



Faculty of Sciences
Department of Physics and Astronomy

SECURITY OF QUANTUM KEY DISTRIBUTION PROTOCOLS: TOWARDS PRACTICAL REALIZATION

by

COMFORT SEKGA

Student ID number: 14102079

BSc (Physics and Radiation Health) (UB), MSc (Physics) (BIUST)

A Thesis Submitted to the Faculty of Sciences in Fulfilment of the Requirements
for the Award of the Doctor of Philosophy in Physics of BIUST

Supervisors:

Prof. Gregory Campbell Hillhouse

Department of Physics and Astronomy

Faculty of Sciences, BIUST

hillhouseg@biust.ac.bw

Dr. Mhlambululi Mafu

Department of Physics

Case Western Reserve University,

Cleveland, OH44106, USA

mhlambululi.mafu@case.edu

October, 2024

Contents

List of Figures	viii
List of Tables	xiv
Declaration	xv
Abstract	xvii
Acknowledgment	xviii
Research Output	xix
List of Abbreviations	xxii
1 Introduction	1
1.1 Contribution and outline of this thesis	7
2 Security of quantum key distribution	9
2.1 Introduction	9
2.2 Generic QKD protocol	9

2.2.1	Quantum phase	10
2.2.2	Classical post processing	11
2.3	Security of QKD	12
2.3.1	Security definition	13
2.3.2	QKD attacks	15
2.3.3	Security against collective attacks	16
2.3.4	Security against coherent attacks using post-selection technique	19
2.3.5	Security against coherent attacks via entropic uncertainty relation	20
2.4	Practical QKD set up	22
2.4.1	Sources of signal states	22
2.4.2	Quantum Channels	24
2.4.3	Detectors	24
2.4.4	Practical QKD key rate	25
3	Security of six state SARG04 protocol with post-selection technique	29
3.1	Introduction	29
3.2	Review of the six-state SARG04 protocol	30
3.3	Security against collective attacks	31
3.3.1	Estimation of error rates	33
3.3.2	Bound on the finite secret key rate	35
3.4	Post-selection technique: SARG04 protocol on multi-photons	37
3.4.1	Simulation	39

3.5	Conclusion	41
4	Three-party reference frame independent QKD	42
4.1	Introduction	42
4.2	Operation of the proposed protocol	43
4.3	Security analysis	46
4.4	Finite security analysis	52
4.4.1	Statistical fluctuation analysis	53
4.5	Simulation results	56
4.6	Conclusion	59
5	Reference frame independent twin field QKD	61
5.1	Introduction	61
5.2	Operation of RFI-TF QKD protocol	62
5.3	Security analysis of the protocol	66
5.4	Estimation of key generation rate	71
5.4.1	Simulation of the key rate	72
5.5	Conclusion	76
6	High dimensional QKD with biphotons	77
6.1	Introduction	77
6.2	Protocol Definition	78
6.3	Security analysis	86
6.4	Simulation results	88

6.5	Conclusion	90
7	Measurement device independent QKD with vector vortex beams under diverse weather conditions	92
7.1	Introduction	92
7.2	Operation of the OAM-based MDI-QKD protocol	93
7.3	Security analysis	99
7.4	Propagation through perturbing media	100
7.5	Simulation	106
7.6	Conclusion	111
8	Concluding remarks	112
Appendix A Fundamental concepts of quantum mechanics and quantum information measures		115
A.1	Introduction	115
A.2	Quantum mechanics concepts	115
A.2.1	Hilbert space	116
A.2.2	Quantum states	116
A.2.3	Density operators	117
A.2.4	Linear operators	118
A.2.5	Tensor Products	119
A.2.6	Reduced Density operator	121
A.2.7	Schmidt decomposition	122
A.2.8	Purification	122

A.2.9	Quantum operations	123
A.2.10	Quantum measurement	124
A.3	Information theory	125
A.3.1	Classical information theory	126
A.3.2	Quantum information theory	128
Appendix B Estimation of key rate parameters and derivation of finite key rate for three-party RFI QKD		130
B.1	Decoy parameters estimation	130
B.2	Secrecy	135
Appendix C Determination of yields in the virtual and actual protocols		139
C.1	Determination of yield for virtual states	139
C.2	Determination of yield of states used in the actual protocol	142
Appendix D Security proof of the TF-QKD and the channel model		147
D.1	Security proof against coherent attacks	147
D.2	Channel model	157
D.2.1	Estimation of gain and error rate from Z basis	158
D.2.2	Estimation of gain in the X and Y bases	160
Appendix E Estimation of key rate parameters and derivation of key rate formula for the MDI-QKD based on biphotons		162
E.1	Estimation of key rate parameters	162
E.1.1	Statistical fluctuation analysis	165

E.2 Secrecy	169
Appendix F Derivation of decoy-state parameters for MDI-QKD with vector vortex beams	172
Bibliography	176

List of Figures

3.1	The plot of secret key fraction versus the number of signals N , for (i) six-state SARG04 protocol under collective attacks with four-photon source, (ii) six-state SARG04 protocol with four-photon source following post-selection technique.	39
3.2	The plot of secret key fraction versus the number of signals N , for (i) four-state SARG04 protocol under collective attacks with two-photon source, (ii) four-state SARG04 protocol with two-photon source following post-selection technique.	40
4.1	The schematic diagram of the three-party RFI-QKD protocol. Alice starts by preparing a two-photon entangled state using a spontaneous parametric down-conversion (SPDC) source. Next, the two photons are modulated into polarized states belonging to three bases $\{X, Y, Z\}$ using a polarization modulator (PM) and sent to Bob and Charlie through an insecure channel. The photons prepared in the X and Y basis experience misalignment by degree β_B and β_C for Bob and Charlie, respectively. The acronyms IM, BS, PBS, HWP, and SPD are intensity modulator, beam-splitter, polarizing beam-splitter, half-wave plate, and single-photon detector, respectively. . .	45

4.2	Plot of secret key rate versus number of signals N for the proposed three-party RFI protocol (solid lines) for security parameters: $\varepsilon_{\text{cor}} = 10^{-15}$, $\varepsilon_{\text{sec}} = 10^{-10}$, and the misalignment error rates $Q = (0.02\%, 0.03\%, 0.05\%)$. Experimental parameters: dark counts rate, $P_d = 1.7 \times 10^{-6}$, the loss coefficient of the channel is 0.2 km/dB, the detection efficiency is $\eta = 14.5\%$. We also plot the two-party RFI protocol (dashed lines) for the same error rates for comparison. . . .	56
4.3	(a) Expected secret key rate (in logarithmic scale) for the proposed three-party RFI protocol (solid red line) as a function of transmission distance measured in km, for the fixed misalignment degree β . From left to right, the curves represent $\beta = \pi/6$, $\beta = \pi/8$ and $\beta = 0$. The number of signals is fixed at 10^9 (b) Expected secret key rate (in logarithmic scale) for the proposed three-party RFI protocol (solid red line) as a function of transmission distance measured in km, for the fixed number of signals, $N = 10^7$, $N = 10^8$ and $N = 10^9$. The relative rotation of reference frames is set at $\beta = \pi/8$ and security parameters are: $\varepsilon_{\text{cor}} = 10^{-15}$, $\varepsilon_{\text{sec}} = 10^{-10}$, experimental parameters: dark counts rate, $P_d = 1.7 \times 10^{-6}$, the loss coefficient of the channel is 0.2 km/dB, the detection efficiency is $\eta = 14.5\%$. For comparison purposes, we show the plots of two-party RFI protocol, represented by blue dashed lines in both figures.	57
4.4	Plots of secret key fraction vs quantum bit error rate, E_{ZZZ} for the BB84 protocol [259], two-party RFI protocol [73] and the proposed three-party RFI protocol.	58

- 5.1 The setup of the proposed RFI TF-QKD. Alice and Bob use their laser sources (LS) to prepare coherent states $|\sqrt{\mu_{a(b)}}e^{i\chi}\rangle$ with random phase χ in the Z basis and states $|\sqrt{\mu_{a(b)}}e^{i(0+\chi)}\rangle$ and $|\sqrt{\mu_{a(b)}}e^{i(\frac{\pi}{2}+\chi)}\rangle$ for X and Y basis, respectively. The phase is encoded using phase modulators (PM). Alice and Bob send the prepared optical signals through an insecure channel to the untrusted Charlie, who is supposed to perform a single-photon interference in a symmetric beam-splitter (BS) followed by threshold detection in either L or R detector. In the X and Y bases, the random phase χ is selected from discrete M phase slices $\Delta_j = (\frac{2\pi j}{M}, \frac{2\pi(j+1)}{M})$ over the semi-interval $[0, 2\pi)$ with $j = \{0, \dots, M-1\}$. During classical post-processing, the random phases are announced, and states are postselected according to the satisfaction of condition; $|j_A - j_B| \bmod M = 0$ or $|j_A - j_B| \bmod M = \frac{M}{2}$ where $j_{A(B)} = (\frac{\Delta_j M}{2\pi}) \bmod M$ 65
- 5.2 Secret key rate (in logarithmic scale) for RFI-TF protocol with source flaws (dashed lines) as a function of transmission distance measured in km, for experimental parameters: dark counts rate, $p_d = 5 \times 10^{-7}$, the loss coefficient of the channel, $\alpha=0.2$ km/dB, the detection efficiency, $\eta = 14.5\%$. From left to right, the plots represent the encoding flaws $\delta = 0.147$, $\delta = 0.127$ and $\delta = 0.090$. The solid line corresponds to the RFI-TF protocol with perfect encoding, and the solid black line represents the PLOB bound [102]. 73
- 5.3 Secret key rate (in logarithmic scale) for RFI-TF protocol with $\delta = 0.127$ (dashed line) as a function of transmission distance measured in km, for experimental parameters: dark counts rate, $p_d = 5 \times 10^{-7}$, loss coefficient of the channel, $\alpha=0.2$ km/dB, the detection efficiency, $\eta = 14.5\%$. For comparison purposes, we plot the curve for Phase matching (PM) QKD [296] denoted by the blue solid line. The solid red line corresponds to the original TF protocol [106] and the black solid line represents the PLOB bound [102]. 74

6.1	Mach-Zehnder interferometer set up used by Alice and Bob for biphoton state preparation. The laser beam is pumped towards a non-symmetric beam-splitter that transmits $2/3$ and reflects $1/3$ of the beam through the long and short arms. The $(\lambda/2)_i$ represents the halve wave plates for manipulating the amplitude, c_i of the states. The phase shifters (PS. 1 and PS. 2) introduce relative phases between the states. The DM denotes the dichroic mirror, which transmits two biphotons created using type I non-linear crystals from the long arm of the interferometer and reflects the pump from the short arm towards the type II non-linear crystal for the creation of state $ 1_h, 1_v\rangle$	80
6.2	The generic measurement set up for our proposed MDI-QKD. Alice and Bob start by preparing the biphoton states from two mutually unbiased bases and sending them to Charlie through the unsecured channel. Charlie allows the states to interfere in the symmetric beam-splitter (BS) upon receiving the states. The photons are directed towards the tritter and eventually detected in the Brown Twiss scheme (mode sorter).	81
6.3	Illustration of the measurement set up at Charlie's site. The incoming biphotons interfere in the beam-splitter (BS) and exit through either of two output ports towards the two non-symmetric beam-splitter (NPBS), where they are further split into three channels and directed towards the tritter. The tritter setup shown in the upper left is a three-input-output port splitter. It comprises three conventional beam-splitters (BS), four-phase shifters (PS), and a mirror. The output ports of the tritter are linked with three Brown Twiss schemes for detecting the three basic states $ \alpha\rangle$, $ \beta\rangle$, and $ \gamma\rangle$. Each Brown Twiss scheme consists of a non-symmetric beam-splitter (NPBS), wave plates (WP), polarization analyzer (A), and detectors ($\mathbf{DP}_i$) where $\mathbf{P} \in \{H, V\}$ represents polarization mode and subscript i denotes single photons forming biphotons. The abbreviation c.c corresponds to coincident counting or detection.	83
6.4	Illustration of the secret key rate (in logarithmic scale) in terms of the transmission distance (km), for a fixed amount of signals $N = 10^{12}$, $N = 10^{13}$, $N = 10^{14}$ and $N = 10^{16}$	88

6.5	Illustration of the secret key rate (in logarithmic scale) in terms of the transmission distance (km) for our proposed biphoton MDI QKD and the qubit-based MDI QKD proposed in Ref. [240] for a fixed amount of signals $N = 10^{16}$	89
6.6	The secret key rate (in logarithmic scale) in terms of the number of signals N , for intrinsic misalignment errors 0.3%, 0.6%, and 1%.	90
6.7	Plots of secret key fraction vs quantum bit error rate, E for the 2-dimensional (qubit based) QKD and the 3-dimensional (qutrit based) QKD based on the secret key fraction formula derived in [302].	90
7.1	An illustration of the proposed OAM-based MDI-QKD. Alice and Bob prepare two mutually unbiased basis states ($\mathbf{V}$, $\mathbf{S}$) and send them to Charlie through the unsecured channel. The $\lambda/2$ plate and the q -plate are used to generate a set of vector and scalar modes, which are then attenuated to intensity $\gamma \in \{\mu, \nu, 0\}$ using intensity modulator IM. Next, the telescope collimates the quantum states with a finite aperture. They are sent through a free atmospheric space link to the measurement site controlled by Charlie. The optical states are then collected by the telescope and allowed to interfere with the symmetric beam-splitter (BS). Next, the photons are passed through the polarization grating that separates the left and right circularly polarized photons, then guided by mirrors (M1, M2, M3, M4) towards a beam-splitter (BS). As a result, the photons are measured using the mode sorters (MS) that map OAM to position and then detected by the detectors (L0, R0, L1, R1).	95
7.2	This plot illustrates the probability of receiving adjacent OAM states (Transmittance), η_{turb} against the ratio of the aperture diameter D to the Fried parameter r_0	107
7.3	A plot of the secret key generation rate, K , versus transmission distance when atmospheric turbulence is varied as measured by the deviation of OAM modes, $\Delta\ell$	107
7.4	A plot of transmittance, η , against the diameter of raindrops, D_{rain}	108

7.5	Plot of the secret key generation rate, K , against transmission distance in km for a range of raindrop diameters.	109
7.6	An illustration showing the relation between the beam extinction coefficient, α_{fog} , and the radius of the fog particles, R_{fog}	109
7.7	A plot of the secret key generation rate, K , against transmission distance in km for various values of the radius of the fog particles. .	110

List of Tables

6.1	The parameter settings for biphoton states from two mutually unbiased bases used in our QKD scheme. The complex amplitudes $ c_i $ are realized through the use of half-wave plates. The ϕ_i are realized by use of phase shifters.	80
6.2	The parameter settings for wave plates in the Brown Twiss schemes.	84
6.3	The possible Bell state measurement results in the Brown Twiss scheme mode sorting.	85
7.1	Probability distribution for Bell state measurement results announced by Charlie when both Alice and Bob choose the same basis.	98
7.2	Post-processing of raw key in the sifting step. Bob flips his bits to ensure a correct correlation with Alice's bit.	99
7.3	Parameters used for simulation.	108

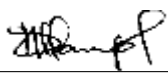
DECLARATION REGARDING THE WORK AND COPYRIGHT

Candidate: COMFORT SEKGA

Student ID:14102079

Thesis Titled: SECURITY OF QUANTUM KEY DISTRIBUTION PROTOCOLS:
TOWARDS PRACTICAL REALIZATION

I, **Comfort Sekga**, certify that the thesis is all my own original work and that I have not obtained a degree in this University or elsewhere on the basis of any of this work. This thesis is copyright material protected under the Berne Convention, the Copyright and Neighbouring Rights Act, Act. No. 8 of 2000 and other international and national enactments, in that behalf, on intellectual property. It must not be reproduced by any means, in full or in part, except for short extracts in fair dealing; for researcher private study, critical scholarly review or discourse with an acknowledgement, without the written permission of the office of the Postgraduate School, on behalf of both the author and the BIUST.

Signature: 

Date: 11/03/2025

Primary Supervisor: Prof. Gregory Campbell Hillhouse

I, the Candidate's **Primary Supervisor**, hereby confirm that I have inspected the above titled thesis and, to the best of my knowledge, it is based on the original work of the candidate.

Signature: 

Date: 11/03/2025

Abstract

Quantum cryptography, or more specifically, quantum key distribution (QKD), guarantees information theoretical security-the Holy Grail of communication security based on the principles of quantum physics. Since the primitive BB84 QKD protocol, great strides have been made both in theory and experiments to develop quantum technologies for real-life applications. Even though QKD has reached this milestone, most security analyses are based on the assumption that the QKD system's preparation and measurement devices are idealized. However, such assumptions can be fatal to the security of a QKD system. As a result, we relax some of these assumptions and prove the security of several QKD protocols by using techniques that closely emulate the imprecisions in preparation and measurement devices and the environment in which the QKD is operated. For instance, we apply the post-selection technique to demonstrate the security of the six-state SARG04 protocol against general attacks with finite resources. Through this approach, one can derive a secure key from a multi-photon source while also taking into account an optimal coherent attack. Moreover, we employ the reference frame independence (RFI) concept, which eliminates the need for active alignment of reference frames to derive the security bounds for several proposed QKD protocols. Our security analyses also incorporate the loss-tolerant method, which allows us to prove the security of QKD by considering imperfections in the state preparation. Furthermore, we propose the variants of the measurement-device-independent (MDI) QKD protocol, which utilizes a measurement device controlled by a third party, who may be an eavesdropper, thus removing the possibility of detector side-channel attacks. We also exploit quantum resources, such as biphotons, that enable us to achieve high dimensional encoding in our proposed protocols. Also, we utilize vector vortex and scalar beams to study the security of proposed protocols through a turbulent

atmospheric link under diverse weather conditions such as rain or haze. The simulation results demonstrate that the proposed protocols can achieve a significant secret key rate at reasonable transmission distances comparable to the key rates obtained under an ideal environment with perfect preparation and measurement devices. Therefore, proving the security of QKD while allowing intrinsic errors due to signal preparation and measurement devices makes a giant step toward realizing practical QKD implementations.

Acknowledgments

First, I would like to thank my supervisor, Dr. Mhlambululi Mafu, who gave me the opportunity to work with him for my PhD study at BIUST. I want to thank him for his support, valuable discussions and advice throughout my research. He was always there to offer moral support and undampening motivation during difficult times. It has been my great honor to work with him. I would also like to thank Prof. Gregory Hillhouse for his unwavering support and for ensuring the completion of this thesis after the resignation of Dr. Mafu from BIUST.

I want to thank my family, colleagues and friends for their encouragement throughout my studies. Lastly, I thank God, who gave me the strength and wisdom to complete this thesis.

Scientific Output

Journal Publications

This thesis is based on the following published articles, of which I am a primary author under the supervision of Dr. Mhlambululi Mafu.

- a) Comfort Sekga & Mhlambululi Mafu. (2021). Security of quantum-key-distribution protocol by using the post-selection technique. *Physics Open* 7, 100075.
- b) Comfort Sekga & Mhlambululi Mafu. (2021). Three-party reference frame independent quantum key distribution protocol. *Chinese Physics B* 30, 120301.
- c) Comfort Sekga & Mhlambululi Mafu. (2021). Reference frame independent twin field quantum key distribution with source flaws. *Journal of Physics Communications* 5, 045008.
- d) Comfort Sekga, Mhlambululi Mafu & Makhamisa Senekane. (2023). High-dimensional quantum key distribution implemented with biphotons. *Scientific Reports* 13(1), 1229.
- e) Comfort Sekga & Mhlambululi Mafu. (2023). Measurement device-independent quantum key distribution with vector vortex modes under diverse weather conditions. *Scientific Reports*, 13(1), 14931.

During my PhD study, I also contributed to the following publications which do not form part of this thesis.

- a) Comfort Sekga & Mhlambululi Mafu. (2021). Quantum state sharing of an arbitrary m-particle state using Einstein-Podolsky-Rosen pairs and application in quantum voting. *Modern Physics Letters A* 36, 2150151.
- b) Mhlambululi Mafu, Comfort Sekga & Makhamisa Senekane. (2021). Loss-tolerant prepare and measure quantum key distribution protocol. *Scientific African* 14, e01008.
- c) Comfort Sekga & Mhlambululi Mafu. (2022). Tripartite quantum key distribution implemented with imperfect sources. *Optics* 3, 191-208.
- d) Mhlambululi Mafu & Comfort Sekga. (2022). Security of Bennett-Brassard 1984 quantum-key distribution under a collective-rotation noise channel. *Photonics* 9, 941.
- e) Keaotshepha Karabo, Comfort Sekga, Connor Kissack, Mhlambululi Mafu & Francesco Petruccione. (2024). A novel quantum key distribution resistant against large-pulse attacks. *IET Quantum Communication* 5(3), 282–290.

Conference Proceedings

- a) Comfort Sekga & Mhlambululi Mafu. (2019). Quantum secret sharing with Greenberger Horne Zeilinger states, in *The Proceedings of SAIP2019, the 64th Annual Conference of the South African Institute of Physics, edited by Prof. Makaiko Chithambo, (SU/2019)*, pp. 336-341. ISBN: 978-0-620-88875-2.
- b) Comfort Sekga & Mhlambululi Mafu. (2021). Three-party reference frame independent quantum key distribution with an imperfect source, in *The Proceedings of SAIP2021, the 65th Annual Conference of the South African Institute of Physics, edited by Prof. Aletta Prinsloo, (UJ)*, pp. 650-655. ISBN: 978-0-620-97693-0.

Conference Presentations

- a) Comfort Sekga & Mhlambululi Mafu. (2019). Quantum secret sharing with graph states. The 64th South Africa Institute of Physics Conference 2019, University of Venda, South Africa.
- b) Comfort Sekga Sekga & Mhlambululi Mafu. (2021). Three-party reference frame independent quantum key distribution with an imperfect source. The 66th South Africa Institute of Physics Conference 2021, North-West University, South Africa.

List of Abbreviations

QKD	quantum key distribution
RFI	reference-frame-independent
RSA	Rivest-Shamir-Adleman
BB84	Bennett-Brassard-1984
SARG04	Scarani-Acin-Ribordy-Gisin-2004
E91	Ekert-1991
BB92	Bennett-Brassard-Mermin-1992
CV	continuous-variable
DPR	distributed-phase-reference
DPS	differential-phase-shift
COW	coherent-one-way
PNS	photon number splitting
WPS	weak coherent photon pulses
SPF	state preparation flaws
MDI	measurement-device-independent
PLOB	Pirandola-Laurenza-Ottaviani-Banchi

TF twin-field

HD high-dimensional

OAM orbital angular momentum

GHZ Greenberger–Horne–Zeilinger

POVM positive operator valued measure

MUB mutually unbiased bases

CPTP completely positive and trace preserving

SPDC spontaneous parametric down-conversion

APD avalanche photodiodes

QBER quantum bit error rate

EDP entanglement distillation procedure

GLLP Gottesman-Lo-Lutkenhaus-Preskill

BS beam-splitter

Introduction

Since over a thousand years ago, humans have used codes as reliable methods of keeping secrets. With the advent of several technological advances, these codes continue to be broken by cryptanalysts, prompting cryptographers to invent even more sophisticated encryption schemes. However, quantum information technology, specifically quantum cryptography, promises to break this vicious classical cryptography cycle. Quantum cryptography permits us to develop communication schemes whose secrecy depends only on quantum mechanical laws and minimal assumptions about cryptographic hardware [1]. The best-known example of quantum cryptography is quantum key distribution (QKD), which offers an information-theoretically secure solution to the key exchange problem [1–3]. The advantage of quantum cryptography is that it allows the completion of various cryptographic tasks that are proven or conjectured impossible using only classical communication. Classical cryptographic schemes are typically built on unproven mathematical assumptions and restrictions on adversary computational powers. Thus, classical cryptographic schemes are designed assuming some underlying mathematical tasks are hard to compute, i.e., no efficient algorithm currently exists for solving the mathematical problem. A typical example is Rivest-Shamir-Adleman (RSA), a widely adopted public-key cryptography encryption protocol based on the difficulty of prime factorization [4]. However, there is no guarantee that no efficient algorithm can be discovered in the future to nullify the security of such a cryptographic protocol. Therefore, such schemes do not guarantee information-theoretic security owing to their vulnerability to future technological advances in hardware and algorithms, including developing a quantum computer. To be more precise, let us assume that a message encrypted today will be kept secret for sixty years. The encryption scheme

must be practically unbreakable even after technological breakthroughs in the next fifty years. However, it has been proved that classical cryptosystems will fall apart with the birth of scalable quantum computers capable of, for instance, implementing Shor’s prime factorization algorithm [5].

Quantum key distribution (QKD), in general, guarantees information theoretical security—the Holy Grail of communication security—based on the principles of quantum physics [1–3, 6, 7]. Essentially, QKD is a key-generating procedure that permits two distant legitimate parties, Alice and Bob, to establish a shared secret key even if an eavesdropper, Eve, who has unlimited computational power, interferes with the communication channel. An eavesdropper who attempts to learn the key can be detected by exploiting the elementary physical limitations implied by quantum physics. For instance, following a well-known principle of quantum physics, which postulates that measurement, in general, perturbs the state of the measured system, any action taken by Eve to gain some information out of quantum states is a generalized form of measurement that will disturb the original quantum states. Eve’s strategy may be to generate a perfect copy of the quantum state Alice sends to Bob; however, this is forbidden by the no-cloning theorem [8]. A third physical argument that Alice and Bob can exploit to deter an eavesdropper from learning any information on the key is the principle of entanglement tied together with the violation of Bell’s inequalities [3].

Based on these quantum mechanical principles, Bennett and Brassard proposed the first QKD protocol in 1984, now commonly known as the BB84 protocol [2]. Notably, the BB84 protocol has become one of the most well-studied QKD schemes and has been shown experimentally. In 1991, Ekert augmented the original idea of BB84 and independently devised a protocol for which security is based on entanglement and violation of Bell’s inequality, resulting in the E91 protocol [3]. By applying E91 ideas to the BB84 protocol in 1992, Bennett, Brassard and Mermin developed the BBM92 protocol, which also relies on entanglement for security [9]. As part of the effort to combat photon number splitting attacks [10, 11], the SARG04 protocol was developed in 2004 [12]. Notably, the quantum state transmission and measurement phases of the SARG04 protocol are similar to those in the BB84 protocol. The difference lies only in the classical post-processing phase. There are three classes of QKD protocols based on the detection technique used to recover the key information encoded within the properties of light. The BB84, E91, BBM92, B92 [13] and SARG04 [12] belong to a class called discrete-variable (DV) protocols. In this class, information is encoded in the photon pulses, which resemble

true single-photon states and utilize single-photon detectors for detection purposes. Due to the challenges associated with producing true single-photon sources and detectors, another class of continuous-variable (CV) protocols was proposed. In this class, information is encoded in the quadratures of the quantized electromagnetic field, for instance, those of coherent or squeezed states [14–23]. To meet other practical QKD implementation requirements, the class of distributed-phase-reference (DPR) protocols in which the coherence of sequential pulses plays a crucial role in security was developed. The DPR class encodes information in photon arrival times or the phase between adjacent weak coherent pulses. Members of this family are the differential-phase-shift (DPS) protocol [24–31] and coherent-one-way (COW) protocol [32–36]. Most importantly, the DPS and COW protocols tolerate photon number splitting (PNS) attacks.

Generally, QKD security is founded on the principle of quantum physics as well as the assumption of ideal preparation and measurement devices. However, in practice, QKD devices exhibit imperfections, which barely conform to idealized theoretical models used to analyze security. For conventional QKD protocols, one usually presumes that preparation and measurement devices are trusted and characterized in security proofs. Based on these assumptions about the behavior of the devices, QKD protocols can be proven to be information-theoretically secure. However, deviation from ideal models during the physical implementation of QKD opens up various security loopholes for Eve, such as the side-channel attacks.

As a result, we discuss some of these implementation challenges and how they have been addressed in the following sections. Most notably, this also provides a motivation for this thesis to address some of these challenges. A case in point, there have been both theoretical demonstrations of side-channel attacks that exploit specific properties of preparation and measurement devices [10, 11, 37, 38] and proof-of-principle attacks on QKD systems [39–48]. A well-known hacking strategy targeting the preparation device is the PNS attacks [10, 11]. The implementation of QKD protocols relies on single photons. However, due to their unavailability, highly attenuated lasers are widely adopted as sources of single photons. These lasers produce weak coherent photon pulses (WCP) whose photon number distribution obeys the Poisson probability distribution; hence, there is a non-zero probability for multiple-photon pulses. Consequently, Eve may utilize the multiple-photon pulses and initiate the PNS attack. Fortunately, a few years after discovering this hacking strategy, the decoy-state method [49, 50], and SARG04 protocol were developed to address the security threat posed by PNS attacks.

Ideally, the encoding of photon signals is executed perfectly without state preparation flaws (SPF). However, this assumption falls short experimentally due to inherent deficiencies in optical modulators. For definiteness, if the quantum states are encoded into the polarization degree-of-freedom of the photon, an encoding flaw may result from a misalignment in the waveplate used to set the polarization. Particularly, Gottesman et al. [51] demonstrated that such inaccuracies in encoding can result in poor secret key rates in the presence of high quantum channel loss. This strong dependency on channel loss stems from the fact that SPFs can be viewed as a form of basis information leakage. This provides Eve with some edge in orchestrating basis-dependent attacks. Recently, a loss-tolerant protocol [52] was devised to make QKD robust against state preparation flaws. Remarkably, by employing a phase error estimation technique involving the use of basis mismatched events, the secret key rate of the loss-tolerant protocol is slightly changed by the increase in SPFs.

