the RSA cryptosystem [RSA78], which is based on the assumption that it is hard to find the prime factor of a large number in polynomial time. However, cryptosystems based

on computational security are prone to becoming compromised with the advent of new technology. The RSA cryptosystem, for example, does not yet have an efficient classical algorithm, but can be broken using a quantum algorithm [Sho99].

1.4 Implementation of Communication Schemes

Quantum communication schemes offer unparalleled advantages, both in efficiency and security of communications, compared to the classical schemes. However, it has been generally difficult to demonstrate this advantage experimentally. This is because quantum based schemes necessitate the preparation of large superposition and/or entangled states, require minimal de-coherence of the quantum states during the experiment run, and apply sophisticated measurement schemes to extract information. This is out of reach for current photonic technologies.

There are two methods to get around this issue. One is to develop technologies that meet the requirement of implementing large scale quantum schemes. Although there has been considerable progress made to improve the technology required for quantum communication, apart from quantum key-distribution, there is still a significant gap between the requirement and availability. To overcome this issue, we use the second method which is to tailor the quantum schemes in order to be implementable with current technology. This alternative method to implement quantum schemes involves: mapping the current quantum protocols into an experimentally accessible framework of coherent states and linear optics. The coherent mapping of qubit protocols contains three important aspects: preparation of qubit states, linear operations on the state, and measurement on the final state. It shows that there is a one-to-one mapping of the qubit formalism with the coherent state formalism, while still maintaining the property that the quantum protocol reveals an exponentially smaller amount of information than the classical protocol [AL14a]. Building on this idea, quantum communication complexity protocols have been proposed [AL14b, KDK17]. Experimental demonstrations of this mapping include [XAW$^+$15, GXY$^+$16]. We further extend this idea in our thesis to propose new problems in quantum communication complexity models and quantum money schemes.

1.5 Results in the Thesis

This thesis contains four major results, divided into four chapters. It is hoped that each of these results will pave the way for other new exciting results.

1. Euclidean Distance Communication Complexity: We propose a multiplexed simultaneous message passing communication complexity model, with the objective of solving Euclidean distance problem within an additive constant, with bounded error. This problem

has applications in machine learning, specifically recommendation systems [KP16]. For this problem, we show for the first time that, after a threshold input size, the coherent state protocol performs better than the classical analogue. We have experimentally implemented this scheme, and although the results have no yet out-performed the classical protocol (due to limited capability of our measurement devices), we identify the devices we need to achieve this.
This has resulted in the publication titled: *Efficient quantum communications with coherent state fingerprints over multiple channels* by N.K., Eleni Diamanti, and Iordanis Kerenidis. [Phys. Rev. A 95, 032337]

2. Sampling Matching Communication Complexity: We introduce a new problem in the one-way randomised communication complexity model, the Sampling Matching model. For this problem, we show that the information resources in the coherent state protocol outperform the information resources in the classical protocol after a certain threshold input size. Further, we perform an experimental demonstration of the coherent state protocol, showing that we beat the best classical protocol to solve this problem.
This has resulted in the publication titled: *Experimental demonstration of quantum advantage for one-way quantum communication complexity* by N.K., Iordanis Kerenidis, and Eleni Diamanti. [arXiv: 1811.09154]

3. Quantum Money using Sampling Matching Verification: We propose a private-key quantum money scheme using classical communication in verification. The features of our scheme include a single round of classical communication with the Bank, re-usability of the Bank note, and robustness under experimental imperfections. Our scheme is the first one to allow an experimental realisation for noise tolerance as high as 21.4%.
This has resulted in the preparation of the manuscript *Practical quantum money schemes via the Sampling Matching problem* by N.K., and Iordanis Kerenidis. [Manuscript 2018]

4. Programmable Measurement with Coherent States: We propose an optimal distinguishing scheme for two coherent states in the setting where one is provided a single copy of one state, and multiple copies of the other state. Our distinguishing scheme involves the linear optics component, 50/50 beam splitter, and the single photon threshold detectors. We show that our setting strictly improves the soundness compared to the setting of single copy of two unknown coherent states.
This has resulted in the preparation of the manuscript *Optimal universal scheme for Quantum Information processing with coherent states* by N.K., Ulysse Chabaud, Damian Markham, and Eleni Diamanti. [Manuscript 2018]

1.6 Outline of the Thesis

This thesis focuses on the design, analysis and implementation of quantum communication and cryptographic protocols using coherent states and linear optics, which are easy to realise in realistic experimental settings. It has been organised as follows.

Chapter 2 starts with all the necessary background in quantum mechanics. We then present an overview of linear optics and coherent states, which is the backbone of our thesis. Next, we talk about coherent state mapping, an abstract mapping scheme to map the prepare-and-measure-based qubit protocols to coherent states. We study the inherent difference between coherent state encoding and single photon encoding. Finally, we define the notions of classical and quantum communication complexity which we will use in coming chapters.

In Chapter 3, we introduce a multiplexed simultaneous message passing communication complexity model, with the objective of solving the Euclidean distance problem in the randomised setting. We define the classical and quantum (coherent state) resources for this problem. Next, we give the experimental methods used to implement this protocol using coherent states and linear optics, and present the experimental analysis of our results which compare the classical and coherent state resources.

Chapter 4 begins with a review of the one-way randomised communication complexity model to solve the Hidden Matching problem. Next, inspired by this model, we introduce an experimentally realisable one-way randomised communication complexity model, the Sampling Matching model. We state the classical resources and compute the quantum coherent state resources to solve this task in the randomised setting. We then give the experimental methods used to implement this protocol using coherent states and linear optics, and present the experimental analysis of our results, comparing the the classical and coherent state resources.

Chapter 5 focuses on a private key quantum money scheme using single photon superposition states and the Sampling Matching verification protocol. We start by defining the private-key quantum money scheme and identify the tools required to construct it. Next, we formally introduce our scheme and provide the full-fledged information theoretic security for our scheme. Finally, we present an experimentally motivated framework of quantum money scheme using attenuated coherent states and discuss the correctness and unforgeability in this framework.

Chapter 6 studies the ability to distinguish two non-orthogonal states, in a setting where one is provided one copy of a state (test state) and multiple copies of the other state (reference state). Our analysis applies specifically for coherent states. We show that the ability to distinguish two different states increases exponentially with the number of copies of the reference state, even in a realistic experimental setting.

In Chapter 7, we conclude the thesis by providing a brief summary and some interesting open problems arising from the results in earlier chapters.

2 Ingredients

In this chapter we provide the ingredients of the basic concepts on quantum mechanics and linear optics that are later used in the thesis. We start by reviewing the notions on quantum mechanics: preparation of quantum states, unitary operation, and measurement. We then talk about linear optics where we review quantum mechanics operations using linear optics elements. Subsequently we move to the description of coherent states which are the backbone of the thesis. We talk about the coherent state mapping, an ideal one-to-one map for any prepare-and-measure qubit state protocols. We point out the inherent difference in quantum protocols with coherent state encoding versus the single photon encoding.

In the last section, we define the notions on communication complexity including the different models studied under this notion and the communication resources.

2.1 Preliminaries on Quantum Mechanics

Quantum mechanics has been one of the most remarkable and accurate theories in physics giving an understanding of the workings of nature at microscopic level. With experiments confirming the postulates of quantum mechanics upto a tremendous precision, it has become an exciting domain to look to apply this theory in enhancing the information processing and computing tasks.

In this section, we review the basics of quantum mechanics. For further understanding please refer [NC02, GS18].

1. Quantum State: A classical bit is a two-state system - 0 or 1. Similar to the classical bit, the smallest possible processing unit for quantum information is a quantum bit (or qubit). It is an element of $\mathbb{C}^2$ and is written as,

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{2.1}$$

where $\alpha, \beta \in \mathbb{C}$ and satisfy $|\alpha|^2 + |\beta|^2 = 1$. The states $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ are the computational basis vectors in two-dimensional Hilbert space $\mathcal{H}_2$. Physically, this state can be realized by any two-level quantum mechanical system with the encoding in physical systems such as photon, coherent state of light, electrons, nucleus, quantum dots, optical lattices, to name a few.

In general, any pure quantum state of d-dimensions can be constructed from the basis vectors in $\mathbb{C}^d$ of the Hilbert space $\mathcal{H}_q$,

$$|\psi\rangle = \sum_{j=1}^{d} \lambda_j |j\rangle , \tag{2.2}$$

where $\{|1\rangle , |2\rangle , ..., |j\rangle\}$ form an orthogonal basis, with $\sum_{j=1}^{d} |\lambda_j|^2 = 1$.

2. Composite Quantum State: A quantum state in composition of multiple physical systems is just a tensor product of the quantum states of individual physical systems. For instance, the quantum state $|\psi_{12}\rangle$ represented by two d-dimensional quantum states is $\mathbb{C}^d \otimes \mathbb{C}^d$,

$$|\psi_{12}\rangle = \sum_{i,j} \lambda_{i,j} |ij\rangle , \tag{2.3}$$

where $\lambda_{i,j} \in \mathbb{C}$ for all i, j, and $\sum_{i,j} |\lambda_{i,j}|^2 = 1$. Here the state $|ij\rangle = |i\rangle \otimes |j\rangle$.

3. Unitary Transformation: A natural question to ask is how does a closed quantum system evolve with time? The postulate of quantum mechanics states that this evolution is via a *unitary transformation*.

A unitary transformation of size d is a bounded linear operation $U_d : \mathcal{H}_d \to \mathcal{H}_d$ on the Hilbert space $\mathcal{H}_d$ that satisfies $U_d U_d^\dagger = I_d$, where $U_d^\dagger$ is the hermitian conjugate of U_d, and I_d is the identity operator that maps the state back to itself.

The quantum state $|\psi\rangle$ at time t_1 is related to the quantum state $|\psi'\rangle$ at time t_2 by a unitary transformation U which depends solely on times t_1 and t_2,

$$|\psi'\rangle = U |\psi\rangle \tag{2.4}$$

Let us look at few commonly used unitary transformations on a single qubit which are important in quantum information and computation.

(i) Pauli Operator: The four most useful single qubit operations are the Pauli operations,

$$I \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, X \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y \equiv \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z \equiv \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{2.5}$$

where $i = \sqrt{-1}$. These matrices, together with $\{-1, \pm i\}$ form the Pauli group $\mathcal{G}_1$ on a single qubit,

$$\mathcal{G}_1 \equiv \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\} \tag{2.6}$$

The Pauli group on n qubits, $\mathcal{G}_n$, is the group generated by the operators described above applied to each of n qubits in the tensor product Hilbert space $\mathcal{H}^n$.

(ii) Hadamard Operator: This operator is defined as follows:

$$H \equiv \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{2.7}$$

This takes the basis states $\{|0\rangle, |1\rangle\} \rightarrow \{\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\}$.

(iii) $\pi/8$ Gate: Also called the T-gate, this is defined as follows,

$$T \equiv \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{pmatrix} \tag{2.8}$$

(iv) Phase Gate: Also called the S-gate, this is defined as follows,

$$S \equiv \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \tag{2.9}$$

Apart from these single-qubit gate operations, the most important two-qubit unitary transformation is C-NOT gate. This is defined as follows,

$$CNOT \equiv \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{2.10}$$

In terms of computational basis, the operation of CNOT is given by $|c\rangle |t\rangle \rightarrow |c\rangle |c \oplus t\rangle$.

There are many more interesting quantum gates apart from the ones we have listed. However, the C-NOT gate combined with the single qubit gates are the universal set of gates, meaning multiple qubit quantum gates can be constructed from these gates. If one restricts the single-qubit gates to the Pauli operators, the $\pi/8$-gate, then combining them with the C-NOT gate, one can approximate to arbitrary precision, any unitary transformation acting on multiple quibts. This result is due to Solovay and Kitaev [NC02].

4. Quantum Measurement: Once the states have been prepared and undergone unitary transformations, the last segment remains, which is the extraction of the information contained in the state. This operation is described by a collection $\{M_m\}$ of measurement operators. These operators act on the quantum state to produce m possible measurement outcomes. For an input quantum state $|\psi\rangle$, the probability of the occurrence of outcome m is given by,

$$p(m) = \text{Tr}(M_m^\dagger M_m |\psi\rangle \langle\psi|) \tag{2.11}$$

where Tr(.) is the trace operation. The state of the system after the measurement operation is,

$$\frac{M_m |\psi\rangle}{\sqrt{\text{Tr}(M_m^\dagger M_m |\psi\rangle \langle\psi|)}} \tag{2.12}$$

The measurement operators form a complete set,

$$\sum_m M_m^\dagger M_m = I \tag{2.13}$$

This also implies that $\sum_m p(m) = \sum_m \text{Tr}(M_m^\dagger M_m |\psi\rangle \langle\psi|) = \sum_m \text{Tr}(|\psi\rangle \langle\psi|) = 1$.

The measurement operation is essentially to distinguish between different quantum states. Classically, two non orthogonal vectors can be distinguished easily by comparing them bit wise. However, the situation is non trivial for non-orthogonal quantum states. In-fact, two non-orthogonal quantum states cannot be perfectly distinguished.

There are essentially two types of measurement operators. The *projective* type measurements $\{M_m\}$ are such that $M_m M_{m'} = \delta_{mm'} M_m$ and $\sum_m M_m^\dagger M_m = I$.

On the other hand, the POVM type of measurements, constructed from the non-negative measurement operators $\{M_m\}$ are defined as $E_m \equiv M_m^\dagger M_m$ such that, $\sum_m E_m = I$. These kind of operators are interesting when one is not much interested in the post-measurement state, and the primary interest is in the probabilities of the measurement outcomes.

5. Mixed Quantum State: The description above is for quantum systems whose state $|\psi\rangle$ is known. In the scenario when the complete information about a state is not available, for instance if a quantum system is in one of the states $\{|\psi_i\rangle\}_{1 \leqslant i \leqslant k}$ with respective probability p_i, then the quantum state can be represented as a *mixed state*. Mathematically, it is described by a *density operator*, that is a positive semi-definite operator with unit trace, given by

$$\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i| . \tag{2.14}$$

Note that a quantum state ρ is pure if it has rank 1, or equivalently if $\text{Tr}[\rho^2] = 1$.

If the transformation of a closed quantum is described by a unitary evolution U between times t_1 and t_2, then the corresponding density operators ρ and ρ' are related through,

$$\rho' = U \rho U^\dagger, \tag{2.15}$$

where $U^\dagger$ is the hermitian conjugate of U.

Measurements can also be described in density operator formulation. If we perform a measurement on a density operator ρ defined by measurement operators $\{M_m\}$, then the probability of obtaining outcome m is given by

$$p(m) = \text{Tr}(M_m^\dagger M_m \rho) \tag{2.16}$$

and the post-measurement state is

$$\frac{M_m \rho M_m^\dagger}{\mathrm{Tr}(M_m \rho M_m^\dagger)}. \tag{2.17}$$

Density operators are also useful to describe subsystems of composite systems. This description is provided by the *reduced density operator*. Suppose we have a bipartite physical system in the state ρ_{AB} on $\mathcal{H}_A \otimes \mathcal{H}_B$, then the reduced density operator for system A is defined as

$$\rho_A = \mathrm{Tr}_B(\rho_{AB}), \tag{2.18}$$

where Tr_B is the *partial trace* over system B. This is the linear map satisfying

$$\mathrm{Tr}_B(|a_1\rangle \langle a_2| \otimes |b_1\rangle \langle b_2|) = |a_1\rangle \langle a_2| \, \mathrm{Tr}(|b_1\rangle \langle b_2|), \tag{2.19}$$

where $|a_1\rangle, |a_2\rangle$ are any two elements of $\mathcal{H}_A$ and $|b_1\rangle, |b_2\rangle \in \mathcal{H}_B$.

6. Trace Distance: This is one of the most natural measures of the closeness of two quantum states. The trace distance between two quantum states ρ and σ is,

$$T(\rho, \sigma) = \frac{1}{2}\mathrm{Tr}|\rho - \sigma|_1 \tag{2.20}$$

where $|A|_1 \equiv \sqrt{AA^\dagger}$ is the Schatten 1-norm. Since the density matrices are Hermitian,

$$T(\rho, \sigma) = \frac{1}{2}\mathrm{Tr}[\sqrt{(\rho - \sigma)^2}] = \frac{1}{2}\sum_i |\lambda_i| \tag{2.21}$$

where λ_i's are the eigenvalues of the Hermitian matrix $\rho - \sigma$.

In the special case when $\rho = |\psi\rangle \langle\psi|$ and $\sigma = |\phi\rangle \langle\phi|$ are pure states then,

$$T(\rho, \sigma) = \sqrt{1 - |\langle\psi|\phi\rangle|^2} \tag{2.22}$$

A second measure on the distance between quantum states is the *fidelity*. However in this thesis, we will only use the concepts of trace distance.

7. No Cloning: One the major features of quantum states is the *no-cloning principle*, discovered by Wootters and Zurek [WZ82]. This principle implies that it is impossible to build a universal copying machine which takes an arbitrary quantum state $|\psi\rangle$ as input and outputs two identical copies of $|\psi\rangle$.

Theorem 1. *Assume there is a unitary operator U_{clone} that can prepare two copies of an arbitrary input state, i.e,*

$$U_{\text{clone}} |\phi\rangle \otimes |0\rangle = |\phi\rangle \otimes |\phi\rangle$$
$$U_{\text{clone}} |\psi\rangle \otimes |0\rangle = |\psi\rangle \otimes |\psi\rangle .$$

Then $\langle\psi|\phi\rangle$ is either 0 or 1.

Proof. Consider the inner product,

$$\begin{aligned}
\langle\phi|\psi\rangle &= (\langle\phi| \otimes \langle 0|)(|\psi\rangle \otimes |0\rangle) \\
&= (\langle\phi| \otimes \langle 0| U_{\text{clone}}^{\dagger})(U_{\text{clone}} |\psi\rangle \otimes |0\rangle) \qquad \text{since } U_{\text{clone}}^{\dagger} U_{\text{clone}} = I \\
&= (\langle\phi| \otimes \langle\phi|)(|\psi\rangle \otimes |\psi\rangle) \\
&= \langle\phi|\psi\rangle^2 .
\end{aligned}$$

This implies that $\langle\phi|\psi\rangle$ is either 0 or 1. □

The significance of Theorem 1 is that only orthogonal states are clonable, which corresponds to copying classical information. This is the basis of the security proof of *private-key quantum money* scheme in Chapter 5.

2.2 Linear Optics

Quantum information processing has attracted a lot of attention of past few decades. There are many different architectures for quantum computers based on different physical systems. These include atom- and ion-trap quantum computing, superconducting charge and flux qubits, nuclear magnetic resonance, spin- and charge-based quantum dots, nuclear spin quantum computing, and optical quantum computing. Each of these architectures have their own advantages and disadvantages in quantum information processing. In this section we look one such architecture, information processing via linear optics. This has the advantage that the smallest unit of quantum information (the photon) is potentially free from de-coherence: The quantum information stored in a photon tends to stay there unless it gets absorbed. However, the photons do not naturally interact with each other. A trivial way to interact with them is to make projective measurements with photo-detectors. More generally, the linear optics interaction is through beam splitters, half- and quarter-wave plates, phase shifters, etc. These constitute the basic building blocks of interaction in linear optics. Here, for our thesis, we discuss the creation of a qubit using single photon in superposition over spatial modes and their interaction using the beam splitter, and measurement in the photo-detectors.

1. Single photon qubit state: A single photon state is created by applying a creation operator on the vacuum state, $|1\rangle = \hat{a}^{\dagger} |0\rangle$. The name creation operator is because it applies on the fock state $|n\rangle$ in the following way,

$$\hat{a} |n\rangle = \sqrt{n} |n-1\rangle \quad \text{and} \quad \hat{a}^{\dagger} |n\rangle = \sqrt{n+1} |n+1\rangle \tag{2.23}$$

When the single photon is in superposition over two modes $|1\rangle_c \equiv |1\rangle \otimes |0\rangle \equiv |10\rangle$ and $|1\rangle_d \equiv |0\rangle \otimes |1\rangle \equiv |01\rangle$ (subscript denotes the mode), then the resulting qubit state can be created by the superposition over the two modes,

$$|1\rangle_{\psi} = \alpha |10\rangle + \beta |01\rangle \tag{2.24}$$

where $|\alpha|^2 + |\beta|^2 = 1$, and any factors $\alpha, \beta \in \mathbb{C}$ can be created by action of beam-splitter and phase shifters.

2. Phase Shifter: An important optical component is the single-mode phase shift. Its action is to change the phase of any given input mode,

$$\hat{a}^\dagger \to e^{i\phi\hat{a}^\dagger\hat{a}}\hat{a}^\dagger e^{i\phi\hat{a}^\dagger\hat{a}} = e^{i\phi}\hat{a}^\dagger \tag{2.25}$$

3. Beam Splitter Transformation: Another important optical component is beam splitter. It consists of a semi-reflective mirror: when light falls on this mirror, part will be reflected and part will be transmitted. The action of beam splitter is to transform the input modes $\{\hat{a}^\dagger, \hat{b}^\dagger\}$ into the output modes $\{\hat{c}^\dagger, \hat{d}^\dagger\}$ as depicted in Figure 2.1.

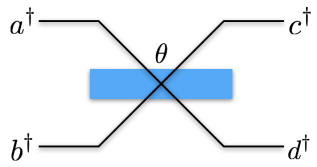

Figure 2.1: Illustration of a beam splitter beam splitter transforming input modes $\{\hat{a}^\dagger, \hat{b}^\dagger\}$ into the output modes $\{\hat{c}^\dagger, \hat{d}^\dagger\}$.

This input to output mode conversion for the beam splitter is given as,

$$\begin{aligned} \hat{c}^\dagger &= \cos\theta\hat{a}^\dagger + ie^{-i\varphi}\sin\theta\hat{b}^\dagger \\ \hat{d}^\dagger &= ie^{i\varphi}\sin\theta\hat{a}^\dagger + \cos\theta\hat{b}^\dagger \end{aligned} \tag{2.26}$$

The reflection and transmission coefficients R and T of the beam splitter are $R = \sin^2\theta$ and $T = 1 - R = \cos^2\theta$. The relative phase shift $ie^{i\varphi}$ ensures that the transformation is unitary. Typically, we choose either $\varphi = 0$ or $\varphi = \pi/2$. Mathematically, the two parameters θ and φ are the angles of a rotation about two orthogonal axes in the Poincaré sphere. The physical beam splitter can be described by any choice of θ and φ, provided the correct phase shifts are applied to the outgoing modes.

A special instance of the beam splitter we consider in our thesis is the 50/50 beam splitter. They are characterised by $R = T = 1/2$ and unto a phase factors, the transformation is,

$$\hat{c}^\dagger = \frac{1}{\sqrt{2}}(\hat{a}^\dagger + \hat{b}^\dagger) \quad \text{and} \quad \hat{d}^\dagger = \frac{1}{\sqrt{2}}(\hat{a}^\dagger - \hat{b}^\dagger) \tag{2.27}$$

For more details refer to [KMN$^+$07].

2.3 Coherent States

Coherent states refer to the states of quantized electromagnetic field that describe maximal kind of coherence and a classical kind of behaviour. Mathematically, a coherent state $|\alpha\rangle$ is defined to be the unique eigenstate of the annihilation operator $\hat{a}$ associated with the eigenvalue α,

$$\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle \tag{2.28}$$

where $\alpha \in \mathbb{C}$ since $\hat{a}$ is not hermitian operation. These are the quantum states that minimize the uncertainty relation with the uncertainty equally distributed between the position and momentum field quadratures. Hence they are addressed as classical like states. These states were completely characterized by Roy J. Glauber who was awarded the 2005 Nobel prize for his contribution to the quantum theory of optical coherence.

Formally, the coherent state $|\alpha\rangle$ is generated from the vacuum state $|0\rangle$ by the action of a displacement operator $D(\alpha)$,

$$|\alpha\rangle = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}\,|0\rangle = D(\alpha)\,|0\rangle \tag{2.29}$$

where α^* is the complex conjugate of α. Expanding Eq.(2.29) in the Fock state basis (also called number state basis) and using the annihilation relation of Eq.(2.23),

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}}\,|n\rangle = e^{-\frac{|\alpha|^2}{2}} e^{\alpha\hat{a}^\dagger}\,|0\rangle \tag{2.30}$$

1. Properties of Coherent States: The coherent states have the photons distributed in the poisonnian distribution. This is a necessary and sufficient condition that all the detection events are statistically independent. The average number of photons in the coherent state is,

$$\mu = \langle\alpha|N|\alpha\rangle = |\alpha|^2 \tag{2.31}$$

where $N = \hat{a}^\dagger\hat{a}$ is the occupation number operator.

The probability of detecting n photons in a coherent state is,

$$p_n = |\langle n|\alpha\rangle|^2 = \frac{\mu^n e^{-\mu}}{n!} \tag{2.32}$$

This helps us characterize the behaviour of single photon threshold detectors. A threshold detector "clicks" if it observes at least one photon $\{|1\rangle\langle 1|, |2\rangle\langle 2|, \cdots\}$, and does not click if it does not observe any photon $\{|0\rangle\langle 0|\}$. The probability of getting a click in the threshold detector is,

$$p_c = \sum_{n=1}^{\infty} |\langle n|\alpha\rangle|^2 = 1 - |\langle 0|\alpha\rangle|^2 = 1 - e^{-\mu} \tag{2.33}$$

2. Scalar Product of two Coherent States: For two coherent states $|\alpha\rangle$ and $|\beta\rangle$, the scalar product is,

$$|\langle\beta|\alpha\rangle| = e^{\frac{|\alpha-\beta|^2}{2}} \tag{2.34}$$

Coherent states are non-orthogonal states and their transition probability only vanishes in the limit of large differences $|\alpha - \beta| \gg 1$

3. Trace Distance: Since coherent states are pure states, hence the trace distance between two quantum states $|\alpha\rangle$ and $|\beta\rangle$ is,

$$\mathrm{T}(\alpha, \beta) = \sqrt{1 - |\langle\beta|\alpha\rangle|^2} \tag{2.35}$$

4. Completeness of Coherent States: Although the coherent states are non orthogonal, it is possible to expand coherent states in terms of a complete set of states. The completeness relation for the coherent states is,

$$\frac{1}{\pi}\int d^2\alpha \, |\alpha\rangle \langle\alpha| = 1 \tag{2.36}$$

In fact, the coherent states are "overcomplete", which means that, as a consequence of their non-orthogonality, any coherent state can be expanded in terms of all the other coherent states. So the coherent states are not linearly independent,

$$|\beta\rangle = \frac{1}{\pi}\int d^2\alpha \, |\alpha\rangle \langle\alpha|\beta\rangle \tag{2.37}$$

More details can be found in [GS18].

Now we describe an abstract mapping that converts quantum protocols that are based on creation of pure states of multiple qubits, applying unitary operations and performing projective measurements into an alternate map that uses sequence of coherent states, linear optics operations, and detection using single photon threshold detectors. The map was introduced by Arrazola et al [AL14a]. This mapping forms the backbone of the various protocols we introduce in subsequent chapters.

2.3.1 Coherent State Mapping

A majority of quantum communication protocols involves preparation of pure state in a hilbert space of fixed dimension, applying of unitary transformation on the states, and projective measurement in the canonical basis. An exact implementation of such protocols can be realised using physical qubits by considering a single photon in superposition over optical modes. A pure state $|\psi\rangle = \sum_{j=1}^{d} \lambda_j |j\rangle$ can be implemented using a single photon state in superposition over d modes,

$$|1\rangle_\psi = \hat{a}_\psi^\dagger |0\rangle = \sum_{j=1}^{d} \lambda_j |1\rangle_j \tag{2.38}$$

where $\sum_{j=1}^{d} |\lambda_j|^2 = 1$. In the language of creation operators, this is $\hat{a}_\psi^\dagger = \sum_{j=1}^{d} \lambda_j \hat{a}_j^\dagger$, where $\hat{a}_j^\dagger$ is the creation operator in j-th mode, and $\hat{a}_j^\dagger |0\rangle = |1\rangle_j$.

The unitary transformation is described in the Section 2.2 and the measurements in the canonical basis include photon counting detectors over each mode.

Motivated by the difficulty in implementing quantum protocols based on single photon encoding, an alternative mapping of such protocols using sequence of coherent states was introduced [AL14a].

1. Hilbert Space Mapping: A qubit protocol in a hilbert space of dimension d with the canonical basis $\{|j\rangle\}_{1\leqslant j\leqslant d}$ is mapped into d optical modes with the operators $\{\hat{a}_j\}_{1\leqslant j\leqslant d}$.

2. State Creation: A pure state $|\psi\rangle = \sum_{j=1}^{d} \lambda_j |j\rangle$ is mapped into a coherent state with parameter α and the creation operator $\hat{a}_\psi^\dagger = \sum_{j=1}^{d} \lambda_j \hat{a}_j^\dagger$,

$$|\alpha\rangle_\psi = e^{-\frac{|\alpha|^2}{2}} e^{\alpha \hat{a}_\psi^\dagger} |0\rangle = \bigotimes_{j=1}^{d} e^{-\frac{|\alpha\lambda_j|^2}{2}} e^{\alpha\lambda_j \hat{a}_j^\dagger} |0\rangle_j = \bigotimes_{j=1}^{d} |\alpha\lambda_j\rangle_j \tag{2.39}$$

where the subscript j denotes the optical mode. The coherent state $|\alpha\rangle_\psi$ is thus sequence of d coherent pulses, where the mean photon number of j-th coherent pulse is $|\alpha\lambda_j|^2$. Thus, over all the d coherent pulse, the mean photon number of the coherent state is $\mu = \sum_{j=1}^{d} |\alpha\lambda_j|^2 = |\alpha|^2$. Experimentally, the time bin optical modes allows for creation of these states for large d, something that was infeasible in single photon encoding of the qubit states.

3. Unitary Transformation: A unitary operation U acting on a pure qubit state is mapped into linear optics transformation corresponding to the same unitary operator U acting on the modes $\{\hat{a}_j\}_{1\leqslant j\leqslant d}$. Thus the transformation of the state is linked to the transformation of the modes as,

$$|\psi'\rangle = U|\psi\rangle \mapsto \begin{pmatrix} \hat{a'}_1 \\ \hat{a'}_2 \\ \vdots \\ \hat{a'}_d \end{pmatrix} = U \begin{pmatrix} \hat{a}_1 \\ \hat{a}_2 \\ \vdots \\ \hat{a}_d \end{pmatrix} \tag{2.40}$$

4. Projective Measurement: The projective measurement of a qubit state in the canonical basis $\{|j\rangle\}_{1\leqslant j\leqslant d}$ is mapped to two-outcome measurements in each of the d modes with single photon threshold detectors.

$$\{|j\rangle\langle j|\}_{1\leqslant j\leqslant d} \mapsto \bigotimes_{j=1}^{d} \mathrm{F}_c^j \tag{2.41}$$

where $c = 1$ for single photon detection, and 0 otherwise. $F_0^j = |0\rangle\langle 0|$, and $F_1^j = I - F_1^j$ are the projectors in the j-th mode. Thus an outcome in this mapping would correspond to the click pattern in the d modes. Coherent state mapping has 2^d possible outcomes compared

to the d possible outcomes of the qubit protocol. Nevertheless, the measurement statistics closely resemble those of the qubit projective measurement and they can be thought of as arising from several independent runs of the original qubit protocol.

5. Dimension of the Coherent State: A qubit state in superposition over d basis states contains $\mathcal{O}(\log_2 d)$ qubits, or in other words, lies in the hilbert space of dimension d. Hilbert space dimension is a good measure for to quantify the amount of qubits in a quantum protocol realised over physical systems,

$$C = \log_2[\dim(\mathcal{H})] \tag{2.42}$$

For coherent-state protocols obtained from the mapping, even though the actual Hilbert space is large (since distinct coherent states in the sequence are linearly independent), they effectively occupy a small Hilbert space, as is expressed in the following theorem:

Theorem 2. *For a pure state $|\psi\rangle$ in Hilbert space of dimension d and for any $\varepsilon > 0$, there exists a Hilbert space of $\mathcal{H}_\alpha$ with dimension d_α such that,*

$$\langle\alpha|_\psi \mathbb{P}_{\mathcal{H}_\alpha} |\alpha\rangle \geqslant 1 - \varepsilon, \quad \textit{and} \quad \log_2 d_\alpha = \mathcal{O}(\log_2 d) \tag{2.43}$$

Proof. The proof is based on the poissonian distribution of photons in the coherent state $|\alpha\rangle$ and that the probability of obtaining photons Δ far away from the mean photon number $|\alpha|^2$ is exponentially low. Consider the Hilbert space $\mathcal{H}_\alpha$ spanned by the set of number states $\otimes_{j=1}^{d} |n_j\rangle$ over d modes with $n = \sum_{j=1}^{d} n_j$, such that $|n - |\alpha|^2| \leqslant \Delta$. This is the space spanned by number states which are close to the average photon number $|\alpha|^2$.

The dimension of H_α is then,

$$d_\alpha = \sum_{n=|\alpha|^2-\Delta}^{|\alpha|^2+\Delta} \binom{n+d-1}{d-1} \leqslant 2\Delta \binom{|\alpha|^2+\Delta+d-1}{d-1} \tag{2.44}$$

which gives us,

$$\log_2 d_\alpha \leqslant (|\alpha|^2 + \Delta) \log_2(|\alpha|^2 + \Delta + d - 1) + \log_2 2\Delta \tag{2.45}$$

□

Now, $\langle\alpha|_\psi \mathbb{P}_{\mathcal{H}_\alpha} |\alpha\rangle$ is the probability of applying the projection $\mathbb{P}_{\mathcal{H}_\alpha}$ onto the coherent state and obtaining the value of n such that $|n - |\alpha|^2| \leqslant \Delta$. Using the poissonian probability of the coherent state, we obtain using the chernoff bound that,

$$P(|n - |\alpha|^2| \leqslant \Delta) \geqslant 1 - 2e^{-|\alpha|^2} \left(\frac{e|\alpha|^2}{|\alpha|^2 + \Delta}\right)^{|\alpha|^2+\Delta} \tag{2.46}$$

which can be reduced to any $\varepsilon > 0$ by appropriately choosing Δ and keeping $|\alpha|^2$ independent of d. Therefore, the fact that the mean photon number is independent of the number of

modes d, leads to the states involved effectively occupying a Hilbert space of dimension that $\mathcal{H}_\alpha \approx d^{|\alpha|^2}$ which is comparable to that of the original $\mathcal{H}$ of dimension d. Thus asymptotically, the protocol using coherent states utilizes the same size of transmitted information resources as the qubit protocol.

6. Outcome Probability: Qubit protocols involve performing projective measurements on the canonical basis $\{|j\rangle\}_{1\leqslant j\leqslant d}$ on the input state $|\psi\rangle = \sum_{j=1}^{d} \lambda_j |j\rangle$. The probability of obtaining an outcome j is,

$$p_k = |\langle j|\psi\rangle|^2 = |\lambda_j|^2 \tag{2.47}$$

For coherent state encoding, since the state is a tensor product of coherent states in d modes, hence we measure each mode independently. However the photon clicks in each modes are not exclusive as this corresponds to the measurement of the coherent state with mean photon number $|\alpha|^2$.

The probability distribution of the number of photons in each mode of the coherent state is equivalent to performing multiple repetitions of the measurement of single photon state $|1\rangle_\psi = \sum_{j=1}^{d} \hat{a}^\dagger |0\rangle$, where the number of measurements is drawn from the poissonian distribution with mean $|\alpha|^2$. This can be seen by the following argument. After the measurement of each modes of the coherent state, the probability of obtaining $n_1, n_2, \cdots, n_d$ photons in the mode $\hat{a}_1, \hat{a}_2, \cdots, \hat{a}_d$, such that $\sum_{j=1}^{d} n_j = n$ is,

$$P(n_1, n_2, \cdots, n_d|n) = \frac{n!}{n_1! n_2! \cdots n_d!} |\lambda|^{2n_1} |\lambda|^{2n_2} \cdots |\lambda|^{2n_d} \tag{2.48}$$

which by the multinomial theorem is exactly equal to the probability of repeating the measurement of the single photon state n times, where n is obtained from the poissonian distribution with mean photon number $|\alpha|^2$ i.e. $p(n) = \frac{e^{-|\alpha|^2}|\alpha|^{2n}}{n!}$.

However, for most quantum states, the coefficients λ_j's are typically very small, so that the mean number of photons $|\alpha\lambda_j|^2$ is small for relatively small α values. Thus the probability of obtaining more than one click in each mode is exponentially low. In these circumstances, the number-resolving detectors are an overkill and the single photon threshold detectors are sufficient. For the threshold detectors, the probability of a click in the j-th mode is,

$$p_{\alpha,j} = 1 - e^{-|\alpha\lambda_j|^2} \approx |\alpha\lambda_j|^2 \tag{2.49}$$

where the approximation holds in the case $|\alpha\lambda_j|^2 \leqslant 1$. When the average photon number across the d modes is $|\alpha|^2 = 1$, then $p_{\alpha,j} \approx |\lambda_j|^2$, thus resembling the behaviour of qubit protocols.

2.3.2 Coherent State vs Single Photon Encoding

Coherent State mapping can be utilised as an alternate mapping to the protocols that employ the single photon encoding. However, contrary to single photon behaviour of observing

the Hong-ou Mandel effect [HOM87] when passing through the beam splitter, the coherent states behave rather deterministically. This is one of the consequences of the classical like behaviour of coherent states. In certain cases, this leads to a better performance of the quantum protocol while using the coherent state encoding. An example of this is the task of distinguishing two unknown quantum states [Chapter 6]. We explicitly emphasise this difference in behaviour by studying the evolution of phase encoded coherent states and phase encoded single photons while interfering through the 50/50 beam splitter.

Coherent State Behaviour

Consider we have two phase encoded coherent states $|\alpha_x\rangle = |-1^x\rangle_{\hat{a}}$ and $|\alpha_y\rangle = |-1^y\rangle_{\hat{b}}$ at modes $\hat{a}$ and $\hat{b}$ respectively, where $x, y \in \{0, 1\}$. We observe the effect when these two coherent states interfere in the 50/50 beam splitter.

The input to the beam splitter is,

$$|-1^x\rangle_{\hat{a}} \otimes |-1^y\rangle_{\hat{b}} = \exp(-1)\exp(-1^x\hat{a}^\dagger + -1^y\hat{b}^\dagger)\,|00\rangle_{\hat{a}\hat{b}} \tag{2.50}$$

where, $|00\rangle_{\hat{a}\hat{b}} = |0\rangle_{\hat{a}} \otimes |0\rangle_{\hat{b}}$

Using the input-output relation of a 50/50 beam splitter of Eq.(2.27), the output is:

$$\begin{aligned}
&\exp(-1)\exp\left(-1^x\frac{\hat{c}^\dagger + \hat{d}^\dagger}{\sqrt{2}} + -1^y\frac{\hat{c}^\dagger - \hat{d}^\dagger}{\sqrt{2}}\right)|00\rangle_{\hat{c}\hat{d}} \\
&= \exp(-1)\exp\left(\frac{(-1)^x + (-1)^y)}{\sqrt{2}}\hat{c}^\dagger + \frac{(-1)^x - (-1)^y}{\sqrt{2}}\hat{d}^\dagger\right)|00\rangle_{\hat{c}\hat{d}} \\
&= \exp(-1/2)\exp\left(\frac{(-1)^x + (1)^y}{\sqrt{2}}\hat{c}^\dagger\right)|0\rangle_{\hat{c}} \otimes \exp(-1/2)\exp\left(\frac{(-1)^x - (-1)^y}{\sqrt{2}}\hat{d}^\dagger\right)|0\rangle_{\hat{d}} \\
&= |\frac{(-1)^x + (-1)^y}{\sqrt{2}}\rangle_{\hat{c}} \otimes |\frac{(-1)^x - (-1)^y}{\sqrt{2}}\rangle_{\hat{d}}
\end{aligned} \tag{2.51}$$

If one uses the single photon threshold detectors characterised by Eq.(2.33) in modes $\hat{c}$ and $\hat{d}$, then if the parity $x \oplus y = 0$, there is zero probability of a click only in the detectors of $\hat{d}$ mode and on contrary, if the parity is 1, then there is zero probability of a click in the detector of $\hat{c}$ mode. Thus the beam splitter and threshold detectors act as an unambiguous parity discrimination tool for phase encoded coherent states, where the only case one would not be able to infer the parity of the inputs is if one does not observe the clicks in any detector.

