Security in Quantum Key Distribution Protocols

by

Mhlambululi Mafu

Submitted in fulfillment of the academic requirements for the degree of
Doctor of Philosophy
in the School of Chemistry and Physics,
University of KwaZulu-Natal, Durban
November 2013

As the candidate's supervisor I have approved this thesis for submission.

Signed:_____ Name:_____ Date:_____

Abstract

Quantum theory forms one of the most studied theories of nature. It has inevitably led to a number of different research areas. One of the breakthroughs was the development of quantum cryptography which now forms one of the most advanced subjects in this field. One aspect of quantum cryptography known as quantum key distribution (QKD) is the art of generating a secure key which is used to encode a secret message between two legitimate parties conventionally known as Alice, the sender, and Bob, the receiver, in the presence of an eavesdropper, known as Eve. The goal of QKD is to guarantee security in the presence of an eavesdropper, who has access to the communication channel and unlimited technology, to ensure she is unable to obtain useful information about the message. Since the generated key is random and unknown to Eve, she is unable to learn anything about the encoded message. The most interesting and amazing phenomenon about a QKD scheme is that its security is based on the laws of physics rather than the computational or mathematical algorithms as in classical cryptography.

The motivation behind this thesis is to provide a study of both theory and practical methods of security in QKD protocols. Concerning theory, we briefly clarify how the laws of physics allow the security of QKD protocols which are used for secret communication. Moreover, we give definitions, analysis and evaluation of tools used for proving the security of different classes of QKD protocols. On the practical side, we show an implementation of the Bennett 1992 (B92) protocol and a high dimensional mutually unbiased basis QKD protocol.

In particular, we derive an irreducible lower bound of the uncertainty on the simultaneous measurement of observables when one use the Tsallis entropy to express the quantum uncertainty relation. This shows a possibility of using the Tsallis entropies for quantifying information in QKD protocols. We highlight that the Tsallis entropies have not been extensively investigated for this application. We will also demonstrate an implementation of the B92 QKD protocol by using the id3100 Clavis^2 system at our laboratory at the University of KwaZulu-Natal. The id3100 Clavis^2 system has been traditionally used for the implementation of the Bennett-Brassard 1984 (BB84) and Scarani-Acín-Ribordy-Gisin 2004 (SARG04) protocols. We investigate also the secure key rates in the B92 protocol by using the Rènyi entropies and the uncertainty relations which have been introduced recently. Lastly, we extend our work by showing an implementation of a high dimensional filter based QKD protocol. This QKD protocol is based on mutually unbiased bases (MUBs) which are implemented by means of photons carrying orbital angular momentum (OAM). In particular, we show that by encoding in high dimension of MUBs leads to an increase in the key generation rate per photon.

Preface

The work described in this thesis was carried out in the School of Chemistry and Physics, University of KwaZulu-Natal, Durban, from January 2011 to November 2013, under the supervision of Professor Francesco Petruccione.

These studies represent original work of the author and have not otherwise been submitted in any form for any qualification to any University. Where use has been made of the work of others it is duly acknowledged in the text.

Declaration 1- Plagiarism

I, _____ declare that

i. The research reported in this thesis, except where otherwise indicated, is my original research.

ii. This thesis has not been submitted for any degree or examination at any other University.

iii. This thesis does not contain any other persons' data , pictures, graphs or other information, unless specifically acknowledged as being sourced from other persons.

iv. This thesis does not contain any other person's writing , unless specifically acknowledged as being sourced from other researchers. Where other written sources have been quoted, then:

- **a.** Their words have been re-written but the general information attributed to them has been referenced;
- **b.** Where their exact words have been used, their writing has been placed inside quotations marks, and referenced.

v. This thesis does not contain text, graphics or tables copied and pasted from the Internet, unless specifically acknowledged, and the source being detailed in the thesis and in the References sections.

Signed: _____

Declaration 2- Publications

This thesis is based on the following publications, which will be referred by their respective letters:

Peer-Reviewed Journal Papers

M1 **Mhlambululi Mafu**, Angela Dudley, Sandeep Goyal, Daniel Giovannini, Melanie McLaren, Miles J. Padgett, Thomas Konrad, Francesco Petruccione, Norbert Lütkenhaus and Andrew Forbes, "Higher-dimensional orbital angular momentum based quantum key distribution with mutually unbiased bases," *Physical Review A 88, 032305* (2013).
My contributions: I conceived the idea of using mutually unbiased bases implemented by orbital angular moment states in order to study security in high dimensional QKD protocols. I interpreted the raw data from the experimentalist in order to extract the required security parameters to be used in the proofs. The interpretation was done under the guidance of my collaborator Prof. N. Lütkenhaus. I also provided the QKD theory to the corresponding author.

M2 **Mhlambululi Mafu**, Kevin Garapo and Francesco Petruccione, "Finite-size key in the Bennet 1992 quantum-key-distribution for Rényi entropies," *Physical Review A 88, 062306 (2013).*
My contributions: I conceived the idea of applying the Rényi entropies together with their smoothed versions and the uncertainty relations to the B92 QKD protocol. I performed all the security proofs/derivations of the equations. I wrote the paper under the guidance of my supervisor Prof. F. Petruccione.

M3 **Mhlambululi Mafu**, Makhamisa Senekane, Abdul Mirza and Francesco Petruccione, "Implementation and security analysis of the Bennet 1992 quantum-key-distribution protocol using id3100 Clavis^2 system," *submitted to JOSA B (2013).*
My contributions: I was responsible for analyzing the raw data, perform the security analysis of the protocol, provide the QKD theory. I was also responsible for writing up the paper under the guidance of Prof. F. Petruccione.

M4 **Mhlambululi Mafu**, Adriana Marais and Francesco Petruccione, "A necessary condition for the security of coherent one-way quantum key distribution," *Appl. Math. Info. Sci. 8, No. 6, 1-6 (2014).*
My contributions: I was responsible for performing the calculations, security

analysis, drawing the diagrams and writing up the paper under the guidelines of the co-authors.

Conference Proceedings

M5 **Mhlambululi Mafu**, Adriana Marais and Francesco Petruccione, "A necessary condition for the security of coherent one-way quantum key distribution," *in Proceedings of the 56th South African Institute of Physics conference, pp. 811-816 (2011).*
My contributions: I was responsible for performing the calculations, security analysis, drawing the diagrams and writing up the paper under the guidelines of the co-authors.

M6 Makhamisa Senekane, Abdul Mirza, **Mhlambululi Mafu** and Francesco Petruccione, "Realization of B92 QKD protocol using id3100 Clavis^2 System," *in Proceedings of the 57th South African Institute of Physics conference (2012).*
My contributions: I was responsible for performing the calculations, security analysis. I was also responsible for providing the QKD theory to the corresponding author.

M7 **Mhlambululi Mafu** and Francesco Petruccione, "Derivation of the quantum bit-error-rate for the BB84 protocol based on the covariant-cloning machine," *in Proceedings of the 57th South African Institute of Physics conference (2012).*
My contributions: I was responsible for performing the calculations, security analysis, drawing the diagrams and writing up the paper.

M8 **Mhlambululi Mafu** and Francesco Petruccione, "Upper bound on the accessible information for the six-state quantum key distribution protocol," *in Proceedings of the 57th South African Institute of Physics conference (2012).*
My contributions: I was responsible for performing the calculations, security analysis and writing up the paper under the guidelines of my supervisor Prof. F. Petruccione.

M9 **Mhlambululi Mafu** and Francesco Petruccione, "Tsallis entropy and quantum uncertainty in information measurement," *in Proceedings of the 58th South African Institute of Physics conference (2013).*
My contributions: I conceived the idea of possibly using the Tsallis entropies in the context of Quantum cryptography. I derived the security bounds and wrote the paper under the guidelines of my supervisor Prof. F. Petruccione.

M10 Angela Dudley, **Mhlambululi Mafu**, Sandeep Goyal, Daniel Giovannini, Melanie McLaren, Miles J. Padgett, Thomas Konrad, Francesco Petruccione, Norbert Lütkenhaus and Andrew Forbes, "Encoding mutually unbiased bases orbital angular momentum for quantum key distribution," *To appear in SPIE conference proceedings (2014).*

My contributions: I conceived the idea of using mutually unbiased bases implemented by orbital angular moment states in order to study security in high dimensional QKD protocols. I interpreted the raw data from the experimentalist in order to extract the required security parameters to be used in the proofs. The interpretation was done under the guidance of my collaborator Prof. N. Lütkenhaus. I also provided the QKD theory to the corresponding author.

Talks presented

1. **Mhlambululi Mafu**, Adriana Marais, Abdul Mirza and Francesco Petruccione, "Security of quantum cryptography protocols," 55^{th} South African Institute of Physics conference (2010).
2. **Mhlambululi Mafu**, Adriana Marais and Francesco Petruccione,"Towards the unconditional security proof of the Coherent-One-Way QKD Protocol," 56^{th} South African Institute of Physics conference (2011).
3. **Mhlambululi Mafu** and Francesco Petruccione, "Finite key-size analysis in QKD protocols," Quantum Information Processing Communication and Control (QIPCC^2) conference, Mont aux Sources Hotel, Northern Drakensberg, South Africa (2011).
4. **Mhlambululi Mafu** and Francesco Petruccione, "Derivation of the quantum bit-error-rate for the BB84 protocol based on the covariant cloning machine," 57^{th} South African Institute of Physics conference (2012).
5. **Mhlambululi Mafu** and Francesco Petruccione, "Finite-size key in B92 QKD for Rényi entropies," 58^{th} South African Institute of Physics conference (2013).

Posters presented

1. **Mhlambululi Mafu**, Adriana Marais and Francesco Petruccione, "Towards the security of COW QKD protocol," QCRYPT Conference, Zurich, Switzerland (2011).
2. **Mhlambululi Mafu** and Francesco Petruccione, "Upper bound on the accessible information for the six-state quantum key distribution protocol," 57^{th} South African Institute of Physics conference (2012).
3. **Mhlambululi Mafu** and Francesco Petruccione, "Tsallis entropy and quantum uncertainty in information measurement," 58^{th} South African Institute of Physics conference (2013).

Schools attended

1. 4th Winter School on Practical Quantum Cryptography
   Les Diablerets, Geneva, Switzerland
   23-26 January 2012.

2. The 2012 South African School and Workshop on Theoretical Aspects of Quantum Information and Quantum Computing
   African Institute for Mathematical Sciences
   CapeTown, South Africa
   11 - 16 June 2012.

Research Visits

1. Visited Professor Norbert Lütkenhaus at Institute for Quantum Computing (IQC), University of Waterloo, Canada
   Research Interest: Security of quantum key distribution
   18 November 2012-17 May 2013.

Awards

1. Golden Key International Honor Society - August 2011.

Signed: _____

Acknowledgments

I would like to thank my supervisor Professor Francesco Petruccione for giving me the opportunity to join his Quantum Research Group. I would also like to thank him for his academic and non-academic support, undampening motivation during all times of my research. I would also like to thank Dr IIya Sinayskiy for his support and his positivity throughout all calculations and discussions which we held together. I am also indebted to thank Mr McLean Sibanda for introducing me to Francesco Petruccione and his encouragement that I join this Quantum Research Group in Durban.

I would like to express my gratitude to Professor Norbert Lütkenhaus for interesting and constructive discussions. In particular, I thank him for the opportunity he afforded me to work with him for six months at Institute for Quantum Ccomputing, University of Waterloo, Canada. His expertise in the field gave me direction and his answers to all my questions have yielded part of this work. I thank also the members of his research Group, Oleg, Juan-Miguel, William and Agnes for all the care and support that they offered me. Sincere thanks goes to Matthew Fries who went through all the administration work during my entire stay in Waterloo.

I would also like to thank my collaborators for affording me the chance to work with them. They are Angela Dudley, Sandeep K. Goyal, Norbert Lütkenhaus, Thomas Konrad, Andrew Forbes, Abdul Mirza, Makhamisa Senekane, Kevin Garapo, Adriana Marais, Daniel Giovannini, Melanie McLaren, Miles J. Padgett and Francesco Petruccione. I also greatly give thanks to Lana Sheridan for all the discussions and email conversations we held during my studies. It has been a pleasure to work with her. Great thanks also to Abdul Mirza for correcting the first draft of my thesis.

Profound thanks also goes to my family particularly Triyiphina Msimanga, Memo Mafu and Enia Msimanga for standing by my side always. I extend my thanks with sincere gratitude to my fiancee' Boithathelo Tracy Mbizo for all her support during my studies. Many thanks also goes to my friends Blessing, Kevin, Butholezwe, Bhekusizi, Malvin, Confident and Makhamisa for the motivation and the fun that we had during my studies.

I would like to extend my sincere thanks to all the criticisms and thoughts which I received from different members of my Quantum Research Group.

Finally, I thank God the Almighty who has brought me this far.

This work is supported by the South African Research Chair Initiative of the Department of Science and Technology and National Research Foundation.

Contents

List of Figures

List of Tables

Chapter 1

Overview and Motivation

1.1 Introduction

It took centuries for mathematicians to discover a system that would enable users to exchange messages in absolute secrecy. It was until the 1940's when Claude Shannon [3] proved that this goal was possible if only the communicating parties shared a random secret key that is as long as the message which they wish to communicate. However, this had a constraint too. This disadvantage motivated the need to find a secure means of key distributor. Quantum cryptography was initially proposed by Stephen Wiesner [4] when he discovered that quantum mechanical effects (i.e., the no cloning theorem [5] and the Heisenberg uncertainty principle [6, 7]) could be used to produce banknotes that would be impossible to counterfeit. Owing to the fact that quantum information cannot be cloned, a copy of a banknote that contained quantum information cannot be produced.

Based on Wiesner's ideas, Gilles Brassard and Charles Bennett came up with a quantum protocol for two cryptographic primitives: for distributing secret keys among distant parties and bit commitment. This gave birth to the first operable QKD protocol in 1984, now known as the BB84 protocol [8]. This protocol is based on the polarization of single photons in which a stream of single photons are distributed between two parties that are in turn used to develop a symmetric key. The BB84 protocol has been proven to be unconditionally secure by using different approaches [9, 10, 11, 12]. In 1991, Artur Ekert proposed an entanglement-based (EB) protocol known as the Ekert 1991 (E91) protocol [13]. In this protocol, entangled pairs of qubits are distributed between two legitimate parties. The key bits are extracted by performing measurements on the received qubits [14]. The security of the E91 protocol is based on the violation of Bell's inequalities. In 1992, Bennett-Brassard-Mermin (BBM92) recognized that a simpler version of an EB QKD protocol can be converted to the BB84 protocol, where Alice and Bob measures the qubit in one of two mutually unbiased bases [15]. Again in 1992, Bennett developed a protocol in which Alice sends one of two the nonorthogonal states to Bob and this protocol is commonly known as the B92 protocol [16]. This protocol uses two weak coherent states together with a strong reference pulse. The B92 protocol

has been proven to be unconditionally secure [17, 18]. In 1998, another variant of the BB84 protocol which instead of using four states uses six states was proposed [19]. In this protocol, Alice sends each qubit to Bob in one of six possible states. Later in 2004, Scarani and others by using the four states of the BB84 protocol with a different encoding invented the SARG04 protocol [20]. This protocol has been proven to be robust when attenuated laser pulses are used instead of the single photon sources. The above protocols belong to a class called Discrete Variable (DV) protocols [14]. The DV protocols have been greatly studied and their unconditional security proofs have also been realized. However, due to demands in communication speeds at high bit rates, another class called the Distributed-Phase-Reference protocols were proposed in 2002 [14]. Members of this class are the Coherent-One-Way protocol [21] and Differential-Phase-Shift protocol [22] where the coherence of sequential pulses plays a crucial role in the security. The Distributed-Phase-Reference protocols are tailored to work with weak coherent pulses at high bit rates and have proven to be most practically implementable in the existing communication fibre network. However, this class of QKD protocols has not been proven to be unconditionally secure [23]. The current methods for proving security as those used in qubit-based protocols cannot be applied in a straight forward way to this class of protocols because they implement a completely different encoding. Another class of protocols called the Continuous Variable (CV) protocols was developed in 2002 [14]. In this class of protocols, information is encoded on the continuous variables of the electromagnetic field. Alice sends squeezed states and Bob performs homodyne measurements. The CV protocols show some good performance over large distances as compared to DV protocols [24]. The security of these protocols has been considered in [25, 26, 27].

This progress in QKD protocols has been followed by a series of review papers that dwell on the theory and implementation of quantum cryptography. Moreover, these developments have led to commercialization of several QKD products [28, 29] and also several QKD implementations notably the QKD-based network that was presented in October 2008 in Vienna, Austria [30] and the realization of long-term quantum cryptography in Durban [31] and the high-rate QKD over 100 km [32], the Tokyo QKD Network [33] and the SwissQuantum QKD [34].

Quantum cryptography, specifically QKD has been built based on physical concepts associated with quantum mechanics. In contrast to conventional cryptography, whose security is based on the complex computational and mathematical algorithms for security, it is founded on the uncertainty relations, Bell's inequalities, entanglement or non-locality [5]. The implementation of QKD consists of detectors, repeaters, quantum memories, decoy states [35, 36, 37]. These concepts form the basis of security proofs [38]. In order for Eve to obtain the secret key, she needs to break the laws of physics, but this is impossible without her presence being detected. Since there is great need for security in a communication system it is necessary to investigate security proofs for QKD systems. This is one of the objectives of this thesis.

Regardless of the challenges that come with developing unconditional security proofs, a lot of progress has been realised in the last two decades. An unconditional security proof considers all kind of attacks that Eve can perform and incorporating this into the security proof is a difficult task. However, a new technique for analysing collective

attacks due to an eavesdropper was developed in 1995 by Yao [39]. Later, Bennett and others realised that if the legitimate parties possess a reliable quantum computer, they can implement an entanglement distillation (ED) protocol to obtain a secure version of an EB key distribution [40]. In 1998, based on this idea, Lo and Chau then developed a formal security proof for the protocol [41]. By using the ideas of Mayers, Lo and Chau then Shor and Preskill developed a simple proof of security for the BB84 protocol in 2000 [42]. This was followed by a proof of Biham who was the second to show an unconditional security proof [43]. In 1991, Biham's proof was then used by Gottesman and Preskill to prove the unconditional security proof of a continuous variable protocol where Alice's signals are sufficiently squeezed [44]. In the same spirit, Inamori *et al.* showed the unconditional security proof of BB84 protocol where Alice's source emits weak coherent states and Bob's detector remains uncharacterized [11]. However, a complete security proof that is secure against arbitrary attacks by the eavesdropper and full realistic implementation of the QKD protocol remains missing. But this progress depicts that major achievements have been made in this field to prove that protocols used in quantum communication are secure for sending messages. Amongst different approaches to security proofs, a number of publications on composable security [45], de Finetti's theorem [38, 46], post-selection technique [47] and recently the finite-length key analysis [12] are now available.

Regardless of enormous progress that has been made in QKD, there are still some theoretical and experimental problems of communicating in absolute secrecy in the presence of an eavesdropper. In particular, matching the theoretical security proofs to real devices still remains unknown. The security proofs still contain assumptions concerning the behavior of devices used by the communicating parties [48]. As a result of this mismatch, an eavesdropper can learn part of the key shared by Alice and Bob, thus rendering some schemes insecure over large distances. Moreover, the existing security proofs have been derived in the asymptotic limit which is not very realistic. In fact, the bits which are processed in QKD are necessarily of finite length. Therefore, thanks to Valerio and Renner for introducing the general framework for the security analysis of QKD with finite resources [12].

1.2 Setting the scene

We recall that the goal of QKD is to provide secure communication between Alice and Bob in the presence of a potential eavesdropper, known as Eve. Alice and Bob use a key to encrypt and decrypt their message either by symmetric key cryptography or an asymmetric key cryptography. Encryption refers to the art of taking a message and apply a mathematical algorithm so that it looks random to the eavesdropper. Decryption refers the process of taking that random data, apply a different operation and then retrieve the original message. In a symmetric scheme, an identical key is distributed between Alice and Bob. Both parties distribute and agree on the secrecy of the key before any secure communication takes place. A function is then used to combine the information with the key to produce a ciphertext (i.e., encryption). This function is publicly known but the symmetric key is transferred privately. Since the key shared

between Alice and Bob is secret, Alice simply compresses her message and XOR it with the key. Alice then sends her result to Bob who XORs it again with the key to recover the compressed message. This is called One-Time Pad (OTP) encryption [49]. Symmetric key cryptography is unconditionally secure only if the symmetrically distributed key is unconditionally secure, while the security of the asymmetric scheme lies on the assumption that factoring integers proves to be a difficult task.

The security of asymmetric cryptography depends on the existence of one-way functions for example the RSA scheme [50], which is based on the prime factorization of large integers. In the RSA scheme, an efficient algorithm multiplies two prime numbers while a different algorithm is used to factor the product of the multiplication into its individual prime numbers. One way functions allow easy computation of a result given some parameters, while the reverse is rather a difficult task. Such functions are known as trap door functions. Unfortunately, there exists no mathematical proofs for one-way functions. In contrast to symmetric cryptography, in this scheme both a public and private key is produced through these functions. The key for encrypting the data can be made public while the key for decrypting the data should be kept private. When given only the public key it is computationally difficult to retrieve the private key, but the reverse is possible [50]. However, the factorisation algorithm proposed by Peter Shor in 1994 offers an efficient quantum algorithm for such reverse functions [51]. Therefore, with the development of quantum computers the security of asymmetric cryptosystems calls for further investigation. Quantum computers promise to be a real threat to classical cryptography.

The integrity of information between Alice and Bob relies on the ability to protect the information from Eve. This means in order to achieve secure communication there has to be a provable secret and a genuinely random binary key of specific length which is going to be used to transfer information between Alice and Bob. However, there lies the problem of distributing the key. The quantum approach to this distribution is therefore called QKD. The quantum information that the approach uses is so fragile that one cannot eavesdrop on a quantum channel without perturbing the quantum information that is being transmitted. So, if Alice tries to transmit a piece of quantum information to Bob, they can always check whether an eavesdropper is present or not. Thus, the most outstanding phenomena about quantum cryptography is that it solves the problem of key distribution considering that the information being transmitted should not be found in the wrong hands of the eavesdropper. With QKD, it is possible for Alice and Bob to perform a protocol that allows them to share an unconditionally secure key, which means that the eavesdropper cannot learn anything about the message except with some small probability.

As much as the theoretical and technological concepts stand to be true there still stands unresolved problems in integrating them into the image of the real world for example, sending secure keys for more that 300km and the problem of side channels.

1.3 Thesis outline

This thesis is arranged as follows:

- Chapter 1 gives an overview and motivation of this thesis. This Chapter briefly outlines the developments in the security of QKD and also sets the scene for this study.
- Chapter 2 presents preliminaries that spells out some of the basic tools and formulas which are going to be used throughout this thesis.
- In Chapter 3 a study of the various information measures and their application is given. In particular, we explore the main concepts of classical information theory and quantum information respectively and their definitions, which are going to be used in our work to quantify information and also in various calculations and derivations. These will also be necessary in order to understand the security of QKD protocols.
- In Chapter 4, a review on QKD protocols is presented. The main concept and principle of QKD on how it allows secure communication is also reviewed. The security of protocols in the asymptotic and non-asymptotic regimes are presented. In this thesis, we follow closely the security framework of Scarani and Renner in [12].
- In Chapter 5, the derivation of security bounds for the Bennett 1992 protocol for finite resources by using the Rényi entropies and uncertainty relations is presented. This work appears in the publication **M2**.
- Chapter 6 studies the Tsallis entropies and their possible application in the security of QKD protocols. This Chapter is based on the manuscript **M9**.
- In Chapter 7, we make a study of the implementation and security analysis of the Bennett 1992 protocol by using the id3100 Clavis^2 system at our laboratory. This Chapter is based on the manuscript **M3** & **M6**.
- In Chapter 8, an outline on the realization and security analysis of a high dimensional filter based QKD protocol by MUBs implemented using OAM states is made. This Chapter appears in the publication **M1** & **M10**.
- In Chapter 9, we draw a conclusion from the obtained results and present further lines of investigation.

Chapter 2

Preliminaries

The objective of this Chapter is to discuss the basic notions of mathematical foundations of quantum mechanics for finite dimensions. The basic principles of linear algebra as used in quantum information theory will also be outlined. We also give definitions and basic formulation of other tools which are needed in the Chapters that follow.

2.1 Probability

Information theory is largely based on probability theory. Therefore, we come to introduce briefly the concept of probability theory. A probability space or event space refers to a set (Ω, P) where Ω is a measurable space and P is a probability measure. This means that to each subset, $A \subset \Omega$ (i.e., event) we associate the probability [52, 53, 54]

$$P(A) = \text{probability of } A, \tag{2.1.1}$$

where $0 \leq P(A) \leq 1$. The probability of the whole space is normalized to be $P(\Omega) = 1$ and $P(\emptyset) = 0$. For two disjoint events A and B, we have $P(A \cup B) = P(A) + P(B)$, and for independent events A and B we have $P(A \cap B) = P(A)P(B)$. The probability that the event A occurs if we already know that the event B has occurred is known as conditional probability. It is defined as [55]

$$P(A|B) = \frac{P(A \cap B)}{P(B)}. \tag{2.1.2}$$

2.2 Hilbert Space

Based on the state space postulate of Quantum mechanics, one can associate any isolated physical system with a Hilbert space, known as the state space of the system [5]. The Hilbert space is a mathematical concept, it is a vector space over the complex numbers $\mathbb{C}$ with a complex valued inner product or scalar product $\langle \cdot, \cdot \rangle : \mathcal{H} \times \mathcal{H} \to \mathbb{C}$, which

is complete with respect to the norm $||x|| = \sqrt{\langle x, x\rangle}$ where $||x||$ is interpreted as the length of vector x [52, 56]. In Quantum mechanics, elements of the Hilbert space are called states kets. If $|x\rangle$ and $|y\rangle$ are arbitrary vectors in the Hilbert space $\mathcal{H}$, then the inner product is denoted as

$$\begin{aligned}\langle x|y\rangle &= (\sum_i x_i|i\rangle, \sum_i y_j|j\rangle) \\ &= \sum_{ij} x_i^* y_j \langle i|j\rangle \\ &= \sum_{ij} x^* y_j \delta_{ij} \\ &= \sum_i x_i^* y_i \end{aligned} \tag{2.2.1}$$

for finite values of i, i.e., $\{|x_i\rangle, |1, ..., n\}$ and similarly for j, i.e., $\{|y_j\rangle, |1, ..., n\}$. An inner product satisfies three basis axioms which are:

1. positive definiteness $\langle x, x\rangle \geq 0$,
2. conjugate symmetry $\langle x, y\rangle = \langle y, x\rangle^*$,
3. linearity in the second variable $\langle x, \alpha y + \beta z\rangle = \alpha\langle x, y\rangle + \beta\langle x, z\rangle$ and $\langle \alpha x + \beta y, z\rangle = \alpha^*\langle x, z\rangle + \beta^*\langle x, z\rangle$ where $\alpha, \beta \in \mathbb{C}$.

These axioms imply the Schwarz inequality, $|\langle x, y\rangle|^2 \leq \langle x, x\rangle\langle y, y\rangle$ [57].

2.3 Tensor product

In order to create a larger vector space from smaller vector spaces, a tensor product operation is used. If $|v_i\rangle$ and $|w_j\rangle$ are two orthogonal bases in vector spaces $\mathcal{V}$ and $\mathcal{W}$ ($\mathcal{V} \cap \mathcal{W} = \emptyset$), respectively, then two arbitrary vectors are denoted as $|\psi\rangle = \sum_i \alpha_i|v_i\rangle$ and $|\phi\rangle = \sum_j \beta_j|w_j\rangle$. The tensor product of these two vectors is given by [58]

$$\begin{aligned}|\psi\rangle \otimes |\phi\rangle &= (\sum_i \alpha_i|v_i\rangle) \otimes (\sum_j \beta_j|w_j\rangle) \\ &= \sum_{ij} \alpha_i\beta_j|v_i, w_j\rangle. \end{aligned} \tag{2.3.1}$$

For example given the states $|101\rangle$ and $|10\rangle$ their tensor product is $|101\rangle \otimes |10\rangle = |10110\rangle$ [5].