Notably, the security proofs of conventional QKD protocols rely on trusted measurement devices, a premise that enables them to achieve significant rates, but also provides a loophole for side-channel attacks [53]. To circumvent detector side-channel attacks, a device-independent (DI) QKD was proposed whose security relies on the violation of a Bell inequality [7, 54–59]. Unfortunately, the DI-QKD requires loophole-free Bell experiments which renders it not viable with current technology. A more practical alternative is measurement-device-independent (MDI) QKD, which is intrinsically unsusceptible to all side-channel attacks aimed at the measurement device and removes all detection-related security loopholes [60–72]. In MDI-QKD the two parties, Alice and Bob are linked by an untrusted relay. This results in a significant increase in attainable transmission distance compared to conventional QKD schemes. However, the practical MDI-QKD still suffers from its relatively low key rate compared to conventional BB84 protocol due to the requirement of Bell state measurements.

Moreover, QKD implementation requires aligning shared reference frames between communicating parties, a requirement that poses a problem for practical implementation. For example, polarization encoding QKD systems require alignment of polarization states, while phase coding QKD systems require interferometric stability. As a result of unstable fiber communication links and imperfections in the measuring devices, these requirements have proven to be challenging to fulfill. It is possible to overcome the potential reference frame misalignment challenge by encoding qubits in larger systems. However, the process requires creating

and manipulating many photon-entangled states that are technically challenging to generate and very susceptible to losses. As a result, reference-frame-independent (RFI) QKD protocols have been devised to address the reference frame alignment issue [73]. The system has achieved impressive results both theoretically [74–92] as well as experimentally [93–101], showing its ability to exchange keys securely under varying reference frames.

Besides the challenges related to QKD security and imperfections in preparing and measuring devices, channel losses also pose a significant obstacle to the practical implementation of QKD, resulting in key rate and distance limitations. Currently, it is well known that any point-to-point implementation of QKD is restricted by the Pirandola, Laurenza, Ottaviani and Banchi (PLOB) bound, named after the authors who discovered it [102]. This bound indicates that for a lossy link with transmittance η , two parties can generate the secret keys at an utmost rate of $-\log_2(1 - \eta)$, which corresponds to the secret key capacity of the channel. This implies that the secret key rate scales linearly with the channel transmittance for any direct point-to-point QKD protocol. For instance, protocols like single-photon-based BB84, decoy-state-based BB84 protocol with weak coherent pulses and Gaussian modulated CVQKD are restricted by key rate scaling of $\simeq \eta$ bits per channel use. Therefore, to circumvent this limit and achieve long-distance high-rate QKD implementations, we must employ quantum repeaters [103, 104] and quantum networks [105]. However, quantum repeaters are still not possible with the current technology. Recently, a novel QKD that relies on phase-randomised twin fields of optical pulses to encode information was developed and can surpass the secret key capacity bound for repeaterless QKD schemes [106–117]. Similar to MDI-QKD, the possibility of detector side-channel attacks is removed in this protocol as an untrusted relay connects the communicating parties. The twin field (TF) protocol is based on single photon interference of optical fields generated with almost identical electromagnetic phases. This single photon interference at the untrusted relay leads to an improved secret key rate, which scales with $\simeq \sqrt{\eta}$.

Furthermore, to address the problem of limited achievable key rate in QKD, high dimensional encoding has been invoked as a perfect solution. Generally, in order to encode information in QKD protocols, parties choose certain degrees of freedom such as the polarization or phase properties of a single photon as quantum states. This implies that only one classical bit of information can be encoded onto each quantum state, resulting in limited secret key rates. However, by using high-dimensional (HD) quantum systems, communicating parties can encode information

beyond one bit per signal. Therefore, by using high-dimensional encoding where each photon can encode $\log_2 d > 1$ bits of information (where d stands for the dimension of the system), a secret key rate naturally reduced by inevitable factors like channel losses, source flaws and detector flaws can be significantly improved. Furthermore, high dimensional quantum states have been found to be more resistant to background noise and hacking attacks compared to their qubit counterparts [118]. Therefore, owing to the benefits associated with high dimensional states, several degrees of freedom have been investigated for HD-QKD which includes position-momentum [119], orbital angular momentum (OAM) [120–129], time energy [130–151] and biphotons [152–154].

Apart from these advances, integrated photonic devices have been identified as a solution to large-scale deployment QKD owing to their characteristics which provide enhanced functionality and miniaturization, in a platform amenable to mass-manufacture and easy integration with existing and emerging classical integrated telecommunications infrastructure [155–160]. Most significantly, these integrated photonic chips offer numerous benefits such as low cost, low power consumption, and well-established batch fabrication techniques [161]. In particular, QKD chips, which utilize well-established integrated techniques, have been developed to create main QKD devices [162–171]. The reliability of these chip-based QKD devices has been proven through the implementation of various QKD protocols, such as decoy-state BB84 [155, 162, 166, 172–177], high-dimensional QKD [178, 179], continuous-variable QKD [180], and measurement-device-independent QKD [156, 158, 181, 182]. These advancements pave the way for integrating QKD into telecommunications networks. For a recent review on the progress in chip-based QKD, see Ref. [160].

Overall, QKD has seen numerous breakthroughs in recent years. This is supported by the continuous emergence of novel protocols designed to bridge the gap between theory and practice. By far, QKD experiments have been demonstrated in efforts to achieve increasingly long distances and/or higher key rates. The establishment of intercity QKD networks can witness the maturity of the field [183–192], successful realization of satellite-based QKD in China [193–195] and other efforts to attain the same feat, development of commercial prototypes in several startup companies can bear witness to the maturity of QKD field.

1.1 Contribution and outline of this thesis

As already mentioned, most security analyses are based on the assumption that the QKD system's preparation and measurement devices are idealized. However, such assumptions can be fatal to the security of a QKD system. As a result, this thesis aims to relax some of these assumptions. Specifically, we demonstrate security proofs of several QKD protocols by using techniques that closely emulate the imprecisions in preparation and measurement devices and the environment in which the QKD is operated. Accordingly, our findings are presented in chapters 3-7. This thesis is arranged as follows.

Chapter 2 describes how to implement generic QKD protocol and reviews the security definition and classification of QKD attacks as well as their security proof methods. We conclude the chapter by discussing the set up of practical QKD and formulation of its secret key rate.

In Chapter 3, we apply the post-selection technique to derive the security bounds for the six-state SARG04 QKD protocol using finite resources. This protocol is robust against the zero-error type of attacks such as PNS attacks. This allows us to demonstrate information theoretical security against optimal coherent attacks under practical conditions where a source emits multiple photons. This chapter is based on Ref. [196].

In Chapter 4, we present a three-party RFI-QKD protocol that can be implemented without actively aligning the reference frame between the sender and receiver. The protocol exploits entangled states to establish a secret key between three communicating parties. We derive the security bounds for the proposed protocol against collective attacks. We then perform a finite-size key security analysis against general attacks in the presence of statistical fluctuations based on entropic uncertainty relations. The work is based on Ref. [197].

Chapter 5 examines the asymptotic security of reference frame independent twin field quantum key distribution (RFITF QKD). The chapter is based on Ref. [198]. By considering an RFI case, we simplify the practical implementation of the protocol by removing the need for active phase stabilization. Moreover, we employ the loss-tolerant method proposed by Tamaki et al. [52] which allows us to prove the security of the protocol by considering imperfections in the state preparation.

Chapter 6 proposes an MDI-QKD protocol that exploits the polarization state of a biphoton to encode information on a qutrit, a three level quantum system. Also, we investigate the performance of the proposed protocol by simulating the secret key rate as a function of transmission distance in the finite regime. The protocol allows communicating parties to encode information beyond one bit per signal. The contents of this chapter are based on Ref. [199]

Chapter 7 introduces an MDI-QKD implemented with vector vortex modes. Specifically, we study the transmission of vector vortex and scalar beams through a turbulent atmospheric link under diverse weather conditions such as rain or haze. By utilizing vector vortex beams, which have largely been ignored in the literature, we demonstrate that a maximum secure key transmission distance of 178 km can be achieved under clear conditions. When raindrops have a diameter of 6 mm and fog particles have a radius of $0.5 \mu\text{m}$, the signals can reach 152 km and 160 km, respectively. Since these distances are comparable, this sheds light on the feasibility of MDI-QKD implemented using vortex vector modes and opens the door to long-distance quantum secure communications. The chapter is based on Ref. [200].

In Chapter 8, we present our conclusions and suggest further research directions. Precisely, the chapter captures the findings of the proposed protocols and insights drawn from the results as far as realization of practical QKD is concerned. We further provide directions on how the proposed protocols can be improved to improve the achieve better key rates and enhanced security.

Security of quantum key distribution

2.1 Introduction

We begin by describing the steps involved in implementing a generic QKD protocol and defining the fundamental notions of security in QKD. Specifically, we describe briefly the quantum mechanical principles that underpin QKD security. This chapter will also provide an overview of security-proof methods against various classes of attacks that could be launched by an eavesdropper. The presented security analysis is mainly based on the composability framework developed by Renner [201]. Further, we provide an overview of a practical quantum key distribution set-up, in which we examine the types of quantum channels used to transmit photons and the detection mechanisms utilized to detect the time of arrival of photons. Lastly, we provide the practical key rate formula for non-decoy and decoy-state methods.

2.2 Generic QKD protocol

In a generic QKD protocol, such as the prepare and measure (P&M) scheme, Alice and Bob exploit two communication channels: an insecure quantum channel and an authenticated classical channel. A quantum channel transmits signal states, which an eavesdropper usually has complete control over it. The classical channel is authenticated such that the eavesdropper can only listen to the communication but cannot modify the messages being sent between Alice and Bob.

2.2.1 Quantum phase

During the quantum phase, Alice and Bob use various properties of photons to encode classical information. They utilize the quantum channel to transmit quantum mechanical signals and perform measurements. Below, we describe three subprotocols that take place in the quantum phase for conventional and MDI QKD schemes.

2.2.1.1 Conventional QKD protocol

Signal preparation Alice prepares randomly a signal state from orthonormal basis $\beta_k := \{|\psi_k\rangle, p_{\beta_k} : k \in \mathcal{K}_A := \{0, \dots, d-1\}\}$ with probability p_{β_k} . She encodes the symbol k in the signal state. Here d denotes the dimension of the Hilbert space, $\mathcal{H}_d$ of the orthonormal bases. The signal states are drawn from mutually unbiased bases (MUB) such that any basis states $|\psi_k^{\beta_0}\rangle$ and $|\psi_k^{\beta_1}\rangle$ from MUBs β_0 and β_1 , respectively satisfy the condition

$$|\langle \psi_k^{\beta_0} | \psi_k^{\beta_1} \rangle|^2 = \frac{1}{d}. \quad (2.1)$$

The protocol can be implemented with a minimum set of two (2) up to $d+1$ MUBs.

Transmission Alice sends the states to Bob via an insecure quantum channel.

Measurement: Bob performs measurements on incoming signal states by means of positive operator valued measure (POVM) $M_B = \{B_{\tilde{k}}\}, \tilde{k} \in \mathcal{K}_B := \{0, \dots, d-1\}$.

2.2.1.2 Measurement device independent QKD protocol

Signal preparation and transmission Alice prepares a state from an ensemble $\beta_k := \{|\psi_k\rangle, p_{\beta_k} : k \in \mathcal{K}_A := \{0, \dots, d-1\}\}$ with probability p_{β_k} and sends it through an insecure quantum channel to an untrusted third-party Charlie. Similarly, Bob prepares a state from an ensemble $\beta_k := \{|\psi_k\rangle, p_{\beta_k} : k \in \mathcal{K}_B := \{0, \dots, d-1\}\}$ and sends it to Charlie.

Measurement Upon receipt of the states, Charlie let them interfere in the symmetric beam-splitters and perform the Bell state measurement. For each run, he publicly informs Alice and Bob whether or not his measurement is successful. After N repetition of the steps in the quantum phase, Alice and Bob continue to the classical post-processing part of the protocol.

2.2.2 Classical post processing

Parameter Estimation Without loss of generality, in this thesis, unless otherwise stated, we assume that Alice and Bob use standard basis, usually the Z (β_0) basis, to extract the key and use other bases for bounding Eve's information. From the cases where they used the key basis β_0 , Alice and Bob randomly select a subset $m_1 = Np_{\beta_0}^2$ out of N rounds to estimate the error rate, $e = r_1/m_1$. Here, r_1 corresponds to the number of mismatches. Similarly, in the cases where they both use the same basis from the remaining d MUBs, Alice and Bob randomly pick a fixed number $m_2 = Np_{\beta_k}^2$. The number of incompatible measurements r_2 yields the error rate $\bar{E} = r_2/m_2$. If the two error rates e and $\bar{E}$ are above the tolerable error threshold, they abort the protocol; otherwise, they proceed with other steps of the protocol.

Sifting: Alice and Bob throw away some rounds with unmatched bases from the remaining $N - (m_1 + m_2)$ signals according to the public announcement. Let n represent the number of remaining key symbols. Alice and Bob's private raw data symbols are then given by $\mathbf{k} \in \{0, 1, \dots, d-1\}^n$ and $\tilde{\mathbf{k}} \in \{0, 1, \dots, d-1\}^n$, respectively.

Key map: Alice applies a key map by keeping only the outcomes from the key basis (Z basis) as the secret key string $z \in \{0, 1, \dots, d-1\}$.

Error correction: Bob obtains an estimate $\tilde{z}$ of z using an information reconciliation scheme. Alice randomly hashes her key string and sends the hash value to Bob. Bob uses the same hash function to obtain his hash value and compares it to the one sent by Alice.

Privacy amplification: Alice and Bob use two-universal hashing to transform their strings z and $\tilde{z}$ into secret keys S_A and S_B of length ℓ .

2.3 Security of QKD

The security of QKD protocols hinges on the fact that an eavesdropper attempting to gain information about the transmitted quantum states introduces some errors due to the laws of quantum physics. Below, we describe the underlying principles which form the basis for QKD security.

2.3.0.1 The no cloning theorem

The no-cloning theorem asserts that it is impossible to duplicate a random unknown quantum state [8]. Consider a quantum cloning machine represented by unitary operator $\mathcal{U}$ that is capable to produce the copies of $|0\rangle$ and $|1\rangle$ according to the following unitary evolution processes

$$|0\rangle_u \xrightarrow{\mathcal{U}} |0\rangle_v \otimes |0\rangle_d \quad (2.2)$$

$$|1\rangle_u \xrightarrow{\mathcal{U}} |1\rangle_v \otimes |1\rangle_d \quad (2.3)$$

The superscript u denotes the initial state, v is the final state, and d corresponds to the duplicate state. Note that $\mathcal{U}$ is independent of the input states $|0\rangle$ and $|1\rangle$ as the copying machine does not have prior knowledge of the state. However, if the same cloner machine is applied to the linear superposition $\alpha|0\rangle + \beta|1\rangle$ of the two orthogonal states (where α and β are complex amplitudes of the states), then by the linearity of quantum mechanics, one obtains from Eqs. (2.2) and (2.3) that

$$(\alpha|0\rangle + \beta|1\rangle)_u \xrightarrow{\mathcal{U}} \alpha|0\rangle_v \otimes |0\rangle_d + \beta|1\rangle_v \otimes |1\rangle_d. \quad (2.4)$$

However, according to the operation of the quantum cloning machine, one should instead obtain the following result $(\alpha|0\rangle + \beta|1\rangle)_v \otimes (\alpha|0\rangle + \beta|1\rangle)_d$. Based on these results, one can conclude that whenever $\alpha, \beta \neq 0$, an arbitrary quantum state cannot be perfectly cloned.

2.3.0.2 Heisenberg Uncertainty Principle

The uncertainty principle posits that a measurement of one quantum observable inherently leads to uncertainty in determining other conjugate properties of the system [202]. This means that it is impractical to measure simultaneously the values of non-commuting observables on a single copy of a quantum state with perfect accuracy. For any two arbitrary quantum mechanical observables X and Y , the uncertainty principle establishes that

$$\langle \Delta X \rangle \langle \Delta Y \rangle \geq \frac{1}{2} \| \langle [X, Y] \rangle \|, \quad (2.5)$$

where ΔX and ΔB are standard deviations of observables X and Y , respectively. The notation $\langle \cdot \rangle$ denotes the expectation value of the observables, $[\cdot, \cdot]$ denotes the commutator and $\| \cdot \|$ represents the norm of the matrices. For incompatible observables, i.e., for observables X and Y such that $[X, Y] \neq 0$, reducing the uncertainty ΔX of X forces the uncertainty ΔY of Y to increase, and vice versa. Thus, the observables X and Y cannot be simultaneously measured to arbitrary precision. In quantum communication, these observables may correspond to the phase and excitation number of a harmonic oscillator, the angle and the orbital angular momentum of a particle, and orthogonal components of spin angular momentum.

2.3.1 Security definition

Typically, secret keys generated from a QKD protocol are used in cryptographic applications such as one-time pad encryption and digital signature schemes where an ideal key is required for message encryption [203]. This requirement relates to the concept of universal composability, which defines the security of a protocol with respect to the ideal functionality of a protocol [204–206]. A proper definition of security would allow the key generated by a real QKD protocol to deviate by a small parameter ε from a perfect key generated by an ideal protocol. The notion of ε -indistinguishability between real and ideal protocols is characterized by correctness, secrecy and robustness criteria. For practical scenarios, these requirements are quantified separately as follows.

2.3.1.1 Correctness

A QKD protocol is considered correct if $S_A = S_B$, for any possible attacking strategy by an eavesdropper [206]. A QKD protocol is ε_{cor} -correct if it deviates from the correct protocol by a small error probability, ε_{cor} , i.e.,

$$\Pr[S_A \neq S_B] \leq \varepsilon_{\text{cor}}. \quad (2.6)$$

The correctness of a QKD protocol is usually guaranteed by the error correction subprotocol.

2.3.1.2 Secrecy

A QKD is considered ε_{sec} -secret if an adversary has no knowledge of the generated key. Precisely, a protocol is ε_{sec} -secret if it is ε_{sec} -indistinguishable from a secret protocol, that is, it outputs ε_{sec} -secret keys with

$$(1 - p_{\text{abort}})\varepsilon \leq \varepsilon_{\text{sec}}, \quad (2.7)$$

with p_{abort} representing the probability that it aborts. The secrecy of a QKD protocol often comes from the two-universal family of hash functions used for the privacy amplification subprotocol. To define the secrecy of a key, we consider the quantum state $\rho_{S_A E}$ that describes the correlation between Alice's classical key S_A and adversary who holds a register E . The quantum register E , is held in some form of quantum state ρ_E . Additionally, she holds a copy of the register containing the classical information she acquired during public discussions. For any error probability ε_{sec} , a key S_A is ε_{sec} -secret with respect to an adversary who holds a register E if it is ε_{sec} -indistinguishable from an ideal protocol that is uncorrelated with the eavesdropper if it satisfies [206]

$$\frac{1}{2} \|\rho_{S_A E} - \rho_\Omega \otimes \rho_E\|_1 \leq \varepsilon_{\text{sec}}, \quad (2.8)$$

where ρ_Ω is the completely mixed state on the key space and $\|\cdot\|_1$ is the trace distance.¹

¹The 1-norm of a linear operator A is $\|A\|_1 = \text{Tr}(|A|) = \text{Tr}(\sqrt{AA^\dagger})$ and the trace distance of two linear operators A and B is $D(A, B) = \frac{1}{2}\|A - B\|_1$. The trace distance is used to measure the closeness between the density operators $\rho_{S_A E}$ and $\rho_\Omega \otimes \rho_E$ in Eq. (2.8).

2.3.1.3 Robustness

Lastly, robustness, ε_{rob} , is the probability that the protocol will abort even though the eavesdropper is inactive. Usually, QKD protocols assume a specific channel model that characterises their noise levels in the absence of an adversary. Therefore, at noise levels above a certain threshold, the protocol should automatically abort. Therefore, a trivial protocol that always aborts is robust according to the above definition.

In summary, if a protocol is ε_{cor} -correct, ε_{sec} -secret and ε_{rob} -robust then it is ε -secure with

$$\varepsilon_{\text{sec}} + \varepsilon_{\text{cor}} + \varepsilon_{\text{rob}} \leq \varepsilon. \quad (2.9)$$

2.3.2 QKD attacks

We discuss some of the attacks that may be executed by an eavesdropper that are considered when developing security proofs for QKD protocols.

2.3.2.1 Individual Attacks

In an individual attack, Eve attacks each of the systems transmitted by Alice to Bob independently and separately, employing the same strategy, and storing each ancilla in quantum memory. Eve is restricted to measuring her ancilla prior to the classical postprocessing [1]. This implies that Alice, Bob, and Eve share a product probability distribution of classical values at the beginning of classical postprocessing. While this kind of attack assists in gaining intuitions about the performance capabilities of the QKD protocols, the restriction to individual attacks is often not rigorous. Consequently, key rates would be overestimated, resulting in insecure keys being generated.

2.3.2.2 Collective attacks

In a collective attack, Eve identically interacts with each individual system sent by Alice to Bob. She keeps her ancilla systems in a quantum memory and may perform

any joint measurement on all intercepted states whenever she deems appropriate [1]. For instance, Eve can keep her ancillas in a quantum memory until a public discussion between Alice and Bob ends. She can also postpone measurement until the key is used in a cryptographic protocol. For most cases, the security analysis is restricted to an i.i.d. (individually and identically distributed) problem when the source in a QKD protocol produces i.i.d. states and Alice's and Bob's interactions with the quantum states are also i.i.d., thus the joint state between Alice, Bob and Eve can be assumed to be of form $\rho_{ABE}^N = \sigma_{ABE}^{\otimes N}$ for an individual copy state σ_{ABE} (Here A , B and E represent Alice, Bob and Eve's state components, respectively).

2.3.2.3 Coherent attacks

Coherent attacks are the most general type of attack. This type of attack does not limit Eve's interaction with signals. Rather than applying identical strategies to individual signals, Eve may attach an ancillary system to entire signals. Then, she can perform a joint unitary measurement with all the signal states and her ancilla. Moreover, she can measure her stored ancilla system at her convenience, perhaps after listening to all classical communication or even after the key has been used for cryptographic purposes. Therefore, in such a case, there is no restriction on the structure of the joint state ρ_{ABE}^N after N rounds.

2.3.3 Security against collective attacks

2.3.3.1 Infinite security analysis

In devising security proofs against various attacks, the indispensable quantity to explicitly determine is the secret key fraction. Thus, all QKD protocols must provide an explicit expression for the secret key fraction. In the asymptotic limit, where a sufficiently large number of signals are exchanged between Alice and Bob, the secret key fraction is expressed as [207]

$$r = \lim_{n \rightarrow \infty} \frac{\ell}{n}, \quad (2.10)$$

where ℓ represents the final secret key length and n refers to the raw key length. For collective attacks, the asymptotic secret key fraction, r in the limit of a key of infinite size under one-way classical postprocessing was established by Devetak and

Winter as [208]

$$r = I(A : B) - \max_{Eve} \chi(A : E), \quad (2.11)$$

where $I(A : B)$ represents the mutual information between Alice and Bob. The quantity is given by

$$I(A : B) = 1 - h(Q), \quad (2.12)$$

where h is the binary entropy. The second term in Eq. (2.11) is the Holevo Bound defined as follows:

$$\chi(A : E) = S(\rho_E) - \frac{1}{2} \sum_a S(\rho_{E|a}), \quad (2.13)$$

where $S(\cdot)$ denotes the von Neumann entropy, a corresponds to Alice's classical symbol selected with a probability distribution $p(a)$, $\rho_{E|a}$ represents Eve's ancilla state, and $\rho_E = \sum_a p(a) \rho_{E|a}$ is Eve's partial state.

2.3.3.2 Finite security analysis

We examine finite-key limit security analysis based on the tools developed in Refs. [207, 209]. The ultimate goal of finite-length key security is to determine the secret key fraction r based on a fixed number of signals. For instance, one can observe that the secret key fraction formula in Eq. (2.10) is impractical since in practice, all QKD protocols use finite resources. The asymptotic analysis assumes that the number of exchanged signals, N , is infinitely large, while in practical implementations, Alice and Bob exchange a fixed number of signals. Thus, we consider a simplified analysis assuming Alice, Bob, and Eve share quantum states with a tensor product structure. This is expressed as $\rho_{ABE}^N = \sigma_{ABE}^{\otimes N}$. We assume that n is the number of signals needed to form the raw key and m is the number of rounds used in the parameter estimation step. According to the notation adopted in the generic QKD protocol description (Section 2.2.2), we use Z to denote the raw key string. For $\varepsilon > 0$, that is, the error probability that the protocol deviates from the ideal protocol, the secret key fraction in the non-asymptotic limit can be expressed as

$$r = q[H_{\min}^{\bar{\varepsilon}}(Z^n | E^n) - \frac{2}{n} \log \frac{2}{\varepsilon_{PA}} - \text{leak}_{EC}], \quad (2.14)$$

where the first term $q = \frac{n}{N}$ means that n out of N signals form the raw key. The term $H_{\min}^{\bar{\epsilon}}(Z^n|E^n)$ corresponds to the smooth min-entropy which quantifies Eve's uncertainty. The parameter is lower bounded by the conditional von Neumann entropy of the individual-copy state according to the following

$$H_{\min}^{\bar{\epsilon}}(Z^n|E^n) \geq n \left(\min_{\sigma_{ZE} \in \Gamma_{\xi}} S(Z|E) - \delta \right), \quad (2.15)$$

where $\delta = 2 \log(d+3) \sqrt{\frac{\log(\frac{2}{\bar{\epsilon}})}{2}}$. The conditional von Neumann entropy function $S(Z|E)$ is minimized by states σ_{ZE} in the set Γ_{ξ} compatible with parameter estimation statistics. The minimization is done mainly to account for fluctuations in error rates due to finite-size effects. In particular, if the statistics λ_m are obtained by measuring m samples of σ_{ZE} according to a positive operator-valued measurement (POVM) with d possible outcomes then for any state σ_{ZE}

$$\Gamma_{\xi} := \{\sigma_{ZE} : \|\lambda_m - \lambda_{\infty}(\sigma_{ZE})\|_1 \leq \xi\}, \quad (2.16)$$

where $\lambda_{\infty}(\sigma_{ZE})$ denotes the statistics obtained in the limit of infinite measurements, and by the law of large numbers [201, 209]

$$\xi := \frac{1}{2} \sqrt{\frac{2 \ln(1/\varepsilon_{\text{PE}}) + d \ln(m+1)}{m}}, \quad (2.17)$$

where ε_{PE} is the probability that parameter estimation fails. The third term in Eq. (2.14) stems from the fact that, in the non-asymptotic scenario, the privacy amplification procedure may fail with probability ε_{PA} . Finally, the parameter leak_{EC} denotes the fraction to be removed in error correction. Generally, in practical implementations, error correction codes do not reach the theoretical Shannon limit. Typically,

$$\text{leak}_{\text{EC}} \approx f_{\text{EC}} H(Z_A|Z_B) - \frac{1}{n} \log \frac{2}{\varepsilon_{\text{EC}}}, \quad (2.18)$$

where $f_{\text{EC}} > 1$ is the error correction efficiency determined by the code employed and ε_{EC} is the probability that the error-correction procedure fails.

2.3.4 Security against coherent attacks using post-selection technique

Proving security against general or coherent attacks is usually a daunting task to deal with directly due to the flexibility given to an eavesdropper on allowed interactions with the signals. One way to overcome this is to consider a simplified approach of proving security under the assumption of collective attacks (subject to the protocol satisfying some requirement, e.g., permutation invariant among different rounds) and then lifting the proof to coherent attacks [210, 211]. The post-selection technique has been proposed as an approach that applies the same principle of translating the security against collective attacks to the security proof for coherent attacks. This section reviews the post-selection technique by Christandl, König and Renner [212]. The proof of the technique originates from the fact that any desired permutation invariant state can be post-selected from a fixed state [213]. Consider Hilbert spaces $\mathcal{H}$ and $\mathcal{H}'$ such that a transformation from one space to the other is represented by linear map $\Delta : \text{End}(\mathcal{H}^{\otimes n}) \mapsto \text{End}(\mathcal{H}')$. A linear map Δ is said to be permutation invariant if for any permutation π there exists a completely positive and trace preserving (CPTP) map K_π such that $K_\pi \circ \Delta = \pi \circ \Delta$. The post-selection theorem states that if Δ is permutation invariant, then

$$\|\Delta\|_\diamond = g_{n,d} \|\Delta \otimes (\text{id}_{\mathcal{R}})(\tau_{\mathcal{H}^n \mathcal{R}})\|_1, \quad (2.19)$$

where

$$g_{n,d} = \binom{n + d^2 - 1}{n} \leq (n + 1)^{d^2 - 1}, \quad (2.20)$$

$\|\cdot\|_\diamond$ is the diamond norm which is directly related to the maximum probability that a difference can be observed between the two CPTP maps $\text{End}(\mathcal{H}^{\otimes n})$ and $\text{End}(\mathcal{H}')$ and d denotes dimension of $\mathcal{H}$, id is the identity map on $\text{End}(\mathcal{R})$. The dimension of the purifying system $\mathcal{R}$ is sufficiently large ($\mathcal{R} \cong (\mathcal{H}^n)^{\otimes 3}$) and the state $\tau_{\mathcal{H}^n \mathcal{R}}$ is a purification of the de Finetti state defined as

$$\tau_{A^N B^N} = \int \sigma_{\mathcal{H}}^{\otimes n} \mu(\sigma_{\mathcal{H}}), \quad (2.21)$$

where $\mu(\cdot)$ is the measure brought about by the Hilbert Schmidt metric on the space of the density operator $\sigma_{\mathcal{H}}$, which represents an identically and independently prepared subsystem. Now, applying the theorem to the security of QKD, we suppose that the operation of an actual QKD protocol is represented by a CPTP map $\mathcal{E}$ and

that of an ideal QKD protocol is given by CPTP map $\mathcal{F}$. Given that $\Delta := \mathcal{E} - \mathcal{F}$ is permutation invariant, then if $\mathcal{E}$ is ε -secure against the collective attacks, we have that

$$\|\Delta\|_{\diamond} \leq \varepsilon(N+1)^{(d^4-1)} = \acute{\varepsilon}. \quad (2.22)$$

The important observation made in the above result is that the security parameter $\acute{\varepsilon}$ for coherent attacks is polynomially related to ε for collective attacks. The result implies that one can determine the security against coherent attacks for the actual QKD protocol represented by the map $\mathcal{E}$ from the security against collective attacks.