Single photon Behaviour

Consider now we have two phase encoded single photon states $|1_x\rangle = |(-1)^x\rangle_{\hat{a}}$ and $|1_y\rangle = |(-1)^x\rangle_{\hat{b}}$ at input modes $\hat{a}$ and $\hat{b}$ respectively, where $x, y \in \{0, 1\}$. We now observe the effect when these two single photon states interfere in the 50/50 beam splitter.

The input of the beam splitter is,

$$|-1^x\rangle_{\hat{a}} \otimes |-1^y\rangle_{\hat{b}} = -1^x \hat{a^\dagger} \hat{b^\dagger} |00\rangle_{\hat{a}\hat{b}} \tag{2.52}$$

The output of the beam splitter is,

$$\begin{aligned} & (-1)^{x\oplus y} \frac{(\hat{c}^\dagger + \hat{d}^\dagger)(\hat{c}^\dagger - \hat{d}^\dagger)}{2} |00\rangle_{\hat{c}\hat{d}} \\ &= (-1)^{x\oplus y} \frac{\hat{c}^{\dagger 2} - \hat{d}^{\dagger 2}}{2} |00\rangle_{\hat{c}\hat{d}} \\ &= (-1)^{x\oplus y} (|2\rangle_{\hat{c}} |0\rangle_{\hat{d}} - |0\rangle_{\hat{c}} |2\rangle_{\hat{d}} \end{aligned} \tag{2.53}$$

If one uses the detector in output modes $\hat{c}$ and $\hat{d}$, then there is an equal probability of getting a click in both modes, irrespective of the parity input $x \oplus y$. The reason for this behaviour is the Hang-ou Mandel effect, i.e. if the two photons have the same polarization, and all other properties being equal (spectrum, arrival time, transverse spatial mode, etc.), then the two photons are said to be indistinguishable irrespectively of the phase $(-1)^x$ of the photons. This constitutes the primary difference in the behaviour of single photons vs coherent states.

The indistinguishability of the single photon encoding can be addressed if instead of phase encoding, the encoding is rather done in the polarization degree of freedom. Consider the following encoding. For input x or y = 0, the photon is encoded in the horizontal H polarization. And for x or y = 1, the photon is encoded in the vertical polarization V.

Now, suppose the parity $x \oplus y = 1$ (for simplicity suppose $x = 0$ and $y = 1$). Then the input of the beam splitter is,

$$|1\rangle_{\hat{a}_V} \otimes |1\rangle_{\hat{b}_H} = \hat{a}_V^\dagger \hat{b}_H^\dagger |00\rangle_{\hat{a}\hat{b}} \tag{2.54}$$

The output of the beam splitter is,

$$\begin{aligned} & \frac{(\hat{c}_V^\dagger + \hat{d}_V^\dagger)(\hat{c}_H^\dagger - \hat{d}_H^\dagger)}{2} |00\rangle_{\hat{c}\hat{d}} \\ &= \frac{1}{2} (\hat{c}_V^\dagger \hat{c}_H^\dagger - \hat{c}_V^\dagger \hat{d}_H^\dagger + \hat{d}_V^\dagger \hat{c}_H^\dagger - \hat{d}_V^\dagger \hat{d}_H^\dagger) |00\rangle_{\hat{c}\hat{d}} \end{aligned} \tag{2.55}$$

The first term contains both photons (H and V) in mode $\hat{c}$, the second and third terms contain one photon in each mode $\hat{c}$ and $\hat{d}$, and the fourth term contains both photons (H and V) in mode $\hat{d}$. This means that we can either get both photons in the $\hat{c}$ or $\hat{d}$ mode, or 1 in $\hat{c}$ and 1 in $\hat{d}$.

Now, suppose the parity $x \oplus y = 0$ (for simplicity suppose $x = 0$ and $y = 0$). Then the input of the polarization beam splitter is,

$$|1\rangle_{\hat{a}_H} \otimes |1\rangle_{\hat{b}_H} = \hat{a}_H^\dagger \hat{b}_H^\dagger |00\rangle_{\hat{a}\hat{b}} \tag{2.56}$$

The output of the beam splitter is,

$$\begin{aligned} & \frac{(\hat{c}_H^\dagger + \hat{d}_H^\dagger)(\hat{c}_H^\dagger - \hat{d}_H^\dagger)}{2} |00\rangle_{\hat{c}\hat{d}} \\ &= \frac{1}{2}(\hat{c}_H^{\dagger 2} - \hat{d}_V^{\dagger 2}) |00\rangle_{\hat{c}\hat{d}} \\ &= |2\rangle_{\hat{c}_H^\dagger} |0\rangle_{\hat{d}_H^\dagger} - |0\rangle_{\hat{c}_H^\dagger} |2\rangle_{\hat{d}_H^\dagger} \end{aligned} \tag{2.57}$$

This means that we can either get both photons in $\hat{c}$ mode, or in $\hat{d}$ mode. When the parity $x \oplus y = 0$, the case of 1 photon each in $\hat{c}$ and $\hat{d}$ mode is not possible.

Thus when the photon is polarization encoded, we can distinguish the parity of the inputs.

Note: We saw that the beam splitter test can distinguish between two phase encoded coherent states but cannot distinguish between two phase encoded single photon states. However, if the input of the beam splitter is a single photon in a superposition over two phase encoded modes, then the beam splitter test can effectively distinguish between the two phase values. Consider the superposition state in the input to the beam splitter,

$$\frac{1}{\sqrt{2}}((-1)^x |10\rangle_{\hat{a}\hat{b}} + (-1)^y |01\rangle_{\hat{a}\hat{b}}) = \frac{1}{\sqrt{2}}((-1)^x \hat{a} + (-1)^y \hat{b}) |00\rangle_{\hat{a}\hat{b}} \tag{2.58}$$

Then the output of the 50/50 beam splitter is,

$$\begin{aligned} & \frac{1}{2}[((-1)^x(\hat{c} + \hat{d}) + (-1)^y(\hat{c} + \hat{d})] |00\rangle_{\hat{c}\hat{d}} \\ &= \frac{1}{2}[((-1)^x + (-1)^y)\hat{c} + ((-1)^x - (-1)^y)\hat{d}] |00\rangle_{\hat{c}\hat{d}} \\ &= \frac{(-1)^x + (-1)^y}{2} |10\rangle_{\hat{c}\hat{d}} + \frac{(-1)^x - (-1)^y}{2} |01\rangle_{\hat{c}\hat{d}} \end{aligned} \tag{2.59}$$

This idea has been used in [ADK17] to develop the verification technique of a quantum phase encoded NP-complete proof.

2.4 Communication Complexity

Communication complexity is the study of amount of communication required by separate parties to jointly compute a distributed task, i.e when the input is distributed among two or more parties. This area was first introduced by [Yao79] to study the communication complexity for two parties, Alice and Bob, who, receive a n-bit string x, y respectively, and their objective is to compute a certain function $f(x, y)$ with the least amount of communication among them.

This area has been extensively studied in the field of theoretical computer science and with connections to other optimisation fields such as Very-Large-Scale-Integration circuit

designing, a process of creating integrated circuit chips by combining large number of transistors in the same chip, with the objective to minimize the energy used by decreasing the amount of electric signals required between the different electrical components during a distributed computation. Communication complexity also has relevance in the study of data structures, and in the optimization of computer networks. More details on application of this field in other domains can be found in [Kus97].

2.4.1 Formal Definition

We formally define the setting of communication complexity. Two parties, Alice and Bob, want to compute a function $f : \mathcal{D} \to Z$, where $\mathcal{D} \subseteq X \times Y$, and typically $Z \in \{0, 1\}$. Alice receives an input $x \in X$, while Bob receives an input $y \in Y$, with $(x, y) \in \mathcal{D}$. Let $r_A \in R_A$ by the private randomness of Alice, $r_B \in R_B$ be the private randomness of Bob, and $r_{AB} \in R_{AB}$ be the shared randomness among Alice and Bob. Let the message communicated by Alice be $m_A \in M_A$, where M_A is the set of all possible messages by Alice. And similarly, let $m_B \in M_B$ be the message communication by Bob, where M_B is the set of all possible messages by Bob. Suppose Alice and Bob use the protocol Π to compute the function f. We denote $\Pi(x, y)$ as the output of the function f when Alice and Bob receive the inputs x and y. The communication cost of the protocol is then defined as,

$$CC(\Pi, f) = \log_2 |M_A| + \log_2 |M_B| \tag{2.60}$$

Then the communication complexity for computing the function f is the minimum over all such protocols,

$$CC(f) = min_{\Pi} CC(\Pi) \tag{2.61}$$

2.4.2 Models of Communication Complexity

There are two major classes of communication complexity studied in the literature,

(i) *Deterministic Communication Complexity*: These class of problems require Alice and Bob to compute the certain function f deterministically. As an example, consider the task where Alice and Bob have to determine if they have the same input. In other words, they want to compute the function $EQ(x, y)$, where $EQ(x, y) = 1$ if the inputs are equal, and 0 otherwise. In this setting, when the players want to succeed with certainty, then the communication complexity for this task is,

$$CC_{det}(EQ) = n \tag{2.62}$$

In other words, one of the players (let us say Alice), needs to send the entire string to Bob, who then compares the inputs bit-wise to output the result with certainty.

(ii) *Randomized Communication Complexity*: This class of problems require Alice and Bob to compute the function f with a small error probability, lets say ε. The communication complexity in this randomized setting is $CC_{rd}(f, \varepsilon)$. In this thesis, all the models that we consider are in this randomized setting.

Both these classes have been richly studied under multiple models of communication complexity,

(i) *Shared Randomness Model*: This model is studied under the randomized communication complexity class. Here, Alice and Bob are allowed to to have a shared common randomness, i.e. they are allowed $r_{AB} \in R_{AB}$. Under this model, any protocol Π is defined by $\Pi_A : X \times R_{AB} \to M_A$, and $\Pi_B : Y \times R_{AB} \to M_B$. The communication cost and complexity of this model is defined by Eq.(2.60) and Eq.(2.61) respectively.

(ii) *Private Randomness Model*: This is a weaker model than the shared randomness, since it does not allow the players Alice and Bob to communicate their random bits. However, this is a more realistic model. It is also studied under the randomized communication complexity class. Here, the players are only allowed to have a private coin, i.e. Alice to have randomness $r_A \in R_A$, and Bob to have randomness $r_B \in R_B$. Under this model, any protocol Π is defined by $\Pi_A : X \times R_A \to M_A$, and $\Pi_B : Y \times R_B \to M_B$. The communication cost and complexity of this model is similarly defined by Eq.(2.60) and Eq.(2.61) respectively. However, by virtue of Newman's theorem [New91], this model is only slightly weaker than the the shared randomness model in a sense that, one needs to send only $\log(\text{Input size})$ bits more to simulate the shared randomness model.

(iii) *Two-Way Communication Model*: The most common model studied under communication complexity is the two-way model. This allows Alice and Bob to have multiple rounds of back-and-forth communication, before one player (say Bob) outputs the value of the certain function $f(x, y)$.

(iv) *One-Way Communication Model*: This model has gained prominence after the Hidden Matching problem introduced by Bar-Yossef et al [BYJK04]. This model allows Alice to communicate with Bob, but Bob is not allowed to communicate back to Alice. In Chapter 4, we have introduced another class of one-way communication model, the Sampling Matching model.

(v) *Simultaneous Message Passing Model*: This model was first introduced by Yao [Yao79] in his paper on communication complexity. It allows an extra party, the Referee, and the communication is only allowed from Alice to the Referee, and Bob to the Referee. In this model, it is the Referee who computes the function f from the message he receives from Alice and Bob. We study this problem in Chapter 3 where the task of the Referee is to compute the Euclidean distance of the inputs $ED(x, y)$ under the private randomness setting.

2.4.3 Classical vs Quantum Communication Complexity

Classical communication complexity [Kus97], is the domain of computing the amount of classical communication required to compute the value of a function $f(x, y)$.

In quantum communication complexity, the players are allowed to make use of a quantum computer, thus allowing them to communicate via qubits and/or entanglement states. This was first addressed by Yao [Yao93] in the two-way randomized communication complexity model, allowing the players to communicate via qubits. Cleve and Buhrman [CB97] introduced the model allowing players to share entangled states and communicating via classical bits. These two models are essential equivalent, in a sense that: a single qubit model in Yao framework is the same as two bit model in the Cleve and Burhman framework. The reason for this is that quantum teleportation allows for the communication of a qubit with one bit of communication and sharing of an EPR pair.

Quantum communication complexity provides an advantage over classical communication complexity in multiple scenarios. However, this not obvious, primarily due to Holevo's theorem [Hol73]. This theorem states that,

Theorem 3. *Let $\{\rho_1, \cdots, \rho_n\}$ be a set of mixed states and let ρ_X be one of these states drawn according to the probability distribution $P = \{p_1, \cdots, p_n\}$,*

Then for any measurement described by POVM's $\{E_Y\}$ and performed on $\rho = \sum_X p_X \rho_X$, the amount of accessible information about the input X without knowing the outcome Y of the measurement, is bounded,

$$I(X : Y) \leqslant S(\rho) - \sum_i p_i S(\rho_i) \tag{2.63}$$

where $\rho = \sum_i p_i \rho_i$, $I(X : Y)$ is the mutual information between X and Y, and $S(.)$ is the von Neumann entropy.

It implies that information retrieved from n qubits is not more than the information retrieved by n classical bits. However, for most of the communication complexity tasks, the task is not to determine the input itself (in which case, quantum communication does not have advantage over classical communication), rather the task is to determine a function f of the input. In these scenarios, it has been show that quantum communication complexity can provide significant advantage compared to the classical communication complexity. A more detailed analysis can be found in [BCMDW10].

2.4.4 Communication Resources

Quantifying the communication resources is the measure of the performance of a communication protocol. The resources can be classified into two categories,

(i) *Transmitted Information*: For a communication model involving Alice and Bob, the transmitted information of a protocol calculates the real bits of information about the inputs that the messages carry. This is the communication complexity of the model as defined in Eq.(2.60). More details on this can be found in [KLLGR16].

(ii) *Time Resource*: The time unit is defined as the time to send a single bit/qubit over the communication channel, and then, in an optimal protocol, bits/qubits and communication time are equal, since one will always send one bit per time unit. However, in realistic implementations of quantum communication protocols, the time resource is the not the same as the number of bits communicated. We look at one such implementation of quantum communication complexity complexity model in Chapter 3 and 4, using the coherent state encoding for which the quantum time resource is not the same as the amount of qubits communicated.

3 Euclidean Distance Communication Problem

3.1 Introduction

Communication complexity is an ideal model for harnessing the power of quantum mechanics and understanding the efficiency of quantum networks over classical networks. This class of problems study the amount of communication required by separate parties to jointly compute a distributed task. We study one specific model of communication complexity, the randomized *simultaneous message passing model* (SMP) which was introduced by Andrew Yao in 1979 [Yao79]. This model investigates the following problem involving two separate parties, Alice and Bob, and a trusted agent, Referee. Alice receives an input $x \in \mathbb{X}$, while Bob receives an input $y \in \mathbb{Y}$. They are not allowed to communicate with one another directly, and the only communication possible is the one-way simultaneous communication from Alice and Bob, to the Referee. The objective for Alice, Bob and the Referee is to collectively output the correct value of some pre-defined function $f(x, y)$ with as high probability as possible, while minimizing the total amount of communication.

In 2001, the work by Buhrman et al [BCWDW01] introduced the notion of quantum fingerprinting for the randomized SMP model with private randomness. Their problem involved Alice and Bob receiving inputs $x, y \in \{0, 1\}^n$ respectively and the task of the Referee is to compute the Equality function EQ(x,y) of the inputs i.e.

$$\text{EQ(x,y)} = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{if } x \neq y \end{cases} \tag{3.1}$$

For this problem, they proposed a quantum protocol which performs the task with exponentially lower resources compared to the classical analogue.

There have been several other examples where communicating quantum information results in considerable savings in the communication overhead [BCW98, Raz99, BYJK04, GKK$^+$07, Gav16, RK11]. Nevertheless, it is in general difficult to test these results ex-

perimentally and demonstrate quantum superiority in practice since the quantum protocols require the creation of high dimensional superposition states and sustaining them for the entire duration of the experiment. These states can either be prepared using single photons in a superposition over large modes, or by preparing large, highly entangled states. These preparation methods are out of the reach of current photonic technologies.

Recently, Arrazola and Lütkenhaus proposed a mapping for encoding quantum communication protocols involving pure states of many qubits, unitary operations and projective measurements to protocols based on coherent states of light in a superposition of optical modes, linear optics operations and single-photon detection [AL14a]. This powerful model was used to propose the practical implementation of coherent state quantum fingerprints [AL14b], leading to two experimental demonstrations: a proof-of-principle use of such fingerprints for solving the Equality task asymptotically better than the best known classical protocol with respect to the transmitted information [XAW$^+$15]; and a subsequent implementation beating the classical lower bound for the transmitted information [GXY$^+$16]. Following these demonstrations that have focused on Equality and on transmitted information, an important question remains:

"Is there a realistic model for proving and testing in practice that quantum information is asymptotically better than classical for communication tasks with respect to all important communication and information resources?"

We answer in the affirmative by proposing a communication model and a task for which we prove that quantum mechanics allows for a considerably more efficient protocol in all relevant resources. We do this by building upon the mapping of [AL14a] to introduce coherent state fingerprints over multiple channels and show how to use them for solving efficiently a task that is at the foundation of many applications in Machine Learning, namely estimating the Euclidean distance of two real vectors within a constant factor. Our results show that, in principle, it is possible to demonstrate quantum superiority for advanced communication tasks in quantum networks using photonic technologies within experimental reach.

Over the next sections, we introduce the SMP model for solving the Euclidean distance problem. Our first model shows savings only in the transmitted information resource. In the second half of this chapter, we propose the modified SMP model involving multiple channels between Alice/Bob, and the Referee. This allows for reductions in the relevant transmitted information as well as time resources. Further we propose a method to implement the modified SMP model using an all-optical orthogonal frequency division multiplexing technique, a common multiplexing technique employed in the classical domain. Finally, we discuss the experimental implementation for the SMP model to solve the Equality problem. Our implementation is the first implementation of SMP model with separate paths for Alice and Bob. This is in contrast to the previous implementation based on sagnac loop interferometers, which allowed for a possibility of a direct communication between Alice and Bob. We discuss the advantages of this implementation and give a proposal to extend this to Euclidean distance implementation.

3.2 Communication Resources

The communication cost of the protocol is the number of bits the two players have to send to the Referee and the communication complexity is the minimum communication cost over all protocols that solve the task. In real world communication networks very often the cost is rather calculated as the time one uses the communication channel, for example on the phone network. We note that these costs are interchangeable, provided that the communication channel has a specific maximum rate. We define the time unit as the time to send a single bit over the communication channel, and then, in an optimal protocol, bits and communication time are equal, since one will always send one bit per time unit. Another resource one can study is the transmitted information, which instead of the number of bits sent, calculates the real bits of information about the inputs that the messages carry. For example, if Alice always sends the same, long message, independent of her input, then the communication time will be large, while the transmitted information will be zero, since no information about the input has been transmitted. Transmitted information is a resource that is important for privacy, when on top of having an efficient protocol, we want the Referee to solve the task without learning much about the players' inputs. One can define the transmitted information as the mutual information between the messages and the inputs and can upper bound it with the logarithm of the number of different messages. The transmitted information is always at most the communication time, since one bit carries at most one bit of information, and hence, the bottleneck is always the time.

We can similarly define the resources for quantum protocols. The communication time is again the number of time units the protocol takes, where in a time unit at most one qubit can be sent in expectation. Here, we have added "in expectation" since typically in quantum communications the qubits are realized by photons emitted by practical light sources and hence their mean number follows a poisson distribution [SBPC$^+$09]. In the following, we also make this change to the classical model to make a more correct comparison, *i.e.*, we allow one bit in expectation per time unit, which does not change the order of the communication time. We will also upper bound the transmitted information as the logarithm of the minimum dimension of the hilbert space that contains all the possible quantum messages that are sent in the protocol. For example, if Alice has as input an n-bit string x and sends a message that contains $n/2$ qubits of the form $|x_1 x_2 .. x_{n/2}\rangle$ and another $n/2$ qubits in the state $|0\rangle$, then the communication time is n, while the transmitted information is $n/2$.

3.3 Euclidean Distance Problem

We now describe a fundamental communication task. Our task involves two parties Alice and Bob, who possess large data sets x and y respectively, which are unit vectors in $\mathcal{R}^n$. They would like to estimate the closeness of their data set, or in words the Euclidean distance (for simplicity we define its square), $||x-y||_2^2 = \sum_{j=1}^{n}(x_j - y_j)^2$ (equivalently, the inner product

relates to Euclidean distance by $\langle x, y \rangle = 1 - ||x - y||_2^2/2)$.

Under this model, Alice and Bob are not allowed to communicate among themselves once the protocol begins. Their only communication is via the Referee. The parties are required to send a single round simultaneous message to the Referee, who after the receiving the message $m(x)$ and $m(y)$ respectively from the parties, outputs the value of Euclidean distance, ED(x,y), within a fixed constant ε, with a desired success probability at-least $1 - \delta$.

Intuitively, to solve the problem, Alice and Bob can transmit their entire data to the Referee, but this is non-optimal. The idea is to send fingerprints of the data, which are much shorter but still allow the Referee to approximate their Euclidean distance within some additive constant. Figure 3.1 illustrates the SMP model to estimate the Euclidean distance problem.

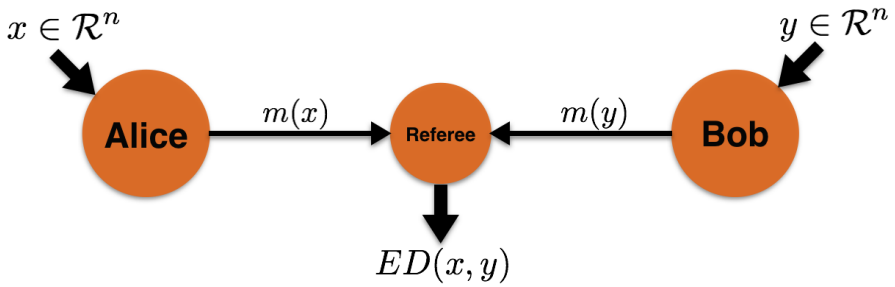

Figure 3.1: Illustration of the *simultaneous message passing model* to estimate the Euclidean distance of two distributed inputs $x, y \in \mathcal{R}^n$.

3.4 Best known Classical Protocol & Lower Bound

3.4.1 Relating Euclidean Distance and Equality

Before talking about the classical protocol and lower bounds for Euclidean distance problem, we see how this problem is related to the problem of computing Equality within some error probability. The idea is to relate the lower bound for Euclidean distance with the already known bounds for Equality.

Suppose we have a classical protocol that solves the Euclidean distance problem. For input size n, this protocol approximates the Euclidean distance within a fixed constant ε with a success probability at least $1 - \delta$. Using this protocol, we can construct the protocol to solve the Equality problem with success probability at least $1 - \delta$. To construct a protocol for Equality, we choose an error-correcting code (ECC) that amplifies the n-bit inputs x and y to m-bit codewords $E(x)$ and $E(y)$ respectively, with the hamming distance for such a code being $d > 2\varepsilon$. Then, upon using the Euclidean distance protocol on the codewords $E(x)$ and

$E(y)$, we have:

$$ED \begin{cases} \leqslant \varepsilon & \text{if } E(x) = E(y) \\ \geqslant (d - \varepsilon) > \varepsilon & \text{if } E(x) \neq E(y) \end{cases} \tag{3.2}$$

Thus Eq.(3.2) implies that $ED \leqslant \varepsilon$ iff $E(x) = E(y)$ which is only possible if $x = y$. The other scenario can occur only iff $x \neq y$. Hence, this protocol solves Equality on inputs x and y with probability $\geqslant 1 - \delta$.

The above reduction implies that any protocol estimating Euclidean distance within an error probability also solves the Equality problem within the same error probability. The resources required for solving the Equality problem with optimal resources is a lower bound on the resources required to estimate the Euclidean distance problem.

3.4.2 Classical Lower Bound

Classically, this problem requires Alice and Bob to send fingerprints of size $\Omega(\sqrt{n})$ as shown independently by Ambainis et al. [Amb96] , Babai et al. [BK97] and Newman et al. [New91, NS96]. We consider here that Alice and Bob do not have access to any shared randomness, otherwise the problem can be solved with only constant communication [KNR99]. It is a natural assumption that parties do not *a priori* have such shared resources, especially in large networks where the communication is between many different pairs of parties.

Further works by [GXY$^+$16] improved on the existing classical lower bounds. The tightest lower bound has been proposed by Arrazola et al. [AT16] where they prove the lower bound on the communication complexity (CC) of any classical protocol that computes Equality in the private randomness SMP model. This is also the lower bound on communication complexity for computing the Euclidean distance function. Their result states that to compute the Equality function within an error probability $\delta \in [0, \frac{1}{2})$, the communication resource is,

$$CC(EQ, \delta) \geqslant 2\sqrt{g(\delta)}\sqrt{n} - g(\delta) - 6, \tag{3.3}$$

where $g(x) = 2(1/2 - x)^2 \log e$.

3.4.3 Best Classical Protocol

As proposed by Babai et al. [BK97], the best classical protocol for solving the Equality problem uses $2\sqrt{n} + 1$ bits and succeeds with probability $1/4$. To get the desired success probability $1 - \delta$, the protocol is repeated $k = \log(\frac{1}{\delta})\frac{1}{\log 4/3}$ times. Thus the classical resource is $2k\sqrt{n} + k$.

3.5 Quantum Protocol

Quantum fingerprints to estimate the Euclidean distance can be exponentially shorter than the classical messages. The qubit protocol involves Alice and Bob creating and sending quantum fingerprints, namely

$$|\text{fin}_z\rangle = \sum_{j=1}^{n} z_j |j\rangle \tag{3.4}$$

where z is the n-bit string x, y of Alice and Bob respectively.

The Referee, upon receiving the fingerprints, estimates the Euclidean distance by performing a controlled swap operation on the fingerprints as shown in Figure 3.2. This gate operation outputs "1" with probability $1/2 + |\langle x, y\rangle|^2/2$ [BCWDW01].

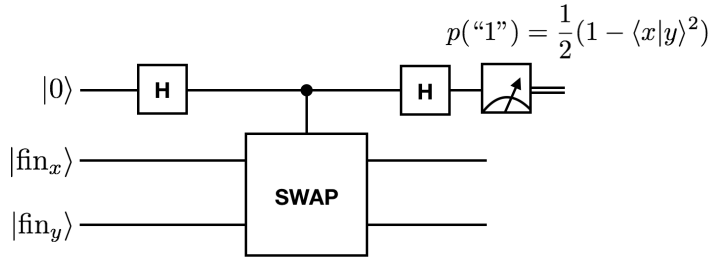

Figure 3.2: Swap test circuit employed by the Referee on the incoming fingerprint states. The probability of obtaining the output "1" relates to the inner product and hence the Euclidean distance of the inputs.

The Referee estimates this probability, and hence the Euclidean distance, within an additive constant ε with probability at least $1 - \delta$, using a constant number of fingerprints equal to $O(\log(1/\delta)/\varepsilon^2)$. The communication time is $\mathcal{O}(\log_2 n)$, since Alice and Bob send a constant number of fingerprints, and each fingerprint consists of $\log_2 n$ qubits and can be sent in $\log_2 n$ time units. The transmitted information is also $\mathcal{O}(\log n)$ and is equal to the communication time. Hence, if we look at the ratio of the quantum over the classical resources, then both the resources asymptotically goes to zero as n grows. Unfortunately, implementing these fingerprints with qubit systems is out of reach for current technologies for large n values.

The notion of quantum fingerprints has been used in practice for the Equality problem [AL14b, XAW$^+$15, GXY$^+$16], where the inputs are n-bit binary strings and the Referee checks whether the two strings are equal or not. We have already established that the Equality problem can be reduced with the help of error correcting codes to approximate the Euclidean distance between the two vectors within a constant factor. Since most real data is represented as real-valued vectors, the Euclidean Distance problem is more pertinent than Equality, since it is rather improbable that two different sets of real-valued data will be exactly equal. Hence,

here, we extend the use of the term quantum fingerprints to real-valued inputs, where we address whether the fingerprints can be used to approximate the distance of the inputs.

3.6 Coherent State Protocol

The coherent state mapping of [AL14a] led to a protocol for Equality with communication time $\mathcal{O}(n)$ and transmitted information $\mathcal{O}(\log_2 n)$. This protocol therefore provides an exponential advantage in the transmitted information, at the expense of a quadratically worse performance in communication time compared to the classical protocol, for which the order of both resources is $\Omega(\sqrt{n})$.

A schematic of the corresponding protocol for Euclidean Distance is shown in Figure 3.3. Alice and Bob's fingerprints are trains of n coherent states sent to the Referee. Alice's state, $|\alpha_x\rangle$, is prepared by the displacement operator $\hat{D}_x(\alpha) = \exp(\alpha\hat{a}_x^\dagger - \alpha^*\hat{a}_x)$ applied to the vacuum state, where $\hat{a}_x = \sum_{j=1}^n x_j\hat{b}_j$ is the annihilation operator of the fingerprint mode [AL14b], and $\hat{b}_j$ is the photon annihilation operator of the j^{th} time mode. Hence,

$$|\alpha_x\rangle = \hat{D}_x(\alpha)\,|0\rangle = \otimes_{j=1}^n |x_j\alpha\rangle_j\,, \tag{3.5}$$

where $|x_j\alpha\rangle_j$ is a coherent state with amplitude $x_j\alpha$ occupying the j^{th} mode. The mean photon number for the state $|\alpha_x\rangle$ is $\mu = \sum_j |x_j\alpha|^2 = |\alpha|^2$, independent of the input size. Bob similarly creates the fingerprint $|\alpha_y\rangle$.

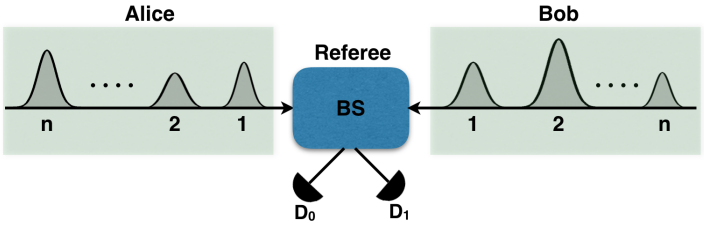

Figure 3.3: Alice and Bob send *n* coherent pulses, with the j^{th} pulse's amplitude determined by $x_j\alpha$ and $y_j\alpha$, respectively. The Referee interferes their states in a 50/50 BS and detects the output signals using single-photon detectors D_0 and D_1.

3.6.1 Euclidean Distance protocol analysis without imperfections

In this section, we analyse the performance of Euclidean Distance protocol in ideal condition i.e. without any experimental imperfections.

Once the coherent state fingerprints from Alice and Bob arrive at the Referee sequentially in time-bin modes, he uses a $50/50$ beam splitter (BS) to interfere the incoming coherent states as shown in Figure 3.3.

At each mode, the beam splitter transforms the input operators $\{\hat{a}^\dagger, \hat{b}^\dagger\}$ into the output modes $\{\hat{c}^\dagger, \hat{d}^\dagger\}$ as depicted in Figure 3.4.

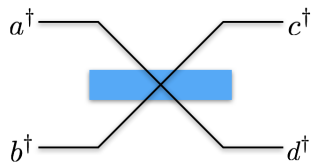

Figure 3.4: Illustration of a 50/50 beam splitter transforming input modes $\{\hat{a}^\dagger, \hat{b}^\dagger\}$ into the output modes $\{\hat{c}^\dagger, \hat{d}^\dagger\}$.

This input to output mode conversion for the 50/50 beam splitter is given as,

$$\begin{aligned} \hat{a}^\dagger &\rightarrow \frac{1}{\sqrt{2}}(\hat{c}^\dagger + \hat{d}^\dagger) \\ \hat{b}^\dagger &\rightarrow \frac{1}{\sqrt{2}}(\hat{c}^\dagger - \hat{d}^\dagger) \end{aligned} \tag{3.6}$$

The input state received by the Referee in the j^{th} time unit is,

$$|x_j\alpha\rangle_j \otimes |y_j\alpha\rangle_j \,, \tag{3.7}$$

In the ideal scenario, this yields the output state,

$$|\frac{(x_j + y_j)}{\sqrt{2}}\alpha\rangle_{j,D_0} \otimes |\frac{(x_j - y_j)}{\sqrt{2}}\alpha\rangle_{j,D_1} \,, \tag{3.8}$$

where the subscripts D_0 and D_1 denote the single-photon detectors placed at the output arms of the BS.

Previously, for Equality, only the clicks of D_1 have been used for the estimation. Then, since the expected number of clicks of the detector depends directly on its dark count probability, it is crucial to keep this probability very low. Here, we try to deal with this problem, by using the clicks from both detectors to construct a more robust estimator for the ED that can also be used for Equality.

More precisely, let Z_j^0 and Z_j^1 be the binary random variables that are 1 with the probability with which D_0 and D_1 clicks respectively at the j^{th} time unit, namely $p_j^0 = 1 - \exp(-\frac{\mu(x_j+y_j)^2}{2}) \approx \mu\frac{(x_j+y_j)^2}{2}$, and $p_j^1 = 1 - \exp(-\frac{\mu(x_j-y_j)^2}{2}) \approx \mu\frac{(x_j-y_j)^2}{2}$. Here, the approximation holds because we take μ to be typically small, and x and y are unit vectors in $\mathcal{R}^n$ and for large n the terms $(x_j + y_j)^2$ and $(x_j - y_j)^2$ are typically in the order of $1/n$. The Euclidean distance ($\tilde{E}$) is equal to

$$\tilde{E} = 2 - \frac{1}{\mu}\mathbb{E}[\sum_{j=1}^{n}(Z_j^0 - Z_j^1)]. \tag{3.9}$$

The advantage of using statistics from both detectors comes from the fact that the Euclidean distance estimator depends now on the difference of the clicks of the detectors, and hence on expectation the number of dark counts cancels out, when we assume the dark count probabilities are the same for both detectors. We remark that this can be enforced by symmetrization procedures [PJL$^+$14], although in practice, since the symmetrization will not be perfect, the estimator will in fact depend on the square of the dark count probability, which is easier to keep low.

By a Chernoff type argument [UM05], we can optimize the experimental parameters so that we can estimate $\sum_{j=1}^{n}(Z_j^0 - Z_j^1)$ within a factor ε with probability at least $1-\delta$. For constant ε, δ, the overall communication time is $\mathcal{O}(n)$ while the transmitted information is $\mathcal{O}(\mu \log n)$. Note that in each time unit, $\mu/n \ll 1$ photons are sent in expectation, thus satisfying our model's criterion of no more than one photon in each time unit.

3.6.2 Analysis in presence of Experimental imperfections

The coherent state fingerprinting implementation has three main sources of error. (i) The transmission loss is characterized by parameter $0 \leqslant \eta \leqslant 1$ which changes the state α to $\alpha' = \sqrt{\eta}\alpha$. This factor decreases the probability of obtaining a click in the detectors by a factor of η. (ii) The limited interferometer visibility $0 \leqslant \nu \leqslant 1$, and (iii) the dark count in the detectors characterized by probability p_{dark}. In presence of these imperfections, the output states for the Referee in the detectors D_0 and D_1 at the j^{th} time unit is,

$$|\frac{\alpha}{\sqrt{2}}\Big(\sqrt{\nu}(x_j+y_j)+\sqrt{1-\nu}(x_j-y_j)\Big)\rangle_{j,D_0} \otimes |\frac{\alpha}{\sqrt{2}}\Big(\sqrt{\nu}(x_j-y_j)+\sqrt{1-\nu}(x_j+y_j)\Big)\rangle_{j,D_1} \tag{3.10}$$

Let Z_j^0 and Z_j^1 be the binary random variables with value 1 with probability $\Pr[\text{click in } j, D_0]$ and $\Pr[\text{click in } j, D_1]$ respectively, for the j^{th} time unit and value 0 otherwise. These probabilities are:

$$\Pr[\text{click in } j, D_0] = p_j^{D_0} \approx \frac{\mu}{2}\Big(\nu(x_j+y_j)^2+(1-\nu)(x_j-y_j)^2+2\sqrt{\nu(1-\nu)}(x_j^2-y_j^2)\Big)+p_d \tag{3.11}$$

$$\Pr[\text{click in } j, D_1] = p_j^{D_1} \approx \frac{\mu}{2}\Big(\nu(x_j-y_j)^2+(1-\nu)(x_j+y_j)^2+2\sqrt{\nu(1-\nu)}(x_j^2-y_j^2)\Big)+p_d, \tag{3.12}$$

where p_d is the dark count probability for both detectors. We define $\Delta Z_j = Z_j^0 - Z_j^1$ as the difference in the clicks from D_0 and D_1 at j^{th} step. Note that ΔZ_j is a random variable that

takes values $\{-1, 0, 1\}$. We define $\Delta Z = \sum_j \Delta Z_j$ and we have

$$\mathbb{E}[\Delta Z] = \frac{\mu}{2}(2\nu - 1)(||x + y||^2 - ||x - y||^2). \tag{3.13}$$

Using Eq.(3.13) and the fact that $||x + y||^2 - ||x - y||^2 = 4(1 - ||x - y||^2/2)$, we obtain the Euclidean distance between the data sets x and y as

$$\tilde{E} = ||x - y||^2 = 2 - \frac{1}{\mu(2\nu - 1)}\mathbb{E}[\Delta Z]. \tag{3.14}$$

The error in the estimation of the Euclidean distance comes from two different sources: (i) the estimation of the mean value of ΔZ; and the (ii) error in parameter estimation of μ and ν, which in general depends on the experimental set-up but can be considered very small.

Let us deal with the first source of error, *i.e.*, the estimation of the mean value of ΔZ. Basically, we can bound the probability that ΔZ is far from its mean value, by using the Chernoff/Hoeffding bounds to get a statement of the form: $\Pr(|\Delta Z - \mathbb{E}[\Delta Z]| \geqslant \varepsilon \mathbb{E}[\Delta Z]) \leqslant \delta$. We prove this bound by the Theorem 4 given below.

Theorem 4. Let $X = \sum_j X_j$ be sum of n random variables with each variable X_j taking values $\{1, -1, 0\}$ with probability $\{p_j^{\{1\}}, p_j^{\{-1\}}, 1 - p_j^{\{1\}} - p_j^{\{-1\}}\}$ respectively. For any $a \in \mathbb{R}$,

$$Pr(X \geqslant a) \leqslant \left(\frac{2P^{\{1\}}}{a + \sqrt{a^2 + 4P^{\{1\}}P^{\{-1\}}}}\right)^a e^{-\left(P^{\{1\}} + P^{\{-1\}} - \sqrt{a^2 + 4P^{\{1\}}P^{\{-1\}}}\right)}, \tag{3.15}$$

where $P^{\{1\}} = \sum_j p_j^{\{1\}}$ and $P^{\{-1\}} = \sum_j p_j^{\{-1\}}$.

Proof: Markov's inequality on $X = \sum_j X_j$ gives us for any $s > 0$,

$$Pr(X \geqslant a) = Pr(e^{sX} \geqslant e^{sa}) \leqslant \frac{\mathbb{E}(e^{sX})}{e^{sa}}. \tag{3.16}$$

Note that $\mathbb{E}(e^{sX}) = \mathbb{E}(e^{s\sum_j X_j}) = \prod_j \mathbb{E}(e^{sX_j})$, where we used the property of independence of variables X_j. This allows us to prove the Chernoff bound by bounding each individual $\mathbb{E}(e^{sX_j})$.