Composite systems According to postulate of composite systems of Quantum mechanics, the state space of a composite physical system is a tensor product of the state spaces of the component physical systems i.e., a tensor product of Hilbert spaces [5].

Composite systems correspond to a system which is described by more than one system, e.g., $|\psi_1\rangle$ and $|\psi_2\rangle$ and these are written in a tensor form as $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ or $|\psi\rangle = |\psi_1\rangle|\psi_2\rangle$. In the study of composite systems, we consider two theorems; Purification and Schmidt decomposition [59]. These are briefly discussed below.

Purification Purification is a mathematical procedure which allows one to associate pure states and mixed states. Suppose the state ρ_A on system A can be represented as $\rho_A = \sum_i p_i |i_A\rangle\langle i_A|$. Then there exists an additional system R and a pure state $|\psi_{AR}\rangle$ on the joint system AR such that $\rho_A = \mathrm{tr}_R |\psi\rangle\langle\psi|_{AR}$. The pure state $|\psi\rangle_{AR}$ is called a purification of ρ_A. If $\{|i_R\rangle\}_i$ is an orthonormal basis on the system R which has the same dimension as A meaning $\langle i_R|j_A\rangle = \delta_{ij}$, then the purification can be constructed as [58, 60]

$$|\psi\rangle_{AR} = \sum_i \sqrt{p_i}|i_A\rangle|i_R\rangle. \tag{2.3.2}$$

Schmidt decomposition The Schmidt decomposition is a mathematical tool used to analyze a pure state and its partial trace [58]. Consider a pure state $|\psi\rangle_{AB}$ of a bipartite system AB with the Hilbert space, $\mathcal{H}_A \otimes \mathcal{H}_B$, d_A=dim$\mathcal{H}_A$ and d_B=dim$\mathcal{H}_B$, with orthonormal bases $\{|j\rangle_A\}$ and $\{|j'\rangle_B\}$ for $\mathcal{H}_A$ and for $\mathcal{H}_B$, respectively, such that

$$|\psi\rangle_{AB} = \sum_j \lambda_j |j\rangle_A |j'\rangle_B, \tag{2.3.3}$$

where $\lambda_j (j = 1, ..., n)$ are non-negative real numbers satisfying $\sum_j {\lambda_j}^2 = 1$. The λ_j's are known as Schmidt coefficients [58]. Equation (2.3.3) is called the Schmidt decomposition of $|\psi\rangle_{AB}$. The number of non-vanishing eigenvalues is called the Schmidt number of $|\psi\rangle_{AB}$. The Schmidt number is an important property of a composite quantum system, in the sense that it quantifies the amount of entanglement between system A and system B. If the Schmidt number is greater than one, then the bipartite pure state is entangled [59]. For the proof of the Schmidt decomposition, see Appendix A.

2.4 Linear Operator

The state change of qubits is performed by linear operators. A linear operator is a transformation which makes a correspondence of vectors from $\mathcal{V}$ to $\mathcal{W}$. We can describe this function in the form of a matrix representation in finite dimensional case, $A = m \times n$. If this matrix is multiplied with a vector $|v\rangle \in \mathbb{C}^n$, it results in a new vector $|w\rangle \in \mathbb{C}^m$. The claim for this representation of the operator in space $\alpha(\mathbb{C}^n, \mathbb{C}^m)$ is that it fulfills the linearity equation

$$A(\sum_i a_i |v_i\rangle) = \sum_i a_i A|v_i\rangle. \tag{2.4.1}$$

Let $A : v \mapsto w$ be the linear operator and $|v_i\rangle, ..., |v_n\rangle$ be a basis of $\mathcal{V}$ and $|w_i\rangle, ..., |w_n\rangle$ be a basis of $\mathcal{W}$, then there exists complex numbers

$$A|v_j\rangle = \sum_i A_{ij}|w_i\rangle \quad \text{with} \quad 1 \le i \le m, 1 \le n, \tag{2.4.2}$$

which constitute a matrix representation of A.

2.5 States

Quantum play an important role in quantum communication. Quantum communication allows secure transfer of classical messages by encoding information in quantum states. Below we shall briefly review these quantum states by giving their definition, properties as well as their applications.

2.5.1 Pure States

Based on the state space postulate of Quantum mechanics, associated to any isolated physical system is a complex vector space with inner product known as a state space of the system [5]. The system is completely characterized by its state vector which is a unit vector in a Hilbert space. In quantum computation and quantum information theory, the conventional unit is a qubit. This corresponds to a classical bit in classical information theory. A classical bit has a state of either 0 or 1 while a qubit exists as a combination (superposition) of the basis states $|0\rangle$ and $|1\rangle$. A pure state is a normalized vector of $\mathbb{C}^2$ represented as:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{2.5.1}$$

where α and β are complex numbers with $|\alpha|^2 + |\beta|^2 = 1$. The basis states $|0\rangle$ and $|1\rangle$ are also known as computational basis. If α and β are real, it can be represented by means of a Bloch sphere. States correspond to density operators, ρ. The density operator has the following properties (i) It is positive-semidefinite, $\rho \geq 0$, (ii) It has unit trace, $\mathrm{tr}(\rho)$=1 and (iii) $\rho = \rho^\dagger$ [61]: For a pure state, the density operator can be written as $\rho = |\psi\rangle\langle\psi|$ and $\mathrm{tr}(\rho^2) = 1$ [52, 61].

2.5.2 Mixed States

A mixed state refers to a state which cannot be represented as a vector in a Hilbert space $|\psi\rangle$. Mixed states are probabilistic mixtures of pure states and therefore form a generalization of pure states. For example, if a quantum state has a probability of p_j to be in the state $|\psi_j\rangle$ for $j = \{1, 2, ...n\}$, then the system is an ensemble of pure states $\{p_j|\psi_j\rangle\}_{j=1}$ and is described by a density matrix [59]

$$\rho = \sum_{j=1}^{n} p_j|\psi_j\rangle\langle\psi_j| \in \mathcal{B}(\mathcal{H}), \quad \text{with} \quad \sum_{j=1}^{n} p_j = 1 \quad \text{and} \quad p_j \geq 0, \tag{2.5.2}$$

where $|\psi_j\rangle \in \mathcal{H}$ and $\mathcal{B}(\mathcal{H})$ is the bounded algebra on the Hilbert space [58, 43].

2.5.3 Entangled States

Quantum mechanics attests that a set of particles can be in an entangled state even if they are spatially separated. This means that a measurement performed on one of the particles may uniquely determine the result of a measurement on the spatially separated paired particle. This led to Einstein calling this phenomenon "spooky action at a distance" [62]. This is because a measurement in one place seems to have an instantaneous effect at another distant place. This forms a useful property in quantum communication, particularly in teleportation [63]. An entangled quantum state contains non-classical correlations which are called quantum correlations or Einstein-Podolsky-Rosen (EPR) correlations. An entangled quantum state cannot be expressed as a tensor product states of individual subsystems [58, 64, 55].

Quantum entanglement forms a precious computation and communication resource, it yields a significant practical application in QKD where Alice and Bob generate a random key through an unconditionally secure way [65]. Entanglement is also used in quantum dense coding where two classical bits can be transmitted by using one qubit provided Alice and Bob share an entangled state before the communication commences [66]. Also, quantum teleportation exploits a shared entangled state to transmit an arbitrary quantum state from Alice to Bob using LOCC [67]. The quantum cryptography scheme by Ekert [13] also relies on the distribution of entangled particles.

A pure state, that is a projector $|\psi_{AB}\rangle\langle\psi_{AB}|$ on a vector $|\psi_{AB}\rangle \in \mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$, is a product state if the states of local systems are also pure states, i.e., if $|\psi_{AB}\rangle = |\psi\rangle_A \otimes |\psi\rangle_B$. However, if states cannot be written in this form then they are called entangled states. An important example of an entangled state in $\mathcal{H}_A \otimes \mathcal{H}_B$ is the Bell state. A Bell state is a maximally entangled quantum state of two-qubits. The two-qubit entangled state consist of four Bell states [5]

$$\begin{aligned}
|\psi^+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B), \\
|\psi^-\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B - |1\rangle_A \otimes |1\rangle_B), \\
|\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B + |1\rangle_A \otimes |0\rangle_B), \\
|\Phi^-\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B). \qquad (2.5.3)
\end{aligned}$$

The Bell states are also referred to as EPR pairs. They possess an important property that their measurement outcomes are correlated [52, 63].

2.6 Quantum operations

Quantum operations play a major role in various aspects of quantum information-theoretic techniques. As an example, they are used to describe any physical process that a quantum mechanical system undergoes. These include; time evolution of the

state of an open system, quantum data compression, and description of what happens to quantum information when it is transmitted from a sender to receiver through a noisy quantum channel. This is analogous to the transmission of information through a noisy channel. In this view, a quantum operation (or superoperator) is also referred to as a quantum channel [61, 68].

2.6.1 Unitary operations

The state $|\psi\rangle$ of a quantum system with the density matrix ρ, can be transformed by applying a unitary operator $\mathcal{U}$. The time evolution according to Schrödinger dynamics gives rise to a unitary operation denoted as

$$\rho \mapsto \mathcal{U}\rho\mathcal{U}^{\dagger}, \tag{2.6.1}$$

where $\mathcal{U}$ is the unitary operator (i.e., $\mathcal{U}^{\dagger}\mathcal{U} = \mathbb{1}$), on the Hilbert space $\mathcal{H}$, of the system. Unitary operations are used to describe only the evolution of closed systems [69].

2.6.2 Quantum Channel

A quantum channel is a completely positive, trace preserving map. Quantum channels are used to transmit quantum information as well as classical information. A quantum channel can be represented as a map $\mathcal{E}$ [61].

$$\mathcal{E}(\rho) = \sum_{m} E_m \rho E_m^{\dagger} \tag{2.6.2}$$

where $\mathcal{E}$ is a linear operator from $\mathcal{H}_A$ to $\mathcal{H}_B$ and $\sum_m E_m^{\dagger} E_m \leq \mathbb{1}$. The term E_m is called the Kraus operator [70]. If $\mathcal{E}$ is a trace preserving process, then the completeness relation holds

$$\sum_{m} E_m^{\dagger} E_m = \mathbb{1}. \tag{2.6.3}$$

If the channel is unitary, then it satisfies the following

$$\sum_{m} E_m E_m^{\dagger} = \mathbb{1}. \tag{2.6.4}$$

2.7 Measurements

2.7.1 Projective Measurements

A projective measurement is described by an observable $\hat{O}$, a Hermitian operator on the state space of the system being observed. The observable has a spectral decomposition given by [5]

$$\hat{O} = \sum_{m} e_m P_m, \tag{2.7.1}$$

where e_m are measurement outcomes, P_m is a Hermitian projector (i.e., $P_m^\dagger = P_m$ and $P_m^2 = P_m$) onto the eigenspace of $\hat{O}$ with eigenvalue m. The expectation value of the observable is given as

$$\langle \hat{O} \rangle = \sum_m e_m p(m), \tag{2.7.2}$$

where $p(m)$ is the probability of obtaining an outcome e_m of measuring the state $|\psi\rangle$, and is expressed as [59]

$$p(m) = \langle \psi | P_m | \psi \rangle. \tag{2.7.3}$$

If e_m occurred, the state of the quantum system after the measurement becomes

$$\begin{aligned} |\psi'\rangle &= \frac{1}{\sqrt{p(\lambda_m)}} P_m |\psi\rangle \\ &= \frac{1}{\sqrt{\langle \psi | P_m | \psi \rangle}} P_m |\psi\rangle. \end{aligned} \tag{2.7.4}$$

2.7.2 Positive Operator-Value Measurements (POVM)

General quantum measurements are objects of quantum information processing which are described by positive operator-valued measure (POVM). For a finite set of Hermitian operators $\{E_m\}$ with any E_m being a positive operator (meaning $\langle \psi | E_m | \psi \rangle \geq 0$ for any normalized state $|\psi\rangle$), satisfy the completeness relation [5]

$$\sum_m E_m = \mathbb{1}. \tag{2.7.5}$$

The operators E_m which satisfy the above condition are known as POVM operators. The projection or von-Neumann measurements, with the set $\{M_m = |\lambda_m\rangle\langle\lambda_m|\}$ being defined by the n eigenstates of an observable, represent a specific case of a POVM set.

2.7.3 Stinespring's Dilation

The Stinespring's factorization theorem or dilation theorem gives us a basic theorem for quantum channels. It states that every completely positive and trace-preserving map can be built from 3 basic operations [71]:

1. tensoring the input with a second system in a specified state which is conventionally called the ancilla system,
2. unitary transformation of the combined input-ancilla system,
3. reduction to a subsystem.

This theorem can be stated formally as:

Theorem. Let $\mathcal{E} : S(\mathcal{H}) \mapsto S(\mathcal{H})$ be a CPTP map on a finite-dimensional Hilbert space $\mathcal{H}$. Then there exist a Hilbert space $\mathcal{K}$ and a unitary operation $\mathcal{U}$ on $\mathcal{H} \otimes \mathcal{K}$ such that:

$$\mathcal{E}(\rho) = \mathrm{tr}_{\mathcal{K}} \mathcal{U}(\rho \otimes |0\rangle\langle 0|)\mathcal{U}^{\dagger}, \tag{2.7.6}$$

for all $\rho \in S(\mathcal{H})$. The ancilla space $\mathcal{K}$ can be chosen such that $\dim \mathcal{K} \leq \dim \mathcal{H}^2$.

This representation is unique up to a unitary equivalence [72, 73]. Therefore, the Stinespring's dilation theorem gives a bound on the dimension of the Hilbert space of the ancilla, and states that the representation is unique up to unitary equivalence [71].

Chapter 3

Information Measures

Information theory is the mathematical theory that allows one to quantify information by deriving bounds on the processes such as acquisition, transmission and storage of information [61]. The three important applications of information theory are: transmission of data through specialised codes that enable error correction, compression and encryption [59]. In this chapter we focus on one of the most important aspects of information, i.e., measurement of information. Information can be measured according to its degree of uncertainty, i.e., if an event is likely then we gain little information in learning that it finally occurred and the converse is true. This brings us to the concept of entropy [53]. A brief review of classical and quantum entropy, the definition, properties and applications are made in the following sections.

3.1 Classical Information Measures

3.1.1 Shannon entropy

The Shannon entropy was introduced by Claude E. Shannon in 1948 [3]. The Shannon entropy is used to quantify the expected value of information contained in a message, i.e., a specific realization of the random variable. Suppose, in a sequence of n letters (where n is large), it is highly likely that many of these sequences depict the relative frequencies within themselves. Therefore, the probability p_i of choosing a letter x_i occurs with probability, $p_i = n_i/n$. There are $n!$ ways of arranging n characters, then for a character x_i, there are n_i permutations which leads to [59, 74]

$$X_n = \frac{n!}{n_1!n_2!...n_N!}, \tag{3.1.1}$$

sequences with $\sum_{i=1}^{N} n_i = n$. In the case of an infinitely long text where $n \mapsto \infty, n_i \mapsto \infty$, then by using Stirling's formula $\log(n!) = n\log n - n + O(\log n)$ for the logarithm

of the number X_n, we arrive at

$$\log X_n \mapsto n \log n - n - \sum_{i=1}^{N} (n_i \log n_i - n_i)$$
$$= -n \sum_{i=1}^{N} p_i \log p_i. \tag{3.1.2}$$

By dividing the logarithm of the number X_n of possibilities by n in order to relate it to the individual characters as an average value, we obtain the Shannon's entropy $H(X)$ which is defined as

$$H(X) = \lim_{n \mapsto \infty} \frac{1}{n} \log X_n$$
$$= -\sum_{i=1}^{N} p_i \log p_i. \tag{3.1.3}$$

By using the Stirling's formula, the number X_n of possible of typical sequences is found to be $X_n = 2^{nH(X)}$ [53, 75].

Properties of the Shannon entropy

If we assume a random source with an event space X, comprising of N elements or symbols with probabilities $p_i (i = 1, ..., N)$, the Shannon entropy, H should meet the following conditions [59]:

1. $H = H(p_1, p_2, ..., p_N)$ is a continuous function of the probability set p_i.
2. H is monotonously increasing with N in the case where all probabilities are equal i.e., $(p_i = 1/N)$.
3. H is additive. In the case of two independent variables X and Y, the characteristic additivity of the Shannon entropy that is, $H(X \times Y) = H(X) + H(Y)$ [76, 60].

3.1.2 Joint entropy

The joint entropy is a measure of information content, or the average uncertainty associated with each of the joint outputs of a pair of sources modeled by discrete random variables X and Y. The joint entropy can be expressed as [5, 59]

$$H(X, Y) = -\sum_{x,y} p(x, y) \log_2(p(x, y)). \tag{3.1.4}$$

If X and Y are independent

$$H(X, Y) = H(X) + H(Y), \tag{3.1.5}$$

which shows the additivity property of the joint entropy.

3.1.3 Relative Entropy/Kullback-Leibler distance

The relative entropy or the Kullback-Leibler distance between two probability distributions p and q of a discrete random variable is defined as [61]

$$D(p||q) = \sum_{x\in\mathcal{X}} p(x) \log \frac{p(x)}{q(x)}. \tag{3.1.6}$$

The relative entropy is always non-negative, ($D(p||q) \geq 0$) and is zero if and only if $p = q$ [53, 61]. It is the average of the logarithmic difference between p and q, where the average is taken by using the probabilities p. However, it is not a true distance because it is not symmetric between the probability distributions p and q i.e., $D(p||q) \neq D(q||p)$ and it also does not satisfy the triangle inequality.

In terms of the Kullback-Leibler distance in Equation (3.1.6), the relative entropy between two quantum systems with density operators ρ and σ can be written as [61]

$$S(\rho||\sigma) = \mathrm{tr}(\rho \log \rho) - \mathrm{tr}(\rho \log \sigma). \tag{3.1.7}$$

The key property of relative entropy, $S(\rho||\sigma) \geq 0$, is for the case where $\rho = \sigma$. This property is referred to as Klein's inequality [5, 77].

Properties of the relative entropy

The relative entropy has the following properties [52, 53]:

1. It is additive. For example, if X and Y are two independent random variables and let $p(x, y)$ and $r(x, y)$ be two possible joint probability mass functions of X and Y, then

   $$D(p(x, y)||r(x, y)) = D(p(x)||r(x)) + D(p(y)||r(y)). \tag{3.1.8}$$

   For the proof of additivity of the Rényi entropy, see Appendix B.1.

2. It is convex for the pair (p, r) provided that (p_1, r_1) and (p_2, r_2) are two pairs of probability mass functions

   $$D(\lambda p_1 + (1-\lambda)p_2)||\lambda r_1 + (1-\lambda)r_2) \leq \lambda D(p_1||r_1) + (1-\lambda)D(p_2||r_2), \tag{3.1.9}$$

3. $D(p||r) \geq 0$ and $D(p||r) = 0$, if and only if when $p = r$. This gives us a fundamental inequality in the theory of information measures known as the Gibbs inequality or divergence inequality [78]. This property follows from the Jensen's inequality [79].

4. The relative entropy is related to the Shannon entropy by

   $$D(p||r) = -H(p) - \sum_{i=1}^{N} p_i \ln r_i. \tag{3.1.10}$$

3.2 Quantum Information Measures

3.2.1 Conditional entropy

The conditional entropy represents the expected value of information content, or the average of uncertainty associated with the random variable Y given that X is known. The conditional entropy of two information measures modeled by discrete random variables X and Y is defined as [5, 52]

$$\begin{aligned} H(X|Y) &= -\sum_y p(y) \sum_x p(x|y) \log_2(p(x|y)) \\ &= -\sum_{x,y} p(x,y) \log_2 \frac{p(x,y)}{p(y)}. \end{aligned} \tag{3.2.1}$$

In the context of QKD, this can be interpreted as the amount of information that one additionally obtains when considering both Alice (X) and Bob's (Y) source, and not only Alice's source X.

3.2.2 Mutual Information

The mutual information gives a reduction in the uncertainty about a random variable X, due to the knowledge of the random variable Y. It is used to quantify the correlations between X and Y. The mutual information of two random variables X and Y, with a joint probability distribution function $p_{X,Y}(x,y)$, is defined as [5]

$$I(X;Y) = \sum_x \sum_y p_{XY}(x,y) \log \frac{p_{XY}(x,y)}{p_X(x) p_Y(y)}. \tag{3.2.2}$$

The symmetry, $I(X;Y) = I(Y;X)$ is a consequence of the definition of mutual information. The mutual information and the conditional entropy are related by taking $p_{XY}(x,y) = p_{X|Y}(x|y) p_Y(y)$, then

$$\begin{aligned} I(X;Y) &= -\sum_x \sum_y p_{XY}(x,y) \log p_X(x) + \sum_x \sum_y p_{XY}(x,y) \log p_{X|Y}(x|y) \\ &= H(X) - H(X|Y). \end{aligned} \tag{3.2.3}$$

In this equation $I(X;Y)$ is equal to the information that can be obtained about X by observing Y. In the case of $X = Y$, $H(X|Y) = 0$, therefore $I(X;Y) = H(X)$. If X and Y are independent then $H(X|Y) = H(X)$, therefore $I(X;Y) = 0$. This means that the two messages do not share any information.

3.2.3 Conditional mutual information

The conditional mutual information of random variables X, Y and Z is defined as [5]

$$I(X;Y|Z) = \sum_x \sum_y \sum_z p_{XYZ}(x,y|z) \log \frac{p_{XY|Z}(x,y|z)}{p_{X|Z}(x|z)p_{Y|Z}(y|z)}, \tag{3.2.4}$$

then it follows that

$$I(X;Y|Z) = H(X|Z) - H(X|Y,Z). \tag{3.2.5}$$

This gives the expected value of the mutual information of two random variables given the value of the third random variable.

3.2.4 von Neumann entropy

The von Neumann entropy $S(\rho_A)$, is used to describe the entropy of a quantum state ρ_A. It is a function of the density matrix expressed as [52]

$$S(\rho_A) = -\text{tr}(\rho_A \log \rho_A). \tag{3.2.6}$$

If λ_x are the eigenvalues of ρ_A, then the von Neumann entropy can be calculated as

$$S(\rho_A) = -\sum_x \lambda_x \log_2 \lambda_x. \tag{3.2.7}$$

If we consider a composite system ρ_{AB}, the von Neumann entropy is expressed as

$$S(A,B) = -\text{tr}_{AB}(\rho_{AB} \log_2 \rho_{AB}). \tag{3.2.8}$$

Suppose, we want to consider the correlations between a classical system X and a quantum system B which is described the classical-quantum state $\rho_{XB} = \sum_x p(x)|x\rangle\langle x|_x \otimes \rho_B^x$, the joint entropy of this state is calculated as

$$S(X,B) = S(\rho_{XB} = H(X) + \sum_x p(x) S(\rho_B^x). \tag{3.2.9}$$

The classical conditional entropy is expressed as

$$S(B|X) = \sum_x p(x) S(\rho_B^x). \tag{3.2.10}$$

Therefore, the mutual information between X and B is expressed as

$$I(X:B) = S(\rho_B) - \sum_x p(x) S(\rho_B^x), \tag{3.2.11}$$

where ρ_B^x is Bob's information state conditioned on x, and $\rho_B = \sum_x p(x)\rho_B^x$. This quantity is called the Holevo quantity, usually written as $\chi(X:B)$ [80]. The Holevo bound gives an upper bound on the amount of classical mutual information $I(X:B)$, that can be accessed from a quantum ensemble used in encoding the information. The mutual information gives a faction of error-free bits that can be extracted from the data which is distributed according to a probability, $p(x,y)$. This is a consequence of the Shannon's coding theorem.

3.2.5 Rényi entropies

The Rényi entropies are a family of functions relating to probability distributions [81]. They quantify the uncertainty or the randomness of a system. The Rényi's entropies generalize the Shannon entropies [82]. They are usually used in the secret-key distillation and for measuring entanglement [83, 84]. The Rényi entropy of order α with $0 < \alpha < \infty$ and $\alpha \neq 1$, of a discrete random variable X with possible outcomes $1, ..., n$, is defined as,

$$H_\alpha(X) = \frac{1}{1-\alpha} \log_2(\sum_{i=1}^{n} {p_i}^\alpha), \tag{3.2.12}$$

where $p_i = \Pr(X = i)$ for $i = 1, ..., n$. Three values of α are typically focused on and these are α=0, 1, ∞. In the case when $\alpha = 0$ the Rényi entropy corresponds to the logarithm of the support size of X. When $\alpha = 1$, the Rényi entropy corresponds to the regular Shannon entropy. When $\alpha = \infty$, it corresponds to the largest symbol probability which is expressed as

$$H_\infty(X) = -\log(\max_i(p_i)). \tag{3.2.13}$$

This entropy is also known as the min-entropy [85]. It has found some useful and interesting application in quantum key distribution. For example, it provides a lower bound in the security of QKD protocols by giving a guessing probability of the random variable X [38]. A special case occurs when $\alpha = 2$, which is in-fact the negative logarithm of the collision probability [83]. This is expressed as,

$$\begin{aligned} 2^{-H_2(X)} &= 2^{\log(\sum_{i=0}^{n-1} p_i^2)} \\ &= \sum_{i=0}^{n-1} p_i^2. \end{aligned} \tag{3.2.14}$$

This entropy shows the probability that two i.i.d random variables will take on the same value (i.e., collision probability). In Appendix B, we show that as $\alpha \mapsto 1$, the Rényi entropy approaches the Shannon entropy.

3.3 Distance measures

In this section, we would like to find a way of distinguishing two quantum states. In oder to do this, we need to consider distance measures and these are static and dynamic. Static measures quantify how close two quantum states are and dynamic measures quantify how well information has been preserved doing a dynamical process.

3.3.1 Trace distance (classical)

The trace distance allows us to compare two probability distributions $\{p_i\}$ and $\{q_i\}$ over the same index set. It is defined by [5]

$$D(p_i, q_i) \equiv \frac{1}{2}\sum_i |p_i - q_i|. \tag{3.3.1}$$

A distance measure must satisfy the properties of a metric:

1. It must be symmetric $D(x, y) = D(y, x)$.
2. It must satisy the triangle inequality $D(x, z) \leq D(x, y) + D(y, z)$.
3. $D(x, x) = 0$.
4. $D(x, y) = 0 \rightarrow x = y$.

3.3.2 Trace distance (quantum)

The trace distance between two quantum states ρ and σ is defined by [5]

$$D(\rho, \sigma) = \tfrac{1}{2}\mathrm{tr}|\rho - \sigma|, \tag{3.3.2}$$

where $|A| = \sqrt{A^\dagger A}$ is the positive square root of $A^\dagger A$. When ρ and σ commute, in which case they are diagonal in the same basis $\rho = \sum_i r_i|i\rangle\langle i|$ and $\sigma = \sum_i s_i|i\rangle\langle i|$, for some orthonormal basis $|i\rangle$, the quantum trace distance between ρ and σ becomes equal to the classical trace distance between the eigenvalues of ρ and σ.

$$\begin{aligned} D(\rho, \sigma) &= \tfrac{1}{2}\mathrm{tr}\left|\sum_i (r_i - s_i)|i\rangle\langle i|\right| \\ &= \tfrac{1}{2}\mathrm{tr}(\sum_i |r_i - s_i||i\rangle\langle i||) \\ &= \frac{1}{2}\sum_i |r_i - s_i| \\ &= D(r_i, s_i). \end{aligned} \tag{3.3.3}$$

3.3.3 Fidelity (quantum)

The fidelity of state ρ and σ is defined as [5]

$$F(\rho, \sigma) = \mathrm{tr}\sqrt{\rho^{1/2}\sigma\rho^{1/2}}. \tag{3.3.4}$$

In a special case when ρ and σ commute, i.e., are diagonal in the same basis, $\rho = \sum_i r_i|i\rangle\langle i|$ and $\sigma = \sum_i s_i|i\rangle\langle i|$, for some orthonormal basis $|i\rangle$ we have

$$\begin{aligned} F(\rho,\sigma) &= \mathrm{tr}\sqrt{\sum_i r_i s_i |i\rangle\langle i|} \\ &= \mathrm{tr}\sum_i \sqrt{r_i s_i}|i\rangle\langle i| \\ &= \sum_i \sqrt{r_i s_i} \\ &= F(r_i, s_i). \end{aligned} \tag{3.3.5}$$

If ρ and σ commute, the quantum fidelity $F(\rho,\sigma)$ reduces to the classical fidelity $F(r_i, s_i)$ between the eigenvalue distributions r_i and s_i of ρ and σ. The fidelity gives a practical measure of "closeness" between two quantum states. This is a consequence of Uhlmann's theorem [86]. This theorem states that for any state ρ and σ and any purification $|\psi\rangle$ of ρ, there exists a purification $|\phi\rangle$ of σ such that [5]

$$F(\rho,\sigma) = \max_{|\psi\rangle,|\phi\rangle} |\langle\psi|\phi\rangle|. \tag{3.3.6}$$

This equation shows that the fidelity between two mixed states can be interpreted as the maximum overlap between two purifications of these states. Based on the Uhlmann's theorem, the properties of the quantum fidelity can be stated as:

1. $0 \leq F(\rho,\sigma) \leq 1$. [1]
2. $F(\rho,\sigma)$=1 if and only if $\rho = \sigma$,
3. It is symmetric in its arguments, i.e., $F(\rho,\sigma) = F(\sigma,\rho)$.