2.3.5 Security against coherent attacks via entropic uncertainty relation

Entropic uncertainty relations are also available techniques that can prove the security of QKD protocols in infinite and finite key analysis [214]. The entropic quantities usually employed for this purpose are the von Neumann entropy and entropic uncertainty relation for smooth entropies. Let us consider three quantum systems denoted by A , B and C . Also, these three systems are correlated in some way or possibly in an entangled state. Now, consider two POVMs $\mathcal{X} = \mathcal{M}_x$ and $\mathcal{Z} = \mathcal{N}_z$ acting on system A , and whose measurement outcomes are represented by X and Z , respectively. The uncertainty relation for the von Neumann entropy [215, 216] of the three systems is given by

$$H(X|B) + H(Z|C) \geq q, \quad (2.23)$$

where

$$q = \log_2 \left(\frac{1}{c} \right), \text{ where } c := \max_{x,z} \|\sqrt{\mathcal{M}_x} \sqrt{\mathcal{N}_z}\|_{\infty}^2. \quad (2.24)$$

Analogously, the entropic uncertainty relation for smooth entropies [217] is given by

$$H(X|B)_{\min}^{\varepsilon} + H(Z|C)_{\max}^{\varepsilon} \geq q, \quad (2.25)$$

where $\varepsilon \geq 0$ is defined as the smoothing parameter. In the discussion that follows, we focus on security proof in the finite key regime based on smooth entropies. In a QKD scenario, the system A corresponds to Alice's quantum systems used for key generation, B is Bob's system and C is Eve's system E . Consider that Alice and Bob establish a secret key from a shared quantum state of form $\rho_{AB}^{\otimes N}$ by performing measurements in the Pauli Z and X bases on their subsystems. Suppose that after

the quantum phase, Alice and Bob possess correlated key strings, $\mathbf{Z}$ and $\mathbf{Z}'$, about which an adversary may have acquired information $\mathbf{E}$. Then, Alice and Bob can perform a classical post-processing procedure (which comprises an error correction followed by a privacy amplification procedure), which distills a shared secret key of length [217]

$$\ell = H(\mathbf{Z}|\mathbf{E})_{\min}^{\varepsilon} - H(\mathbf{Z}|\mathbf{Z}')_{\max}^{\varepsilon}. \quad (2.26)$$

From the above expression, we observe that the key-length is basically obtained from the difference between the uncertainty that the eavesdropper has about Alice's key string $\mathbf{Z}$, determined in terms of the smooth min-entropy and the uncertainty that Bob has about $\mathbf{Z}$, represented by the smooth max-entropy. The second term of (2.26), $H(\mathbf{Z}|\mathbf{Z}')_{\max}^{\varepsilon}$, is closely related to the correlation strength between the raw keys. The correlation is obtained through the parameter estimation step by determining the error rate between $\mathbf{Z}$ and $\mathbf{Z}'$. Usually, the sample bits used for parameter estimation are allowed to disagree by, at most, a fraction ξ . Therefore, we have that

$$H(\mathbf{Z}|\mathbf{Z}')_{\max}^{\varepsilon} \leq nh(\xi + \mu), \quad (2.27)$$

where μ takes into account statistical fluctuations in the parameter estimation [218] and n is the number of bits in the raw key. Following the notion of composability discussed in Section 2.3.1, the correctness of the protocol is determined by the degree of correlation between Alice and Bob's data. Any incompatibilities between $\mathbf{Z}$ and $\mathbf{Z}'$ are corrected by the error correction procedure. This procedure has a failure probability of ε_{cor} . In practical implementations, the error correction procedure is imperfect, and its efficiency is typically represented as $f_{\text{EC}} > 1$ depending on the code used. By incorporating the contributions from imperfect error correction we have:

$$H(\mathbf{Z}|\mathbf{Z}')_{\max}^{\varepsilon} \leq \text{leak}_{\text{EC}} \approx f_{\text{EC}}nh(\xi + \mu) + \log_2 \left(\frac{2}{\varepsilon_{\text{cor}}} \right). \quad (2.28)$$

The first term in (2.26), $H(\mathbf{Z}|\mathbf{E})_{\min}^{\varepsilon}$, gives the mutual information between $\mathbf{Z}$ and the Eve's information $\mathbf{E}$. Since in this case, Eve's information is unknown to Alice and Bob; it becomes a daunting task to determine $H(\mathbf{Z}|\mathbf{E})_{\min}^{\varepsilon}$ from correlations between Alice and Bob's key strings $\mathbf{Z}$ and $\mathbf{Z}'$. To overcome this, one can consider a hypothetical protocol where Alice and Bob as usual select the X and Z bases following the predefined probability distribution. However, in this fictitious protocol, they always measure their quantum states using a basis complementary to the key basis, resulting in outcomes $\mathbf{X}$ and $\mathbf{X}'$, respectively. Now, to establish the secrecy of

the protocol, we may apply uncertainty relations for smooth entropies, which gives

$$H(\mathbf{Z}|\mathbf{E})_{\min}^{\varepsilon} \geq nq - H(\mathbf{X}|\mathbf{X}')_{\max}^{\varepsilon} = nq - H(\mathbf{Z}|\mathbf{Z}')_{\max}^{\varepsilon}, \quad (2.29)$$

where q is defined as in Eq. (2.24) and usually correspond to performance of Alice's apparatus [218]. The last equality in (2.29) stems from the fact that the basis was selected randomly for each qubit, and hence the correlation between $\mathbf{X}$ and $\mathbf{X}'$ is the same as the one between $\mathbf{Z}$ and $\mathbf{Z}'$. In addition to the uncertainty relation, the secrecy criterion of the composability definition is satisfied by employing the Quantum Leftover Hash Lemma [210, 219], which provides a direct operational significance to the smooth min-entropy. It asserts that, using a random universal₂ hash function, it is possible to obtain a Δ -secret key of length ℓ from $\mathbf{Z}$, where

$$\Delta \leq 2\varepsilon + \frac{1}{2}\sqrt{2^{\ell - H_{\min}^{\varepsilon}(\mathbf{Z}|\mathbf{E})}} \leq \varepsilon + \varepsilon_{\text{sec}}/2. \quad (2.30)$$

Using the bounds on smooth entropies we obtained from uncertainty relations (2.27) and (2.29), and error correction (2.28), we find that

$$\ell = n(q - h(\xi + \mu)) - \text{leak}_{EC}. \quad (2.31)$$

2.4 Practical QKD set up

The practical implementation of QKD consists of three main components: source, channel and detection. We present the widely used sources of photon signals, quantum channels, and detection systems in a real-life QKD implementation.

2.4.1 Sources of signal states

2.4.1.1 Weak coherent state source

The majority of QKD schemes are based on the use of single photons. Unfortunately, the single-photon signals are practically challenging to realize. The laser sources have been widely chosen as light sources due to their practicality and versatility. The laser sources are usually attenuated to produce weak coherent states with a low average number of photons μ , approximating single-photon Fock states [220].

The coherent state produced is defined as

$$|\sqrt{\mu}e^{i\theta}\rangle \equiv |\alpha\rangle = e^{-\mu/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle, \quad (2.32)$$

where θ is the phase of the coherent state, n is the photon number and $\mu = |\alpha|^2$ correspond to the intensity of the photon source. The phase factor $e^{i\theta}$ is accessible if a reference for the phase is available; otherwise, if the phase of the laser is randomized for each pulse, the produced coherent state is instead described by the mixture

$$\rho = \int_0^{2\pi} \frac{d\theta}{2\pi} |\alpha\rangle\langle\alpha| = \sum_n P(n|\mu) |n\rangle\langle n|. \quad (2.33)$$

The probability of finding n photons in such a coherent state is given by Poisson statistics

$$P(n, \mu) = \frac{\mu^n}{n!} e^{-\mu}. \quad (2.34)$$

2.4.1.2 Sources of Entangled Photons by Parametric Down-Conversion

Entangled photon pairs usually used for entanglement-based protocols or triggered (heralded) single-photon QKD are generated by spontaneous parametric down-conversion (SPDC) [1, 221]. In this process, a non-linear crystal is used to convert photons from a pump laser beam into pairs of photons referred to as signal and idler. During this process, the total energy and momentum are conserved. The generated photon pairs have a lower frequency than the pump due to non-linear interaction in the optical crystal. The two output modes are defined as

$$|\psi\rangle_{SPDC} = \sqrt{1 - \lambda^2} \sum_{n=0}^{\infty} \lambda^n |n_A, n_B\rangle, \quad (2.35)$$

where $\lambda = \tanh \gamma$ with γ proportional to the pump amplitude and $|n_A, n_B\rangle$ is the state with n photons in each the mode. The probability of finding n photons in such entangled state is given by

$$p(n) = \frac{(n+1)(\frac{\gamma}{2})^n}{(1 + \frac{\gamma}{2})^{n+2}}. \quad (2.36)$$

2.4.2 Quantum Channels

A quantum channel links the signal state preparation site and the measurement site. Two main types of quantum channels used in QKD are the optical fiber and free space. A key parameter that characterizes the quantum channel is the rate of loss, and studying the expected behavior of the channel is critical when designing a QKD setup. In a fiber channel, the loss is largely caused by random scattering processes. It has an exponential relation with the transmission distance l given by [222]

$$\eta_{\text{fib}} = 10^{-\alpha l/10}, \quad (2.37)$$

where α denotes the attenuation coefficient with a typical value of 0.2 dB/km for a telecommunication wavelength of around 1550 nm. Free-space links can be used in various scenarios, from short-distance point-to-point links with small telescopes mounted on rooftops to earth-satellite links or even space-space links with astronomical telescopes. Losses in these channels can be divided roughly into geometric and atmospheric contributions. For free space-based QKD, defining losses in terms of dB/km is generally challenging. Relative to atmospheric scattering, from a wavelength range of 700–10 000 nm we find several “atmospheric transmission windows,” e.g., 780–850 nm and 1520–1600 nm, which have an attenuation < 0.1 dB/km in clear weather [222]. The adverse weather conditions contribute heavily to such losses.

2.4.3 Detectors

A quantum phase of a QKD process is complete when Bob’s side detects signals. This can generally be accomplished through various methods, such as photomultipliers or avalanche diodes. Multiple factors influence detector performance, such as quantum detection efficiency, signal-to-noise ratio, and recovery time [220].

2.4.3.1 Avalanche Photodiodes (APDs)

The APDs are commonly used single-photon detectors in the field of cryptography. The detectors are designed from silicon, germanium, and indium gallium arsenide with a choice of material depending on the wavelength to be detected.

For QKD purposes, the APDs are usually operated in the Geiger gated mode [1, 220]. In this mode, the APD is set below the breakdown voltage and momentarily raised above the breakdown voltage when the signal photon is about to arrive. A single photon can then trigger an avalanche of millions of electrons and generate a macroscopic current pulse. After detecting an event, the avalanche is stopped, gated to lower dark counts, and APD is ready for the next count.

2.4.4 Practical QKD key rate

We have seen in Sections (2.3.3), (2.3.4) and (2.3.5) where we consider security proofs that the secret key fraction r is an indispensable parameter in guaranteeing the security of QKD. However, in practical QKD, another set of parameters to consider is the gain Q and the sifting factor q . The latter depends partially on the nature of the protocol, while the former is largely dependent on the details of the setup. These details include the repetition rate of the source, losses in the channel, efficiency and dead time of the detectors, possible duty cycle, etc. The practical key rate, R , is obtained from three terms: the secret key fraction r , the sifting factor, q , and the gain Q . This section is devoted to a detailed study of parameter Q and how it contributes to the final practical secret key rate. We, therefore, start with this description.

Concerning the preparation device, we assume that the single photons are generated using highly attenuated lasers and SPDC, which have the following photon number distributions: $p(n) = \mu^n e^{-\mu} / n!$ and $p(n) = (n+1)(\frac{\mu}{2})^n / (1 + \frac{\mu}{2})^{n+2}$, respectively. The channel loss is characterized by transmittance denoted by η_{ch} and related to the transmission distance by a loss attenuation coefficient α measured in dB/km. For a detection system, the parameters of interest are as follows [223].

- The detection efficiency, η_{det} which comprises of detector efficiency and the internal transmission efficiency of optical components inside the measurement site.
- Dark count rate P_d , which is calculated by adding up the dark count rate contributions from all detectors used in a QKD system.
- Intrinsic detector error probability e_d , which characterizes the misalignment and stability of the optical system.

Key exchange statistical parameters are basically detection and error rates. For detection rate at the measurement site, the first contributing parameter is total transmittance, η given by [223]

$$\eta = \eta_{\text{det}}\eta_{\text{ch}}, \quad (2.38)$$

where η_{ch} represents the quantum channel transmittance. Usually, in the simulation, the n photons in the n -photon signal pulse are assumed to behave independently, hence the transmittance of the n -photon signal pulse is given by

$$\eta_n = 1 - (1 - \eta)^n. \quad (2.39)$$

The transmittance provides the conditional probability of a detection event at the measurement site. However, a more appropriate parameter to describe detection events is the yield, Y_n for an n -photon signal. The yield comprises of detection events that emanate from the dark counts and the true signals and is given by

$$Y_n = P_d + \eta_n - P_d\eta_n. \quad (2.40)$$

From the yield, one can obtain the gain, Q_n which represents the probability that n -photon signal pulses sent through the quantum channel get detected at the measurement site. The gain of n -photon signals is given by

$$Q_n = Y_n p(n). \quad (2.41)$$

Then, the overall gain is obtained from the summation of Q_n s as

$$Q = \sum_{n=0}^{\infty} Y_n p(n). \quad (2.42)$$

The error rate on n -photon signals is given by

$$e_n = \frac{1/2P_d + e_d\eta_n}{Y_n}, \quad (2.43)$$

where the factor $1/2$ stems from the fact that error rate due to background counts is assumed to be random, hence assigned a 50% occurrence probability. Then the overall quantum bit error rate (QBER) is given by

$$E = \frac{1}{Q} \sum_{n=0}^{\infty} e_n Y_n p(n). \quad (2.44)$$

The practical key rate is thus given by

$$R = q\{Q(I_E - \text{leak}_{EC})\}, \quad (2.45)$$

where I_E is Eve's information which depends on the security proof method employed, and $\text{leak}_{EC} = f_{EC}H(E)$.

2.4.4.1 Decoy state method

The decoy state method was first proposed by Hwang [49] to guard against the PNS attack and enhance the security of the coherent state QKD. In this section, we exploit the decoy method of [50, 223] to describe the performance of a practical QKD protocol. The idea of decoy states is that Alice adjusts the laser intensity randomly during the protocol; at the end of the quantum signal exchange, she will disclose which state she sent in each run. Here, we consider a decoy scheme implemented with finite decoy states. In particular, Alice randomly prepares the photons using three different intensities (μ, ν, ω) where μ is the intensity for signal states, ν for decoy states, and ω for vacuum states [223]. The three intensities are usually selected with the probabilities $P_\mu > P_\nu > P_\omega$ where P_μ, P_ν and P_ω correspond to the probabilities for signal, decoy and vacuum states respectively. The signal states obtained with intensity μ are used for generating the final key. Decoy states acquired from intensity ν are for bounding Eve's knowledge to the key. Thus, the key generation rate for the decoy state-based protocol is given by

$$R = q[Q_\omega + Q_{\mu,1}^Z(I_E^U - \text{leak}_{EC})], \quad (2.46)$$

where upper bound, I_E^U is obtained from the upper bound for error rate in

the Z basis, $e_1^{Z,U}$ for single photon components. The error rate is expressed as

$$e_1^{Z,U} = \frac{E_\mu^Z Q_\mu^Z - e_0 Q_\omega^Z p(\mu|0)}{Y_{1,L} p(\mu|1)}, \quad (2.47)$$

where

$$Y_{1,L} = \frac{p(\mu|2)[Q_\nu^Z - p(\nu|0)Q_\omega^Z] - p(\nu|2)[Q_\mu^Z - p(\mu|0)Q_\omega^Z]}{p(\mu|2)p(\nu|1) - p(\mu|1)p(\nu|2)}. \quad (2.48)$$

Here Q_ω , Q_μ and Q_ν correspond to the gains for photon states obtained with intensities ω , μ and ν , respectively. The parameter $Q_{\mu,1}^Z$ corresponds to the gain for the single photon pulses prepared and measured in the Z basis. The probability $p(\gamma|n)$ with $\gamma \in \{\omega, \mu, \nu\}$ represents the photon number distribution for different intensities.

Security of six state SARG04 protocol with post-selection technique

3.1 Introduction

This chapter provides a finite security analysis of the six-state SARG04 protocol using a post-selection technique [212]. The SARG04 protocol [12] was developed in an attempt to combat the photon number splitting (PNS) attacks [10, 11]. The SARG04 protocol generates the secret key by encoding information in a pair of non-orthogonal states. The security assertion with this type of encoding comes from the fact that a protocol using N states for encoding can only result in unambiguous state discrimination if at least $N - 1$ copies of any of the states are in the possession of an eavesdropper [224]. For instance, in the original SARG04 protocol that utilises four states, Eve can determine with a certain probability the state sent by Alice from the pulses that contain at least three photons. As a result, protocols that use many states for encoding are more robust to PNS attacks since an eavesdropper needs more photons to unambiguously discriminate between states. On this basis, we study the security of the six-state SARG04 protocol, which produces a secure key using a source that emits a maximum of four photons per signal. As a result of its intriguing property of uncertainty in the discrimination of quantum states, non-orthogonal state coding has been applied to prove security against forgery attacks in quantum digital signature schemes [225, 226]. Moreover, it has been extensively investigated both theoretically [227–233] and experimentally [234, 235]. It should be noted that all these works considered the asymptotic key size regime when ob-

taining security bounds. However, the tools for computing information theoretical security in the finite-key regime have become available and proofs of security for finite length keys have been studied mostly under the assumptions of collective and coherent attacks for single-photon BB84 protocols [201, 218, 236–241], BB84 decoy state protocols [242–252] CV protocols [20, 21, 253–256] and for DPR protocols [257]. Other efforts have been made to improve the bounds on the secret key rates, for example, using a technique that uses uncertainty relations associated with smooth entropies [214, 217, 218]. This approach is elegant since it provides bounds for general kinds of attacks rather than collective attacks. However, this strategy works perfectly for protocols implemented with two mutually unbiased bases; thus, we cannot employ this strategy in the six-state SARG04 protocol because of the additional Y basis. Therefore, in this chapter, we apply the post-selection technique to derive the security bounds for the six-state SARG04 QKD protocol using finite resources. This protocol is robust against the zero-error type of attacks, such as PNS attacks, and this allows us to demonstrate information theoretical security against optimal coherent attacks under practical conditions where a source emits multiple photons. This chapter is based on the work in Ref. [196].

3.2 Review of the six-state SARG04 protocol

The six-state SARG04 protocol was first introduced in Refs. [224, 230]. This protocol uses the same six quantum states as the original six-state protocol [258]. Thus, the quantum state transmission and measurement phases are similar to those in the six-state protocol, and the experimental implementations are the same. The main difference lies in the classical post-processing phase. Furthermore, a secure key can be generated from a signal pulse containing a single photon to four photons in six-state SARG04 instead of a single photon pulse in the six-state protocol. The protocol can be described using the entanglement distillation procedure (EDP) as follows. The EDP utilizes four eigenstates $\{|0_x\rangle, |1_x\rangle\}, \{|0_z\rangle, |1_z\rangle\}$ from the X and Z bases, respectively for defining the rotation operators applied by Alice and Bob on their qubits. The rotation operations performed by Alice and Bob on their pairs of qubits are defined as: $R = \cos(\frac{\pi}{4})\mathbb{1} + \sin(\frac{\pi}{4})(|1_x\rangle\langle 0_x| - |0_x\rangle\langle 1_x|)$; $\Gamma_0 = \mathbb{1}$ is the identity rotation; $\Gamma_1 = \cos(\frac{\pi}{4})\mathbb{1} - i\sin(\frac{\pi}{4})\frac{Z+X}{\sqrt{2}}$ and $\Gamma_2 = \cos(\frac{\pi}{4})\mathbb{1} - i\sin(\frac{\pi}{4})\frac{Z-X}{\sqrt{2}}$. The protocol starts with Alice preparing the qubit pairs in the following state

$$|\psi\rangle_{AB}^{\otimes k} = (|0_z\rangle_A |\varphi_0\rangle_B^{\otimes k} + |1_z\rangle_A |\varphi_1\rangle_B^{\otimes k})/\sqrt{2}, \quad (3.1)$$

where $|\varphi_i\rangle = \cos(\frac{\pi}{8})|0_x\rangle + (-1)^i \sin(\frac{\pi}{8})|1_x\rangle$, $i \in (0, 1)$ and k corresponds to the number of photons emitted by Alice's photon source. After that, Alice applies the rotation operation $\Gamma_l R^m$ and sends the other qubit to Bob. Here, $l \in \{0, 1, 2\}$ and $m \in \{0, 1, 2, 3\}$. Following the receipt of qubits Bob executes the reverse operation $R^{-m'} \Gamma_l^{-1}$ followed by a filtering operation described by the Kraus operator $F = \sin(\frac{\pi}{8})|0_x\rangle\langle 0_x| + \cos(\frac{\pi}{8})|1_x\rangle\langle 1_x|$. Finally, Alice and Bob keep only the qubits where they used the same rotation operations to obtain a raw key.

3.3 Security against collective attacks

In this section we provide security bounds for six state SARG04 protocol in the asymptotic regime. The results from this section will form a basis for development of the secret key fraction formula for SARG04 in the finite key analysis regime. The security proof of SARG04 from the EDP based QKD described in the previous section goes as follows. Alice and Bob select a random subset of m qubit pairs and perform Z measurements on them. The measurement outcomes are announced publicly in order to estimate the bit error rate on the remaining pairs (key bits). Thanks to the random sampling theorem, this process provides an precise estimation of the bit error rate on the key bits, while the phase error rate is inferred from this estimation as shown in section 3.3.1 following methods derived in [230]. After estimation of the error rates, they choose a Calderbank-Shor-Steane (CSS) code that is sufficient to correct all bit and phase errors so that they share some maximally entangled states in the form of $|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$ where A and B correspond to Alice and Bob's qubits, respectively. Finally, by performing Z -basis measurement on those states, they share a secret key. From the EDP based on CSS codes, the asymptotic secret key fraction for the six-state SARG04 protocol using one way classical communication is given by [258, 259]

$$\begin{aligned} r &= 1 - H(X) - H(Z|X) \\ &= 1 - h(e_{\text{bit}}) - \sum_{k=1}^4 h(e_{\text{ph}}^k | e_{\text{bit}}). \end{aligned} \quad (3.2)$$

The parameter $H(X)$ correspond to uncertainty in the bit flip error patterns whilst $H(Z|X)$ is the conditional entropy used to determine phase error patterns conditioned on the knowledge of the bit error patterns. The parameters e_{bit} and e_{ph}^k correspond to the bit error rate and the phase error rate due to k -photon pulses.

It is important to note that a secure key can be extracted from six state SARG04 protocol executed with a source that emits up to four-photon signal pulse. Thus, the conditional entropy $h(e_{\text{ph}}^k | e_{\text{bit}})$ in Eq. (3.2) is the contributions to the secret key fraction from single-photon states up to four-photon states. We show security assertion of the foregoing statement based on the theorem that follows.

Theorem 1. *A protocol implemented with N -states and utilising non-orthogonal states for encoding can extract a secure key if a photon source emits less $N - 1$ -photon signal state.*

Proof. We prove that for protocols using N -states, Eve can obtain either partial or full information from states containing $N - 1$ -photons through the unambiguous state discrimination (USD) strategy [260, 261]. We demonstrate this with the six-state protocol, where the states used are $|+z\rangle$, $|-z\rangle$, $|+x\rangle$, $|-x\rangle$, $|+y\rangle$ and $|-y\rangle$ from the Pauli Z , X and Y eigen-bases, respectively. For the six-state SARG04 protocol, the USD attack compromises security when a source emits pulses with five photons. These pulses will be in one of the six states, $|\psi_1\rangle = |+z\rangle^{\otimes 5}$, $|\psi_2\rangle = |-z\rangle^{\otimes 5}$, $|\psi_3\rangle = |+x\rangle^{\otimes 5}$, $|\psi_4\rangle = |-x\rangle^{\otimes 5}$, $|\psi_5\rangle = |+y\rangle^{\otimes 5}$ and $|\psi_6\rangle = |-y\rangle^{\otimes 5}$. These states form a six-dimensional symmetric subspace, and since they are linearly independent [260], there exists a set of positive operator-valued measures (POVMs) that can distinguish between them with some probability of success p_{ok} . For definiteness, for any $i = \pm z, \pm x, \pm y$, let's define $|\psi_i^\perp\rangle \in (\mathbb{C}^2)_{sym}^{\otimes 5}$ as the state orthogonal to the five-photon state $|\psi_j\rangle^{\otimes 5}$, with $j \neq i$. The measurement that distinguishes between the five-photon states $|\psi_j\rangle^{\otimes 5}$ consists of seven positive operators that sum to the identity operator, $\mathbb{1}_{5,sym}$ in this symmetric subspace $(\mathbb{C}^2)_{sym}^{\otimes 5}$. These operators are denoted by

$$\begin{aligned} \mathcal{M}_i &= \frac{2}{3} |\psi_i^\perp\rangle \langle \psi_i^\perp| \\ \mathcal{M}_{inc} &= \mathbb{1}_{5,sym} - \sum_i \mathcal{M}_i. \end{aligned} \quad (3.3)$$

The probability of an inconclusive result from this measurement is given as

$$p_{inc} = \langle \psi_j |^{\otimes 5} \mathcal{M}_{inc} | \psi_j \rangle^{\otimes 5} = \frac{1}{2}. \quad (3.4)$$

Thus, the measurement is optimal if we restrict that the probability of a conclusive result is the same for all six states being distinguished. It has been shown in [261, 262] that the maximal probability of unambiguous discrimination is equal to

the reciprocal of the maximum eigenvalue of the operator

$$\frac{1}{6} \sum_{i=\pm z, \pm x, \pm y} (|\psi_i^\perp\rangle\langle\psi_i^\perp|), \quad (3.5)$$

which gives $p_{ok} = \frac{1}{3}$. From this, it follows that Eve can gather full information by blocking pulses containing all the one-photon pulses, two-photons pulses, three-photon pulses, four-photon pulses and a third of the five-photon pulses, by performing the PNS attack which is described by the following steps. (a) She measures the number of photons in a pulse; (b) she throws away all pulses containing less than five photons; (c) on the pulses containing at least 5 photons, she executes a measurement $\mathcal{M}$, and if the result is conclusive (which happens with probability $p_{ok} \gtrsim \frac{1}{3}$) she prepares a photon in a state that she just learnt and sends it to Bob. This attack is referred to as an intercept-resend with unambiguous discrimination (IRUD) attack. It is clear from IRUD attack that six state SARG04 can extract a secure key up to four-photon pulse contributions.