Lemma 1. *Let Y be a random variable that takes value 1 with probability p_1, -1 with probability p_{-1} and 0 otherwise, then for all $s \in \mathbb{R}$,*

$$\mathbb{E}(e^{sY}) \leqslant e^{p_1(e^s - 1) + p_{-1}(e^{-s} - 1)}.$$

Proof: We have

$$\begin{aligned}
\mathbb{E}(e^{sY}) &= p_1.e^s + p_{-1}.e^{-s} + (1 - (p_1 + p_{-1})).1 \\
&= 1 + \Big(p_1(e^s - 1) + p_{-1}(e^{-s} - 1)\Big) \\
&\leqslant e^{p_1(e^s - 1) + p_{-1}(e^{-s} - 1)}.
\end{aligned}$$

Applying Lemma 1, we obtain

$$\mathbb{E}(e^{sX}) \leqslant \prod_j e^{p_j^{\{1\}}(e^s-1)+p_j^{\{-1\}}(e^{-s}-1)} = e^{\sum_j p_j^{\{1\}}(e^s-1)+p_j^{\{-1\}}(e^{-s}-1)}. \tag{3.17}$$

We denote $P^{\{1\}} = \sum_j p_j^{\{1\}}$ and $P^{\{-1\}} = \sum_j p_j^{\{-1\}}$, and by applying the result of Eq.(3.17) on Markov's inequality Eq.(4.8) we obtain,

$$Pr(X \geqslant a) \leqslant e^{P^{\{1\}}(e^s-1)+P^{\{-1\}}(e^{-s}-1)-sa}. \tag{3.18}$$

It can be easily verified that $s' = ln\Big(\frac{a+\sqrt{a^2+4P^{\{1\}}P^{\{-1\}}}}{2P^{\{1\}}}\Big)$ minimizes the upper bound in Eq.(refeq: 9). This concludes our proof:

$$Pr(X \geqslant a) \leqslant \left(\frac{2P^{\{1\}}}{a+\sqrt{a^2+4P^{\{1\}}P^{\{-1\}}}}\right)^a e^{-\Big(P^{\{1\}}+P^{\{-1\}}-\sqrt{a^2+4P^{\{1\}}P^{\{-1\}}}\Big)}. \tag{3.19}$$

To use the above theorem, let us define $\Lambda = P^{\{1\}} - P^{\{-1\}}$ and $a = \Lambda(1+\varepsilon)$, with $0 < \varepsilon < 1$. Using the inequality $\sqrt{(\Lambda(1+\varepsilon))^2+4P^{\{1\}}P^{\{-1\}}} \leqslant (P^{\{1\}}+P^{\{-1\}})+\Lambda\varepsilon$ we can relax Eq[3.19] further to:

$$Pr(X \geqslant \Lambda(1+\varepsilon)) \leqslant \left(\frac{e^{\varepsilon}}{\Big(1+\frac{\Lambda}{P^{\{1\}}}\varepsilon\Big)^{1+\varepsilon}}\right)^{\Lambda}. \tag{3.20}$$

Last, using the following inequalities, which are derived from Eqs[3.11,3.12,3.13], $\mathbb{E}[\Delta Z] \leqslant 2\mu(2\nu-1)$ and $\sum_j p_j^{D_0} \leqslant 2\mu\nu + (n-2\mu)p_d$ we have:

$$Pr(|\Delta Z - \mathbb{E}[\Delta Z]| \geqslant \varepsilon\mathbb{E}[\Delta Z]) \leqslant 2\left(\frac{e^{\varepsilon}}{\Big(1+\frac{2\nu-1}{\nu+\frac{n-2\mu}{2\mu}p_d}\varepsilon\Big)^{1+\varepsilon}}\right)^{2\mu(2\nu-1)} = \delta. \tag{3.21}$$

Eq.(3.21) highlights the contributions of n, μ, ν and p_d in the estimation of Euclidean distance, which can be estimated within any $0 < \delta < 1$ by controlling the mean photon number μ, since ν and p_d are fixed by the experimental setup used.

3.6.3 Coherent State Resource

The first two rows in Table 3.1 summarize the resources of the two protocols for ED. The performance achieved with the coherent state fingerprint protocol is the same as for Equality, *i.e.*, exponentially better in transmitted information but quadratically worse in communication time. We describe now a quantum protocol that can outperform any classical protocol in both resources.

	Comm. Time	Trans. Info.
Classical	$\Omega(\sqrt{n})$	$\Omega(\sqrt{n})$
Coherent	$\mathcal{O}(n)$	$\mathcal{O}(\mu \log_2 n)$
Multiple-channel Classical	$\Omega(\frac{\sqrt{n}}{\log_2 k})$	$\Omega(\frac{\sqrt{n}}{\log_2 k})$
Multiple-channel Coherent	$\frac{n}{k}$	$\mathcal{O}(\mu \log_2 n)$

Table 3.1: The order of the communication time and transmitted information for all classical and quantum protocols for Euclidean Distance described in this work.

3.7 Multiplexed SMP Model for Euclidean Distance

As mentioned in Table 3.1, the coherent state fingerprinting protocol allows for exponentially better savings w.r.t to classical analogue but is quadratically worse in the communication time. To address the issue of improving the communication time, we propose a new extended classical and quantum communication models to allow Alice and Bob to have multiple channels with the Referee. In particular, Alice and Bob can use k channels, where in every communication time unit, they can send in expectation at most one bit or one photon in total over all k channels. Of course, it may be possible that the Referee can process more than one bit or photon over the k channels but as we will explain below this does not change the nature of the advantage gained in the quantum case: the key point for our model is that for each bit or photon that can be processed by the Referee in one time unit, he and the sender can choose among k different channels, *i.e.*, the number of available channels exceeds the number of bits or photons that can be processed by the Referee by a factor of k.

In this model, in the classical case, the use of multiple channels reduces the communication by at most a $\log k$ factor, since we can simulate any multiple channel protocol with a single channel one with a $\log_2 k$ overhead: for every bit sent through one of the k channels, we send the same bit and the index of the channel in $\log k$ bits through the single channel.

In the quantum case, we can take a better advantage of the multiple channels and have a protocol with communication time of order n/k, while the transmitted information remains of order $\mathcal{O}(\log_2 n)$. The reason is that most of the pulses sent are empty of photons and hence we can use the multiple channels to send in parallel many pulses, without sending more than one photon in expectation per time unit. More precisely, Alice and Bob divide their n bit input into k sub-strings, each of length n/k. They create coherent state fingerprints for each of the k sub-strings and at each time unit they send k pulses through the channels, one from each of the k fingerprints. The Referee interferes the corresponding pulses as in the initial protocol, either by using k sets of BS and detectors, or by time ordering the pulses and using a single set of BS and detectors. The communication time is now reduced by a factor of k. By choosing k to be $\Omega(\sqrt{n})$, we can make both resources of the quantum protocol asymptotically smaller than the best classical protocol. The expected number of photons in each time unit is $\mu k/n$, which for large enough n and since k is asymptotically smaller than

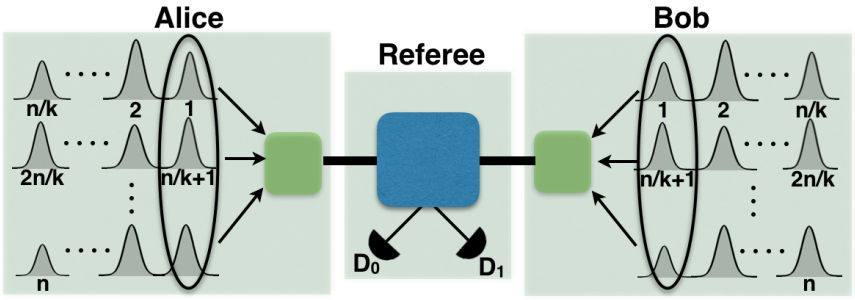

Figure 3.5: Our multiple-channel protocol. Alice and Bob create coherent state fingerprints for each of the k sub-strings and at each time unit they send the corresponding set of k pulses to the Referee. The Referee interferes all k pairs of pulses through a BS and processes the resulting information (at most 1 bit or photon per time unit). The protocol proceeds similarly for all n/k time units and the Referee estimates the ED.

n can be made < 1, hence satisfying the no more than one photon per time unit constraint.

As we mentioned above, if the Referee can treat more than one bit or photon per time unit, say t, then by assuming we have $k \times t$ available channels, both the classical and quantum protocols save an additional factor t and so the ratio of the classical and quantum communication time remains unchanged. Figure 3.5 illustrates our model for $t = 1$. In the next section, we describe a possible realization of our protocol using multiplexing techniques.

The last two rows of Table 3.1 compare the classical and quantum multiple-channel protocols for ED. This is the first example of a model and a task, for which in principle, a realistic quantum protocol is asymptotically more efficient both in the communication time and the transmitted information than any classical protocol.

3.7.1 OFDM Multiplexed Implementation

One way to implement the multiple-channel protocol proposed in our work is by using k physical channels. This would be the case for backbone communication networks, where nodes are connected via a large number of channels. Another way could be to employ all-optical orthogonal frequency division multiplexing (OFDM), an advanced classical multiplexing technique that has recently been adapted for performing high-rate quantum key distribution [BRS15]. Here, we propose an idea of using frequency multiplexing techniques to send multiple fingerprints in parallel along the k frequency channels in order to reduce the run time of the protocol.

Orthogonal Frequency Division Multiplexing: The most spectrally efficient method to multiplex different channels is to use OFDM (Orthogonal Frequency Division Multiplexing). This is a method of encoding digital data into multiple narrow band orthogonal frequency sub-carriers. The major advantage of the sub-carriers being orthogonal is that although the

side-bands from adjacent carriers overlap, they do not interfere with each other. Hence they can be demultiplexed easily because the carriers being sine/cosine wave, the two sinusoids of different frequencies cancel out over a period.

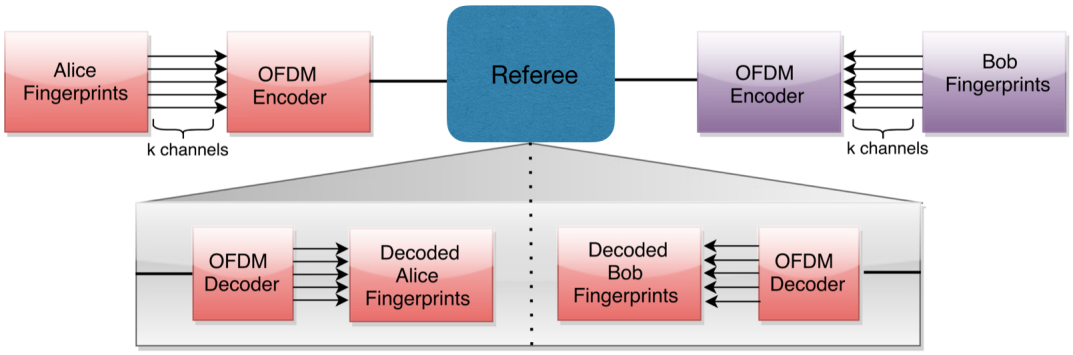

Figure 3.6: Illustration of fingerprints over an OFDM encoder and decoder. The fingerprints are multiplexed by an all optical OFDM encoder and the Referee uses the OFDM decoder to get back the fingerprints for both Alice and Bob.

Under this scheme, Alice and Bob create their coherent state fingerprints for each of the k sub-strings using k orthogonal frequency sub-carriers and pass it on to the OFDM encoder which multiplexes the sub-carriers. This is then sent to the Referee for demultiplexing. The decoding is usually carried out using the Fast Fourier Transform (FFT) to get back the individual fingerprints. These individual fingerprints are then subsequently interfered in the Referee's BS to estimate the Euclidean distance. Figure 3.5 gives a pictorial illustration of fingerprints being encoded with sub-carriers, multiplexed with OFDM encoder and finally demultiplexed by the referee to get back the fingerprints.

The OFDM sub-carriers that carry the fingerprints in parallel can either be generated from a bank of frequency offset locked laser diodes or alternatively, the output of a pulsed laser source such as a mode locked laser(MLL) is split into several paths using an optical splitter (such as an optical Inverse Fast Fourier Transform (IFFT) structure to generate orthogonal frequency sub-carriers.

Encoding

We consider the creation of OFDM sub-carriers using a MLL. Once the output of a MLL is split into k orthogonal sub-carriers, Alice and Bob encode their k sub-fingerprints sequentially into these k sub-carriers.

Each adjacent sub-carrier is separated by the frequency Δf and the pulse width of the encoded fingerprint signal is T = $1/\Delta f$. Now assume that at the time unit t_1, each sub-carrier j has a creation operator $E_{1j}^{\dagger}$ associated with it such that it carries the quantum state $E_{1j}^{\dagger}|0\rangle$.

The encoded OFDM fingerprint signal $\hat{E}_1(t)$ (subscript denotes time),

$$\hat{E}_1(t)\,|0\rangle = \sum_{j=1}^{k} E_{1j}^{\dagger} e^{i\omega_j t}, \quad 0 < t < T, \tag{3.22}$$

where the frequency of the i-th sub-carrier is denoted by $\omega_i = \omega_0 + 2\pi i \Delta f$.

At the first time unit t_1, Alice's coherent pulses for each of the k sub-strings are $\{|x_1\alpha\rangle_1$, $|x_{\frac{n}{k}+1}\alpha\rangle_1$,.. , $|x_{\frac{(k-1)n}{k}+1}\alpha\rangle_1\}$. They get encoded in the OFDM signal,

$$\hat{E}_1(t)\,|0\rangle = \sum_{j=1}^{k} e^{-\frac{|x_{\frac{(j-1)n}{k}+1}|^2\mu}{2}} e^{x_{\frac{(j-1)n}{k}+1}\alpha\hat{a}_j^{\dagger}} e^{i\omega_j t}\,|0\rangle \tag{3.23}$$

for $0 < t <$ T. Bob employs the same multiplexing technique to prepare his OFDM signal.

Once the Referee receives the OFDM signal, he proceeds to demultiplex them in order to obtain the individual fingerprint coherent pulses from Alice and Bob respectively and interfere them sequentially in his 50/50 BS. It takes $\frac{n}{k}$ time-units for the Referee to receive the entire fingerprint state from Alice and Bob.

Decoding

The decoding is performed when the Referee applies an Optical Discrete Fourier Transform (ODFT) on the input signal $\hat{E}_1(t)$ received in the first time unit t_1. The ODFT circuit effectively samples the input signal $\hat{E}_1(t)$, with pulse width T, into *k* time-equidistant signals $\hat{E}_1(t-(q-1)T_c)$, where the sub-channels $q \in \{1,..,k\}$ and, $\mathrm{T}_c = T/k$. The output state of the ODFT decoder is,

$$\hat{D}_1^q(t)\,|0\rangle = \frac{1}{k}\sum_{j=1}^{k} \hat{E}_1(t-(q-1)T_c) e^{i2\pi(j-1)q/k} \tag{3.24}$$

Using the orthogonality condition $\Delta f = \frac{1}{T}$ and from Eq.(3.23), the ODFT operator reduces to,

$$\hat{D}_1^q(t) = \sum_{l=1}^{k} e^{-\frac{|x_{\frac{(l-1)n}{k}+1}|^2\mu}{2}} e^{x_{\frac{(l-1)n}{k}+1}\alpha\hat{a}_j^{\dagger}} e^{i\omega_l t}\Big(\frac{1}{k}\sum_{j=1}^{k} e^{i2\pi(j-1)(q-l)/k}\Big) \tag{3.25}$$

Analysing Eq.(3.25), the term in the bracket is non-zero iff $q = l$, which thus extracts the coherent pulse $|x_{\frac{q-1}{k}+1}\alpha\rangle_1$. Similarly the fingerprint pulses in other time-steps are decoded via the ODFT decoder.

Passive Circuit Implementation for ODFT

There are two approaches (active and passive) to implement the ODFT decoder circuit. Here, inspired by Bahrani et al.[BRS15], we look at the passive circuit implementation of the

ODFT circuit. The major advantage in using passive circuit implementation is it does not involve any extra power consumption and is easier to implement compared to the active circuit.

The ODFT circuit to decode a k-ODFM signal requires an ordering of k-1 Mach Zhender Interferometer (MZI)'s. To illustrate the extraction mechanism using the MZI's we take an ODFT circuit for the number of sub-channels k = 4. The implementation of this circuit requires 3 MZIs.

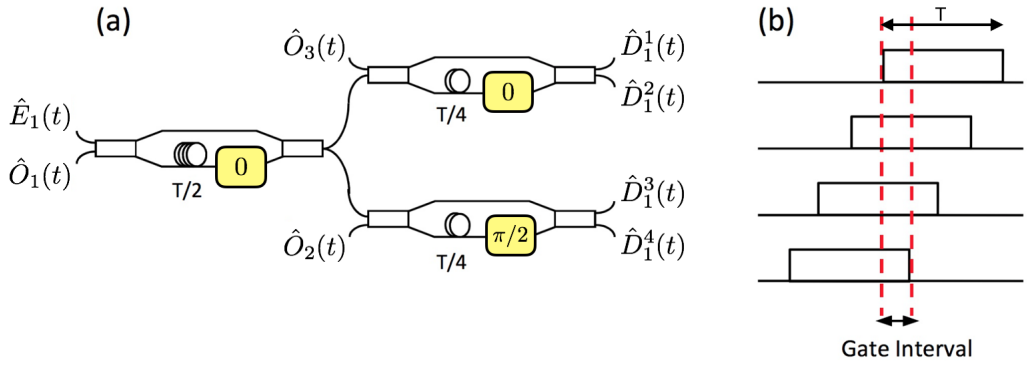

Figure 3.7: (a) Passive ODFT circuit implementation for k = 4 channels with delays and phase shifts. This ordering of MZIs directly does the serial-to-parallel conversion of the input signal and then does the FFT leading to the individual channel extraction. (b) shows the shifted replica of input ODFM signal for k = 4. The shift values are {0, T/4, T/2, 3T/4}.

Figure 3.7 shows the left MZI take as input the signal $\hat{E}_1$(t) and the vacuum operator $\hat{O}_1$(t) = $\sum_{j=1}^{k} \hat{O}_{1k} e^{i\omega_k t}$. The outputs from the left MZI has a delay of T/2 between them. They are respectively fed to right up and right bottom MZI. The right up MZI has the vacuum operator $\hat{O}_2$(t) = $\sum_{j=1}^{k} \hat{O}_{2k} e^{i\omega_k t}$ and the right bottom has $\hat{O}_3$(t) = $\sum_{j=1}^{k} \hat{O}_{3k} e^{i\omega_k t}$ as one of the inputs. The output operators $\{\hat{D}_1^1(t), \hat{D}_1^2(t), \hat{D}_1^3(t), \hat{D}_1^4(t)\}$ leads to the individual channel extraction.

The operation of a MZI can be written as a transformation matrix taking the inputs to outputs. For a frequency ω, the matrices are,
For the left MZI :

$$B_{\omega,1} = \frac{1}{2} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & e^{-i(\omega \frac{T}{2})} \end{bmatrix} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}, \tag{3.26}$$

for the right up MZI :

$$B_{\omega,1} = \frac{1}{2} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & e^{-i(\omega \frac{T}{4})} \end{bmatrix} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}, \tag{3.27}$$

for the right bottom MZI :

$$B_{\omega,1} = \frac{1}{2}\begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & ie^{-i(\omega\frac{T}{4})} \end{bmatrix}\begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}, \tag{3.28}$$

Now, by applying these transformations to the OFDM signal for the sub-carrier q at time unit t_1, we obtain,

$$\begin{pmatrix} \hat{E}^{\dagger\prime}_{1q}(t) \\ \hat{O}'_q(t) \end{pmatrix} = B_{\omega_q,1}\begin{pmatrix} \hat{E}^{\dagger}_{1q}(t) \\ \hat{O}_{1q}(t) \end{pmatrix} \tag{3.29}$$

$$\begin{pmatrix} \hat{D}^{1,q}_1(t) \\ \hat{D}^{2,q}_1(t) \end{pmatrix} = B_{\omega_q,2}\begin{pmatrix} \hat{E}^{\dagger\prime}_{1q}(t) \\ \hat{O}_{2q}(t) \end{pmatrix} \tag{3.30}$$

$$\begin{pmatrix} \hat{D}^{3,q}_1(t) \\ \hat{D}^{4,q}_1(t) \end{pmatrix} = B_{\omega_q,1}\begin{pmatrix} \hat{O}'_q(t) \\ \hat{O}_{3q}(t) \end{pmatrix} \tag{3.31}$$

The output decoder operator for channel q can then be obtained by taking the superposition of different frequencies.

$$\hat{D}^q_1(t) = \sum_{j=1}^{4} \hat{D}^{j,q}_1(t) \tag{3.32}$$

The output operators will have contribution from vacuum operators $\hat{O}_1$, $\hat{O}_2$ and $\hat{O}_3$, but they can be collected together and ignored in the final result. Similarly, the generalised construction for the passive decoding circuit can be done for any arbitrary k value.

3.8 Experimental Implementation

In this section we propose a novel proof-of-principle experimental setup to estimate the Euclidean distance problem using coherent state fingerprints and demonstrate the quantum advantage in the transmitted information resource. This implementation is done using the home made set-up as shown in Figure 3.8. This proposal is in sharp contrast with the previous proof-of-principle experiments to solve the Equality problem using coherent state fingerprints [XAW$^+$15, GXY$^+$16]. The previous set-ups relied on sagnac loop based experiments to cancel the path difference between Alice and Bob and to make sure that the fingerprints from the two parties arrive at the Referee's beam splitter (BS) at the same time. Under the sagnac loop based experiments, Alice's modulated pulses traverses through Bob's paths and vice-versa. This opens up the possibility of communication between the two parties during the protocol run which is strictly not allowed in the model.

Our proposal does not have this possibility of intercommunication between the two parties. We ensure this by separating the paths of Alice and Bob and carefully adjusting their path lengths to ensure that the pulses arrive at the Referee's BS simultaneously. This amounts to having high visibility (ν) factor in the experiments. The first row of Table 3.2 shows the

experimental imperfection values obtained during the experiment. We see that we are able to reach pretty high ν values in our experiment.

3.8.1 Experimental Methods

Our experimental set-up is divided into two loops. *Front loop* and the *Phase correction loop*.

Front loop: The coherent state for Alice and Bob is produced by the ultra low line-width ($\sim$10kHz) continuous wave laser source, Laser1 (Pure Photonics $\sim$ 1563nm). This is then chopped into time-bin coherent pulses by the amplitude modulator (AM) that is modulated using a function generator to create pulses with the repetition rate of 1MHz and duty cycle of 50%.The variable optical attenuator (VOA) is then used to bring the mean photon number in the pulses to the desired level. The isolator (IS) after the VOA is introduced to ensure that the laser power is transmitted only in the forward direction and pulses coming from the Laser2 are blocked, thus ensuring no harm to Laser 1. We use the balanced 50/50 beam splitter(BS1) to monitor the power of the pulses. The second 50:50 BS2 splits the two paths, the upper path corresponding to Alice, and the lower corresponding to Bob. We introduce a delay line (DL) to perfectly fine tune the path lengths of Alice and Bob. This ensures that the pulses from Alice and Bob arrive simultaneously in the 50/50 BS3. In our setting, Bob's path is longer than Alice's path by 17.1mm (fiber length). We compensate this path difference with the DL. Alice does the phase (PM) and amplitude modulation (AM) of her coherent pulses sequentially according to the input string $x \in \mathcal{R}^n$. This voltage corresponding to the input is provided to the modulators via the data acquisition card (DAQ) in our set-up. Bob performs the similar modulation according to her input bit $y \in \mathcal{R}^n$. The pulses from Alice and Bob interact sequentially in the Referee' BS3. Normally, all the pulses should interact according to Eq.(3.10), but in reality there is a phase drift over time in Alice's and Bob's pulses. This phase drift is due to the laser pulses traversing in the optical fiber. Usually under stable temperature conditions, this phase drift is slow and can be tracked and corrected effectively. To make sure we cancel the effect of phase drift, we introduce the phase correction loop to monitor and correct the phase drift in the pulses.

The path leading to the single photon detector (D_0) has the circulator C, which allows the transmission only in anticlockwise direction. The length of the circulator is $\sim$ 2m. We introduce a fiber length of 2m in the lower path to maintain the same arrival times for the pulses in the detectors D_0 and D_1. We introduce the optical filters(OF) just before the detection, to allow only the pulses from the Laser1 ($\lambda = 1563$nm) to pass through and blocks any contribution from Laser2 in the photon counts. Finally for the detection, we use the two high efficiency, low dark count pulsed ID201 (manufactured by ID Quantique) detectors. The clicks are recorded in the DAQ (manufactured by National Instruments).

Phase correction Loop: We introduce the second continuous wave laser source, Laser2 (Pure photonics $\sim$ 1527nm) to monitor the phase drift in Alice and Bob's paths. The laser source is modulated with the AM to produce laser pulses at 1MHz repetition rate and duty

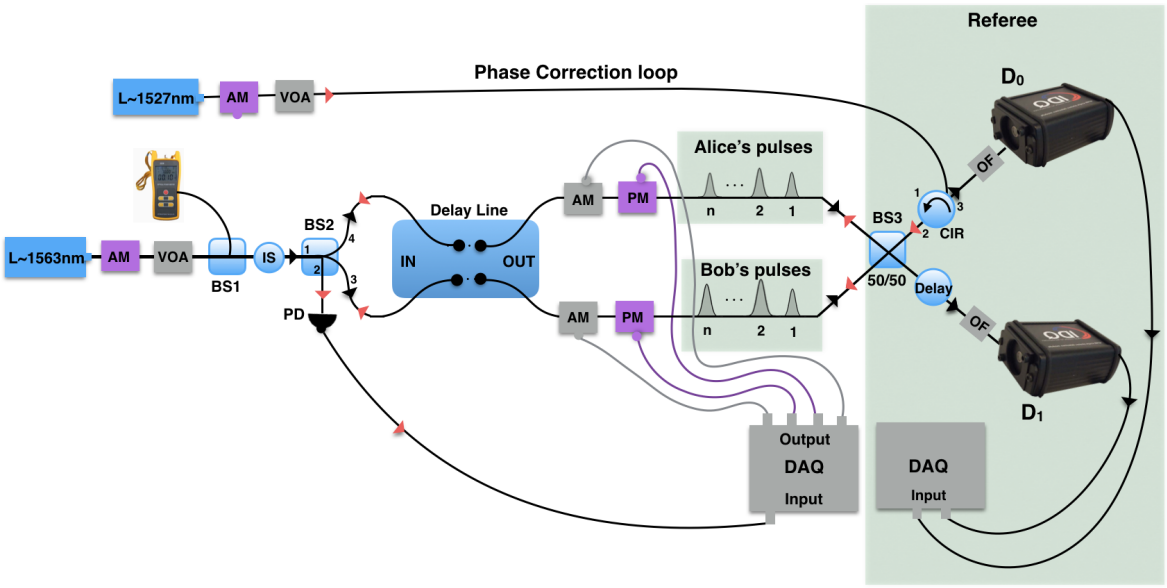

Figure 3.8: Experimental set-up for estimating the Euclidean distance using coherent state fingerprints. The set-up has a Front loop, operated by continuous wave laser source, Laser1, at $\lambda = 1563$nm, while the Phase correction loop is operated by the laser source, Laser2, at $\lambda = 1527$nm. In the Front loop, the amplitude modulator AM creates coherent pulses, which are brought to the desired mean photon level using the variable optical attenuator (VOA). The Isolator (IS) ensures that no power of the pulses from Laser2 reaches Laser1, thus preventing the Laser1 from any harm. One output arm of the 50/50 beam splitter (BS1) is given to power meter to monitor the power, and hence the average photons in the pulse. BS2 splits the two paths, the upper path for Alice and lower path for Bob. We introduce a delay line (DL) in the paths to perfectly fine tune the paths lengths of Alice and Bob to ensure that they arrive at the Referee's BS3 simultaneously. Alice and Bob use their AM and PM to modulate their pulses sequentially according to the input strings $x, y \in \mathcal{R}^n$. We use the data acquisition card (DAQ) to provide the voltage (according to the input) to the AM and PM. After interaction of the pulses in BS3, the path leading to single photon detector D_0, has a circulator (C) which directs the Laser1 pulses into the detector. An optical filter (OF) only lets pulses from Laser1 to pass through and blocks the Laser2 pulses. We use the Phase correction loop to monitor and correct the phase drift over time in Alice's and Bob's paths. The pulses from Laser2 enter the set-up from an arm of C, passes through BS3 to split into Alice and Bob's paths, and interfere in BS2. We monitor the phase drift in the photo diode (PS) connected to the output arm of BS2.

cycle of 50%. The pulses then enter set-up via one arm of C. They are split into Alice's and Bob's paths via the BS3. Upon interacting in BS2, the output of the phase correction pulses are then collected into the photo-diode PD which gives the information of the phase drift in the two paths. The phase drift is then analysed and corrected using the following

technique. Before describing the technique, we note that the phase drift is not corrected for each and every pulse. This is because our experiment runs at a high speed of 1Mhz and, it is realistically not feasible to for the computer to process the phase information and correct it for each and every pulse. Second, the phase drift is slow due the high stability of the laser and the set-up, hence it is not required to correct this drift for each pulse. We rather correct an average phase drift over a number of pulses. We make blocks of pulses and track the average the phase drift in one block to use it to correct the drift for the next block. This block construction is illustrated in Figure 4.8. We choose a block size of 8192 pulses. The first 7680 pulses are used for protocol run. The second segment of block $\text{Alice}_{\text{track}}$, tracks the phase drift in the path corresponding to Alice's PM. This is done by giving a ramp voltage in Alice's PM from -5V to +5V, and 0V in Bob's PM across 256 pulses. The response of the linear ramp voltage across a phase modulator is a cosine function $A\cos(\omega t + \phi)$ which is tracked in the PD. While modelling the expected response with the actual response, we get the information of phase and phase drift upto a certain error. Let V_{bias} be the voltage corresponding to the phase drift, then the voltage across Alice's PM for the next block gets added by factor V_{bias} i.e. $V_{PM} = V_{x_i} + V_{bias}$. We similarly track and correct the phase drift in Bob's PM over the last 256 pulses of the block, $\text{Bob}_{\text{track}}$.

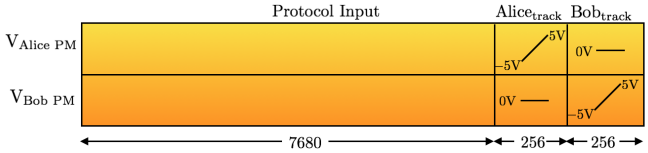

Figure 3.9: Block illustration for analysing the phase drift in pulses. Phase tracking is done once for every block of 8192 pulses. The first 7680 pulses are used for protocol encoding. The second part of the block $\text{Alice}_{\text{track}}$, tracks the phase drift in Alice's PM. For this we give a ramp voltage from -5V to +5V in Alice's PM and 0V in Bob's PM. The third part of the block $\text{Bob}_{\text{track}}$, tracks Bob's PM by giving a ramp voltage from -5V to +5V in Bob's PM and 0V to Alice's PM.

3.8.2 Experimental Analysis

We perform a proof-of-principle experiment using coherent state fingerprints over a standard telecom wavelength of $\lambda = 1563$nm at 1Mhz.

Table 3.2: Experimental & Simulated parameters

	$\eta_{channel}$	η_{det}	ν	p_{dark}
Exp.	3.5dB	15%	$(98.8 \pm 0.3)\%$	$(2.1 \pm 0.2) * 10^{-5}$
Sim.	3.5dB	90%	$(98.8 \pm 0.3)\%$	$(1 \pm 0.1) * 10^{-8}$

The overall channel loss in the channel i.e. the loss before Alice and Bob apply their phase modulator (PM) to the input of detectors D_0 and D_1 is 3.5dB. This parameter is shown

in Table 3.2. Further, our detectors operate at 15% efficiency. The combined effect of channel loss and limited detector efficiency results in transmission of higher mean photon number μ in the pulses to achieve the desired error rate δ.

The limited visibility (ν) in the set-up, accounts for the mismatch in the interference of Alice and Bob's pulses. This is maximized by reducing the optical path length difference between the two parties using the delay line (DL). This adjustment was done by first sending an input string 0^n to both Alice and Bob and recording the clicks obtained in two detectors and then sending 0^n and 1^n to Alice and Bob respectively and observing the clicks.

We further carefully inspected the dark counts in our detectors when there was no signal from the lasers. Our detectors are set at the dead time of 10μs. This means that after the detector records a click, there is no recording of the clicks for the next 10 pulses. This is not an issue for us as the probability of a click across 10 pulses $\ll$ probability of the click across rest of the pulses in the input. The reason for this is the extremely low photon number per pulse.

With the experimental imperfection values obtained in the testing phase, we calculate the optimal average photon number μ required for each input size, n, that estimates the Euclidean distance problem. Figure 3.10 includes the plot of observed experimental transmitted information points for these input sizes $[10^9, 2 \times 10^9, 3 \times 10^9, 4 \times 10^9, 5 \times 10^9]$

3.9 Resource Comparison with Classical Protocol $\&$ Lower Bound

We compared the resources for the optimal classical protocol and classical lower bound, with the coherent state protocol to compute the Euclidean distance problem within $\varepsilon = 0.2$ with error probability $\delta \leqslant 10^{-6}$. In Figure 3.10 we plot the transmitted information and communication time resource as a function of input size n for the multiple-channel protocol with $k = O(\sqrt{n})$, and compare its performance with the classical lower bound and with the best known classical protocol.

3.9.1 Comparison of Transmitted Information Resource

We have already looked at the transmitted information resource in non-multiplexed scenario, by computing the classical lower bound in Section 3.4.2, and the optimal classical protocol in Section 3.4.3. In the multiplexed scenario, the classical transmitted information resource gets reduced by a factor of $\log k$. This has been argued in the Section 3.7 and we show this resource in Table 3.1.

The coherent state protocol which sends n coherent pulses with a total average photon number μ, has the transmitted information resource of $\mu \log n$. The optimal value of μ

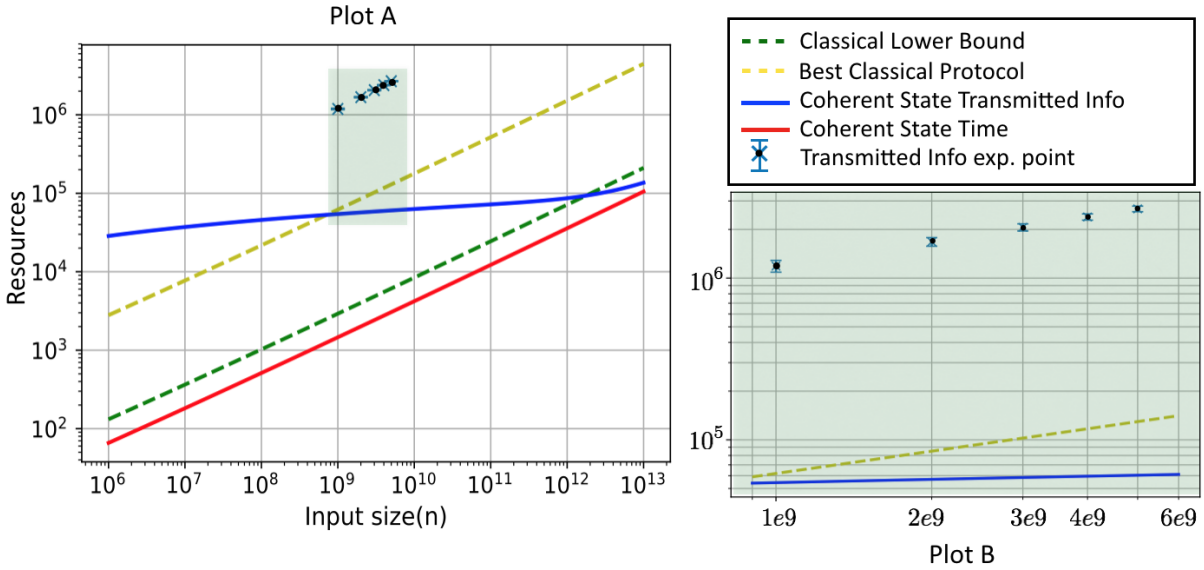

Figure 3.10: Log-log plot of the transmitted information and time resources vs input size (n) for solving ED within $\varepsilon = 0.2$ with error $\delta \leqslant 10^{-6}$. In Plot A, we compare the simulated classical lower bound, the best known classical protocol, and our multiple-channel coherent state Euclidean distance protocol. The simulation of coherent state transmitted information resource (blue line) is done with Sim. values of Table 3.2. With these values, the minimum n to outperform best classical protocol is $n_{min} = 6.74 \times 10^9$, while to outperform the classical lower bound is $n_{min} = 1.67 \times 10^{12}$. The optimized mean photon number for the coherent states is $\mu = 1129$ The red line shows the performance of multiplexed coherent state fingerprint in time resource. The number of multiplexed channels scales as $k = O(\sqrt{n})$. Plot B shows the experimental points for input sizes $[10^9, 2 \times 10^9, 3 \times 10^9, 4 \times 10^9, 5 \times 10^9]$. These points have been plotted with our current available detectors parameters as listed in the Exp. row of Table 3.2.

depends on the how well we want to estimate the Euclidean distance, δ, and the success probability of the estimation, ε. It also depends on the experimental parameters, and is especially sensitive to the two experimental parameters, η and p_{dark}. The current detectors used in the experiment have the η, p_{dark} values as mentioned in the Exp. row of Table 3.1. With these parameters, we run the experiment for the input sizes $[10^9, 2 \times 10^9, 3 \times 10^9, 4 \times 10^9, 5 \times 10^9]$, by providing the optimal μ that estimates the Euclidean distance within desired ε, δ. The μ values provided for these input sizes were $[35787 \pm 100, 49082 \pm 100, 59301 \pm 100, 67923 \pm 100, 75520 \pm 100]$. This was achieved by attenuating the laser pulses using the VOA.

As is evident in Plot B of Figure 3.10, the current set of detectors are far away from beating even the optimal classical protocol. Rather, in Plot A of Figure 3.10, we plot the coherent state transmitted information resource (blue line) with the best available super-

conducting detectors [XAW$^+$15]. Their values are listed under Table 3.2 (Sim. row). With these detectors, the coherent state protocol beats the optimal classical protocol from input size $n_{min} = 6.74 \times 10^9$, and the classical lower bound for $n_{min} = 1.67 \times 10^{12}$. Thus, the bottleneck in further reducing the coherent state transmitted information resource are efficient detectors and currently there has been a lot of progress made in this front by manufacturers including, PhotonSpot [SJZ$^+$18] , SingleQuantum, IDQuantique.

3.9.2 Comparison of Time Resource

The classical communication time in the multiplexed model is the same as transmitted information resource. This is because, we define the time unit as the time taken by Alice and Bob to send 1 bit to the Referee. In the coherent non-multiplexed setting, the total communication time is n, since Alice and Bob are sending n coherent pulses to the Referee. This communication time is reduced by a factor of k, upon using k-multiplexed channels. The communication time can be made less that the classical lower bound as long as $k > k_{crit}$, where k_{crit} makes the quantum protocol time equal to the time in the classical lower bound and is of the order of $\mathcal{O}(\sqrt{n})$. We plot this in Figure 3.10 (red line).

We first see that if we are only interested in the communication time, which is often the case, then our protocol outperforms the classical limit even for small n and by consequence for small number of channels which can be feasible in practice. Moreover for large n, our protocol outperforms the classical limit for both resources. For current parameters, the number of channels needed is about 10^5, which may not be realistic. By improving the experimental parameters one may decrease this number.

3.10 Conclusion

We presented a new multiplexed SMP scheme to solve the Euclidean distance problem within an additive constant, and with a desired success probability. For this, we demonstrated how the quantum protocol based on highly attenuated coherent states, linear optics elements, and single photon threshold detectors can achieve quantum advantage compared to the classical analogue.