[1] This is a consequence of the Cauchy-Schwarz inequality.

Chapter 4

Quantum Key Distribution and Security

4.1 Introduction

In this chapter, we briefly cover the background of QKD and also define the basic notion of security in QKD protocols. We recall that QKD is a technique that uses the power of quantum mechanics in order to establish a string of random bits called a key. This key is shared between Alice and Bob. Since the key is random and unknown to an eavesdropper, Eve, she is unable to learn anything about the message simply by intercepting the ciphertext. This phenomenon is beyond the ability of classical information processing. Therefore, we investigate how quantum mechanics plays a role in QKD and also in the security of QKD protocols. We will also study some of the tools which are used in the derivation of security proofs for the infinite and finite-length key limit. The security study is mainly based on the framework introduced by Devetak-Winter, Csiszár-Körner and Renner security [38, 87]. For a detailed overview of QKD, we refer the reader to [14, 23].

4.2 Quantum features

4.2.1 Detection of Measurements

Based on the measurement postulate of Quantum mechanics [88], it is impossible to perform a measurement on an unknown quantum state without introducing a disturbance unless the state is an eigenstate to the observable being measured [58]. This means that Eve is unable to perform a measurement on an unknown quantum state without introducing a disturbance that can be discovered by Alice and Bob.

4.2.2 Uncertainty principle

The uncertainty principle states that a measurement of one quantum observable intrinsically creates an uncertainty in other properties of the system. This means that it is impossible to measure the simultaneous values of non-commuting observables on a single copy of a quantum state [89]. This ensures that an eavesdropper cannot perform measurements that leave the quantum state undisturbed [90]. This automatic detection of an eavesdropper is impossible with classical cryptography.

4.2.3 No-Cloning Theorem

In Quantum mechanics, it is impossible to make a perfect copy of an unknown state with perfect fidelity. This is called the no-cloning theorem [91]. This prevents an eavesdropper from simply intercepting the communication channel and making copies (so as to make measurements on them later) of the transmitted quantum states, while passing on an undisturbed quantum state to Bob [92, 93]. Therefore, the no-cloning theorem forms an important property in the security of QKD protocols [94].

4.2.4 Non-orthogonality principle

Suppose, we have quantum states $|\psi_i\rangle$ which are not orthogonal, then it can be proved that there exists no quantum measurement that is able to distinguish states [88]. In this case, a non-zero component of the state $|\psi_1\rangle$ parallel to the state $|\psi_2\rangle$ always gives a non-zero probability of the measurement outcome associated with the state $|\psi_2\rangle$ also occurring when the measurement is applied to the state $|\psi_1\rangle$. This is because $|\psi_2\rangle$ can be decomposed into a non-zero component parallel to $|\psi_1\rangle$ and a component orthogonal to $|\psi_1\rangle$. Then, there is no measurement of any kind that can reliably determine which of the two non-orthogonal quantum states was measured [16]. This feature is very useful for cryptographic applications such as QKD [58].

4.3 QKD schemes

There are two major types of QKD schemes, namely, Prepare and Measure (P&M) and Entanglement-Based (EB) schemes [14, 23]. A P&M scheme is based on individual qubits while an EB scheme is based on entangled qubits. Either of these schemes can be used by two parties in order to end up with a shared secret key. However, a P&M scheme can immediately be translated into an EB scheme [23, 95]. Below, we will briefly describe the processes for each scheme.

4.3.1 Prepare and Measure (P&M) scheme

In a P&M scheme, Alice encodes some classical information into a set of quantum states and sends them via an insecure quantum channel to Bob. Bob then performs measurements on the quantum states he receives. This results in classical data generated by quantum means being shared between Alice and Bob. Examples of protocols that use this scheme are BB84 [96], B92 [16], six-state [19] and SARG04 [20] protocols.

4.3.2 Entanglement-Based (EB) scheme

In an EB scheme, a source prepares and distributes a maximally entangled quantum state where one system is sent to Alice and another to Bob. Alice and Bob then perform measurements in two mutually unbiased bases on their system respectively. Upon measurement they obtain perfectly correlated outcomes which are completely random. Since the source prepares a pure state, it means that this state cannot be correlated with an eavesdropper. This implies secrecy of the key. An example of a protocol which uses this scheme is the E91 protocol [13].

4.4 QKD procedure

In this section, we describe what happens in a P&M scheme, specifically in the BB84 protocol [96]. In this protocol, Alice and Bob are connected by two communication channels, namely an insecure quantum channel and an authenticated classical channel [14]. The quantum channel is used for the transmission of qubits and is controlled by the eavesdropper. The classical channel is authenticated so that the eavesdropper can only listen to the communication but cannot alter the messages being transmitted. This ensures that Alice and Bob can prove that they are communicating between each other. Otherwise, an eavesdropper could simply block all quantum and classical communication between Alice and Bob and perform QKD with Alice while taking on Bob's role and vice versa. Therefore, Alice and Bob have to identify each message they send as originating from themselves before any post-processing can begin.

4.4.1 Quantum Phase

In the quantum phase, Alice and Bob make use of the quantum channel. They employ the quantum mechanical signals (i.e., qubits) and they also perform measurements. Three subprotocols take place which are:

1. Signal preparation - Alice prepares a random sequence of strings which are drawn from a set of four signal states and encodes each bit value in the state of a quantum system. The basis states are horizontal, vertical, diagonal and anti-diagonal.

2. Transmission - The encoded quantum system is sent to Bob via the quantum channel.

3. Measurement - Bob applies a quantum measurement on the quantum system to decode a bit value. The signals are measured in a random sequence of polarization bases, either in the horizontal/vertical or diagonal/anti-diagonal bases.

Afterwards, Alice keeps the record of signal choices, Bob keeps the record of his basis choices and the corresponding measurement result.

4.4.2 Classical phase

In this phase, Alice and Bob use some classical communication protocol in order to distill a secret key from their correlated data. They achieve this by means of a discussion over the authenticated classical channel. The key extraction procedure is described as follows:

1. Parameter estimation - Alice randomly chooses some fraction of her signal slots and announces for these slots to Bob which signal she sent. Bob announces the measurement he performed and the outcome which he obtains. Depending on the amount of errors which they obtain from their comparisons, they may also decide whether to continue or abort the protocol.

2. Sifting - In the sifting protocol, Alice and Bob announce the polarization bases they used for the preparation of the signals and which bits are discarded. In order to prevent Eve from modifying the transmitted messages, Alice and Bob use the authentication scheme. The remaining data is called sifted data. Alice and Bob proceed to the reconciliation phase or error correction phase.

3. Key map - Alice and Bob discard the basis which they were using so that Eve may not learn any information about the encoding. During key map, Alice and Bob map their event records of the sifted data into a raw key. This step applies to Prepare and Measure protocols.

4. Error correction - The sifted data may still contain some errors, therefore, Alice and Bob execute a classical error correction protocol in order to reconcile their data. They need to exchange additional information about their respective data over the public channel. In addition, they need to authenticate this phase because Eve is still able to modify the messages in this step. As a result of this protocol, Alice and Bob agree now on a key which is identical with very high probability but Eve might still have some small additional information about they key. After this stage, privacy amplification takes place.

5. Privacy amplification - After Alice and Bob have reconciled their key, they can cut the correlations between their key and Eve by using so-called privacy amplification. In this stage, Alice and Bob map their string via a special family of functions called universal hash functions to a shorter final key [38].

4.5 Security in QKD

4.5.1 Security definition

A good definition of security would allow the key generated by a QKD protocol to deviate by a small parameter ε, from a perfect key [14]. This definition should be able to bound Eve's knowledge about the final key. A perfect key refers to a uniformly distributed bit string whose value is completely independent and remains unknown to an eavesdropper [12]. The main requirement that the definition of security must fulfill is composability [38]. The composable definition characterizes the security of a protocol with respect to the ideal functionality. This means that the security of the key generated could be used in any subsequent cryptographic task such as the one-time pad for message encryption, where an ideal key is expected. However, there always exist some challenges in constructing security proofs without making any assumptions either about the devices or the parties. For example, attacks against practical schemes exists, photon-number-splitting attacks (PNS) [97], time-shift attacks [98], and large pulse attacks [99, 48], blinding attacks [100] and high-power damage attack [101]. Some of the assumptions made in the definition of QKD security are [102]:

1. there should be no side-channels. Side channels are basically discrepancies between the theoretical model and a practical implementation. They always exists if some information about the raw key is encoded in degrees of freedom not considered in the theoretical model. Therefore, this leads to a wrong assessment of the dimension of the Hilbert space which describes the protocol,
2. there should be access to perfect or almost perfect randomness (locally),
3. quantum theory is correct and complete.

If there is randomness and quantum theory is correct then this leads to completion of the security proofs. However, in classical cryptography the security is based on the difficulty or complication of a certain mathematical algorithm to afford security of the protocol. Therefore, the security is mainly based on the failure to solve the algorithm. This can fail in four ways:

1. conjecture of hardness/difficulty in this case is wrong,
2. underlying computation model could be wrong or could be unphysical,
3. the algorithm is easy for many instances,
4. the computation could be small.

4.5.2 Security requirements

In this section, we shall follow closely the definitions in [38, 103]. A QKD protocol outputs a key S_A on Alice's side and also a key S_B on Bob's side. The length of the key

is $\ell > 0$, otherwise no key is extracted. The length of the key depends on the noise level of the communication channel as well as security and on the correctness requirements of the protocol. Depending on the deviation of the output key from the ideal one, the protocol aborts in which case $S_A = S_B = \perp$ [103].

1. Correctness

A QKD protocol is called "correct", if, for any strategy by the eavesdropper $S_A = S_B$. This occurs whenever Alice and Bob output the classical keys S_A and S_B, respectively, such that $\Pr[S_A \neq S_B] \leq \varepsilon_{\text{cor}}$. The term ε_{cor}, is the maximum probability that the protocol deviates from the behavior of the correct protocol. In order for correctness to be achieved, the QKD devices must perform what they are supposed to do as according to a specified model. The devices generate the correct correlations which they are supposed to output, otherwise the protocol aborts. In other terms, the devices should not send any other information to the outside world, in which it is not supposed to do (i.e., devices work according to their specification),

2. Secrecy

A random variable S drawn from the set $\mathcal{S}$ is said to be ε-secure with respect to an eavesdropper holding a quantum system E if

$$\min_{\in \sigma_E} \frac{1}{2} \text{tr} |\rho_{SE} - \rho_U \otimes \sigma_E| \leq \varepsilon, \tag{4.5.1}$$

where $\rho_{SE} = \sum_{s \in S} P_s(s) |s\rangle\langle s| \otimes \rho_{E|S=s}$ is the actual state that contains some correlations between the final key and Eve and ε gives the maximum failure probability of the key extraction process. The state $\rho_U = \sum_{s \in S} |s\rangle\langle s| |\mathcal{S}|$ is the completely mixed state on $\mathcal{S}$ and $|\mathcal{S}|$ is the size of S. Since the trace distance i.e., $\frac{1}{2}\text{tr}|\rho_0 - \rho_1|$ refers to the maximum probability of distinguishing between two quantum states (ρ_0, ρ_1), this composable security definition naturally gives rise to the operational meaning that the protocol is ε-secure, i.e., S is identical to an ideal key U except with probability ε [38]. Again, according to the Helstrom's Theorem, the probability of distinguishing between the two quantum states ρ_0 and ρ_1, is bounded by $\frac{1}{2} + \frac{1}{4}\text{tr}|\rho_0 - \rho_1|$ [104].

3. Robustness

A QKD protocol is said to be "not robust" if the protocol aborts even though the eavesdropper is inactive. While correctness and secrecy is difficult to prove, robustness can simply be proven by running the protocol.

4.5.3 Infinite-length key security in QKD

Over the last decade, a lot of work in QKD has been devoted to the derivation of unconditional security proofs [9, 10, 12, 105, 41, 106]. One of the main problems is that Eve has the power to perform any type of eavesdropping strategy. In particular, she can evade detection by attributing noise caused by her eavesdropping attack to normal noise in the channel. Therefore, it remains difficult to accurately bound the amount of information that Eve may obtain from the communication channel. The most important resource which should be determined when constructing security proofs for QKD protocols is the secret key rate. Therefore, all QKD protocols must be able to provide a clear expression for the secret key rate, r. In the asymptotic limit, the secret key rate is expressed as

$$r = \lim_{n\to\infty} \frac{\ell}{n}, \tag{4.5.2}$$

where ℓ is the length of the final secret key and n is a list of symbols called raw keys [14]. This rate was established by Devetak and Winter [87]. The secret key rate against collective attacks was derived by Kraus, Gisin and Renner [107] and is expressed as

$$r = I(X:Y) - \chi(X:E) \tag{4.5.3}$$

where $I(X:Y) = H(X) - (X|Y)$ quantifies the amount of bits need to be satisfied for error correction. The term $\chi(X:E) = H(X) + S(E) - S(X,E)$ refers to the Holevo quantity, where H is the Shannon entropy and S is the von Neumann entropy [108, 109]. The Holevo quantity refers to the amount of privacy amplification required in order to eliminate Eve's information.

The upper bound on the secret key rate r, can be expressed as

$$r \leq I(A:B \downarrow E), \tag{4.5.4}$$

where $I(A:B \downarrow E)$ is the intrinsic conditional mutual information (intrinsic information for short) between two information sources held by Alice and Bob after Eve has performed an optimal individual attack [110]. The intrinsic information between two information sources A and B given $\bar{E}$ is defined as, $I(A:B \downarrow E) = \inf_{\bar{E}} I(A:B|\bar{E})$, where the infimum is taken over all discrete random variables E such that $AB \to E \to \bar{E}$ is a Markov chain [111]. It has been shown that $I(A:B \downarrow E)$ is an upper bound on the rate $S = S(A;B||E)$ at which such a key can be extracted [110].

4.5.4 Finite-length key security

Many efforts have been made to improve the bounds on the secret key rates for a finite amount of resources [38, 112, 12, 113, 114, 84]. Since the tools for analysing the security under non-asymptotic regime have become available there is need to provide new security definitions. In this section, we follow closely the techniques demonstrated in [12] to discuss some of the parameters used in the security of QKD for finite-length key limit. The main goal of finite-length key security is to obtain a secret key rate r, based on a certain number of signals, a security parameter ε, and certain losses from the error

correction without making any assumptions about the post processing (sifting, error correction and privacy amplification). For example, one can recognize that the limit in this expression of Equation (4.5.2) is unrealistic because in all implementations of QKD protocols finite resources are used. This is because in this scenario, N is assumed to be large i.e., it approaches infinity, while in practice Alice and Bob exchange a limited number of symbols or signals. In the non-asymptotic limit, the secret key rate can be expressed as

$$r = \frac{n}{N}[S_\xi(X|E) - \triangle - \text{leak}_{\text{EC}}/n]. \tag{4.5.5}$$

This shows that only a fraction of n out of N signals exchanged contributes to the key. This is because of the fact that $m = N - n$ are used for parameter estimation thus leading the presence of a pre-factor of n/N. The expression $S_\xi X(X|E)$ takes into account the finite precision of the parameter estimation. Eve's information is calculated by using measured parameters, for example error rates. In the finite-key scenario, these parameters are estimated on samples of finite length. The parameter $\triangle$ is related to the security of privacy amplification. Its value is given by

$$\triangle \equiv (2\log_2 d + 3)\sqrt{\frac{\log_2(2/\bar{\varepsilon})}{n}} + \frac{2}{n}\log_2\frac{1}{\varepsilon_{\text{PA}}}, \tag{4.5.6}$$

where d is the dimension of the Hilbert space, $\bar{\varepsilon}$ is a smoothing parameter, and ε_{PA} is the failure probability of the privacy amplification procedure. Eve's uncertainty is quantified by a generalized conditional entropy called the smooth min-entropy and is denoted as $H_{\text{min}}^{\bar{\varepsilon}}(X^{(n)}|E^{(N)})$ [38]. The smoothing parameter, $\bar{\varepsilon}$ and ε_{PA} are parameters which should be optimized numerically. The square-root term corresponds to the speed of convergence of the smooth-min entropy which is used to measure the key length of an identical and independently distributed (i.i.d) state toward the von Neumann entropy. In the asymptotic limit, the smooth-min entropy of an i.i.d state is equal to the von Neumann entropy. The second term ε_{PA}, is directly linked to the failure probability of the privacy amplification procedure. Finally, $\text{leak}_{\text{EC}}/n$ corresponds to the amount of information which needs to be exchanged by Alice and Bob during the reconciliation phase. This quantity may not reach the Shannon limit, so $\text{leak}_{\text{EC}} \geq nH(X|Y)$. Typically,

$$\text{leak}_{\text{EC}} \approx f_{\text{EC}}H(X|Y) + \frac{1}{n}\log_2(2/\varepsilon_{\text{EC}}), \tag{4.5.7}$$

where $f_{\text{EC}} > 1$ depends on the code and ε_{EC} refers to the failure probability of the error correction procedure.

Unlike in the asymptotic scenario, one needs to fix an overall security parameter ε, for the QKD protocol. The parameter ε, corresponds to the maximum probability failure that is tolerated on the key extraction protocol. This can be expressed as $\varepsilon = \varepsilon_{\text{PE}} + \varepsilon_{\text{EC}} + \bar{\varepsilon} + \varepsilon_{\text{PA}}$, where ε_{PE} is the error in the parameter estimation step and the other terms are as previously defined. All the parameters $\varepsilon_{\text{PE}}, \varepsilon_{\text{EC}}, \bar{\varepsilon}, \varepsilon_{\text{PA}}$ can independently be fixed at arbitrarily low values.

As a result the overall security parameter ε can be chosen arbitrarily small, to a value corresponding to Alice and Bob's wishes, but this comes at a cost of decreasing the final secret key rate. If m signals have been used to estimate the parameter λ, then the

deviation of measurement outcomes λ_m obtained from measuring the m samples from the ideal estimate λ_∞ can be quantified by using the law of large numbers resulting [38, 53].

$$|\lambda_m - \lambda_\infty| \leq \xi(m, d) = \sqrt{\frac{\ln(1/\varepsilon_{\mathrm{PE}}) + d\ln(m+1)}{2m}}. \tag{4.5.8}$$

The objective of the privacy amplification step is to minimize the quantity of correct information which the eavesdropper may have obtained about Alice and Bob's reference raw key. After privacy amplification, the length of the raw key that remains will be

$$\ell \leq H_{\min}^{\varepsilon}(X|E) - 2\log_2(1/\varepsilon_{\mathrm{PA}}), \tag{4.5.9}$$

where $H_{\min}^{\varepsilon}(X|E)$, expresses Eve's uncertainty and $\varepsilon_{\mathrm{PA}} = 2^{-\frac{1}{2}[H_{\min}^{\varepsilon}(X|E)-\ell]}$, is the error in the privacy amplification step.

Chapter 5

Tsallis entropy and uncertainty measurements in QKD security

5.1 Introduction

In this chapter we study the Tsallis entropy. The Tsallis entropy defines an important generalisation of the usual concept of entropy which depends on a parameter α. The Tsallis entropy forms a generalisation of the standard Boltzmann-Gibbs entropy [115]. Our goal is to establish a connection between the quantum uncertainty principle and the Tsallis entropy for single discrete observables. We show that there exist a generalised uncertainty bound reached in order to appropriately express the quantum uncertainty principle in terms of the Tsallis entropy. Later, we show a possible immediate application of the Tsallis entropy on how they can be useful in quantifying information in QKD. This kind of connection forms an initial important step towards finding an important application of this α-entropy in the area of quantum communication for which entropies like Shannon entropy and Rényi entropy have been used. This chapter is based on manuscript **M9**.

Depending on the application, a number of entropic forms [116] and uncertainty relations [7, 117, 118] have been derived. Many generalisations or versions of the Shannon entropy have already been found and one of these is the Tsallis entropy [115]. The Tsallis entropy was introduced by Havrda and Charvát in 1967 [119] and later studied by Darcózy in 1970 [78]. It was in 1988 when Tsallis [115] exploited its features and placed a physical meaning on this entropy as a basis for generalising the standard statistical mechanics. Therefore, this entropy is now known as the Tsallis entropy. It has also been established that the Tsallis and Shannon entropies can be connected by means of some transformation [120]. Therefore, this connection between these two entropies shows a possibility of interchangeability between these two entropies, however only up to some bound. Similar to the Shannon entropy, the Tsallis entropy has also found many interdisciplinary applications [120].

5.2 Tsallis entropy

For a probability distribution p_i, on a finite set, the Tsallis entropy, $S_\alpha(p_i)$ of order α is defined as [115]

$$S_\alpha(p_i) = \frac{1}{1-\alpha}\left(\sum_i p_i^\alpha - 1\right), \tag{5.2.1}$$

where $0 < \alpha < \infty$. At $\alpha = 1$, $S_\alpha(p_i)$ does not exist, therefore we use the L'Hospital's rule to show that the Tsallis entropy approaches the Shannon entropy as $\alpha \mapsto 1$, i.e., $\lim_{\alpha\mapsto 1} S_\alpha(p_i) = -\sum_i p_i \ln p_i$ which is the Shannon entropy [121]. The proof is shown in Appendix E. There is also a close relationship between the Rényi entropy and the Tsallis entropy which is expressed as

$$\begin{aligned} H_\alpha(p_i) &= \frac{1}{1-\alpha}\ln[1+(1-\alpha)S_\alpha(p_i)] \\ &= \xi[S_\alpha(p_i)], \end{aligned} \tag{5.2.2}$$

where $\xi(u) = 1/1-\alpha\ln[1+(1-\alpha)u]$ and $H_\alpha(p_i)$ is the Rényi entropy. The function $\xi(u)$ is well defined when $1+(1-\alpha)u > 0$ and if its strictly increasing because

$$\xi'(u) = \frac{1}{1+(1-\alpha)u} > 0. \tag{5.2.3}$$

When the entropy is maximized in a variational principle [122], it cannot make any difference whether the Tsallis entropy functional is used or Rényi's entropy. This is because when one of the two reaches its maximum then the other will also be at its maximal.

Similar to the Shannon entropy, the Tsallis entropy reaches its maximum for uniform distribution. We can demonstrate this by maximizing it under some normalization constraint $\sum_{i=1}^n p_n = 1$, and by introducing a Lagrange multiplier λ as follows

$$\begin{aligned} 0 &= \frac{\partial}{\partial p_i}\left[\frac{\sum_{i=1}^n p_i^\alpha - 1}{1-\alpha} - \lambda\left(\sum_{i=1}^n p_i - 1\right)\right] \\ &= -\frac{\alpha}{1-\alpha}p_i^{1-\alpha} - \lambda. \end{aligned} \tag{5.2.4}$$

We can recognize it follows that

$$p_i = \left[\frac{\lambda(1-\alpha)}{\alpha}\right]^{\frac{1}{1-\alpha}}. \tag{5.2.5}$$

Since this is independent of i, so by imposing the normalising constraint immediately yields $p_i = 1/n$.

Again, just like the Shannon and Rényi entropy, one can investigate the concavity ($\alpha > 0$) and convexity ($\alpha < 0$) of the Tsallis entropy by finding its Hessian matrix as

$$\frac{\partial^2}{\partial p_i p_j}\left[S_\alpha(p) - \lambda\left(\sum_{k=1}^n p_k - 1\right)\right] = -\alpha p_i^{\alpha-2}\delta_{ij}, \tag{5.2.6}$$

which is positive definite for $\alpha < 0$ and negative definite for $\alpha > 0$. Similar to the concavity ($0 < \alpha < 1$) property of the Rényi entropy, for two probability mass functions p and r, the Tsallis entropy concavity property can be written as

$$S_\alpha(\lambda p + (1 - \lambda r)) \leq \lambda S_\alpha(p) + (1 - \lambda) S_\alpha(r), \tag{5.2.7}$$

for $\lambda \in [0,1]$. This follows from the Jensen's inequality and concavity of $(x^\alpha/(1-\alpha))$ [79].

5.3 On the uncertainty relation

The uncertainty relation forms the most characteristic and fundamental result of Quantum mechanics. The uncertainty relations have attracted a lot of attention for extensive research since Heisenberg's famous paper was published [6, 123]. An established and well known approach is by Robertson [123]. The first uncertainty relation to be derived was by Hirschman [124]. This uncertainty relation was a position-momentum relation which is based on the Shannon entropy. In particular, Robertson showed that a product of two standard deviations of two discrete observables A and B measured in the quantum state $|\psi\rangle$ is bounded from below [123]. This is expressed as

$$\triangle A \cdot \triangle B \geq \frac{1}{2} |\langle \psi | [A, B] | \psi \rangle|, \tag{5.3.1}$$

where $\triangle A$ and $\triangle B$ represent the standard deviation of the outcomes of the corresponding observables. However, this Robertson's uncertainty formulation comes with some lacks. For example, it is impossible to use it in order to characterize randomness of measurement outcomes by using the standard deviations. Furthermore, it cannot deal with the most general types of measurements, i.e., POVMs. Again, it has also been observed that this Robertson's bound does not express all the features expected from an uncertainty relation if the observables A and B are finite [125]. Following these shortcomings, Deutsch [89] proposed an uncertainty relation which was based on the Shannon entropy. We recall that the Shannon entropy can be expressed as

$$H(p) = -\sum_i p_i \ln p_i, \tag{5.3.2}$$

where $\sum_i p_i = 1$ and $p_i \geq 0$. For a general probability distribution $p = (p_1, ..., p_N)$ and $q = (q_1, ..., q_N)$ on a set of N possible outcomes. The uncertainty relation proposed was of the form

$$H(p) + H(q) \geq -2 \ln \frac{1}{2}(1 + c), \tag{5.3.3}$$

where $c = \max_{i,j} |\langle a_i | b_j \rangle|$, defines the incompatibility of the two measurements. Kraus conjectured that this relation can be improved to [126]

$$H(p) + H(q) \geq -2 \ln c. \tag{5.3.4}$$

An advantage of this relation is that they are independent of the state vector ψ unlike in the Robertson's relation. These proposed uncertainty were later improved by Maassen and Uffink [127] and they can be restated as

$$H(A|\rho) + H(B|\rho) \geq -2 \log \max ||A_a^{\frac{1}{2}} B_b^{\frac{1}{2}}||_1, \tag{5.3.5}$$

where $A = \{A_a\}$ and $B = \{B_b\}$ are POVM's and $H(A|\rho)$ and $H(B|\rho)$ are the Shannon entropy of the probability of the measurement outcome A and B in a state ρ respectively.

Recently, the entropic uncertainty relations have found several applications especially in quantum information [128, 129]. Such applications are based on the properties of the Shannon entropy. However, the Tsallis entropy has not been utilized in such applications. This might be due to a major difference which exists between the Shannon and the Tsallis entropy, i.e., the Shannon entropy and Rényi entropies are additive for independent probability distributions while the Tsallis entropy is non-additive or is pseudo-additive [130]. This pseudo-additivity property in general is defined as

$$S_\alpha(p_i, p_j) = S_\alpha(p_i) + S_\alpha(p_j) + (1-\alpha)S_\alpha(p_i)S_\alpha(p_j), \tag{5.3.6}$$

where p_i and p_j are probability distributions for independent random variables A and B respectively. Similarly, if a system is composed of two subsystems which are independent of each other say A and B with the probability distribution p_i and p_j respectively, then the Rényi entropy $H_\alpha(p)$ is equal to the sum of $H_\alpha(p_i)$ and $H_\alpha(p_j)$ i.e.,

$$H_\alpha(p_i \times p_j) = H_\alpha(p_i) + H_\alpha(p_j). \tag{5.3.7}$$

Therefore, this non-additivity property proves to be a challenge in trying to immediately connect the Tsallis entropy to these applications in quantum information.