3.3.1 Estimation of error rates

Due to the symmetry of the protocol and assumptions based on collective attacks by Eve, Alice and Bob's systems are described by a Bell diagonal density matrix, ρ_{AB} which can be expressed in terms of four orthogonal Bell states given by

$$|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \text{ and } |\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle).$$

If the initial state prepared by Alice is $|\Phi^+\rangle$, after applying projective measurements represented by Pauli operators, X , Y , and Z , then the probability of getting only a bit flip error is $\Pr_X = \text{Tr}(\rho_{AB}|\Psi^+\rangle\langle\Psi^+|)$ and the probability of getting only a phase flip error corresponds to $\Pr_Z = \text{Tr}(\rho_{AB}|\Phi^-\rangle\langle\Phi^-|)$. Finally, the probability of both the phase and bit flip errors is given by $\Pr_Y = \text{Tr}(\rho_{AB}|\Psi^-\rangle\langle\Psi^-|)$. The bit error rate is therefore given by

$$e_{\text{bit}} = \Pr_X + \Pr_Y,$$

and the phase error rate is expressed as

$$e_{\text{ph}} = \Pr_Z + \Pr_Y.$$

Let $\delta = \Pr_Y$ be the probability that both phase and bit flip errors occur. This probability quantifies the mutual information between phase flip errors and bit-flip errors, and it can be used to estimate the phase error rate from the bit error rate [230]. The relationship between phase error rate and bit flip error rate for one-photon part is given by

$$e_{\text{ph}}^1 = \frac{3}{2}e_{\text{bit}}, \quad \delta = \frac{3}{4}e_{\text{bit}}. \quad (3.6)$$

For the two-photon part, the relationship between the error rates is expressed as

$$e_{\text{ph}}^2 = \frac{2 - \sqrt{2}}{4} + \frac{3}{2\sqrt{2}}e_{\text{bit}}, \quad \delta = \frac{4 + \sqrt{2}}{8}e_{\text{bit}}. \quad (3.7)$$

In the case of three photons emitted by the source, the error rates are given by

$$e_{\text{ph}}^3 = \frac{1}{4} + \frac{3}{4}e_{\text{bit}}, \quad \frac{1}{2} \leq \delta \leq \frac{3}{4}e_{\text{bit}}. \quad (3.8)$$

Finally, for the four-photon part, the error rates are expressed as

$$\begin{aligned} e_{\text{ph}}^4 &= \min_x \{xe_{\text{bit}} + f(x)\} \quad \forall x, \\ \frac{2 - 2\sqrt{2}}{4}e_{\text{bit}} &\leq \delta < \frac{4 + \sqrt{2}}{8}e_{\text{bit}} \\ \text{where } f(x) &= \frac{6 - 4x + \sqrt{6 - 12\sqrt{2}x + 16x^2}}{12}. \end{aligned} \quad (3.9)$$

The conditional entropy $h(e_{\text{ph}}^k | e_{\text{bit}})$ quantifies the amount of information that Eve has on the error-corrected key. It is given by

$$h(e_{\text{ph}}^k | e_{\text{bit}}) = - \sum p(e_{\text{bit}}, e_{\text{ph}}^k) \log_2 \left(\frac{p(e_{\text{bit}}, e_{\text{ph}}^k)}{p(e_{\text{bit}})} \right), \quad (3.10)$$

which can be explicitly expressed as

$$\begin{aligned} h(e_{\text{ph}}^k | e_{\text{bit}}) &= - (1 + \delta - e_{\text{bit}} - e_{\text{ph}}^k) \log_2 \left(\frac{1 + \delta - e_{\text{bit}} - e_{\text{ph}}^k}{1 - e_{\text{bit}}} \right) \\ &\quad - (e_{\text{ph}}^k - \delta) \log_2 \left(\frac{e_{\text{ph}}^k - \delta}{1 - e_{\text{bit}}} \right) - (e_{\text{bit}} - \delta) \log_2 \left(\frac{e_{\text{bit}} - \delta}{e_{\text{bit}}} \right) \\ &\quad - \delta \log_2 \left(\frac{\delta}{e_{\text{bit}}} \right). \end{aligned} \quad (3.11)$$

3.3.2 Bound on the finite secret key rate

It is important to note that the secret key fraction formula for six state SARG04 derived in the previous section is only valid under assumption that Alice and Bob exchange infinite number of signals. In this section we show modifications to the formula for secret key fraction r introduced by finite security analysis, where Alice and Bob perform a total number of N measurements. After the parameter estimation and sifting phase, the parties remain with n raw bits in which the final key of length ℓ is distilled through error correction and privacy amplification. We consider the six-state SARG04 coding with asymmetric bases choice by Alice. We write p_Z the probability that the Z basis is chosen and $p_c = \frac{1-p_Z}{2}$ the probability that the bases complementary to the Z basis are chosen. However, Bob is restricted to always choose the bases with uniform probability $p_{\text{Bob}} = \frac{1}{3}$. Therefore, denoting N as the length of Alice's and Bob's qubit pairs before sifting, the raw key will be of length $n = \frac{1}{2}Np_{\text{Bob}}p_Z$, Eve's information is estimated on a sample consisting of $m = \frac{1}{2}p_{\text{Bob}}Np_c$. Here the factor $\frac{1}{2}$ corresponds to the probability that detection leads to conclusive results (which correspond to successful filtering in the EDP protocol). The finite secret key fraction for the six-state SARG04 protocol under collective attack sketched along the lines in Ref. [238] is now reformulated in this form

$$r_{\text{col}} = q \left[\min_{\sigma_{ABE} \in \Gamma_\xi} H(A|E) - H(A|B) - \frac{1}{n} \log \frac{2}{\varepsilon_{\text{EC}}} - \frac{2}{n} \log \frac{1}{\varepsilon_{\text{PA}}} - (2 \log d + 3) \sqrt{\frac{\log(\frac{2}{\varepsilon})}{n}} \right], \quad (3.12)$$

where the first term $q = \frac{n}{N}$ means that n out of N signals form the raw key, and the value d represents the dimension of the quantum systems used in the protocol. The function, $\min_{\sigma_{ABE} \in \Gamma_\xi} H(A|E)$ is equivalent to summation of conditional entropies, $\sum_{k=1}^4 h(e_{\text{ph}}^k | e_{\text{bit}})$ from each k -photon contribution. This corresponds to the bits sacrificed to remove Eve's knowledge of the final key during privacy amplification. The function is minimized by states σ_{ABE} (purification of ρ_{AB}) in the set Γ_ξ compatible with parameter estimation statistics [237]. The minimization is done mainly to account for fluctuations in the error rates due to finite-size effects. To account for statistical fluctuations we leverage a quantitative version of the law of large numbers defined in [209, 237] which states that the measurement statistics $\lambda_\infty(\sigma_{ABE})$ obtained in the limit of infinite measurements must be close to statistics λ_m that are obtained by measuring m samples (the number of signals used for parameter

estimation) of σ_{ABE} according to a positive operator-valued measurement (POVM) with j possible outcomes. In particular, by the law of large numbers, for any ε_{PE} , we have that σ_{ABE} is contained in the set

$$\Gamma_\xi := \left\{ \sigma_{ABE} : \|\lambda_m - \lambda_\infty(\sigma_{ABE})\|_1 \leq \xi := \frac{1}{2} \sqrt{\frac{2 \ln(1/\varepsilon_{PE}) + j \ln(m+1)}{m}} \right\}, \quad (3.13)$$

except with error probability ε_{PE} . Basically Eq. (3.13) allows us to establish a relation between asymptotic values and the observed values (e_{bit}). Specifically, λ_m corresponds to observed error rate e_{bit} from the randomly sampled m data set. For the error rate, the number of outcomes for the POVM needed to estimate it equals 2 since the outcomes are ‘Alice’s bit = Bob’s bit’ and ‘Alice’s bit $\neq$ Bob’s bit’. Therefore, the upper bound on error rate, e_{bit} compatible with fluctuations is estimated as

$$e_{\text{bit}}^U = e_{\text{bit}} + \xi. \quad (3.14)$$

Then, from the upper bound on the bit error rate e_{bit} we can determine the upper bounds on the phase error rates, e_{ph}^k , due signal pulses with different photon number statistics. For instance, for the two-photon signal pulses, the upper bound is given by

$$e_{\text{ph}}^{2,U} = \frac{2 - \sqrt{2}}{4} + \frac{3}{2\sqrt{2}} e_{\text{bit}}^U, \quad \delta = \frac{4 + \sqrt{2}}{8} e_{\text{bit}}^U. \quad (3.15)$$

In Eq. (3.12), the parameter $H(A|B)$ corresponding to $h(e_{\text{bit}})$ represents the fraction of bits that leaked to Eve during error correction. The term ε_{PE} is the failure probability of the parameter estimation step, and $\bar{\varepsilon}$ is the smoothing parameter that gives the accuracy of parameter estimation. Finally, the parameter ε_{EC} is the probability that the error correction procedure fails. Furthermore, ε_{PA} corresponds to a bound in which the privacy amplification procedure fails to distill a secure key. These probabilities are subject to the following constraint,

$$\varepsilon = \varepsilon_{PE} + \varepsilon_{EC} + \bar{\varepsilon} + \varepsilon_{PA}. \quad (3.16)$$

Here, ε is the overall security parameter corresponding to the most considerable failure probability allowed to distill a secure key from the protocol.

3.4 Post-selection technique: SARG04 protocol on multi-photons

In this section, we lift up the security bounds of the six-state SARG04 protocol obtained against collective attacks in the preceding section to coherent attacks by applying the post-selection technique proposed in [212].

Theorem 2. *The secret key fraction for six-state SARG04 protocol obtained under collective attacks can be lifted to the security against coherent attacks by applying the post-selection theorem [212] and yields;*

$$r_{coh} = r_{col} - \frac{2(d^4 - 1)\log_2(N + 1)}{N}. \quad (3.17)$$

Proof. In the composable framework of security, the operation of the six-state SARG04 protocol can be represented by a completely positive (CP) map $\mathcal{E}$ that takes the joint state $\rho_{A_1 B_1 \dots A_n B_n}$ of the particle pairs (A_i, B_i) as inputs and outputs the state ρ_{SC} of the key. The transcript C represents the communication exchanged over the classical channel. Let presume $\mathcal{S}$ is a map that takes as input the bit strings of the keys $\{S^A, S^B, C\}$ produced by the map $\mathcal{E}$ and output perfect keys $\{S'^A, S'^B, C\}$. In order to find the security, we compare this mapping for the six-state SARG04 protocol with the ideal mapping $\mathcal{F}$ of a protocol that outputs a perfect key. The ideal CP map $\mathcal{F}$ can be constructed by concatenating the map $\mathcal{S}$ with the map $\mathcal{E}$ i.e., $\mathcal{F} = \mathcal{S} \circ \mathcal{E}$.

Based on the security definition and the post-selection theorem [212], it can be argued that $\mathcal{E}$ is ε -secure for any attack by an adversary if

$$\|\mathcal{E} - \mathcal{F}\|_{\diamond} \leq \varepsilon. \quad (3.18)$$

The threshold on ε is given by the distance between two CP maps, which is computed by evaluating the deviation of key generated by the map $\mathcal{E}$ from a perfect key produced by the map $\mathcal{F}$. The input states of the map $\mathcal{E}$ are de Finetti Hilbert Schmidt states. The latter correspond to the mixture of states which has product form $\rho_{AB}^{\otimes N}$ prepared from a source that generates identical and independent copies of density operator ρ_{AB} . These particular states are expressed as

$$\tau_{A^N B^N} = \int \rho_{AB}^{\otimes N} \mu(\rho_{AB}), \quad (3.19)$$

where $\mu(\rho_{AB})$ is the measure on the space of ρ_{AB} brought about by the Hilbert Schmidt metric.

The result obtained from the comparison of the distance between the two permutations invariant CP maps $\mathcal{E}$ and $\mathcal{F}$ under the assumption of collective attacks can be translated into security against the optimal coherent attacks as stated initially in [263]. By applying Theorem 1 in [212] to our scenario implies that $\mathcal{E}$ is ε secure if

$$\Delta(\mathcal{E}, \mathcal{F})_{\rho_{A^N B^N}} \leq (N+1)^{(D^2-1)} \Delta(\mathcal{E}, \mathcal{F})_{\tau_{A^N B^N}}, \quad (3.20)$$

where $\Delta(\mathcal{E}, \mathcal{F})_{\rho_{A^N B^N}}$ is the diamond norm distance for the protocol taking as inputs arbitrary states $\rho_{A^N B^N}$. $\Delta(\mathcal{E}, \mathcal{F})_{\tau_{A^N B^N}}$ correspond to the diamond-norm distance for the protocol using de Finetti states. The N qubit pairs shared by Alice and Bob span the Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ which has dimension $D = d^2$. The security parameter ε_{coh} for optimal coherent attacks is therefore given by

$$\varepsilon_{\text{coh}} = \varepsilon(N+1)^{(d^4-1)}. \quad (3.21)$$

In order to compute the finite secret key fraction under coherent attacks, it is essential to remark that Eve holds the purification of Alice and Bob's density operator $\rho_{A^N B^N}$. This can be conveniently described under collective attacks where Eve holds purification of each subsystem ρ_{AB} . The joint state of N subsystems of unknown density operators ρ_{AB} which is correlated with Eve's system $\rho_E \in \{\mathcal{H}_E\}$ is described by de Finetti state

$$\tau'_{A^N B^N E^N} = \int \rho_{ABE}^{\otimes N} \mu(\rho_{ABE}). \quad (3.22)$$

Since Eve's attack is not restricted, she may also gain more information on the key as a consequence of holding the purification of the joint state of N systems $\tau'_{A^N B^N E^N}$. Let $\mathcal{H}_{E'}$ denote the Hilbert space in which the purification of the joint state resides. Then, to bound Eve's knowledge on the key considering optimal coherent attacks, we have to minimize the conditional entropy $H_{\min}^{\varepsilon_{\text{coh}}}(A^N | E^N E')$. The entropy is given by

$$H_{\min}^{\varepsilon_{\text{coh}}}(A^N | E^N E') \geq H_{\min}^{\varepsilon_{\text{coh}}}(A^N | E^N) - 2H(E'). \quad (3.23)$$

Due to restriction from the security parameter ε_{coh} the dimension of the Hilbert

space $\mathcal{H}_{E'}$ is bounded by $(N+1)^{d^4-1}$. This implies that $\mathcal{H}_{E'}$ can hold at most $\log_2(N+1)^{d^4-1}$ bits of information. Consequently, the conditional entropy $H_{\min}^{\epsilon_{\text{coh}}}(A^N|E^N E')$ can be rewritten as

$$H_{\min}^{\epsilon_{\text{coh}}}(A^N|E^N E') \geq H_{\min}^{\epsilon_{\text{coh}}}(A^N|E^N) - 2(d^4 - 1)\log_2(N+1). \quad (3.24)$$

The first term on the right-hand side of Eq. (3.24) is the conditional entropy for the collective attacks in Eq (3.12). The idea is then to compensate the extra information available to the Eve in the space $\mathcal{H}_{E'}$ by reducing the key size obtained from collective attacks with $2(d^4 - 1)\log_2(N+1)$ key bits. Therefore, the secret key fraction for coherent attacks can be formulated as

$$r_{\text{coh}} = r_{\text{col}} - \frac{2(d^4 - 1)\log_2(N+1)}{N}. \quad (3.25)$$

3.4.1 Simulation

The simulation results demonstrate the performance of the six-state SARG04 protocol under collective attacks and coherent attacks when we apply the post-selection technique. It can be observed that the six-state SARG04 protocol under collective attacks provides a better secret key fraction when compared to the same protocol under coherent attacks. Based on Figure 3.1, the protocol for collective attacks (i)

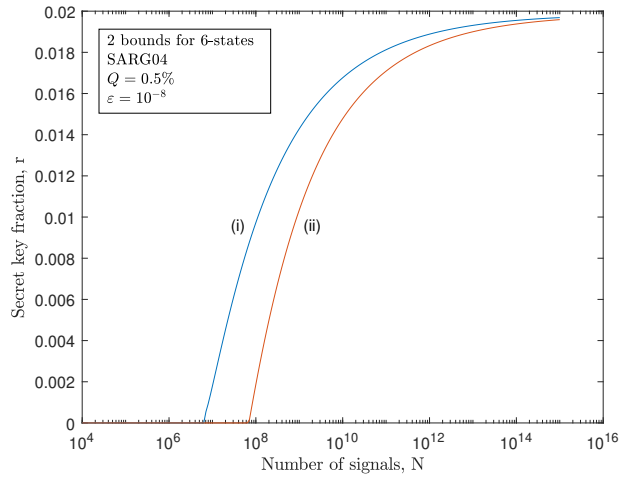


Figure 3.1: The plot of secret key fraction versus the number of signals N , for (i) six-state SARG04 protocol under collective attacks with four-photon source, (ii) six-state SARG04 protocol with four-photon source following post-selection technique.

requires fewer signals to achieve the positive secret key fraction as compared to the

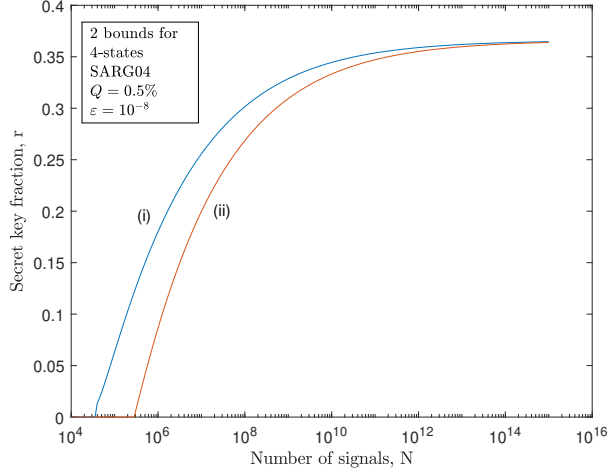


Figure 3.2: The plot of secret key fraction versus the number of signals N , for (i) four-state SARG04 protocol under collective attacks with two-photon source, (ii) four-state SARG04 protocol with two-photon source following post-selection technique.

one that uses post-selection technique (ii). However, the difference is not substantial, considering that the bounds obtained with the post-selection technique do not impose any restrictions on adversary attacks. As a result, this protocol provides a better alternative for proving the security of realistic QKD implementations.

We also compare our results for the six-state SARG04 protocol with the original four-state SARG04 protocol. This is shown in Figure 3.2. The original SARG04 protocol yields better secret key fraction with fewer signals than the six-state SARG04 protocol. When the post-selection technique is applied, a positive secret key fraction is obtained with approximately 2×10^5 signals for the four-state SARG04 protocol. In contrast, the six-state SARG04 protocol requires a minimum of 6×10^7 signals to achieve a positive secret key fraction. Nevertheless, in a realistic QKD scenario with an attenuated laser source, the six-state SARG04 protocol is more robust to the PNS attacks when compared to the original four-state SARG04 protocol. With the four-state SARG04 protocol, a secure key can be distilled from a source that emits at most two photons per pulse, whilst the six-state SARG04 protocol allows the secret key to be obtained even when a source produces pulses that contain four photons. It is worth noting that the six-state SARG04 protocol can be implemented with current state-of-the-art optical devices, as its experimental implementation is identical to that of the conventional six-state protocol. The numerical simulations presented in this work play a crucial role in determining the optimal experimental parameters and the necessary signals for generating a positive key rate. Notably,

the SARG04 protocol was successfully implemented experimentally in [264]. Additionally, the six-state protocol was demonstrated experimentally in [94], and the experimental setup used for its execution can be adapted to implement the six-state SARG04 protocol, with the only difference being the classical post-processing of the experimental data.

3.5 Conclusion

We have analyzed the security of the six-state SARG04 protocol by applying the post-selection technique for a finite number of resources. The technique translates security bounds restricted to collective attacks to the optimal coherent attacks by an adversary. Most security proofs have been derived based on the assumption of the availability of a perfect source and have been restricted to collective attacks. In contrast, our approach considers a multi-photon source and optimal coherent attacks as posited by the post-selection technique, enabling us to spell out the security bounds under realistic conditions. Furthermore, we compare the security bounds for the four-state protocol and six-state SARG04 protocol under collective attacks to the security bounds obtained after applying the post-selection technique when a finite number of resources are used. Our results demonstrate that the bounds for optimal attack are close to the bound for collective attack for a large number of signals. The six-state SARG04 protocol proves to be more robust to the PNS attacks when compared to the original four-state SARG04 protocol. When the four-state SARG04 protocol is implemented, a secure key can be distilled from a source that emits at most two photons per pulse. In contrast, the six-state SARG04 protocol allows the secret key to be obtained even when a source produces pulses that contain four photons. Thus, this demonstrates the power of the post-selection technique in deriving the security bounds for the six-state protocol when finite resources are used. This means it is possible to distill a secure, reasonable secret key from a reasonably good number of signals, even when considering the optimal attack by an adversary.

Three-party reference frame independent QKD

4.1 Introduction

One of the challenges in the practical implementation of QKD is the requirement of an aligned reference frame between the communicating parties [73]. For instance, alignment of polarization states for polarization encoding and interferometric stability for phase coding. These requirements have proven challenging to satisfy due to unstable fiber communication links and imperfections in measurement devices [265]. Efforts to address potential reference frame misalignment by encoding qubits with larger systems require the creation and manipulation of many photon entangled states that are very difficult to generate and are very sensitive to losses [74, 75, 77]. Fortunately, the reference frame independent (RFI) protocol was proposed by Laing et al. [73] to address this alignment problem. Since the inception of the RFI protocol, outstanding results have been achieved both theoretically [76, 78–92] and experimentally [93–101], thus demonstrating its capability to achieve a higher secure key rate under a varying reference frame.

In this chapter, we widen the reach of QKD by considering the RFI protocol employing two-qubit entangled photons to establish a secret key between three communicating parties. We show that the number of communicating parties can be extended further and still achieve a secret key rate and transmission distance comparable to the traditional two-party QKD. We also demonstrate the feasibility of multipartite

QKD and its potential for achieving global-scale quantum networks. Multipartite QKD schemes have also been shown to be robust in some noise regimes [266], making them secure compared to generating a multipartite secret key through many independent bipartite protocols. Moreover, we provide a composable finite-key analysis for the proposed three-party protocol implemented with decoy states based on entropic uncertainty relations. The entropic uncertainty relations are a direct and robust method for quantifying the information held by communicating parties and the eavesdropper. This method also provides tight bounds on the secret key rates obtained from finite resources and avoids estimates compared to preexisting approaches such as post-selection technique [212] and the de Finetti theorem [263], which provide pessimistic finite key rate estimates.

Moreover, our security analysis considers implementation with decoy states, making our proposed protocol robust against photon number splitting (PNS) attacks [11]. This allows us to demonstrate information theoretical security against general attacks under practical conditions where a source produces multiple photons. To account for statistical fluctuations in the finite regime, we employ the tail inequality for random sampling without replacement and multiplicative Chernoff bound proposed in Ref. [267], which provides the tightest bounds on expected and observed values. A large-deviation Chernoff bound [240] is another preexisting method used for statistical analysis, which is equally rigorous as the multiplicative Chernoff bound but fails to produce tight bounds on observed values in the high-loss regime leading to a rapid decrease in the achieved secret key rate. The Gaussian analysis method [223] is also comparable to the multiplicative Chernoff bound. However, it is not rigorous as it is limited to independently and identically distributed random variables. The tail inequality for random sampling without replacement provides the tightest bounds on observed error rates and avoids inequality scaling compared to pre-existing methods used in Refs. [240, 268]. This chapter is based on manuscript [197].

4.2 Operation of the proposed protocol

The proposed three-party RFI QKD protocol is described as follows. Alice starts by preparing a two-photon entangled state using a spontaneous parametric down-conversion (SPDC) source. She then applies polarization modulation in these entangled photons using the same basis chosen from three Pauli encoding bases, X ,

Y , and Z . To combat the PNS attack, Alice randomly prepares the photons using three different intensities (μ, ν, ω) where μ is the intensity for signal states, ν for decoy states, and ω for vacuum states [223]. The three intensities are selected with the probabilities $P_\mu > P_\nu > P_\omega$ where P_μ, P_ν and P_ω correspond to the probabilities for signal, decoy and vacuum states respectively. The two photons are sent to communicating parties, Bob and Charlie, via insecure quantum channels. Upon receipt of photons, they (Bob and Charlie) measure them using any of the three randomly selected measuring bases, $\{X, Y, Z\}$, to guess the Alice preparation basis. The signal states obtained with intensity μ are used for generating the final key, while decoy states acquired from the intensity ν are for bounding Eve's knowledge to the key. In the proposed protocol, Alice measures all the signal pulses, (μ) in the Z basis, and weak decoy pulses, ν in all bases $\{X, Y, Z\}$. Furthermore, in this protocol, Alice, Bob, and Charlie share a common aligned measurement basis $Z_A = Z_B, Z_A = Z_C$ while other measurement bases X and Y are allowed to slowly vary by an arbitrary angle β (See Figure 4.1). Due to drift in reference frames, the measurement bases complementary to the Z basis are given by

$$X_B = \cos \beta X_A + \sin \beta Y_A, \quad X_C = \cos \beta X_A + \sin \beta Y_A,$$

$$Y_B = \cos \beta Y_A - \sin \beta X_A, \quad Y_C = \cos \beta Y_A - \sin \beta X_A.$$

We consider the asymmetric basis choice in which the Z basis is chosen with probability $p_z > \frac{1}{2}$ and the complementary bases, $\{X, Y\}$ with probability $p_c = 1 - p_z$ [269]. The three parties uniformly choose a random bit $r_i \in \{0, 1\}$ to encode information for their chosen basis. The first steps of the protocol are repeated until they have exchanged enough qubits for the sifting process. Alice, Bob, and Charlie announce their basis choices over an authenticated classical channel and proceed with parameter estimation. The raw key is extracted from the cases where Alice prepared her states in the Z basis while Bob and Charlie measured their received qubits in the Z direction. Therefore, the quantum bit error rate is given by

$$E_{ZZZ} = \frac{1 - \langle Z_A Z_B Z_C \rangle}{2} \quad (4.1)$$

where Z_A represents that Alice sends the two states prepared in the Z basis while Z_B and Z_C denote that Bob and Charlie measure received states in the Z direction, respectively. The measurement results in the complementary bases are used to estimate the information that has leaked to Eve. The information is bounded by

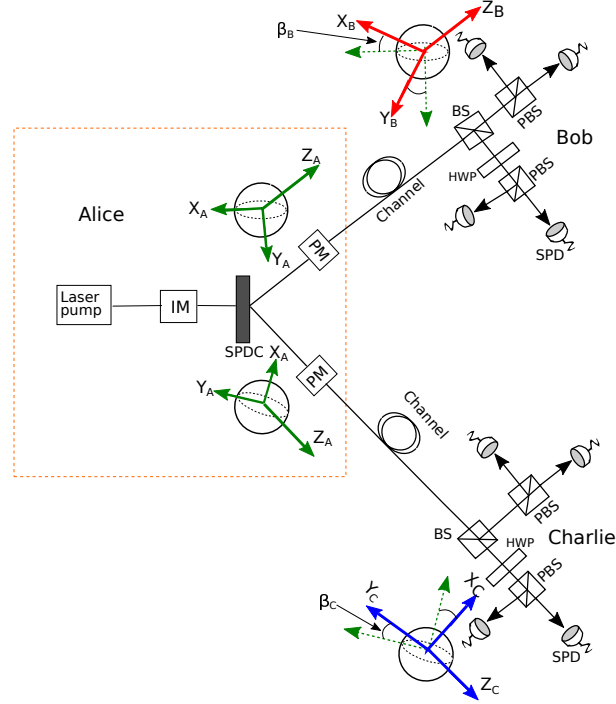


Figure 4.1: The schematic diagram of the three-party RFI-QKD protocol. Alice starts by preparing a two-photon entangled state using a spontaneous parametric down-conversion (SPDC) source. Next, the two photons are modulated into polarized states belonging to three bases $\{X, Y, Z\}$ using a polarization modulator (PM) and sent to Bob and Charlie through an insecure channel. The photons prepared in the X and Y basis experience misalignment by degree β_B and β_C for Bob and Charlie, respectively. The acronyms IM, BS, PBS, HWP, and SPD are intensity modulator, beam-splitter, polarizing beam-splitter, half-wave plate, and single-photon detector, respectively.

the statistical quantity C , defined as

$$C = \langle X_A X_B X_C \rangle^2 + \langle X_A Y_B X_C \rangle^2 + \langle X_A X_B Y_C \rangle^2 + \langle Y_A X_B X_C \rangle^2 + \langle Y_A Y_B X_C \rangle^2 + \langle Y_A X_B Y_C \rangle^2 + \langle Y_A Y_B Y_C \rangle^2 + \langle X_A Y_B Y_C \rangle^2, \quad (4.2)$$

where $\langle \Gamma_A \Gamma_B \Gamma_C \rangle$ (with $\Gamma \in \{X, Y\}$), corresponds to the expectation that Alice prepares two states in the basis Γ_A while Bob and Charlie measure received states in basis Γ_B and Γ_C , respectively. Furthermore, it can be shown that C is independent of the value β when substituting the relations X_B , Y_B and X_C , Y_C in Eq. (4.2). However, to get an accurate estimate of C , the angle β is assumed to vary slowly in time short enough to allow for the key exchange.

4.3 Security analysis

In this section we derive the secret key fraction, r for the three-party RFI-QKD and establish the security bounds by considering the collective attacks, where Eve applies the same attack to each system of Bob and Charlie. The security analysis is sketched along the lines in Ref. [73, 270]. The analysis is done in three steps as follows. In the first step, we derive the statistical parameter C which is used to bound Eve's knowledge of the key.