A noteworthy feature of the Euclidean Distance protocol studied in our work is that Alice and Bob do not need a memory to store their inputs and they do not perform global operations on them. In other words, this protocol works also in the *streaming* scenario, where Alice and Bob receive their inputs one bit at a time [NAS99]. We note that this is not the case neither for the Equality protocol, where an error correcting code needs to be applied to the entire input string, nor for the qubit protocol where the fingerprint is encoded in a superposition of $\log n$ qubits. It will be interesting to further explore this scenario for efficient quantum communications. More generally, expanding the family of distributed tasks in the coherent

state communication model studied in this work is important for demonstrating in practice quantum superiority in a network setting.

4 Sampling Matching Communication Problem

4.1 Introduction

Communication complexity, as an ideal resource model for proving quantum superiority, has been studied in the previous chapter. It involves two or more parties who each receive an input and their goal to is to jointly perform a distributed task with minimum possible resources. A lot of previous works towards this end have proved that quantum resources lead to exponential asymptotic savings compared to the classical resources [BCWDW01, BCW98, Raz99, BYJK04, GKK$^+$07, Gav16, RK11]. However these protocols have been difficult to demonstrate experimentally until few years back primarily because these quantum protocols necessitate creating and sustaining highly entangled states (dimension ~ 30) with phase and amplitude encoding, which are out of reach of the current photonic technologies. With the recent works of Arrazola and Lütkenhaus [AL14a] on an alternative encoding scheme for quantum communication protocols using coherent states and linear optics, there has been a significant progress made towards demonstrating these protocols with the current photonic technologies.

In this chapter, we study two different tasks in single-round one way communication complexity model. This model consists of two parties, let's say Alice and Bob. Only Alice is allowed to send a single round communication message to Bob, who then conditioned on the message, outputs a solution to the given communication task. We start by considering the already known Hidden Matching problem introduced by Bar-Yossef et.al [BYJK04]. This task has been known to have an exponential reduction in quantum transmitted information resource, compared to the classical analogue. For this communication task, we propose the coherent state fingerprinting protocol under realistic experimental settings, and show that the coherent state protocol also demonstrates an exponential reduction in communication resources compared to the classical analogue. Our simulation result comparing the classical and coherent state resources shows the reduction in the resource for coherent protocol compared to the classical from input sizes as low as 2927.

In the second half, we define a new communication task in one-way communication complexity model and for the first time, experimentally demonstrate the quantum superiority in this model. Motivated from the Hidden Matching problem, we define this new problem as the Sampling Matching problem.

Sampling Matching is a one way communication problem which has been has been inspired from the works on round-robin differential phase-shift (RRDPS) quantum key distribution [LGQW17, ZYCM15] where passive-decoy techniques have been used to tolerate the experimental noise and side channel attacks and also enhance the key generation rate. For this communication problem, we show an exponential reduction in quantum transmitted information resources compared to the classical analogue. More importantly, the implementation of the Sampling Matching protocol with coherent states can be achieved with current state-of-the-art technology as we show with our experimental demonstration.

Although a problem in one-way complexity, the Hidden Matching problem, has already been well known, we justify the need to introduce the Sampling Matching communication problem, because the major advantage with Sampling Matching implementation using coherent states is that the number of linear optical components to implement this problem is constant, independent of the input size. This is a huge advantage, in contrary to the Hidden Matching task, where the number of such components increases with the input size, and thus it becomes increasingly difficult to implement those circuits in practice.

We further present a proof-of principle implementation of our Sampling Matching problem for different input sizes that beats the best known classical protocol in terms of the transmitted information resource. The implementation was done with our in-house set-up using highly stable (ultra low line-width) continuous laser source, linear optics component, and high efficiency, low dark count single photon detectors. Our major result is that for the input sizes as low as 3000, we demonstrate a quantum advantage. Further, if we allow for post-selection, then we beat the best classical protocol for input sizes as low as 2000.

4.2 Hidden Matching Problem

We start by describing the Hidden Matching problem as defined in [BYJK04], and show how to translate the qubit protocol to solve the Hidden Matching into the coherent state protocol framework. We will also describe the linear optics circuit necessary for implementing this protocol, which will showcase the need for defining our novel problem, the Sampling Matching, which will drastically reduce the necessary resources for demonstrating quantum superiority in the model of one-way communication complexity.

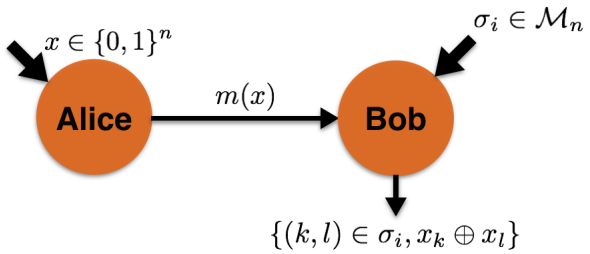

Figure 4.1: Hidden matching problem. Alice gets an input $x \in \{0,1\}^n$ while Bob gets a matching σ_i uniformly randomly from the set $\mathcal{M}_n \in \{\sigma_1, ..\sigma_{n-1}\}$. The objective of the problem is for Bob to output the correct parity value, b, for any tuple $\langle (k,l) \in \sigma_i, b = x_k \oplus x_l \rangle$. Only one-way communication, Alice to Bob, is allowed.

In this section we review some known results for Hidden Matching (HM) [BYJK04, AL14a]. This is a one-way communication complexity task involving two players Alice and Bob. It is described as follows. For any positive even integer n, Alice receives as input a string $x \in \{0,1\}^n$ while Bob receives a $n/2$ tuples matching σ_i uniformly randomly from $\mathcal{M}_n \in \{\sigma_1, .., \sigma_{n-1}\}$. Here $\mathcal{M}_n$ is the set of $n-1$ perfect disjoint matchings on n nodes. The objective of the problem is for Bob to output any one of the $n/2$ possible parity values $x_k \oplus x_l$ for a pair (k,l) that belongs to the matching σ_i with minimum communication resources. Here x_k, x_l are k^{th} and l^{th} bit of x respectively. We analyse this problem in the randomized setting where Bob has to output the tuple parity value with high enough success probability. This problem further imposes the restriction of communication only from Alice to Bob, otherwise it is easy to see that the task can be done with logarithmic communication, since Bob can send to Alice the tuple indices k, l of the matching σ_i she receives.

4.3 Optimal Classical Protocol & Lower Bound

For this problem, the randomized classical lower bound of $\Omega(\sqrt{n})$ was shown by Bar-Yossef et al [BYJK04] and Buhrman et al [BRSDW11]. In high level, Alice's message should allow Bob to output the parity of an edge from each one of the possible matchings, in other words

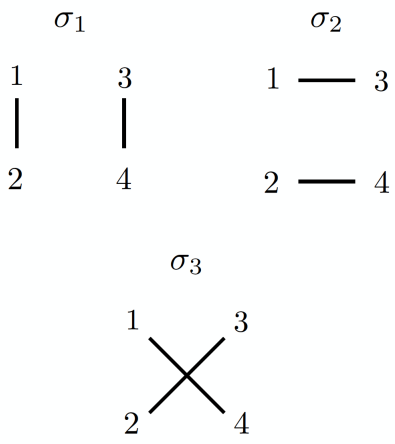

Figure 4.2: An illustration of a perfect disjoint matching set for size $n = 4$: $\mathcal{M}_4 : \Big[\sigma_1 : \{(1,2),(3,4)\}; \sigma_2 : \{(1,3),(2,4)\}; \sigma_3 : \{(1,4),(2,3\} \Big]$

for $\mathcal{O}(n)$ different edges. No matter which edges one picks, they will always contain at least $\Omega(\sqrt{n})$ different bits of the input x, and hence Alice must send at least $\Omega(\sqrt{n})$ bits of information and hence communication. The proof structure for computing lower bound in [BRSDW11] is as follows: if Alice's message to Bob is small, let's say c bit, then the set of inputs $x \in \{0,1\}^n$ for which Alice sends a particular message m, will be large (typically of the order of 2^{n-c}). This would mean that Bob will have very little knowledge of most of the bits of x. Using the KKL inequality [KKL88], this implies that Bob would not be able to correctly answer the parity $x_i \oplus x_j$ for most of the $\binom{n}{2}$ tuples of the form (i,j). Even though Bob has some relaxation in a sense that he can output the parity outcome of any one of the $n/2$ tuples of σ_i, still it turns out that on average it is hard for him to output the correct parity outcome. Using this idea, and the KKL inequality, the classical lower bound to succeed with an error probability p_{error} is,

$$c \geqslant \frac{\log_2 e}{e}(\frac{1}{2} - p_{error})\sqrt{n-1} \tag{4.1}$$

Bar-Yossef et al. also proved that this bound is tight by describing a randomized one way protocol using birthday paradox argument to show that only $\mathcal{O}(\sqrt{n})$ classical bits is sufficient to implement the problem. The proof structure is as follows: Let us assume that Bob's matching set $\mathcal{M}_n$ is restricted to be one of the $n-1$ disjoint matchings. Since Alice has no information about which matching Bob has received, to maximize the winning condition she encodes her message to contain the parity information of at least one pair from each matching with high probability. Suppose she does this by sending c random bits of the input x or equivalently $c(c-1)/2$ tuples to Bob. Each perfect disjoint matching σ_i that Bob would receive has $n/2$ tuples. Thus the matching set $\mathcal{M}_n$ has in total $n(n-1)/2$ distinct tuples. The probability that none of the tuples that Alice sends to Bob is in the matching σ_i received

by Bob is,

$$p_{error} = \left(1 - \frac{1}{n-1}\right)^{c(c-1)/2} \approx \exp(-c^2/2n) \tag{4.2}$$

For $p_{error} \leqslant 0.1$, the communication c is

$$c \geqslant \sqrt{2\log_e 10}\sqrt{n} \tag{4.3}$$

This is plotted in the Figure 4.4.

4.4 Quantum Protocol

Using a simple quantum protocol, the above task can be solved by transmitting exponentially fewer number of qubits. Alice encodes her input $x \in \{0,1\}^n$ into the following superposition:

$$|x\rangle = \frac{1}{\sqrt{n}} \sum_{k=1}^{n} (-1)^{x_k} |k\rangle \,, \tag{4.4}$$

where x_k is the k-th bit of the string x. She then sends it to Bob. For any matching $\sigma_i \in \mathcal{M}_n$ that Bob has as input, there exists a measurement by Bob which allows him to give the correct answer with certainty. To do so, he just measures the quantum state in the basis $\{\frac{1}{\sqrt{2}}(|k\rangle \pm |l\rangle\}$, $\forall (k,l) \in \sigma_i$. The outcome $\frac{1}{\sqrt{2}}(|k\rangle + |l\rangle)$ occurs iff $x_k \oplus x_l = 0$ whereas $\frac{1}{\sqrt{2}}(|k\rangle - |l\rangle)$ occurs iff $x_i \oplus x_j = 1$. Thus Bob gets the parity result of one of the tuples $(k,l) \in \sigma_i$ with certainty.

4.4.1 Quantum Resource

This protocol uses only $\log_2 n$ qubits, and hence both the communication and the transmitted information is exponentially better than the classical counterpart.

4.5 Coherent State Protocol

The physical implementation of the qubit protocol is extremely challenging due to the high dimensionality of superposition states, thus requiring the preparation of high entangled states sustainable over the entire run of the protocol. Here, we instead propose an alternative quantum protocol implementation using coherent states. This is based on the coherent state mapping proposed by Arrazola et al [AL14b]. Under this scheme, Alice prepares the message $|\alpha_x\rangle$, by applying the displacement operator $\hat{D}_x(\alpha) = \exp(\alpha \hat{a}_x^\dagger - \alpha^* \hat{a}_x)$ to the vacuum state,

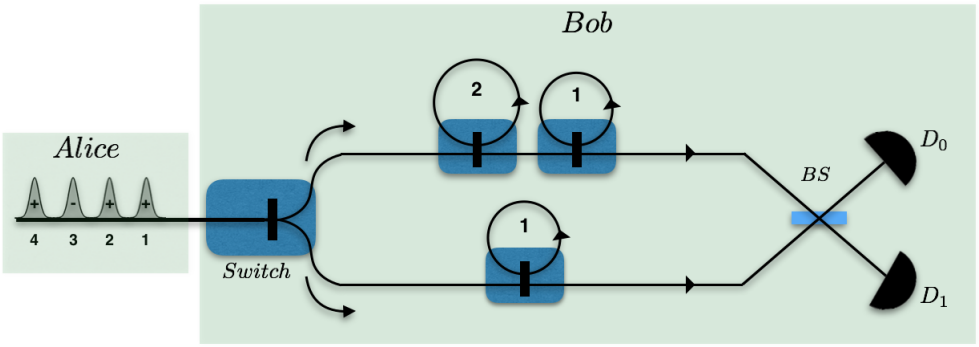

Figure 4.3: Figure depicting the circuit implementation of the Hidden Matching problem using coherent states, for matchings from the set in Figure 5.1. Alice encodes her input $x \in \{0,1\}^4$ as a train of four pulses and sends it Bob. Depending on his input matching $\sigma_i \in \mathcal{M}_4$, Bob uses an active switch to send the coherent state in the upper or the lower arm. The upper and lower arms have switch+delay loop construction with the number denoting the number of time steps the loop will delay the coherent pulse. The number of active elements needed to implement the protocol is 4. For a general input size n, the number of active elements to implement the protocol grows as $O(\log n)$.

where $\hat{a}_x = \sum_{k=1}^{n} x_k \hat{a}_k$ is the annihilation operator of the coherent state mode, and $\hat{a}_k$ is the photon annihilation operator of the k^{th} time mode. Hence,

$$|\alpha_x\rangle = \hat{D}_x(\alpha)\,|0\rangle = \bigotimes_{k=1}^{n} |(-1)^{x_k}\frac{\alpha}{\sqrt{n}}\rangle_k \,, \tag{4.5}$$

where $|(-1)^{x_k}\frac{\alpha}{\sqrt{n}}\rangle_k$ is a coherent state with amplitude $\frac{\alpha}{\sqrt{n}}$ occupying the k^{th} time mode. Here $|\alpha_x\rangle$ can be thought of as a train of n time-bin coherent pulses with the total mean photon number being $\mu = \sum_k |\frac{\alpha}{\sqrt{n}}|^2 = |\alpha|^2$, which is independent of the input size.
Upon receiving the state $|\alpha_x\rangle$ from Alice, Bob rearranges the input modes of $|\alpha_x\rangle$ according to the tuples $(k,l) \in \sigma_i$ using a number of active switches and delay lines as shown in Figure 4.3, interferes all the tuples in σ_i sequentially in a balanced beam splitter and observes the clicks in detectors D_0 and D_1.

4.5.1 Error Analysis under perfect Experiment settings

In the ideal setting the incoming modes in the beam splitter for tuples (k,l) are

$$|(-1)^{x_k}\frac{\alpha}{\sqrt{n}}\rangle_k \otimes |(-1)^{x_l}\frac{\alpha}{\sqrt{n}}\rangle_l \,, \tag{4.6}$$

the output modes are

$$|\frac{1+(-1)^{x_k \oplus x_l}}{\sqrt{2}}\frac{\alpha}{\sqrt{n}}\rangle_{D_0} \otimes |\frac{1-(-1)^{x_k \oplus x_l}}{\sqrt{2}}\frac{\alpha}{\sqrt{n}}\rangle_{D_1} \,, \tag{4.7}$$

From Eq [4.7] we see that D_0 clicks only if $x_k \oplus x_l = 0$ and D_1 clicks otherwise. Now if Bob gets clicks across multiple time bins, then he randomly chooses one of the click values to output the tuple $\langle (k,l) \in \sigma_i, b = x_k \oplus x_l \rangle$. The only way in which he can output an incorrect parity value is if he does not observe any click during the entire run of the protocol, which happens with $p_0 = \exp(-|\alpha|^2)$. Thus his error probability is $p_{error} = \frac{1}{2}p_0$.

4.5.2 Error Analysis under Experiment Imperfection

The coherent state implementation has three main sources of error. (i) The transmission loss is characterized by parameter $0 \leqslant \eta \leqslant 1$ which changes the state α to $\sqrt{\eta}\alpha$. The probability of obtaining a click in the detectors reduces by a factor η. (ii) The limited set-up visibility $0 \leqslant \nu \leqslant 1$, and (iii) the dark count in the detectors characterized by probability p_{dark}. In the experiments, our $\alpha \approx 1$ and while the input size is not huge, p_{dark} $(\approx 10^{-6})$ becomes insignificant compared to the click probability p_c $(\approx 1/n)$. Thus we do not consider the effect of dark counts in our analysis. Considering experimental imperfections (η, ν), the incoming state becomes,

$$|(-1)^{x_k}\sqrt{\frac{\eta}{n}}\alpha\rangle_k \otimes |(-1)^{x_l}\sqrt{\frac{\eta}{n}}\alpha\rangle_l \tag{4.8}$$

and the output state is,

$$\begin{aligned} &|\Big(\frac{(1+(-1)^{x_k\oplus x_l})}{\sqrt{2}}\sqrt{\nu} + \frac{(1-(-1)^{x_k\oplus x_l})}{\sqrt{2}}\sqrt{1-\nu}\Big)\sqrt{\frac{\eta}{n}}\alpha\rangle_{D_0} \otimes \\ &|\Big(\frac{(1-(-1)^{x_k\oplus x_l})}{\sqrt{2}}\sqrt{\nu} + \frac{(1+(-1)^{x_k\oplus x_l})}{\sqrt{2}}\sqrt{1-\nu}\Big)\sqrt{\frac{\eta}{n}}\alpha\rangle_{D_1} \end{aligned} \tag{4.9}$$

Eq [4.9] shows us that due to the ν factor, the probability that there is a click in the correct detector is,

$$p_c = 1 - \exp(-2\eta\nu\frac{|\alpha|^2}{n}) \tag{4.10}$$

while the probability that click is in the wrong detector is,

$$p_w = 1 - \exp(-2\eta(1-\nu)\frac{|\alpha|^2}{n}) \tag{4.11}$$

Let us now consider the cases where Bob can output an incorrect parity value outcome.
Case 1: He does not observe any single click over the entire run of the experiment. The probability of this happening is $p_{\neg 1} = (1-p_1)^{n/2}$, where $p_1 = p_c(1-p_w) + p_w(1-p_c)$. Bob's error probability in this case is $\frac{1}{2}p_{\neg 1}$.
Case 2: When Bob observes at least one single click in the time bin modes. He then randomly chooses any one of those modes to output the parity value. The probability that he outputs the wrong parity value is $p_{1w} = \frac{p_w(1-p_c)}{p_w(1-p_c)+p_c(1-p_w)}$.

From the above two cases, Bob's error probability is,

$$p_{error} = \frac{1}{2}p_{\neg 1} + (1-p_{\neg 1})p_{1w} \tag{4.12}$$

4.5.3 Coherent State Resource

The resource we are interested here is the transmitted information which for our coherent state protocol $\mathcal{O}(|\alpha|^2 \log_2 n)$, where $|\alpha|^2$ is the average photon number in the coherent state. Note that our protocol offers an exponential advantage compared to the classical, only for the information resource. The communication resource for the coherent state protocol is n. This can be reduced by using the multiplexed scheme as proposed in the Chapter 3.

4.5.4 Comparison with Classical Resource

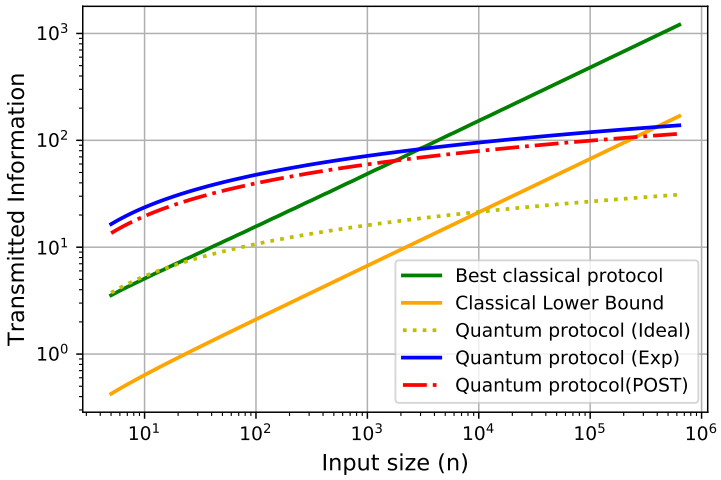

Figure 4.4: Log-Log Plot of Transmitted information resource vs. the input size n for solving Hidden matching within error value $p_{error} = 0.1$. We compare the optimum classical protocol, classical lower bound, quantum protocol in ideal setting, and, quantum protocol under the experimental parameters of Table 4.1. The optimal mean photon number to obtain an error probability of 0.1 is $|\alpha|^2_{ideal} \approx 1.6$ whereas $|\alpha|^2_{exp} \approx 7.1$. The minimum input size needed for the coherent protocol to beat the classical protocol in ideal setting is $n = 17$, while in the experimental quantum protocol needs $n = 2926$. In the post-selected case when Bob only outputs the parity outcome when he observes atleast one click in the protocol run, the coherent protocol performs better than classical analogue for $n_{min} = 1760$. To beat the classical lower bound, the minimum input size for the coherent protocol in the ideal setting is $n = 10189$, whereas with the experimental imperfections, $n = 394272$.

Experimentally demonstrating the Hidden Matching coherent protocol for large input sizes is extremely challenging due to the large number of linear optical elements in the quantum circuit. Nevertheless, we performed a simulation of the protocol to compare the transmitted information resources for the optimal classical protocol vs the coherent state quantum protocol in the ideal and experimental settings with a desired minimum error value

p_{error}. In Figure 4.4 we plot the resources for $p_{error} = 0.1$. In the ideal case, the coherent protocol with mean photon number $|\alpha|^2_{ideal} \approx 1.6$, outperforms the classical protocol from input size $n_{min} = 17$. In the experimental case with experimental parameters of Table[4.1], the coherent protocol with mean photon number $|\alpha|^2_{exp} \approx 7.1$ outperforms the classical protocol from $n_{min} = 2927$. We also analyse the case when Bob only outputs the parity outcome when he observes at least one click in the protocol run. Under this post-selected case, the coherent protocol beats the classical analogue from $n_{min} = 1760$.

For these small input sizes, $p_{dark} \ll p_c$, thus confirming that it is insignificant in the experiment.

4.6 Sampling Matching Problem

The Sampling Matching (SM) is a communication problem based on the Hidden Matching problem, with the difference that now Bob does not receive a uniformly random matching $\sigma_i \in \mathcal{M}_n$ as input, but samples it himself. In other words, he can output any matching $\sigma_i \in \mathcal{M}_n$ and the parity $x_k \oplus x_l$, with $(k, l) \in \sigma_i$, with the constraint that the distribution of the matching is uniform in $\mathcal{M}_n : \{\sigma_1, ..\sigma_{n-1}\}$ even conditioned on the message $m(x)$ sent from Alice, or in other words

$$\mathbb{P}(\sigma_i | m(x)) = \frac{1}{n-1}, \quad \forall \sigma_i \in \mathcal{M}_n \tag{4.13}$$

This constraint of uniform matching output conditioned on Alice's message is important because otherwise Alice and Bob can trivially solve the problem by sharing a public random coin which determines the matching, and then Alice sends the parity of an edge for that specific matching to Bob. This would solve the problem with $\mathcal{O}(1)$ transmitted information and thus becomes easy classically. Since this is a communication complexity task, we expect Alice and Bob to be honest and perform the task according to the constraint. We define this problem in detail below and show that there is still an exponential gap in classical vs quantum transmitted information resources.

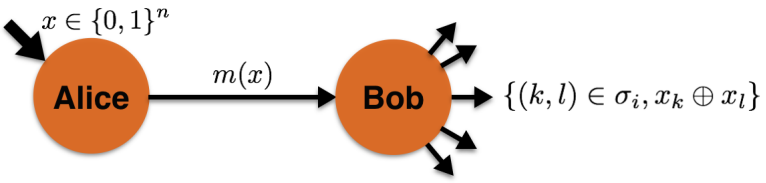

Figure 4.5: Sampling matching problem. Alice gets an input $x \in \{0,1\}^n$ and sends a message $m(x)$ to Bob who outputs the tuple $\langle (k,l) \in \sigma_i, b = x_k \oplus x_l \rangle$ for a matching σ_i, whose distribution is uniform in $\mathcal{M}_n$, even conditioned on $m(x)$. The parity should be correct with high probability for all choices of matching.

4.7 Comparison with Hidden Matching Problem

Classical equivalence of SM and HM problems. It is quite easy to see that the Sampling Matching, which is effectively a sampling problem where Bob uniformly samples a matching from a set $\mathcal{M}_n$ and then uses Alice's message to find the parity of an edge in the matching, and HM, where Bob a priori receives a uniformly random matching from the set, are effectively equivalent problems.

- SM $\rightarrow$ HM: Imagine there exists a protocol for the Sampling Matching, meaning Alice sends a message m and Bob can sample uniformly a matching σ_i from all matchings and then use m to output a parity of an edge in σ_i. Then, Bob uses the same protocol until the output is the matching that he has received as input, in which case he computes the parity and outputs as in the Sampling Matching protocol. The error in HM is the same as in SM.

- HM $\rightarrow$ SM: Imagine there exists a protocol for Hidden Matching. Then, to solve the Sampling Matching, Bob first samples a matching uniformly at random, and then Alice and Bob use the protocol for HM and output accordingly. The error remains the same.

Thus there is an equivalence between these two problems and the communication complexity bounds that hold in HM, also hold in the SM problem.

4.8 Optimal Classical Protocol $\&$ Lower Bound

The classical randomized one-way lower bound for Sampling Matching to succeed with an error probability p_{error} is the same as the one for the Hidden Matching problem,

$$c \geqslant \frac{\log_2 e}{e}(\frac{1}{2} - p_{error})\sqrt{n-1} \tag{4.14}$$

This lower bound is tight, as the classical protocol based on the birthday paradox that succeeds with $p_{error} \leqslant 0.1$, requires a message size,

$$c \geqslant \sqrt{2\log_e 10}\sqrt{n} \tag{4.15}$$

Thus the message size is $\mathcal{O}(\sqrt{n})$. We plot this communication resource in Figure 4.9.

4.9 Quantum Protocol

The protocol for the Sampling Matching problem is exactly the same as that for the Hidden Matching problem. Alice encodes her n-bit input x into the superposition state and sends it to Bob

$$|x\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} (-1)^{x_i} |i\rangle \,. \tag{4.16}$$

Bob picks uniformly a matching $\sigma_i \in \mathcal{M}_n$ and then measures the state $|x\rangle$ in the basis $\{\frac{1}{\sqrt{2}}(|k\rangle \pm |l\rangle\}$, with $(k,l) \in \sigma_i$ to output the tuple $\langle (k,l), b = x_k \oplus x_l \rangle$ with certainty.

4.9.1 Quantum Resource

This protocol uses only $\log_2 n$ qubits, and hence both the communication and the transmitted information is exponentially better than the classical counterpart.

4.10 Coherent State Protocol

The primary reason to introduce the Sampling Matching problem is that for the coherent scheme implementation, this implementation of the protocol is highly simplified compared to the Hidden Matching problem. The number of active+passive elements for Bob to implement the Sampling Matching problem is $\mathcal{O}(1)$. Thus this problem can be implemented for arbitrarily large input sizes. In contrast, for the Hidden Matching problem, the circuit size scales with the input size n, thus making it increasingly difficult to implement the circuit for large input sizes. We analyse the performance of this protocol in the ideal and experimental settings.

4.10.1 State Preparation

Alice prepares the quantum message as a sequence of n-time bin coherent pulses. She phase modulates (PM) the pulses according to her input $x \in \{0,1\}^n$ and an additional constant factor of $\phi \in \{0,1\}$ chosen uniformly randomly,

$$|\alpha_x\rangle = \bigotimes_{i=1}^{n} |(-1)^{x_i \oplus \phi} \frac{\alpha}{\sqrt{n}}\rangle_i \tag{4.17}$$

where $|\alpha|^2$ is the mean photon number for that state $|\alpha_x\rangle$ chosen independently of the input length n. As shown in Figure 4.6 Bob introduces his local-reference n time-bin coherent pulses $|\beta_x\rangle = \bigotimes_{i=1}^{n} |\frac{\alpha}{\sqrt{n}}\rangle_i$, and interacts them one-by-one with the corresponding pulses from Alice. However, it is important to see that when Alice sends the state Eq.(4.17), then Bob satisfies the constraint Eq.(4.13).

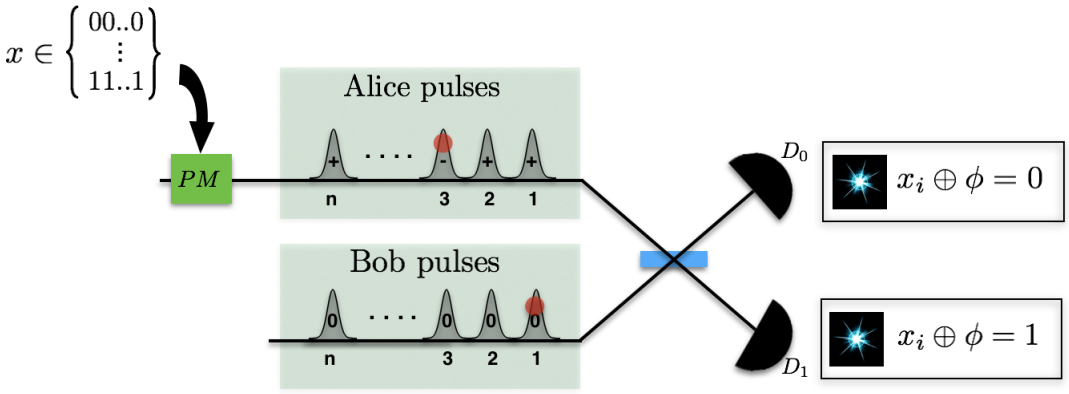

Figure 4.6: Sampling matching circuit illustration using coherent states for any input size n. Alice's quantum message in form of sequence of time-bin phase encoded pulses ($|\alpha_x\rangle$) are shown in the upper arm. The information encoding of the input $x \in \{0,1\}^n$ is done sequentially on the pulses through the phase modulator (*PM*). The lower arm is used by Bob to produces a sequence of n-time bin local reference pulse ($|\beta\rangle$) with same average photon number as the Alice's states. The pulses are then interfered into the 50:50 beam splitter and the parity information is inferred from the detector clicks in D_0 and D_1. The red dot in the 1^{st} and 3^{rd} time sequence means that the Bob observes a single click at D_1 and D_0 detectors respectively for these time steps and thus he outputs $x_1 \oplus x_3 = 1$. If he obtains single clicks in more than two time steps, then he randomly chooses any two time steps to output the parity outcome.

4.10.2 Bob's Uniform Outcome Constraint

Theorem 5. *For the state* $|\alpha_x\rangle = \bigotimes_{i=1}^{n} |(-1)^{x_i \oplus \phi} \frac{\alpha}{\sqrt{n}}\rangle_i$ *sent by Alice, with the amplitude of state in each mode* $i \in [n]$ *being the same, i.e.* $|\alpha_i|^2 = \frac{|\alpha|^2}{n}$*, the probability that Bob outputs the parity value across the matching relations* $\mathcal{M}_n \in \{\sigma_1, .., \sigma_{n-1}\}$*, is uniformly random. In other words,*

$$\mathbb{P}(\sigma_i | \, |\alpha_x\rangle) = \frac{1}{n-1}, \quad \forall i \in [n] \tag{4.18}$$

Proof. Each matching relation $\sigma_i \in \mathcal{M}_n$ contains $n/2$ distinct tuples. And since there are $n-1$ different matching relations in the set, the total number of distinct tuples for input size n is $\frac{n(n-1)}{2}$. Let us denote $\mathbb{P}(\sigma)$ as the probability that Bob outputs the parity value from the matching relation σ,

$$\mathbb{P}(\sigma) = \frac{\sum_{tuple=1}^{n/2} p_{tuple}}{\sum_{\#tuples} p_{tuple}} \tag{4.19}$$

where p_{tuple} is the probability of obtaining the particular tuple, and $\#tuples$ is the total number of tuples.

For each tuple (j,k), the probability of obtaining the parity outcome is equal to the probability of simultaneously having a single click in time modes j and k. Now, if Alice sends the state with same amplitude across all the n modes, then the probability of obtaining a single-click is the same across all modes. If we denote $p_{1,j}$ as the single-click probability in j^{th} mode,

$$p_{1,j} = p = 1 - \exp(-\frac{2}{n}), \tag{4.20}$$

Thus $p_{tuple} = p^2$, for each of the $\frac{n(n-1)}{2}$ tuples. This reduces the Eq.(4.19) to $\mathbb{P}(\sigma) = \frac{1}{n-1}$, thus completing the proof.

□

4.10.3 Error Analysis under perfect Experiment settings

In the perfect experimental settings, the incoming states in the Bob's beam splitter (BS) at the k^{th} time step are,

$$|(-1)^{x_k \oplus \phi} \frac{\alpha}{\sqrt{n}}\rangle_i \otimes |\frac{\alpha}{\sqrt{n}}\rangle_k, \tag{4.21}$$

and the output states are,

$$|\frac{(1+(-1)^{x_k\oplus\phi})}{\sqrt{2}} \frac{\alpha}{\sqrt{n}}\rangle_{D_0} \otimes |\frac{(1-(-1)^{x_k\oplus\phi})}{\sqrt{2}} \frac{\alpha}{\sqrt{n}}\rangle_{D_1} \tag{4.22}$$

Therefore at each time step, the output state is either a vacuum state or a weak coherent state with mean photon number $\frac{2|\alpha|^2}{n}$. In the ideal scenario, D_0 would click only if $x_k \oplus \phi = 0$ while D_1 clicks only if $x_k \oplus \phi = 1$. Now suppose Bob gets the clicks at k^{th} and l^{th} time step in detectors D_0 and D_1 respectively. This implies $x_k \oplus \phi = 0$ while $x_l \oplus \phi = 1$. Combining them results in $x_k \oplus x_l = 1$ since the $2\phi \equiv 0 \pmod 2$. Bob, thus successfully outputs the tuple $\langle (k,l) \in \sigma_i, b = x_k \oplus x_l \rangle$ for the matching $(k,l) \in \sigma_i$. This protocol only lets Bob gather the parity information of the bits and not the bit values x_k, x_l because of the hiding factor ϕ.

Let us analyse the cases where Bob could make an error to infer the correct parity values of any matching.
Case 1: When Bob does not observe any single click over the entire run of the experiment.The probability of this happening is $p_{\neg 1} = \exp(-2|\alpha|^2)$. Bob's error probability in this case is $\frac{1}{2}p_{\neg 1}$.
Case 2: When Bob observes exactly one single click over the entire run of the experiment. Since the parity of a tuple is inferred from the clicks at two distinct time steps, thus in this case, Bob does not infer any parity outcome with certainty. The probability of exactly one single click happening is

$$p_1 = \binom{n}{1} p_c (1-p_c)^{n-1} \tag{4.23}$$

where $p_c = 1 - \exp(-2\frac{|\alpha|^2}{n})$ is the probability of getting a click in one time step. Bob's error probability in this event would be $\frac{1}{2}p_1$.

Combining the two cases, Bob's error probability is

$$p_{error} = \frac{1}{2}(p_{\neg 1} + p_1) \tag{4.24}$$

4.10.4 Error Analysis under Experiment Imperfection

We consider the same imperfection model as in the Hidden Matching. In presence of imperfections, the incoming state in Bob's BS at the k^{th} time step is

$$|(-1)^{x_k \oplus \phi}\sqrt{\frac{\eta}{n}}\alpha\rangle_k \otimes |\sqrt{\frac{\eta}{n}}\alpha\rangle_k \tag{4.25}$$

and the output state is

$$\begin{aligned} &|\Big(\frac{(1+(-1)^{x_k\oplus\phi})}{\sqrt{2}}\sqrt{\nu} + \frac{(1-(-1)^{x_k\oplus\phi})}{\sqrt{2}}\sqrt{1-\nu}\Big)\sqrt{\frac{\eta}{n}}\alpha\rangle_{D_0,k} \otimes \\ &|\Big(\frac{(1-(-1)^{x_k\oplus\phi})}{\sqrt{2}}\sqrt{\nu} + \frac{(1+(-1)^{x_k\oplus\phi})}{\sqrt{2}}\sqrt{1-\nu}\Big)\sqrt{\frac{\eta}{n}}\alpha\rangle_{D_1,k} \end{aligned} \tag{4.26}$$

The marked contrast from the ideal setting is that whereas in the ideal case, there is a non-zero click probability only in the correct detector for any time step, in presence of experimental imperfections, due to the finite visibility factor, there is a non-zero click probability in both the correct and incorrect detectors in the same time step. From Eq.(4.26), it is obvious that larger the visibility ν, the bigger the chances of the photons going in the correct detector. Across each time step, the probability of a click in the correct detector is,

$$p_c = 1 - \exp(-2\eta\nu\frac{|\alpha|^2}{n}) \tag{4.27}$$

while the probability that a click occurs in the wrong detector is,

$$p_w = 1 - \exp(-2\eta(1-\nu)\frac{|\alpha|^2}{n}) \tag{4.28}$$

Now we look at the cases where Bob can output the incorrect parity outcome:
Case 1: When Bob does not observe any two single-click time modes in the experiment. The probability $\mathbb{P}$(no two single-clicks) = $\mathbb{P}$(no single-clicks) + $\mathbb{P}$(exactly one single-click).

$$p_{\neg 11} = (1-p_1)^n + \binom{n}{1}p_1(1-p_1)^{n-1} \tag{4.29}$$

where $p_1 = p_c(1-p_w) + p_w(1-p_c)$ is the probability of observing a single click in one time mode. Bob's error probability in this case is $\frac{1}{2}p_{\neg 11}$.

Case 2: When Bob observes at least two single-click time modes. He then randomly chooses any two of those single-click modes (k, l) to output the parity for matching $(k, l) \in \sigma_i$. The probability that he outputs the wrong parity value is:

$$p_{11w} = \frac{2p_c(1-p_w)p_w(1-p_c)}{[pc(1-p_w)+p_w(1-p_c)]^2} \tag{4.30}$$

Combining these 2 cases, Bob's total error probability is

$$p_{error} = \frac{1}{2}p_{\neg 11} + (1-p_{\neg 11})p_{11w} \tag{4.31}$$

4.11 Coherent State Resource

The transmitted information of the protocol is $\mathcal{O}(|\alpha|^2 \log_2 n)$, where $|\alpha|^2$ is independent of the input size n. The optimal $|\alpha|^2$ value for each n is obtained by setting error probability the $p_{error} = 0.1$ in Eq.(4.31). Better experimental equipments result in lower imperfection values and thus a lower $|\alpha|^2$ value to reach the desired p_{error}.

4.12 Experimental Analysis of Coherent State Protocol

We demonstrate the proof-of principle short distance implementation of Sampling matching problem using the home made set-up as shown in Figure 4.7. Our set-up involves the coherent pulse generation with a single laser which is split using the 50/50 beam splitter into pulses for Alice and Bob. Below we describe the experimental methods, followed by the analysis of our experimental data.

4.12.1 Experimental Methods

Our set-up is divided into *Front loop* and *Phase correction loop*.