5.4 Tsallis entropy and Uncertainty Relations

In order to arrive at our goal, we start by summarizing the result of Ref [89]. Of importance, Deutsch established that the generalized Heisenberg inequality does not properly express the quantum uncertainty principle except in the canonically conjugate observables. In general, he found that in order to properly quantify the quantum uncertainty principle, there exists an irreducible lower bound in the result of uncertainty of a measurement. This can be written quantitatively as

$$\mathcal{U}(\hat{A}, \hat{B}; \psi) \geq \mathcal{B}(\hat{A}, \hat{B}), \tag{5.4.1}$$

where $\mathcal{U}$ is the uncertainty in the measurement of $\hat{A}$ and $\hat{B}$ which are simultaneously prepared observables, $|\psi\rangle$ is the outcome state and $\mathcal{B}$ is the irreducible lower bound as according to Ref [89]. The function $\mathcal{U}(\hat{A}, \hat{B})$ depends only on the state $|\psi\rangle$ and the sets $\{|a\rangle\}$ and $\{|b\rangle\}$ while $\mathcal{B}(\hat{A}, \hat{B})$ depends on the set $\{\langle a|b\rangle\}$ of inner products between the eigenstates of A and B respectively.

Based on Ref [89], the most natural measure of uncertainty is the result of a measurement or preparation of a single discrete observable which can be expressed in the entropic form as

$$S_{\hat{A}}(|\psi\rangle) = -\sum_a |\langle a|\psi\rangle|^2 \ln |\langle a|\psi\rangle|^2. \tag{5.4.2}$$

We can recognize that the right hand side of Equation (5.4.2) is expressed in terms of the Shannon's entropy where, $p_i = |\langle a_i|\psi\rangle|^2$ is the probability. It has been shown in Ref

[126] that

$$\mathcal{U}(\hat{A},\hat{B};\psi) \geq 2\ln\frac{1}{1+c}. \tag{5.4.3}$$

As stated previously, this bound was later improved by Maassen and Uffink [127] for which they obtained

$$\mathcal{U}(\hat{A},\hat{B};\psi) \geq 2\ln\frac{1}{c}, \tag{5.4.4}$$

by considering measurements from two mutually unbiased bases. Therefore, we aim to investigate whether the non-extensivity property of the Tsallis entropy will ever make a difference on the requirements of $\mathcal{B}$ instead of using the Shannon entropy. Surprisingly, we reach a bound which can be expressed in a similar manner as in Ref [89].

In our scenario, we again consider two observables $\hat{A}$ and $\hat{B}$ which are simultaneously measured and a state $|\psi\rangle$ which represents the outcome of a measurement. In order to find the bound on $\mathcal{B}(\hat{A},\hat{B})$, we relate this function to the additivity of Tsallis entropy instead of using additivity of Shannon entropy and without loss of generality we write Equation (5.3.6) as

$$\mathcal{B}(\hat{A},\hat{B};\psi) = S_\alpha(\hat{A};\psi) + S_\alpha(\hat{B};\psi) + (1-\alpha)S_\alpha(\hat{A};\psi)S_\alpha(\hat{B};\psi). \tag{5.4.5}$$

Now, we can calculate the bound $\mathcal{B}$ by using the Tsallis entropy as an information measure by proceeding as follows

$$\begin{aligned}
\mathcal{B}(\hat{A},\hat{B};\psi) &= -\frac{1}{1-\alpha}\left[\sum_a |\langle\psi|a\rangle|^{2\alpha}\ln|\langle\psi|a\rangle|^{2\alpha} - \sum_b |\langle\psi|b\rangle|^{2\alpha}\ln|\langle\psi|b\rangle|^{2\alpha}\right] \\
&+ (1-\alpha)\sum_a |\langle\psi|a\rangle|^2\ln|\langle\psi|a\rangle|^2 \sum_b |\langle\psi|b\rangle|^2\ln|\langle\psi|b\rangle|^2 \\
&= -\sum_{ab}|\langle\psi|a\rangle|^2|\langle\psi|b\rangle|^2[\ln|\langle\psi|a\rangle|^2 + \ln|\langle\psi|b\rangle|^2) \\
&- (1-\alpha)\ln|\langle\psi|a\rangle|^2\ln|\langle\psi|b\rangle|^2].
\end{aligned} \tag{5.4.6}$$

We can maximize Equation (5.4.6), by performing the following operations:

$$\begin{aligned}
\mathcal{B}(\hat{A},\hat{B};\psi) &= \max_{|\psi\rangle}|\langle\psi|a\rangle\langle b|\psi\rangle| \\
&\leq |\langle\psi|\left(\frac{|a\rangle\langle a| + |b\rangle\langle b|}{2}\right)|\psi\rangle|.
\end{aligned} \tag{5.4.7}$$

In order to calculate the maximum eigenvalue of the expression in Equation (5.4.7), we apply the following substitution

$$|a\rangle = \begin{pmatrix}1\\0\end{pmatrix}, \quad |b\rangle = \begin{pmatrix}\cos\theta e^{-i\alpha}\\ \sin\theta\end{pmatrix}$$

and arrive at an expression of the form

$$\begin{aligned}\left(\frac{|a\rangle\langle a| + |b\rangle\langle b|}{2}\right) &= \frac{1}{2}\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} + \frac{1}{2}\begin{pmatrix}\cos^2\theta & \cos\theta\sin\theta e^{-\alpha}\\ \sin\theta\cos\theta e^{-i\alpha} & \cos^2\theta\end{pmatrix}\\ &= \frac{\mathbb{1}}{2} + \frac{\sin\theta\cos\alpha}{2}X - \frac{\sin\theta\cos\theta\sin\alpha}{2}Y + \frac{\cos^2\theta}{2}Z, \quad (5.4.8)\end{aligned}$$

where X, Y and Z are the Pauli matrices.

Theorem: If we consider $M = a\mathbb{1} + bX + cY + dZ$ where $a, b, c, d \in \mathbb{R}^+$ where $m = a \pm \sqrt{b^2 + c^2 + d^2}$ are the eigenvalues of M.

Based on Equation (5.4.6) find that $a = \frac{1}{2}$, $b^2 = \frac{\sin^2\theta\cos^2\theta\cos^2\alpha}{4}$, $c^2 = \frac{\sin^2\theta\cos^2\theta\sin^2\alpha}{4}$ and $d^2 = \frac{\cos^4\theta}{4}$. By substitution and some few algebraic steps we arrive at the value of

$$m = \frac{1}{2} \pm \frac{\cos\theta}{2}. \quad (5.4.9)$$

The maximum eigenvalue of M i.e., $m_{\max} = (1 + \cos\theta)/2$ corresponds to $|\psi\rangle$ and occurs midway between $|a\rangle$ and $|b\rangle$. Therefore, we can express this as a function

$$\begin{aligned}f(a,b) = \mathcal{B}(\hat{A},\hat{B}) &= -2\ln\left[\frac{1 + \langle a|b\rangle}{2}\right]\\ &= 2\ln\frac{2}{1 + \langle a|b\rangle}. \quad (5.4.10)\end{aligned}$$

Using the fact that $\sum_a |\langle\psi|a\rangle|^2 = 1$ and $\sum_b |\langle\psi|b\rangle|^2 = 1$, we can express

$$\begin{aligned}\sum_{a,b} |\langle\psi|a\rangle|^2 \cdot |\langle\psi|b\rangle|^2 \cdot f(a,b) &\geq \min_{a,b} f(a,b)\\ &\geq 2\ln\frac{2}{1 + \langle a|b\rangle}. \quad (5.4.11)\end{aligned}$$

Considering that

$$\min\left[\frac{\ln 2}{1 + \langle a|b\rangle}\right] = \frac{\ln 2}{1 + \max|\langle a|b\rangle|}, \quad (5.4.12)$$

we can put everything together as

$$\begin{aligned}\mathcal{B}(\hat{A},\hat{B}) &= S_\alpha(\hat{A};\psi) + S_\alpha(\hat{B};\psi) + (1-\alpha)S_\alpha(\hat{A};\psi)S_\alpha(\hat{B};\psi)\\ &\geq \frac{1}{1-\alpha}\left[1 - \left(\frac{2}{1 + \max|\langle a|b\rangle|}\right)^{2(\alpha-1)}\right]. \quad (5.4.13)\end{aligned}$$

If we take $c = \max_{ij}|\langle a_i|b_j\rangle|$, where $|a_i\rangle$ and $|b_j\rangle$ are the eigenvectors of A and B respectively, we obtain the bound

$$\mathcal{B}(\hat{A},\hat{B}) \geq \frac{1}{1-\alpha}\left[1 - \left(\frac{2}{1+c}\right)^{2(\alpha-1)}\right]. \quad (5.4.14)$$

With the help of the Riesz's theorem [127, 131] in the region of $1/2 \leq \alpha \leq 1$, a better hence tighter bound is obtained which can be expressed as

$$\mathcal{B}(\hat{A},\hat{B}) \geq \frac{1}{1-\alpha}\left[1 - \left(\frac{1}{c}\right)^{2(\alpha-1)}\right]. \quad (5.4.15)$$

This result has the same form as shown in Ref [89]. This gives an irreducible lower bound (generalized uncertainty measure) of the uncertainty on the simultaneous measurement of observables when one use the Tsallis entropy to express the quantum uncertainty relation.

Based on this connection, one can directly use this result as an information measure in QKD protocols where the two legitimate parties, Alice and Bob generate a secret key based on the measurements of the states which they receive. However, this communication takes place in the presence of an eavesdropper, Eve who tries to learn the information being communicated. The eavesdropper can perform any kind of attack on the communication channel but however is only limited by the laws of physics [23]. Provided the correlations are stronger between the measurements of the two legitimate parties, they can still generate a secret key. We therefore appeal to the result by Devetak and Winter [87]. This result quantifies the amount of extractable key K, and is expressed as

$$K \geq H(X|E) - H(X|B), \tag{5.4.16}$$

where K is the final shared secret key, $H(X|E)$ is the amount of key that Alice can extract from a string X when given the uncertainty of the adversary about X, and $H(X|B)$ is the amount of information that Bob needs to correct his errors, using optimal error correction, given by his uncertainty about the shared string X.

Below we provide the heuristic bound for the secret key rate of QKD security proof. We give this analogy because the irreducible lower bound for the Tsallis entropy has the same form as that for the Shannon entropy, then a key bound should also follow. Therefore, without loss of generality we can simply re-write this lower bound in terms of Tsallis entropy as

$$K \geq \frac{1}{1-\alpha}\left[1 - \left(\frac{1}{c}\right)^{2(\alpha-1)}\right] - S_\alpha(X|B) - S_\alpha(Y|B). \tag{5.4.17}$$

Suppose that Alice's measurements are represented by X and X' and Bob's measurements are represented by Y and Y', therefore in order to generate a secret key the two parties need to communicate the choice of their measurements to each other. Based on the property that measurements cannot decrease entropy [88] we can write

$$K \geq \frac{1}{1-\alpha}\left[1 - \left(\frac{1}{c}\right)^{2(\alpha-1)} - S_\alpha(X|X') - S_\alpha(Y|Y')\right]. \tag{5.4.18}$$

By assuming symmetry i.e., $S_\alpha(X|X') = S_\alpha(Y|Y')$, this gives us a simple proof against collective attacks which was shown in Ref [42] for the BB84 protocol by using the Shannon entropy.

5.5 Conclusion

We have shown that the quantum uncertainty principle can be expressed in terms of the Tsallis entropy. We remark that this result preserves a form similar to an important

result which was obtained by Deutsch [89]. Regardless of the Tsallis entropies being non-additive, we have shown that a limit with a similar form can be reached as shown by Deutsch's derivation which is based on the Shannon entropy. We highlight this result provides an initial step in finding more interesting applications of the Tsallis entropy in the area of quantum information for example, as a measure of information in QKD protocols for evaluating important parameters such as secret key rates.

Chapter 6

Finite-size key analysis in the B92 protocol using the Rényi entropies

6.1 Introduction

We recall that tools to study unconditional security in the finite-key regime for all discrete variable protocols are now available in [12, 38]. Many efforts have been undertaken to improve the bounds on the secret key rates for a finite number of resources [113, 114, 132, 133, 84]. Recently, a technique involving the uncertainty relations for smooth entropies has been realized [134]. This approach has proved to be elegant since it provides bounds for general kinds of attacks rather than coherent attacks. The security bounds for the BB84 and the six-state protocols have been calculated using the smooth min-entropies in Ref [38, 113]. The secret key rate for the six-state protocol via Rényi entropies has been presented in Ref [84]. The B92 protocol has also been proven to be unconditionally secure [18, 135]. A number of key implementations of the B92 protocol have also been performed [136, 137]. To our knowledge, this technique has not been used for the B92 protocol [138]. Therefore, in this chapter we present bounds on the achievable key length for the B92 protocol [138], which involves a preprocessing step by using the uncertainty relations [134] and the Rényi entropies [139]. For a more detailed study of the B92 protocol we refer the reader to Chapter 7. This chapter is based on manuscript **M2**.

6.2 The B92 QKD Protocol

This protocol was proposed by Bennett in 1992 [138]. In contrast to the BB84 protocol which uses four states, the B92 protocol utilizes two non orthogonal states. By encoding in the non orthogonal states of the quantum system, it is not possible for the eavesdropper to make an exact copy of the system or to gain partial information about the system without disturbing it. Below we describe the steps taken in the execution of the B92 protocol.

State preparation. Alice sends one of the two non-orthogonal states which we denote by $|\psi_{\pm}\rangle$, to Bob. Bob randomly chooses to measure in one of the two von Neumann measurements. The first measurement projects onto the basis $|\psi_{+}\rangle$ which consists of the vectors $\{|\psi_{-}\rangle, |\tilde{\psi}_{-}\rangle\}$, where $|\tilde{\psi}_{-}\rangle$ is orthogonal to $|\psi_{-}\rangle$. The second measurement similarly projects onto the basis $|\psi_{-}\rangle$ which consist of the vectors $\{|\psi_{+}\rangle, |\tilde{\psi}_{+}\rangle\}$, where $|\tilde{\psi}_{+}\rangle$ is orthogonal to $|\psi_{+}\rangle$. Then Bob announces an acceptance if he gets an outcome which corresponds to $|\tilde{\psi}_{\pm}\rangle$; otherwise, both parties discard the values that they recorded.

Sifting and measurement. Alice records the bit value 0 or 1 if she sends $|\psi_{+}\rangle$ or $|\psi_{-}\rangle$, and Bob records 0 or 1 if he obtains $|\tilde{\psi}_{-}\rangle$ or $|\tilde{\psi}_{+}\rangle$, respectively. Alice sends each quantum state with equal probability, while Bob randomly chooses between his two measurements.

Parameter estimation. The role of parameter estimation is to minimize the set of compatible states Γ, given m sample points. Let $\Gamma_{\varepsilon_{\mathrm{PE}}}$ be a set of states from which a key is extracted with a non-negligible probability. The failure probability in the parameter estimation step is denoted as $\varepsilon_{\mathrm{PE}}$. The parameter estimation passes, although the raw key does not contain sufficient secret information. In particular, if the statistics λ_m are obtained by measuring m samples of ρ_{AB} (i.e., the entangled state shared by Alice and Bob) according to a positive operator-valued measure (POVM) with d possible outcomes and if $\lambda_{\infty}(\rho_{AB})$ denotes the perfect statistics in the limit of infinitely many measurements, then for any state ρ_{AB} (see also Section 4.5.4) [12]

$$\Gamma_{\xi} := \{\rho_{AB} : ||\lambda_m - \lambda_{\infty}(\rho_{AB})||_1 \leq \xi\}, \tag{6.2.1}$$

where by the law of large numbers [38]

$$\xi := \sqrt{\frac{\ln(1/\varepsilon_{\mathrm{PE}}) + 2\ln(m+1)}{2m}}. \tag{6.2.2}$$

Error correction. The error-correction step serves the purpose of correcting all the erroneously received bits and giving an estimate of the error rate. Alice and Bob hold correlated bits strings denoted as X^n and Y^n. The number of bits leaked during the classical communication to an eavesdropper is given by [12, 113]

$$\mathrm{leak}_{\mathrm{EC}} = f_{\mathrm{EC}} n h(Q) + \log_2(\frac{2}{\varepsilon_{\mathrm{EC}}}), \tag{6.2.3}$$

where f_{EC} is a constant larger than 1 (in practice, f ≈1.05 - 1.2), $h(Q)$ is the binary Shannon entropy, Q is the quantum bit-error rate, (QBER), and $\varepsilon_{\mathrm{EC}}$ is the error probability in the error-correction step.

Privacy amplification. The objective of this step is to minimize the quantity of correct information which the eavesdropper may have obtained about Alice's and Bob's raw key. Let Alice and Bob hold a perfectly correlated bit string X^n on which Eve may

have some information. Alice chooses at random a function $\mathcal{F}$ from a two-universal hash function and sends a description of $\mathcal{F}$ to Bob. Then Alice and Bob compute their keys $S_A = \mathcal{F}(X^n)$ and $S_B = \mathcal{F}(\hat{X}^n)$. By using the result in [107], it has been found that the achievable length of the secret key that can be computed from X by the two universal hash function, $\mathcal{F}$ can be expressed as

$$\ell = H_{\max}^{\bar{\varepsilon}}(X|E) - H_{\min}^{\bar{\varepsilon}}(X|Y) - 2\log_2(1/\varepsilon), \tag{6.2.4}$$

where $\bar{\varepsilon} = (\varepsilon/8)^2$ and ε quantifies the security of the final key.

6.3 Definitions

6.3.1 Rényi entropy

The Rényi entropies are a family of functions on probability distributions which quantify the uncertainty or randomness of a system. For the definition of the Rényi we refer the reader to Section 3.2.5. The min-Rényi entropy (i.e., $\alpha > 1$) is defined as

$$H_\alpha^\varepsilon(A)_\rho = \min_{\bar{\rho}} H_\alpha(A)_{\bar{\rho}}, \tag{6.3.1}$$

and the max-Rényi entropy (i.e., $\alpha < 1$) is defined as

$$H_\alpha^\varepsilon(A)_\rho = \max_{\bar{\rho}} H_\alpha(A)_{\bar{\rho}}. \tag{6.3.2}$$

The maximization in each case is over an ε-ball of states $\bar{\rho}$ close to ρ [140].

6.3.2 Smooth Min-and Max-entropy

The idea of min- and max-entropy was introduced by Renner [38]. Since then, a lot of efforts have been made to investigate various properties and applications in the area of quantum information theory especially in the security of quantum cryptography and related tasks such as information reconciliation. Smooth entropies are used to quantify the number of uniform bits that can be extracted from a random source. The Rényi entropy with $\alpha > 1$ are close to the smooth min-entropy by considering that

$$H_{\min}^\varepsilon(X) \geq H_\alpha(X) - \frac{1}{\alpha - 1}\log_2\frac{1}{\varepsilon}, \quad \alpha > 1, \tag{6.3.3}$$

while those with $\alpha < 1$ are close to the smooth-max entropy. The smooth min-entropy is used to characterize the reliable transmission in one single use of a classical channel while the smooth max-entropy is used to characterize data compression in a one-time scheme. The smooth min-entropy can be interpreted as a guessing probability [140]. For a detailed overview of smooth conditional entropies and their basic properties we refer to [38, 141].

6.3.3 Min- and Max-entropy

We follow closely the definitions of the smooth min- and max-entropy as introduced by Renner [38]. For a finite-dimensional Hilbert space $\mathcal{H}$, we use $\mathcal{P}(\mathcal{H})$ to denote the set of positive semi-definite operators on $\mathcal{H}$. The set of normalized quantum states $\mathcal{S}(\mathcal{H}) := \{\rho \in \mathcal{P}(\mathcal{H}) : \mathrm{tr}\rho = 1\}$ and the set of sub-normalized states $\mathcal{S}_{\leq}(\mathcal{H}) := \{\rho \in \mathcal{P}(\mathcal{H}) : \mathrm{tr}\rho \leq 1\}$. We use indices to denote multipartite Hilbert spaces for example, $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$.

Conditional min-entropy

Let $\rho_{AB} \in S_{\leq}(\mathcal{H}_{AB})$ and $\sigma_{AB} \in \mathcal{S}(\mathcal{H}_B)$; then the min-entropy of A conditioned on B of state ρ_{AB} is defined as

$$H_{\min}(A|B)_{\rho|\sigma} := \max_{\sigma} \sup\{\lambda \in \mathbb{R} : \rho_{AB} \leq 2^{-\lambda} \mathbb{1}_A \otimes \sigma_B\}, \tag{6.3.4}$$

where the maximum is taken over all states $\sigma \in \mathcal{S}_{\leq}(\mathcal{H}_B)$. Furthermore, we define

$$H_{\min}(A|B)_{\rho} := \max_{\sigma_B \in \mathcal{S}(\mathcal{H}_B)} H_{\min}(A|B)_{\rho|\sigma}. \tag{6.3.5}$$

The min-entropy, $H_{\min}(A|B)_\rho$ is finite if and only if $\mathrm{supp}\{\sigma_B\} \supseteq \mathrm{supp}\{\rho_B\}$ and $-\infty$ otherwise. The max-entropy is its dual with regards to a purification ρ_{ABC} of ρ_{AB} on an auxiliary Hilbert space $\mathcal{H}_C$.

Conditional max-entropy

Let $\rho_{ABC} \in S_{\leq}(\mathcal{H}_{ABC})$ be pure; then the max-entropy of A conditioned on B of state ρ_{AB} is defined as

$$H_{\max}(A|B)_{\rho} := -H_{\min}(A|C)_{\rho}. \tag{6.3.6}$$

The quantum entropies can be ordered as follows

$$H_{\min}(A|B)_{\rho} \leq H(A|B)_{\rho} \leq H_{\max}(A|B)_{\rho}. \tag{6.3.7}$$

In order to define smooth versions, we consider the set of states close to ρ in the following sense. For $\varepsilon > 0$, we define an ε-ball of states around $\rho \in \mathcal{S}(\mathcal{H})$ as

$$\mathcal{B}^{\varepsilon}(\rho) := \{\tilde{\rho} \in \mathcal{S} = (\mathcal{H}) : D(\rho, \tilde{\rho}) \leq \varepsilon\}, \tag{6.3.8}$$

where $D(\rho, \tilde{\rho}) := \sqrt{1 - F^2(\rho, \tilde{\rho})}$ is a distance measure based on the fidelity $F(\rho, \tilde{\rho}) := \mathrm{tr}|\sqrt{\rho}\sqrt{\tilde{\rho}}|$ introduced in Section 3.3. We use this choice of measure because it is invariant under purifications and is directly related to the trace distance for pure states. Smoothed versions of the min-entropy are then defined as:

$$\begin{aligned} H^{\varepsilon}_{\min}(A|B)_{\rho|\sigma} &:= \max_{\tilde{\rho} \in \mathcal{B}^{\varepsilon}(\rho_{AB})} H_{\min}(A|B)_{\tilde{\rho}|\sigma}, \\ H^{\varepsilon}_{\min}(A|B)_{\rho} &:= \max_{\tilde{\rho} \in \mathcal{B}^{\varepsilon}(\rho_{AB})} H_{\min}(A|B)_{\tilde{\rho}}, \end{aligned} \tag{6.3.9}$$

and similarly

$$H^{\varepsilon}_{\max}(A|B)_{\rho} := \min_{\tilde{\rho} \in \mathcal{B}^{\varepsilon}(\rho_{AB})} H_{\max}(A|B)_{\tilde{\rho}}. \tag{6.3.10}$$

6.4 Results

6.4.1 Bound on the secure key rate

According to [38], for any $\varepsilon \geq 0$, a final key S is said to be ε secure with respect to an adversary Eve if the joint state ρ_{SE} satisfies (see also Section 4.5.2)

$$\min_{\rho_E} \frac{1}{2}||\rho_{SE} - \rho_S \otimes \rho_E||_1 \leq \varepsilon, \tag{6.4.1}$$

where $\rho_{SE} = \sum_{s\in\mathcal{S}} P_s(s)|s\rangle\langle s| \otimes \rho_E^s$, $\{|s\rangle\}_{s\in\mathcal{S}}$ is an orthonormal basis of some Hilbert space $\mathcal{H}_s$, $\rho_S = \sum_{s\in\mathcal{S}} P_s \frac{1}{|S|}|s\rangle\langle s|$ is a fully mixed state on $\mathcal{H}_s$, ρ_E is the state held by an eavesdropper and $||A||_1 = \mathrm{tr}|A| = \mathrm{tr}\sqrt{A^\dagger A}$ is the trace distance. The parameter ε, represents the maximum failure probability in which an adversary may have gained some information on S, or it can be interpreted as the maximum failure probability in which the extracted key deviates from the ideal key.

The secret key rate in the asymptotic regime is expressed as $\lim_{N\to\infty} r = S(X|E) - H(X|Y)$, where $S(X|E)$ and $H(X|Y)$ are the conditional von Neumann and Shannon entropies [113]. However, in the non-asymptotic regime this equation becomes invalid as we have a finite number of bits that Alice sends to Bob [12].

In order to determine the length ℓ of ε-secure key bits that can be generated by this protocol we use the following results on the uncertainty relation [134]. The amount of key that can be extracted from a string X is given by the uncertainty of the adversary about X, measured in terms of the smooth Rényi entropies. The amount of information B needs to correct his errors, using optimal error correction is given by his uncertainty about A's string, again measured in terms of the smooth Rényi entropies. Combining these two results, we have [103]

$$H_{\min}^{\bar{\varepsilon}}(\mathbf{X}|E) + H_{\max}^{\bar{\varepsilon}}(\mathbf{Z}|B) \geq \log_2 \frac{1}{c}, \tag{6.4.2}$$

where $\bar{\varepsilon} \geq 0$ is the smoothing parameter and c quantifies the 'incompatibility' between the measurements $\mathbf{Z} = Z^{\otimes n}$ and $\mathbf{X} = X^{\otimes n}$. It is defined as $c = -\max_{x,z}||\sqrt{M_X}\sqrt{N_Z}||_\infty^2$, where $\{M_X\}$ and $\{N_Z\}$ are POVM elements for preparing the state corresponding to the $\mathbf{X}$ and $\mathbf{Z}$ bases respectively [103]. This norm is called the Schatten p-norm where $p = \infty$. It is defined as $||A||_p = \left(\sum_{i=1}^{\min\{m,n\}} \sigma_i^p\right)$ [52]. This definition also applies to the entanglement based version of the protocol.