Theorem 1. *If we consider the state shared by Alice, Bob and Charlie to be described by density matrix ρ_{AbAcBC} which is diagonal in some Bell basis known to Eve, then the statistical parameter C is obtained from eigenvalues λ_i of the density matrix ρ_{AbAcBC} ;*

$$C = 4[(\lambda_1 - \lambda_2)^2 + 4(\lambda_3 - \lambda_4)^2 + 4(\lambda_5 - \lambda_6)^2 + (\lambda_7 - \lambda_8)^2 + (\lambda_9 - \lambda_{10})^2 + 4(\lambda_{11} - \lambda_{12})^2 + 4(\lambda_{13} - \lambda_{14})^2 + (\lambda_{15} - \lambda_{16})^2]. \quad (4.3)$$

Proof. We consider an entanglement-based protocol in which Alice, Bob and Charlie initially share an entangled state $|\phi^+\rangle_{AbAcBC} = \frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle)$ with the first two particles A_b and A_c belonging to Alice and last two particles, B and C are in possession of Bob and Charlie, respectively. Alice measures her qubits in the same direction using three Pauli basis $\{X, Y, Z\}$ while Bob and Charlie also measure their particles using the same mutually unbiased bases. This protocol is equivalent to the prepare and measure protocol described in Section 4.2. In this entanglement-based description, Alice performs measurement on two particles (which we refer to as b and c) to encode her bit of information, equivalent to preparing two states sent to Bob and Charlie in prepare and measure protocol. For collective attacks, the density matrix describing the state shared by Alice, Bob, and Charlie is diagonal in the GHZ state basis known to Eve and is written as

$$\begin{aligned} \rho_{AbAcBC} = & \mu_1|\phi^+\rangle\langle\phi^+| + \mu_2|\phi^-\rangle\langle\phi^-| + \mu_3|\psi^+\rangle\langle\psi^+| + \mu_4|\psi^-\rangle\langle\psi^-| + \mu_5|\Phi^+\rangle\langle\Phi^+| \\ & + \mu_6|\Phi^-\rangle\langle\Phi^-| + \mu_7|\Psi^+\rangle\langle\Psi^+| + \mu_8|\Psi^-\rangle\langle\Psi^-| + \mu_9|\varphi^+\rangle\langle\varphi^+| + \mu_{10}|\varphi^-\rangle\langle\varphi^-| \\ & + \mu_{11}|\Phi^+\rangle\langle\Phi^+| + \mu_{12}|\Phi^-\rangle\langle\Phi^-| + \mu_{13}|\Psi^+\rangle\langle\Psi^+| + \mu_{14}|\Psi^-\rangle\langle\Psi^-| \\ & + \mu_{15}|\chi^+\rangle\langle\chi^+| + \mu_{16}|\chi^-\rangle\langle\chi^-|, \end{aligned} \quad (4.4)$$

where $|\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|0000\rangle \pm |1111\rangle)$, $|\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|0001\rangle \pm |1110\rangle)$, $|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|0011\rangle \pm |1100\rangle)$, $|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|0100\rangle \pm |1011\rangle)$, $|\varphi^\pm\rangle = \frac{1}{\sqrt{2}}(|1000\rangle \pm |0111\rangle)$, $|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|0101\rangle \pm$

$|1010\rangle\rangle$, $|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|1001\rangle \pm |0110\rangle)$ and $|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|0010\rangle \pm |1101\rangle)$. The eigenvalues in Eq. (4.4) are complex numbers that satisfy the normalization condition

$$\sum_i^{16} |\mu_i|^2 = 1. \quad (4.5)$$

Based on the fact that C is invariant under the following transformations $X_{A_{b(c)}} \rightarrow -X_{A_{b(c)}}, X_B \rightarrow -X_B, X_C \rightarrow -X_C, Y_{A_{b(c)}} \rightarrow -Y_{A_{b(c)}}, Y_B \rightarrow -Y_B, Y_C \rightarrow -Y_C$, we can equivalently represent these transformations with the quantum operation $\rho_{A_b A_c B C} \rightarrow (Z_{A_b} \otimes Z_{A_c} \otimes Z_B \otimes Z_C) \rho_{A_b A_c B C} (Z_{A_b} \otimes Z_{A_c} \otimes Z_B \otimes Z_C)$. Thus, in the presence of such symmetry we can replace the state $\rho_{A_b A_c B C}$ by a mixture

$$\tilde{\rho}_{A_b A_c B C} = \frac{1}{2} \left(\rho_{A_b A_c B C} + (Z_{A_b} Z_{A_c} Z_B Z_C) \rho_{A_b A_c B C} (Z_{A_b} Z_{A_c} Z_B Z_C) \right). \quad (4.6)$$

The new mixed state does not change the measurement statistics for Alice, Bob and Charlie's measured values E_{ZZZ} and C . The state $\tilde{\rho}_{A_b A_c B C}$ can be explicitly written as

$$\begin{aligned} \tilde{\rho}_{A_b A_c B C} = & \mu_1 |\phi^+\rangle \langle \phi^+| + \mu_2 |\phi^-\rangle \langle \phi^-| + \left(\frac{a}{2} |\phi^-\rangle \langle \phi^+| + H.c \right) + \mu_3 |\psi^+\rangle \langle \psi^+| \\ & + \mu_4 |\psi^-\rangle \langle \psi^-| + \left(\frac{b}{2} |\psi^-\rangle \langle \psi^+| + H.c \right) + \mu_5 |\Phi^+\rangle \langle \Phi^+| + \mu_6 |\Phi^-\rangle \langle \Phi^-| \\ & + \left(\frac{c}{2} |\Phi^-\rangle \langle \Phi^+| + H.c \right) + \mu_7 |\Psi^+\rangle \langle \Psi^+| + \mu_8 |\Psi^-\rangle \langle \Psi^-| + \left(\frac{d}{2} |\Psi^-\rangle \langle \Psi^+| + H.c \right) \\ & + \mu_9 |\varphi^+\rangle \langle \varphi^+| + \mu_{10} |\varphi^-\rangle \langle \varphi^-| + \left(\frac{e}{2} |\varphi^-\rangle \langle \varphi^+| + H.c \right) + \mu_{11} |\Phi^+\rangle \langle \Phi^+| \\ & + \mu_{12} |\Phi^-\rangle \langle \Phi^-| + \left(\frac{f}{2} |\Phi^-\rangle \langle \Phi^+| + H.c \right) + \mu_{13} |\Psi^+\rangle \langle \Psi^+| + \mu_{14} |\Psi^-\rangle \langle \Psi^-| \\ & + \left(\frac{g}{2} |\Psi^-\rangle \langle \Psi^+| + H.c \right) + \mu_{15} |\chi^+\rangle \langle \chi^+| + \mu_{16} |\chi^-\rangle \langle \chi^-| + \left(\frac{h}{2} |\chi^-\rangle \langle \chi^+| + H.c \right), \end{aligned} \quad (4.7)$$

where $H.c$ denotes the complex conjugate of each matrix in the bracket. For ease of notation, let us denote $\tilde{\rho}_{A_b A_c B C}$ as $\tilde{\rho}(a, b, \dots, h)$. By computing $C = \sum_{\alpha_{A_b} \alpha_{A_c} \beta_B \delta_C} [\text{Tr}(\alpha_{A_b} \otimes \alpha_{A_c} \otimes \beta_B \otimes \delta_C \tilde{\rho}_{A_b A_c B C})]^2$ with $\alpha, \beta, \delta \in \{X, Y\}$ this yields

$$\begin{aligned} C = & 4[(\mu_1 - \mu_2)^2 + 4(\mu_3 - \mu_4)^2 + 4(\mu_5 - \mu_6)^2 + (\mu_7 - \mu_8)^2 + (\mu_9 - \mu_{10})^2 \\ & + 4(\mu_{11} - \mu_{12})^2 + 4(\mu_{13} - \mu_{14})^2 + (\mu_{15} - \mu_{16})^2 + \text{Im}(a)^2 + \text{Im}(b)^2 + \text{Im}(c)^2 \\ & + \text{Im}(d)^2 + \text{Im}(e)^2 + \text{Im}(f)^2 + \text{Im}(g)^2 + \text{Im}(h)^2]. \end{aligned} \quad (4.8)$$

This result is also attained for its conjugate $\tilde{\rho}(-a^*, -b^*, \dots, -h^*)$. By using the

same logic as before, it is not restrictive to analyze the mixture of $\tilde{\rho}(a, b, \dots, h)$ and $\tilde{\rho}(-a^*, -b^*, \dots, -h^*)$ which can be written as $\dot{\rho}_{AaBbC} = \frac{1}{2}[\tilde{\rho}(a, b, \dots, h) + \tilde{\rho}(-a^*, -b^*, \dots, -h^*)] = \tilde{\rho}(i\mathbf{A}, i\mathbf{B}, \dots, i\mathbf{H})$ to obtain the value of C . Here $\mathbf{A} = \text{Im}(a)$, $\mathbf{B} = \text{Im}(b)$, $\mathbf{H} = \text{Im}(h)$ and other imaginary values have the same meaning. The state $\dot{\rho}_{AaBbC}$ can be expressed as

$$\dot{\rho}_{AaBbC} = \sum_{k=1}^{16} \lambda_k |\Phi_k\rangle \langle \Phi_k|, \quad (4.9)$$

where $|\Phi_{1,2}\rangle = \frac{1}{\sqrt{2}}(e^{i\theta_1}|0000\rangle \pm e^{-i\theta_1}|1111\rangle)$, $|\Phi_{3,4}\rangle = \frac{1}{\sqrt{2}}(e^{i\theta_2}|0001\rangle \pm e^{-i\theta_2}|1110\rangle)$, $|\Phi_{5,6}\rangle = \frac{1}{\sqrt{2}}(e^{i\theta_3}|0011\rangle \pm e^{-i\theta_3}|1100\rangle)$, $|\Phi_{7,8}\rangle = \frac{1}{\sqrt{2}}(e^{i\theta_4}|0100\rangle \pm e^{-i\theta_4}|1011\rangle)$, $|\varphi_{9,10}\rangle = \frac{1}{\sqrt{2}}(e^{i\theta_5}|1000\rangle \pm e^{-i\theta_5}|0111\rangle)$, $|\Phi_{11,12}\rangle = \frac{1}{\sqrt{2}}(e^{i\theta_6}|0101\rangle \pm e^{-i\theta_6}|1010\rangle)$, $|\Psi_{13,14}\rangle = \frac{1}{\sqrt{2}}(e^{i\theta_7}|1001\rangle \pm e^{-i\theta_7}|0110\rangle)$ and $|\chi_{15,16}\rangle = \frac{1}{\sqrt{2}}(e^{i\theta_8}|0010\rangle \pm e^{-i\theta_8}|1101\rangle)$. The parameters are related as follows. Define $\dot{\mathbf{A}} = \sqrt{(\mu_1 - \mu_2)^2 + \mathbf{A}^2}$, then $\lambda_{1,2} = \frac{1}{2}(\mu_1 + \mu_2 \pm \dot{\mathbf{A}})$ and $\cos^2 \theta_1 = \frac{1}{2} + (\mu_1 - \mu_2)/\dot{\mathbf{A}}$. Similarly, if $\dot{\mathbf{B}} = \sqrt{4(\mu_3 - \mu_4)^2 + \mathbf{B}^2}$, then we have that $\lambda_{3,4} = \frac{1}{2}(\mu_3 + \mu_4 \pm \dot{\mathbf{B}})$ and $\cos^2 \theta_2 = \frac{1}{2} + (\mu_3 - \mu_4)/\dot{\mathbf{B}}$. The expressions for other eigenvalues and imaginary parts are calculated in a similar manner. This implies that the parameter C can now be expressed as

$$C = 4[(\lambda_1 - \lambda_2)^2 + 4(\lambda_3 - \lambda_4)^2 + 4(\lambda_5 - \lambda_6)^2 + (\lambda_7 - \lambda_8)^2 + (\lambda_9 - \lambda_{10})^2 + 4(\lambda_{11} - \lambda_{12})^2 + 4(\lambda_{13} - \lambda_{14})^2 + (\lambda_{15} - \lambda_{16})^2]. \quad (4.10)$$

In the second step, we now determine the relationship between parameter C and the error rate, E_{ZZZ} in the analogous manner to the method employed in Appendix A of [1]. To show the connection between two parameters, we leverage the restrictions that the eigenvalues λ_i have to satisfy the condition: $\sum \lambda_i = 1$ and yield the measured values E_{ZZZ} and C . Since the key is obtained from the measurements in computational basis (Z basis) this implies that $\lambda_1 + \lambda_2 = 1 - E_{ZZZ}$ and $\lambda_3 + \lambda_4 + \lambda_5 + \lambda_6 + \lambda_7 + \lambda_8 + \lambda_9 + \lambda_{10} + \lambda_{11} + \lambda_{12} + \lambda_{13} + \lambda_{14} + \lambda_{15} + \lambda_{16} = E_{ZZZ}$. The following parametrization is chosen so that it satisfies the above conditions;

$$\lambda_1 = (1 - E_{ZZZ}) \left(\frac{1+u}{2}\right), \lambda_2 = (1 - E_{ZZZ}) \left(\frac{1-u}{2}\right), \lambda_3 = \frac{1}{7}E_{ZZZ} \left(\frac{1+v}{2}\right), \lambda_4 = \frac{1}{7}E_{ZZZ} \left(\frac{1-v}{2}\right), \lambda_5 = \frac{1}{7}E_{ZZZ} \left(\frac{1+v}{2}\right), \lambda_6 = \frac{1}{7}E_{ZZZ} \left(\frac{1-v}{2}\right), \lambda_7 = \frac{1}{7}E_{ZZZ} \left(\frac{1+v}{2}\right), \lambda_8 = \frac{1}{7}E_{ZZZ} \left(\frac{1-v}{2}\right), \lambda_9 = \frac{1}{7}E_{ZZZ} \left(\frac{1+v}{2}\right), \lambda_{10} = \frac{1}{7}E_{ZZZ} \left(\frac{1-v}{2}\right), \lambda_{11} = \frac{1}{7}E_{ZZZ} \left(\frac{1+v}{2}\right), \lambda_{12} = \frac{1}{7}E_{ZZZ} \left(\frac{1-v}{2}\right), \lambda_{13} = \frac{1}{7}E_{ZZZ} \left(\frac{1+v}{2}\right), \lambda_{14} = \frac{1}{7}E_{ZZZ} \left(\frac{1-v}{2}\right), \lambda_{15} = \frac{1}{7}E_{ZZZ} \left(\frac{1+v}{2}\right), \lambda_{16} = \frac{1}{7}E_{ZZZ} \left(\frac{1-v}{2}\right), \text{ where } u, v \in [0, 1]. \text{ Based on these parametrization, Eq. (4.10) can}$$

be rewritten as

$$\begin{aligned}
 C &= 4 \left(\left[(1 - E_{ZZZ}) \left(\frac{1+u}{2} - \frac{1-u}{2} \right) \right]^2 + 19 \left[\frac{1}{7} E_{ZZZ} \left(\frac{1+v}{2} - \frac{1-v}{2} \right) \right]^2 \right) \\
 &= 4 \left[(1 - E_{ZZZ})^2 u^2 + \frac{19}{49} E_{ZZZ}^2 v^2 \right]. \tag{4.11}
 \end{aligned}$$

The final step is to determine the security bounds from asymptotic secret key fraction. The asymptotic secret key fraction under collective attacks given by [73]

$$r = 1 - h(E_{ZZZ}) - I_E. \tag{4.12}$$

In what follows we determine the second term in the formula above using two parameters E_{ZZZ} and C . Eve's information, I_E , is given by the Holevo bound,

$$I_E = S(\rho_E) - \frac{1}{2} S(\rho_{E|0}) - \frac{1}{2} S(\rho_{E|1}). \tag{4.13}$$

Eve holds a purification of the state shared by Alice, Bob and Charlie. Therefore this implies $S(\rho_E) = S(\rho_{AaBbC}) = H(\lambda)$. To compute $S(\rho_{E|i})$, $i \in [0, 1]$ we trace out Bob and Charlie from the state $|\Psi\rangle_{A_b A_c B C E}$ and project Alice on $|+z\rangle$ for $i = 0$ and on $|-z\rangle$ for $i = 1$. Since both $S(\rho_{E|0})$ and $S(\rho_{E|1})$ occur with equal probability we obtain $S(\rho_{E|0}) = S(\rho_{E|1}) = h(E_{ZZZ})$. The explicit computation of $H(\lambda)$ from the eigenvalues λ_i (with $i \in \{0, \dots, 16\}$) is given by

$$\begin{aligned}
H(\lambda) &= - \sum_i \lambda_i \log \lambda_i \\
&= - \left[(1 - E_{ZZZ}) \left(\frac{1+u}{2} \right) \log(1 - E_{ZZZ}) \left(\frac{1+u}{2} \right) + (1 - E_{ZZZ}) \left(\frac{1-u}{2} \right) \right. \\
&\quad \times \log(1 - E_{ZZZ}) \left(\frac{1-u}{2} \right) \Big] - 7 \left[\frac{E_{ZZZ}}{7} \left(\frac{1+v}{2} \right) \log \frac{E_{ZZZ}}{3} \left(\frac{1+v}{2} \right) \right. \\
&\quad \left. + \frac{E_{ZZZ}}{7} \left(\frac{1-v}{2} \right) \log \frac{E_{ZZZ}}{7} \left(\frac{1-v}{2} \right) \right] \\
&= -(1 - E_{ZZZ}) \left[\left(\frac{1+u}{2} \right) \log \left(\frac{1+u}{2} \right) + \left(\frac{1-u}{2} \right) \log \left(\frac{1-u}{2} \right) \right] \\
&\quad - E_{ZZZ} \left[\left(\frac{1+v}{2} \right) \log \left(\frac{1+v}{2} \right) + \left(\frac{1-v}{2} \right) \log \left(\frac{1-v}{2} \right) \right] \\
&\quad - (1 - E_{ZZZ}) \left[\left(\frac{1+u}{2} \right) \log(1 - E_{ZZZ}) + \left(\frac{1-u}{2} \right) \log(1 - E_{ZZZ}) \right] \\
&\quad - E_{ZZZ} \left[\left(\frac{1+v}{2} \right) \log \frac{E_{ZZZ}}{3} + \left(\frac{1-v}{2} \right) \log \frac{E_{ZZZ}}{3} \right] \\
&= h(E_{ZZZ}) + (1 - E_{ZZZ})h\left(\frac{1+u}{2}\right) + E_{ZZZ}h\left(\frac{1+v}{2}\right) + E_{ZZZ} \log 7, \quad (4.14)
\end{aligned}$$

where $h(x) = -x \log(x) - (1-x) \log(1-x)$ is the Shannon entropy function. This yields the following results for Eve's information bound

$$\begin{aligned}
I_E(E_{ZZZ}, u, v) &= S(\rho_E) - \frac{1}{2}S(\rho_{E|0}) - \frac{1}{2}S(\rho_{E|1}) \\
&= h(E_{ZZZ}) + (1 - E_{ZZZ})h\left(\frac{1+u}{2}\right) + E_{ZZZ}h\left(\frac{1+v}{2}\right) + E_{ZZZ} \log 7 \\
&\quad - h(E_{ZZZ}) \\
&= (1 - E_{ZZZ})h\left(\frac{1+u}{2}\right) + E_{ZZZ}h\left(\frac{1+v}{2}\right) + E_{ZZZ} \log 7, \quad (4.15)
\end{aligned}$$

where the terms in the bracket of left hand side of the equation indicate that I_E is obtained in terms of the three parameters. Now to compute Eve's information in terms of the parameters E_{ZZZ} and C one needs to maximise Eq. (4.15);

$$I_E(E_{ZZZ}, C) = \max_C I_E(E_{ZZZ}, u, v). \quad (4.16)$$

We can make use of Eq. (4.11) to define the parameters u and v in terms of C and E_{ZZZ} , and then maximizes Eq. (4.16) over the parameters E_{ZZZ} , u and v . For $E_{ZZZ} = 0$ it can be shown that $I_E(E_{ZZZ}, C) = h[(1 + \sqrt{C/4})/2]$ which gives $I_E(E_{ZZZ}, C) = 0$ which is the case for maximally entangled states where $C = 4$. For $E_{ZZZ} > 0$, we have that $v(u) = \frac{\sqrt{\frac{49}{19}[(C/4) - (1 - E_{ZZZ})^2 u^2]}}{E_{ZZZ}}$, and the condition

that $v \in [0, 1]$ implies that $u \in [u_{\min}, u_{\max}]$ where $u_{\min} = \max \left[\frac{\sqrt{(C/4 - \frac{19}{49}E_{ZZZ}^2)}}{1 - E_{ZZZ}}, 0 \right]$, $u_{\max} = \min \left[\frac{\sqrt{C/4}}{1 - E_{ZZZ}}, 1 \right]$. When $E_{ZZZ} \leq 15.9\%$, which is a reasonable value for the practical implementation, we find that $\frac{d}{du}I_E(E_{ZZZ}, u, v(u)) > 0$ between $u_{\min}$ and $u_{\max}$. This implies that Eve's information can be bounded by

$$I_E(E_{ZZZ}, C) = I_E(E_{ZZZ}, u_{\max}, v(u_{\max})). \quad (4.17)$$

Now, to simplify our analysis we determine Eve's information in terms of parameter E_{ZZZ} . In doing so, without loss of generality, we estimate the parameter C by considering a case where the state $|\phi^+\rangle_{A_b A_c BC} = \frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle)$ initially shared by Alice, Bob and Charlie, goes through a depolarising channel and give rise to Werner state, $\rho_{A_b A_c BC} = p|\phi^+\rangle\langle\phi^+| + (1 - p)\mathbf{I}/16$. Here $\mathbf{I}$ denotes the identity matrix and p is the probability for the state to remain unchanged while $(1 - p)$ represents the probability for the state to transform into a mixed state. For this four-qubit Werner state, the measurement statistics by Alice, Bob and Charlie satisfy $E_{ZZZ} = \frac{(1-p)}{2}$ and $C = 4p^2 = 4(1 - 2E_{ZZZ})^2$. Substituting this value of C in the expressions for $u_{\max}$ and $v(u_{\max})$ then Eq. (4.17) can be rewritten in terms of error rate E_{ZZZ}

$$I_E(E_{ZZZ}) = (1 - E_{ZZZ})h\left(\frac{1 - 3E_{ZZZ}/2}{1 - E_{ZZZ}}\right) + E_{ZZZ} + E_{ZZZ} \log 7. \quad (4.18)$$

The corresponding secret key fraction (4.12) is therefore given by

$$r = 1 - h(E_{ZZZ}) - (1 - E_{ZZZ})h\left(\frac{1 - 3E_{ZZZ}/2}{1 - E_{ZZZ}}\right) - E_{ZZZ} - E_{ZZZ} \log 7. \quad (4.19)$$

The lower bound on error rate E_{ZZZ} can be obtained for the worst case value of the secret key fraction r and hence given by the solution to the equation

$$1 - h(E_{ZZZ}) - (1 - E_{ZZZ})h\left(\frac{1 - 3E_{ZZZ}/2}{1 - E_{ZZZ}}\right) - E_{ZZZ} - E_{ZZZ} \log 7 = 0. \quad (4.20)$$

4.4 Finite security analysis

We study the performance of the proposed protocol under a realistic scenario where the communicating parties exchange a finite number of signals N and subsequently account for statistical fluctuations due to finite-size effects. Our finite key rate analysis is sketched along the lines presented in [218, 239–241, 267] based on a universally composable framework. First, we point out that the three-party RFI protocol generates a triplet of key bit strings S_A , S_B and S_C for Alice, Bob, and Charlie, respectively. The key bit strings are of the length ℓ and are subject to satisfying the correctness and secrecy criteria for the protocol to be deemed secure. Under the composability criteria, a QKD protocol is regarded correct if $S_A = S_B = S_C$, for any given attacking strategy by an eavesdropper. Therefore, an ε_{cor} -correct protocol is invariant from the correct one by a small error probability, ε_{cor} , i.e., $\Pr[S_A \neq S_B \neq S_C] \leq \varepsilon_{\text{cor}}$. Furthermore, the secrecy conditions are defined as follows: let ρ_E be the state of a quantum system containing the information acquired by an eavesdropper during the execution of a QKD protocol. The correlation of Alice's key bit string S_A with Eve's quantum state ρ_E can be described by classical-quantum state, $\rho_{S_A E}$. There is no correlation between Eve's system and Alice's key bit string in an ideal case, i.e., $\rho_U \otimes \rho_E$ where ρ_U is a completely mixed state on the keyspace. The classical-quantum state, $\rho_{S_A E}$ is said to be Δ -secret if

$$\min_{\rho_E} \frac{1}{2} \|\rho_{S_A E} - \rho_U \otimes \rho_E\|_1 \leq \Delta. \quad (4.21)$$

In particular, a ε_{sec} -protocol is one which generates Δ -secure keys with $(1-p_{\text{abort}})\Delta \leq \varepsilon_{\text{sec}}$, with p_{abort} representing the probability that it aborts. Therefore, the key rate of $\varepsilon_{\text{sec}} + \varepsilon_{\text{cor}}$ -three-party RFI protocol is given by

$$\frac{\ell}{N_{\text{total}}} = q \left[Q_0 + Q_{\mu, ZZZ}^1 (1 - I_E^U) - \text{leak}_{EC} - \log_2 \frac{2}{\varepsilon_{\text{cor}}} - 2 \log_2 \frac{11}{\varepsilon_{\text{sec}}} \right], \quad (4.22)$$

with $q = \frac{N_{\mu} p_z^3}{N_{\text{total}}}$, N_{μ} is the number of exchanged signals of intensity μ while p_z is the probability of selecting Z basis for preparation and measurement of states, and N_{total} is total number of exchanged signals. The parameter $\text{leak}_{EC} = f_{EC} Q_{\mu, ZZZ} H(E_{\mu, ZZZ})$ correspond to the fraction of bits that have leaked to Eve during the error correction procedure and $f_{EC} \geq 1$ is the error correction efficiency. The finite key rate formula and decoy state parameters in Eq. (4.22) above are given in the Appendix B.

4.4.1 Statistical fluctuation analysis

In the finite key distillation case, the parameter estimation is not perfect due to fluctuations in the observed error rates and detection rates. Below we provide estimates for the parameters that yield Eq. (4.22).

4.4.1.1 Estimation of $Q_{\mu,ZZZ}^1$

From the value directly observed from the experiment, $n_\mu = Q_\mu N_\mu$ (where we omitted basis choice for simplicity), which corresponds to the number of detected signal states, we can use variant multiplicative Chernoff bound presented in Lemma 3 of Ref. [267] to estimate the lower and upper bounds of the expected detection events. To demonstrate that, we rewrite n_μ in terms of photon number statistics as

$$n_{k,\mu} = \sum_{l=1}^n \chi_{k,l}^\mu, \quad (4.23)$$

where

$$\chi_{k,l}^\mu = \begin{cases} 1 & \text{with probability } p(k|\mu) \\ 0 & \text{with probability } (1 - p(k|\mu)) \end{cases}, \quad l = 1, \dots, n \quad (4.24)$$

are independent Bernoulli random variables. In particular, $\chi_{k,l}^\mu = 1$ means that k -photon signal state has resulted in the l th detection event while $\chi_{k,l}^\mu = 0$ means either vacuum or decoy state has been used. The term $p(k|\mu)$ is the conditional probability that a source set at signal intensity μ produces a k -photon state. It then follows that for a set of Bernoulli random variables, $\chi_{k,1}^\mu, \chi_{k,2}^\mu, \dots, \chi_{k,n}^\mu$, the expected value of $n_{k,\mu}$ is $\bar{n}_{k,\mu} = \mathbb{E}[n_{k,\mu}] = \sum_{l=1}^n p(k|\mu)$. Let an observed outcome, $n_{k,\mu}$ be denoted by x for a given trial. Then, for any $\varepsilon_3 > 0$ we have that

$$\begin{aligned} \bar{n}_{k,\mu} &\geq \max\{0, x - \Delta(x, \varepsilon_3)\} \\ \bar{n}_{k,\mu}^L &:= \max\{0, x - \Delta(x, \varepsilon_3)\}, \end{aligned} \quad (4.25)$$

holds with failure probability ε_3 , where $\bar{n}_{k,\mu}^L$ is the lower bound and $\Delta(x, \varepsilon_3)$ is the positive root of the equation $\Delta(x, \varepsilon_3) - [x + \Delta(x, \varepsilon_3)] \ln[1 + \Delta(x, \varepsilon_3)/x] - \ln x = 0$. Also, for any $\varepsilon_3 > 0$, we have that

$$\begin{aligned}\bar{n}_{k,\mu} &\leq x + \Delta(x, \varepsilon_3) \\ \bar{n}_{k,\mu}^U &:= x + \Delta(x, \varepsilon_3),\end{aligned}\tag{4.26}$$

holds with failure probability ε_3 , where $\bar{n}_{k,\mu}^U$ is the upper bound of $\bar{n}_{k,\mu}$ and $\Delta(x, \varepsilon_3)$ is the positive root of equation $\Delta(x, \varepsilon_3) + x \ln(x/[x + \Delta(x, \varepsilon_3)]) + \ln \varepsilon_3 = 0$. The same argument can be applied to determine the lower and upper bounds of expected value $\bar{n}_\nu$ from observed detection events $n_\nu = Q_\nu N_\nu$ for decoy states. Next, the lower and upper bounds of $\bar{n}_\mu$ and $\bar{n}_\nu$ are used to calculate the lower and upper bounds of gains, $\bar{Q}_\mu^L = \bar{n}_{k,\mu}^L/N_\mu$, $\bar{Q}_\mu^U = \bar{n}_{k,\mu}^U/N_\mu$, $\bar{Q}_\nu^L = \bar{n}_{k,\nu}^L/N_\nu$ and $\bar{Q}_\nu^U = \bar{n}_{k,\nu}^U/N_\nu$ which are in turn used to calculate $\bar{Y}_{1,L}$ and $\bar{Y}_{1,U}$, respectively as follows

$$\bar{Y}_{1,L} = \frac{p(\mu|2)[\bar{Q}_\nu^L - p(\nu|0)Y_0] - p(\nu|2)[\bar{Q}_\mu^U - p(\mu|0)Y_0]}{p(\mu|2)p(\nu|1) - p(\mu|1)p(\nu|2)},\tag{4.27}$$

$$\bar{Y}_{1,U} = \frac{p(\mu|2)[\bar{Q}_\nu^U - p(\nu|0)Y_0] - p(\nu|2)[\bar{Q}_\mu^L - p(\mu|0)Y_0]}{p(\mu|2)p(\nu|1) - p(\mu|1)p(\nu|2)}.\tag{4.28}$$

Estimation of bounds for $n_{1,\mu}$ The parameters $\bar{Y}_{1,U}$ and $\bar{Y}_{1,L}$ are used to evaluate the upper and lower bounds on the observed yield for single photon components. We use multiplicative Chernoff bound (Lemma 2) of Ref. [267] to deduce the upper and lower bounds of observed yield from expected values $\bar{Y}_{1,U}$ and $\bar{Y}_{1,L}$ as follows. According to results of Lemma 2, if $g(\bar{Y}_{1,U}, \delta) = [e^\delta/(1+\delta)^{1+\delta}]^{\bar{Y}_{1,U}}$, for any $\delta > 0$, then upper tail is defined as

$$\Pr[Y_{1,U} \geq (1+\delta)\bar{Y}_{1,U}] < g(\bar{Y}_{1,U}, \delta) = \varepsilon_2,\tag{4.29}$$

where δ is the positive root of the equation $\bar{Y}_{1,U}[\delta - (1+\delta)\ln(1+\delta)] - \ln \varepsilon_2 = 0$. For any $0 < \hat{\delta} \leq 1$, we have the lower tail given by

$$\Pr[Y_{1,L} \leq (1-\hat{\delta})\bar{Y}_{1,L}] < g(\bar{Y}_{1,L}, -\hat{\delta}) = \hat{\varepsilon}_2,\tag{4.30}$$

where $\hat{\delta}$ is the positive root of equation $\bar{Y}_{1,L}[\hat{\delta} + (1 - \hat{\delta}) \ln(1 - \hat{\delta})] + \ln \hat{\varepsilon}_2 = 0$. From these results, the observed lower bound of single photon detection events is given by $n_{1,\mu}^L = Y_{1,L} N_\mu p(1|\mu)$. The detection events are used to compute the gain for single photon events as $Q_\mu^1 = n_{1,\mu}^L / N_\mu$.