Front loop: The the coherent state for Alice and Bob is produced by the ultra low line-width ($\sim$10kHz) continuous wave laser source, Laser1 (Pure Photonics $\sim$ 1563nm). This is then chopped into time-bin coherent pulses by the amplitude modulator (AM) that is modulated using a function generator to create pulses with the repetition rate of 1MHz and duty cycle of 1.6%.The variable optical attenuator (VOA) is then used to bring the mean photon number in the pulses to the desired level. The circulator (C) after the VOA is

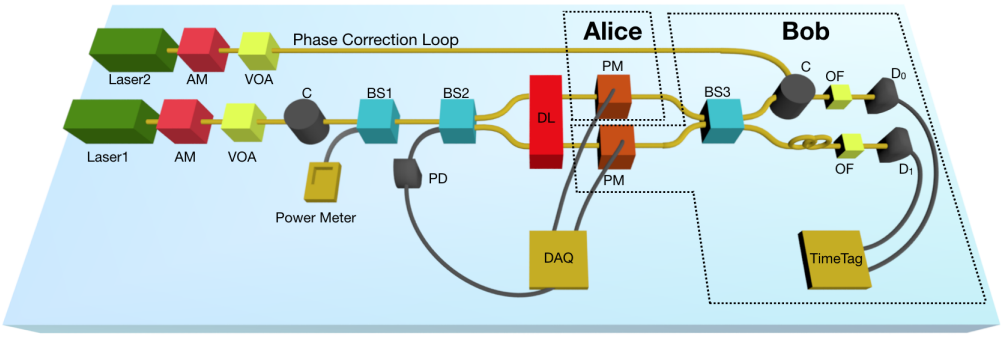

Figure 4.7: Experimental set-up for Sampling Matching circuit implementation. The set-up has Front loop, operated by continuous wave laser source, Laser1, at $\lambda = 1563$nm, while the Phase correction loop is operated by the laser source, Laser2, at $\lambda = 1527$nm. In the Front loop, the amplitude modulator AM creates coherent pulses, which are brought to the desired mean photon level using the variable optical attenuator (VOA). The circulator (C), ensures that no power of the pulses from Laser2, reaches Laser1, thus preventing the Laser1 from any harm. One output arm of the 50/50 beam splitter (BS1) is given to power meter to monitor the power, and hence the average photons in the pulse. BS2 splits the two paths, the upper path for Alice and lower path for Bob. We introduce a delay line (DL) in the paths, to perfectly fine tune the path lengths. This ensures that Alice and Bob's pulses arrive at BS3 simultaneously. Alice modulates her pulses sequentially according to the input string $x \in \{0,1\}^n$ she receives. Similarly Bob modulates her pulses with the string 0^n. We use the data acquisition card (DAQ) to provide the voltage corresponding to the strings to PMs. After interaction of the pulses in BS3, the path leading to single photon detector D_0, has a circulator (C) which directs the Laser1 pulses into the detector. An optical filter (OF) only lets pulses from Laser1 to pass through and blocks the Laser2 pulses. We use the Phase correction loop to monitor and correct the phase drift over time in Alice's and Bob's paths. The pulses from Laser2 enter the set-up from an arm of C, passes through BS3 to split into Alice and Bob's paths, and interfere in BS2. We monitor the phase drift in photo diode (PS) connected to the output arm of BS2.

introduced to ensure that the laser power is transmitted only in the forward direction and pulses coming from the Laser2 are blocked, thus ensuring no harm to Laser 1. We use the balanced 50/50 beam splitter(BS1) to monitor the power of the pulses. The second 50/50 BS2 splits the two paths, the upper path corresponding to Alice, and the lower corresponding to Bob. We introduce a delay line (DL) to perfectly fine tune the path lengths of Alice and Bob. This ensures that the pulses from Alice and Bob arrive simultaneously in the 50/50 BS3. In our setting, Bob's path is longer than Alice's path by 17.1mm (fiber length). We compensate this path difference with the DL. Alice phase modulates (PM) her coherent pulses sequentially according to the input string $x \in \{0,1\}^n$ she receives. Since the input is binary string, we provide to the PM a voltage V_0 when the input bit is 0 and V_π when the input bit is

1. This voltage is provided using the data acquisition card (DAQ) in our set-up. Similary for Bob, we provide the voltage V_0 to all the n pulses. The pulses from Alice and Bob interact sequentially in BS3. Normally, all the pulses should interact according to Eq.(4.26), but in reality there is a phase drift over time in the two paths. To make sure we cancel the effect of phase drift, we introduce the phase correction loop to monitor and correct the phase drift in the pulses.

The path leading to the single photon detector (D_0) has the circulator C, which allows the transmission only in anticlockwise direction. The length of the circulator is $\sim$ 2m. We introduce a fiber length of 2m in the lower path to maintain the same arrival times for the pulses in the detectors D_0 and D_1. We introduce the optical filter (OF) just before the detection, to allow only the pulses from the Laser1 ($\lambda = 1563$nm) to pass through and block any contribution from Laser2 in the photon counts. Finally for the detection, we use the two high efficiency, ultra low dark count free running ID230 (manufactured by ID Quantique) detectors. The clicks are recorded upto a precision of 1ps in the TimeTag analyser (manufactured by QuTools).

Phase correction Loop: We introduce the second continuous wave laser source, Laser2 (Pure photonics $\sim$ 1527nm) to monitor the phase drift in Alice and Bob's paths. The laser source is modulated with the AM to produce laser pulses at 1MHz repetition rate and duty cycle of 1.6%. The pulses then enter set-up via one arm of C. They are split into Alice's and Bob's paths via the BS3. Upon interacting in BS2, the output of the phase correction pulses are then collected in the photo-diode PD which gives the information of the phase drift in the two paths. The phase drift is then analysed and corrected using the following technique. Before describing the technique, we note that the phase drift is not corrected for each and every pulse. This is because our experiment runs at a high speed of 1Mhz and, it is realistically not feasible to for the computer to process the phase information and correct it for each and every pulse. Second, the phase drift is slow due the high stability of the laser and the set-up, hence it is not required to correct this drift for each pulse. We rather correct an average phase drift over a number of pulses. We make blocks of pulses and track the average the phase drift in one block to use it to correct the drift for the next block. This block construction is illustrated in Figure 4.8. We choose a block size of 8192 pulses. The first 7680 pulses are used for protocol run. The second segment of block $\text{Alice}_{\text{track}}$, tracks the phase drift in the path corresponding to Alice's PM. This is done by giving a ramp voltage in Alice's PM from -5V to +5V, and 0V in Bob's PM across 256 pulses. The response of the linear ramp voltage across a phase modulator is a cosine function $A\cos(\omega t + \phi)$ which is tracked in the PD. While modelling the expected response with the actual response, we get the information of phase and phase drift upto a certain error. Let V_{bias} be the voltage corresponding to the phase drift, then the voltage across Alice's PM for the next block gets added by factor V_{bias} i.e. $V_{PM} = V_{x_i} + V_{bias}$. We similarly track and correct the phase drift in Bob's PM over the last 256 pulses of the block, $\text{Bob}_{\text{track}}$.

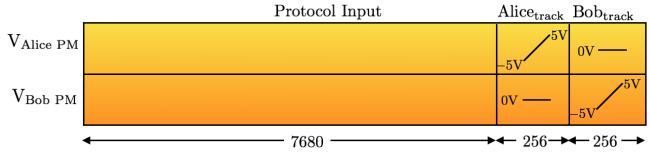

Figure 4.8: Block illustration for analysing the phase drift in pulses. Phase tracking is done once for every block of 8192 pulses. The first 7680 pulses are used for protocol encoding. The second part of the block Alice$_{track}$, tracks the phase drift in Alice's PM. For this we give a ramp voltage from -5V to +5V in Alice's PM and 0V in Bob's PM. The third part of the block Bob$_{track}$, tracks Bob's PM by giving a ramp voltage from -5V to +5V in Bob's PM and 0V to Alice's PM.

4.12.2 Experimental Results

We perform our proof-of-principle short distance implementation of Sampling Matching problem over the standard telecom wavelength $\lambda = 1563$nm at 1Mhz. The overall channel

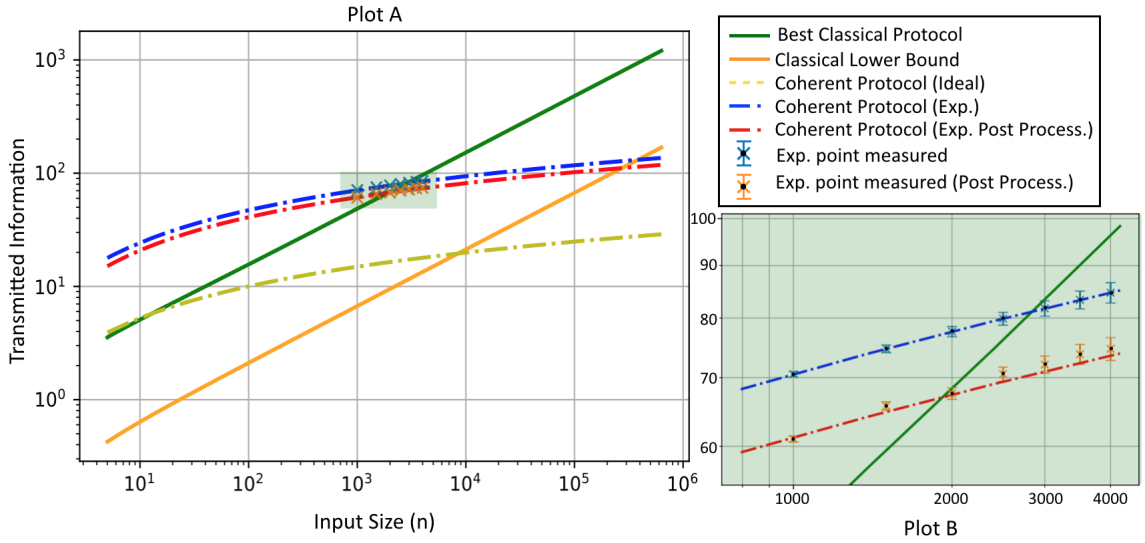

Figure 4.9: Log-log plot of Transmitted information resource vs. the Input size (n) for solving the Sampling matching problem within error $p_{error} = 0.1$. Plot A compares the optimal classical protocol, classical lower bound, quantum protocol in ideal setting, quantum protocol with the experimental parameters of Table 4.1, and the quantum protocol when Bob post processes to output the parity outcome only in cases when he obtains atleast two single clicks in the run. Plot B is the magnified version of the green section in Plot A where we show the input sizes for which we beat the best classical protocol in normal and post processing scenarios. The dotted blue/red line is the simulated transmitted information resource vs n in normal and post-processing scenario respectively. The points with error bars are the experimentally obtained points for the selected input sizes. The optimal mean photon number are shown in Table 4.2

Table 4.1: Experimental parameters

$\eta_{channel}$	η_{det}	ν	p_{dark}
3.5dB	25%	$(98.8 \pm 0.3)\%$	$(2.3 \pm 0.2) * 10^{-6}$

n	1000	1500	2000	2500	3000	3500	4000
ε	0.1	0.1	0.1	0.1	0.1	0.1	0.1
μ/pulse ($*10^{-3}$)	7.08 ± 0.01	4.72 ± 0.01	3.54 ± 0.01	2.83 ± 0.01	2.36 ± 0.01	2.02 ± 0.01	1.77 ± 0.01
#Runs	848	568	475	381	317	272	238
$\#\text{Runs}_{\text{no click}}$	115	68	62	45	38	31	28
$\#\text{Runs}_{\text{click}}^{\text{wrong}}$	26	26	20	17	16	7	11
ε_{POST}	0.03	0.04	0.04	0.04	0.05	0.03	0.05
μ_{POST}/pulse ($*10^{-3}$)	6.12 ± 0.01	4.15 ± 0.01	3.08 ± 0.01	2.50 ± 0.01	2.08 ± 0.01	1.79 ± 0.01	1.56 ± 0.01

Table 4.2: Detailed experimental analysis: We carried out Sampling matching scheme for seven different input sizes $1000 - 4000$. The objective was to output the matching parity outcome with an error rate of at-most $\varepsilon = 0.1$. To obtain the statistics, we run the scheme #Runs times for each input size. Out of the runs, $\#\text{Runs}_{\text{no clicks}}$, are the copies where we do not obtain atleast two single clicks. Based on this, we compute the average photon number μ_{POST} in our the scheme when Bob only post-selects to output the parity outcome of those runs where he gets atleast two single clicks. Finally, $\#\text{Runs}_{\text{click}}^{\text{wrong}}$ are the number of copies where Bob obtains atleast two single clicks and he outputs the wrong parity outcome. This determines the error rate (ε_{POST}) after post processing.

loss in the channel i.e. the loss before Alice and Bob apply their phase modulator (PM) to the input of detectors D_0 and D_1 is 3.5dB. This parameter is shown in Table[4.1]. Further our detectors operate at 25% efficiency. The combined effect of channel loss and limited detector efficiency results in transmission of higher mean photon number μ in the pulses, as compared to the scenario when the set-up had no experimental imperfections, to achieve the desired error rate ε.

The limited visibility (ν) in the set-up accounts for the imperfection in the interference of Alice and Bob's pulses. We introduced the delay line (DL) to get as close as possible to the ideal visibility factor of 1. This adjustment was done by first sending an input of 0^n to both Alice and Bob and recording the clicks obtained in two detectors and then sending 0^n and 1^n to Alice and Bob respectively and observing the clicks.

We further inspected the dark counts to make sure it is safe to neglect them in our analysis and indeed we observed that the signal click probability is substantially $(10^3\times)$ more probable than the dark count probability. Our detectors at set at the dead time of 10μs. This means that after the detector records a click, there is no recording of the clicks for the next 10 pulses. This is not an issue for us, as, for the input size of $\geqslant 1000$ that we run the protocol for, the probability of a click across 10 pulses $\ll$ probability of the click across rest of the pulses in the input. The reason for this is the extremely low photon number across the pulses, and thus it can be safely neglected compared to other sources of error.

With the experimental imperfection values obtained in the testing phase, we estimate the optimal average photon number μ required for each input size, n, that achieves the desired error rate ε. We provide the optimal μ in our set-up for each of the n we tested. This is illustrated in Table 4.2. Figure 4.9 plots the simulated and observed experimental transmitted information points for these input sizes. We see that the input sizes $3000 - 4000$ transmit less information resource compared to the best classical protocol, even under the error bars.

Further, we also looked at the average case when Bob runs the protocol for Sampling Matching multiple times (#Runs) and post selects to output only for those runs where he gets a parity outcome. Without the post-selection, every time Bob would not obtain the parity outcome, he would output a random parity with error rate $\frac{1}{2}$. However, with post selection, since he rejects those no-parity outcome cases, this enables him to succeed with a lower error rate ε_{POST}. This can also be interpreted as performing the protocol with lower average photon number, since we are rejecting the runs with no outcome.

$$\mu_{POST} = \mu \frac{(\#\text{Runs} - \#\text{Runs}_{\text{no clicks}})}{\#\text{Runs}} \tag{4.32}$$

In Figure 4.9, we also plot the transmitted information points under the post-selected scenario. We observe that the quantum protocol performs the sampling matching task with lower resources than the classical counterpart from the chosen input sizes 2000 and beyond.

4.13 Conclusion

The Sampling Matching is first such example of a one way communication complexity problem where we can experimentally demonstrate the quantum advantage using coherent state fingerprints. A noteworthy feature of our implementation is the separation of the paths for Alice and Bob, and perfect fine tuning of their path lengths such that Alice's input pulses and Bob's local pulses arrive at Bob's beam splitter at the same time. We also have a proposal to go from proof-of-principle implementation to the full scale implementation by separating the laser sources of Alice and Bob. A typical issue in going to full-scale implementation involves maintaining the stable phase across the two paths. The phase fluctuation would be accounted due to the drift of the laser pulses traversing over the optical channel and the internal jitter in the lasers. In our experiment, we address the first source of fluctuation by introducing a *Phase correction loop*. The second source of fluctuation can be addressed by having two highly stable lasers (low line width $\sim$ kHz) such that any differnce in phase drift between them is much slower than the duration of expeirment run [CLF$^+$16].

The Sampling Matching problem, similar to Euclidean distance communication problem, does not need Alice to have a memory to store her input as Bob does not perform a global operation on input. In other words, this protocol works also in the *streaming* scenario, where Alice receives her input one bit at a time [NAS99].

Finally, Sampling Matching problem also has applications in cryptographic as well as

computational settings. In the cryptographic front, this problem is the back-bone of quantum retrieval games (QRG) and quantum money scheme that we will talk about in the next chapter. This problem also finds applications in verification of NP-complete problems where the quantum verifier can verify a partial quantum proof in polynomial time, whereas to verify the same amount of classical proof, the classical prover needs exponential time steps.

5 Private-key Quantum Money

5.1 Introduction

In the 1970s, Wiesner [Wie83] proposed the idea of quantum money to create unforgeable bank notes which are quantum states. The unforgeability of the note relied on the no-cloning property of quantum mechanics [WZ82]. This was incidentally also the first quantum cryptographic primitive to be introduced. Subsequently other cryptographic tasks were proposed, such as quantum key distribution, digital signatures, coin flipping etc. [SBPC$^+$09, DCK$^+$16, PJL$^+$14].

In the Wiesner scheme, the bank notes are several BB84 states prepared by an honest authority, $Bank$, who then distributes them to the untrusted parties. The party in possession of this note has to send the quantum note to the *Bank* for verification, who then authenticates the validity of the note. This scheme, as studied by [Lut10, BNSU14], soon ran into problems. The first issue was (a) verification of the note required quantum communication with the *Bank*. As pointed out by Gavinsky [Gav12], an adversary can interfere in the communication and can modify or destroy the note, and, (b) several new attacks to this scheme, the *adaptive attacks* [BNSU14], have shown that for an adversary using these attacks, the forging probability of the adversary no longer remains vanishingly small.

These two drawbacks were first addressed by Gavinsky [Gav12]. His private-key quantum money scheme was based on the idea of quantum retrieval games (QRG). The verification of the note in this scheme requires three rounds of classical communication between the *Bank* and the note holder and it is also secure against any adaptive attack. This scheme however only works in ideal scenario and does not take into account the noise due to experimental imperfections. Also, this scheme requires three rounds of communication between the *Bank* and holder, thus necessitating the *Bank* to have a temporary memory during the note verification phase. Several other quantum money schemes have been proposed since then [PYJ$^+$12, AC12, FGH$^+$12, Gav12, GK15, MP16, AA17].

Further independent works by Georgiou et al [GK15] and Amiri et al [AA17] have reduced the number of rounds of classical communication between the *Bank* and the holder to a single round. While the scheme of [GK15] is based on 1-out-of-2 QRG, and can tolerate the noise of upto 12.5%, the scheme of [AA17] is based on the Hidden Matching quantum retrieval games, HM-QRG, [GKK$^+$07, AKL16], and they show that it exhibits noise tolerance of up to 23.3%. They further conjecture that maximal noise tolerance for money schemes based on Matching QRGs can reach up to 25%. Here, the maximal noise tolerance is the maximum theoretical error that can be tolerated by an honest note holder during the verification of the note. The note has an information theoretic security against a forger trying to forge the bank note.

Till date, there have been two proof-of-principle experimental demonstrations for quantum money, based on one round classical verification with the *Bank*, the first by Bozzio et al [BOV$^+$18] which is based on the scheme of [GK15]. Here the quantum money encoding is done via polarized weak coherent states and they demonstrate the error rate $\beta = 2.8\%$. The other demonstration is by Guan et al [GAA$^+$18] which is based on the scheme of [AA17] has an encoding based on phase parity of corresponding pairs of weak coherent states. They did an implementation for input string size $n = 4$, which theoretically has the maximal noise tolerance of 16.6%, while their measured error rate was $\beta = 3\%$.

In this work, we introduce the private-key quantum money scheme using many copies of single photon states in superposition over multiple modes, and the verification protocol based on the Sampling Matching quantum scheme. Our money scheme achieves a noise tolerance of 21.4%, and can reach up to 25% if the conjecture of [AA17] on the noise tolerance of Matching scheme holds true. The features of our scheme include single round classical interaction with the *Bank*, multiple note re-usability (linear in the size of the note), and robustness even against adaptive kind of attacks by the adversary. Building on this work, we propose the private-key quantum money scheme using coherent states. The verification protocol involving coherent states offers a significant advantage compared to the previous Hidden Matching based verification protocols. In the protocols based on Matching schemes, the tolerance against the noise, increases with the input size of the note. Thus the money scheme becomes more robust against forging by going to higher input sized bank notes. For the schemes based on Hidden Matching, the verification protocol involves a complex circuit with the number of optical elements (switches, delays, beam splitter) increasing with the input size. Thus it gets increasingly difficult to implement the circuit for large input sizes. This is the primary reason why the only implementation based on Hidden Matching has been shown for input size $n = 4$. With the Sampling Matching based verification procedure, the number of optical components needed for verification is $\mathcal{O}(1)$, and thus independent of the input size. This enables us to go to arbitrarily large input sizes, thus reaching higher robustness than what was previously experimentally feasible.

We start by giving the definitions for private-key quantum money. Then we identify the tools required to construct our money scheme. We follow this up by introducing our money scheme using single photon encoding and later using coherent states.

5.2 Definitions for Private-key Quantum Money

In this section, we go through the definitions for private-key quantum money. We also define a private-key quantum money **mini-scheme** and then use the result of Aaronson et al [AC12] to directly go from a mini-scheme to a full scheme.

Informally, a private-key quantum money scheme involves an algorithm used by a trusted entity, the *Bank* to produce multiple notes, and a protocol which is run between a holder H of the note and the *Bank* to verify the authenticity the note. The requirement for the verification protocol to be secure is that it must be impossible for an adversary note holder to create more notes that what it received from the *Bank*.

Definition 1 (Private-key quantum money). A quantum money scheme with classical verification consists of an algorithm by the *Bank*, and a verification protocol, *Verification*, such that,

1. *Bank* algorithm produces a quantum note $\$ = (\rho, \text{s.n.})$ where ρ is a quantum state of the note and s.n. is the classical serial number of the note.

2. *Verification* is a verification protocol with classical communication that is run on the note $\$$, between the note holder H who claims to posses the note $\$$ and the *Bank*. The output of the protocol is a bit b sent by the *Bank* to denote whether the note is valid or not. We denote this final bit as $\text{Ver}_H^B(\$)$.

For this scheme to be secure, it must satisfy two important properties,

- Correctness: The scheme is ε correct if for every honest holder H, it holds that

$$\mathbb{P}[\text{Ver}_H^B(\$) = 1] \geqslant 1 - \varepsilon \tag{5.1}$$

- Unforgeability: The scheme is ε unforgeable if for any quantum adversary who possesses m notes, has interacted a finitely bounded number of times with the *Bank* and has managed to produce m' notes $\$_1, \$_2, \cdots, \$_{m'}$, it holds that,

$$\mathbb{P}\left[\left(\bigwedge_{i\in[m']} \text{Ver}_H^B(\$_i) = 1\right) \wedge (m' > m)\right] \leqslant \varepsilon \tag{5.2}$$

where H is any honest note holder.

The correctness condition ensures that all the honest note holders can get their note verified with an exponentially close to 1 probability (by setting ε exponentially close to 0). While the unforgeability condition ensures that an adversary trying to create more notes than what he had from the *Bank*, would fail with an exponentially close to 1 probability in being

able to verify all the notes. Our definition includes possibility of adaptive attacks by the adversary since we allow him to interact with the *Bank* during the verification protocol a finite number of times.

Aaronson et al [AC12] studied the security of the full scheme and deduced that it is enough to prove the security of a smaller money scheme (mini-scheme) in order to guarantee security of the full scheme. Under this mini-scheme the *Bank* produces one quantum note $\$$. The goal of the note adversary is, after finite interactions with the Bank, to produce two quantum notes $\$_1$ and $\$_2$ which successfully passes the verification test of the *Bank*. In this scheme, since the *Bank* produces only a single note $\$$, hence it does not need to have a classical serial number.

Definition 2 (Private-key quantum money mini-scheme). A quantum money min-scheme with classical verification consists of an algorithm by the *Bank*, and a verification protocol, *Verification*, such that,

1. *Bank* algorithm produces a quantum note $\$ = \rho$ where ρ is a quantum state of the note.
2. *Verification* is a verification protocol with classical communication that is run on the note $\$$, between the note holder H who claims to posses the note $\$$ and the *Bank*. The output of the protocol is a bit b sent by the *Bank* to denote whether the note is valid or not. We denote this final bit as $\text{Ver}_H^B(\$)$.

For this scheme to be secure, it must satisfy two important properties,

- Correctness: The scheme is ε correct if for every honest holder H, it holds that

$$\mathbb{P}[\text{Ver}_H^B(\$) = 1] \geqslant 1 - \varepsilon \tag{5.3}$$

- Unforgeability: The scheme is ε unforgeable if for any quantum adversary who possesses the note $\$$, has interacted a finitely bounded number of times with the *Bank* and has managed to produce two notes $\$_1$ and $\$_2$, it holds that,

$$\mathbb{P}\left[\left(\text{Ver}_H^B(\$_1) = 1 \wedge \text{Ver}_H^B(\$_1) = 1\right)\right] \leqslant \varepsilon \tag{5.4}$$

where H is any honest note holder.

To go from a private-key quantum money mini-scheme to a full scheme, it is enough for the *Bank* to add a serial number to a note of the mini-scheme. Then the *Bank* can just run the verification protocol of the mini-scheme for that note with the serial number.

We therefore propose a quantum money mini-scheme and rely on the above results to extend this mini-scheme into full scheme.

5.3 Tools for the Money Scheme

In this section we define an essential tool required for the construction of our scheme, the verification protocol based on the Sampling Matching problem. We first define this problem, a problem in one-way communication model, as we have seen in Section 4.6. Then we construct the verification protocol based on this problem.

5.3.1 Sampling Matching Problem

We have already introduced the Sampling Matching (SM) problem in Section 4.6. Here, we use a variant of our SM problem that involves two parties, Alice and Bob. Alice receives a binary string $x \in \{0,1\}^n$. Bob, on the other hand, does not receive any input.

The objective of this problem is the following: Bob, after receiving a message $m(x)$ from Alice, needs to output a tuple (k,l) from the set containing a total of $\mathcal{T}_n = n(n-1)/2$ distinct tuples of the form (k,l) and the corresponding bit value $b = x_k \oplus x_l$, where x_k and x_l are the k-th and l-th bit of the string x respectively. An example of the tuple set $\mathcal{T}_4$ for $n = 4$ is shown in Figure 5.1. We look at the model of one-way communication where we only allow a single message from Alice to Bob.

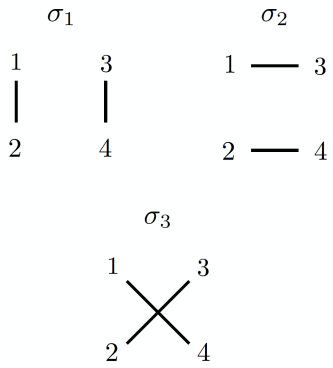

Figure 5.1: An example of all possible distinct tuples for the size $n = 4$: $\mathcal{T}_4$: $\Big[(1,2),(3,4),(1,3),(2,4),(1,4),(2,3)\Big]$

For our quantum money proposal, we study the case when Alice is untrusted and Bob is trusted and honest. If Alice is honest, then conditioned on the message sent by her, Bob's relative probability of sampling the tuple (k,l) from the set $\mathcal{T}_n$ must be uniformly random. In other words,

$$\mathbb{P}((k,l)|m(x)) = \frac{1}{n(n-1)/2}, \ \forall (k,l) \in \mathcal{T}_n \tag{5.5}$$

However, a dishonest Alice can force Bob to sample one tuple more than the other. This constitutes a test to distinguish an honest Alice from a dishonest one. Bob certifies the honesty

of Alice by asking for multiple copies of the message and comparing the measurement result statistics with what she should expect from an honest Alice.

We will see how Bob samples a tuple from the set $\mathcal{T}_n$ when Alice sends a quantum message to Bob. We analyse Bob's scheme when the message sent by Alice is a single photon state in a superposition over n modes.

5.3.2 SM Scheme with Single Photon States

Sampling Matching scheme is Bob's testing scheme to extract the parity outcome of a tuple from the perfect disjoint set $\mathcal{T}_n$ containing $n(n-1)/2$ distinct tuples to solve the Sampling Matching problem. Here we look at the testing scheme when Alice sends a single photon state to Bob.

The technique is depicted as follows: When an honest Alice receives the binary string $x \in \{0,1\}^n$, she encodes the information of this string into a single photon state in a superposition over n different modes,

$$|x\rangle = \frac{1}{\sqrt{n}} \sum_{k=1}^{n} (-1)^{x_k} \hat{a}_k^\dagger |0\rangle \,, \tag{5.6}$$

where x_k is the k-th bit of the string x. The operator $\hat{a}_k^\dagger$ is the creation operator for the k^{th} mode, and, $\hat{a}_k^\dagger |0\rangle = |1\rangle_k$. Figure 5.2 illustrates one of the methods to create of equal superposition state of Eq.(5.6) by passing the initial state $\hat{a}^\dagger |0\rangle$ through the cascade of 50/50 beam splitters and adding the phase information of each bit of the input in the n modes.

Alice sends this state to Bob. In order to output the parity outcome of a tuple, Bob prepares his local superposition state

$$|\beta\rangle = \frac{1}{\sqrt{n}} \sum_{k=1}^{n} \hat{b}_k^\dagger |0\rangle \,, \tag{5.7}$$

We denote the action of creation operator $\hat{b}_k^\dagger |0\rangle = |1'\rangle_k$.

Bob's action is then to apply the n-beam splitter operation on the state $|x\rangle \otimes |\beta\rangle$. This is illustrated in Figure 5.3.

Prior to the n-beam splitter operation, the input of Bob is,

$$\frac{1}{\sqrt{n}} \sum_{k=1}^{n} (-1)^{x_k} \hat{a}_k^\dagger |0\rangle \otimes \frac{1}{\sqrt{n}} \sum_{l=1}^{n} \hat{b}_l^\dagger |0\rangle \tag{5.8}$$

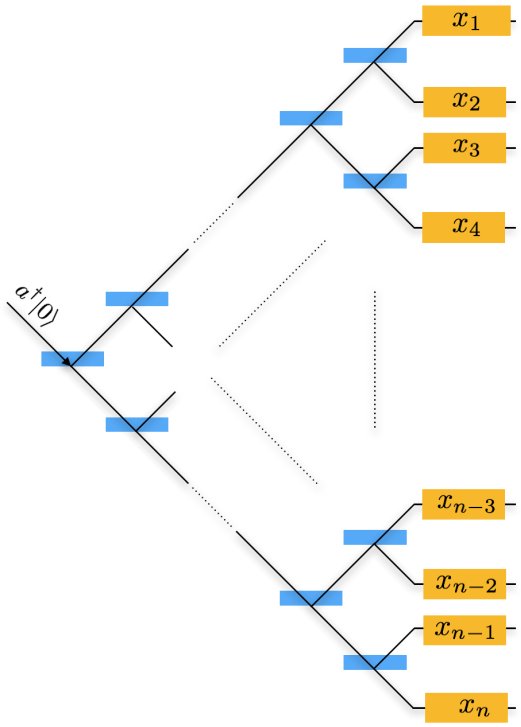

Figure 5.2: Circuit model by Alice to create a single photon state in equal superposition over n modes. This is done by passing a single photon through a cascade of beam splitters, which are then subject to a phase-shift that depends on the corresponding secret string $x \in \{0,1\}^n$ of Alice.

The output mode $\hat{O}^\dagger$ of Bob after interacting with the corresponding modes of Alice is,

$$\begin{aligned}
\hat{O}^\dagger &= \frac{1}{2n}\sum_{k=1}^{n}(-1)^{x_k}(\hat{c}_k^\dagger + \hat{d}_k^\dagger)\sum_{l=1}^{n}(\hat{c}_l^\dagger - \hat{d}_l^\dagger), \\
&= \frac{1}{2n}\sum_{k,l=1}^{n}(-1)^{x_k}(\hat{c}_k^\dagger\hat{c}_l^\dagger + \hat{d}_k^\dagger\hat{c}_l^\dagger - \hat{c}_k^\dagger\hat{d}_l^\dagger - \hat{c}_k^\dagger\hat{d}_l^\dagger), \\
&= \frac{1}{2n}\sum_{k=1}^{n}(-1)^{x_k}(\hat{c}_k^{\dagger 2} - \hat{d}_k^{\dagger 2}) \; + \\
&\quad \frac{1}{2n}\sum_{(k,l)\in\mathcal{T}_n}((-1)^{x_k} + (-1)^{x_l})(\hat{c}_k^\dagger\hat{c}_l^\dagger - \hat{d}_k^\dagger\hat{d}_l^\dagger) \; + \\
&\quad \frac{1}{2n}\sum_{(k,l)\in\mathcal{T}_n}((-1)^{x_k} - (-1)^{x_l})(\hat{c}_k^\dagger\hat{d}_l^\dagger - \hat{d}_k^\dagger\hat{c}_l^\dagger)
\end{aligned} \tag{5.9}$$

where $\mathcal{T}_n$ is the set of all possible $\frac{n(n-1)}{2}$ distinct tuples.

From Eq.(5.9), we observe the following,

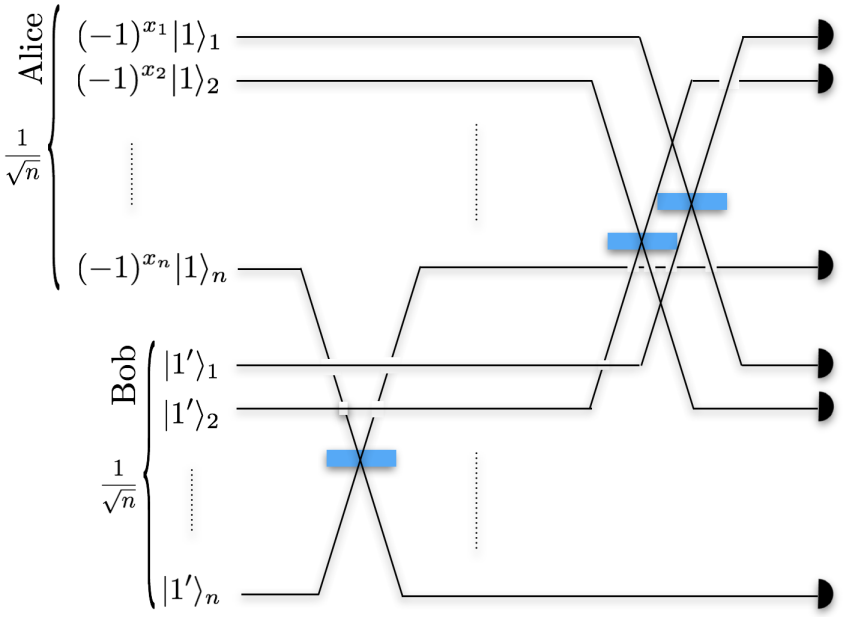

Figure 5.3: Sampling Matching circuit model in single photon encoding. Alice encodes a secret string $x \in \{0,1\}^n$ in the single photon state $|x\rangle$ in an equal superposition over n modes. This is then sent to Bob. Bob creates his local superposition state and applies mode-by-mode beam splitter operation with Alice's state.

- Simultaneous single photon clicks observed in $\{\hat{c}_k^\dagger, \hat{c}_l^\dagger\}$ or $\{\hat{d}_k^\dagger, \hat{d}_l^\dagger\}$, for two distinct modes (k,l), implies $x_k \oplus x_l = 0$.
- Simultaneous single photon clicks observed in $\{\hat{c}_k^\dagger, \hat{d}_l^\dagger\}$ or $\{\hat{d}_k^\dagger, \hat{c}_l^\dagger\}$, for two distinct modes (k,l), implies $x_k \oplus x_l = 1$.
- 2 photons observed in the same mode $\hat{c}_k^\dagger$ or $\hat{d}_k^\dagger$ results in inconclusive outcome for Bob.

The probability of observing 2 photons in the same mode $\hat{c}_k$ is

$$p_2^{\hat{c}_k} = |\langle 00|\, \hat{c}_k^2 \cdot \hat{O}_j^\dagger\, |00\rangle\,|^2 = \frac{1}{2n^2} \tag{5.10}$$

Similarly, the probability of having 2 photons in the same mode $\hat{d}_k$ is,

$$p_2^{\hat{d}_k} = |\langle 00|\, \hat{d}_k^2 \cdot \hat{O}_j^\dagger\, |00\rangle\,|^2 = \frac{1}{2n^2} \tag{5.11}$$

Over all the n modes, the probability of having 2 photons in the same mode is

$$p_2 = \sum_{k=1}^{n} p_2^{\hat{c}_k} + p_2^{\hat{d}_k} = \frac{1}{n} \tag{5.12}$$

In these cases, Bob does not get a conclusive parity outcome. Here he outputs the parity outcome $d = \emptyset$.

In the rest of the case, Bob always gets exactly two single photon clicks in two different time modes $k, l \in [n]$ with the correct parity outcome $d = x_k \oplus x_l$. The probability that he outputs a tuple $(k, l) \in \mathcal{T}_n$ with the correct parity outcome is,

$$p_{kl} = |\langle 00| \hat{T}_{kl} \cdot O^\dagger |00\rangle|^2 = \frac{2}{n^2} \tag{5.13}$$

where $\hat{T}^\dagger_{kl} = \frac{1}{2\sqrt{2}}\Big(((-1)^{x_k} + (-1)^{x_l})(\hat{c}^\dagger_k \hat{c}^\dagger_l - \hat{d}^\dagger_k \hat{d}^\dagger_l) + ((-1)^{x_k} - (-1)^{x_l})(\hat{c}^\dagger_k \hat{d}^\dagger_l - \hat{d}^\dagger_k \hat{c}^\dagger_l)\Big)$ is the operator corresponding to the correct parity outcome for the tuple (k, l).

We now define our private-key quantum money scheme using the verification protocol based on the Sampling Matching scheme.

5.4 Private-key Quantum Money Scheme

In this section we propose our private-key quantum money scheme. This scheme involves a trusted money producing entity, the *Bank*, untrusted note holders, and trusted note verifiers. The features of our money scheme are the following:

- Multiple note re-usability feature, meaning the same note can be reused by the holder a number (linear in the size of the note) of times,
- Single round of classical interaction between the note verifier and the *Bank*,
- Security of up to 21.4% noise against any all powerful note adversary.