The definitions of the smooth min and max-entropies have been given above. The measure of uncertainty for Bob's measurement $H_{\max}$ can only increase under information processing such that

$$H_{\max}^{\bar{\varepsilon}}(\mathbf{Z}|B) \leq H_{\max}^{\bar{\varepsilon}}(\mathbf{Z}|\mathbf{Z}'), \tag{6.4.3}$$

where the measurement $\mathbf{Z}' = Z'^{\otimes n}$ is made on Bob's system [142]. The protocol does not need to prescribe the actual measurements of $\mathbf{Z}$ and $\mathbf{Z}'$. However, based on the observed parameters we can replace the measurement on $\mathbf{X}$ and $\mathbf{X}'$ in this hypothetical

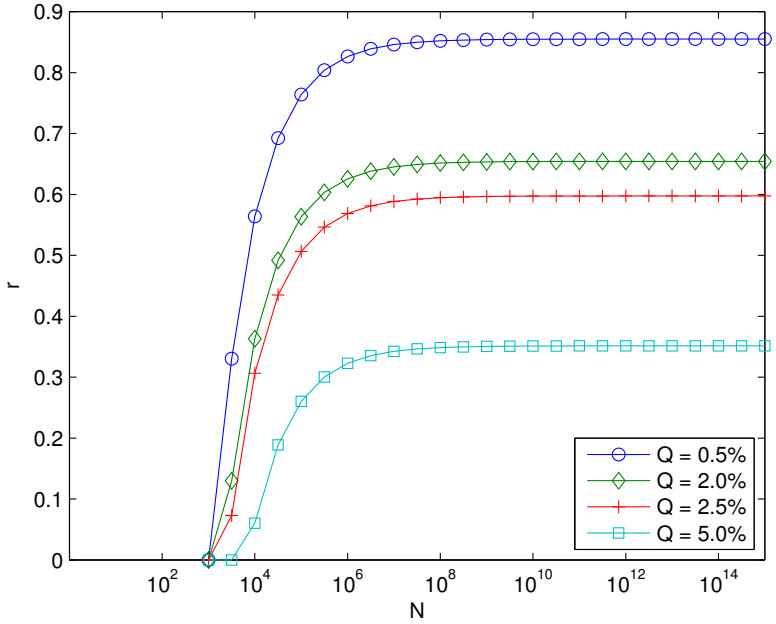

Figure 6.1: Lower bound on the secret key fraction, r, for the finite B92 protocol as a function of the exchanged quantum signals N for bit errors Q = 0.5%, 2%, 2.5%, 5%. The maximum failure probability of the protocol is $\varepsilon = 10^{-5}$ and the failure probability of the error-correction procedure is $\varepsilon_{\mathrm{EC}} = 10^{-10}$ [**M2**].

protocol by highly correlated measurements $\mathbf{Z}$ and $\mathbf{Z}'$ respectively. This means that the uncertainty in $H_{\max}^{\bar{\varepsilon}}(\mathbf{Z}|\mathbf{Z})$ is small and the following bound on the smooth max-entropy

$$H_{\max}^{\bar{\varepsilon}}(\mathbf{Z}|\mathbf{Z}') \leq nh(Q), \tag{6.4.4}$$

holds, where Q is the QBER. This result follows the argument in [103].

6.4.2 Bound on the achievable key length

Let ρ_{XBE} be the state describing Alice's bit string X^n and Bob's string B^n as well as Eve's quantum information represented by ρ_{E^n}. Let $\bar{\varepsilon}, \varepsilon_{\mathrm{PA}} \geq 0$. If the length of the key is such that

$$\ell \leq \left(H_{\min}(\mathbf{X}|E)_{\rho_{XBE}} - 2\log_2 \frac{1}{2\bar{\varepsilon}} - 2\log_2 \frac{1}{2\varepsilon_{\mathrm{PA}}} \right), \tag{6.4.5}$$

then the protocol is secure.

Proof. Let $\rho_{XB} \in \mathcal{P}(\mathcal{H}_X \otimes \mathcal{H}_B)$ be a density operator which is classical with respect to an orthonormal basis $\{|x\rangle\}_{x\in\mathcal{X}}$ of $\mathcal{H}_X$, let $\mathcal{F}$ be a two universal family of hash functions from $\mathcal{X}$ to $\{0,1\}^\ell$, and let $\varepsilon \geq 0$. Then the security of the key can be defined with respect to the L_1 distance as [38],

$$d(\rho_{F(X)BF}|BF) \leq 2\varepsilon + \frac{1}{2} 2^{-\frac{1}{2}[H_{\min}^{\varepsilon}(X|B)-\ell]}. \tag{6.4.6}$$

However, the L_1 distance is equal to the composable definition of security then,

$$||\rho_{F(X)BF} - \rho_U \otimes \rho_{BF}||_1 \leq 2\varepsilon + \frac{1}{2}2^{-\frac{1}{2}[H_{\min}^{\varepsilon}(X|B)-\ell]}, \tag{6.4.7}$$

where $\rho_{F(X)BF} = \sum_{f\in\mathcal{F}} P_F(f)\rho_{f(X)B} \otimes |f\rangle\langle f|$ for $\rho_{F(X)BF} \in \mathcal{P}(\mathcal{H}_Z \otimes \mathcal{H}_B \otimes \mathcal{H}_F)$.

By introducing the transcript of the classical communication C and without loss of generality we have

$$||\rho_{F(X)^{\ell}ECF} - \rho_U \otimes \rho_{ECF}|| \leq 2\varepsilon + 2^{-\frac{1}{2}[H_{\min}^{\varepsilon}(X|B)-\ell]}, \tag{6.4.8}$$

where $\rho_{F(X^n)^{\ell}ECF} = \sum_{f\in\mathcal{F}} P_F(f)\rho_{f(X^n)^{\ell}EC} \otimes |f\rangle\langle f|$. By using the triangle inequality and using the fact that the trace distance does not increase after applying the partial trace, we have

$$\begin{aligned}
&||\rho_{F(X)^{\ell}ECF} - \rho_U \otimes \rho_{ECF}|| \\
&\leq \; ||\rho_{F(X)CEF} - \bar{\rho}_{F(X)CEF}||_1 + ||\bar{\rho}_{F(X)CEF} \\
&- \; \rho_U \otimes \bar{\rho}_{CEF}||_1 + ||\bar{\rho}_{CEF} - \rho_{CEF}||_1 \\
&\leq \; 2\bar{\varepsilon} + ||\bar{\rho}_{F(X)CEF} - \rho_{F(X)CEF}||_1 \\
&\leq \; 2\bar{\varepsilon} + 2^{-\frac{1}{2}[H_{\min}^{\varepsilon}(X|B)-\ell]} \\
&\leq \; 2\bar{\varepsilon} + \varepsilon_{\text{PA}}.
\end{aligned} \tag{6.4.9}$$

With the help of the data-processing inequality [38] and the uncertainty relation in Equation (6.4.2) we obtain

$$\begin{aligned}
H_{\min}^{\varepsilon'}(\mathbf{X}|E') \;&\geq\; H_{\min}^{\varepsilon'}(\mathbf{X}|E) - \text{leak}_{\text{EC}} \\
&\geq\; nq - H_{\max}^{\bar{\varepsilon}}(\mathbf{Z}|\mathbf{Z}') - \text{leak}_{\text{EC}} \\
&\geq\; nq - \frac{(1-2\delta)\eta + 2\delta}{2}[\varepsilon - (1-\varepsilon)h(x)] \\
&-\; nh(Q) - \text{leak}_{\text{EC}},
\end{aligned} \tag{6.4.10}$$

where $q = \log_2 1/c$ is the quality factor and

$$x = \frac{(1-5\delta)(1-\delta)\eta(1-\eta)}{[\delta + (1-2\delta)\eta](1-\delta) - (1-5\delta)\eta},$$

In the above Equation, $\eta = (2\alpha\beta)^2$, where $\alpha \in (0, \frac{1}{\sqrt{2}})$ and $\beta = \sqrt{1-\alpha^2}$ are complex numbers and $\delta = 2/3p, (0 < p < 1)$, where p describes the amount of noise in the depolarizing channel. The error rate conditioned on acceptance is given by $\varepsilon = \delta/(1-2\delta)\eta + 2\delta$ [143]. By substitution of Eq (6.4.10) into Eq (6.4.5), we find that the secret key rate r varies with the number of signals N, as shown in Figure 6.1. Again, if we combine Eq (6.4.10) with the proposed bound on the achievable key length in Eq (6.4.5) and also by using the quantum leftover hash lemma [144], we have

$$\triangle \leq \varepsilon' + \frac{1}{2}\sqrt{2^{\ell - H_{\min}^{\varepsilon'}}(X|E')} \leq 2\bar{\varepsilon} + \varepsilon_{PA}, \tag{6.4.11}$$

where $\triangle = \varepsilon$ (from Equation 6.4.1), E' summarizes all information Eve learned about $\mathbf{X}$ during the protocol, including the classical communication sent by Alice and Bob over the authenticated channel.

6.5 Conclusion

We have demonstrated how one can use results of the uncertainty relations and smooth Rényi entropies to derive security bounds for the B92 QKD protocol when a finite number of signals are used. The key rate is slightly lower than that for the BB84 protocol derived from the same principles [103]. However, these results show that a minimum number of approximately $10^4 - 10^6$ of signals is required in order to extract a reasonable length of the secret key in QKD protocols under realistic scenarios. Similar results have also been discussed in [12, 113, 114, 133]. Therefore, the uncertainty relations and the smooth Rényi entropies prove to be a powerful technique for the derivation of the security bounds in QKD protocols in the finite-size-key regime.

Chapter 7

Implementation and security analysis of the B92 protocol using the id3100 Clavis system

7.1 Introduction

In this chapter, we present an experimental demonstration of the B92 QKD protocol [16] by using the id300 Clavis^2 system from idQuantique. Despite the B92 protocol [16] being theoretically simpler to implement than the BB84 protocol [8], surprisingly this advantage has not been fully exploited. For example, it uses only two states provided they are non-orthogonal, hence it requires less resources. Therefore, we show in this chapter the feasibility of implementing the B92 protocol by using the id3100 Clavis^2 system. The system shows a secure key generation rate of 6.42 kilobits per second and a quantum bit error rate of 1.1% at a mean photon number (μ) = 0.03 over an optical line length of 30km. Our results scale similarly to BB84 protocol results thus showing the feasibility of an implementation of a two-state protocol over a fibre network in a system which was traditionally used for running the BB84 [8] and SARG04 [145] protocols. This chapter is based on the manuscripts **M3** & **M6**.

7.2 The B92 QKD protocol

Similar to the familiar BB84 protocol, the B92 protocol follows the usual QKD procedure, with a quantum phase and a classical phase. However, as opposed to the BB84 protocol which makes use of four quantum states, the B92 protocol uses two non-orthogonal quantum states to encode information. In principle, encoding information between two non-orthogonal states makes it impossible for an eavesdropper to distinguish between the two quantum states of the system [14]. Again, instead of single photon states, the B92 protocol relies on the coherent states and also implements a homodyne measurement at Bob [16]. Moreover, because of the type of encoding in the

B92 protocol this makes it less tolerant to noise because of the high probability for Eve to perform unambiguous discrimination of the encoded key bit. But, this is impossible in the BB84 protocol because Alice's encoding is chosen at random [146]. In the B92 protocol, Alice chooses one of two non-orthogonal states with a priori probability of 1/2. The bits '0' and '1' are encoded into these two quantum states. The non-orthogonal quantum states are encoded into weak coherent states $|\pm\alpha\rangle$ for $\alpha \in \mathbb{R}$, which are accompanied by a strong reference pulse [14].

A number of theoretical and experimental progress has been reported in various papers for this protocol in the last decade. In particular, an unconditional security proof of the B92 protocol by first reducing it to an entanglement distillation protocol which is initiated by a local filtering process was reported by Tamaki and Lütkenhaus in 2003 [147]. A proof against individual attacks over a realistic channel was obtained by Tamaki, Koashi and Imoto [148]. An unconditional security proof for the B92 protocol implemented by a strong phase-reference pulse instead of the weak pulse assumption was shown by Koashi in 2004 [17]. Later, again Tamaki and Lütkenhaus showed that this protocol over loss-free channel can be adapted to accommodate loss and they obtained an unconditional security proof over a lossy and noisy channel. In the proof, it is assumed that Alice and Bob employ an error discarding protocol [149]. However, when compared to the BB84 protocol, the B92 protocol is very sensitive to channel noise. Therefore, in order to compensate for channel noise, the protocol uses weak coherent states together with a strong reference pulse. In particular, by using a strong reference pulse, the eavesdropper, Eve is prevented from blocking the whole signal without causing any errors. This is seen in Tamaki *et al.* where an unconditional security proof is reported when this protocol is implemented with a strong reference pulse [18].

Regardless of the challenges that come with aligning and stabilising both interferometers which makes the system very sensitive and a need for active control in the B92 scheme, a successful implementation of the protocol was demonstrated in Ref [150]. Moreover, a key distribution for over a 48 km optical length for both the B92 and BB84 protocols was shown by Hughes *et al.* [136]. Notably, an experiment of the B92 protocol reaching a distance of 122km of standard telecom fiber by Gobby *et al.* in 2000 [137]. Moreover, a prototype of a free-space QKD scheme based on the B92 protocol was reported by Canale *et al.* in Ref [151].

7.3 Plug and Play scheme

The Plug and Play scheme for QKD was introduced by Muller *et al.* [1]. Figure 7.1 shows the Plug and Play system. It features Bob's equipment which consists of the laser, couplers, Faraday rotators, FR, mirrors, M_i's and a single photon detector, D0; while Alice's equipment consists of a coupler, C, classical detector, D, a phase modulator, PM and a Faraday rotator, FR. In the scheme, Bob sends a classical signal to Alice which she attenuates to an average of a single photon per pulse. She then encodes the intended key value into the pulses of the received signal. Alice then sends the received signal back to Bob who then performs measurements. This scheme automatically and passively compensates for a phase drift during the signal transmission, thereby providing

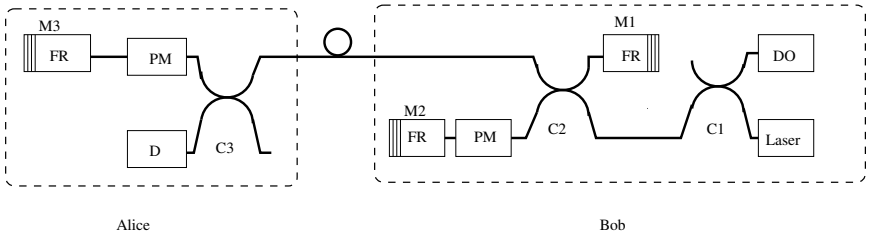

Figure 7.1: Plug and Play system as introduced by Muller *et al.* [1]. The system makes use of the following components: single photon detector, D0; fiber coupler, C_i; phase modulator, PM; Faraday rotator, FR; mirror, M_i; classical detector, D.

stability in optical fibre communication. A major advantage of the Plug and Play system is that it does not require additional optical adjustment during operation. It is justifiable to implement the B92 protocol on the Plug and Play system (which is an interferometric set-up), since the original B92 protocol was based on an interferometric set-up [16]. The scheme has has been shown to be robust against environmental noises and there are still some outstanding security issues regarding this configuration [152]. However, an implementation of QKD for over 67 km by using a Plug and Play system was demonstrated by Stucki *et al.* in 2002 [2]. Notably, the Plug and Play has also been used as part of the devices in the SECOQC QKD network in Vienna [30].

7.4 Experimental setup

The Clavis^2 system is a QKD research platform which was developed by idQuantique, Switzerland. It is used to deploy the Plug and Play implementations of the QKD protocols. It uses a proprietary auto-compensating optical platform which reduces the value of the QBER. The system can provide secure key exchanges up to a distance of about 100km. Our system consists of a dual-computer Plug and Play configuration where two separate computers are used to control the two quantum communication nodes; on the left for Alice's equipment and on the right for Bob's equipment. The set-up is shown in Figure 7.2. The two nodes are themselves connected by an optical fiber, which acts as a quantum channel. The system operates at the telecommunication wavelength (λ=1500 nm). The classical channel is realized through the ethernet connection between the two communicating computers.

For a four state QKD protocol when implemented by using the Clavis^2 system, Alice encodes the quantum system by applying a phase shift of 0, π, $\frac{\pi}{2}$ or $\frac{3\pi}{2}$. Bob then completes the protocol by performing some measurements, where he chooses the measurement basis by applying a phase shift of either 0 or $\frac{\pi}{2}$ and either π or $\frac{3\pi}{2}$. However, in our experiment, we implemented a two state protocol by limiting the phase shift to two states only. The phase modulators are adjusted in order to compensate for this change. The voltages applied to the modulators define the phase shift applied to each pulse. These voltages are adjusted such that Alice outputs only two relative phases in accordance to the bit choice. Bob measurement basis induced an interference at the exit

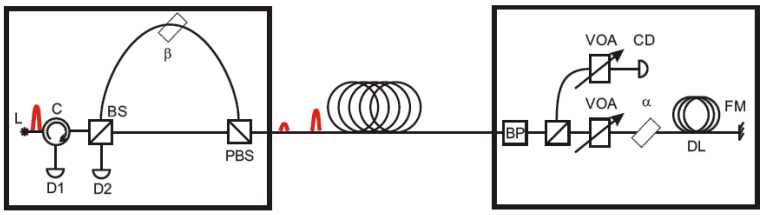

Figure 7.2: Experimental set-up for the id3100 Clavis^2 System used for the implementation the B92 protocol. Two separate computers are used to control nodes: Alice on the left and Bob on the right. The nodes are themselves connected by the optical fiber. The system makes use of the following; laser, L; beam splitter, BS; polo arising beam splitter, PBS; C, circulator; α, β, phase modulator; BP, bandpass filter; D_i, quantum detector; Faraday mirror, FM; coupler, C; delay line, DL; optical attenuator, VOA.

of the interferometer to provide discrete measurements upon a compatible basis choice. The software was reprogrammed to accommodate these changes while no additional hardware was required to be added to the system. We highlight that this step achieves the realization of the B92 QKD protocol. Since the B92 protocol is very vulnerable to bright-pulse attack [19], fortunately the Clavis^2 system has a strong classical reference frame. This enables a secure implementation of the B92 protocol.

Laser output power was measured to be -14 dB. Additionally, detection probabilities were determined for different optical losses, together with the corresponding visibility measurements, and the results are given in Table 7.5. The next step was the raw key exchange session. This session is more or less similar to the one used for the SARG04 protocol in Clavis^2 System. The difference is that for the B92 protocol, only one pair of non-orthogonal states is used by Alice for state preparation, while the other pair is used by Bob for measurement. This was followed by the key distillation step, from which the QBER and secure key rates for different optical loses were determined. Finally, key generation rates for the B92 protocol were compared to the key generation rates for the BB84 protocol, in order to ascertain the utility of the B92 implementation. Quantum signals were then detected at either detector D1 or D2 shown in Figure 7.2. During initialization, the dark count probabilities of D1 and D2 were measured to be 5.78 $\times 10^{-5}$ and 5.60 $\times 10^{-5}$, respectively.

7.5 Results and Discussion

Table 7.1 presents the QKD parameters which we measured and are later used in the security analysis. These parameters are loss, QBER, P_s probability of detecting a signal and P_d dead time probability and V, visibility.

The number of photons n, in the pulse is Poisson distributed with a mean photon number, μ. Therefore, the probability of finding n photons in a pulse $P(n, \mu)$ can be

Loss (dB)	QBER	P_s	P_d	Visibility
1	0.0098324	0.1393725	0.0000500	99.65
2	0.0102556	0.1245905	0.0000596	99.55
3	0.0104741	0.1130995	0.0000545	99.30
4	0.0107115	0.105114	0.0000536	99.18
5	0.0109773	0.0947909	0.0000540	98.46
6	0.0110112	0.0856511	0.0000552	97.24
7	0.0110323	0.0417971	0.0000560	94.83

Table 7.1: Experimentally measured QKD parameters for the set-up shown in Fig 7.2. The parameters are; Loss(dB), which is achieved by varying the attenuation of the signal, Quantum Bit Error Rate (QBER) which is obtained by using Equation (7.5.6); P_t refers to the overall probability of photon detection on Bob's side. This probability is evaluated from Equation (7.5.4); P_d refers to the dark count probability and V is the visibility of the quantum channel in percentage.

expressed as [14]

$$P(n,\mu) = \frac{\mu^n e^{-\mu}}{n!}. \tag{7.5.1}$$

The signals sent through an optical fibre, in practice, suffer from losses as distance of transmission increases. This loss is mainly due to scattering in the fibre. The most important parameter which needs to be evaluated in any QKD system is the raw key rate, R_{raw} [14]. The R_{raw} between Alice and Bob is expressed as

$$R_{\text{raw}} = qv\mu t_{AB} t_B \eta_B, \tag{7.5.2}$$

where q relies on the implementation, v is the repetition frequency, μ is the average number of photons per pulse, t_{AB} is the transmission on the line between Alice and Bob, t_B is Bob's internal transmission per pulse and η_B is the Bob's detection efficiency ($t_B \approx 0.67$) and η_B is Bob's detection efficiency ($\eta_B \approx 0.1$). The transmittivity t, of a fibre is given by $t = 10^{-\alpha d/10}$, where α is the attenuation constant and is currently optimal at $\alpha = 0.2$ and d is the transmission distance in km [14]. The overall transmission can be expressed similarly as $\eta = t_c \eta_B$ where t_c is the channel transmission. The probability P_s of detecting a signal at the detector is expressed as

$$P_s = 1 - e^{-\eta\mu}. \tag{7.5.3}$$

Now, we can evaluate the overall detection probability, P_t which can be expressed as

$$\begin{aligned} P_t &= P_s + P_d - P_s P_d \\ &\cong P_s + P_d, \end{aligned} \tag{7.5.4}$$

where P_d is the dark count probability and $P_s P_d$ is the coincidence of detection between signal and dark count and is usually neglected in the experiment.

In order to test the quality of our QKD scheme we use the quantum bit error rate (QBER). The QBER is an important parameter in QKD because it is used to investigate

the security in QKD protocols [14]. The QBER is simply the fraction of error bits f_c to the total number of bits t_c. The QBER which is expressed as

$$QBER = \frac{f_c}{t_c} \tag{7.5.5}$$

where f_c are false counts and t_c are total counts. The false counts, $f_c = e_0 P_d + P_s$ where e_0 is the error detection due to background and signal respectively while $t_c = P_t$. This is achieved through the use of some extra classical post-processing steps in order to extract the secret key. The QBER can also be written as

$$QBER = QBER_{\text{opt}} + QBER_{\text{dark}} + QBER_{\text{after}} + QBER_{\text{stray}}. \tag{7.5.6}$$

In this expression, $QBER_{\text{opt}}$ is the probability that a photon hits the wrong detector. This can also be used as a way to determine the optical alignment of the polarization components and the stability of the fibre link. This is expressed as

$$QBER_{\text{opt}} = \frac{1 - V}{2}, \tag{7.5.7}$$

where V is the visibility. The $QBER_{\text{dark}}$ is the error due to dark counts. The $QBER_{\text{dark}}$ is expressed as

$$QBER_{\text{dark}} \cong \frac{p_{\text{dark}}}{\mu t_{AB} t_B \eta_B}. \tag{7.5.8}$$

The $QBER_{\text{dark}}$ forms the most important parameter in the sense that it increases with distance and therefore limits the range of key distribution. Based on Table 7.1, as the loss increases the QBER increases as well as the dark count probability. This leads to a decrease in the secret key rate as distances increases. This is shown in Figure 7.3. The $QBER_{\text{after}}$ is the error due to after pulses. It is expressed as

$$QBER_{\text{after}} \cong \sum_{n=0}^{n=1/p_{det}} p_{\text{after}}(\tau + \frac{n}{v}), \tag{7.5.9}$$

Due to the unavailability of a single photon source, we use a weak laser source. However, this comes with costs as it is associated with some attacks from an eavesdropper called the photon number splitting attacks [153]. This allows her to get full information without being detected.

Based on our measured parameters, we can calculate the secret key generation rate r, against the PNS attacks as

$$r = P_t[(1 - \xi')\beta - f_{EC} h(Q)], \tag{7.5.10}$$

where $\xi' = \xi(Q/\beta)$ and again $\xi(Q) = \log_2(1 + 4Q - 4Q^2)$, $\beta = (P_t - P')/P_t$, $f_{EC} = 1.05$ is the error correction efficiency and Q is the QBER. Again, in the expression, ξ is the fraction of key discarded during privacy amplification and $P' = 1 - (1 + \mu + \mu^2/2 + \mu^3/12)Q^{-\mu}$. The term $h(Q)$ is the binary entropy function and is expressed as $h(Q) = -Q\log_2(Q) - (1 - Q)\log_2(1 - Q)$. The variation of the secret rate against distance for the B92 protocol is shown in Figure 7.3. The secret key rate obtained is slightly lower than that of BB84 protocol as expected [23], however it still scales similarly with that

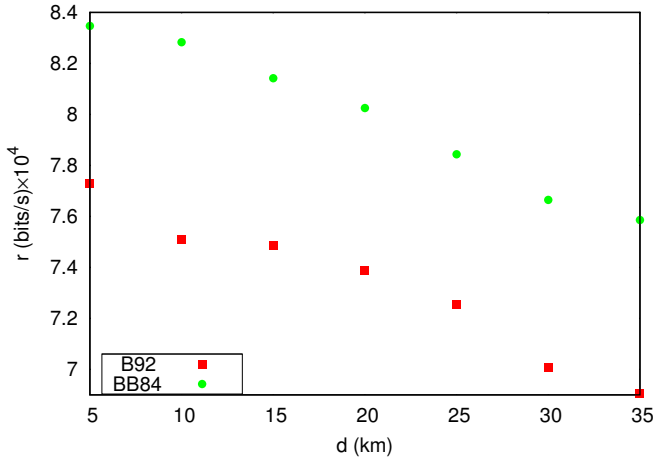

Figure 7.3: Experimental secret key rate for the B92 and BB84 protocols as a function of distance. In order to find the key rates, we use formalism developed in Ref [2].

of the standard BB84 protocol. The difference between the two mutual informations is given as

$$\eta_{\text{dist}} = I(A:B) - I(A:E), \tag{7.5.11}$$

where $I(A:B) = 1 + D\log_2 D + (1-D)\log_2(1-D)$ and D is equal to the total QBER and $I(A:E) \cong 0.03 + I_{2v}$. I_{2v} is a consequence of multi-photon pulses and is about 0.06, 014 and 0.40 for 5, 10 and 20dB losses respectively for μ=0.25dB/km. In Figure 7.4, we show the variation of Shannon mutual information between Alice and Bob $I(A:B)$ and between Alice and Eve $I(A:E)$ against optical loss. As the optical loss increases the amount of noise in the channel also increases. This leads to an increase in the amount of information which the eavesdropper gains. For simplicity, we attribute all the noise to the eavesdropper. The secret key can only be extracted if $I(A:B) > I(A:E)$. Therefore, as $I(A:E)$ increases the amount of secret key decreases as shown in Figure 7.3.

7.6 Conclusion

In this work we have experimentally demonstrated that we can adapt the set-up which was originally designed to run the BB84 and SARG04 protocols and use it to implement the B92 protocol. We have shown how the quantum bit error rate behaves as we vary loss. In particular, we show that in our implementation we can achieve reasonable secret key rates which scale similarly as the BB84 protocol for some reasonable communication distance on a fibre optic network. In summary, these results show that it is possible to implement the B92 QKD protocol using the Clavis^2 system. This is very useful in the sense that as opposed to the four state protocol, the B92 protocol uses less resources hence it is simpler to implement thus extending the applicability of the Clavis^2 system.

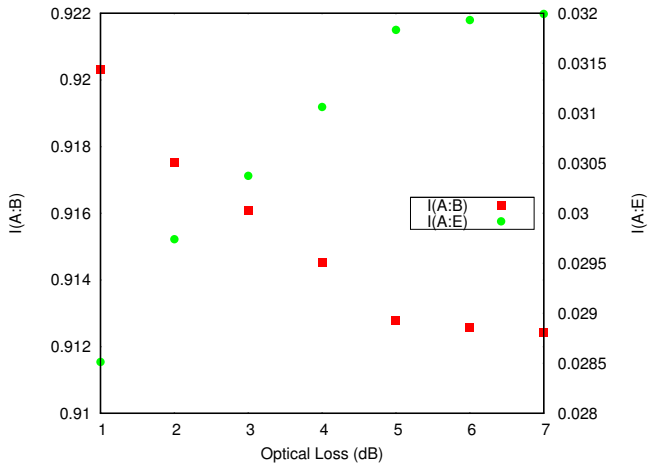

Figure 7.4: The Shannon mutual information between Alice and Bob $I(A : B)$ and between Alice and Eve $I(A : E)$ against optical loss. The mutual information are evaluated by using the formalism in Ref [2].

Chapter 8

QKD in d-dimensions

8.1 Introduction

In this chapter, we present an experimental study of higher-dimensional QKD protocol based on mutually unbiased bases (MUBs), implemented by means of photons carrying orbital angular momentum (OAM). We perform (d+1) mutually unbiased measurements in a classical P&M scheme and on a pair of entangled photons for dimensions ranging from $d = 2$ to 5. In our analysis, we pay attention to the detection efficiency and photon pair creation probability. As security measures, we determine from experimental data the average error rate, the mutual information shared between the sender and receiver and the secret key generation rate per photon. We demonstrate that increasing the dimension leads to an increased information capacity as well as higher key generation rates per photon up to a dimension of $d = 4$. This chapter is based on the manuscripts **M1** & **M10**.