4.4.1.2 Estimation of $e_{ZZZ}^{U,1}$

The tail inequality for random sampling without replacement is exploited to provide an upper bound for the expected error rates from the observed error rates in the sampled data. The method is described in Lemma 1 of Ref. [267] as follows.

Lemma 1. [267] *For a given $n + m$ string of binary bits $\mathcal{X}_{n+m}\{x_1, x_2, \dots, x_{n+m}\}$. Let $\mathcal{X}_m$ denotes a random sample (without replacement) of size m bit strings and $\mathcal{X}_n$ represents the remaining n bit strings. Then, for λ_m and λ_n , the probabilities of observing bit 1 value in the string $\mathcal{X}_m$ and $\mathcal{X}_n$, respectively, it holds that for any $\epsilon > 0$*

$$Pr[\lambda_n \leq \lambda_m + \mu(n, m, \lambda_m, \epsilon)] > 1 - \epsilon,$$

where $\mu(n, m, \lambda_m, \epsilon)$ is the positive root of the following equation

$$\ln C_m^{m\lambda_m} + \ln C_n^{m\lambda_m + n\mu} - \ln C_{n+m}^{(n+m)\lambda_m + n\mu} - \ln \epsilon = 0$$

Here $C = i!/[j!(1-j)!]$ is the binomial coefficient.

We can use Lemma 1 to estimate the upper bound on expected error rate in the Z basis, $\bar{E}_{\mu,ZZZ}$ by considering a thought experiment picture where an $n + m$ string of bits correspond to compatible measurements made by Alice, Bob and Charlie in the Z basis. If the observed average error rate obtained from m random bit strings is $E_{\mu,ZZZ} = \sum_{i=1}^m r_{Z,A} \oplus r_{Z,B} \oplus r_{Z,C}$ ($r_{Z,A}$, $r_{Z,B}$ and $r_{Z,C}$ are Alice, Bob and Charlie's bits) then by using the upper tail inequality, the remaining n bits give upper bound for error rate in the Z basis under the condition that

$$\bar{E}_{\mu,ZZZ}^U \leq E_{\mu,ZZZ} + \xi(n, m, E_{\mu,ZZZ}, \epsilon_1), \quad (4.31)$$

with probability $1 - \epsilon_1$. We leverage this result and the outcome of (4.27) to compute

the upper bound on the error rate for single photon events as

$$e_{ZZZ}^{1,U} = \frac{\bar{E}_{\mu,ZZZ}^U \bar{Q}_{\mu}^U - e_0 Y_0 p(\mu|0)}{\bar{Y}_{1,L} p(\mu|1)}. \quad (4.32)$$

The upper bounds on the error rates in the complementary bases $e_{\alpha\beta\delta}$ with $\alpha, \beta, \delta \in \{X, Y\}$ can be obtained analogously by applying Lemma 1.

4.5 Simulation results

In this section, we simulate the performance of the proposed protocol on a fiber-based QKD system model. We use the following experimental parameters: the loss coefficient of the fiber is 0.2 dB/km, Bob and Charlie's detection efficiencies, $\eta = 14.5\%$, dark count rate of the single-photon detector, $P_d = 1.7 \times 10^{-6}$. The security parameters of secrecy and correctness are fixed at $\varepsilon_{\text{cor}} = 10^{-15}$ and $\varepsilon_{\text{sec}} = 10^{-10}$. We assume that error correction efficiency, $f_{EC} = 1.22$ and the expected photon number for signal states is set at $\mu = 0.6$. The optimal probability, p_z for key basis is set at 0.95 according to Ref. [271].

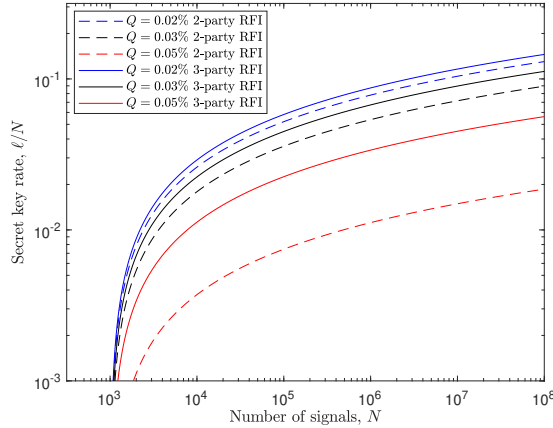


Figure 4.2: Plot of secret key rate versus number of signals N for the proposed three-party RFI protocol (solid lines) for security parameters: $\varepsilon_{\text{cor}} = 10^{-15}$, $\varepsilon_{\text{sec}} = 10^{-10}$, and the misalignment error rates $Q = (0.02\%, 0.03\%, 0.05\%)$. Experimental parameters: dark counts rate, $P_d = 1.7 \times 10^{-6}$, the loss coefficient of the channel is 0.2 km/dB, the detection efficiency is $\eta = 14.5\%$. We also plot the two-party RFI protocol (dashed lines) for the same error rates for comparison.

Figure 4.2 shows the secret key rate, ℓ/N , as a function of signal size N for the two-party and three-party RFI protocols. The key rates are obtained at different values

for the intrinsic error rate, $Q = (0.02\%, 0.03\%, 0.05\%)$ due to the misalignment and instability of the optical system. Our proposed protocol can achieve a positive key rate with a minimum of 10^3 signals. It can also be observed that higher key rates are achieved for the three-party protocol than the two-party counterparts for the same number of signals exchanged. Our simulation result demonstrates that the three-party RFI QKD is a feasible scheme in the finite-key regime.

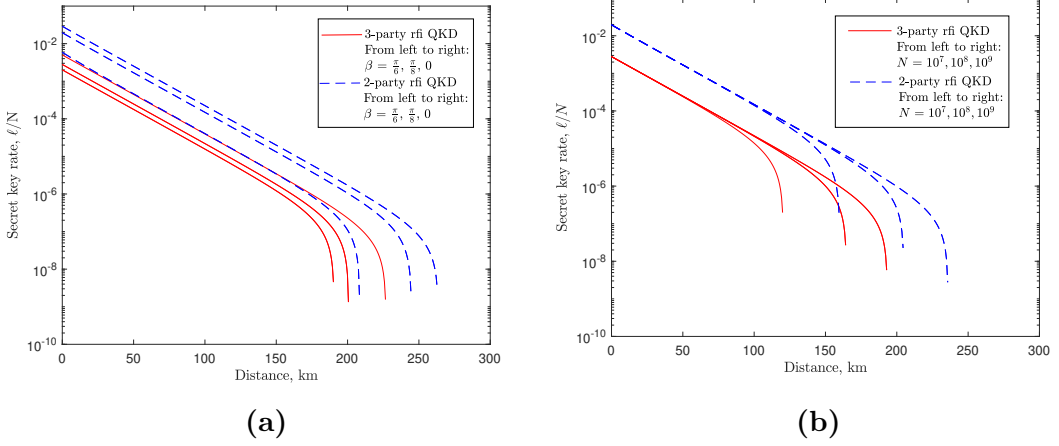


Figure 4.3: (a) Expected secret key rate (in logarithmic scale) for the proposed three-party RFI protocol (solid red line) as a function of transmission distance measured in km, for the fixed misalignment degree β . From left to right, the curves represent $\beta = \pi/6$, $\beta = \pi/8$ and $\beta = 0$. The number of signals is fixed at 10^9 (b) Expected secret key rate (in logarithmic scale) for the proposed three-party RFI protocol (solid red line) as a function of transmission distance measured in km, for the fixed number of signals, $N = 10^7$, $N = 10^8$ and $N = 10^9$. The relative rotation of reference frames is set at $\beta = \pi/8$ and security parameters are: $\varepsilon_{\text{cor}} = 10^{-15}$, $\varepsilon_{\text{sec}} = 10^{-10}$, experimental parameters: dark counts rate, $P_d = 1.7 \times 10^{-6}$, the loss coefficient of the channel is 0.2 km/dB, the detection efficiency is $\eta = 14.5\%$. For comparison purposes, we show the plots of two-party RFI protocol, represented by blue dashed lines in both figures.

In Figure 4.3a, we simulate the secret key rate for three-party RFI protocol as a function of transmission distance for fixed misalignment degree $\beta = 0, \pi/6, \pi/8$. For comparison, we also simulate the key rate for the two-party RFI protocol (dashed line) for the same parameters. We observed that despite the increase in misalignment of reference frames, the achievable transmission distance is still comparable to when there is no misalignment in reference frames (when $\beta = 0$). Also, our results indicate that the two-party RFI protocol outperforms our proposed three-party RFI protocol in terms of maximum attainable transmission distance for different misalignment degrees of β . These results may be attributed to the fact that the three-party RFI protocol considers misalignment in two channels linking Alice to

Bob and Charlie. On the contrary, the two-party RFI protocol employs one channel linking Alice and Bob, hence a slight increase in signal gain and superiority in performance. Nevertheless, our proposed three-party RFI protocol is more efficient for secure communication involving multiple parties. A secret key for each party is produced from a single run of the protocol rather than performing multiple bipartite QKD protocols to establish a secret key for each communication party.

In Figure 4.3b, we demonstrate the performance of three-party RFI protocol for a fixed number of signals, $N = 10^7$, 10^8 and 10^9 . For comparison, we provide the plots for the two-party RFI protocol for the same number of signals. Our results demonstrate that with a minimum data size of $N = 10^7$, it is possible to achieve a secure key rate at a reasonable transmission distance of approximately 120 km for the three-party protocol. We also observe the slight superiority of two-party RFI protocol over three-party RFI protocol regarding achievable secret key rate and transmission distance. Thus, this demonstrates that our proposed protocol fares well against the two-party protocol, which proves its feasibility.

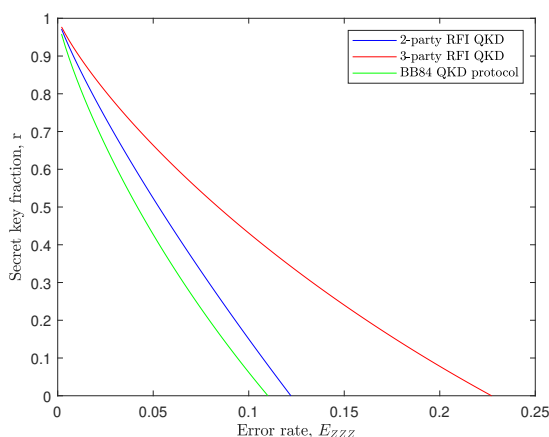


Figure 4.4: Plots of secret key fraction vs quantum bit error rate, E_{ZZZ} for the BB84 protocol [259], two-party RFI protocol [73] and the proposed three-party RFI protocol.

In Figure 4.4, we plot the secret key fraction against the quantum bit error rate E_{ZZZ} in the asymptotic regime to deduce the lower bound on the tolerable error rate. We obtain $E_{ZZZ} \approx 0.2265$ for the proposed protocol, which indicates that a secure key is achievable at higher error rates compared to the two-party RFI protocol [73] with an error bound of 12.62% and the well-known error bound for BB84 protocol of 11.0% [259]. We note that the simulation results presented in this work provide valuable insights into the potential performance of the proposed three-party RFI protocol when practically implemented. We emphasize that the protocol

is feasible for practical implementation for the following reasons. The SPDC source used in our protocol is easily realizable, as demonstrated in [130, 221, 272–275]. Significant progress has been made in developing on-chip SPDC sources, which offer advantages such as scalability, small size, and high stability [276–278]. Additionally, experimental setups for executing polarization-based QKD have been developed and demonstrated in [177, 279–281]. Moreover, experimental setups for phase-encoding QKD are available and are compatible with our proposed three-party RFI QKD [94, 282].

4.6 Conclusion

We presented a three-party RFI QKD protocol that can be implemented without any alignment between the sender and receiver. The protocol exploits entangled states to establish a secret key between three communicating parties. We derived the asymptotic secret key fraction for the proposed protocol against collective attacks and performed finite-size key security of the three-party RFI QKD protocol. Furthermore, we simulate the secret key rate for three-party RFI protocol as a function of transmission distance for different misalignment degrees ($\beta = \pi/6, \pi/8$) to investigate the impact on statistical quantity C and stability of the protocol. The simulation results demonstrate that our proposed protocol is not heavily affected by increased misalignment of reference frames as the achievable transmission distances are still comparable to the case where there is no misalignment in reference frames (when $\beta = 0$).

Furthermore, we investigated the performance of our proposed three-party RFI protocol for a fixed number of signals. The simulation results demonstrate that the protocol can achieve a significant secret key rate at reasonable transmission distances of about 120 km with 10^7 signals. However, a further distance of 195 km can be achieved with about 10^9 finite signals. The proposed protocol presents a suitable alternative for practical QKD implementations. This was demonstrated by reasonable secret key rates obtained with rigorous and tight statistical fluctuation analysis methods for finite-size key effects. Furthermore, our protocol is more efficient than the two-party RFI protocol in terms of resource consumption, as few data signals are required to produce reasonable secret key rates, as evidenced by the finite key analysis results. Moreover, we have also shown that our protocol is robust against noise in the quantum channel based on the realized error rate threshold of 22.7%,

which is an improvement to the existing two-party BB84 protocols.

Reference frame independent twin field QKD

5.1 Introduction

The trade-off between distance and secret key generation rate remains one of the significant challenges in the practical implementation of quantum key distribution (QKD). As things stand, it is well known that there is a fundamental secret key rate limit that restricts any point-to-point implementation of QKD called Pirandola, Laurenza, Ottaviani and Banchi (PLOB) bound—named after authors who discovered the bound [102]. This bound indicates that for a lossy link with transmittance η , two parties can generate the secret keys at an utmost rate of $-\log_2(1 - \eta)$, which is the secret key capacity of the channel. This implies that the secret key rate scales linearly with the channel transmittance for any direct point-to-point QKD protocol. For instance, protocols like single-photon-based BB84, decoy-state-based BB84 protocol with weak coherent pulses and Gaussian modulated CVQKD are restricted by key rate scaling of $\simeq \eta$ bits per channel use. Therefore, to circumvent this limit and achieve long-distance high-rate implementations of QKD, we must employ quantum repeaters [103, 104] and quantum networks [105]. However, it is still impossible to realize quantum repeaters with the current technology. Recently, a novel QKD that relies on phase-randomized twin fields of optical pulses to encode information was developed and can surpass the secret key capacity bound for repeaterless QKD schemes [106]. Similar to MDI-QKD, the possibility of side-channel attacks is removed in this protocol as an untrusted relay connects the communicating parties.

The protocol is based on the single-photon interference of optical fields generated with almost identical electromagnetic phases. This single-photon interference at the untrusted relay leads to an improved secret key rate, which scales with the square root of channel transmittance. Since the original TF-QKD scheme lacked rigorous security proof, variant TF protocols aimed at proving TF-QKD security have been proposed [107–117, 283–285]. Moreover, the experimental demonstrations of TF-QKD have already been successfully implemented [107, 108, 110, 286–289]. The QKD systems mentioned above exploit the phase to encode information, which presents the problem of active stabilization of interferometers. Although it is feasible to share a reference frame between Alice and Bob, it comes at a cost as additional systems required for phase calibration may lead to more information leakage and thus reduce practical systems' performance [290, 291]. Fortunately, a reference-frame-independent (RFI) QKD protocol was proposed to address these challenges [73]. Ideally, light pulses are encoded perfectly without any state preparation flaw (SPF). However, this assumption falls short experimentally due to the inherent deficiencies of phase modulators. The problem with SPFs can be addressed using the Gottesman-Lo-Lutkenhaus-Preiskill (GLLP) security analysis [51]. However, the main drawback is that the approach leads to a low achievable secret key rate and is not robust against channel loss. Tamaki et al. recently proposed a loss-tolerant protocol that is robust against channel losses due to SPFs and capable of attaining key rates comparable to a protocol that assumes perfect encoding [52]. The protocol is resource-efficient, employing only three out of the possible four states for BB84 protocol and considering modulation errors due to an imperfect phase modulator. It is conjectured that the protocol can be generalized to the six-state protocol, where only four states are required instead of the usual six states. In light of the above, we investigate the practicality of TF-QKD by employing the loss-tolerant protocol to derive the security bounds under imperfect state preparation. We also study the protocol under reference frame independence condition, eliminating the need for active phase stabilization. This chapter is based on manuscript [198].

5.2 Operation of RFI-TF QKD protocol

We propose a loss tolerant-based RFI-TF QKD protocol that uses four signal states from three mutually unbiased bases defined by the Pauli operators, X , Y and Z . This protocol is conjectured to achieve error rates similar to the QKD protocol that employs all six states from three bases $\{Z, X, Y\}$ [52]. The four states are denoted

as $|\phi_{0Z}\rangle = |0_Z\rangle$, $|\phi_{1Z}\rangle = |1_Z\rangle$, $|\phi_{0X}\rangle = \frac{1}{\sqrt{2}}(|0_Z\rangle + |1_Z\rangle)$ and $|\phi_{0Y}\rangle = \frac{1}{\sqrt{2}}(|0_Z\rangle + i|1_Z\rangle)$ where $|0\rangle$, $|1\rangle$ represent vacuum and one photon states, respectively. We describe the protocol implemented with the idealized photon source and then discuss the practical protocol that employs the weak coherent laser source.

Protocol 1 The entanglement-based description of the protocol and is as follows:

1. Alice (Bob) starts by preparing the entangled state $|\Psi\rangle_{Aa(Bb)} = (\sqrt{1-\gamma}|0\rangle_{A(B)}|0\rangle_{a(b)} + \sqrt{\gamma}|1\rangle_{A(B)}|1\rangle_{a(b)})$ with $\gamma \in (0, 1)$. System $A(B)$ represents the qubits that remain in Alice and Bob's possession.
2. Alice (Bob) sends signal states a (b) through the insecure quantum channel to the untrusted third party, Charlie.
3. Upon receipt of the pulses, Charlie executes the single-photon Bell state measurement with a symmetric beam-splitter followed by two threshold detection. Charlie announces the successful events of single-photon Bell state measurement. The two detectors labeled L and R in Figure 5.1 are associated with destructive and constructive interference, respectively. A coincidence detection with a click in L no click in R indicates a projection into Bell state $|\Phi^+\rangle_{ab} = \frac{1}{\sqrt{2}}(|0\rangle_a|1\rangle_b + |1\rangle_a|0\rangle_b)$ while a click in R and no click in L corresponds to projection onto Bell state $|\Phi^-\rangle_{ab} = \frac{1}{\sqrt{2}}(|0\rangle_a|1\rangle_b - |1\rangle_a|0\rangle_b)$.
4. Following the results announcement, Alice and Bob measure their qubits in the Z basis with probability p_z and choose the complementary bases with probability $1 - p_z$. Moreover, they post select the events of a compatible basis to obtain a raw key.
5. Lastly, to ensure that their bit strings match, Bob always flips his qubit for all successful Bell state measurement results in the Z basis and only flips his bit for Bell state measurement result $|\Phi^-\rangle_{ab} = \frac{1}{\sqrt{2}}(|0\rangle_a|1\rangle_b - |1\rangle_a|0\rangle_b)$ in the complementary bases. In the RFI protocol, the key is obtained from the Z basis where the reference frames linking Alice (Bob) and Charlie are assumed to be well aligned, while in the other measurement bases (X , Y) the frames are allowed to slowly vary by an arbitrary angle β . The allowed deviations in the bases are given by $X_B = \cos \beta X_A + \sin \beta Y_A$ and $Y_B = \cos \beta Y_A - \sin \beta X_A$.

The above protocol can be converted to an equivalent prepare and measure protocol where Alice and Bob measure their qubits $A(B)$ before sending the signal states $a(b)$ to Charlie. In principle, this implies that Alice and Bob directly prepare the signal states $a(b)$, i.e., their qubits measurements herald the formation of signal states. This measurement operation does not change operations results in other steps; thus, the protocol can be alternatively described as follows.

1. Alice (Bob) prepares the signal states $a(b)$ in the state $|\phi_{0Z}\rangle = |0_Z\rangle$, $|\phi_{1Z}\rangle = |1_Z\rangle$ with probabilities $1 - \gamma$ and γ in the Z basis for logic bits 0 and 1, respectively. The states in complementary bases $|\phi_{0X}\rangle = \sqrt{1 - \gamma}|0_Z\rangle + \sqrt{\gamma}|1_Z\rangle$ and $|\phi_{0Y}\rangle = \sqrt{1 - \gamma}|0_Z\rangle + i\sqrt{\gamma}|1_Z\rangle$ are prepared with equal probabilities and encoded as logic bit 0.
2. They send the signal states $a(b)$ through the quantum channel to untrusted Charlie, who executes the single-photon Bell state measurement with a symmetric beam-splitter followed by two threshold detection.
3. Charlie announces the successful single-photon Bell state measurement events to Alice and Bob, who then postselect the events they prepared their states on the Z basis to obtain a raw key.
4. Lastly, to ensure that their bit strings match, Bob always flips his qubit for all successful Bell state measurement results in the Z basis and only flips his bit for Bell state measurement result $|\Phi^-\rangle_{ab} = \frac{1}{\sqrt{2}}(|0\rangle_a|1\rangle_b - |1\rangle_a|0\rangle_b)$ in the complementary bases. The measurement results in the complementary bases are used to estimate the adversary's knowledge about the key.

Protocol 2 Since realizing a superposition between a vacuum and a single photon is challenging (for the realization of states in complementary bases in protocol 1), we now describe the practical protocol implemented with weak coherent sources (see Figure 5.1). It exploits the interference of a vacuum state and a coherent state in a symmetric beam-splitter to generate a secret key. Also, twin optical fields with identical random phases are used in the complementary bases to estimate Eve's information. The protocol runs as follows:

1. In the Z basis, Alice (Bob) randomly prepares weak coherent states $|\sqrt{\mu_{a(b)}}e^{i\chi}\rangle$ with intensities 0 (vacuum) and μ with probabilities $1 - \gamma$ and γ , respectively.

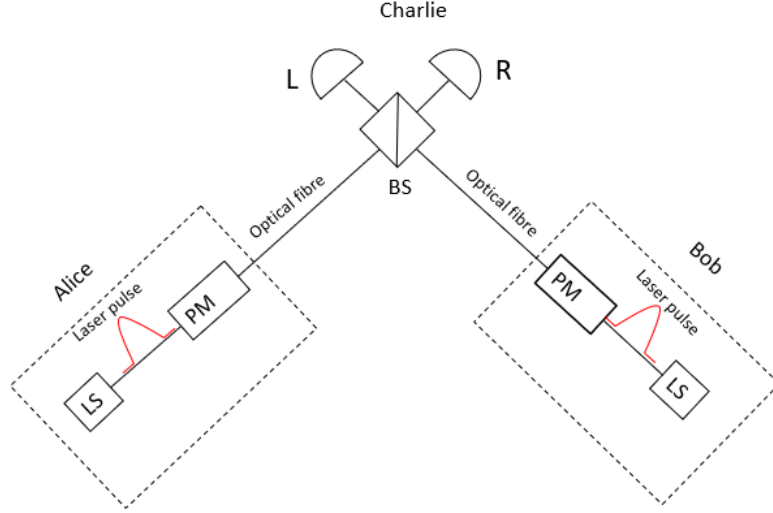


Figure 5.1: The setup of the proposed RFI TF-QKD. Alice and Bob use their laser sources (LS) to prepare coherent states $|\sqrt{\mu_{a(b)}}e^{i\chi}\rangle$ with random phase χ in the Z basis and states $|\sqrt{\mu_{a(b)}}e^{i(0+\chi)}\rangle$ and $|\sqrt{\mu_{a(b)}}e^{i(\frac{\pi}{2}+\chi)}\rangle$ for X and Y basis, respectively. The phase is encoded using phase modulators (PM). Alice and Bob send the prepared optical signals through an insecure channel to the untrusted Charlie, who is supposed to perform a single-photon interference in a symmetric beam-splitter (BS) followed by threshold detection in either L or R detector. In the X and Y bases, the random phase χ is selected from discrete M phase slices $\Delta_j = (\frac{2\pi j}{M}, \frac{2\pi(j+1)}{M})$ over the semi-interval $[0, 2\pi)$ with $j = \{0, \dots, M-1\}$. During classical post-processing, the random phases are announced, and states are postselected according to the satisfaction of condition; $|j_A - j_B| \bmod M = 0$ or $|j_A - j_B| \bmod M = \frac{M}{2}$ where $j_{A(B)} = (\frac{\Delta_j M}{2\pi}) \bmod M$.

The bit values 0 and 1 encodes for intensity 0 and μ , respectively. If the parties (Alice and Bob) choose complementary bases, they prepare the states $|\sqrt{\mu_{a(b)}}e^{i(\theta_{A(B)}+\chi)}\rangle$ with phase values $\theta_{A(B)} = 0$ and $\theta_{A(B)} = \pi/2$ for X and Y basis, respectively with both states coding for bit value 0. In these two bases, the optical pulses are prepared with intensity $\mu_{a(b)} \in \{u/2, v/2, 0\}$ (where u , v and 0 represent the signal, decoy and vacuum pulses). Furthermore, in this protocol the random phase χ is picked from discrete M phase slices $\Delta_j = (\frac{2\pi j}{M}, \frac{2\pi(j+1)}{M})$ over the semi-interval $[0, 2\pi)$ with $j = \{0, \dots, M-1\}$.

2. The optical pulses are sent through an insecure channel to Charlie, who allows them to interfere in the symmetric beam-splitter. This is followed by threshold detection, and after that, Charlie announces the successful detection events. The successful results correspond to a click in the L detector and no click in the R detector or vice versa.

3. Following the announcement of results, Alice and Bob perform sifting by post-selecting the successfully detected states, which were prepared using the same basis. Precisely, in the Z basis, these events correspond to cases where Alice chose intensity μ while Bob selected intensity 0 and vice versa. For complementary bases, they consider the states prepared with the same intensity and in which they picked the random phase slices according to the phase post-selection matching method, i.e., $|j_A - j_B| \bmod M = 0$ or $|j_A - j_B| \bmod M = \frac{M}{2}$ where $j_{A(B)} = \left(\frac{\Delta_j M}{2\pi}\right) \bmod M$. Note that during sifting, Alice and Bob only announce the random phase χ for the states prepared in the complementary bases, while random phases for Z basis states are not disclosed. The key is generated from measurements in the Z basis. The results in X and Y bases are used to monitor eavesdropping. It should be noted that these bases are allowed to vary by an arbitrary angle β . The allowed deviations in the bases are given by $X_B = \cos \beta X_A + \sin \beta Y_A$ and $Y_B = \cos \beta Y_A - \sin \beta X_A$.