We divide our quantum money scheme into two phases. First is the *Note preparation phase*, where the *Bank* chooses multiple n-bit binary strings independently and randomly. The *Bank* takes each of these individual strings and encodes them into a single photon state in superposition over n modes. The quantum note $\$$ of the *Bank* is then the tensor product of single photon states corresponding to all the input strings. This is then distributed among the untrusted holders. In the *Verification phase*, a note holder who wants to use his note for transaction, sends it to the verifier. Upon receiving the note, the verifier randomly selects some copies of the note state (here the note consists of multiple copies, where one copy corresponds to the single photon state that encodes one n-bit string). He then runs the verification protocol using the Sampling Matching, SM scheme (Section 5.3.2). He locally checks if the statistics of the measurement outcome obtained by running the SM-scheme is what he should expect from an honest note holder. If he finds discrepancies, then he rejects the note. If the note passes this test, then the outcomes from the SM-scheme are classically

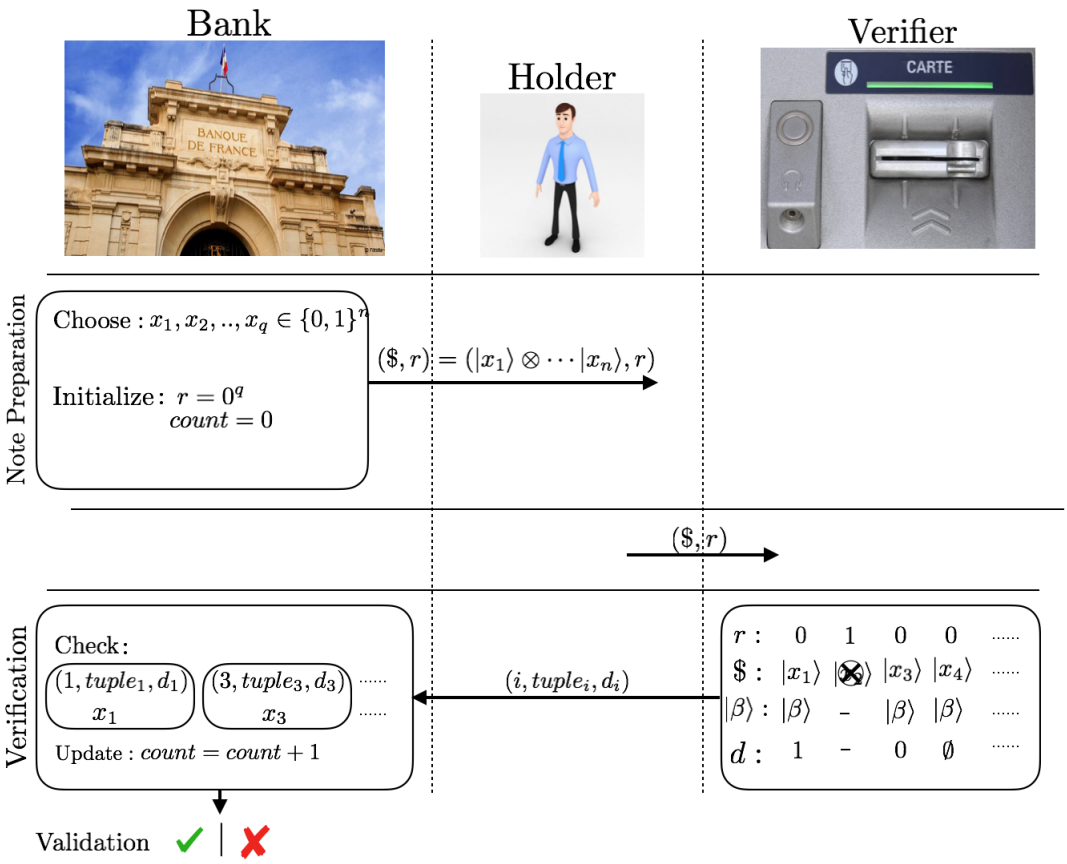

Figure 5.4: Illustration of our quantum money scheme based on the verification protocol using the SM-scheme. In the *Note Preparation* phase, the *Bank* independently and randomly selects q n-bit binary strings and produces single photon superposition note states $\$ = |x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_q\rangle$. The *Bank* further initializes the r register to keep a track of the number of positions in $[q]$ where the states have been used for verification and the $count$ register to keep track of number of verification attempts on the note. The note is then sent to the holder. To be able to carry out any transaction, the holder sends the note to an honest verifier. In the *Verification* phase, the verifier selects a fraction of the q copies of the note state which have an $r = 0$. He creates his local state $|\beta\rangle$ and applies the SM-scheme on those selected copies. The verifier sends the outcome of the measurement scheme to the *Bank*. Finally the *Bank* compares the outcomes with his secret string x_j's and outputs a bit Ver_H^B stating whether the note is valid or not.

communicated with the *Bank*. The *Bank* compares these outcomes with the his private n-bit strings. If a high fraction of the outcomes are correct, then he outputs the bit $\text{Ver}_H^B = 1$ implying that the note is valid. Otherwise, he outputs $\text{Ver}_H^B = 0$.

The money scheme we use here is the **quantum money mini-scheme**. Under this scheme

the *Bank* produces one quantum note \$, consisting of many copies of single photon states. The goal of the note adversary is, after finite interactions with the Bank, to produce two quantum notes $\$_1$ and $\$_2$ which successfully passes the verification test by two independent verifiers. We have already emphasized that the security against any adversary in the quantum money mini-scheme is enough to guarantee the security in the full fledged private-key quantum money scheme with multiple notes and a classical serial number assigned to them.

We now describe the quantum money mini-scheme based on single photon states, linear optics transformations and photon number resolving detectors.

5.4.1 Note Preparation Phase

1. The *Bank* independently and randomly chooses q n-bit binary strings $x_1, x_2, .., x_q \in \{0,1\}^n$

2. The *Bank* encodes each the binary string x_j into the single photon state in superposition over n modes,

$$|x_j\rangle = \frac{1}{\sqrt{n}} \sum_{k=1}^{n} (-1)^{x_{j,k}} \hat{a}_k^\dagger |0\rangle \tag{5.14}$$

   where $x_{j,k}$ is the k^{th} bit value of string x_j and $\hat{a}_k^\dagger$ is the creation operator for the mode k with $\hat{a}_k^\dagger |0\rangle = |1\rangle_k$.

3. The *Bank* creates a classical binary register r and initializes it to 0^q. This register keeps the track of positions j where the states have been used for the verification.

4. The *Bank* creates a counter variable $count$ and initializes it to 0. This keeps a track of the number of verification attempts.

5. The *Bank* sends the quantum note (\$, r) to the holder.

5.4.2 Verification Phase

Once the *Bank* distributes the notes, the holder in order to be able to carry out any transaction, has to get the note verified from an honest verifier Ver. The verification procedure is listed below.

Local testing

1. The holder gives the note $\$'(=: \$$ if the holder is honest) to Ver.

2. Ver checks the re-usability of the note by verifying that the hamming distance of r register $d(r, 0^q) \leqslant T$, where T is a predefined maximum number of copies in the note that are allowed for verification. If $d(r, 0^q) > T$, the note is rendered useless and must be returned to the *Bank*.

3. Ver uniformly and randomly selects a subset $L \subset [q]$ copies from the states marked $r = 0$. He marks all the corresponding L copies in the r register to 1.

4. For each chosen copy $j \in L$, Ver prepares his local coherent state $|\beta\rangle = \frac{1}{\sqrt{n}} \sum_{k=1}^{n} \hat{b}_k^\dagger |0\rangle$ and runs the SM scheme (Section 5.7.1). Here $\hat{b}_k$ is the creation operator for the mode k with $\hat{b}_k^\dagger |0\rangle = |1'\rangle_k$.

5. Ver first checks if he gets 2 photon clicks in all the chosen L copies. If not, he rejects.

6. Ver counts the number of successful copies l_{succ}, where he obtains two single photon clicks in two different modes. For these copies he outputs the parity outcome $d_j = x_{j,k} \oplus x_{j,l}$ where the clicks have been obtained in times modes k and l. For the rest of the copies, he sets $d_j = \emptyset$.

7. Ver checks if $l_{succ} \geqslant l_{min}$, where $l_{min} = \mathbb{E}_h[l_{succ}](1 - \varepsilon)$ is the minimum number of copies that will locally guarantee his acceptance of the note, where $0 \leqslant \varepsilon \leqslant 1$ is the security factor. Here $\mathbb{E}_h[l_{succ}]$ is the expected number of copies where the honest note holder obtains two single photon clicks in two different modes when Ver runs the SM scheme.

8. Ver proceeds to the communication with the *Bank* only when the note passes this test.

Communication with the *Bank*

9. Ver forwards the outcomes $\{j \in L, (k, l), d_j\}$ to the *Bank*.

10. The *Bank* checks if $count < \lceil \frac{T}{|L|} \rceil$, otherwise he renders the verification attempt as invalid.

11. For each copy $j \in L$ with $d_j \neq \emptyset$, the *Bank* compares the parity value d_j with the secret string x_j. He validates the note if the number of correct outcomes

$$l_{succ}^{cor} \geqslant \mathbb{E}_h[l_{succ}^{cor}](1 - \delta) \tag{5.15}$$

where $\mathbb{E}_h[l_{succ}^{cor}]$ is the expected number of copies that give the correct parity outcome when the note holder is honest, and $0 \leqslant \delta \leqslant 1$ is a positive constant.

12. The *Bank* updates the $count$ by 1.

Note: The optimal values of ε and δ in the scheme are determined by the forging probability of the adversary. This is explained in further sections.

5.5 Correctness

In this section we compute the probability that an honest note holder fails the verification test. We use the Chernoff-Hoeffding inequality to prove our results.

We first remark that the note holder always passes the step 5 of the *Verification phase*, since he sends the entire *Bank* note to the verifier Ver, who after performing the SM-scheme on the chosen L copies, always obtains the two photon clicks.

However, the note holder can fail the step 7 of the *Verification phase* if the number of successful copies, where he obtains two single photon clicks in two different time modes, $l_{succ} < l_{min} = \mathbb{E}[l_{succ}](1-\varepsilon)$, where $\mathbb{E}[l_{succ}]$ is the expected number of copies where Ver obtains two single photon clicks in two different modes when he runs the SM scheme, and ε is the security parameter chosen by Ver. Eq.(5.12) tells us that for each of these chosen copy $j \in L$, the probability that the verifier obtains two single clicks in two different time modes is,

$$p_{11} = 1 - \frac{1}{n} \tag{5.16}$$

Thus for L copies chosen from the holder note state, the expected number of successful outcomes by Ver is,

$$\mathbb{E}[l_{succ}] = |L| p_{11} \tag{5.17}$$

Using the Chernoff-Hoeffding bound, the probability that the holder fails this test is,

$$\mathbb{P}[l_{succ} < l_{min}] \leqslant \exp\left(-\frac{2\varepsilon^2 \mathbb{E}^2[l_{succ}]}{|L|}\right) = \exp(-2\varepsilon^2 p_{11}^2 |L|) \tag{5.18}$$

If the note passes this local test of Ver then the honest note holder always passes the verification test of the *Bank*. This is because across all the l_{succ} copies that Ver sends to the Bank, the probability that the Bank obtains the correct parity outcome is $c = 1$. This implies $l_{succ}^{cor} = l_{succ}$.

Thus the probability that the honest holder fails the verification test is,

$$\mathbb{P}[\text{Honest fail}] = \mathbb{P}[l_{succ} < l_{min}] \leqslant \exp(-2\varepsilon^2 p_{11}^2 |L|) \tag{5.19}$$

5.6 Unforgeability of Bank notes

In this section, we explicitly calculate the forging probability for the adversary when he tries to duplicate the *Bank* note \$, to be able to pass the verification tests from two verifiers, Ver1 and Ver2, simultaneously. Our proof utilises the results of the proof by Amiri et al [AA17] where they prove the unforgeability of the *Bank* notes when the verifier uses the Hidden Matching verification scheme [BYJK04].

Here we look at the security proof when the *Bank* encodes his note states as single photon superposition states. In the unforgeability proof, we assume that the adversary has in possession a valid *Bank* note. From this valid note, he wants to create to two notes that pass verification test of the verifiers, Ver1 and Ver2.

First we address one forging technique based on the manipulation of the r register by the adversary. Since in each verification, the verifier chooses $|L|$ copies and the maximum number of verification attempts of the note is T, hence the adversary is allowed to set at most $(T-1)|L|$ of the r register to 1. Suppose the adversary creates two notes (δ_1, r_1) and (δ_2, r_2) and sends it to the verifiers Ver1 and Ver2 respectively. If the adversary sets $r_1(j) = 0$ and $r_2(j) = 1$ for the j-th copy, then he is sure that Ver2 would not select that state for verification. This way he can set at max $(T-1)|L|$ copies of r_1 and r_2 register to 1. In the copies where he has set $r_1 = 1$, he can send the *Bank* note states to Ver2, and similarly for the copies where he has set $r_2 = 1$, he can send *Bank* note states to Ver1. This results in him exactly replicating the $2(T-1)|L|$ copies of the note state for both verifiers. This strategy also considers the worst case adaptive attack, where the adversary applies the auxiliary verification attempt on at most $T|L|$ permissible copies, and completely obtains the information of the state for those copies. Thus now he has complete information of $(3T-2)|L|$ copies of the note state.

Now to prove the unforgeability condition, we consider what happens in the remaining $q' = q - (3T-2)|L|$ copies of the states sent to Ver1 and Ver2 where the adversary has no auxiliary information of the states and for which $r_1(j)$ and $r_2(j)$ are 0. Our structure of the unforgeability proof is to relate the forging probability of the adversary to the average fidelity of the remaining q' states of Ver1 and Ver2 with the honest note state. An optimal attack would correspond to maximization of the average fidelity, which can be written as a semi definite problem (SDP). Solving this gives us an upper bound on the average forging probability of the adversary.

First we remark that the adversary has to send a state across each these q' copies to Ver1 and Ver2, because otherwise he fails the step 5 test in *Verification phase* with certainty.

Now suppose for the copy $j \in [q']$, the adversary has the honest note state,

$$|x_j\rangle = \frac{1}{\sqrt{n}} \sum_{k=1}^{n} (-1)^{x_{j,k}} \hat{a}_k^\dagger |0\rangle \,, \tag{5.20}$$

The adversary uses this note to create two states, η_{x_j} and τ_{x_j} and sends them to Ver1 and Ver2 respectively. We consider the normalized mixed state sent to Ver1,

$$\eta_{x_j} = \sum_{k,l}^{n} A_{kl} \hat{a}_k^\dagger |0\rangle \langle 0| \hat{a}_l \tag{5.21}$$

where $\hat{a}_k^\dagger$ is the creation operator of the k^{th} mode, and the normalization factor being $\sum_{k=1}^{n} A_{kk} = 1$.

Ver1 now runs the SM-scheme as shown in Figure 5.3. The input of the interaction of the mixed adversary state with the local state of Ver1 $|\beta\rangle = \frac{1}{\sqrt{n}} \sum_{k=1}^{n} \hat{b}_k^\dagger |0\rangle$ results in the combined mixed state,

$$\begin{aligned} \eta_j^{In} &= |\beta\rangle \otimes \eta_{x_j} \otimes \langle\beta| \\ &= \frac{1}{n}\left(\sum_{k=1}^{n} \hat{b}_k^\dagger |0\rangle \otimes \sum_{l,m}^{n} A_{lm} \hat{a}_l^\dagger |0\rangle \langle 0| \hat{a}_m \otimes \sum_{o=1}^{n} \langle 0| \hat{b}_o \right) \end{aligned} \tag{5.22}$$

while the output of the the state after the n-beam splitter interaction is,

$$\begin{aligned} \eta_j^{Out} = \frac{1}{4n}\Bigg(& \sum_{k=1}^{n} (\hat{c}_k^\dagger - \hat{d}_k^\dagger) |0\rangle \ \otimes \\ & \sum_{l,m=1}^{n} A_{lm} (\hat{c}_l^\dagger + \hat{d}_l^\dagger) |0\rangle \langle 0| (\hat{c}_m + \hat{d}_m) \ \otimes \\ & \sum_{o=1}^{n} \langle 0| (\hat{c}_o - \hat{d}_o) \Bigg) \end{aligned} \tag{5.23}$$

Now let us look at the probability with which Ver1 observes 2 photons in the same mode $\hat{c}_k$,

$$p_2^{\hat{c}_k} = \langle 00| \hat{c}_k^2 \cdot \eta_j^{Out} \cdot \hat{c}_k^{\dagger 2} |00\rangle = \frac{A_{kk}}{2n} \tag{5.24}$$

Similarly, the probability of having 2 photons in the same mode $\hat{d}_k$ is,

$$p_2^{\hat{d}_k} = |\langle 00| \hat{d}_k^2 \cdot \eta_j^{Out} \cdot \hat{d}_k^{\dagger 2} |00\rangle = \frac{A_{kk}}{2n} \tag{5.25}$$

Over all the n modes, the total probability of having 2 photons in the same mode is

$$p_2 = \sum_{k=1}^{n} p_2^{\hat{c}_k} + p_2^{\hat{d}_k} = \sum_{k=1}^{n} \frac{A_{kk}}{n} = \frac{1}{n} \tag{5.26}$$

Comparing Eq.(5.12) and Eq.(5.26), we see that the total probability of obtaining 2 photons in the same mode for an adversary is the same as that for an honest note holder. Thus even for the adversarial state, Ver1 receives two single photons in different modes with a probability $p_{11} = 1 - \frac{1}{n}$.

Thus over the L copies chosen by Ver1, he receives on average $|L|p_{11}$ copies with 2 single clicks in different modes. This implies that the adversary passes the local step 7 of Ver1's *Verification Phase* test with the probability,

$$\mathbb{P}[\text{Ver1 accepts}] = \mathbb{P}[l_{succ} \geqslant l_{min}] \geqslant 1 - \exp(-2\varepsilon^2 p_{11}^2 |L|) \tag{5.27}$$

where l_{succ} is the total copies where he gets single photon clicks in two different modes and $l_{min} = |L|p_{11}(1-\varepsilon)$.

Now suppose that adversary passes this test. Then Ver1 communicates the parity outcomes of l_{succ} copies to the *Bank*. According to Eq.(5.9), Ver1 correctly outputs the parity $x_{j,e} \oplus x_{j,f}$ of a particular tuple $(e, f) \in \mathcal{T}_n$ if he operates $\hat{T}^{\dagger}_{ef} = \frac{1}{2\sqrt{2}}\Big((-1)^{x_{j,e}}(\hat{c}^{\dagger}_e\hat{c}^{\dagger}_f - \hat{d}^{\dagger}_e\hat{d}^{\dagger}_f + \hat{c}^{\dagger}_e\hat{d}^{\dagger}_f - \hat{d}^{\dagger}_e\hat{c}^{\dagger}_f) + (-1)^{x_{j,f}}(\hat{c}^{\dagger}_f\hat{c}^{\dagger}_e - \hat{d}^{\dagger}_f\hat{d}^{\dagger}_e + \hat{c}^{\dagger}_f\hat{d}^{\dagger}_e - \hat{d}^{\dagger}_f\hat{c}^{\dagger}_e)\Big)$ on the state η_j^{Out}.

An incorrect outcome is obtained when he incorrectly outputs the parity outcome $x_{j,e} \oplus x_{j,f}$ of the tuple (e, f). This happens when the outcome is of the form,

$$\hat{I}^{\dagger}_{ef}\,|00\rangle = \frac{1}{2\sqrt{2}}\Big((-1)^{x_{j,e}}(\hat{c}^{\dagger}_e\hat{c}^{\dagger}_f - \hat{d}^{\dagger}_e\hat{d}^{\dagger}_f + \hat{c}^{\dagger}_e\hat{d}^{\dagger}_f - \hat{d}^{\dagger}_e\hat{c}^{\dagger}_f) - (-1)^{x_{j,f}}(\hat{c}^{\dagger}_f\hat{c}^{\dagger}_e - \hat{d}^{\dagger}_f\hat{d}^{\dagger}_e + \hat{c}^{\dagger}_f\hat{d}^{\dagger}_e - \hat{d}^{\dagger}_f\hat{c}^{\dagger}_e)\Big)\,|00\rangle \tag{5.28}$$

The probability of obtaining an incorrect parity outcome for the tuple $(e, f) \in \mathcal{T}_n$ is,

$$p^{ef}_{Ver1} = \langle 00|\,\hat{I}_{ef} \cdot \eta_j^{Out} \cdot \hat{I}^{\dagger}_{ef}\,|00\rangle \tag{5.29}$$

Over all the tuples in $\mathcal{T}_n$, the probability of having an incorrect outcome is,

$$\begin{aligned} p^{x_j}_{Ver1} &= \sum_{(e,f)\in\mathcal{T}_n} p^{ef}_{Ver1} \\ &= \frac{1}{2n}\sum_{(e,f)\in\mathcal{T}_n}(A_{ee} + A_{ff} - (-1)^{x_{j,e}\oplus x_{j,f}}(A_{ef} + A_{fe})) \\ &= \frac{1}{2n}\sum_{e,f}^{n}(n - n(-1)^{x_{j,e}\oplus x_{j,f}}A_{ef}) \\ &= \frac{1}{2}(1 - F_{x_j}) \end{aligned} \tag{5.30}$$

where, $F_{x_j} = \langle x_j|\,\eta_{x_j}\,|x_j\rangle = \frac{1}{n}\sum_{e,f}^{n}(-1)^{x_{j,e}\oplus x_{j,f}}A_{ef}$.

Now since the adversary does not know the secret string x_j, instead of having the state Eq.(5.21), he instead holds the mixture $\eta = \frac{1}{2^n}\sum_{x_j}\eta_{x_j}$. Thus the error probability for Ver1 averaged over all possible x_j values is,

$$\begin{aligned} p_{Ver1} &= \frac{1}{2^n}\sum_{x_j} p^{x_j}_{Ver1} \\ &= \frac{1}{2}(1 - F) \end{aligned} \tag{5.31}$$

where $F = \frac{1}{2^n}\sum_{x_j} F_{x_j}$.

Similarly, for Ver2, who receives the mixed state τ_{x_j}, the fidelity with the honest note state is $G_{x_j} = \langle x_j|\,\tau_{x_j}\,|x_j\rangle$. The average error probability of obtaining an incorrect outcome is $p_{Ver2} = \frac{1}{2}(1 - G)$, where $G = \frac{1}{2^n}\sum_{x_j} G_{x_j}$.

Thus the combined average error probability of Ver1 and Ver2 is

$$p_{Ver1} + p_{Ver2} = 1 - \frac{F+G}{2} \tag{5.32}$$

This problem can be cast as SDP, where the objective is to find a lower bound of the combined average probability of obtaining an incorrect outcome for Ver1 and Ver2. This amounts to maximizing the average fidelity

$$\bar{F} = \frac{F+G}{2}$$

.

Amiri et al [AA17] numerically solved this SDP for $n \leqslant 14$ and verified that

$$\bar{F} \leqslant \frac{1}{2} + \frac{1}{n} \tag{5.33}$$

They further conjecture that it is true for any n. Eq.(5.33) allows us to give a lower bound on the average probability of giving an incorrect outcome for Ver1 and Ver2.

$$\begin{aligned} p_{Ver1} + p_{Ver2} &= 1 - \frac{1}{2}(F+G) \\ &\geqslant \frac{1}{2} - \frac{1}{n} \end{aligned} \tag{5.34}$$

This is the probability for a single copy j chosen by the verifier. The verifier chooses randomly and uniformly chooses L states from the q copies of the states from the holder. Using the teleportation argument of Clarke and Kent [CK12], it can be shown that this lower bound on error probability Eq.(5.34) is the same for all the L copies. This implies that the verifier's error probability for a copy remains the same, irrespective of the outcome of previous copies. Since Eq.(5.34) is gives us a lower bound on the average error probability for both verifiers, this implies that one verifier, lets say Ver1, must definitely have an error probability e_{min} at least

$$e_{min} = \frac{1}{4} - \frac{1}{2n} \tag{5.35}$$

The above error probability has been calculated for $q' = q - (3T-2)|L|$ copies. Over the remaining $q - q' = (3T-2)|L|$ copies, since the adversary has full information of the state, his error probability is 0. Thus the average error probability for Ver1 across the l_{succ} copies with not-null parity outcomes is,

$$e_{min} = \frac{q-(3T-2)|L|}{q-(T-1)|L|}\Big(\frac{1}{4} - \frac{1}{2n}\Big) \tag{5.36}$$

Suppose, $T|L| = \lambda q$, for some small fraction $\lambda < 1$ (for example $1/1000$), then Eq.(5.36) is,

$$e_{min} \approx \frac{997}{999}\Big(\frac{1}{4} - \frac{1}{2n}\Big) \approx \frac{1}{4} - \frac{1}{2n} \tag{5.37}$$

We know that if the holder is honest then the probability of him obtaining the correct parity outcomes across all the l_{succ} copies is $c = 1$. From Eq.(5.37), we see that for the adversary, this is $c_{\text{adv}} = 1 - e_{min}$. We define the cut-off $\delta = (c - c_{\text{adv}})/2$. Then using the Chernoff-Hoeffding bound, the probability that adversary's note passes the test of *Verification Phase* by both Ver1 and Ver2 is,

$$\begin{aligned}
&\mathbb{P}[\text{Ver1 and Ver2 accept}] \cdot \mathbb{P}[\text{Ver1}_H^B = 1 \text{ and Ver2}_H^B = 1 | \text{Ver1 and Ver2 accept}] \\
&\leqslant \mathbb{P}[\text{Ver1 accepts}] \cdot \mathbb{P}[\text{Ver1}_H^B = 1 | \text{Ver1 accepts}] \\
&\leqslant \mathbb{P}[\text{Ver1}_H^B = 1 | \text{Ver1 accepts}] \\
&\leqslant \exp(-2\delta l_{min}^2)
\end{aligned} \tag{5.38}$$

The condition $c > c_{\text{adv}}$ always holds as long as $n > 2$, hence the probability that both verifiers pass the verification test is exponentially low. Since the Eq.(5.33) has been verified until $n = 14$, the maximum error tolerance of the scheme is up to 21.4%. However, if the conjecture by [AA17] holds true, then the maximum noise asymptotic noise tolerance of 25% can be achieved with this scheme.

5.7 Quantum Money scheme with Coherent States

In this section, we propose the private-key quantum money scheme when the *Bank* encodes the secret strings as attenuated coherent states instead of the single photon superposition states. The verification step by the honest verifier involves performing the Sampling Matching scheme where he interacts the holder's states with his local coherent uniform state. The advantage of the Sampling Matching verification protocol in coherent state formalism is that the verifier, irrespective of the input size n of each copy of the bank note, requires only a single beam splitter to interact the holder's states with his local state, and two single photon threshold detectors to collect the photon clicks. From the above analysis in single photon encoding, we see that the cut-off $\delta = (c - c_{\text{adv}})/2$ increases with the size n. Thus going to larger n makes it harder for an adversary to duplicate the *Bank* note and successfully pass the verification protocol by two independent verifiers. Our Sampling Matching verification scheme in the coherent setting is an ideal experimentally motivated framework to go to large enough size n leading to a more robust quantum money scheme.

We start by first describing the Sampling Matching scheme when one party Alice sends a coherent state to Bob, who interacts Alice's state with his local state to output parity outcome of a tuple $(k, l) \in \mathcal{T}_n$. In the next section we describe our money mini-scheme using the Sampling Matching protocol as the verification scheme. Towards the end we analyse our money scheme for correctness and unforgeability condition in presence of experimental imperfection model.

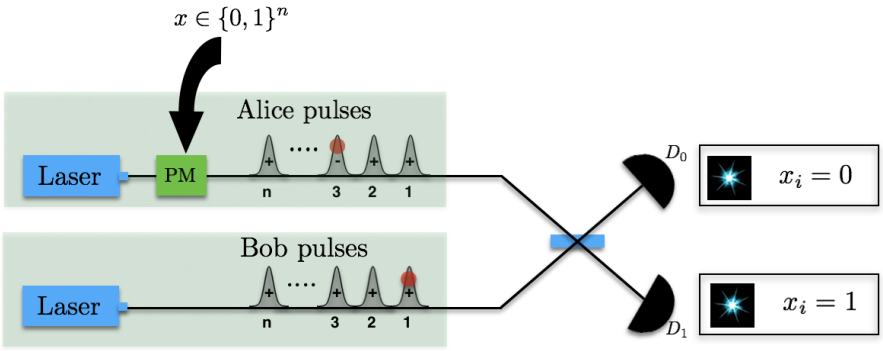

Figure 5.5: Sampling Matching (SM) circuit implementation using attenuated coherent states, 50/50 beam splitter (BS) and single photon threshold detectors. The upper arm illustrates honest Alice's state as a coherent state $|\alpha_x\rangle$, which consists of sequence of coherent pulses. The coherent state is encoded with a random phase $x \in \{0,1\}^n$ through the phase modulator (PM). The lower arm is used by Bob to produce a local reference coherent state $|\beta\rangle$, consisting of a sequence of coherent pulses, with an average photon number of 1. Bob interferes the states into the 50/50 BS and infers the parity information from the detector clicks in D_0 and D_1. This allows Bob to obtain the parity outcome of a tuple in $\mathcal{T}_n$. The red dot in the 1^{st} and 3^{rd} time sequence denotes that Bob observed clicks at D_1 and D_0 detectors respectively for these time steps. Thus he infers the parity outcome for the tuple $(1,3)$, $x_1 \oplus x_3 = 1$.

5.7.1 Sampling Matching (SM) Scheme with Coherent States

As we have already emphasised in the Section 5.3.2, Sampling Matching scheme is the testing scheme for Bob to extract the parity outcome of a tuple from the perfect disjoint set $\mathcal{T}_n$ containing $n(n-1)/2$ distinct tuples. Here we look at the testing scheme when Alice sends a coherent state to Bob.

The technique, as depicted in Figure 5.5, is the following: When an honest Alice receives the binary string $x \in \{0,1\}^n$, she encodes this information of the string into the coherent state $|\alpha_x\rangle$ and sends it to Bob,

$$|\alpha_x\rangle = \bigotimes_{k=1}^{n} |(-1)^{x_j} \frac{1}{\sqrt{n}}\rangle_k \tag{5.39}$$

where $|\alpha_x\rangle$ is the sequence of n coherent pulses with amplitude $\frac{1}{n}$ in each of the modes.

Bob prepares his local coherent state consisting of a sequence of n coherent pulses in n modes.

$$|\beta\rangle = \bigotimes_{k=1}^{n} |\frac{1}{\sqrt{n}}\rangle_k \tag{5.40}$$

He then sequentially mode-by-mode interacts his local pulses with Alice's incoming pulses. The interaction is via the 50/50 beam splitter (BS). In absence of any experimental

imperfections, the coherent pulse modes at the input of Bob's BS in k-th step are,

$$|(-1)^{x_k}\frac{1}{\sqrt{n}}\rangle_k \otimes |\frac{1}{\sqrt{n}}\rangle_k , \tag{5.41}$$

and the output modes are,

$$|\frac{(1+(-1)^{x_k})}{\sqrt{2}}\frac{1}{\sqrt{n}}\rangle_{k,D_0} \otimes |\frac{(1-(-1)^{x_k})}{\sqrt{2}}\frac{1}{\sqrt{n}}\rangle_{k,D_1} \tag{5.42}$$

The output modes are fed into the single photon threshold detectors D_0 and D_1 to observe the clicks. When any coherent state $|\alpha\rangle$ is incident on the threshold detector, then the probability of the click is given by,

$$p_c = 1 - \exp(-|\alpha|^2) \tag{5.43}$$

Let us see how Bob obtains the parity outcomes of one of the tuples in $\mathcal{T}_n$ from the detector clicks. The output state in Eq.(5.42) denotes that the detector D_0 clicks iff $x_k = 0$ while D_1 clicks iff $x_k = 1$. For Bob to output a parity outcome a tuple with certainty, he needs to obtain single photon clicks in the detectors at two different time modes. Bob decides that he would output the parity outcome only if he receives exactly two single photon clicks at two different time modes. The probability that he obtains exactly two clicks in two different time modes is,

$$p_{11} = \binom{n}{2} p_1^2 (1-p_1)^{n-2} \tag{5.44}$$

where $p_1 = 1 - \exp(-\frac{2}{n})$ is the probability of observing a single click in one time mode.

Now suppose Bob observes the clicks in the k-th and l-th time modes are in detectors D_0 and D_1 respectively. This implies $d = x_k \oplus x_l = 1$. This enables Bob to output the parity outcome of $(k, l) \in \mathcal{T}_n$.

If on the other hand, Bob does not obtain exactly two clicks in two different time modes, then he outputs the parity outcome $d = \emptyset$.

5.7.2 Private-key Quantum Money Scheme

In this section we propose our private-key quantum money mini-scheme using coherent states. We divide our quantum money scheme into two phases. First is the *Note preparation phase*, where the *Bank* chooses multiple n-bit binary strings independently and randomly. The *Bank* takes each of these individual strings and adds a randomized phase in $[0, 2\pi]$ to produce the attenuated coherent states. The quantum note \$ of the *Bank* is then the combined tensor product of coherent states corresponding to all the input strings. This is then distributed among the untrusted holders. In the *Verification phase*, a note holder who wants to use his note for transaction, sends it to the verifier. Upon receiving the note, the verifier randomly

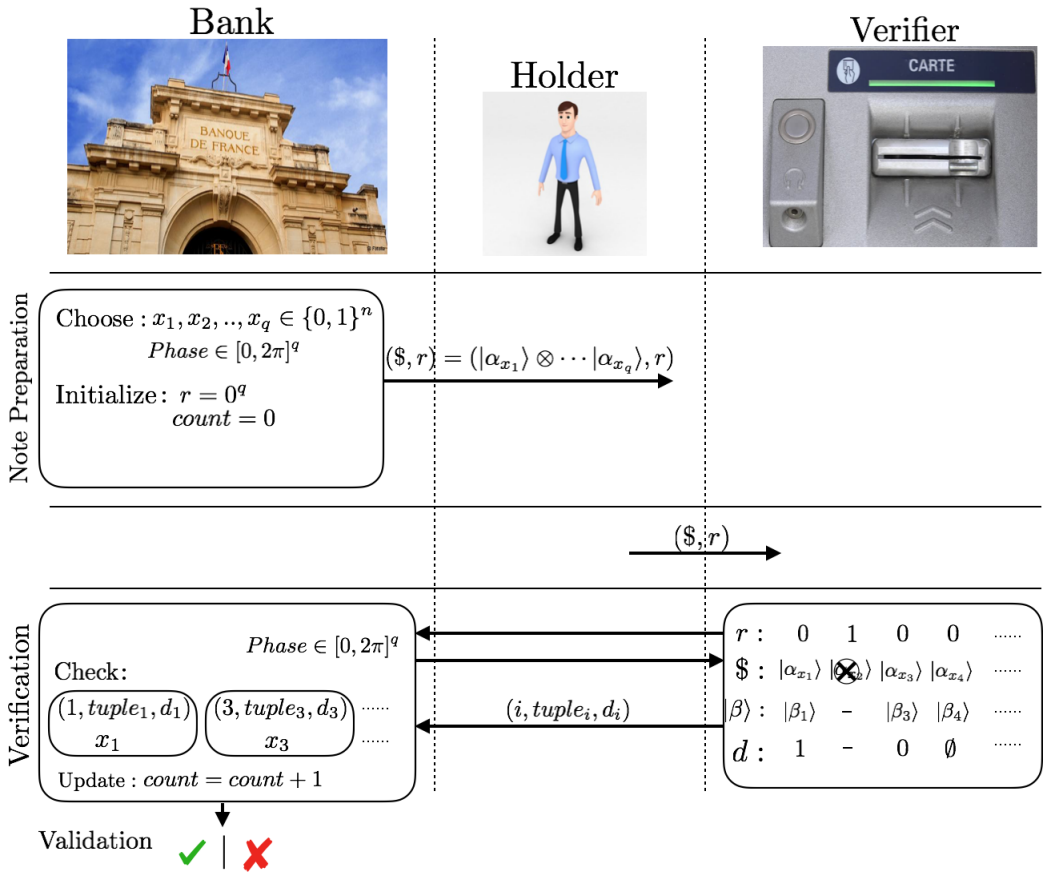

Figure 5.6: Illustration of our quantum money scheme based on the verification protocol using the SM-scheme. In the *Note Preparation* phase, the *Bank* independently and randomly selects q n-bit binary strings and produces phase randomized note coherent states $\$ = |\alpha_{x_1}\rangle \otimes |\alpha_{x_2}\rangle \otimes \cdots \otimes |\alpha_{x_q}\rangle$, where each coherent state $|\alpha_{x_j}\rangle$ is phase randomized with $\theta_j \in [0, 2\pi]$. The *Bank* stores the phase randomization information in the register *Phase*$\in [0, 2\pi]^q$. The *Bank* further initializes the r register to keep a track of the number of positions in $[q]$ where the states have been used for verification and the $count$ register to keep track of number of verification attempts on the note. The note is then sent to the holder. To be able to carry out any transaction, the holder sends the note to an honest verifier. In the *Verification* phase, the verifier selects a fraction of the q copies of the note state which have an $r = 0$. The verifier queries the phase randomization information of the selected copies from the *Bank*. He then creates his local state $|\beta_j\rangle$ and applies the SM-scheme on those selected copies. The verifier sends the outcome of the measurement scheme to the *Bank*. Finally the *Bank* compares the outcomes with his secret string x_j's and outputs a bit Ver_H^B stating whether the note is valid or not.

selects some copies of the note state (here the note consists of multiple copies, where one copy

corresponds to the coherent state that encodes one n-bit string). He then queries the phase randomized information of those selected copies from the *Bank* and runs the verification protocol using the Sampling Matching, SM scheme (Section 5.7.1). He then locally checks if the statistics of the measurement outcome obtained by running the SM-scheme is what he should expect from an honest note holder. If he finds discrepancies, then he rejects the note. If the note passes this test, then the outcomes from the SM-scheme are classically communicated with the *Bank*. The *Bank* compares these outcomes with his private n-bit strings. If a high fraction of the outcomes are correct, then he outputs the bit $\text{Ver}_H^B = 1$ implying that the note is valid. Otherwise, he outputs $\text{Ver}_H^B = 0$.

In the section where we talk about the unforgeability of the note against an adversary, we emphasize on the importance of phase randomization of the note states by the *Bank*. We effectively show that without this condition, the note adversary can possibly use the unambiguous state discrimination attack, which allows him to forge the note with substantially high probability. This is one of the possible attacks by the adversary. In general, the adversary could use an optimal POVM technique to cheat with a non-negligible probability.

We now describe the quantum money mini-scheme based on attenuated coherent states, linear optics transformations and single photon threshold detectors.

5.7.3 Note Preparation Phase

1. The *Bank* independently and randomly chooses q n-bit binary strings $x_1, x_2, .., x_q \in \{0,1\}^n$

2. The *Bank* encodes each the binary string x_j into the phase randomized coherent state $|\alpha_{x_j}\rangle$, with an average photon number 1,

$$|\alpha_{x_j}\rangle = \bigotimes_{k=1}^{n} |e^{i\theta_j}(-1)^{x_{j,k}} \frac{1}{\sqrt{n}}\rangle_k \tag{5.45}$$

   where $x_{j,k}$ is the k^{th} bit value of string x_j, and $\theta_j \in [0, 2\pi]$ is a random phase chosen by the *Bank* for all $j \in [q]$. The coherent state $|\alpha_{x_j}\rangle$ is a sequence of n coherent pulses in n modes.

3. The Bank stores this phase information in the classical register $Phase \in [0, 2\pi]^q$.

4. The *Bank* creates a classical binary register r and initializes it to 0^q. This register keeps the track of positions j where the states have been used for the verification.

5. The Bank creates a counter variable $count$ and initializes it to 0. This keeps a track of the number of verification attempts.

6. The *Bank* sends the quantum note (\$, r) to the holder.

5.7.4 Verification Phase

Once the *Bank* distributes the notes, the holder in order to be able to carry out any transaction, has to get the note verified from an honest verifier Ver. The verification procedure is listed below.

Local testing

1. The holder gives the note $\$'(=: \$$ if the holder is honest) to Ver.

2. Ver checks the re-usability of the note by verifying that the hamming distance of r register $d(r, 0^q) \leqslant T$, where T is a predefined maximum number of copies in the note that are allowed for verification. If $d(r, 0^q) > T$, the note is rendered useless and must be returned to the *Bank*.

3. Ver uniformly and randomly selects a subset $L \subset [q]$ copies from the states marked $r = 0$. He marks all the corresponding $|L|$ copies in the r register to 1.

4. Ver queries the *Bank* for the randomized phase information of the L copies from the *Phase* register. At this stage, *Bank* publicly broadcasts the randomized phase information of the L copies.

5. For each copy $j \in L$, Ver prepares his local coherent state $|\beta_j\rangle = \otimes_{k=1}^{n} |e^{i\theta_j} \frac{1}{\sqrt{n}}\rangle_k$ and runs the SM scheme (Section 5.7.1).

6. Ver counts the number of successful copies l_{succ}, where he obtains exactly two single photon clicks in two different time modes. For these copies he outputs the parity outcome $d_j = x_{j,k} \oplus x_{j,l}$ where the clicks have been obtained in times modes k and l. For the rest of the copies, he sets $d_j = \emptyset$.

7. Ver checks if $l_{succ} \geqslant l_{min}$, where $l_{min} = \mathbb{E}_h[l_{succ}](1 - \varepsilon)$ is the minimum number of copies that will locally guarantee his acceptance of the note, where $0 \leqslant \varepsilon \leqslant 1$ is the security factor. Here $\mathbb{E}_h[l_{succ}]$ is the expected number of copies where the honest note holder obtains exactly two single photon clicks when Ver runs the SM scheme.

8. Ver proceeds to the communication with the *Bank* only when the note passes this test.

Communication with the *Bank*

9. Ver forwards the outcomes $\{j \in L, (k, l), d_j\}$ to the *Bank*.

10. The *Bank* checks if $count < \lceil \frac{T}{|L|} \rceil$, otherwise he renders the verification attempt as invalid.

11. For each copy $j \in L$ with $d_j \neq \emptyset$, the ***Bank*** compares the parity value d_j with the secret string x_j. He validates the note if the number of correct outcomes

$$l_{succ}^{cor} \geqslant \mathbb{E}_h[l_{succ}^{cor}](1-\delta) \tag{5.46}$$

where $\mathbb{E}_h[l_{succ}^{cor}]$ is the expected number of copies that give the correct parity outcome when the note holder is honest, and $0 \leqslant \delta \leqslant 1$ is a positive constant.