8.2 Theory of MUB protocols

Generally, QKD protocols in higher dimensions primarily follow the same arguments of the standard qubit based protocols. In particular, it has been found that MUBs [154, 155, 156] for high-dimensional OAM states of photons can be used to encode bits of information in the same way as in the BB84-based schemes [157, 158, 159, 160]. MUBs have found other applications in quantum state tomography [156, 161, 162, 163], quantum entanglement [164] and quantum error-correction codes [165, 166] and also appear useful in QKD protocols. The MUBs in QKD protocols offer greatest advantage in the sense that encoding in the mutually unbiased bases of OAM states leads to higher key generation rates thus providing increased security against an eavesdropper [167]. Therefore, in the same spirit we propose and experimentally demonstrate a QKD scheme that makes use of d MUBs for higher dimensional OAM states.

The simplest example of MUBs of dimension $d = 2$ are the horizontal or vertical, diag-

onal or anti-diagonal, and left- or right-handed polarization bases as they are unbiased with respect to each other, forming a set of three MUBs. Although MUBs offer security against eavesdropping, encoding states in the polarization degree of freedom only allows a maximum of one bit of information transmitted per photon which results in a limited key generation rate. Since systems with higher-dimensional Hilbert space can store more information per carrier, the question arises whether QKD protocols using higher-dimensional MUBs also result in higher generation rates of secure key bits; indeed, such protocols can be expected to be more robust in terms of abstract noise measures [132, 168]. Their actual performance in terms of secure key rate however, depends on whether the amount of noise in higher-dimensional implementations grows faster with increasing dimension than their robustness against noise. This Chapter addresses this question for implementations using the OAM of photons. Beams that carry OAM have an azimuthal angular dependence of $\exp(i\ell\theta)$ [169] where ℓ is the azimuthal index and θ is the azimuthal angle. It has been shown theoretically that MUBs for higher-dimensional OAM states can be used to encode bits of information in alignment with the BB84 protocol [157, 158, 159, 160]. A standard P&M implementation of a generalized BB84 protocol, relying on 11 OAM states and superpositions of these 11 OAM states, has previously been performed [170], using 2 of the 12 available MUBs.

In this Chapter, we experimentally investigate an EB scheme for QKD encoded in complete sets of higher-dimensional MUBs, which we first verify with a classically simulated P&M scheme. Although we only focus on the quantum phase of the protocol and do not execute the classical communication channel, we show that the quantum phase is good enough such that one can execute the whole protocol. We implement our protocol with MUBs encoded in OAM states and present values for the corresponding average error rates, classical Shannon information and secret key rates. As with all OAM protocols, our QKD protocol uses filter measurements that project onto one MUB element at a time; we provide the connection between these protocols to the established theory for protocols using full MUB measurements. To achieve this, we prove that the detection efficiency depends only on the basis choice and not on the elements within a basis, otherwise the security parameters of the protocol cannot be evaluated. This allows us to map our protocol to the key rates, thus arriving at the standard MUB protocol. By increasing the dimension d, we obtain an increase in the secret key rate which has been theoretically observed in recent papers [132, 168], resulting in higher key generation rates for dimension $d = 4$. Similarly the Shannon mutual information increases, demonstrating an improvement in the information capacity.

8.3 Mutually unbiased bases

Two orthonormal bases $\mathcal{M}_1 = \{|\phi_{(1,i)}\rangle, i = 0, 1, \cdots, d-1\}$ and $\mathcal{M}_2 = \{|\phi_{(2,j)}\rangle, j = 0, 1, \cdots, d-1\}$ of a d-dimensional Hilbert space $\mathcal{H}_d$ are said to be mutually unbiased if, and only if, all pairs of basis vectors $|\phi_{(1,i)}\rangle$ and $|\phi_{(2,j)}\rangle$ satisfy

$$|\langle\phi_{(1,i)}|\phi_{(2,j)}\rangle|^2 = \frac{1}{d}. \tag{8.3.1}$$

Physically, this means that for a system prepared in the basis $\mathcal{M}_1$ and measured with respect to basis $\mathcal{M}_2$, all outcomes are equally probable. This property of mutually unbiased bases makes them important for QKD protocols.

Mutually unbiased bases were introduced by Schwinger [154] in 1960 as optimum incompatible measurement bases. In 1981, Ivonovic showed their application in quantum state discrimination [155]. Later Wootters and Fields [156] gave a constructive proof that there exist complete sets of MUBs for prime power dimensions and proved that for any dimension d there are not more than $d+1$ MUBs within any particular set of MUBs.

The smallest prime dimension is 2, and for that an example of a complete set of MUBs consists of the eigenstates of the three Pauli spin operators $\sigma_z, \sigma_x, \sigma_y$, i.e.,

$$\{|0\rangle, |1\rangle\}; \tag{8.3.2}$$

$$\left\{\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right), \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)\right\}; \tag{8.3.3}$$

$$\left\{\frac{1}{\sqrt{2}}\left(|0\rangle + i|1\rangle\right), \frac{1}{\sqrt{2}}\left(|0\rangle - i|1\rangle\right)\right\}. \tag{8.3.4}$$

Pauli operators can be generalized to higher dimension, known as the Weyl operators. These are unitary operators of the form $X^k Z^l$ for $k, l \in \{0, 1, \cdots, d-1\}$. The operator Z is diagonal in the standard basis $\{|0\rangle, |1\rangle, \cdots, |d-1\rangle\}$:

$$Z = \sum_{i=0}^{d-1} \omega^i |i\rangle\langle i|, \tag{8.3.5}$$

with $\omega = \exp(i2\pi/d)$ whereas, the operator X reads:

$$X = \sum_{i=0}^{d-1} |i+1 \bmod d\rangle\langle i|. \tag{8.3.6}$$

The eigenbases belonging to the different operators in the set $\{Z, XZ^l | l \in \{0, 1, \cdots, d-1\}\}$ form a complete set of MUBs for any prime number d as the dimension of the underlying Hilbert space. For $d = 2$, the operator X is identical with the Pauli operator σ_x and the operator Z is given by the Pauli operator σ_z.

In the present study of MUB based QKD a complete set of MUBs is implemented following the recipe above by means of photons carrying OAM. The MUBs are obtained by assuming that the standard basis (eigenbasis of the operator Z) is realized by single-photon states which correspond to an elementary excitation of Laguerre-Gauss modes (LG_ℓ) carrying OAM value $l\hbar$. For $d = 2$ we employ the LG_ℓ modes with $\ell = \pm 1$ to generate the standard basis.

For $d = 3$, our choice of the standard basis corresponds to LG_ℓ modes with OAM values $\ell = -1,\ 0,\ 1$:

$$\left\{|-1\rangle \equiv \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, |0\rangle \equiv \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, |1\rangle \equiv \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}\right\}; \tag{8.3.7}$$

The remaining three bases are given in matrix notation with respect to the standard basis as:

$$\frac{1}{\sqrt{3}}\begin{pmatrix}1 & 1 & 1\\ 1 & \omega & \omega^2\\ 1 & \omega^2 & \omega\end{pmatrix}, \frac{1}{\sqrt{3}}\begin{pmatrix}1 & 1 & \omega\\ 1 & \omega & 1\\ \omega & 1 & 1\end{pmatrix}, \frac{1}{\sqrt{3}}\begin{pmatrix}1 & 1 & \omega^2\\ 1 & \omega^2 & 1\\ \omega^2 & 1 & 1\end{pmatrix}. \tag{8.3.8}$$

Here each matrix represents a complete orthonormal basis with its columns reflecting the basis vectors. In general, for prime dimension d, the standard basis consists of d LG_ℓ modes, while the remaining d bases pertain to superpositions of the LG_ℓ modes. Examples of the LG_ℓ modes and their superpositions are given in Fig. (8.1), which contains images of the measurement holograms and their corresponding intensity profiles.

8.4 Filter based MUB QKD protocol

We will now describe how our QKD protocol which is based on filter measurements operates. In both scenarios, Alice (SLM A) prepares her mode in a state chosen randomly from one of the $(d+1)$ bases, while Bob (SLM B) performs a measurement on his mode by randomly selecting a state in one of the $(d+1)$ bases chosen out of $(d+1)^2$ different basis settings but biased towards one basis. Each party then announces from which basis the filter measurement was chosen (sifting) and keeps measurements if they all arrived in the same basis. They later make announcements as to whether photon coincidences occurred (post-selection).

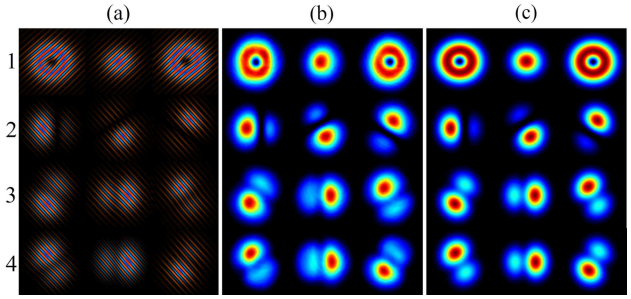

Figure 8.1: The states for each of the 4 MUBs for $d = 3$. The images on the left represent the measurement filters (or holograms) for each of the 12 states. The images in the middle and on the right contain the corresponding experimentally produced and theoretically calculated intensity profiles of the LG_ℓ modes produced by each hologram [**M1**].

A coincidence event represents a conclusive result, otherwise it becomes inconclusive. This is followed by parameter estimation (error rate in the remaining data), error correction and privacy amplification. The announcement step allows our filter measurement based QKD protocol to be mapped back to the original protocol which uses full MUB measurements.

In standard EB QKD protocols both parties perform measurements on the states that they receive, followed by a public announcement of their measurement basis. The two

parties then compare a small portion of their measurements in order to obtain an estimate of the average error rate. This quantifies the error in the QKD protocol resulting from all sources of noise, such as noise in the transmission channel and errors in the measurements. Moreover, the noise could also be caused by an eavesdropper. The error rate refers to the probability that Alice sends the state $|\phi_{(\beta,k)}\rangle$, while Bob receives an orthogonal state $|\phi_{(\beta,k')}\rangle$. Given the MUB β, the corresponding average error rate in each basis Q^β, is expressed as

$$Q^\beta = \sum_{\substack{k,k' \\ k' \neq k}} \mathrm{tr}\left[|\phi^*_{(\beta,k)}\rangle\langle\phi^*_{(\beta,k)}| \otimes |\phi_{(\beta,k')}\rangle\langle\phi_{(\beta,k')}|\rho_{AB}\right]. \tag{8.4.1}$$

The total average error rate is the total error obtained as an average over the different MUBs, $\mathcal{L}$ [168] and is defined as

$$Q = \frac{1}{\mathcal{L}} \sum_{\beta \in \mathcal{L}} Q^\beta. \tag{8.4.2}$$

We use the full set of available MUBs, therefore $\mathcal{L} = d + 1$.

The resulting key rate for this protocol is given as [132, 168]

$$r_{\min} = \log_2 d + \frac{d+1}{d} Q \log_2 \left(\frac{Q}{d(d-1)}\right) + \left(1 - \frac{d+1}{d} Q\right) \log_2 \left(1 - \frac{d+1}{d} Q\right), \tag{8.4.3}$$

The limit on the tolerable error rate that is safe for secret key generation can be improved by implementing a full set of $(d+1)$ MUBs [168, 160]. Using a full set of MUBs results in an increase in the tolerable error rate in which we can still extract a reasonable secret key without compromising the security of the protocol. However, this happens at the cost of reducing the transmission rate which is proportional to the probability $1/(d+1)$ that Alice and Bob choose the same basis. But in our protocol, this is not a problem since we make use of the asymmetric [171] basis choice, so one does not pay the high cost of sifting with MUBs. In order to calculate the maximum tolerable error rate, $Q_{\max}$, the secret key rate, $r_{\min}$, is set to zero.

8.5 Experimental Setup

Our EB QKD protocol was implemented at the single photon level on entangled photon pairs depicted in Fig. 8.2. A collimated 350 mW UV laser (Vanguard 355-2500) was directed to pump a 3 mm-thick type-I BBO crystal, producing collinear frequency-degenerate entangled photon pairs at 710 nm. A beam-splitter was used to separate the collinear signal and idler photons (depicted by arms A and B) which were directed and imaged (2×) from the plane of the crystal onto spatial light modulators (SLMs) by a 4-f telescope. The SLMs were used to execute the filter measurements and were encoded to manipulate both the phase and amplitude of the incident light [172, 173, 174, 175], allowing only one particular superposition of the LG modes to be detected by the detector, while all the others are blocked. False colour images of the types of filters (or holograms) encoded on the SLMs are presented in Fig. 8.1. The projected mode

obtained at the plane of the SLM, be it either Gaussian or non-Gaussian, depending on whether the filter either does or does not match the state of the incident photon, was imaged (0.004×) by a 4-f telescope onto a single-mode fibre. The fibres were connected to avalanche photodiodes which detected the photon pairs via a coincidence counter. The single count rates, S_A and S_B, and the coincidence count rates, C, were recorded simultaneously and accumulated over an integration time of 10 s.

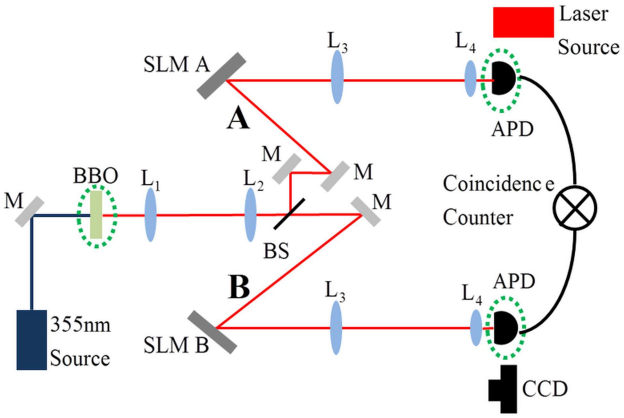

Figure 8.2: The experimental setup used to perform both the EB and P&M QKD protocols. The plane of the crystal was relayed imaged onto SLMs A and B with the use of lenses, L_1 and L_2 ($f_1 = 200$ mm and $f_2 = 400$ mm). Lenses L_3 and L_4 ($f_3 = 500$ mm and $f_4 = 2$ mm) were used to relay image the SLM planes to single-mode fibres [**M1**].

An initial step in conducting our EB QKD protocol, was to test it classically in a P&M based scheme. Our experimental setup for the P&M scheme can be illustrated with the use of Figure 8.2 where the BBO crystal is considered to be reflective and the APD in Arm A is replaced with a laser source and the APD in Arm B with a CCD camera. This procedure is commonly referred to as back-projection or retrodiction [176]. Conducting the protocol in this manner, provided a quicker and simpler method for the verification of the experimental procedure.

8.6 Results and Discussion

By way of example we consider $d = 3$ in our P&M based protocol. We scanned through all possible states, defined by Equations (8.3.7) and (8.3.8) and depicted in Figure 8.1, on SLM A and SLM B. Figure 8.3 (a) contains the cross-sectional intensity profiles recorded on the CCD (depicted in Figure 8.2) when SLM A and SLM B scanned through the states pertaining to the first basis. It is evident that when SLM A and SLM B select the same (different) states, a Gaussian mode (singularity) appears on axis. The normalized on-axis intensities are depicted in Figure 8.3 (b) for the permutation of all the bases elements for $d = 3$. We note that the diagonal elements are equal to $1/3$ ($1/d$) and the elements corresponding to different bases are found to be $1/9$ ($1/d^2$). This validates the implementation of the filters (holograms) and their normalization. Our approach in

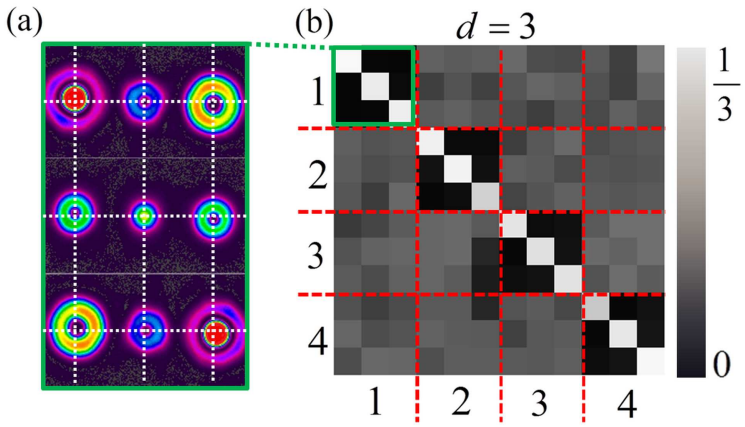

Figure 8.3: (a) Cross-sectional intensity profiles of the field recorded on the CCD for permutations of the first basis's states encoded on SLM A and SLM B. White cross-hairs mark the axis of propagation. (b) The normalized intensity recorded at the CCD when SLM A (Alice) and SLM B (Bob) select one of the three states from one of the 4 bases [**M1**].

obtaining the normalized joint probabilities is outlined in the Appendix F.

Following the successful implementation of the P&M scheme, we proceeded to the EB scheme. For each permutation of the projective measurements by Alice and Bob in the EB scheme, the single count rates and coincidence count rates were recorded and the normalized joint probabilities calculated for $d = 2, 3, 4$ and 5 are given in Figure 8.4. In studying the data in Figure 8.4, it is evident that when the filter settings are the same, anti-correlations in all the bases are observed (denoted by the white diagonal elements). In performing the projective measurements, completely orthogonal filter settings result in no correlations (an inconclusive measurement), while the overlap between the remaining filter settings is given as the inverse of the dimension (i.e., $1/d$).

Based on the results from the normalized joint probabilities, we calculated the average error rate Q according to Equation (8.4.2). We find that for $d = 2$, 3, 4 and 5, the average error rate, $Q = 0.016$, 0.040, 0.088, and 0.14, respectively. By using these values of Q together with Equation (8.4.3) we calculate the secret key rate to be $r_{\min} = 0.7590$, 1.123, 1.139 and 0.8606 for $d = 2$, 3, 4 and 5, respectively. Figure 8.5 contains the measured secret key rates plotted as a function of the measured average error rates for dimensions $d = 2$, 3, 4 and 5, denoted by the data points. The curves denote the theoretical secret key rate as a function of the average error rate, plotted with the use of Equation (8.4.3). For each dimension, d, the intersection between the dashed curves and the horizontal axis (i.e., where $r_{\min} = 0$) corresponds to the maximum permissible error rate ($Q_{\max}$) in order to enable the secure distribution of a secret key. Ideally, we want to minimize the error rate Q in order to maximize the secret key rate $r_{\min}$.

The Shannon information for $d = 2$, 3, 4 and 5 is calculated to be $I(A : B) = 0.9999$, 1.313, 1.478 and 1.487, respectively (depicted by the green data points in Figure 8.7), while the Shannon mutual information increases monotonically, it seems to level off for $d = 4$ and 5. On the other hand $r_{\min}$ first increases and then decreases for $d = 5$. This means that we have reached a finite limit on the dimension in which the protocol

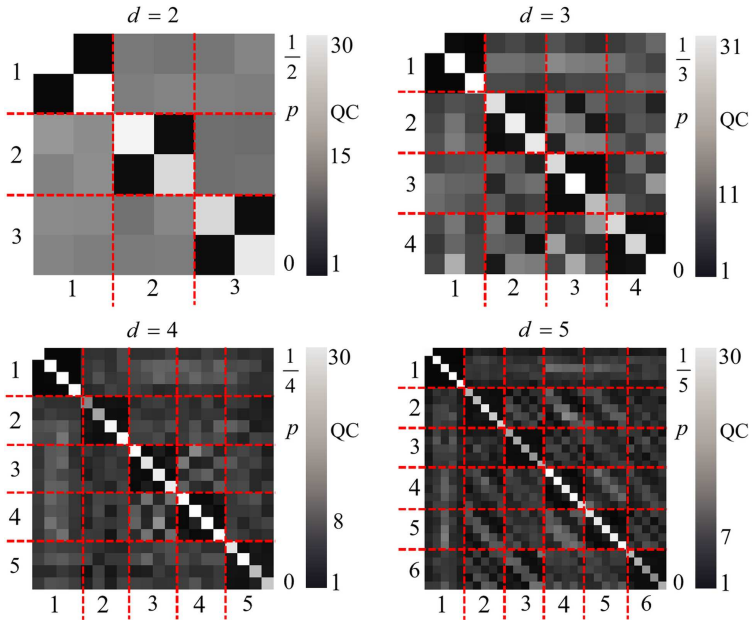

Figure 8.4: The normalized joint probabilities when SLM A (Alice) and SLM B (Bob) select one of the d states from one of the $d+1$ bases for the EB scheme [**M1**].

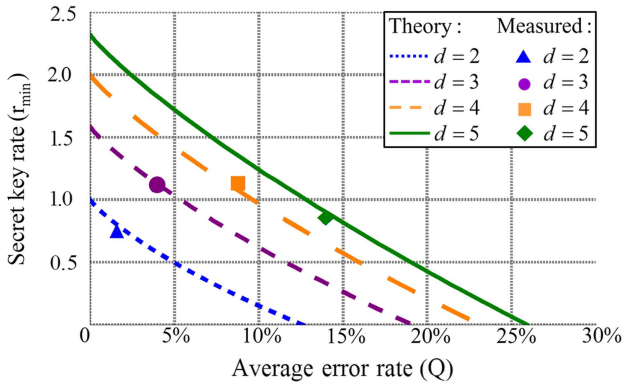

Figure 8.5: The secret key rate, $r_{\min}$, as a function of the average error rate, Q, for different dimensions. The solid data points denote the measured values and the dashed curves the theoretical values calculated from Equation (8.4.3) [**M1**].

can encode, while still resulting in higher generation rates per photon. The difference between these two quantities ($I(A:B)$ and $r_{\min}$) is the mutual information between Alice and Eve, in other words the information that is shared between Alice and Eve (denoted by the red lines in Figure 8.7). From our results it is evident that the noise (attributed to a disturbance by Eve) grows faster than the correlations between Alice and Bob that can be used to generate a key. As this is not expected theoretically, this may be due to the complexity associated with encoding higher-dimensional states holographically on pixelated, finite resolution, spatial light modulators. Our detection efficiency is low because our filter measurements are based on intensity masking and serve as a proof-of-principle experiment.

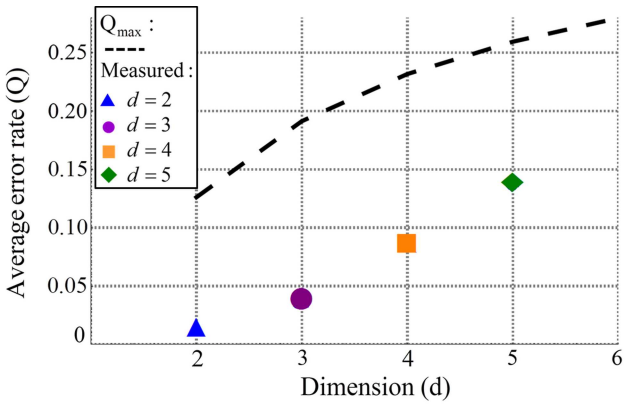

Figure 8.6: The measured average error rate (Q) and the maximum permissible error rate ($Q_{\max}$) evaluated when $r_{\min} = 0$ [**M1**].

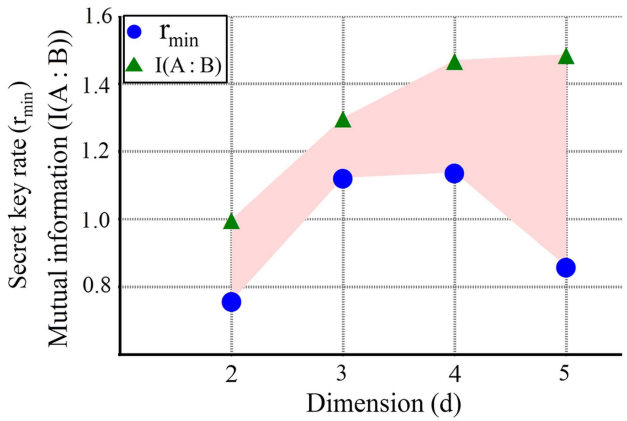

Figure 8.7: The Shannon mutual information I(A:B) *(green)* and the secret key rate $r_{\min}$ *(blue)* plotted as a function of the dimension [**M1**].

8.7 Conclusion

In this work, we have realized a P&M and an EB QKD protocol for $d = 2$ to 5 MUB measurements encoded in the OAM degree of freedom. We show that our protocol which is based on filter measurements can be mapped back into the original MUB protocol which uses full measurements. In particular, we verify our claim that detection efficiency depends on a basis choice and not on the element within a basis, an important consideration for the protocol to work. We provide the proof of the claim in Appendix F. We show this explicitly for $d = 2$ and attest to the fact that this dependency holds for all dimensions. We infer from our measurements the average error rate, mutual information and secret key generation rate per photon for each dimension. We observe that encoding in higher-dimensional MUBs, leads to an increase in the encoding density per photon and increased key generation rates per photon.

Chapter 9

Conclusion

It is the objective of this thesis to review the tools used for quantifying information in quantum communication and to derive security bounds for the B92 protocol in the finite length analysis and also the bounds for a high dimensional protocol. We studied various security methods used for proving the security of QKD protocols. From the tools which we reviewed, we have shown how one can derive security bounds for various QKD protocols. Although QKD protocols appear to be simple, proving their security is not a trivial task.

In particular, we have shown that there exists a connection between the Tsallis entropy and the quantum uncertainty relations in Ref **M9**. Previously, the Shannon entropy and the Rènyi entropies have been used to express such a relationship. This shows the possibility of using the Tsallis entropies in the security of QKD protocols. This is based on their connection to the Shannon entropy and their generalizations to uncertainty relations regardless of their non-additivity property. The question of whether the Tsallis entropies provide better security bounds as compared to the Shannon and Rènyi entropies remains work for the future research.

In **M2**, we have derived the security bounds for the B92 QKD protocol for finite resources by using the Rènyi entropies and uncertainty relations. This shows further the applicability and power of Rènyi entropies together with the elegant method of uncertainty relations in providing security bounds for QKD protocols. Our results show that a minimum of $10^4 - 10^6$ signals are required in order to extract a reasonable secret key. We highlight that these results have also been shown in various finite-length key analysis papers.

Furthermore in **M3** & **M6**, we have shown the possibility of the implementation and security analysis of the B92 protocol by using the id3100 Clavis^2 system at our laboratory. We highlight that this system has traditionally been used for the implementation of the BB84 and SARG04 protocols. We exploited the commercial success and ease of deployment of these "Plug and Play" systems. Such an implementation is that the B92 protocol requires less resources when compared to the other two protocols. Moreover, we demonstrated that with our set-up we can achieve reasonable key rates which scale similarly as in the BB84 protocol and send them over a distance of about 80km.

This shows that one can implement the B92 QKD protocol by using the id3100 Clavis^2 system. Such kind of an implementation offers a great advantage in the sense that it requires less resources.

Finally, in **M1** & **M10**, we have shown an implementation and the security analysis of a high dimensional filter based QKD protocol by using MUBs implemented by OAM states. We show that up to $d = 5$, we can achieve higher secret key generation rates. We also give values of the average error rate and mutual information as our security measures. In particular, we have shown that by encoding in higher dimensional MUBs one can obtain high encoding density per photon which in turn leads to higher key generation rates per photon.