5.3 Security analysis of the protocol

Following the sequential transmission and measurement of optical pulses, Alice and Bob now possess partially correlated bit strings. They proceed with the parameter estimation step to deduce the bit error rate in the key basis. The quantum bit error rate is given by

$$E_{ZZ} = \frac{1 - \langle Z_A Z_B \rangle}{2} \quad (5.1)$$

where Z_A and Z_B represent that Alice and Bob send the two states prepared in the Z basis, respectively. The notation $\langle \cdot \rangle$ denotes the expectation value. To compute Eve's knowledge of the key, we consider a depolarizing channel $E_{ZZ} \leq 15.9\%$ [73]. The bound is given by

$$I_E = (1 - E_{ZZ})h\left(\frac{1 + u_{\max}}{2}\right) - E_{ZZ}h\left(\frac{1 + v(u_{\max})}{2}\right), \quad (5.2)$$

where

$$u_{\max} = \min \left[\frac{1}{1 - E_{ZZ}} \sqrt{C/2}, 1 \right],$$

$$v(u_{\max}) = \sqrt{[C/2 - (1 - E_{ZZ})^2 u_{\max}^2] / E_{ZZ}}. \quad (5.3)$$

The quantity C is obtained from the measurement results in the complementary bases and is given by

$$C = \langle X_A X_B \rangle^2 + \langle X_A Y_B \rangle^2 + \langle Y_A X_B \rangle^2 + \langle Y_A Y_B \rangle^2. \quad (5.4)$$

This expression can be rewritten in terms of the error rates as

$$C = (1 - 2E_{XX})^2 + (1 - 2E_{XY})^2 + (1 - 2E_{YX})^2 + (1 - 2E_{YY})^2. \quad (5.5)$$

To compute C , we employ a loss tolerant technique where Alice and Bob prepare their optical pulses using four states $|\phi_{0Z}\rangle$, $|\phi_{1Z}\rangle$, $|\phi_{0X}\rangle$ and $|\phi_{0Y}\rangle$. Due to imperfections in the phase modulation, the actual states that Alice (Bob) prepares can be described by

$$|\phi_{j\beta}\rangle_{A(B)} = |\sqrt{\mu}e^{i\chi}\rangle_r |\sqrt{\mu}e^{i(\chi+\theta_{A(B)}+\delta\theta_{A(B)}/\pi)}\rangle_s \quad (5.6)$$

where $r(s)$ denotes reference (signal) states, μ corresponds to the intensity of pulses and δ represents the deviation from desired encoding angle θ in the actual states. Here $\beta \in \{X, Y, Z\}$ and $j \in \{0, 1\}$. Note that a coherent state of intensity μ and global phase χ is a linear superposition of photon number states $\{|n\rangle\}$ of $|\sqrt{\mu}e^{i\chi}\rangle = \sum_{n=0}^{\infty} e^{-\mu/2} \frac{(\sqrt{\mu}e^{i\chi})^n}{\sqrt{n!}} |n\rangle$. Therefore, the single-photon part of the coherent states in Eq. (5.6) prepared by Alice and Bob can be expressed as

$$|\phi_{j\beta}\rangle_{A(B)} = \frac{1}{\sqrt{2}}(|1\rangle_r |0\rangle_s + e^{i(\theta_{A(B)}+\delta\theta_{A(B)}/\pi)} |0\rangle_r |1\rangle_s) \quad (5.7)$$

where 0 and 1 represent the photon number. From above representation we define $|1\rangle_r |0\rangle_s = |0_Z\rangle$, $|0\rangle_r |1\rangle_s = |1_Z\rangle$, $|0_X\rangle = \frac{1}{\sqrt{2}}(|0_Z\rangle + |1_Z\rangle)$, $|1_X\rangle = \frac{1}{\sqrt{2}}(|0_Z\rangle - |1_Z\rangle)$, $|0_Y\rangle = \frac{1}{\sqrt{2}}(|0_Z\rangle + i|1_Z\rangle)$ and $|1_Y\rangle = \frac{1}{\sqrt{2}}(|0_Z\rangle - i|1_Z\rangle)$. Therefore, Eq. (5.7) can be

equivalently rewritten as

$$e^{i\left(\frac{\theta_{A(B)} + \delta\theta_{A(B)}/\pi}{2}\right)} \left[\cos\left(\frac{\theta_{A(B)}}{2} + \frac{\delta}{2}\right) |0_X\rangle + i \sin\left(\frac{\theta_{A(B)}}{2} + \frac{\delta}{2}\right) |1_X\rangle \right]. \quad (5.8)$$

Similar expression as above can be obtained for the eigenstates $|0_Y\rangle, |1_Y\rangle$. If the overall phase factor in Eq. (5.8) is ignored, we obtain the following expressions for the four states

$$\begin{aligned} |\phi_{0Z}\rangle &= |0_Z\rangle \\ |\phi_{1Z}\rangle &= \frac{1}{\sqrt{2}}(|0_Z\rangle + |1_Z\rangle) \\ |\phi_{0X}\rangle &= \cos\left(\frac{0}{2} + \frac{\delta_1}{2}\right) |0_X\rangle + i \sin\left(\frac{0}{2} + \frac{\delta_1}{2}\right) |1_X\rangle \\ &= \cos\left(\frac{\delta_1}{2}\right) |0_X\rangle + i \sin\left(\frac{\delta_1}{2}\right) |1_X\rangle \\ |\phi_{0Y}\rangle &= \cos\left(\frac{\pi}{2} + \frac{\delta_2}{2}\right) |0_Y\rangle + i \sin\left(\frac{\pi}{2} + \frac{\delta_2}{2}\right) |1_Y\rangle, \end{aligned}$$

where $\theta_{A(B)} = 0, \pi/2$ for X and Y , respectively. These signal states can be written in terms of an identity ($\mathbb{1}$) and Pauli matrices (σ_z, σ_x and σ_y) and their density matrices representation are

$$\rho_{0Z} = |\phi_{0Z}\rangle\langle\phi_{0Z}| = (\mathbb{1} + \sigma_z)/2, \quad (5.9)$$

$$\begin{aligned} \rho_{1Z} &= |\phi_{1Z}\rangle\langle\phi_{1Z}| = \frac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \\ &= \frac{1}{2} \mathbb{1} - \frac{1}{2} \sigma_x, \end{aligned} \quad (5.10)$$

$$\begin{aligned} \rho_{0X} &= |\phi_{0X}\rangle\langle\phi_{0X}| \\ &= \frac{1}{2} \begin{bmatrix} \cos^2\left(\frac{\delta_1}{2}\right) + \sin^2\left(\frac{\delta_1}{2}\right) & \cos^2\left(\frac{\delta_1}{2}\right) + i \sin(\delta_1) - \sin^2\left(\frac{\delta_1}{2}\right) \\ \cos^2\left(\frac{\delta_1}{2}\right) - i \sin(\delta_1) - \sin^2\left(\frac{\delta_1}{2}\right) & \cos^2\left(\frac{\delta_1}{2}\right) + \sin^2\left(\frac{\delta_1}{2}\right) \end{bmatrix} \\ &= \frac{1}{2} \mathbb{1} + \frac{1}{2} \cos(\delta_1) \sigma_x, \end{aligned} \quad (5.11)$$

$$\begin{aligned}
\rho_{0Y} &= |\phi_{0Y}\rangle\langle\phi_{0Y}| = \begin{bmatrix} \frac{1}{2}\cos^2\Theta + \frac{1}{2}\sin^2\Theta & -\frac{i}{2}\cos^2\Theta + \frac{i}{2}\sin^2\Theta \\ & +\sin\Theta\cos\Theta \\ \frac{i}{2}\cos^2\Theta - \frac{i}{2}\sin^2\Theta & \frac{1}{2}\cos^2\Theta + \frac{1}{2}\sin^2\Theta \\ & +\sin\Theta\cos\Theta \end{bmatrix} \\
&= \frac{1}{2}\mathbb{1} + \frac{1}{2}\sin(2\Theta)\sigma_x,
\end{aligned} \tag{5.12}$$

where $\Theta = \frac{\pi}{2} + \frac{\delta_2}{2}$. From this representation of signal states, one can obtain the joint probability, $Y_{\Phi^\pm, j_\alpha k_\beta}$ that Alice (Bob) prepares any of the state $|\phi_{j_\alpha}\rangle(|\phi_{k_\beta}\rangle)$ ($j, k \in [0, 1]$) and Charlie declares $|\Phi^\pm\rangle$ by exploiting transmission rate of the Pauli operators and subsequently estimate error rates E_{XX} , E_{XY} , E_{YX} and E_{YY} used for calculating C . Here, we show how to estimate the phase error rate E_{XX} ; other parameters can be obtained similarly. The parameter E_{XX} is computed by considering a virtual protocol where Alice and Bob prepare entangled state $|\Psi_Z\rangle = \frac{1}{\sqrt{2}}(|0\rangle_{A(B)}|\phi_{0Z}\rangle_C + |1\rangle_{A(B)}|\phi_{1Z}\rangle_C)$, (here C denotes the system sent to Charlie) and measure their subsystems in the X basis when Charlie announces the measurement result $|\Phi^+\rangle$. The error rate is expressed as

$$E_{XX} = \frac{Y_{\Phi^+; 0_X 1_X}^{Z, \text{vir}} + Y_{\Phi^+; 1_X 0_X}^{Z, \text{vir}}}{Y_{\Phi^+; 0_X 1_X}^{Z, \text{vir}} + Y_{\Phi^+; 1_X 0_X}^{Z, \text{vir}} + Y_{\Phi^+; 0_X 0_X}^{Z, \text{vir}} + Y_{\Phi^+; 1_X 1_X}^{Z, \text{vir}}} \tag{5.13}$$

where $Y_{\Phi^+; j_X k_X}^{Z, \text{vir}}$ denotes the joint probability that Alice and Bob measured $|j_X\rangle$ and $|k_X\rangle$, respectively and Charlie declares the result $|\Phi^+\rangle$. In this hypothetical protocol, the state of pulses received by Charlie can be expressed as

$$\hat{\sigma}_{C; j_X k_X}^{\text{vir}} = \text{Tr}_{AB}[\hat{P}(|j_X\rangle_A) \otimes \hat{P}(|k_X\rangle_B) \otimes \mathbb{1}_C \hat{P}(|\Psi_Z\rangle_{AC} \otimes |\Psi_Z\rangle_{BC})]. \tag{5.14}$$

Here $\hat{P}(|x\rangle) = |x\rangle\langle x|$ corresponds to a projection operator for a particular pure state $|x\rangle$. The normalized state can be defined as $\hat{\sigma}_{C; j_X k_X}^{\text{vir}} = \hat{\sigma}_{C; j_X k_X}^{\text{vir}} / \text{Tr}(\hat{\sigma}_{C; j_X k_X}^{\text{vir}})$. The joint probability that Alice (Bob) measures $|j_X\rangle$ ($|k_X\rangle$) and Charlie declares $|\Phi^+\rangle$ is given by

$$Y_{\Phi^+; j_X k_X}^{Z, \text{vir}} = p(j_X)p(k_X)\text{Tr}(\hat{D}_{\Phi^+}\hat{\sigma}_{C; j_X k_X}^{\text{vir}}) \tag{5.15}$$

where $\hat{D}_{\Phi^+}$ is the operator that contains Eve's operation and Charlie's single photon Bell state measurement and $p(j_X)$, $p(k_X)$ represent the probabilities for Alice and Bob to choose X basis, respectively. Since the virtual state $\hat{\sigma}_{C; j_X k_X}^{\text{vir}}$ can also be

expressed in terms of identity and Pauli operators as

$$\hat{\sigma}_{C;j_X k_X}^{\text{vir}} = \frac{1}{2} \left(\mathbb{1} + \sum_{s=x,y,z} \mathbf{n}_s^{j_X} \hat{\sigma}_s \right) \otimes \frac{1}{2} \left(\mathbb{1} + \sum_{t=x,y,z} \mathbf{n}_t^{j_X} \hat{\sigma}_t \right), \quad (5.16)$$

it follows that Eq. (5.15) can be rewritten as

$$Y_{\Phi^+;j_X k_X}^{Z,\text{vir}} = p(j_X)p(k_X) \sum_{s,t=X,Y,Z} \mathbf{n}_s \mathbf{n}_t q_{\Phi^+|s,t}. \quad (5.17)$$

Therefore, to obtain $Y_{\Phi^+;j_X k_X}^{Z,\text{vir}}$, it suffices to calculate the transmission rate of Pauli operators defined by

$$q_{\Phi^+|s,t} = \text{Tr}(\hat{D}_{\Phi^+} \sigma_s \otimes \sigma_t) / 4 \quad (5.18)$$

with $s, t \in \{\mathbb{1}, X, Y, Z\}$. The parameters $\mathbf{n}_s$ and $\mathbf{n}_t$ denote the coefficients of Pauli matrices. Note that the transmission rate of operators can also be determined from the yield of signal states used in the actual protocol. To evaluate the yield of these states we employ the entanglement description where Alice (Bob) prepares state $|\Psi_Z\rangle = \frac{1}{\sqrt{2}}(|0_Z\rangle_{A(B)}|\phi_{0Z}\rangle_C + |1_Z\rangle_{A(B)}|\phi_{1Z}\rangle_C)$ in the Z basis and likewise the preparation of optical pulses in the complementary bases can be described as a process where Alice (Bob) generates $|\Phi_X\rangle = |0_X\rangle_{A(B)}|\phi_{0X}\rangle_C$ or $|\Phi_Y\rangle = |0_Y\rangle_{A(B)}|\phi_{0Y}\rangle_C$. By using the same method previously described for the yield of virtual states, we obtain the expression for the yield of actual states as

$$\begin{aligned} Y_{\Phi^+;j_\alpha k_\beta} &= p(j_\alpha)p(k_\beta) \text{Tr}(\hat{D}_{\Phi^+} \rho_{j_\alpha} \otimes \rho_{k_\beta}) \\ &= p(j_\alpha)p(k_\beta) \sum_{s,t=X,Y,Z} \mathbf{n}_s \mathbf{n}_t q_{\Phi^+|s,t} \end{aligned} \quad (5.19)$$

with $p(j_\alpha)$ and $p(k_\beta)$ denoting probabilities for Alice and Bob to measure their subsystems as state j_α and k_β , respectively. The states ρ_{j_α} and ρ_{k_β} correspond to the four states defined in Eqs. (5.9) to (5.12). We demonstrate in Appendix C.1 that explicit computation of Eq. (5.17) can lead to the realization of the transmission rate of identity and Pauli operators $q_{\Phi^+|s,t}$. Furthermore, in Appendix C.2, we determine the transmission rate of operators from the yield of actual states as defined in Eq. (5.19). By combining the results of Eqs. (C.13) and (C.34), we can deduce the yield of virtual states and subsequently obtain the error rate E_{XX} using Eq. (5.13).

Indeed, with this formalism of estimating error rate E_{XX} , we have shown that it is possible to obtain the yield of states which have not been sent during the actual protocol, such as $Y_{\Phi^+;1_X1_X}^{Z,\text{vir}}$. We have shown how to represent this yield in terms of the transmission rate of identity and Pauli operators in Eq. (C.4). Furthermore, we demonstrated how to obtain the transmission rate of Pauli operators from the yield of states used in the actual protocol in Appendix C.2, hence enabling us to substitute the obtained results into Eq. (C.4), and subsequently obtaining $Y_{\Phi^+;1_X1_X}^{Z,\text{vir}}$. The same argument can be used to obtain the yield of states such as $Y_{\Phi^+;1_X1_Y}^{Z,\text{vir}}$, $Y_{\Phi^+;1_Y1_X}^{Z,\text{vir}}$ and $Y_{\Phi^+;1_Y1_Y}^{Z,\text{vir}}$ which are used to obtain error rates E_{XY} , E_{YX} and E_{YY} , respectively. Remarkably, the error rates obtained are the same as the ones achieved for protocol employing two orthonormal states from the X and Y bases. Therefore, additional states, $|\phi_{1X}\rangle$ and $|\phi_{1Y}\rangle$ that are used in the six-state protocol seem to be redundant.

5.4 Estimation of key generation rate

In our protocol, Alice and Bob never reveal their random phase for coherent states prepared in the key (Z) basis. Therefore, the phase randomized coherent states $|\sqrt{\mu}e^{i\chi}\rangle$ prepared by Alice and Bob can be described as

$$\int_0^{2\pi} |\sqrt{\mu}e^{i\chi}\rangle \langle \sqrt{\mu}e^{i\chi}| d\chi = \sum_0^\infty \frac{e^{-\mu} \mu^n}{n!} |n\rangle \langle n|, \quad (5.20)$$

which is a classical mixture of photon number states. This means that the photon number channel model [292] holds and tagging method [51] proposed by Gottesman et al. can be employed in our protocol. Therefore, the key generation rate for RFI TF-QKD is given by

$$R = q[-f_{EC}Q_\mu^Z H(E_\mu^Z) + Q_1^Z(1 - I_E)]. \quad (5.21)$$

where q is the sifting factor and in an asymmetric encoding $q \sim 1$ for an infinitely large number of signals. The terms Q_μ^Z and E_μ^Z correspond to the gain and quantum bit error rate (QBER) in the Z basis. According to the decoy-state theory, the overall gain is given by [50]

$$Q_\mu^Z = \sum_{n=0}^\infty Y_n \frac{\mu^n}{n!} e^{-\mu}, \quad (5.22)$$

and the corresponding quantum bit error rate is given by

$$E_\mu^Z Q_\mu^Z = \frac{1}{2}e^\mu Y_0 + e_1^Z \mu e^{-\mu} Y_1 + \sum_{n \geq 2} e_1^Z \frac{\mu e^{-\mu}}{n!} Y_n. \quad (5.23)$$

The gain for single photon components in the Z basis is expressed as

$$Q_1^Z = \mu e^{-\mu} (Y_{\Phi^\pm;0Z0Z}^1 + Y_{\Phi^\pm;0Z1Z}^1 + Y_{\Phi^\pm;1Z0Z}^1 + Y_{\Phi^\pm;1Z1Z}^1). \quad (5.24)$$

The parameter I_E is estimated from the lower bound of C and upper bound on the error rate, $E_{ZZ}^{1,U}$ from single-photon contributions as shown in Eq. (5.2). The parameter $E_{ZZ}^{1,U}$ is estimated from the yield of single photons as follows

$$E_{ZZ}^{1,U} = \frac{E_\mu^Z Q_\mu^Z - e_0 Y_0 e^{-\mu}}{e^{-\mu} (Y_{\Phi^\pm;0Z0Z}^{1,L} + Y_{\Phi^\pm;0Z1Z}^{1,L} + Y_{\Phi^\pm;1Z0Z}^{1,L} + Y_{\Phi^\pm;1Z1Z}^{1,L})}, \quad (5.25)$$

where

$$Y_{\Phi^\pm;j\alpha s\beta}^{1,L} = \frac{\mu}{\mu\nu - \nu^2} \left[Q_{\nu;j\alpha k\beta} e^\nu - Q_{\mu;j\alpha k\beta} \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Q_0 \right]. \quad (5.26)$$

The values $Q_{\nu;j\alpha k\beta}$, $Q_{\mu;j\alpha k\beta}$ are gains obtained on conditional probabilities that Alice and Bob measure the states $j\alpha$, $k\beta$ while Q_0 is the background gain. Finally, the parameter C is computed from the error rates in complementary bases as follows

$$C = (1 - 2E_{XX})^2 + (1 - 2E_{XY})^2 + (1 - 2E_{YX})^2 + (1 - 2E_{YY})^2. \quad (5.27)$$

These error rates are computed using yields obtained from the virtual protocol, which are evaluated as shown in the previous section.

5.4.1 Simulation of the key rate

We demonstrate the performance of the proposed protocol based on fibre implementation. The simulation formulas for parameters Q_μ^Z and E_μ^Z are given in Appendix D.2. We set intensity parameters for Alice and Bob at $u_{a,b} = 0.6$ and $v_{a,b} = 0.053$. We also assume Charlie uses detectors with efficiency $\eta_{\text{det}} = 14.5\%$ and the dark count rate is assumed to be $p_d = 5 \times 10^{-7}$ which is in line with the current technolo-

gies [293–295]. The channel loss coefficient is $\alpha = 0.2\text{dBkm}^{-1}$ and its transmittance is $\eta_{\text{ch}} = 10^{-\frac{0.1\alpha L}{2}}$, with L denoting the fibre length. We consider error correction efficiency, $f_{\text{EC}} = 1.16$.

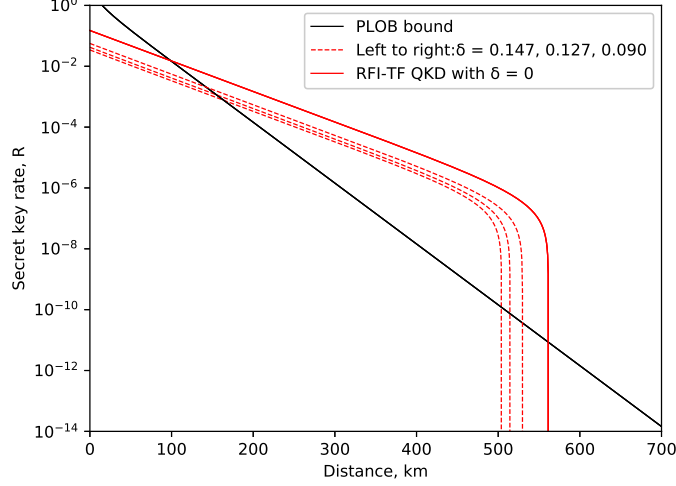


Figure 5.2: Secret key rate (in logarithmic scale) for RFI-TF protocol with source flaws (dashed lines) as a function of transmission distance measured in km, for experimental parameters: dark counts rate, $p_d = 5 \times 10^{-7}$, the loss coefficient of the channel, $\alpha = 0.2 \text{ km/dB}$, the detection efficiency, $\eta = 14.5\%$. From left to right, the plots represent the encoding flaws $\delta = 0.147$, $\delta = 0.127$ and $\delta = 0.090$. The solid line corresponds to the RFI-TF protocol with perfect encoding, and the solid black line represents the PLOB bound [102].

Our simulation results are depicted in Figure 5.2 and Figure 5.3. In Figure 5.2 the plots were obtained with $\delta = 0.090$, $\delta = 0.127$ and $\delta = 0.147$, which correspond to deviation of 5.15° , 7.28° and 8.42° from the desired phase angle, respectively. For comparison, we plotted the curve for $\delta = 0$, corresponding to the perfect encoding scenario. The characterization of parameter δ is based on its relation to the extinction ratio according to the definition; $|\tan(\delta/2)|^2 = \eta_{\text{ex}}$ [297]. The non-zero extinction ratio is mainly due to imperfections in phase modulators and is of order 10^{-3} in typical experiments. For this value of extinction ratio, we obtain $\delta \approx 0.063$. However, in our simulation, we chose pessimistic values to estimate encoding imperfection to demonstrate the capability of beating repeaterless bound with currently available devices. The results demonstrate that the key rates achieved are comparable to the perfect encoding scenario despite increased encoding flaws. It is also evident that our protocol implemented with an imperfect source still achieves transmission distances that are beyond the PLOB bound for repeaterless QKD [102]. We obtain the maximum transmission distance of 505 km, 516 km and

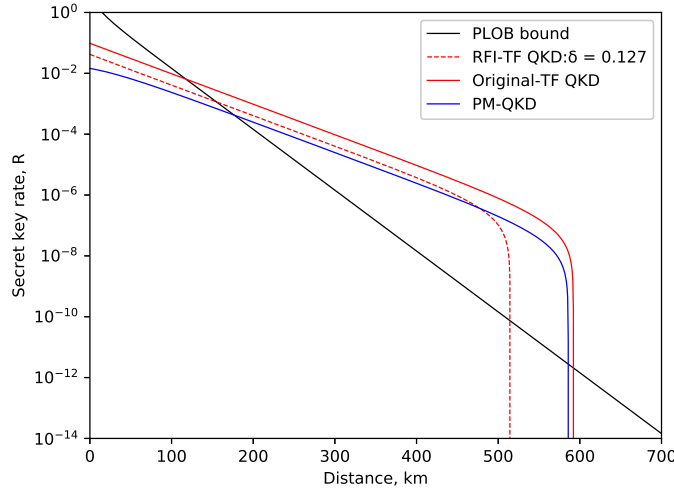


Figure 5.3: Secret key rate (in logarithmic scale) for RFI-TF protocol with $\delta = 0.127$ (dashed line) as a function of transmission distance measured in km, for experimental parameters: dark counts rate, $p_d = 5 \times 10^{-7}$, loss coefficient of the channel, $\alpha = 0.2$ km/dB, the detection efficiency, $\eta = 14.5\%$. For comparison purposes, we plot the curve for Phase matching (PM) QKD [296] denoted by the blue solid line. The solid red line corresponds to the original TF protocol [106] and the black solid line represents the PLOB bound [102].

530 km for preparation flaws $\delta = 0.147$, $\delta = 0.127$ and $\delta = 0.090$, respectively. For comparison, the curves for original TF QKD [106], Phase matching (PM) QKD [296] and RFI-TF QKD are plotted in Figure 5.3. The results show that the original TF QKD attains a maximum transmission distance of 592 km and RFI-TF QKD can reach a maximum secure distance of 516 km. At a distance of 0 km, the key rate for original TF QKD and RFI-TF QKD are 9.10×10^{-2} and 4.90×10^{-2} , respectively. The gap between the two curves is small and almost remains constant when the distance increases. This demonstrates that the performance of RFI-TF QKD is still comparable to the original TF-QKD. It is also evident that PM QKD outperforms our proposed protocol in terms of maximum transmission distance realized. However, our protocol achieves slightly better key rates at shorter distances than the PM QKD. Moreover, the merit of the RFI-TF QKD protocol is that it eliminates the need for aligning reference frames and active phase stabilization.

Furthermore, we compare our results with some TF QKD schemes in the literature. More recently, Tamaki et al. [298] proposed a modified version of the original TF QKD, which employs a testing mode for monitoring an eavesdropper and the coding mode for key generation. The phase error rate is estimated in their protocol by considering the bias between two bases (coding and testing modes). On

the contrary, our protocol exploits the mismatched basis data to determine error rates in complementary bases (X, Y) to estimate Eve's information. Also, our protocol employs the GLLP tagging key rate method [51] since Alice and Bob never reveal the phase information in the key basis. Hence, their coherent states are regarded as a mixture of photon number states in the Fock space. In contrast, the GLLP tagging model does not hold in the protocol by Tamaki et al. [298] since Alice and Bob announce the phase information in the coding mode. Remarkably, our simulation results agree very well with their results. The observed superiority in their results compared to ours may be attributed to a different choice of experimental parameters and the fact that we consider the source flaws in our analysis.

Moreover, we compare our protocol's performance with a TF variant scheme proposed by Lin et al. [299]. The first noticeable difference between this work and ours is in key generation mode. In their protocol, Lin et al. consider phase-matching coherent states for key generation purposes, while in our protocol, we exploit vacuum and phase-randomized coherent states to extract secure keys. As already stated, our approach enables us to use the traditional BB84 tagging key generation formula since the phase-randomized coherent states are regarded as a mixture of photon number states. However, the method is not applicable to the scheme in [299]. Moreover, the scheme in [299] employs non-phase randomized coherent test states to perform a variation of tomography on the quantum channel to deduce the information leaked to Eve. In our approach, we use the yields of rejected data to estimate the error rates in the X and Y bases, which are used to deduce Eve's information. Regarding maximum attainable distances, we observe that our protocol outperforms the scheme proposed in [299]. We obtained a maximum distance of approximately 500 km, while a distance of 400 km was achieved for the previous scheme. We emphasize that optical devices are available for the practical implementation of our proposed twin-field RFI protocol. Experimental setups for the "sending or not sending" twin-field QKD scheme have already been developed and successfully demonstrated [108, 288]. These setups are compatible with our proposed RFI twin-field QKD protocol and can be directly adapted for its practical implementation.

5.5 Conclusion

We proved the security of the RFI-TF QKD protocol with state preparation flaws. Our results demonstrate that our protocol can overcome the repeaterless PLOB bound. In addition, our protocol is capable of extracting a secure key over a transmission distance of $l=505$ km, $l=516$ km and $l=530$ km for encoding flaws $\delta = 0.090$, $\delta = 0.127$ and $\delta = 0.147$, which corresponds to the deviation of 5.15° , 7.28° and 8.42° from the desired phase angle, respectively. The results show that despite the state preparation flaws, the key rates achieved are still comparable to those of perfect encoding scenarios. The results show that despite the state preparation flaws, the key rates achieved are still comparable to perfect encoding scenarios. Although our protocol cannot achieve a transmission distance beyond the original TF-QKD protocol, its most significant advantage is that it can be implemented without aligning reference frames, eliminating the need for active stabilization of interferometers.

High dimensional QKD with biphotons

6.1 Introduction

In this chapter, we present a high-dimensional MDI-QKD protocol that encodes information on qutrit states by exploiting the polarization state of single-mode biphoton field. Using biphotons as qutrits enhances the attainable secret key rate and security due to improved information capacity per photon and the high noise tolerance [300]. To examine the practicality of the proposed protocol, we investigate the finite-key bounds against the general attacks based on entropic uncertainty relations. Moreover, this security analysis pertains to the implementation using the decoy states. This enables the proposed protocol to be secure against Photon-Number-Splitting (PNS) attacks [220]. For the finite-key study, the statistical fluctuations are catered by leveraging the large deviation theory, particularly the multiplicative Chernoff bound [301]. This bound provides the tightest bounds on estimated parameters for the high-loss regime. This chapter is based on the work in Ref. [199].

6.2 Protocol Definition

Biphotons

The pure polarization state for a single-mode biphoton field is expressed according to the following [152, 300]:

$$|\Phi\rangle = c_1|2_h, 0_v\rangle + c_2|1_h, 1_v\rangle + c_3|0_h, 2_v\rangle, \quad (6.1)$$

where $c_i = |c_i|e^{i\phi_i}$ are complex amplitudes. The notation $|n_h, n_v\rangle$ represents a state that consists of n photons in the horizontal (h) mode as well as n photons in the vertical (v) polarization mode. Therefore, from Eq. (6.1), we can observe that a biphoton has a three-level quantum system (qutrit) representation, hence its use for ternary quantum information encoding. To realize the QKD protocol, one needs at least two mutually unbiased bases (MUB) from available $d+1$ MUBs. The two orthonormal bases $\mathcal{M}_1 = |\phi\rangle_i$, where $i \in \{0, 1, 2\}$ and $\mathcal{M}_2 = |\Phi\rangle_j$, where $j \in \{0, 1, 2\}$ for a 3-dimensional Hilbert space $\mathcal{H}_3$ are considered mutually unbiased when all pairs of basis vectors $|\phi\rangle_i$ and $|\Phi\rangle_j$ satisfies

$$|\langle\phi_i|\Phi_j\rangle|^2 = \frac{1}{3}. \quad (6.2)$$

For biphotons, the standard basis is expressed in terms of the orthonormal states $|\alpha\rangle = |2_h, 0_v\rangle$, $|\beta\rangle = |0_h, 2_v\rangle$ and $|\gamma\rangle = |1_h, 1_v\rangle$. The states $|2_h, 0_v\rangle$ and $|0_h, 2_v\rangle$ represent type-I phase matching, while $|1_h, 1_v\rangle$ corresponds to type II phase matching, and one can obtain these biphoton fields through spontaneous parametric down-conversion (SPDC). The other three MUBs are realized from the superposition of the basis vectors as follows

$$|\acute{\alpha}\rangle = \frac{1}{\sqrt{3}}(|\alpha\rangle + |\beta\rangle + |\gamma\rangle) \quad (6.3)$$

$$|\acute{\beta}\rangle = \frac{1}{\sqrt{3}}(|\alpha\rangle + \omega|\beta\rangle + \omega^2|\gamma\rangle) \quad (6.4)$$

$$|\acute{\gamma}\rangle = \frac{1}{\sqrt{3}}(|\alpha\rangle + \omega^2|\beta\rangle + \omega|\gamma\rangle), \quad (6.5)$$

$$|\bar{\alpha}\rangle = \frac{1}{\sqrt{3}}(|\alpha\rangle + |\beta\rangle + \omega|\gamma\rangle) \quad (6.6)$$

$$|\bar{\beta}\rangle = \frac{1}{\sqrt{3}}(|\alpha\rangle + \omega|\beta\rangle + |\gamma\rangle) \quad (6.7)$$

$$|\bar{\gamma}\rangle = \frac{1}{\sqrt{3}}(\omega|\alpha\rangle + |\beta\rangle + |\gamma\rangle), \quad (6.8)$$

and

$$|\tilde{\alpha}\rangle = \frac{1}{\sqrt{3}}(|\alpha\rangle + |\beta\rangle + \omega^2|\gamma\rangle) \quad (6.9)$$

$$|\tilde{\beta}\rangle = \frac{1}{\sqrt{3}}(|\alpha\rangle + \omega^2|\beta\rangle + |\gamma\rangle) \quad (6.10)$$

$$|\tilde{\gamma}\rangle = \frac{1}{\sqrt{3}}(\omega^2|\alpha\rangle + |\beta\rangle + |\gamma\rangle), \quad (6.11)$$

where $\omega = \exp(i2\pi/3)$. In our scenario, to realize high dimensional encoding with biphotons, we propose an MDI-QKD protocol exploiting two Fourier transformed bases, $\mathcal{M}_1 = \{|\acute{\alpha}\rangle, |\acute{\beta}\rangle, |\acute{\gamma}\rangle\}$ and $\mathcal{M}_2 = \{|\bar{\alpha}\rangle, |\bar{\beta}\rangle, |\bar{\gamma}\rangle\}$.