12. The ***Bank*** updates the $count$ by 1.

Note: The optimal values of ε and δ in the scheme are determined by the experimental imperfection parameters and the forging probability of the adversary. This is explained in further sections.

5.8 Correctness

In this section we compute the probability that an honest note holder fails the verification test in the ideal and experimental imperfection scenario. We use the Chernoff-Hoeffding inequality to prove our results.

5.8.1 Analysis in Ideal scenario

In the ideal scenario, the note holder fails the verification test if he fails the local step 7 of the ***Verification Phase*** of Ver i.e. if the number of successful copies $l_{succ} < l_{min} = \mathbb{E}[l_{succ}](1-\varepsilon)$, where $\mathbb{E}[l_{succ}]$ is the expected number of copies where the verifier Ver obtains exactly two single photon clicks when he runs the SM scheme, and ε is the security parameter chosen by Ver. For each of these chosen copy $j \in L$, the probability that the verifier obtains exactly two single clicks in different time modes is,

$$p_{11} = \binom{n}{2} p_1^2 (1-p_1)^{n-2} \tag{5.47}$$

where $p_1 = 1 - \exp(-\frac{2}{n})$ is the probability of observing a single click in one time mode.

Thus for $|L|$ copies chosen from the holder note state, the expected number of successful outcomes by Ver is,

$$\mathbb{E}[l_{succ}] = |L| p_{11} \tag{5.48}$$

Using the Chernoff-Hoeffding bound, the probability that the holder fails this test is,

$$\mathbb{P}[l_{succ} < l_{min}] \leqslant \exp\left(-\frac{2\varepsilon^2 \mathbb{E}^2[l_{succ}]}{|L|}\right) = \exp(-2\varepsilon^2 p_{11}^2 |L|) \tag{5.49}$$

If the note passes this local test of Ver then the honest note holder always passes the verification test of the *Bank*. This is because across all the l_{succ} copies that Ver sends to the Bank, the probability that the Bank obtains the correct parity outcome is $c = 1$. This implies $l_{succ}^{cor} = l_{succ}$.

Thus the probability that the honest holder fails the verification test is,

$$\mathbb{P}[\text{Honest fail}] = \mathbb{P}[l_{succ} < l_{min}] \leqslant \exp(-2\varepsilon^2 p_{11}^2 |L|) \tag{5.50}$$

5.8.2 Analysis with experimental imperfections

We now analyse the probability that an honest note holder fails the verification test in presence of realistic experimental imperfections. This imperfection is due to three major sources:

(i) The limited detector efficiency + channel transmission loss, characterized by parameter $0 \leqslant \eta \leqslant 1$. This changes the state α to $\sqrt{\eta}\alpha$ thus reducing the probability of the verifier obtaining a click in his single photon detector by a factor η,

(ii) The limited set-up visibility $0 \leqslant \nu \leqslant 1$, which leads to a finite probability of a click in the wrong detector, and

(iii) The dark count in the detectors characterized by probability p_{dark}. In our scheme, the Bank produces coherent states with average photon number 1. Under this regime, for relatively small input sizes, the signal click probability is significantly larger than the dark count probability p_{dark} ($\sim 10^{-6}$). Thus the effect of dark counts can be safely ignored in our analysis.

In this scenario, Ver runs the SM scheme in presence of imperfections (η, ν). For each copy $j \in L$, Ver interacts the incoming holder state with his local state $|\beta_j\rangle$. The input in the Ver's beam splitter at the k-th time step is,

$$|e^{i\theta_j}(-1)^{x_{j,k}}\sqrt{\frac{\eta}{n}}\rangle_k \otimes |e^{i\theta_j}\sqrt{\frac{\eta}{n}}\rangle_k \tag{5.51}$$

and the output state is

$$\begin{aligned} &|e^{i\theta_j}\Big(\frac{(1+(-1)^{x_{j,k}})}{\sqrt{2}}\sqrt{\nu} + \frac{(1-(-1)^{x_{j,k}})}{\sqrt{2}}\sqrt{1-\nu}\Big)\sqrt{\frac{\eta}{n}}\rangle_{k,D_0} \otimes \\ &|e^{i\theta_j}\Big(\frac{(1-(-1)^{x_{j,k}})}{\sqrt{2}}\sqrt{\nu} + \frac{(1+(-1)^{x_{j,k}})}{\sqrt{2}}\sqrt{1-\nu}\Big)\sqrt{\frac{\eta}{n}}\rangle_{k,D_1} \end{aligned} \tag{5.52}$$

The contrast from the ideal setting is that, in the ideal case, at any time step, the non-zero click probability is only in the correct detector. But in presence of experimental imperfections, due to the finite visibility factor, there is a non-zero click probability of a click in both the

correct and incorrect detectors. From the Eq.(5.52), it is obvious that larger the visibility ν, more are the chances of the photons going in the correct output mode. Across each time modes, the probability of a click in the correct detector is

$$p_c = 1 - \exp(-\frac{2\eta\nu}{n}) \tag{5.53}$$

while the probability that click is in the wrong detector is

$$p_w = 1 - \exp(-\frac{2\eta(1-\nu)}{n}) \tag{5.54}$$

Similar to the ideal case, for each position $j \in L$, the probability that the verifier obtains exactly two single clicks in different time modes is,

$$p_{11} = \binom{n}{2} p_1^2 (1-p_1)^{n-2} \tag{5.55}$$

where $p_1 = p_c(1-p_w) + p_w(1-p_c)$ is the probability of observing a single click in one time mode.

Thus for $|L|$ copies chosen from the holder note state, the expected number of successful outcomes by Ver is,

$$\mathbb{E}[l_{succ}] = |L| p_{11} \tag{5.56}$$

Using the Chernoff-Hoeffding bound, the probability that the holder fails this test is,

$$\mathbb{P}[l_{succ} < l_{min}] \leqslant \exp\left(-2\frac{\varepsilon^2 \mathbb{E}^2[l_{succ}]}{|L|} \right) = \exp(-2\varepsilon^2 p_{11}^2 |L|) \tag{5.57}$$

Passing this local test of Ver does not guarantee that honest holder passes the verification test. This is because in presence of experimental imperfections, the probability that Ver runs the SM scheme and obtains the correct parity outcome for all the l_{succ} copies is $c < 1$. This is the consequence of the non-zero click probability in the wrong detector across each time step which could lead to a wrong parity outcome. The probability that Ver outputs the wrong parity value when he obtains exactly two single-click time modes is,

$$p_{\text{wrong parity}} = \frac{2p_c(1-p_w)p_w(1-p_c)}{[p_c(1-p_w) + p_w(1-p_c)]^2} \tag{5.58}$$

This implies that the probability that the outcome parity is correct is $c = 1 - p_{\text{wrong parity}}$. The expected number of correct outcome copies of the verifier is $\mathbb{E}[l_{succ}^{cor}] = l_{succ}c$. We define the cut-off $\delta = (c - c_{\text{adv}})/2$, where c_{adv} is the maximum average success probability achieved by an adversary [5.9]. Then using the Chernoff-Hoeffding bound, the probability that the honest holder fails this test is,

$$\mathbb{P}[l_{succ}^{cor} < \mathbb{E}[l_{succ}^{cor}](1-\delta)] \leqslant \exp(-2\delta^2 c^2 l_{min}) \tag{5.59}$$

The total probability that the honest note holder fails the verification test in presence of experimental imperfection, taking into account the possible failures at Ver's local step and *Bank*'s step is,

$$\mathbb{P}[\text{Honest fail}] \leqslant \exp(-2\varepsilon^2 p_{11}^2 |L|) + \exp(-2\delta^2 c^2 l_{min}) \tag{5.60}$$

The more is the cut-off value δ, the lesser is the probability of the honest note holder failing the verification test.

5.9 Unforgeability of Bank notes

In this section, we look at the idea to calculate the forging probability for the adversary when he tries to duplicate the *Bank* note \$, to be able to pass the verification tests of two verifiers, Ver1 and Ver2, simultaneously.

When the *Bank* prepares each copy the coherent state with average photon number 1, then, since the number of photons in the coherent state follows a poissonian behaviour, hence there are three cases that might emerge when the *Bank* sends these coherent states:

1. **Zero photons emitted**: If the state emitted by the *Bank* does not have any photon, then it is as if the *Bank* is sending a vacuum state. In this case the adversary cannot do much apart from inducing a 50% error rate. The probability of obtaining zero photon is $p_0 = \exp(-1)$.

2. **Exactly one photon emitted**: If the state emitted by the *Bank* has exactly 1 photon, then the state is equivalent to a single photon state . In this case, one can perform the security analysis by considering that the *Bank* is sending single photon states. This happens with a probability $p_1 = \exp(-1)$.

3. **More than one photon emitted**: When the state emitted by the *Bank* has more than one photon, then we assume the worst scenario and say that the adversary can perfectly forge the state. This happens with the probability $p_{1^+} = 1 - p_0 - p_1 = 1 - 2\exp(-1)$

Building on these ideas, we can explicitly calculate the average forging probability c_{adv} of the adversary across each copy chosen the verifier. As long as the honest holder probability c is greater than c_{adv}, we can ensure that our money scheme remains unforgeable even against an all powerful adversary. This, along with the experimental implementation of the money scheme with coherent state, is an on-going work.

In the next section we justify the need of phase randomization of the coherent states by the *Bank*, without which the adversary substantially increases his forging probability.

5.9.1 Phase Randomization

Each note produced by the Bank consists of q copies of note states with each copy $j \in [q]$ being sequence of coherent states $|\alpha_{x_j}\rangle = \bigotimes_{k=1}^{n} |e^{i\theta_j}(-1)^{x_{j,k}} \frac{1}{\sqrt{n}}\rangle_k$, where $x_{j,k}$ is the k-th bit of string $x_j \in \{0,1\}^n$, and $e^{i\theta_j}$ is the global random phase of the coherent state. We study the case when the Bank does not phase randomize the coherent states. Further, we assume that the adversary has complete information of the phase reference used by the Bank. For simplicity let us assume that the phase reference $e^{i\theta_j} = 1, \forall j \in [q]$. Now, when the Bank sends this note to the holder, then because of the phase reference information, the holder is sure that for each copy and across each time step, he receives either $|+\rangle$ coherent pulse or the $|-\rangle$ coherent pulse where,

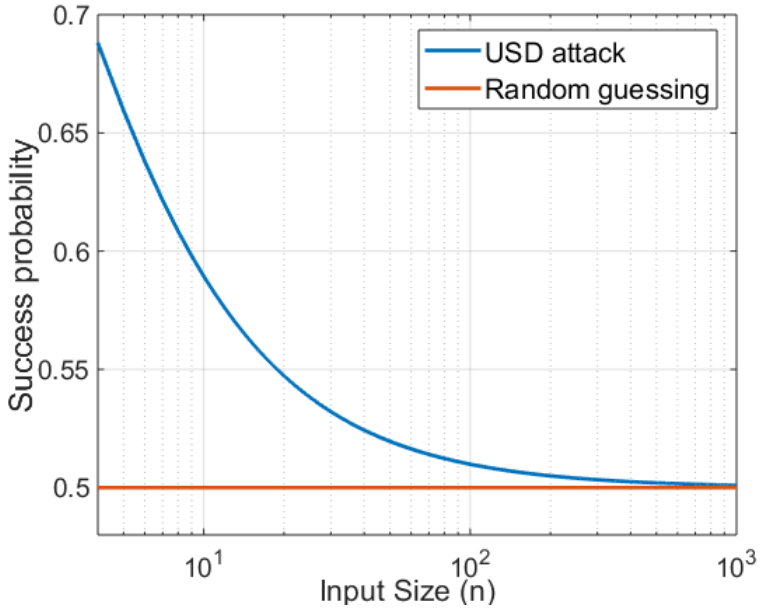

Figure 5.7: Figure comparing the success probability of the attacker to determine the bit value when he uses the USD attack vs when he just randomly guesses the bit value. Since the input n-bit string is binary encoded, the probability of the attacker to correctly guess the bit value is 0.5. In contrast, for low input sizes, the success probability of the attacker increases substantially when he uses the unambiguous state discrimination attack (USD).

$$\begin{aligned} |+\rangle &= e^{-1/n}(|0\rangle + \frac{1}{\sqrt{n}}|1\rangle + \frac{1}{2n}|2\rangle ..), \\ |-\rangle &= e^{-1/n}(|0\rangle - \frac{1}{\sqrt{n}}|1\rangle + \frac{1}{2n}|2\rangle ..) \end{aligned} \tag{5.61}$$

This allows the holder to perform an unambiguous state discrimination (USD) by per-

forming the POVM measurement $\{M_+, M_-, M_{inc}\}$ on the incoming density state $\rho = \frac{1}{2}(|+\rangle\langle+| + |-\rangle\langle-|)$ for each time mode. Here

- M_+ corresponds to outcome of bit value 0,
- M_- to outcome of bit value 1.
- M_{inc} returns inconclusive bit value outcome. In this case the holder guess the bit value with 50% correctness.

The objective of the adversary then is to maximize the function: $\text{Tr}((M_+ + M_-)\rho) + \frac{1}{2}\text{Tr}(M_{inc}\rho)$. This can be explicitly written as a semi-definite programming SDP,

$$\begin{aligned} \max \quad & \text{Tr}((M_+ + M_-)\rho) + \frac{1}{2}\text{Tr}(M_{inc}\rho) \\ \text{subject to} \quad & M_+ + M_- + M_{inc} = \mathbb{I}, \\ & M_+ |+\rangle = 0, \\ & M_- |-\rangle = 0, \\ & M_-,\ M_+,\ M_{inc} \geqslant 0 \end{aligned}$$

For the SDP, we take the contribution of only $|0\rangle, |1\rangle, |2\rangle, |3\rangle$ photon number states for our density matrix ρ. This assumption holds because the state has 1 photon on average spread over n-time bin modes, and the probability of obtaining 4-photons or more is negligibly small. Figure 5.7 is the simulation plot of the success probability of the attacker to determine the bit value when he uses the USD attack vs when he just randomly guesses the bit value. We see that for low input sizes, the adversary substantially enhances his success probability to correctly output the bit value, thus enabling him to forge the note with higher success probability.

In contrast, if the *Bank* phase randomizes the the coherent states, then at each time step holder effectively sees a classical mixture,

$$\int_0^{2\pi} \frac{d\theta}{2\pi} |e^{i\theta}\frac{(-1)^{x_{j,k}}}{\sqrt{n}}\rangle\langle e^{i\theta}\frac{(-1)^{x_{j,k}}}{\sqrt{n}}| = e^{-1/n}\sum_l \frac{1}{n^l l!} |l\rangle\langle l|, \tag{5.62}$$

Thus under phase randomization, the attacker is no longer able to perform the USD attack and the best he can do is randomly guess the bit value.

5.10 Conclusion

We introduced the private-key quantum money as the cryptographic task using Sampling Matching verification protocol. We first analysed the money scheme when the *Bank* encodes

each copy of the note into single photon states in superposition over many modes. We analysed the correctness and unforgeability of our scheme and showed that an honest note holder passes the verification protocol with an exponentially close-to-one probability, while an adversary, trying to duplicate the note to be able to pass the verification protocol of two independent verifiers, fails the test with exponentially close-to-one probability.

Building on this result, we have proposed an experimentally motivated framework of the quantum money scheme using attenuated coherent states. This framework eases out the implementation of quantum money schemes since the verification protocol by the verifier requires just a single 50/50 beam splitter and two threshold detectors as optical elements.

The coherent based scheme we have proposed has two rounds of classical interaction with the *Bank*. We don't see it as a problem because both rounds are classical interaction, and both the rounds of interactions involve the public broadcast of information by the *Bank* and verifier, thus posing no security threat to the note.

The future line of work involves explicitly proving the forging probability of the adversary in the coherent state framework, and experimental demonstration of our money scheme.

Another interesting future line of direction in the coherent state framework would involve reducing the classical interaction between the verifier and the *Bank* to a single round by removing the constraint of phase randomization and identifying whether we can still achieve a positive gap between the honest note holder success probability and the adversary forging probability.

6 Programmable Measurement with Coherent States

6.1 Introduction

All the experiments involving measurement of a quantum state (or sets of quantum states) requires preparing a circuit, which is often classically controlled, to perform a vast majority of operations on the state, with the aim of creating a universal quantum computer. The choice of measurement typically depends on task at hand. A scenario that involves the programmable projective measurement is the implementation of Hidden Matching communication problem [Chapter 4.2]. The implementation of a matching from the matching set involves reprogramming the circuit involving optical switches and delays as we have depicted in Figure 4.3.

There have also been recent works on constructing a reprogrammable optical circuit to control the measurement that is sufficient to implement all possible linear optical protocols up to the size of that circuit [CHS$^+$15]. Their circuit involves Mach-Zhender interferometers and thermo-optic phase shifters which are electronically and optically controlled.

In this work, we will investigate the case where the choice of measurement is instead controlled by the input quantum state. This setting has been previously investigated in the communication complexity problems involving Euclidean Distance [Chapter 3] and Sampling Matching [Chapter 4], and also in the cryptographic setting involving the verification procedure in quantum money protocol [Chapter 5], where in all these cases, the input states controls the outcome of the measurement performed using the beam splitter operation. The heart of our previous works is to find the best possible way to discriminate the two unknown quantum states. The task of discriminating two states is trivial in the classical world, where the two states can be checked bit wise and thus the maximum check that needs to be performed is on all the bits of the states (size of the states). However, comparing two quantum states is non-trivial due to the fact that the states cannot be cloned [WZ82]. Buhrman et al [BCWDW01] introduced the technique, control-swap operation, to discriminate two unknown quantum states with a one sided error probability. This technique

is optimal if one has only a single copy of the two quantum states [BCJ03]. However, in order to succeed with an arbitrarily small error probability τ, this technique need $\mathcal{O}(\log \frac{1}{\tau})$ copies of the qubit states. Motivated by this scenario, Chabaud et al [CDM$^+$18] provided an generalised version of controlled-swap test by considering a situation when the input state is a single copy of one qubit state, called the test state, and multiple copies of the other qubit state, called the reference states. They asked the question: Can two unknown qubit states have a better discrimination probability in just a single run of the test. Their answer was in affirmative by stating that the discrimination probability increases with the number of copies of reference states.

In our work, we extend the results of [CDM$^+$18] to case when the unknown quantum states are encoded using coherent states. Our result shows a better convergence towards perfect discrimination of the unknown quantum states, compared to the previous results. Over the next sections, we review the existing state discrimination techniques for qubit states and for coherent states. We then introduce the discrimination technique using coherent states for single test state and multiple reference states. Further, we analyse the scenarios in realistic experimental settings and compare our result with the previous known results. We conclude by giving the proof for the optimality of our projective measurement test for two unknown coherent states in our generalised setting.

6.2 State Discrimination with Single Copy of States

The discrimination measurement circuit for two unknown qubit states under one sided error was first introduced by [BCWDW01]. If the encoding of the qubit states is using coherent states, then it translates to applying a beam splitter operation and observing the photon clicks in the output modes.

6.2.1 C-SWAP Circuit

The C-SWAP operation is applied to two unknown qubit states $|\phi\rangle$ and $|\psi\rangle$, and an ancillary qubit $|0\rangle$ as shown in Figure 6.1. Applying the circuit and measuring the ancilla qubit, returns the output "1" with a probability $p(\text{“1”}) = \frac{1}{2}(1 - |\langle\phi|\psi\rangle|^2)$, while it returns the output "0" with probability $1 - p(\text{“1”})$.

Completeness: If the states $|\phi\rangle$ and $|\psi\rangle$ are the same, then there is a zero probability of the outcome being "1". We say that the test has perfect completeness, where completeness $c_2 = 1 - p(\text{“1”})$ when the states are the same. The subscript denote the two states used for testing.

Soundness: If the states are different, then with finite probability $1 - p(\text{“1”})$, one is not able to discriminate the states. Thus the soundness $s_2 = 1 - p(\text{“1”})$ is strictly greater than 0. The soundness of this scheme can be increased to any desired $1 - \tau$, by repeating the this

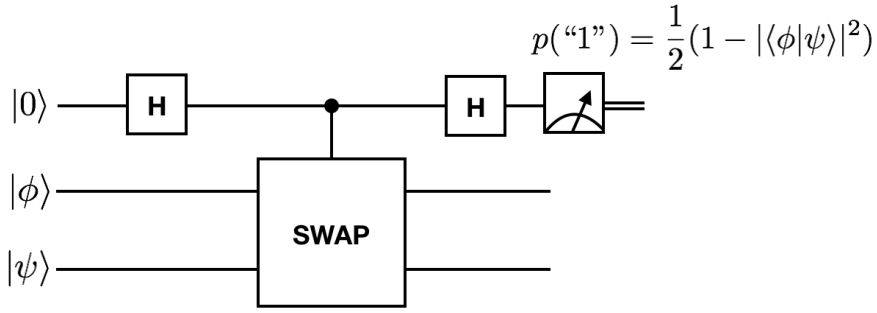

Figure 6.1: Controlled Swap test circuit employed by to discriminate the incoming qubit states. The ancilla qubit is measured in the computational basis and this relates to the probability of discriminating the two qubit states.

technique $\mathcal{O}(\log \frac{1}{\tau})$ times.

6.2.2 Beam Splitter Operation for Coherent States

The above C-SWAP circuit applies to any general unknown qubit states. If the qubit states are prepared using coherent states, then the C-SWAP operation can be performed using a 50/50 beam splitter (BS) and observing the photon click in the single photon threshold detector D_1. The interference of two unknown coherent states $|\alpha\rangle$ and $|\beta\rangle$ is shown in Figure 6.2.

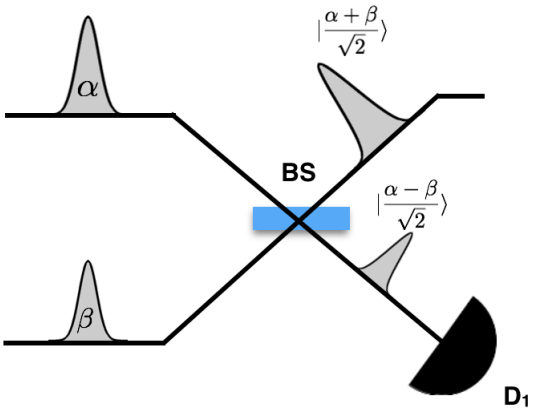

Figure 6.2: 50/50 Beam splitter (BS) operation on input states $|\alpha\rangle$ and $|\beta\rangle$. The output modes of BS are put in single photon threshold detector D_1. The probability of obtaining a click in D_1 constitutes to the projective measurement test of distinguishing the two unknown states.

The input states at the beam-splitter are,

$$|\alpha\rangle_a \otimes |\beta\rangle_b \,, \tag{6.1}$$

where the subscripts denote the mode at which coherent states enter the beam splitter. In the absence of experimental imperfections, this yields the output state,

$$|\frac{\alpha+\beta}{\sqrt{2}}\rangle_{c} \otimes |\frac{\alpha-\beta}{\sqrt{2}}\rangle_{d}, \tag{6.2}$$

The probability of obtaining a click in the detector D_1 is,

$$p_{D_1} = 1 - \exp(-\frac{|\alpha-\beta|^2}{2}) = 1 - |\langle\alpha|\beta\rangle| \tag{6.3}$$

The Hadamard interferometer interpretation

Another technique to view the above the 50/50 beam-splitter operation is performing a Hadamard-Welsh transformation of order 1 on the input coherent states $|\alpha\rangle$ and $|\beta\rangle$. [Cre15, COR$^+$16].

$$H\,|\alpha\rangle \otimes |\beta\rangle = |\frac{\alpha+\beta}{\sqrt{2}}\rangle \otimes |\frac{\alpha-\beta}{\sqrt{2}}\rangle \tag{6.4}$$

where, $H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$ is the Hadamard-Walsh transform of order 1. Later, we see that this interpretation facilitates an easy computation of state discrimination in the generalised setting.

Completeness & **Soundness**

We introduce the completeness c_2 and soundness s_2 in terms of the trace distance of the states $|\alpha\rangle$ and $|\beta\rangle$. The trace distance for two coherent states $\{|\alpha\rangle, |\beta\rangle\}$ is,

$$\| \,|\alpha\rangle\langle\alpha| - |\beta\rangle\langle\beta|\,\|_{\text{tr}} = \sqrt{1 - |\langle\alpha|\beta\rangle|^2} = \sqrt{1 - e^{-|\alpha-\beta|^2}} \tag{6.5}$$

We assign to the detection event (obtaining a click in D_1) the value "1", and to the other detection event (no click in detector D_1) the value "0".

Completeness: If the states are the same, then the trace distance = 0. Thus the probability of having the detection event "1" is zero. This ensures perfect completeness $c_2 = 1$, where the subscript denotes the size, or, the order of Hadamard interferometer.

Soundness: Suppose $\| \,|\alpha\rangle\langle\alpha| - |\beta\rangle\langle\beta|\,\|_{\text{tr}} \geqslant \varepsilon$. Then the soundness, which is the probability of failing to obtain the detection event "1", is $s_2 \geqslant 1 - \sqrt{1-\varepsilon^2}$. Thus it is strictly greater than 0. The soundness can be increased to any $s_2 = 1 - \tau$ by repeating the measurement procedure for $\log\frac{1}{\tau}$ runs.

6.3 Generalised Single Run State Discrimination

We now consider the scenario when one receives a single copy of the unknown test state $|\alpha\rangle$, and the objective is to check if the test state is equal to the reference coherent state $|\beta\rangle$. Here one can have multiple copies of the reference state but is limited to just a single copy of the test state. In the trivial case, the state discrimination can be performed with a single copy of the test and reference states. This succeeds with a probability given by Eq.(6.3). In this section, we prove that having multiple copies of reference state $|\beta\rangle$ increases the success probability of discriminating with the test state $|\alpha\rangle$. For this, we provide a generalised interferometer construction using Hadamard transformations.

Input State: Suppose the input to the generalised interferometer is M coherent states,

$$|\alpha\rangle_1 \otimes |\beta\rangle_2 ... \otimes |\beta\rangle_M \tag{6.6}$$

where the subscript denotes the mode in which the coherent state enters the generalised interferometer. For simplicity, we address this states as $|\alpha\beta...\beta\rangle$.

The input is then fed in the M sized generalised interferometer. For $M = 4$ spatial modes, this interferometer is described by the Hadamard-Walsh transform of order 2:

$$H_2 = H^{\otimes 2} = \frac{1}{\sqrt{2}} \begin{pmatrix} H & H \\ H & -H \end{pmatrix} \tag{6.7}$$

where H is a Hadamard matrix. The implementation for $M = 4$ interferometer construction is shown in Figure 6.3.

In the general case, the Sylvester-Hadamard interferometer of order M is described by the Hadamard-Walsh transform of order $n = \log M$ and is defined by:

$$H_n = H^{\otimes n}, \tag{6.8}$$

with $H_0 = 1$ and $H_1 = H$.

Output state: The input coherent states $|\alpha\beta \dots \beta\rangle$ upon interaction with the interferometer of order n transforms as,

$$|\alpha\beta \dots \beta\rangle \mapsto H_n |\alpha\beta \dots \beta\rangle = |\delta_1\delta_2 \dots \delta_M\rangle , \tag{6.9}$$

where, with a simple induction technique, we obtain $\delta_1 = \frac{\alpha+(M-1)\beta}{\sqrt{M}}$ and $\delta_k = \frac{\alpha-\beta}{\sqrt{M}}$ for $k \neq 1$. Thus out of M output modes, the last $M - 1$ modes have the same probability of a click.

We now assume that we detect the last $M - 1$ output modes of the generalised Hadamard

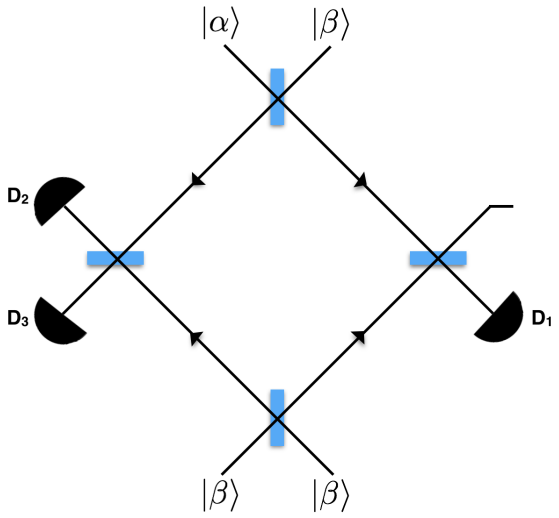

Figure 6.3: Sylvester-Hadamard interferometer with 4 input modes.The input states are one test state $|\alpha\rangle$ and three local states $|\beta\rangle$, one in each mode. The detectors D_i are single photon threshold detectors, $\forall i \in \{1, 3\}$.

interferometer. The probability $\mathbb{P}_\emptyset$ that none of the $M-1$ detectors clicks is,

$$\begin{aligned} P_\emptyset(\alpha, \beta, M) &= \prod_{k=2}^{M} [1 - \mathbb{P}(\text{click in } k^{\text{th}} \text{ mode})] \\ &= \prod_{k=2}^{M} [1 - (1 - \exp(-|\delta_k|^2))] \\ &= \exp(-\frac{M-1}{M}|\alpha - \beta|^2) \\ &= (|\langle\alpha|\beta\rangle|^2)^{1-\frac{1}{M}}. \end{aligned} \tag{6.10}$$

In particular, for all $\alpha, \beta \in \mathbb{C}$, $\mathbb{P}_\emptyset(\alpha, \beta, +\infty) = |\langle\alpha|\beta\rangle|^2$, which corresponds to a perfect projective measurement of the states $|\alpha\rangle$ and $|\beta\rangle$. Writing $x = |\langle\alpha|\beta\rangle|^2$ the overlap of the different input states, we obtain,

$$\mathbb{P}_\emptyset(x, M) = x^{1-\frac{1}{M}}. \tag{6.11}$$

Assigning to this detection event (none of the detectors click) the value "0", and to other detection events (at least one of the $M-1$ detectors clicks) the value "1", we obtain a device whose statistics mimic those of a projective measurement, with

$$\mathbb{P}_M(\text{“0”}) = 1 - \mathbb{P}_M(\text{“1”}) = x^{1-\frac{1}{M}}. \tag{6.12}$$

For the single-photon encoding, with an M input state $|\phi\psi\ldots\psi\rangle$, the corresponding statistics as obtained by Chabaud et al [CDM$^+$18] are,

$$\mathbb{P}_M(\text{“0”}) = 1 - \mathbb{P}_M(\text{“1”}) = \frac{1}{M} + \left(1 - \frac{1}{M}\right) x. \tag{6.13}$$

The single photon encoding implies having M number resolving detectors. On the contrary, the encoding with coherent states, requires $M-1$ single photon threshold detectors. Experimentally, this is more cost effective and relatively easier to implement. The other advantage with coherent state encoding is it gives a more faithful projective measurement than the single-photon encoding. Indeed, the statistics produced by coherent state encoding is closer to the ones of a perfect projective measurement. For any given value of the overlap x:

$$\forall x \in [0,1], \quad x \leqslant x^{1-\frac{1}{M}} \leqslant \frac{1}{M} + \left(1 - \frac{1}{M}\right) x. \tag{6.14}$$

Moreover, the convergence speed towards a perfect projective measurement is faster with the coherent state encoding. For a giving size M, the maximal gap with the perfect projective measurement is,

$$\begin{aligned} e_{SP}(M) &= \max_{x\in[0,1]} \left| \left[\frac{1}{M} + \left(1 - \frac{1}{M}\right) x \right] - x \right| \\ &= \frac{1}{M} \end{aligned} \tag{6.15}$$

for the single-photon encoding, and

$$\begin{aligned} e_{CS}(M) &= \max_{x\in[0,1]} \left| \left(x^{1-\frac{1}{M}}\right) - x \right| \\ &= \frac{(M-1)^{M-1}}{M^M} \\ &\sim \frac{1}{M} e^{-(1-\frac{1}{M})} \end{aligned} \tag{6.16}$$

for the coherent state encoding.

Thus the coherent state encoding decreases the gap faster compared to the single photon encoding. This happens because for the single-photon encoding no assumption is made about the states $|\phi\rangle$ and $|\psi\rangle$, while the states $|\alpha\rangle$ and $|\beta\rangle$ are assumed to be coherent states. This additional information about the states allows for the better discrimination of the two states. A related question would be, is the generalised Hadamard gate operation optimal? Or can a better measurement setting improve the state discrimination. We show in Section 6.5 that the generalised Hadamard interferometer is actually optimal for approaching perfect projective measurement with coherent states.

6.3.1 Completeness & Soundness in Generalised Model

In the generalised model of order M using coherent states, we observe the clicks in the last $M-1$ threshold detectors.

Completeness: If the states are the same, then the trace distance $\| |\alpha\rangle \langle\alpha| - |\beta\rangle \langle\beta| \|_{\text{tr}} = 0$, and hence the probability of having the detection event "1" is 0. Thus, the completeness of this scheme $c_M = 1$.

Soundness: If the states $\{|\alpha\rangle, |\beta\rangle\}$ are ε far apart in trace distance, then the soundness of this scheme is $s_M \geqslant 1 - (1-\varepsilon^2)^{1-\frac{1}{M}}$.

6.4 Analysis with Experimental Imperfections

In this section, we consider the effect of generalised Hadamard operation in presence of experimental imperfections. Our model of imperfection is the same as described in the previous chapters. There are three major sources of error. (i) The limited detector-efficiency and channel transmission loss, characterized by parameter $0 \leqslant \eta \leqslant 1$. This changes the state α to $\sqrt{\eta}\alpha$ thus reducing the probability of the verifier obtaining a click in his single photon detector by a factor η, (ii) The limited beam-splitter visibility $0 \leqslant \nu \leqslant 1$, which may lead to a click in the wrong detector, and (iii) the dark count in the detectors characterized by probability p_{dark}. For our analysis, the click probability due to coherent state is of O(1) and thus significantly larger than the dark count probability p_{dark} ($\sim 10^{-8}$). The dark count effect can thus be safely ignored.

	η(channel + det)	ν	p_{dark}
Exp.	0.9	$(98.8 \pm 0.3)\%$	$(1 \pm 0.1) * 10^{-8}$

Table 6.1: Experimental parameters achievable with super-conducting detectors [SJZ+18] and the beam-splitter set-up in our experimental lab.

For $M = 2$, when the input $|\alpha\rangle$, $|\beta\rangle$ is fed in the imperfect beam-splitter the transformation from input modes $\{\hat{a}^\dagger, \hat{b}^\dagger\}$ into the output modes $\{\hat{c}^\dagger, \hat{d}^\dagger\}$, is the following,

$$|\alpha\rangle_a \otimes |\beta\rangle_b \mapsto \left|\sqrt{\nu}\frac{\alpha+\beta}{\sqrt{2}} + \sqrt{1-\nu}\frac{\alpha-\beta}{\sqrt{2}}\right\rangle_c \otimes \left|\sqrt{\nu}\frac{\alpha-\beta}{\sqrt{2}} + \sqrt{1-\nu}\frac{\alpha+\beta}{\sqrt{2}}\right\rangle_d, \quad (6.17)$$

In the Hadamard-Walsh interpretation the input-output transformation is,

$$\begin{bmatrix}|\alpha\rangle & |\beta\rangle\end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix}A & B \\ A & -B\end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix}|A\alpha + B\beta\rangle \\ |A\alpha - B\beta\rangle\end{bmatrix} \quad (6.18)$$

where $A = \sqrt{\nu} + \sqrt{1-\nu}$, and $B = \sqrt{\nu} - \sqrt{1-\nu}$.

The imperfect Hadamard-Walsh transform of order 1 is then, $H' = \frac{1}{\sqrt{2}} \begin{bmatrix}A & B \\ A & -B\end{bmatrix}$. Using the method similar to the construction of any general Hadamard-Walsh transformation, we construct this transformation of order $n = \log M$,

$$H'_n = H'^{\otimes n}, \quad (6.19)$$

where $H'_0 = 1$ and $H'_1 = H'$.

6.4.1 Completeness & Soundness under Exp. Imperfection

Here, we restrict ourselves to the special case of $M = 4$ spatial modes (Fig 6.3). We apply the imperfect Hadamard transformation on the input $|\alpha\beta\beta\beta\rangle$. This results in,

$$|\alpha\beta\beta\beta\rangle \mapsto H'_2 |\alpha\beta\beta\beta\rangle = |\delta_1\delta_2\delta_3\delta_4\rangle , \tag{6.20}$$

where we obtain, $\delta_1 = \frac{\alpha+\beta(4\nu-1)+2\sqrt{\nu(1-\nu)}(\alpha-\beta)}{2}$, $\delta_2 = \delta_3 = \frac{\alpha-\beta+2\sqrt{\nu(1-\nu)}(\alpha+\beta)}{2}$, and $\delta_4 = \frac{\alpha-\beta(4\nu-3)+2\sqrt{\nu(1-\nu)}(\alpha-\beta)}{2}$. Adding the channel loss and limited detector-efficiency factor η, the output $\delta_k \mapsto \sqrt{\eta}\delta_k$, for all k.

Similar to the analysis without experimental imperfection, we detect the last 3 output modes of the imperfect Hadamard interferometer, with the coherent state input being $|\alpha\beta\beta\beta\rangle$. The probability $\mathbb{P}_\emptyset$ that none of the last 3 detectors clicks is,

$$\begin{aligned} \mathbb{P}_\emptyset(\alpha, \beta, \nu, \eta, M = 4) &= \prod_{k=2}^{4} [1 - (1 - \exp(-\eta|\delta_k|^2))] \\ &= \exp\Big(- \eta(2|\delta_2|^2 + |\delta_4|^2)\Big) \end{aligned} \tag{6.21}$$

Assigning to the detection event (none of the 3 detectors clicks) the value "0", and to other detection events (at least one of the 3 detectors clicks) the value "1", we obtain a device whose statistics mimic those of a projective measurement.

Completeness: When the states are the same, the correctness, which is the probability of not obtaining the detection event "1" is,

$$c_4^{exp} = \mathbb{P}_\emptyset(\alpha, \alpha, \nu, \eta, 4) = \exp(-4\eta(1 - \nu^2)|\alpha|^2) \tag{6.22}$$

We observe that if $\nu = 1$ (no imperfections), then $c_4^{exp} = 1$, thus we obtain perfect completeness. For the imperfection values of Table 6.1, we plot the c_4^{exp} behaviour vs $|\alpha|^2$ in Fig 6.4, and see that it is close to 1 for fairly small $|\alpha|^2$ values.

Comparison of Completeness with $M = 2$ scheme: The analogous completeness in $M = 2$ scheme is,

$$c_2^{exp} = \mathbb{P}_\emptyset(\alpha, \alpha, \nu, \eta, 2) = \exp(-2\eta(1 - \nu)|\alpha|^2) \tag{6.23}$$

From Eq.(6.23) and Eq.(6.22), we observe that $c_2^{exp} < c_4^{exp}$, which implies that the completeness in the $M = 4$ scheme is less than the completeness in $M = 2$ scheme. However, the reduction in completeness probability for $M = 4$ scheme is precisely what accounts for an

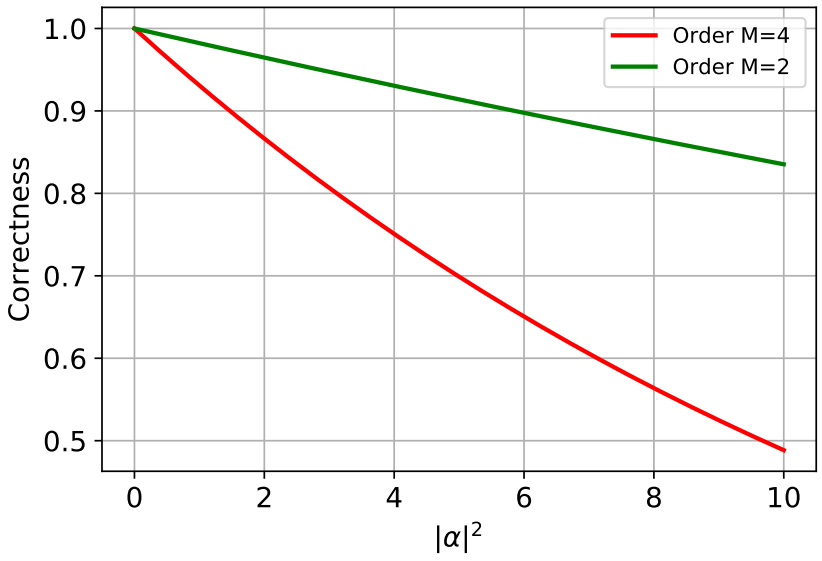

Figure 6.4: Plot of the completeness probability (c_4^{exp} and c_2^{exp}) vs average photon number in the coherent state $|\alpha|^2$, for the $M = 2$ and $M = 4$ modes. The plot is under the experimental imperfection values given in Table 6.1.

increase in soundness probability (when the local and reference states are different), which we discuss in the next section.