Appendix A

Proof of the Schmidt decomposition

In this section we show the Schmidt decomposition for a tensor product of finite Hilbert spaces. We consider an arbitrary pure-state $|\psi\rangle_{AB}$. Let $\{|r_A\rangle\}$ be an orthonormal basis in $\mathcal{H}_A$ and $\{|\alpha_B\rangle\}$ be an orthonormal basis in $\mathcal{H}_B$, and then we can write

$$|\psi\rangle_{AB} = \sum_{r=1}^{d_A}\sum_{\alpha=1}^{d_B} a_{r\alpha}|r_\alpha\rangle \otimes |\alpha_\beta\rangle, \tag{A.0.1}$$

where the coefficients $a_{r\alpha}$ can be considered to be the elements of a $d_A \otimes d_B$ matrix A. The matrix formed by the coefficients $a_{r\alpha}$ can be written as

$$[A]_{r,\alpha} = a_{r,\alpha}. \tag{A.0.2}$$

This matrix admits a singular value decomposition of the form $A = U \wedge V$ where U is a $d_A \times d_A$ unitary matrix, V is a $d_B \times d_B$ unitary matrix and $\wedge$ is a diagonal $d_A \times d_B$ matrix with non-negative entries with elements $d_{j\beta} = \delta_{j\beta} d_{jj}$. If we denote the matrix of U and V by u_{rj} and $v_{\beta\alpha}$, we have

$$a_{r\alpha} = \sum_{j=1}^{d_A}\sum_{\beta=1}^{d_B} u_{rj} v_{\beta\alpha}. \tag{A.0.3}$$

By substitution in the Equation (A.0.1), we get

$$\begin{aligned} |\psi_{AB}\rangle &= \sum_{j=1}^{d_A}\sum_{\beta=1}^{d_B} d_{j\beta} \sum_{r=1}^{d_A} u_{rj}|r_A\rangle \otimes \sum_{\alpha=1}^{d_B} v_{\beta\alpha}|\alpha_\beta\rangle \\ &= \sum_{j=1}^{d_A}\sum_{\beta=1}^{d_B} \delta_{j\beta} d_{jj} \sum_{r=1}^{d_A} |r_A\rangle \otimes \sum_{\alpha=1}^{d_B} v_{\beta\alpha}|\alpha_\beta\rangle \\ &= \sum_{j=1}^{\min(d_A,d_B)} \lambda_j |j_A\rangle|j_B\rangle, \end{aligned} \tag{A.0.4}$$

where we defined the orthonormal basis on the A system as $|j_A\rangle = \sum_{r=1}^{d_A} u_{rj}|r_A\rangle$ and similarly we define the orthonormal basis on the B system as $|j_B\rangle = \sum_{\alpha=1}^{d_B} v_{j\alpha}|\alpha_\beta\rangle$ and also $\lambda = d_{jj}$.

Appendix B

Proof of the Rényi entropy as $\alpha \mapsto 1$

The Rényi entropy of the sample at $\alpha = 1$ is undefined. Therefore, we apply the L'Hospitals rule in order to evaluate the limit

$$\lim_{\alpha \mapsto a} \frac{f(q)}{g(q)} = \lim_{\alpha \mapsto a} \frac{f'(q)}{g'(q)}, \tag{B.0.1}$$

where in this case $a = 1$. Consider a sample of probabilities p_i, such that $\sum_{i=1}^{N} p_i = 1$ and by substitution, we write $f(q) = \ln \sum_{i=1}^{N} p_i^{\alpha}$ and $g(q) = 1 - \alpha$. On differentiation, we have $\frac{\partial}{\partial q} g(q) = -1$, and by applying the chain rule

$$\begin{aligned} \frac{\partial}{\partial q} f(q) &= \frac{1}{\sum_{i=1}^{N} p_i^{\alpha}} \sum_{i=1}^{N} \frac{\partial}{\partial q} p_i^{\alpha} \\ &= \frac{1}{\sum_{i=1}^{N} p_i^{\alpha}} \sum_{i=1}^{N} p_i^{\alpha} \ln p_i. \end{aligned} \tag{B.0.2}$$

In the case when $\alpha \mapsto 1$ we have

$$\frac{\partial}{\partial q} f(q) = \frac{1}{\sum_{i=1}^{N} p_i^{a}} \sum_{i=1}^{N} p_i \ln p_i. \tag{B.0.3}$$

The probabilities p_i, sum to unity hence

$$\lim_{\alpha \mapsto 1} \ln \sum_{i=1}^{N} p_i^{\alpha} = -\sum_{i=1}^{N} p_i \ln p_i, \tag{B.0.4}$$

which gives the Shannon entropy.

The Rényi entropy is a decreasing function of the parameter α depicted as

$$(1-\alpha)^2 (\sum p(i)^{\alpha}) \frac{\partial s^{\alpha}}{\partial \alpha} = f(\sum p(i)^{\alpha}) + (1-\alpha) \sum p(i)^{\alpha} \ln p(i), \tag{B.0.5}$$

with $f(x) = x \ln x$. The function $f(x)$ is convex hence

$$\begin{aligned} f(\sum p(i)^{\alpha}) &\leq \sum p(i) f(p(i)^{\alpha-1}) \\ &= \sum p(i)^{\alpha} \ln p(i)^{\alpha-1} \\ &= (\alpha - 1) \sum p(i)^{\alpha} \ln p(i). \end{aligned} \tag{B.0.6}$$

The Rényi entropy can also be expressed by conditioning between the random variables X and Y. This can be written as a chain rule $H_{\alpha}(Y|X) = H_{\alpha}(X,Y) - H_{\alpha}(X)$. Again, from this definition it can be shown that the conditional Rényi entropy reduces to the conditional Shannon entropy as $\alpha \to 1$.

B.1 Proof of additivity of the Rényi entropy

If $p(i,j) = p_A(i) p_B(j)$ then we can write

$$\begin{aligned} H_{\alpha}(p) &= \frac{1}{1-\alpha} \ln \left(\sum_{i,j} p(i,j)^{\alpha} \right) \\ &= \frac{1}{1-\alpha} \ln \left(\sum_{i} p_A(i)^{\alpha} \right) \left(\sum_{j} p_B(j)^{\alpha} \right) \\ &= \frac{1}{1-\alpha} \ln \left(\sum_{i} p_A(i)^{\alpha} \right) + \frac{1}{1-\alpha} \ln \left(\sum_{j} p_B(j)^{\alpha} \right) \\ &= H_{\alpha}(p_A) + H_{\alpha}(p_B), \end{aligned} \tag{B.1.1}$$

which completes the proof.

Appendix C

Proof of the non negativity of the Relative entropy

In order to prove that $D(p||q) \geq 0$, we recall the definition of the relative entropy

$$\begin{aligned} D(p||q) &= \sum_{x\in\mathcal{X}} p(x) \log \frac{p(x)}{q(x)} \\ &= -\frac{1}{\ln 2} \sum_{x} p(x) \ln \frac{q(x)}{p(x)} \\ &\geq -\frac{1}{\ln 2} \sum_{x} p(x) \left(\frac{q(x)}{p(x)} - 1 \right). \end{aligned} \tag{C.0.1}$$

We have used the inequality $\ln x \leq x - 1$ which is a convexity of the ln function. Then, by using the fact that $p(x)$ and $q(x)$ sum to one, we get $D(p||q) \geq 0$. The equality property is achieved if and only if for all x,

$$\ln \frac{q(x)}{p(x)} = \frac{q(x)}{p(x)} - 1, \tag{C.0.2}$$

which is equivalent to $p(x) = q(x)$ for all x.

Appendix D

Proof of the Heisenberg uncertainty principle

If two Hermitian operators represent physical observables are denoted by A and B in an N-dimensional Hilbert space, their corresponding set of normalized eigenvectors can be written as $\{|a_i\rangle\}$ and $\{|b_i\rangle\}$ with $i = 1, ..., N$ [60]. Then according to the Uncertainty principle, it is impossible for any quantum state $|\psi\rangle$ with probability distributions $p_i = (p_1, ..., p_N)$ and $q = (q_1, ..., q_N)$ which are defined as [60, 89]

$$\begin{aligned} p_i &= |\langle a_i|\psi\rangle|^2 \\ q_i &= |\langle b_i|\psi\rangle|^2, \end{aligned} \tag{D.0.1}$$

to be measured accurately except with limited precision provided that A and B are sufficiently non-commuting. Robertson formulated the uncertainty relations according to the inequality

$$\triangle A_p \triangle B_p \geq \frac{1}{2}\mathrm{tr}(\rho[\hat{A}, \hat{B}]), \tag{D.0.2}$$

where $\triangle A_p$ and $\triangle B_p$ represent the standard deviation of the outcomes of the corresponding observables which can be expressed as

$$\begin{aligned} (\triangle A_p)^2 &= \langle A^2\rangle_p - (\langle A\rangle_p)^2 \\ (\triangle B_p)^2 &= \langle B^2\rangle_p - (\langle B\rangle_p)^2, \end{aligned} \tag{D.0.3}$$

and $[\hat{A}, \hat{B}]$ represents the commutator, $[\hat{A}, \hat{B}] \equiv \hat{A}\hat{B} - \hat{B}\hat{A}$ or the incompatibility of the two operators $\hat{A}$ and $\hat{B}$. Therefore, in order to prove the Heisenberg uncertainty principle let

$$|\phi\rangle := (A + i\gamma B)|\psi\rangle, \tag{D.0.4}$$

where γ is a real parameter. By substitution we obtain

$$\begin{aligned} \langle\phi|\phi\rangle &= \langle\psi|(A + i\gamma B)^\dagger(A + i\gamma B)|\psi\rangle \\ &= \langle\psi|(A^\dagger - i\gamma B^\dagger)(A + i\gamma B)|\psi\rangle \\ &= \langle\psi|A^\dagger A|\psi\rangle + i\gamma\langle\psi|(A^\dagger B - B^\dagger A)|\psi\rangle + \langle\psi|B^\dagger B|\psi\rangle \\ &\equiv \langle\psi|A^2|\psi\rangle + i\gamma\langle\psi|[A, B]|\psi\rangle + \gamma^2\langle\psi|B^2|\psi\rangle \\ &\geq 0. \end{aligned} \tag{D.0.5}$$

The commutator definition has been used and also the fact that the observables A and B are Hermitian. For any observable $X = A, B$ and state $|\psi\rangle$ we have $\langle\psi|X^2|\psi\rangle$ (if $X = X^\dagger$) as shown

$$\begin{aligned}\langle\psi|X^2|\psi\rangle &= \left(\sum_i \bar{\xi}_i\langle\gamma_i|\right) XX \left(\sum_j \xi|\gamma_j\rangle\right) \\ &= \sum_i\sum_j \bar{\xi}_i\xi_j\gamma_i\gamma_j\delta_{ij} \\ &= \sum_i {\gamma_i}^2|\xi_i|^2 \\ &\geq 0. \end{aligned} \tag{D.0.6}$$

This means that $i\langle\psi|[A,B]|\psi\rangle$ must be real and should be equal to $\pm|\langle\psi|[A,B]|\psi\rangle|$. The equation above (3rd from last) is of a polynomial form which corresponds to a discriminant $\delta = b^2 - 4ac$ so that we have

$$\begin{aligned}\delta &= |\langle\psi|[A,B]|\psi\rangle|^2 - 4\langle\psi|A^2|\psi\rangle\langle\psi|B^2|\psi\rangle \\ &\leq 0. \end{aligned} \tag{D.0.7}$$

We use this result in the equality of form

$$\begin{aligned}\langle\psi|A^2|\psi\rangle\langle\psi|B^2|\psi\rangle &\equiv \langle A^2\rangle\langle B^2\rangle \\ &\geq \frac{1}{4}|\langle\psi|[A,B]|\psi\rangle|^2. \end{aligned} \tag{D.0.8}$$

For the observables A, B we define new observables $\tilde{A}, \tilde{B}$ according to

$$A = \tilde{A} - \langle\psi|\tilde{A}|\psi\rangle \equiv \tilde{A} - \langle\tilde{A}\rangle$$

$$B = \tilde{B} - \langle\psi|\tilde{B}|\psi\rangle \equiv \tilde{B} - \langle\tilde{B}\rangle.$$

By substituting these set of equations in the previous equation we arrive at

$$\langle A^2\rangle\langle B^2\rangle = \langle(\tilde{A} - \langle\tilde{A}\rangle)^2\langle(\tilde{B} - \langle\tilde{B}\rangle)^2, \tag{D.0.9}$$

which can also be written as

$$\triangle\tilde{A}^2\triangle\tilde{B}^2 \geq \frac{1}{4}|\langle\psi|\tilde{A},\tilde{B}|\psi\rangle|^2, \tag{D.0.10}$$

and this can be expressed as

$$\triangle\tilde{A}\triangle\tilde{B} \geq \frac{1}{2}|\langle\psi|\tilde{A},\tilde{B}|\psi\rangle|. \tag{D.0.11}$$

For any operator $X = A, B$, it is found that $\triangle X^2 = \triangle\tilde{X}^2$ thus leading to the Heisenberg's uncertainty relation

$$\triangle A\triangle B \geq \frac{1}{2}|\langle\psi|[A,B]|\psi\rangle|. \tag{D.0.12}$$

Appendix E

Proof of the Tsallis entropy as $\alpha \mapsto 1$

Similar to the Rényi entropy at $\alpha = 1$, the entropy fails and therefore we apply the L'Hospital's Rule

$$\lim_{\alpha \to a} \frac{f(q)}{g(q)} = \lim_{\alpha \to a} \frac{f'(q)}{g'(q)}. \tag{E.0.1}$$

By substitution, $f(q) = \sum_{i=1}^{N} (p_i^{\alpha} - 1)$ and $g(q) = 1 - \alpha$ and taking $a = 1$, then by chain rule we arrive at

$$\frac{\partial}{\partial q} f(q) = \sum_{i=1}^{N} \frac{\partial}{\partial q} p_i^{\alpha}. \tag{E.0.2}$$

We recall that a^x can be differentiated with respect to x as

$$\frac{\partial}{\partial x} a^x = \frac{\partial}{\partial x} e^{x \ln a} \frac{\partial}{\partial x} x \ln a = a^x \ln a. \tag{E.0.3}$$

By following the same trick as in the Rènyi entropy in Section 3.2.5, for the above equation we get

$$\frac{\partial}{\partial x} f(q) = \sum_{i=1}^{N} p_i^{\alpha} \ln p_i, \tag{E.0.4}$$

of which in the limit $\alpha \to 1$, we obtain

$$\frac{\partial}{\partial q} f(q) = \sum_{i=1}^{N} p_i \ln p_i, \tag{E.0.5}$$

then we have

$$\lim_{\alpha \to 1} \frac{1}{1 - \alpha} \left(\sum_{i=1}^{N} p_i^{\alpha} - 1 \right) = - \sum_{i=1}^{N} p_i \ln p_i, \tag{E.0.6}$$

This shows that as $\alpha \mapsto 1$, the Tsallis entropy is equal to the Shannon entropy.

Appendix F

Calculation of detection efficiencies

In this section, we show how to formalize and verify the claim that the detection efficiencies depend only on the bases but are the same for all elements within a basis. We demonstrate the calculation of detection efficiencies by comparing the expected and detected number of clicks for the case of qubit pairs ($d = 2$). For this purpose, we first calculate the expected number of detection events by following the light beam from the laser source to the detection device. Afterwords we relate them to the measured counts. By comparing the single count rates and the coincidence count rates we obtain an expression for the detection efficiency for each basis state.

F.0.1 Photon pair creation and action of the beam splitter

The state of the light exiting the laser source can be represented by a coherent state with complex parameter α which specifies the intensity and phase of the light:

$$|\alpha\rangle = \mathcal{D}(\alpha)|0\rangle = \exp(\alpha b_0^\dagger - \alpha^* b_0)|0\rangle, \tag{F.0.1}$$

where $|0\rangle$ is the vacuum state, b_0 and $b_0^\dagger$ are annihilation and creation operators, respectively, with index referring to OAM value $l = 0$. The operator $\mathcal{D}(\alpha)$ is called a displacement operator. The laser beam pumps a BBO crystal, creating pairs of photons with OAM values $\pm l$ by type I parametric down conversion. This process can be modeled by the following transformation of creation operators

$$b_0^\dagger \to \sum_\ell \sqrt{\chi_\ell} a_\ell^\dagger a_{-\ell}^\dagger, \tag{F.0.2}$$

where χ_ℓ is the creation probability of a photon pair with OAM values $\pm\ell$ and $a_{\pm\ell}^\dagger$ are the corresponding creation operators. After passing through the BBO crystal the light is sent to a $50:50$ beam splitter resulting in the transformation:

$$a_\ell^\dagger \to \frac{1}{\sqrt{2}} \left(a_{\ell,A}^\dagger + a_{\ell,B}^\dagger \right), \tag{F.0.3}$$

where A and B refer to the two beams exiting the beam splitter. Thus, the combined action of the BBO crystal and the beam splitter reads

$$a_0^\dagger \to \sum_{\ell=0}^{\infty} \sqrt{\chi_\ell} \left(\frac{a_{\ell,A}^\dagger + a_{\ell,B}^\dagger}{\sqrt{2}} \right) \left(\frac{a_{-\ell,A}^\dagger + a_{-\ell,B}^\dagger}{\sqrt{2}} \right). \tag{F.0.4}$$

It maps the displacement operator $\mathcal{D}(\alpha)$ to a squeeze operator $\mathcal{S}(\alpha\sqrt{\chi_\ell})$ given by

$$\begin{aligned} \mathcal{S}(\alpha\sqrt{\chi_\ell}) = \exp\Bigg(& \alpha \sum_{\ell=0}^{\infty} \sqrt{\chi_\ell} \left(\frac{a_{\ell,A}^\dagger + a_{\ell,B}^\dagger}{\sqrt{2}} \right) \\ & \times \left(\frac{a_{-\ell,A}^\dagger + a_{-\ell,B}^\dagger}{\sqrt{2}} \right) - \alpha^* \sum_{\ell=0}^{\infty} \sqrt{\chi_\ell} \\ & \times \left(\frac{a_{\ell,A} + a_{\ell,B}}{\sqrt{2}} \right) \left(\frac{a_{-\ell,A} + a_{-\ell,B}}{\sqrt{2}} \right) \Bigg). \end{aligned} \tag{F.0.5}$$

Thus, the initial coherent state is transformed into a (two-mode) squeezed vacuum state: $|\tilde{\alpha}\rangle = \mathcal{S}(\alpha\sqrt{\chi_\ell})|0\rangle$. For small value of $\alpha\sqrt{\chi_\ell}$ the state $|\tilde{\alpha}\rangle$ can be approximated to the first order in $\alpha\sqrt{\chi_\ell}$ as:

$$\begin{aligned} |\tilde{\alpha}\rangle \approx \mathcal{N} \Bigg[& 1 + \alpha \sum_{\ell=0}^{\infty} \sqrt{\chi_\ell} \left(\frac{a_{\ell,A}^\dagger + a_{\ell,B}^\dagger}{\sqrt{2}} \right) \\ & \times \left(\frac{a_{-\ell,A}^\dagger + a_{-\ell,B}^\dagger}{\sqrt{2}} \right) \Bigg] |0\rangle, \end{aligned} \tag{F.0.6}$$

where $\mathcal{N}$ is the normalization constant. The vacuum does not play any role as far as photon detections are concerned, thus, one can ignore the vacuum component. This results in the (unnormalized) state $|\psi\rangle$ which reads:

$$|\psi\rangle = \alpha \sum_{\ell=0}^{\infty} \sqrt{\chi_\ell} \left(\frac{a_{\ell,A}^\dagger + a_{\ell,B}^\dagger}{\sqrt{2}} \right) \left(\frac{a_{-\ell,A}^\dagger + a_{-\ell,B}^\dagger}{\sqrt{2}} \right) |0\rangle, \tag{F.0.7}$$

$$\begin{aligned} = \frac{\alpha}{2} \sum_{\ell=0}^{\infty} \sqrt{\chi_\ell} (& a_{\ell,A}^\dagger a_{-\ell,A}^\dagger + a_{\ell,A}^\dagger a_{-\ell,B}^\dagger \\ & + a_{\ell,B}^\dagger a_{-\ell,A}^\dagger + a_{\ell,B}^\dagger a_{-\ell,B}^\dagger) |0\rangle, \end{aligned} \tag{F.0.8}$$

F.0.2 Measurements

After the BBO crystal and the beam spitter filter measurements projecting onto individual basis modes were carried out independently in both beams A and B. The signal for each basis mode was detected by means of avalanche photodiodes. These detectors respond to incident photons, but do not discriminate between a single photon and multiple photons. However, the probability for a click varies for different photon numbers.

The probability to obtain a click in a filter measurement of mode s can be modeled by the expectation value of the effect P_s defined by

$$P_s = \sum_{n=1}^{\infty} \eta_s^{(n)} |n_s\rangle\langle n_s|, \tag{F.0.9}$$

where $\eta_s^{(n)}$ represents the probability for n photons in mode s to trigger a detector click and reads [177]

$$\begin{aligned} \eta_s^{(n)} &= 1 - (1 - \eta_s^{(1)})^n, \\ &\approx n\eta_s^{(1)} \quad \text{for small} \quad \eta_s^{(1)}. \end{aligned} \tag{F.0.10}$$

Because of photon loss on the path from source to detector and non-ideal detection, only a fraction of the detection events expected under ideal conditions is measured in the experiment. We attribute any loss to non-ideal detection. The probability of coincidence can be calculated as an expectation value of the operator $P_s \otimes P_{s'}$ with respect to the state $|\psi\rangle$ (cp. Eq. (F.0.8)) after the beam splitter.

From Eq. (F.0.8) it is clear that only the single photon components of state $|\psi\rangle$ can yield a click of detector A for OAM value ℓ, leading to a detection probability of

$$p_{\ell,A} = \langle\psi|P_\ell \otimes \mathbb{I}|\psi\rangle = \eta_{\ell,A}^{(1)} |\alpha|^2 \chi_\ell / 2\,. \tag{F.0.11}$$

Similarly, we can calculate the other probabilities as:

$$p_{-\ell,A} = \langle\psi|P_{-\ell} \otimes \mathbb{I}|\psi\rangle = \eta_{-\ell,A}^{(1)} |\alpha|^2 \chi_\ell / 2\,, \tag{F.0.12}$$

$$p_{\ell,B} = \langle\psi|\mathbb{I} \otimes P_\ell|\psi\rangle = \eta_{\ell,B}^{(1)} |\alpha|^2 \chi_\ell / 2\,, \tag{F.0.13}$$

$$p_{-\ell,B} = \langle\psi|\mathbb{I} \otimes P_{-\ell}|\psi\rangle = \eta_{-\ell,B}^{(1)} |\alpha|^2 \chi_\ell / 2\,. \tag{F.0.14}$$

The probability of the coincidence count in detector A with OAM value ℓ and in detector B with OAM value $-\ell$ amounts to

$$p_{\ell,A,-\ell,B} = \langle\psi|P_\ell \otimes P_{-\ell}|\psi\rangle = \eta_{\ell,A}^{(1)} \eta_{-\ell,B}^{(1)} |\alpha|^2 \chi_\ell / 4\,. \tag{F.0.15}$$

For the measured count of clicks $C_{\ell,A}$ in detector A with OAM value ℓ, and the measured count $C_{-\ell,B}$ in detector B with OAM value $-\ell$ we obtain the expressions:

$$C_{\ell,A} = N p_{\ell,A}, \tag{F.0.16}$$

$$C_{-\ell,B} = N p_{-\ell,B}, \tag{F.0.17}$$

$$C_{\ell,A,-\ell,B} = N p_{\ell,A,-\ell,B}, \tag{F.0.18}$$

where N is the number of photon pairs created by consecutive pump pulses during the measurement period. For the coincidence counts $C_{\ell,A,-\ell,B}$ in the last equation it is assumed that photon loss in beam A and beam B are independent. Note that $p_{\ell,A,-\ell,B}/p_{\ell,A} = \eta_{-\ell,B}^{(1)}/2$ and hence one can calculate the efficiencies as:

$$\eta_{-\ell,B}^{(1)} = 2\frac{C_{\ell,A,-\ell,B}}{C_{\ell,A}}, \tag{F.0.19}$$

$$\eta_{\ell,A}^{(1)} = 2\frac{C_{\ell,A,-\ell,B}}{C_{-\ell,B}}. \tag{F.0.20}$$

Basis vectors	Detector A	Detector B
1	0.01504	0.02145
2	0.01517	0.02106
3	0.00536	0.00886
4	0.00503	0.00727
5	0.00508	0.00787
6	0.00556	0.00874

Table F.1: Detection efficiencies for different detectors projecting on different bases vectors. Here the first two vectors belong to the σ_z basis, the following two to the σ_x basis, and the last two to the σ_y basis.

For the SLM-filter setting $(|\ell\rangle \pm |-\ell\rangle)/\sqrt{2}$ which is a superposition of $\pm\ell$ OAM modes, the corresponding creation operators read $a^\dagger_\pm \equiv (a^\dagger_{\ell,A} \pm a^\dagger_{-\ell,A})/\sqrt{2}$. Thus, we can represent $a^\dagger_{\ell,A}$ and $a^\dagger_{-\ell,A}$ in terms of $a^\dagger_\pm$ as:

$$a^\dagger_{\pm\ell} = \frac{a^\dagger_{+,A} \pm a^\dagger_{-,A}}{\sqrt{2}}. \tag{F.0.21}$$

Substituting Eq. (F.0.21) in Eq. (F.0.8) we obtain:

$$\begin{aligned} |\psi\rangle = \frac{\alpha}{4}\sum_{\ell=0}^{\infty}\sqrt{\chi_\ell}\Bigg(&\sqrt{2}\frac{(a^\dagger_{+,A})^2}{\sqrt{2}} - \sqrt{2}\frac{(a^\dagger_{-,A})^2}{\sqrt{2}} \\ &+2a^\dagger_{+,A}a^\dagger_{+,B} - 2a^\dagger_{-,B}a^\dagger_{-,A} \\ &+\sqrt{2}\frac{(a^\dagger_{+,B})^2}{\sqrt{2}} - \sqrt{2}\frac{(a^\dagger_{-,B})^2}{\sqrt{2}}\Bigg)|0\rangle. \end{aligned} \tag{F.0.22}$$

Thus, the probability of a click in detector A for the SLM setting + amounts to $p_{+,A} = \eta^{(1)}_{+,A}|\alpha|^2\chi_\ell/2$ while the coincidence probability for the SLM setting + in the detector A and the detector B reads $p_{+,A,+,B} = \eta^{(1)}_{+,A}\eta^{(1)}_{+,B}|\alpha|^2\chi_\ell/4$. The observed number of clicks are related to the expected detection counts as:

$$C_{+,A} = Np_{+,A}, \tag{F.0.23}$$
$$C_{+,B} = Np_{+,B}, \tag{F.0.24}$$
$$C_{+,A,+,B} = Np_{+,A,+,B}, \tag{F.0.25}$$

Since $p_{+,A,+,B}/p_{+,A} = \eta^{(1)}_{+,B}/2$, if follows for the efficiencies that:

$$\eta^{(1)}_{+,B} = 2\frac{C_{+,A,+,B}}{C_{+,A}}, \tag{F.0.26}$$
$$\eta^{(1)}_{+,A} = 2\frac{C_{+,A,+,B}}{C_{+,B}}. \tag{F.0.27}$$

Similarly for SLM settings $(|\ell\rangle \pm i|-\ell\rangle)/\sqrt{2}$ the state $|\psi\rangle$ can be rewritten as:

$$\begin{aligned}|\psi\rangle = \frac{\alpha}{4}\sum_{\ell=0}^{\infty}\sqrt{\chi_\ell}(\sqrt{2}\frac{(a^\dagger_{+y,A})^2}{\sqrt{2}} + \sqrt{2}\frac{(a^\dagger_{-y,A})^2}{\sqrt{2}} \\ + 2a^\dagger_{+y,A}a^\dagger_{+y,B} + 2a^\dagger_{-y,B}a^\dagger_{-y,A} \\ + \sqrt{2}\frac{(a^\dagger_{+y,B})^2}{\sqrt{2}} + \sqrt{2}\frac{(a^\dagger_{-y,B})^2}{\sqrt{2}})|0\rangle,\end{aligned} \tag{F.0.28}$$

where

$$a^\dagger_{\pm y,A} = \frac{a^\dagger_{\ell,A} \pm i a^\dagger_{-\ell,A}}{\sqrt{2}}. \tag{F.0.29}$$

Thus, the relation for the efficiencies in this filter setting is obtained as:

$$\eta^{(1)}_{+y,B} = 2\frac{C_{+y,A,+y,B}}{C_{+y,A}}, \tag{F.0.30}$$

$$\eta^{(1)}_{+y,A} = 2\frac{C_{+y,A,+y,B}}{C_{+y,B}}. \tag{F.0.31}$$

Using the expressions derived above, we calculated the detection efficiencies for the case of a two-level system for different SLM settings (cp. Table F.1). We found that even though the detection efficiencies vary for different bases, the fluctuation in the values is very small for all the basis vectors within each basis which proves the claim for qubits.