Soundness: If the states are ε far apart in the trace distance, the probability of obtaining the detection event "1" (soundness) is,

$$s_4^{exp} = 1-\exp\left[-\frac{\eta}{4}\left(2\left|\alpha-\beta+2\sqrt{\nu(1-\nu)}(\alpha+\beta)\right|^2+\left|\alpha-\beta(4\nu-3)+2\sqrt{\nu(1-\nu)}(\alpha-\beta)\right|^2\right)\right] \tag{6.24}$$

Now let us analyse Eq.(6.24) to see if we express the soundness with respect to the trace distance. Using the equalities, $|\alpha+\beta|^2 = 2|\alpha|^2+2|\beta|^2-|\alpha-\beta|^2$ and $\alpha^*\beta+\beta^*\alpha = |\alpha|^2+|\beta|^2-|\alpha-\beta|^2$ we obtain,

$$\begin{aligned} s_4^{exp} = 1-\exp\Bigg[&-\eta\left(\frac{3}{4}-(1-\nu^2)+(2\nu-1)\sqrt{\nu(1-\nu)}\right)|\alpha-\beta|^2 \\ &-\eta\left((4\nu+1)(1-\nu)+(4-2\nu)\sqrt{\nu(1-\nu)}\right)|\alpha|^2 \\ &-\eta\left(3(1-\nu)-(4-2\nu)\sqrt{\nu(1-\nu)}\right)|\beta|^2\Bigg] \end{aligned} \tag{6.25}$$

The analogous soundness in $M = 2$ experimental imperfection scheme is,

$$s_2^{exp} = 1 - \exp\Bigg[-\eta\left(\nu - \frac{1}{2}\right)|\alpha - \beta|^2 - \eta\left(1 - \nu + \sqrt{\nu(1-\nu)}\right)|\alpha|^2 \\ - \eta\left(1 - \nu - \sqrt{\nu(1-\nu)}\right)|\beta|^2\Bigg] \tag{6.26}$$

Comparing the soundness in the $M = 4$ experimental imperfection scheme with the $M = 4$ scheme, we observe that,

$$s_4^{exp} > s_2^{exp} \qquad \forall \varepsilon \in [0, 1] \tag{6.27}$$

where $\| \, |\alpha\rangle \langle\alpha| - |\beta\rangle \langle\beta| \, \|_{\text{tr}} \geqslant \varepsilon$. The reasoning for the above equation is that when $\varepsilon = 0$, i.e. when the test and reference states are the same, $s_4^{exp} = 1 - c_4^{exp}$, and similarly $s_2^{exp} = 1 - c_2^{exp}$. From Eq.(6.23) and Eq.(6.22), $s_4^{exp} > s_2^{exp}$ for $\varepsilon = 0$. Further, it can be verified that the difference $s_4^{exp} - s_2^{exp}$ is always positive for any visibility factor ν. Thus for the experimental visibility factor as given in Table 6.1, Eq.(6.27) always holds.

In the absence of any experimental imperfections, it can be shown relatively easily that the soundness s_4 is always greater than s_2. Our results with experimental imperfections also show that even in imperfect $M = 4$ scheme $s_4^{exp} > s_2^{exp}$. Thus $M = 4$ outperforms $M = 2$ scheme in the soundness.

6.5 Optimality Test for Coherent States

A simple extension of the proof of [SZP$^+$07] provides the optimality of the Hadamard interferometer for approaching a projective measurement with coherent states.

6.5.1 Optimal POVM for Discrimination under the One-Sided Error

We first compute the expressions of optimal POVM for coherent state discrimination under the one-sided error requirement.

Let Π_0 and Π_1 be a POVM for discriminating coherent states $|\alpha\rangle$ and $|\beta\rangle$, when provided a single copy of $|\alpha\rangle$ and $M - 1$ copies of $|\beta\rangle$ (the proof of [SZP$^+$07] assumes $M = 2$). The operator Π_0 corresponds to saying that the states $|\alpha\rangle$ and $|\beta\rangle$ are the same, while the operator Π_1 corresponds to saying that they are different. These operators thus verify the following conditions:

$$\Pi_0, \Pi_1 \geqslant 0, \ \Pi_0 + \Pi_1 = 1 \quad \text{and} \quad \forall \alpha \in \mathbb{C}, \ \text{Tr}\left[\Pi_1 \, |\alpha\rangle \langle\alpha|^{\otimes M}\right] = 0, \tag{6.28}$$

where the last condition is the one-sided error requirement. Integrating this condition over $\mathbb{C}$ yields

$$0 = \int d^2\alpha \text{Tr}\left[\Pi_1 \, |\alpha\rangle \langle\alpha|^{\otimes M}\right] = \text{Tr}\left[\Pi_1 \Delta_M\right], \tag{6.29}$$

where we have defined

$$\Delta_M = \int d^2\alpha \, |\alpha\rangle \langle\alpha|^{\otimes M} \geqslant 0. \tag{6.30}$$

Note that the condition in (6.29) is equivalent to the one-sided requirement in (6.28) because the operators Π_1 and $|\alpha\rangle \langle\alpha|^{\otimes M}$ are positive.

The operator $\frac{M}{\pi}\Delta_M$ is actually a projector. This result can be obtained by writing the state $|\alpha\rangle$ in the Fock basis and an integration in polar coordinates, where $\alpha = re^{j\theta}$. From Eq. (6.30) we obtain

$$\begin{aligned}
\Delta_M &= \int d^2\alpha \, \exp[-M|\alpha|^2] \sum_{\substack{k_i,l_i=0 \\ \forall i\in[M]}}^{\infty} \frac{\alpha^{\sum_i k_i}(\alpha^*)^{\sum_i l_i}}{\sqrt{k_1!\dots k_M! l_1!\dots l_M!}} |k_1\dots k_M\rangle \langle l_1\dots l_M| \\
&= \sum_{k_i,l_i=0}^{\infty} \frac{|k_1\dots k_M\rangle \langle l_1\dots l_M|}{\sqrt{k_1!\dots k_M! l_1!\dots l_M!}} \int_{r=0}^{\infty} dr \, \exp[-Mr^2] r^{\sum_i k_i + l_i} \int_{\theta=0}^{2\pi} d\theta \, \exp[j\theta \sum_i (k_i - l_i)] \\
&= \frac{\pi}{M} \sum_{k_i,l_i=0}^{\infty} \frac{\delta_{\sum_i k_i, \sum_i l_i}}{M^{\frac{\sum_i k_i}{2}} M^{\frac{\sum_i l_i}{2}}} \sqrt{\frac{(\sum_i k_i)!(\sum_i l_i)!}{k_1!\dots k_M! l_1!\dots l_M!}} |k_1\dots k_M\rangle \langle l_1\dots l_M| \\
&= \frac{\pi}{M} \sum_{N=0}^{\infty} \sum_{\substack{\sum_i k_i = N \\ \sum_i l_i = N}} M^{-N} \sqrt{\frac{N!}{k_1!\dots k_M!}} \sqrt{\frac{N!}{l_1!\dots l_M!}} |k_1\dots k_M\rangle \langle l_1\dots l_M| \\
&= \frac{\pi}{M} \sum_{N=0}^{\infty} |\chi_N^M\rangle \langle\chi_N^M|,
\end{aligned} \tag{6.31}$$

where we have defined for all $N \geqslant 0$,

$$|\chi_N^M\rangle = M^{-N/2} \sum_{\sum_i k_i = N} \sqrt{\frac{N!}{k_1!\dots k_M!}} |k_1\dots k_M\rangle. \tag{6.32}$$

With the multinomial formula, we obtain $\langle\chi_N^M|\chi_N^M\rangle = 1$ for all $N \geqslant 0$, and since the states $|\chi_N^M\rangle$ have exactly N photons, we have $\langle\chi_N^M|\chi_{N'}^M\rangle = \delta_{N,N'}$ for all $N, N' \geqslant 0$. The states $|\chi_N^M\rangle$ thus are orthonormal and with Eq.(6.31), the operator $\frac{M}{\pi}\Delta_M$ is a projector.

By Eq.(6.29), the supports of Π_1 and $\frac{M}{\pi}\Delta_M$ are disjoint, and by Eq.(6.28) we see that $\Pi_0 + \Pi_1 = 1$, so the support of $\frac{M}{\pi}\Delta_M$ is included in the support of Π_0. The optimal POVM $\{\Pi_0^{opt}, \Pi_1^{opt}\}$ for state discrimination minimises the error probability, hence with the one-sided error requirement Π_0^{opt} must have minimal support, meaning that

$$\Pi_0^{opt} = \frac{M}{\pi}\Delta_M = \sum_{N=0}^{+\infty} |\chi_N^M\rangle \langle\chi_N^M| \quad \text{and} \quad \Pi_1^{opt} = 1 - \Pi_0^{opt}. \tag{6.33}$$

Note that, with the same proof, this choice of POVM is also optimal in the generalised setting where one is given M coherent states and is asked to test if all the states are identical or not.

6.5.2 Optimality of The Hadamard Interferometer

We show that the POVM $\{\Pi_0^h, \Pi_1^h\}$ corresponding to the Hadamard interferometer with a threshold detection of the last $M-1$ modes is optimal for coherent state discrimination under the one-sided error requirement, i.e. that

$$\Pi_0^h = \Pi_0^{opt}, \tag{6.34}$$

where Π_0^{opt} is defined in Eq.(6.33). We have

$$\Pi_0^h = H_n^\dagger \Pi_0^d H_n, \tag{6.35}$$

where H_n is the Hadamard transform of order M defined in Eq.(6.8), with $n = \log M$, and $\Pi_0^d = I \otimes |0\rangle \langle 0|^{\otimes(M-1)}$ is the POVM operator corresponding to the event where none of the $M-1$ threshold detectors clicks. We obtain

$$\begin{aligned} \Pi_0^h &= H_n^\dagger \left(I \otimes |0\rangle \langle 0|^{\otimes(M-1)} \right) H_n \\ &= \sum_{N=0}^{+\infty} H_n^\dagger \left(|N\rangle \langle N| \otimes |0\rangle \langle 0|^{\otimes(M-1)} \right) H_n. \end{aligned} \tag{6.36}$$

For $k = 1 \dots M$, we write $a_k^\dagger$ the creation operator for the k^{th} mode. For all $N \geqslant 0$ we have

$$\begin{aligned} H_n^\dagger \left(|N\rangle \otimes |0\rangle^{\otimes(M-1)} \right) &= \frac{1}{\sqrt{N!}} H_n^\dagger (a_1^\dagger)^N |0\rangle^{\otimes M} \\ &= \frac{1}{\sqrt{N!}} (H_n^\dagger a_1^\dagger H_n)^N |0\rangle^{\otimes M} \\ &= \frac{M^{-N/2}}{\sqrt{N!}} (a_1^\dagger + \dots + a_M^\dagger)^N |0\rangle^{\otimes M} \\ &= \frac{M^{-N/2}}{\sqrt{N!}} \sum_{k_1+\dots+k_M=N} \frac{N!}{k_1! \dots k_M!} (a_1^\dagger)^{k_1} \dots (a_M^\dagger)^{k_M} |0\rangle^{\otimes M} \\ &= M^{-N/2} \sum_{k_1+\dots+k_M=N} \sqrt{\frac{N!}{k_1! \dots k_M!}} |k_1 \dots k_M\rangle \\ &= |\chi_N^M\rangle , \end{aligned} \tag{6.37}$$

where we have used $H_n |0\rangle^{\otimes M} = |0\rangle^{\otimes M}$, $H_n^\dagger H_n = 1$, $H_n^\dagger a_1^\dagger H_n = \frac{a_1^\dagger + \dots + a_M^\dagger}{\sqrt{M}}$, the multinomial formula, and Eq.(6.32). With Eqs[6.33,6.36], this concludes the proof.

6.6 Conclusion

We have presented the optimal scheme to discriminate two unknown coherent states under one-sided error probability using linear optics implementation and single photon threshold

detectors. The implementation of this interferometer circuit is efficient and the threshold detectors with high efficiency and ultra low dark counts are commercially available, with the manufactures including PhotonSpot [SJZ$^+$18] , SingleQuantum, IDQuantique.

This projective measurement implementation could act as a backbone in improving the performance of a range of quantum protocols in communication complexity [BCWDW01, dB04], cryptography and computational regimes [ABD$^+$08, MKB05, WRD$^+$06, HM13, EAO$^+$02, LMR13]. We have already mentioned one communication complexity task in Chapter 3, computing Euclidean distance of two real vectors, an important problem with applications in recommendation systems. The communication protocol using coherent state fingerprints provides an asymptotic exponential savings in communication resources [KDK17]. The performance of the protocol can be further improved by using the generalised Hadamard interferometer scheme.

The Hadamard interferometer scheme with coherent states encoding can be set-up easily, and to perform an order M transformation involves measuring the detector clicks of $M-1$ output modes. In the applications, for which only the classical output statistics are sufficient, we only restrict ourselves to measuring $M-1$ output modes. However, there could be other potential applications, where depending on the statistics we obtain in the $M-1$ modes, we want to perform an operation on the single unmeasured output mode which still is a quantum state containing the information of the unknown input states. This is in contrast to the single photon proposal by Chabaud et al [CDM$^+$18], which requires a destructive measurement on all the output modes to perform the state discrimination testing.

7 Conclusion and Future Directions

In this thesis, we have we have focussed on designing protocols for quantum information processing tasks that can be implemented with current photonic technologies.

In Chapter 3, we studied the Euclidean distance problem in simultaneous message passing model. Euclidean distance is an important problem with applications in recommendation systems. We proposed a multiplexed quantum protocol based on attenuated coherent states, linear optics transformations, and single photon threshold detectors. This protocol performs asymptotically better than the classical analogue in transmitted information resource, and even outperforms the optimal classical protocol in time resource. A noteworthy feature of the Euclidean Distance protocol studied in our work is that the communicating parties do not need a memory to store their inputs and they do not perform global operations on them. In other words, this protocol works also in the *streaming* scenario, where the parties receive their inputs one bit at a time [NAS99]. We performed a proof-of-principle implementation of protocol whose performance is limited by the threshold detectors. With the new technology in superconducting detectors, the performance of our protocol dramatically increases. An interesting future direction would be to further explore other quantum communication models. More generally, expanding the family of distributed tasks in the coherent state communication model studied in this work is important for demonstrating in practice quantum superiority in a network setting.

In Chapter 4, we provided a first such example of a one way communication complexity problem, the Sampling Matching, where we can experimentally demonstrate the quantum advantage using coherent state fingerprints. A noteworthy feature of our proof-of-principle implementation is the separation of the paths for Alice's incoming pulse and Bob's local pulses and careful caliberation of the path lengths, contrary to the previous proposed sagnac loop based implementations which introduces a possibility of cross-talk between the parties during the protcol run. We also have a proposal to go from proof-of-principle implementation to the full scale implementation by separating the laser sources of Alice and Bob. A typical issue in going to full-scale implementation involves maintaining the stable phase across the two paths. The phase fluctuation is typically due to the phase drift of the laser pulses

traversing over the optical channel, and the internal jitter in the lasers. In our experiment, we address the first source of fluctuation by introducing a phase correcting loop to track and correct the phase drift. The second source of fluctuation can be addressed by having two highly stable lasers (low line width $\sim$ kHz) [CLF$^+$16]. A line of research using Sampling Matching involves its applications as a crypto primitive, includig quantum money schemes and sound verification for tasks such as NP-complete proofs [ADK17].

In Chapter 5, we introduced the quantum money as a cryptographic task using the verification protocol based on the Sampling Matching quantum scheme. This framework was experimentally motivated to facilitate an easy verification procedure in quantum money scheme. The ease of verification allows for the Bank sending large input size notes, resulting in higher noise tolerance in our scheme that what is realistically feasible with other quantum money schemes. The scheme we have proposed has two rounds of classical interaction with the Bank. We don't see it as a problem because both rounds are classical interaction which involve public broadcasting of information by Bank and verifier, thus posing no security threat to the note. Future line of direction involves reducing the classical interaction to a single round by removing the constraint of phase randomization and identifying the regions of security.

In Chapter 6, we have presented the optimal scheme two discriminate two unknown coherent states using linear optics implementation, the Sylvester-Hadamard interferometer and single photon threshold detectors. The implementation of this interferometer circuit is efficient and uses the 50/50 beam splitter. This projective measurement implementation could act as a backbone in improving the performance of a range of quantum protocols in communication complexity [BCWDW01, dB04], cryptography and computational regimes [ABD$^+$08, MKB05, WRD$^+$06, HM13, EAO$^+$02, LMR13]. The Hadamard interferometer scheme with coherent states encoding can be set-up easily, and to perform an order M transformation involves measuring the detector clicks of $M-1$ output modes. In the applications, for which only the classical output statistics are sufficient, we only restrict ourselves to measuring $M-1$ output modes. However, there could be other potential applications, where depending on the statistics we obtain in the $M-1$ modes, we want to perform an adaptive operation on the single unmeasured output mode which is a quantum state containing the information of the unknown input states.

Bibliography

[AA17] Ryan Amiri and Juan Miguel Arrazola. Quantum money with nearly optimal error tolerance. *Physical Review A*, 95(6):062334, 2017.

[ABD+08] Scott Aaronson, Salman Beigi, Andrew Drucker, Bill Fefferman, and Peter Shor. The power of unentanglement. In *Computational Complexity, 2008. CCC'08. 23rd Annual IEEE Conference on*, pages 223–236. IEEE, 2008.

[ABG+07] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters*, 98(23):230501, 2007.

[AC12] Scott Aaronson and Paul Christiano. Quantum money from hidden subspaces. In *Proceedings of the forty-fourth annual ACM symposium on Theory of computing*, pages 41–60. ACM, 2012.

[AC16] Scott Aaronson and Lijie Chen. Complexity-theoretic foundations of quantum supremacy experiments. *arXiv preprint arXiv:1612.05903*, 2016.

[ACMT+07] Koenraad MR Audenaert, John Calsamiglia, Ramón Munoz-Tapia, Emilio Bagan, Ll Masanes, Antonio Acin, and Frank Verstraete. Discriminating states: The quantum chernoff bound. *Physical review letters*, 98(16):160501, 2007.

[ADK17] Juan Miguel Arrazola, Eleni Diamanti, and Iordanis Kerenidis. Quantum superiority for verifying np-complete problems with linear optics. *arXiv preprint arXiv:1711.02200*, 2017.

[AKL16] Juan Miguel Arrazola, Markos Karasamanis, and Norbert Lütkenhaus. Practical quantum retrieval games. *Physical Review A*, 93(6):062311, 2016.

[AL14a] Juan Miguel Arrazola and Norbert Lütkenhaus. Quantum communication with coherent states and linear optics. *Phys. Rev. A*, 90:042335, 2014.

[AL14b] Juan Miguel Arrazola and Norbert Lütkenhaus. Quantum fingerprinting with coherent states and a constant mean number of photons. *Phys. Rev. A*, 89(6):062305, 2014.

[Amb96] Andris Ambainis. Communication complexity in a 3-computer model. *Algorithmica*, 16(3):298–301, 1996.

[AT16] Juan Miguel Arrazola and Dave Touchette. Quantum advantage on information leakage for equality. *arXiv preprint arXiv:1607.07516*, 2016.

[AWB+09] Markus Ansmann, H Wang, Radoslaw C Bialczak, Max Hofheinz, Erik Lucero, M Neeley, AD O'Connell, D Sank, M Weides, J Wenner, et al. Violation of bell's inequality in josephson phase qubits. *Nature*, 461(7263):504–506, 2009.

[BB14] Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.*, 560(P1):7–11, 2014.

[BCJ03] Stephen M Barnett, Anthony Chefles, and Igor Jex. Comparison of two unknown pure quantum states. *Physics Letters A*, 307(4):189–195, 2003.

[BCMDW10] Harry Buhrman, Richard Cleve, Serge Massar, and Ronald De Wolf. Nonlocality and communication complexity. *Reviews of modern physics*, 82(1):665, 2010.

[BCW98] 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*, pages 63–68, 1998.

[BCWDW01] Harry Buhrman, Richard Cleve, John Watrous, and Ronald De Wolf. Quantum fingerprinting. *Phys. Rev. Lett.*, 87(16):167902, 2001.

[Bel01] John S Bell. Einstein-podolsky-rosen experiments. In *John S Bell on the Foundations of Quantum Mechanics*, pages 74–83. World Scientific, 2001.

[BFK09] Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi. Universal blind quantum computation. In *Foundations of Computer Science, 2009. FOCS'09. 50th Annual IEEE Symposium on*, pages 517–526. IEEE, 2009.

[BGK17] Sergey Bravyi, David Gosset, and Robert Koenig. Quantum advantage with shallow circuits. *arXiv preprint arXiv:1704.00690*, 2017.

[BIS+18] Sergio Boixo, Sergei V Isakov, Vadim N Smelyanskiy, Ryan Babbush, Nan Ding, Zhang Jiang, Michael J Bremner, John M Martinis, and Hartmut Neven. Characterizing quantum supremacy in near-term devices. *Nature Physics*, 14(6):595, 2018.

[BK97] László Babai and Peter G Kimmel. Randomized simultaneous messages: Solution of a problem of yao in communication complexity. In *Computational Complexity, 1997. Proceedings., Twelfth Annual IEEE Conference on (Formerly: Structure in Complexity Theory Conference)*, pages 239–246. IEEE, 1997.

[BMS17] Michael J Bremner, Ashley Montanaro, and Dan J Shepherd. Achieving quantum supremacy with sparse and noisy commuting quantum computations. *Quantum*, 1:8, 2017.

[BNSU14] Aharon Brodutch, Daniel Nagaj, Or Sattath, and Dominique Unruh. An adaptive attack on wiesner's quantum money. *arXiv preprint arXiv:1404.1507*, 2014.

[BOV+18] Mathieu Bozzio, Adeline Orieux, Luis Trigo Vidarte, Isabelle Zaquine, Iordanis Kerenidis, and Eleni Diamanti. Experimental investigation of practical unforgeable quantum money. *npj Quantum Information*, 4(1):5, 2018.

[BRS15] Sima Bahrani, Mohsen Razavi, and Jawad A Salehi. Orthogonal frequency-division multiplexed quantum key distribution. *Journal of Lightwave Technology*, 33(23):4687–4698, 2015.

[BRSDW11] Harry Buhrman, Oded Regev, Giannicola Scarpa, and Ronald De Wolf. Near-optimal and explicit bell inequality violations. In *Computational Complexity (CCC), 2011 IEEE 26th Annual Conference on*, pages 157–166. IEEE, 2011.

[BVHS+18] Juan Bermejo-Vega, Dominik Hangleiter, Martin Schwarz, Robert Raussendorf, and Jens Eisert. Architectures for quantum simulation showing a quantum speedup. *Physical Review X*, 8(2):021010, 2018.

[BYJK04] Ziv Bar-Yossef, Thathachar S Jayram, and Iordanis Kerenidis. Exponential separation of quantum and classical one-way communication complexity. In *Proceedings of the thirty-sixth annual ACM symposium on Theory of computing*, pages 128–137. ACM, 2004.

[CB97] Richard Cleve and Harry Buhrman. Substituting quantum entanglement for communication. *Physical Review A*, 56(2):1201, 1997.

[CDM+18] Ulysse Chabaud, Eleni Diamanti, Damian Markham, Elham Kashefi, and Antoine Joux. Programmable projective measurement with linear optics. *arXiv preprint arXiv:1805.02546*, 2018.

[CHS+15] Jacques Carolan, Christopher Harrold, Chris Sparrow, Enrique Martín-López, Nicholas J Russell, Joshua W Silverstone, Peter J Shadbolt, Nobuyuki Matsuda, Manabu Oguma, Mikitaka Itoh, et al. Universal linear optics. *Science*, 349(6249):711–716, 2015.

[CK12] Sarah Croke and Adrian Kent. Security details for bit commitment by transmitting measurement outcomes. *Physical Review A*, 86(5):052309, 2012.

[CLF+16] LC Comandar, M Lucamarini, B Fröhlich, JF Dynes, AW Sharpe, SW-B Tam, ZL Yuan, Richard Vincent Penty, and AJ Shields. Quantum key distribution without detector vulnerabilities using optically seeded lasers. *Nature Photonics*, 10(5):312, 2016.

[CM91] Olivier Carnal and Jürgen Mlynek. Young's double-slit experiment with atoms: A simple atom interferometer. *Physical review letters*, 66(21):2689, 1991.

[COR+13] Andrea Crespi, Roberto Osellame, Roberta Ramponi, Daniel J Brod, Ernesto F Galvão, Nicolò Spagnolo, Chiara Vitelli, Enrico Maiorino, Paolo Mataloni, and Fabio Sciarrino. Integrated multimode interferometers with arbitrary designs for photonic boson sampling. *Nature Photon.*, 7(7):545–549, 2013.

[COR+16] Andrea Crespi, Roberto Osellame, Roberta Ramponi, Marco Bentivegna, Fulvio Flamini, Nicolò Spagnolo, Niko Viggianiello, Luca Innocenti, Paolo Mataloni, and Fabio Sciarrino. Suppression law of quantum states in a 3d photonic fast fourier transform chip. *Nature communications*, 7:10469, 2016.

[Cre15] Andrea Crespi. Suppression laws for multiparticle interference in sylvester interferometers. *Physical Review A*, 91(1):013811, 2015.

[CW08] John Clarke and Frank K Wilhelm. Superconducting quantum bits. *Nature*, 453(7198):1031, 2008.

[dB04] J Niel de Beaudrap. One-qubit fingerprinting schemes. *Physical Review A*, 69(2):022307, 2004.

[DCK+16] Ross James Donaldson, Robert John Collins, Klaudia Kleczkowska, Ryan Amiri, Petros Wallden, Vedran Dunjko, John Jeffers, Erika Andersson, and Gerald Stuart Buller. Experimental demonstration of kilometer-range quantum digital signatures. *Phys. Rev. A.*, 93:012329, 2016.

[EAO+02] Artur K Ekert, Carolina Moura Alves, Daniel KL Oi, Michał Horodecki, Paweł Horodecki, and Leong Chuan Kwek. Direct estimations of linear and nonlinear functionals of a quantum state. *Physical review letters*, 88(21):217901, 2002.

[Fey82] Richard P Feynman. Simulating physics with computers. *International journal of theoretical physics*, 21(6-7):467–488, 1982.

[FGH+12] Edward Farhi, David Gosset, Avinatan Hassidim, Andrew Lutomirski, and Peter Shor. Quantum money from knots. In *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, pages 276–289. ACM, 2012.

[FH16] Edward Farhi and Aram W Harrow. Quantum supremacy through the quantum approximate optimization algorithm. *arXiv preprint arXiv:1602.07674*, 2016.

[FL02] Michael Fleischhauer and Mikhail D Lukin. Quantum memory for photons: Dark-state polaritons. *Physical Review A*, 65(2):022314, 2002.

[GAA+18] 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. *Physical Review A*, 97(3):032338, 2018.

[Gav12] Dmitry Gavinsky. Quantum money with classical verification. In *Computational Complexity (CCC), 2012 IEEE 27th Annual Conference on*, pages 42–52. IEEE, 2012.

[Gav16] Dmitry Gavinsky. Entangled simultaneity versus classical interactivity in communication complexity. *arXiv preprint arXiv:1602.05059*, 2016.

[GBHA10] Rodrigo Gallego, Nicolas Brunner, Christopher Hadley, and Antonio Acín. Device-independent tests of classical and quantum dimensions. *Physical review letters*, 105(23):230501, 2010.

[GK15] Marios Georgiou and Iordanis Kerenidis. New constructions for quantum money. In *LIPIcs-Leibniz International Proceedings in Informatics*, volume 44. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2015.

[GKK+07] 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*, pages 516–525, 2007.

[GKK17] Alexandru Gheorghiu, Theodoros Kapourniotis, and Elham Kashefi. Verification of quantum computation: An overview of existing approaches. *arXiv preprint arXiv:1709.06984*, 2017.

[GS18] David J Griffiths and Darrell F Schroeter. *Introduction to quantum mechanics*. Cambridge University Press, 2018.

[GWD17] Xun Gao, Sheng-Tao Wang, and L-M Duan. Quantum supremacy for simulating a translation-invariant ising spin model. *Physical review letters*, 118(4):040502, 2017.

[GXY+16] 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, et al. Observation of quantum fingerprinting beating the classical limit. *Phys. Rev. Lett.*, 116:240502, 2016.

[HBD+15] Bas Hensen, Hannes Bernien, Anaïs E Dréau, Andreas Reiserer, Norbert Kalb, Machiel S Blok, Just Ruitenberg, Raymond FL Vermeulen, Raymond N Schouten, Carlos Abellán, et al. Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526(7575):682, 2015.

[HM13] Aram W Harrow and Ashley Montanaro. Testing product states, quantum merlin-arthur games and tensor optimization. *Journal of the ACM (JACM)*, 60(1):3, 2013.

[Hol73] Alexander Semenovich Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problemy Peredachi Informatsii*, 9(3):3–11, 1973.

[Hol07] Katherine B Holt. Diamond at the nanoscale: applications of diamond nanoparticles from cellular biomarkers to quantum computing. *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 365(1861):2845–2861, 2007.

[HOM87] Chong-Ki Hong, Zhe-Yu Ou, and Leonard Mandel. Measurement of subpicosecond time intervals between two photons by interference. *Physical review letters*, 59(18):2044, 1987.

[IMV] Iker Millan Irigoyen, Lucas Lamata Manuel, and Enrique Solano Villanueva. D-wave quantum computer.

[JKJL+13] Paul Jouguet, Sébastien Kunz-Jacques, Anthony Leverrier, Philippe Grangier, and Eleni Diamanti. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nature Photonics*, 7(5):378–381, 2013.

[JSC+04] Brian Julsgaard, Jacob Sherson, J Ignacio Cirac, Jaromír Fiurášek, and Eugene S Polzik. Experimental demonstration of quantum memory for light. *Nature*, 432(7016):482, 2004.

[KDK15] Theodoros Kapourniotis, Vedran Dunjko, and Elham Kashefi. On optimising quantum communication in verifiable quantum computing. *arXiv preprint arXiv:1506.06943*, 2015.

[KDK17] Niraj Kumar, Eleni Diamanti, and Iordanis Kerenidis. Efficient quantum communications with coherent state fingerprints over multiple channels. *Physical Review A*, 95(3):032337, 2017.

[KKL88] Jeff Kahn, Gil Kalai, and Nathan Linial. *The influence of variables on Boolean functions*. IEEE, 1988.

[KLLGR16] Iordanis Kerenidis, Mathieu Lauriere, François Le Gall, and Mathys Rennela. Information cost of quantum communication protocols. *Quantum Information & Computation*, 16(3&4):181–196, 2016.

[KMN+07] Pieter Kok, William J Munro, Kae Nemoto, Timothy C Ralph, Jonathan P Dowling, and Gerard J Milburn. Linear optical quantum computing with photonic qubits. *Reviews of Modern Physics*, 79(1):135, 2007.

[KMW02] David Kielpinski, Chris Monroe, and David J Wineland. Architecture for a large-scale ion-trap quantum computer. *Nature*, 417(6890):709, 2002.

[KNR99] Ilan Kremer, Noam Nisan, and Dana Ron. On randomized one-round communication complexity. *Computational Complexity*, 8(1):21–49, 1999.

[KP16] Iordanis Kerenidis and Anupam Prakash. Quantum recommendation systems. *arXiv preprint arXiv:1603.08675*, 2016.

[Kus97] Eyal Kushilevitz. Communication complexity. In *Advances in Computers*, volume 44, pages 331–360. Elsevier, 1997.

[LBGP+07] Jérôme Lodewyck, Matthieu Bloch, Raúl García-Patrón, Simon Fossier, Evgueni Karpov, Eleni Diamanti, Thierry Debuisschert, Nicolas J Cerf, Rosa Tualle-Brouri, Steven W McLaughlin, et al. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Physical Review A*, 76(4):042305, 2007.

[LD98] Daniel Loss and David P DiVincenzo. Quantum computation with quantum dots. *Physical Review A*, 57(1):120, 1998.

[LGQW17] Li Liu, Fen-Zhuo Guo, Su-Juan Qin, and Qiao-Yan Wen. Round-robin differential-phase-shift quantum key distribution with a passive decoy state method. *Scientific Reports*, 7:42261, 2017.

[LME+09] Daniel Lancho, J Martinez, David Elkouss, M Soto, and Vicente Martin. Qkd in standard optical telecommunications networks. In *International Conference on Quantum Comunication and Quantum Networking*, pages 142–149. Springer, 2009.

[LMR13] Seth Lloyd, Masoud Mohseni, and Patrick Rebentrost. Quantum algorithms for supervised and unsupervised machine learning. *arXiv preprint arXiv:1307.0411*, 2013.

[LST09] Alexander I Lvovsky, Barry C Sanders, and Wolfgang Tittel. Optical quantum memory. *Nature photonics*, 3(12):706, 2009.

[Lut10] Andrew Lutomirski. An online attack against wiesner's quantum money. *arXiv preprint arXiv:1010.0256*, 2010.

[Mah18] Urmila Mahadev. Classical verification of quantum computations. *arXiv preprint arXiv:1804.01082*, 2018.

[MKB05] Florian Mintert, Marek Kuś, and Andreas Buchleitner. Concurrence of mixed multipartite quantum states. *Physical Review Letters*, 95(26):260502, 2005.

[MMM+08] DN Matsukevich, Peter Maunz, DL Moehring, Steven Olmschenk, and Chris Monroe. Bell inequality violation with two remote atomic qubits. *Phys. Rev. Lett.*, 100(15):150404, 2008.

[MP16] Subhayan Roy Moulick and Prasanta K Panigrahi. Quantum cheques. *Quantum Information Processing*, 15(6):2475–2486, 2016.

[MPA11] Lluís Masanes, Stefano Pironio, and Antonio Acín. Secure device-independent quantum key distribution with causally independent measurement devices. *Nature communications*, 2:238, 2011.

[NAS99] Yossi Matias Noga Alon and Mario Szegedy. The space complexity of approximating the frequency moments. *Journal of Computer and System Sciences*, 58(1):137–147, 1999.

[NC02] Michael A Nielsen and Isaac Chuang. Quantum computation and quantum information, 2002.

[New91] Ilan Newman. Private vs. common random bits in communication complexity. *Information Processing Letters*, 39(2):67–71, 1991.

[NS96] Ilan Newman and Mario Szegedy. Public vs. private coin flips in one round communication games. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 561–570, 1996.

[NVG+14] A Nicolas, L Veissier, L Giner, E Giacobino, D Maxein, and J Laurat. A quantum memory for orbital angular momentum photonic qubits. *Nature Photonics*, 8(3):234, 2014.

[PJL+14] Anna Pappa, Paul Jouguet, Thomas Lawson, André Chailloux, Matthieu Legré, Patrick Trinkler, Iordanis Kerenidis, and Eleni Diamanti. Experimental plug and play quantum coin flipping. *Nature Commun.*, 5:3717, 2014.

[PKL+15] Anna Pappa, Niraj Kumar, Thomas Lawson, Miklos Santha, Shengyu Zhang, Eleni Diamanti, and Iordanis Kerenidis. Nonlocality and conflicting interest games. *Phys. Rev. Lett.*, 114(2):020401, 2015.

[Pla13] Max Planck. *The theory of heat radiation*. Courier Corporation, 2013.

[PYJ+12] Fernando Pastawski, Norman Y Yao, Liang Jiang, Mikhail D Lukin, and J Ignacio Cirac. Unforgeable noise-tolerant quantum tokens. *Proceedings of the National Academy of Sciences*, 109(40):16079–16082, 2012.

[Raz99] Ran Raz. Exponential separation of quantum and classical communication complexity. In *Proceedings of the thirty-first annual ACM symposium on Theory of computing*, pages 358–367, 1999.

[RK11] Oded Regev and Bo'az Klartag. Quantum one-way communication can be exponentially stronger than classical communication. In *Proceedings of the forty-third annual ACM symposium on Theory of computing*, pages 31–40, 2011.

[RSA78] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[SBPC+09] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81(3):1301, 2009.

[Sha49] Claude E Shannon. Communication theory of secrecy systems. *Bell system technical journal*, 28(4):656–715, 1949.

[Sho99] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.

[SJZ+18] Lucas Schweickert, Klaus D Jöns, Katharina D Zeuner, Saimon Filipe Covre da Silva, Huiying Huang, Thomas Lettner, Marcus Reindl, Julien Zichi, Rinaldo Trotta, Armando Rastelli, et al. On-demand generation of background-free single photons from a solid-state source. *Applied Physics Letters*, 112(9):093106, 2018.

[SVB+14] Nicolò Spagnolo, Chiara Vitelli, Marco Bentivegna, Daniel J Brod, Andrea Crespi, Fulvio Flamini, Sandro Giacomini, Giorgio Milani, Roberta Ramponi, Paolo Mataloni, et al. Experimental validation of photonic boson sampling. *Nature Photon.*, 8(8):615–620, 2014.

[SZP+07] Michal Sedlák, Mário Ziman, Ondřej Přibyla, Vladimír Bužek, and Mark Hillery. Unambiguous identification of coherent states: Searching a quantum database. *Physical Review A*, 76(2):022326, 2007.

[TBZG98] Wolfgang Tittel, Jürgen Brendel, Hugo Zbinden, and Nicolas Gisin. Violation of bell inequalities by photons more than 10 km apart. *Physical Review Letters*, 81(17):3563, 1998.

[TDH+13] Max Tillmann, Borivoje Dakić, René Heilmann, Stefan Nolte, Alexander Szameit, and Philip Walther. Experimental boson sampling. *Nature Photon.*, 7(7):540–544, 2013.

[UM05] E Upfal and M Mitzenmacher. Probability and computing: Randomized algorithms and probabilistic analysis, 2005.

[VSB+01] Lieven MK Vandersypen, Matthias Steffen, Gregory Breyta, Costantino S Yannoni, Mark H Sherwood, and Isaac L Chuang. Experimental realization of shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature*, 414(6866):883, 2001.

[Wie83] Stephen Wiesner. S. wiesner, sigact news 15, 78 (1983). *Sigact News*, 15:78, 1983.

[WRD+06] SP Walborn, PH Souto Ribeiro, L Davidovich, F Mintert, and A Buchleitner. Experimental determination of entanglement with a single measurement. *Nature*, 440(7087):1022, 2006.

[WZ82] William K Wootters and Wojciech H Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.

[XAW+15] 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 Commun.*, 6:8735, 2015.

[Yao79] Andrew Chi-Chih Yao. Some complexity questions related to distributive computing (preliminary report). In *Proceedings of the eleventh annual ACM symposium on Theory of computing*, pages 209–213, 1979.

[Yao93] A Chi-Chih Yao. Quantum circuit complexity. 1993.

[ZYCM15] Zhen Zhang, Xiao Yuan, Zhu Cao, and Xiongfeng Ma. Round-robin differential-phase-shift quantum key distribution. *arXiv preprint arXiv:1505.02481*, 2015.