Furthermore, this method can be used to show that the detection efficiencies are independent of the basis vectors within each basis, regardless of the dimension. However, let us point out that the analysis of our measurement data indicated an anomaly for the detection efficiency for the OAM value $\ell = 0$, which is different from the other values of OAM. Although not so important in the present context, this case has to be investigated more carefully when it comes to actual key transmission and will be the subject of future work.

Bibliography

[1] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin. plug and play systems for quantum cryptography. *Applied Physics Letters*, 70:793, 1997.

[2] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden. Quantum key distribution over 67 km with a plug&play system. *New Journal of Physics*, 4:41, 2002.

[3] C. E. Shannon. A Mathematical Theory of Communication. *Bell System Tech. J.*, 27(379):623, 1948.

[4] S. Wiesner. Conjugate Coding. *ACM Sigact News*, 15(1):78–88, 1983.

[5] M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2002.

[6] Werner Heisenberg. Über den anschaulichen inhalt der quantentheoretischen kinematik und mechanik. *Zeitschrift für Physik*, 43(3-4):172–198, 1927.

[7] Paul Busch, Teiko Heinonen, and Pekka Lahti. Heisenberg's uncertainty principle. *Physics Reports*, 452(6):155–176, 2007.

[8] C.H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, volume 175. Bangalore, India, 1984.

[9] Stefan Wolf. Unconditional security in cryptography. In *Lectures on data security*, pages 217–250. Springer, 1999.

[10] D. Mayers. Unconditional Security in Quantum Cryptography. *Journal of the ACM (JACM)*, 48(3):351–406, 2001.

[11] H. Inamori, N. Lütkenhaus, and D. Mayers. Unconditional security of practical quantum key distribution. *The European Physical Journal D-Atomic, Molecular, Optical and Plasma Physics*, 41(3):599–627, 2007.

[12] V. Scarani and R. Renner. Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. *Physical Review Letters*, 100(20):200501, 2008.

[13] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67(6):661–663, 1991.

[14] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 74(1):145–195, Mar 2002.

[15] G. Bennett C. H., Brassard and N. D. Mermin. Quantum Cryptography without Bell's Theorem. *Phy. Rev. A*, 68:558, 1992.

[16] Charles H. Bennett. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, 68:3121–3124, May 1992.

[17] Masato Koashi. Unconditional security of coherent-state quantum key distribution with a strong phase-reference pulse. *Phys. Rev. Lett.*, 93:120501, Sep 2004.

[18] Kiyoshi Tamaki, Norbert Lütkenhaus, Masato Kaoshi, and Jamie Batuwantudawe. Unconditional security of of the bennett 1992 quantum-key-distribution with a strong phase reference pulse. *Physical Review A*, 80.

[19] Dagmar Bruß. Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.*, 81(14):3018–3021, Oct 1998.

[20] Valerio Scarani, Antonio Acín, Grégoire Ribordy, and Nicolas Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.*, 92(5):057901, Feb 2004.

[21] D. Stucki, S. Fasel, N. Gisin, Y. Thoma, and H. Zbinden. Coherent one-way quantum key distribution. In *Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series*, volume 6583, page 18, 2007.

[22] Kyo Inoue, Edo Waks, and Yoshihisa Yamamoto. Differential phase shift quantum key distribution. *Phys. Rev. Lett.*, 89(3):037902, Jun 2002.

[23] 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):1301–1350, Sep 2009.

[24] Nicolas J Cerf and Philippe Grangier. From quantum cloning to quantum key distribution with continuous variables: A review. *JOSA B*, 24(2):324–334, 2007.

[25] Raúl García-Patrón and Nicolas J Cerf. Unconditional optimality of gaussian attacks against continuous-variable quantum key distribution. *Physical review letters*, 97(19):190503, 2006.

[26] Miguel Navascués, Frédéric Grosshans, and Antonio Acín. Optimality of gaussian attacks in continuous variable quantum cryptography. *arXiv preprint quant-ph/0608034*, 2006.

[27] Anthony Leverrier, Frédéric Grosshans, and Philippe Grangier. Finite-size analysis of a continuous-variable quantum key distribution. *Physical Review A*, 81(6):062343, 2010.

[28] http://www.idquantique.com.

[29] http://www.magiqtech.com.

[30] Momtchil Peev, Christoph Pacher, Romain Alléaume, Claudio Barreiro, Jan Bouda, W Boxleitner, Thierry Debuisschert, Eleni Diamanti, M Dianati, JF Dynes, et al. The secoqc quantum key distribution network in vienna. *New Journal of Physics*, 11(7):075001, 2009.

[31] Abdul Mirza and Francesco Petruccione. Realizing long-term quantum cryptography. *JOSA B*, 27(6):A185–A188, 2010.

[32] N Namekata, H Takesue, T Honjo, Y Tokura, and S Inoue. High-rate quantum key distribution over 100 km using ultra-low-noise, 2-ghz sinusoidally gated ingaas/inp avalanche photodiodes. *Optics Express*, 19(11):10632–10639, 2011.

[33] M Sasaki, M Fujiwara, H Ishizuka, W Klaus, K Wakui, M Takeoka, S Miki, T Yamashita, Z Wang, A Tanaka, et al. Field test of quantum key distribution in the tokyo qkd network. *Optics Express*, 19(11):10387–10409, 2011.

[34] D Stucki, M Legré, F Buntschu, B Clausen, N Felber, N Gisin, L Henzen, P Junod, G Litzistorf, P Monbaron, et al. Long-term performance of the swissquantum quantum key distribution network in a field environment. *New Journal of Physics*, 13(12):123001, 2011.

[35] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. Quantum Cryptography. *Reviews of Modern Physics*, 74(1):145–195, 2002.

[36] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Phys. Rev. Lett.*, 94(23):230504, Jun 2005.

[37] V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev. The security of practical quantum key distribution. *Reviews of Modern Physics*, 81(3):1301–1350, 2009.

[38] Renato Renner. Security of quantum key distribution. *International Journal of Quantum Information*, 6(01):1–127, 2008.

[39] Andrew Chi-Chih Yao. Security of quantum protocols against coherent measurements. In *Proceedings of the twenty-seventh annual ACM symposium on Theory of computing*, pages 67–75. ACM, 1995.

[40] Charles H Bennett, Gilles Brassard, Sandu Popescu, Benjamin Schumacher, John A Smolin, and William K Wootters. Purification of noisy entanglement and faithful teleportation via noisy channels. *Physical Review Letters*, 76(5):722, 1996.

[41] Hoi-Kwong Lo and Hoi Fung Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283(5410):2050–2056, 1999.

[42] Peter W Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Physical Review Letters*, 85(2):441–444, 2000.

[43] Eli Biham, Michel Boyer, P Oscar Boykin, Tal Mor, and Vwani Roychowdhury. A proof of the security of quantum key distribution. *Journal of Cryptology*, 19(4):381–439, 2006.

[44] Daniel Gottesman and John Preskill. Secure quantum key distribution using squeezed states. In *Quantum Information with Continuous Variables*, pages 317–356. Springer, 2003.

[45] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim. The universal composable security of quantum key distribution. *Theory of Cryptography: Second Theory of Cryptography Conference, TCC 2005, J.Kilian (ed.) Springer Verlag 2005*, vol.3378 of Lecture Notes in Computer Science, pp. 386-406.

[46] R. Renner and J. I. Cirac. de finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. *Phys. Rev. Lett.*, 102(11):110504, Mar 2009.

[47] M. Christandl, R. König, and R. Renner. Postselection technique for quantum channels with applications to quantum cryptography. *Physical review letters*, 102(2):20504, 2009.

[48] V. Makarov and Norges teknisk-naturvitenskapelige universitet Institutt for elektronikk og telekommunikasjon. *Quantum cryptography and quantum cryptanalysis*. Norwegian University of Science and Technology, Faculty of Information Technology, Mathematics and Electrical Engineering, Department of Electronics and Telecommunications, 2007.

[49] Bruce Schneier. *Applied cryptography: protocols, algorithms, and source code in C*. john wiley & sons, 2007.

[50] Ronald L Rivest, Adi Shamir, and Len Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[51] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM journal on computing*, 26(5):1484–1509, 1997.

[52] John Watrous. Theory of quantum information. *Lecture Notes, University of Waterloo*, 2008.

[53] T. M. Cover and Thomas J. A. *Elements of Information Theory*. John Willey, New York, 1991.

[54] Masanori Ohya and Igor V Volovič. *Mathematical foundations of quantum information and computation and its applications to nano-and bio-systems*. Springer, 2011.

[55] Jun John Sakurai, San-Fu Tuan, and Eugene D Commins. Modern quantum mechanics. *American Journal of Physics*, 63:93, 1995.

[56] Pavel Exner and Miloslav Havlíček. *Hilbert space operators in quantum physics*. Springer, 2008.

[57] J Michael Steele. *The Cauchy-Schwarz master class: An introduction to the art of mathematical inequalities*. Cambridge University Press, 2004.

[58] J. Audretsch. *Entangled Systems: New Directions in Quantum Physics*. Wiley-VCH, 2007.

[59] J. Preskill. Lecture notes for Physics 229: Quantum information and computation. *California Institute of Technology, www.theory.caltech.edu/ preskill/ph229/*, 1998.

[60] E. Desurvire. *Classical and Quantum Information Theory.* Cambridge University Press, 2009.

[61] H.P. Breuer and F. Petruccione. *The Theory of Open Quantum Systems*. Oxford University Press, Oxford, 2002.

[62] L. Hardy. Spooky action at a distance in quantum mechanics. *Contemporary physics*, 39(6):419–429, 1998.

[63] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Reviews of Modern Physics*, 81(2):865, 2009.

[64] A. Peres. *Quantum Theory: Concepts and Methods*. Kluwer Academic Publishers, 1993.

[65] C. H. Bennett and D. P. DiVincenzo. Quantum information and computation. *Nature*, 404(6775):247–255, 2000.

[66] X. Li, Q. Pan, J. Jing, J. Zhang, C. Xie, and K. Peng. Quantum dense coding exploiting a bright Einstein-Podolsky-Rosen beam. *Physical Review Letters*, 88(4):47904, 2002.

[67] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70(13):1895–1899, 1993.

[68] Gary Bowman. *Essential quantum mechanics*. Oxford University Press, 2007.

[69] M. A. Nielsen and Carlton M. Caves. Reversible quantum operations and their application to teleportation. *Phys. Rev. A*, 55(4):2547–2556, Apr 1997.

[70] K. Kraus, A. Böhm, J. D. Dollard, and W. H Wootters. *States, effects, and operations*. Springer-Verlag New York, 1983.

[71] Dennis Kretschmann, Dirk Schlingemann, and Reinhard F Werner. The information-disturbance tradeoff and the continuity of stinespring's representation. *Information Theory, IEEE Transactions on*, 54(4):1708–1717, 2008.

[72] W Forrest Stinespring. Positive functions on c*-algebras. *Proceedings of the American Mathematical Society*, 6(2):211–216, 1955.

[73] Man-Duen Choi. Completely positive linear maps on complex matrices. *Linear algebra and its applications*, 10(3):285–290, 1975.

[74] Shannon C. E. and W. Weaver. *The Mathematical Theory of Communication*. University of Illinos Press, Chicago, 1948.

[75] János Aczél and Zoltán Daróczy. On measures of information and their characterizations. *New York*, 1975.

[76] Hartley R.V.L. Transmission of information. *Bell Syst. Tech. J*, 7(July):535, 1928.

[77] Alfred Wehrl. General properties of entropy. *Reviews of Modern Physics*, 50(2):221, 1978.

[78] Z. Daróczy. Generalized information functions. *Information and control*, 16(1):36–51, 1970.

[79] Johan Ludwig William Valdemar Jensen. Sur les fonctions convexes et les inégalités entre les valeurs moyennes. *Acta Mathematica*, 30(1):175–193, 1906.

[80] A. S. Holevo. Quantum Coding Theorems. *Russian Mathematical Surveys*, 53:1295, 1998.

[81] A. Rényi. On measures of information and entropy. In *Proceedings of the 4th Berkeley Symposium on Mathematics, Statistics and Probability*, volume 1, pages 547–561, 1961.

[82] P. Jizba and T. Arimitsu. Observability of Rényis entropy. *Physical Review E*, 69(2):26128, 2004.

[83] G. Van Assche. *Quantum Cryptography and Secret-Key Distillation*. Cambridge University Press, 2006.

[84] S. Abruzzo, H. Kampermann, M. Mertz, and D. Bruß. Quantum key distribution with finite resources: Secret key rates via rényi entropies. *Physical Review A*, 84(3):032321, 2011.

[85] G. Van Assche. *Quantum Cryptography and Secret-Key Distillation*. Cambridge University Press, 2006.

[86] A. Uhlmann. The "Transition Probability" in the State Space of a* − *Algebra. Rep. Math. Phys*, 9 : 273 − −279, (1976).

[87] Igor Devetak and Andreas Winter. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Science*, 461(2053):207–235, 2005.

[88] M. A. Nielsen, I. Chuang, and L. K. Grover. Quantum Computation and Quantum Information. *American Journal of Physics*, 70:558, 2002.

[89] David Deutsch. Uncertainty in quantum measurements. *Phys. Rev. Lett.*, 50:631–633, Feb 1983.

[90] Christopher A. Fuchs and Asher Peres. Quantum-state disturbance versus information gain: Uncertainty relations for quantum information. *Phys. Rev. A*, 53(4):2038–2045, Apr 1996.

[91] W. K. Wooters and W. H. Zurek. A quantum state cannot be cloned. *Nature*, 299:802.

[92] D. Bruss and G. Leuchs. *Lectures on Quantum Information*. Wiley, 2007.

[93] A. Peres and W. K. Wootters. Optimal detection of quantum information. *Physical Review Letters*, 66(9):1119–1122, 1991.

[94] D.G.B.J. Dieks. Communication by epr devices. *Physics Letters A*, 92(6):271–272, 1982.

[95] Tim Meyer. *Finite key analysis in quantum cryptography*. PhD thesis, Heinrich Heine University Dsseldorf, 2007. http://d-nb.info/987330772.

[96] C.H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, volume 175. Bangalore, India, 1984.

[97] Norbert Lütkenhaus. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A*, 61:052304, Apr 2000.

[98] B. Qi, C. H. F. Fung, H. K. Lo, and X. Ma. Time-shift attack in practical quantum cryptosystems. *Quantum Information and Computation*, 7:073–082, 2007.

[99] A. Vakhitov, V. Makarov, and D. R. Hjelme. Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography. *Journal of modern optics*, 48(13):2023–2038, 2001.

[100] Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar, and Vadim Makarov. Avoiding the blinding attack in qkd. *Nature Photonics*, 4(12):801–801, 2010.

[101] Audun Nystad Bugge, Vadim Makarov, and Johannes Skaar. Preparation of experiment for controlled laser damage of single-photon avalanche photodiode. *arXiv*.

[102] Lecture notes by renato renner at winter school on practical quantum cryptography, available online: http://www.idquantique.com/training-services/winter-school.html.

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

[104] Carl W Helstrom. Quantum detection and estimation theory. *Journal of Statistical Physics*, 1(2):231–252, 1969.

[105] David Deutsch, Artur Ekert, Richard Jozsa, Chiara Macchiavello, Sandu Popescu, and Anna Sanpera. Quantum privacy amplification and the security of quantum cryptography over noisy channels. *Physical Review Letters*, 77(13):2818, 1996.

[106] K. Tamaki and H.K. Lo. Unconditionally secure key distillation from multiphotons in a single-photon polarization based quantum key distribution. In *Information Theory, 2005. ISIT 2005. Proceedings. International Symposium on*, pages 1603–1606. IEEE, 2005.

[107] B. Kraus, N. Gisin, and R. Renner. Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication. *Physical review letters*, 95(8):80501, 2005.

[108] A. Holevo. Statistical problems in quantum physics. In *Proceedings of the Second Japan-USSR Symposium on Probability Theory*, pages 104–119. Springer, 1973.

[109] A.S. Holevo. Probabilistic and statistical aspects of quantum theory, 1982.

[110] M. Christandl, R. Renner, and S. Wolf. A property of the intrinsic mutual information. In *IEEE International Symposium on Information Theory*, pages 258–258, 2003.

[111] U. Maurer and S. Wolf. Unconditionally secure key agreement and the intrinsic conditional information. In *IEEE Transactions on Information Theory*, volume 45, pages 499–514, 1999.

[112] Masahito Hayashi. Upper bounds of eavesdroppers performances in finite-length code with the decoy method. *Physical Review A*, 76(1):012329, 2007.

[113] R.Y.Q. Cai and V. Scarani. Finite-key analysis for practical implementations of quantum key distribution. *New Journal of Physics*, 11:045024, 2009.

[114] Lana Sheridan, Thinh Phuc Le, and Valerio Scarani. Finite-key security against coherent attacks in quantum key distribution. *New Journal of Physics*, 12(12):123019, 2010.

[115] C. Tsallis. Possible generalization of boltzmann-gibbs statistics. *Journal of Statistical Physics*, 52(1):479–487, 1988.

[116] Antonio Maria Scarfone. Entropic forms and related algebras. *Entropy*, 15(2):624–649, 2013.

[117] Michael JW Hall. Universal geometric approach to uncertainty, entropy, and information. *Physical Review A*, 59(4):2602, 1999.

[118] Steeve Zozor, Mariela Portesi, and Christophe Vignat. Some extensions of the uncertainty principle. *Physica A: Statistical Mechanics and its Applications*, 387(19):4800–4808, 2008.

[119] J. Havrda and F. Charvát. Quantification method of classification processes. *Kybernetika*, 3(3):0–3, 1967.

[120] E Rufeil Fiori and A Plastino. A shannon-tsallis transformation. *arXiv preprint arXiv:1201.4507*, 2012.

[121] C.E. Shannon. A mathematical theory of communication. *ACM SIGMOBILE Mobile Computing and Communications Review*, 5(1):3–55, 2001.

[122] Cassel Kevin W. *Variational Methods with Applications in Science and Engineering*. Cambridge University Press, 2013.

[123] H. P. Robertson. The uncertainty principle. *Phys. Rev.*, 34:163–164, Jul 1929.

[124] II Hirschman. A note on entropy. *American Journal of Mathematics*, 79(1):152–156, 1957.

[125] Robert Prevedel, Deny R Hamel, Roger Colbeck, Kent Fisher, and Kevin J Resch. Experimental investigation of the uncertainty principle in the presence of quantum memory and its application to witnessing entanglement. *Nature Physics*, 7(10):757–761, 2011.

[126] K. Kraus. Complementary observables and uncertainty relations. *Phys. Rev. D*, 35:3070–3075, May 1987.

[127] Hans Maassen and J. B. M. Uffink. Generalized entropic uncertainty relations. *Phys. Rev. Lett.*, 60:1103–1106, Mar 1988.

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

[129] Mario Berta, Matthias Christandl, Roger Colbeck, Joseph M Renes, and Renato Renner. The uncertainty principle in the presence of quantum memory. *Nature Physics*, 2010.

[130] Ambedkar Dukkipati, M Narasimha Murty, and Shalabh Bhatnagar. Nonextensive triangle equality and other properties of tsallis relative-entropy minimization. *Physica A: Statistical Mechanics and its Applications*, 361(1):124–138, 2006.

[131] G. H Hardy, JE Littlewood, and G Pólya. *Inequalities*. Cambridge University Press, London and New York, 1934.

[132] Lana Sheridan and Valerio Scarani. Security proof for quantum key distribution using qudit systems. *Phys. Rev. A*, 82:030301, Sep 2010.

[133] YG Tan and QY Cai. Practical decoy state quantum key distribution with finite resource. *The European Physical Journal D*, 56(3):449–455, 2010.

[134] M. Tomamichel and R. Renner. Uncertainty relation for smooth entropies. *Physical Review Letters*, 106(11):110506, 2011.

[135] Kiyoshi Tamaki, Masato Koashi, and Nobuyuki Imoto. Unconditionally secure key distribution based on two nonorthogonal states. *Physical Review Letters*, 90(16):167904, 2003.

[136] Richard J Hughes, George L Morgan, and C Glen Peterson. Quantum key distribution over a 48 km optical fibre network. *Journal of Modern Optics*, 47(2-3):533–547, 2000.

[137] C Gobby, ZL Yuan, and AJ Shields. Quantum key distribution over 122 km of standard telecom fiber. *Applied Physics Letters*, 84(19):3762–3764, 2004.

[138] C. H. Bennett. Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, 68(21):3121–3124, 1992.

[139] A. Rényi. On measures of entropy and information. In *Fourth Berkeley Symposium on Mathematical Statistics and Probability*, pages 547–561, 1961.

[140] Marco Tomamichel. A framework for non-asymptotic quantum information theory. *arXiv:1203.2142*, 2012.

[141] R. Konig, R. Renner, and C. Schaffner. The operational meaning of min-and max-entropy. *Information Theory, IEEE Transactions on*, 55(9):4337–4347, 2009.

[142] Le Phuc Thinh, Lana Sheridan, and Valerio Scarani. Tomographic quantum cryptography protocols are reference frame independent. 2011.

[143] M. Christandl, R. Renner, and A. Ekert. A generic security proof for quantum key distribution. *arXiv:0402131v2*, 2004.

[144] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner. Leftover hashing against quantum side information. *IEEE Transactions on Information Theory*, 57(8):5524 –5535, aug. 2011.

[145] V. Scarani, A. Acin, G. Ribordy, and N. Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Physical Review Letters*, 92(5):57901, 2004.

[146] Anthony Chefles and Stephen M Barnett. Optimum unambiguous discrimination between linearly independent symmetric states. *Physics Letters A*, 250(4):223–229, 1998.

[147] Kiyoshi Tamaki, Masato Koashi, and Nobuyuki Imoto. Unconditionally secure key distribution based on two nonorthogonal states. *Physical review letters*, 90(16):167904, 2003.

[148] Kiyoshi Tamaki, Masato Koashi, and Nobuyuki Imoto. Security of the bennett 1992 quantum-key distribution protocol against individual attack over a realistic channel. *Physical Review A*, 67(3):032310, 2003.

[149] Kiyoshi Tamaki and Norbert Lütkenhaus. Unconditional security of the bennett 1992 quantum key-distribution protocol over a lossy and noisy channel. *Phys. Rev. A*, 69:032316, Mar 2004.

[150] Mohamed Bourennane, Daniel Ljunggren, Anders Karlsson, Per Jonsson, Alexandru Hening, and Juan Pena Ciscar. Experimental long wavelength quantum cryptography: from single-photon transmission to key extraction protocols. *Journal of Modern Optics*, 47(2-3):563–579, 2000.

[151] M Canale, D Bacco, S Calimani, F Renna, N Laurenti, G Vallone, and P Villoresi. A prototype of a free-space qkd scheme based on the b92 protocol. In *Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies*, page 186. ACM, 2011.

[152] Yi Zhao, Bing Qi, and Hoi-Kwong Lo. Quantum key distribution with an unknown and untrusted source. *Physical Review A*, 77(5):052327, 2008.

[153] Antonio Acín, Nicolas Gisin, and Valerio Scarani. Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks. *Phys. Rev. A*, 69(1):012309, Jan 2004.

[154] J. Schwinger. Unitary operator bases. *Proceedings of the national academy of sciences of the United States Of America*, 46(4):570, 1960.

[155] ID Ivonovic. Geometrical description of quantal state determination. *Journal of Physics A: Mathematical and General*, 14:3241, 1981.

[156] W.K. Wootters and B.D. Fields. Optimal state-determination by mutually unbiased measurements. *Annuals of Physics*, 191(2):363–381, 1989.

[157] H. Bechmann-Pasquinucci and A. Peres. Quantum cryptography with 3-state systems. *Phys. Rev. Lett.*, 85(15):3313–3316, 2000.

[158] S. Gröblacher, T. Jennewein, A. Vaziri, G. Weihs, and A. Zeilinger. Experimental quantum cryptography with qutrits. *New Journal of Physics*, 8(5):75, 2006.

[159] I-Ching Yu, Feng-Li Lin, and Ching-Yu Huang. Quantum secret sharing with multilevel mutually (un)biased bases. *Phys. Rev. A*, 78:012344, Jul 2008.

[160] Nicolas J. Cerf, Mohamed Bourennane, Anders Karlsson, and Nicolas Gisin. Security of quantum key distribution using d-level systems. *Phys. Rev. Lett.*, 88:127902, Mar 2002.

[161] R. B. A. Adamson and A. M. Steinberg. Improving quantum state estimation with mutually unbiased bases. *Phys. Rev. Lett.*, 105:030406, Jul 2010.

[162] A. Fernández-Pérez, A. B. Klimov, and C. Saavedra. Quantum process reconstruction based on mutually unbiased basis. *Phys. Rev. A*, 83:052332, May 2011.

[163] D. Giovannini, J. Romero, J. Leach, A. Dudley, A. Forbes, and M. J. Padgett. Characterization of high-dimensional entangled systems via mutually unbiased measurements. *Phys. Rev. Lett.*, 110:143601, Apr 2013.

[164] Christoph Spengler, Marcus Huber, Stephen Brierley, Theodor Adaktylos, and Beatrix C. Hiesmayr. Entanglement detection via mutually unbiased bases. *Phys. Rev. A*, 86:022311, Aug 2012.

[165] A.R. Calderbank, E.M. Rains, P.W. Shor, and N.J.A. Sloane. Quantum error correction and orthogonal geometry. *Phys. Rev. Lett.*, 78(3):405–408, 1997.

[166] Daniel Gottesman. Class of quantum error-correcting codes saturating the quantum hamming bound. *Phys. Rev. A*, 54:1862–1868, Sep 1996.

[167] M Wieśniak, Tomasz Paterek, and Anton Zeilinger. Entanglement in mutually unbiased bases. *New Journal of Physics*, 13(5):053047, 2011.

[168] Agnes Ferenczi and Norbert Lütkenhaus. Symmetries in quantum key distribution and the connection between optimal attacks and optimal cloning. *Phys. Rev. A*, 85:052310, May 2012.

[169] L. Allen, M.W. Beijersbergen, R.J.C. Spreeuw, and J.P. Woerdman. Orbital angular momentum of light and the transformation of Laguerre-Gaussian laser modes. *Phys. Rev. A*, 45:8185–8189, 1992.

[170] B. Rodenburg, M. J. P. Lavery, M. Malik, M. N. O'Sullivan, M. Mirhosseini, D. J. Robertson, M. J. Padgett, and R. W. Boyd. Influence of atmospheric turbulence on states of light carrying orbital angular momentum. *Opt. Lett.*, 37:3735–3737, 2012.

[171] H.K. Lo, H.F. Chau, and M. Ardehali. Efficient quantum key distribution scheme and a proof of its unconditional security. *Journal of Cryptology*, 18:133–165, 2005.

[172] M. T. Gruneisen, W. A. Miller, R. C. Dymale, and A. M. Sweiti. Holographic generation of complex fields with spatial light modulators: application to quantum key distribution. *Applied Optics*, 47:A32–A42, 2008.

[173] V. Arrizón, U. Ruiz, R. Carrada, and A. González. Pixelated phase computer holograms for the accurate encoding of scalar complex fields. *J. Opt. Soc. Am. A*, 24:3500, 2007.

[174] J. A. Davies, D. M. Cottrell, J. Campos, M. J. Yzuel, and I. Moreno. Encoding amplitude information onto phase-only filters. *Applied Optics*, 38:5004, 1999.

[175] G. Lima, L. Neves, R. Guzmán, E. S. Gómez, W. A. T. Nogueira, A. Delgado, A. Vargas, and Saavedra C. Experimental quantum tomography of photonic qudits via mutually unbiased basis. *Opt. Express*, 19:3542, 2011.

[176] D. Klyshko. A simple method of preparing pure states of an optical field, of implementing the einsteinpodolskyrosen experiment, and of demonstrating the complementarity principle. *Soviet Physics Uspekhi*, 31(74):74–85, 1988.

[177] T. Jennewein, M. Barbieri, and A. G. White. Single-photon device requirements for operating linear optics quantum computing outside the post-selection basis. *J. Mod. Phys.*, 58:276–287, 2011.