Preparation of states

Alice (Bob) starts by randomly preparing qutrit states from two mutually unbiased bases $\mathcal{M}_1 = \{|\acute{\alpha}\rangle, |\acute{\beta}\rangle, |\acute{\gamma}\rangle\}$ and $\mathcal{M}_2 = \{|\bar{\alpha}\rangle, |\bar{\beta}\rangle, |\bar{\gamma}\rangle\}$. The biphoton states $\{|\acute{\alpha}\rangle, |\bar{\alpha}\rangle\}$, $\{|\acute{\beta}\rangle, |\bar{\beta}\rangle\}$ and $\{|\acute{\gamma}\rangle, |\bar{\gamma}\rangle\}$ are assigned bit values 0, 1 and 2, (the value 2 is converted to binary digit during sifting to obtain two bits per signal) respectively. The states are prepared using a Mach-Zehnder interferometer consisting of 3 arms and appropriate non-linear crystals in each arm. This is illustrated in Figure 6.1. The laser beam is pumped onto a non-symmetric beam-splitter that transmits two-thirds of the beam through the interferometer's long arm and reflects the other beam via the short arm. The beam in the long arm is pumped towards the type I non-linear crystals for generating states $|2_h, 0_v\rangle$ and $|0_h, 2_v\rangle$, resulting in a superposition

$$|\Phi\rangle = c_1|2_h, 0_v\rangle + e^{i\phi_{31}}c_3|0_h, 2_v\rangle, \quad (6.12)$$

with $e^{i\phi_{31}}$ representing the relative phase between the states realized through phase shifters. The half-wave plate is used for manipulating the amplitudes of these states. A cut-off filter is employed to remove the pump. After passing through the filter, the states arrive at the piezoelectric translator, where the phase shift, ϕ_2 , is introduced between the superposition of states defined in Eq. (6.12) and

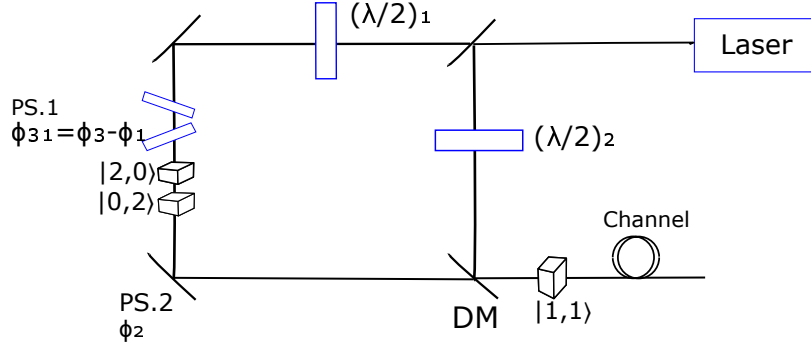


Figure 6.1: Mach-Zehnder interferometer set up used by Alice and Bob for biphoton state preparation. The laser beam is pumped towards a non-symmetric beam-splitter that transmits 2/3 and reflects 1/3 of the beam through the long and short arms. The $(\lambda/2)_i$ represents the half wave plates for manipulating the amplitude, c_i of the states. The phase shifters (PS. 1 and PS. 2) introduce relative phases between the states. The DM denotes the dichroic mirror, which transmits two biphotons created using type I non-linear crystals from the long arm of the interferometer and reflects the pump from the short arm towards the type II non-linear crystal for the creation of state $|1_h, 1_v\rangle$.

the state $|1_h, 1_v\rangle$. The reflected beam traveling through the short arm is guided towards the half-wave plate to control the amplitude corresponding to the state $|1_h, 1_v\rangle$. The pump is reflected at the dichroic mirror towards the type II non-linear crystals to create the state $|1_h, 1_v\rangle$. The type I biphotons from the long arm of the interferometer are transmitted via the dichroic mirror. Thus, at the interferometer's output, we have the superposition of three basic states in Eq. (6.1), which are then propagated through the insecure channel to the measurement site. Different states from two mutually unbiased bases are produced by adjusting the phase shifters and half wave plates according to Table 6.1.

Table 6.1: The parameter settings for biphoton states from two mutually unbiased bases used in our QKD scheme. The complex amplitudes $|c_i|$ are realized through the use of half-wave plates. The ϕ_i are realized by use of phase shifters.

State	$ c_1 $	$ c_2 $	$ c_3 $	ϕ_1	ϕ_2	ϕ_3
$ \acute{\alpha}\rangle$	$\frac{1}{\sqrt{3}}$	$\frac{1}{\sqrt{3}}$	$\frac{1}{\sqrt{3}}$	0	0	0
$ \acute{\beta}\rangle$	$\frac{1}{\sqrt{3}}$	$\frac{1}{\sqrt{3}}$	$\frac{1}{\sqrt{3}}$	0	120°	-120°
$ \acute{\gamma}\rangle$	$\frac{1}{\sqrt{3}}$	$\frac{1}{\sqrt{3}}$	$\frac{1}{\sqrt{3}}$	0	-120°	120°
$ \bar{\acute{\alpha}}\rangle$	$\frac{1}{\sqrt{3}}$	$\frac{1}{\sqrt{3}}$	$\frac{1}{\sqrt{3}}$	120°	0	0
$ \bar{\acute{\beta}}\rangle$	$\frac{1}{\sqrt{3}}$	$\frac{1}{\sqrt{3}}$	$\frac{1}{\sqrt{3}}$	0	120°	0
$ \bar{\acute{\gamma}}\rangle$	$\frac{1}{\sqrt{3}}$	$\frac{1}{\sqrt{3}}$	$\frac{1}{\sqrt{3}}$	0	0	120°

Measurement

Charlie allows the biphotons from Alice and Bob to interfere in a symmetric beam-splitter upon receiving the states (see Figure 6.2). As a result, the Hong Ou Mandel effect occurs. The beam-splitter action can be described as follows. Let us assume

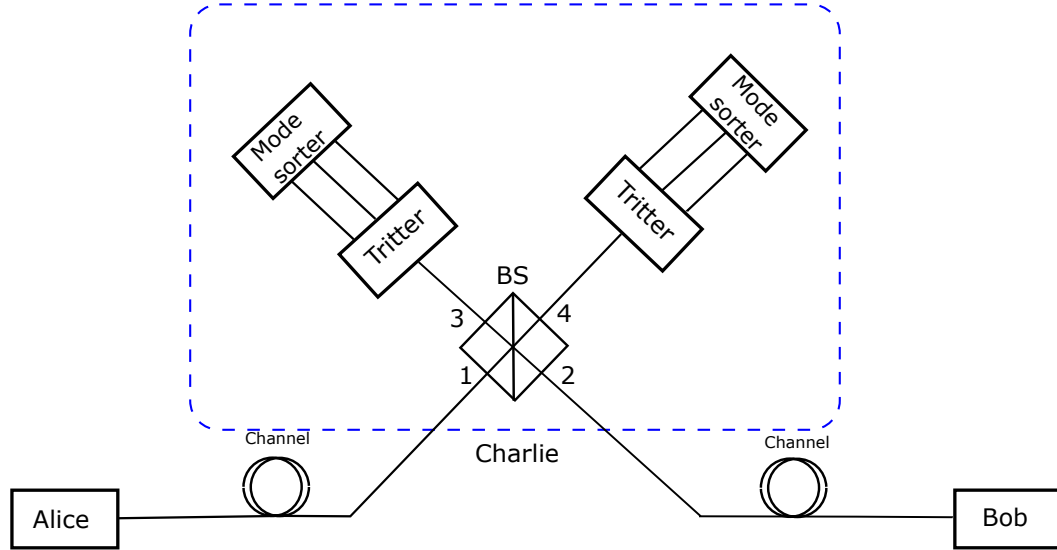


Figure 6.2: The generic measurement set up for our proposed MDI-QKD. Alice and Bob start by preparing the biphoton states from two mutually unbiased bases and sending them to Charlie through the unsecured channel. Charlie allows the states to interfere in the symmetric beam-splitter (BS) upon receiving the states. The photons are directed towards the tritter and eventually detected in the Brown Twiss scheme (mode sorter).

Alice's biphoton state at the input arm of the beam-splitter is denoted by $|\psi\rangle_1$, then its transformation can be described as

$$a_1^\dagger |\psi\rangle_1 \rightarrow \frac{1}{\sqrt{2}}(|\psi\rangle_3 + |\bar{\psi}\rangle_4). \quad (6.13)$$

Similarly if Bob's state at the input arm is $|\psi\rangle_2$ then the action of the beam-splitter is described as

$$a_2^\dagger |\psi\rangle_2 \rightarrow \frac{1}{\sqrt{2}}(|\bar{\psi}\rangle_3 - |\psi\rangle_4), \quad (6.14)$$

where $a_i^\dagger$ denotes the creation operator and $|\bar{x}\rangle$ is the reflected state. The overall beam-splitter transformations are described as

$$\begin{aligned}
|\psi\rangle_1|\psi\rangle_2 &\xrightarrow{BS} \frac{1}{\sqrt{2}}(|\psi\rangle_3 + |\bar{\psi}\rangle_4) \otimes \frac{1}{\sqrt{2}}(|\bar{\psi}\rangle_3 - |\psi\rangle_4) \\
&= \frac{1}{\sqrt{2}}(|\psi\rangle_3|\bar{\psi}\rangle_3 - |\psi\rangle_3|\psi\rangle_4 + |\bar{\psi}\rangle_4|\bar{\psi}\rangle_3 - |\bar{\psi}\rangle_4|\psi\rangle_4) \\
&= \frac{1}{\sqrt{2}}(|\Psi^+\rangle + |\Psi^-\rangle)
\end{aligned} \tag{6.15}$$

where

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|\psi\rangle_3|\bar{\psi}\rangle_3 - |\bar{\psi}\rangle_4|\psi\rangle_4) \tag{6.16}$$

and

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|\bar{\psi}\rangle_4|\bar{\psi}\rangle_3 - |\psi\rangle_3|\psi\rangle_4). \tag{6.17}$$

The subscripts 1, 2, and 3, 4 denote a beam-splitter's input and output ports, respectively. According to the Hong Ou Mandel interference, identical photons will leave the beam-splitter from a similar output port, and distinguishable photons from both input ports of the beam-splitter will exit in both output ports. Let Alice and Bob choose a similar biphoton states $|\alpha_A\rangle$ and $|\alpha_B\rangle$, respectively. Therefore, based on the Hong Ou Mandel interference, the state $|\Psi^-\rangle$ in Eq. (6.17) will disappear, and the resultant state is

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|\alpha_A\rangle_3|\bar{\alpha}_B\rangle_3 - |\bar{\alpha}_B\rangle_4|\alpha_A\rangle_4). \tag{6.18}$$

Therefore, identical biphotons will always appear in the same output arm of BS (3rd arm or 4th arm). Otherwise, if Alice and Bob prepare opposite biphotons, both $|\Psi^-\rangle$ and $|\Psi^-\rangle$ will exist, and there is a non-zero probability that the biphotons will exit at both output arms of the BS. The photons that exit the beam-splitter are transmitted toward the three input-output ports beam-splitter (tritter). The photons are directed toward the two non-polarizing beam-splitters to separate them into three channels from each output of the symmetric beam-splitter connected to each input of the two tritters (See Figure 6.3). The probability of photons exiting

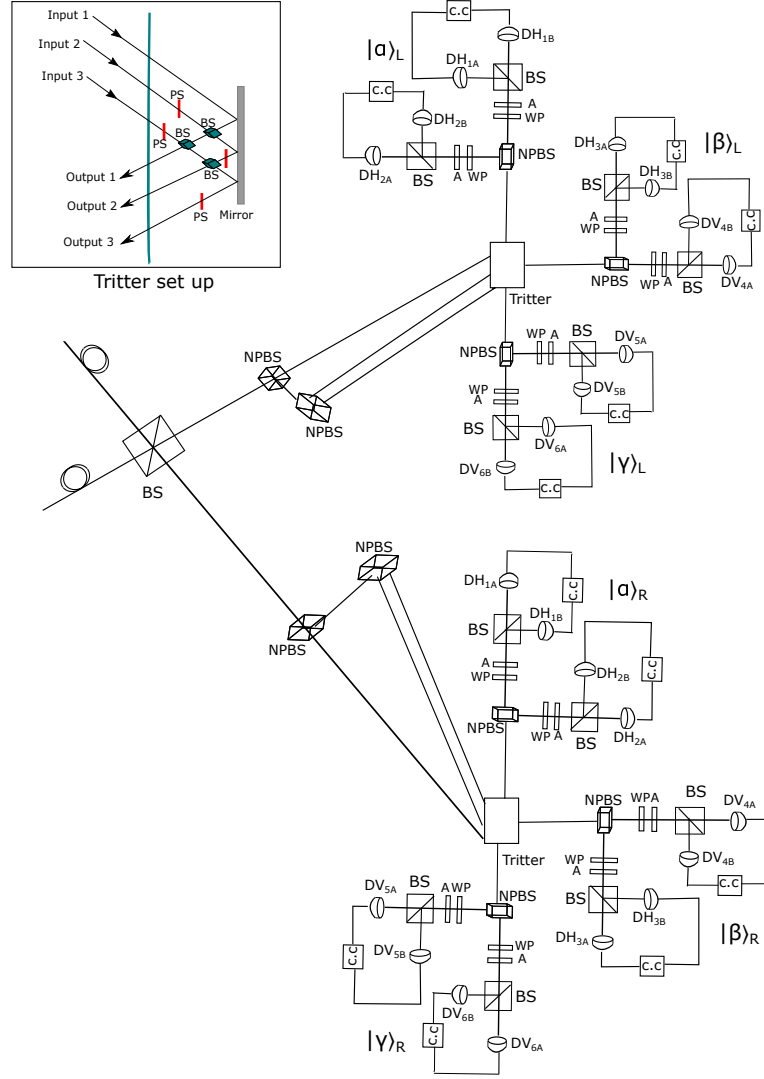


Figure 6.3: Illustration of the measurement set up at Charlie's site. The incoming biphotons interfere in the beam-splitter (BS) and exit through either of two output ports towards the two non-symmetric beam-splitter (NPBS), where they are further split into three channels and directed towards the tritter. The tritter setup shown in the upper left is a three-input-output port splitter. It comprises three conventional beam-splitters (BS), four-phase shifters (PS), and a mirror. The output ports of the tritter are linked with three Brown Twiss schemes for detecting the three basic states $|\alpha\rangle$, $|\beta\rangle$, and $|\gamma\rangle$. Each Brown Twiss scheme consists of a non-symmetric beam-splitter (NPBS), wave plates (WP), polarization analyzer (A), and detectors (DP_i) where $\mathbf{P} \in \{H, V\}$ represents polarization mode and subscript i denotes single photons forming biphotons. The abbreviation c.c corresponds to coincident counting or detection.

through any of the output ports of the tritter is governed by the unitary matrix

$$\mathcal{U} = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & e^{i2\pi/3} & e^{i4\pi/3} \\ 1 & e^{i4\pi/3} & e^{i8\pi/3} \end{pmatrix}. \quad (6.19)$$

In a case where each input of the tritter is injected with biphoton state, the resultant output state after the evolution induced by $\mathcal{U}$ is given by

$$|1, 1, 1\rangle \xrightarrow{\mathcal{U}} \sqrt{\frac{2}{3}}|3, 0, 0\rangle - \frac{1}{\sqrt{3}}|1, 1, 1\rangle, \quad (6.20)$$

where $|1, 1, 1\rangle$ corresponds to one biphoton state in each input or output of the tritter, and $|3, 0, 0\rangle$ represents three biphoton states exiting through one output port and no photons in the other two output ports. The output ports of each tritter are linked with three biphoton mode sorters. At the output of each tritter, the biphoton states from Alice and Bob are directed towards the Brown Twiss schemes, which are tuned to measure the standard basis biphoton modes $|\alpha\rangle$, $|\beta\rangle$ and $|\gamma\rangle$. Each Brown Twiss scheme is made up of polarization filters in the arms. The filters comprise a pair of phase-plates and a polarization analyzer used to realize the polarization states of single-photons creating the biphoton. Each Brown Twiss scheme is tuned to detect a certain polarization state of biphoton by setting wave plates ($\lambda/4$ plate, $\lambda/2$ plate) to angle positions that realize desired polarization and setting the polarization analyzer to allow the desired polarization to pass through. Table 6.2 shows different angle settings for wave plates. When a Brown Twiss scheme is tuned to the settings for detecting specific polarization states, the orthogonal biphoton states cannot result in coincidence detection. For instance, in the Brown Twiss scheme used to detect $|\beta\rangle$ biphoton mode, there are two detectors for the horizontal polarization contributions from Alice and Bob's biphoton states, which are labelled as D_{HA} and D_{HB} . Furthermore, there are two detectors for measuring the vertical polarization contributions of biphoton states from Alice and Bob labelled as D_{VA} and D_{VB} as shown in Figure 6.3. Similarly, appropriate parameters are set in the filters of both arms of the Brown Twiss scheme for detecting other states to allow coincidence detection. Note that states prepared by Alice and Bob are a

Table 6.2: The parameter settings for wave plates in the Brown Twiss schemes.

Wave plate	$ \alpha\rangle$			$ \beta\rangle$		$ \gamma\rangle$
	H	H	H	V	V	V
$\lambda/4$	$-\frac{\pi}{4}$	$-\frac{\pi}{4}$	$-\frac{\pi}{4}$	$-\frac{\pi}{4}$	$-\frac{\pi}{4}$	$-\frac{\pi}{4}$
$\lambda/2$	$\frac{\pi}{8}$	$\frac{\pi}{8}$	$\frac{\pi}{8}$	$-\frac{\pi}{8}$	$-\frac{\pi}{8}$	$-\frac{\pi}{8}$

superposition of the three basic states $|\alpha\rangle$, $|\beta\rangle$ and $|\gamma\rangle$. Therefore, a successful Bell state measurement in the Brown Twiss scheme corresponds to the observation of precisely 12 detectors being triggered; for instance, D_{H1A} , D_{H1B} , D_{H2A} and D_{H2B} (associated with $|\alpha\rangle_L$ biphoton mode), D_{H3A} , D_{H3B} , D_{V4A} and D_{V4B} (associated

with $|\beta\rangle_L$ biphoton mode) and D_{V5A} , D_{V5B} , D_{V6A} and D_{V6B} (associated with $|\gamma\rangle_L$ biphoton mode). These measurement results can be simplified in terms of Bell measurements as $\frac{1}{\sqrt{2}}(D_{\alpha_L}D_{\beta_L}D_{\gamma_L} + D_{\alpha_R}D_{\beta_R}D_{\gamma_R})$ which represent a click in detectors on the left-hand side for $|\alpha\rangle$, $|\beta\rangle$ and $|\gamma\rangle$ modes (i.e., D_{α_L} denotes coincidence detection in detectors of $|\alpha\rangle$ mode) or a click on the right-hand side for $|\alpha\rangle$, $|\beta\rangle$ and $|\gamma\rangle$ modes detectors. A conclusive result is given by clicking in detectors of the mode sorters on the left-hand side or the right-hand side only. The other Bell state measurements result in inconclusive measurement results, e.g., $\frac{1}{\sqrt{2}}(D_{\alpha_L}D_{\beta_L}D_{\gamma_R} + D_{\alpha_R}D_{\beta_R}D_{\gamma_L})$. The results are provided in Table 6.3.

Table 6.3: The possible Bell state measurement results in the Brown Twiss scheme mode sorting.

Charlie's measurement results	States sent by Alice and Bob		
	$ \acute{\alpha}\rangle$ or $ \bar{\alpha}\rangle$	$ \acute{\beta}\rangle$ or $ \bar{\beta}\rangle$	$ \acute{\gamma}\rangle$ or $ \bar{\gamma}\rangle$
$D_{\alpha_L}D_{\beta_L}D_{\gamma_L}$	Conclusive	Conclusive	Conclusive
$D_{\alpha_R}D_{\beta_R}D_{\gamma_R}$	Conclusive	Conclusive	Conclusive
$D_{\alpha_L}D_{\beta_L}D_{\gamma_R}$	Inconclusive	Inconclusive	Inconclusive
$D_{\alpha_L}D_{\beta_R}D_{\gamma_R}$	Inconclusive	Inconclusive	Inconclusive
$D_{\alpha_L}D_{\beta_R}D_{\gamma_L}$	Inconclusive	Inconclusive	Inconclusive
$D_{\alpha_R}D_{\beta_L}D_{\gamma_L}$	Inconclusive	Inconclusive	Inconclusive
$D_{\alpha_R}D_{\beta_L}D_{\gamma_R}$	Inconclusive	Inconclusive	Inconclusive
$D_{\alpha_R}D_{\beta_R}D_{\gamma_L}$	Inconclusive	Inconclusive	Inconclusive

Sifting

Alice and Bob post select states prepared using the same basis when Charlie reports a conclusive event and discards the rest of the data. A conclusive event corresponds to a case where there is a coincidence detection in three Brown Twiss schemes (linked to the same tritter) for three different basis states $|\alpha\rangle$, $|\beta\rangle$ and $|\gamma\rangle$. This occurs when Alice and Bob have prepared the same biphoton state. We define the set $\mathcal{K}$ comprising of biphoton signals if Alice and Bob selected the key basis $\mathcal{M}_1$ and Charlie gets a successful measurement. Similarly, $\mathcal{C}$ is a set of post-selected signals from measurement basis $\mathcal{M}_2$, which are used for monitoring the presence of an adversary. The protocol repeats the first steps until the sifting conditions $|\mathcal{K}| \geq n$ and $|\mathcal{C}| \geq m$ are met for all N signals prepared by Alice and Bob.

Parameter estimation

The participating parties, Alice and Bob, make use of the random bits obtained from $\mathcal{K}$ to create a raw key consisting of bit strings $\mathbf{K}_A$ and $\mathbf{K}_B$. Then, they compute the average error $\frac{1}{|\mathcal{C}|} \sum a_i \oplus b_i$ where a_i and b_i are Alice and Bob's bit values.

Error correction

The information reconciliation scheme is performed, which leaks at least leak_{EC} bits of classical error-correction data. Alice evaluates a bit string (i.e., a hash) measuring length $\log_2(1/\varepsilon_{\text{cor}})$ using a random universal₂ hash function to $\mathbf{K}_A$. Then, Alice transmits the choice of the function, including the hash, to the receiver, Bob. When the hash of $\mathbf{K}_B$ does not match the hash of $\mathbf{K}_A$, the protocol is aborted.

Privacy amplification

During this step, Alice uses a random universal₂ hash function for extracting the length ℓ bits of secret key $\mathbf{S}_A$ from $\mathbf{K}_A$. Bob exploits a similar hash function for extracting the key $\mathbf{S}_B$ of length ℓ from $\mathbf{K}_B$.

6.3 Security analysis

We consider the realistic scenarios where participating parties exchange finite signals N and determine the statistical fluctuations of finite-size key effects. The security analysis follows the proofs provided in Refs. [218, 239–241, 267] based on a universally composable framework. The protocol creates a pair of key bit strings $\mathbf{S}_A$ for Alice and $\mathbf{S}_B$ for Bob. These key bit strings measure length ℓ and must satisfy the correctness and secrecy requirements so that the protocol can be considered secure. Based on the composability requirement, the QKD protocol is considered to be correct when $\mathbf{S}_A = \mathbf{S}_B$ for any eavesdropping attack. Thus, the ε_{cor} -correct protocol differs from a correct one according to the error probability, ε_{cor} , where $\Pr[\mathbf{S}_A \neq \mathbf{S}_B] \leq \varepsilon_{\text{cor}}$. Therefore, the classical-quantum (CQ) state, $\rho_{\mathbf{S}_A E}$ is Δ -secret when

$$\min_{\rho_E} \frac{1}{2} \|\rho_{\mathbf{S}_A E} - \rho_U \otimes \rho_E\|_1 \leq \Delta, \quad (6.21)$$

where $\rho_{S_A E}$ is the CQ state, which represents the correlation between Alice's key bit string S_A and Eve's quantum state ρ_E , and ρ_U corresponds to the completely mixed state on the key space. Since we consider signals generated using spontaneous parametric down-conversion (SPDC) sources that sometimes emit at least one photon pair, our protocol is susceptible to photon number splitting (PNS) attacks. Therefore, we apply the decoy states technique analysis. With the decoy-state approach, Alice prepares photons at random by using the three different intensities (μ, ν, ω) with μ denoting the signal state intensity, ν for decoy states, and ω represents the vacuum states [223]. These intensities are generally chosen according to the following probabilities $P_\mu > P_\nu > P_\omega$ whereby P_μ, P_ν , and P_ω represent signal, decoy and vacuum states. Accordingly, signal states attained with the intensity μ are utilized to generate the final secure key. Finally, the decoy-states acquired based on intensity ν are used to bound the knowledge of Eve about the key. Therefore, the key rate of the $\varepsilon_{\text{sec}} + \varepsilon_{\text{cor}}$ -MDI protocol with biphotons is expressed as

$$\frac{\ell}{N_{\text{total}}} = q \left[Q_{\mu_a \mu_b, \mathcal{M}_1}^{1,1} (\log_2 3 - h_3(e_{\mathcal{M}_2}^{1,1U})) - \text{leak}_{EC} - \log_2 \frac{2}{\varepsilon_{\text{cor}}} - 2 \log_2 \frac{4}{\varepsilon_{\text{sec}}} \right], \quad (6.22)$$

with $q = \frac{N_\mu p_\kappa^2}{N_{\text{total}}}$, N_μ represents the number of detected signals prepared according to the intensity μ . In contrast, p_κ denotes the probability of measuring in the key basis $\mathcal{M}_1$ and N_{total} is the total amount of exchanged signals. The term $Q_{\mu_a \mu_b, \mathcal{M}_1}^{1,1}$ represents the gain of biphotons prepared by Alice and Bob in the key basis $\mathcal{M}_1$ with intensities μ_a and μ_b , respectively. Accordingly, the term $e_{\mathcal{M}_2}^{1,1U}$ denotes the upper bound on the error rate emanating from single-photon components in the non-key basis $\mathcal{M}_2$ and leak_{EC} represents the quantity of information leaked to Eve in the error correction step which equals to $N_\mu f_{EC} h_3(E_{\mu_a \mu_b, \mathcal{M}_1})$. Here f denotes the efficiency due to error correction and $h_3(x)$ is the entropy corresponding to three-dimensional quantum states given by $h_3(x) = -x \log_2(\frac{x}{2}) - (1-x) \log_2(1-x)$. Finally, the correction terms $\log_2(1/\varepsilon_{\text{cor}})$ and $2 \log_2(4/\varepsilon_{\text{sec}})$ correspond to the bits of information lost through computation of universal hash function during error correction step and the privacy amplification. The applicable parameters in Eq. (6.22) are derived in Appendix E.

6.4 Simulation results

We present the analysis of the behavior of the secret key rate in Eq. (6.22). The simulation results correspond to a fibre-based QKD scheme where the expected key rate is maximized by using the following experimental values where fiber loss coefficient 0.2 dB/km, detector efficiency $\eta = 14.5\%$, single-photon detector dark count rate $P_d = 1.7 \times 10^{-6}$, error correction efficiency $f_{EC} = 1.22$, signal states mean photon number $\mu = 0.6$ and optimal probability p_z for the key basis is 0.95 Ref. [271].

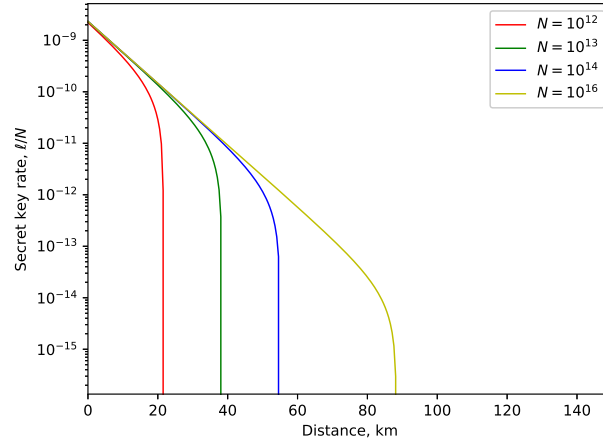


Figure 6.4: Illustration of the secret key rate (in logarithmic scale) in terms of the transmission distance (km), for a fixed amount of signals $N = 10^{12}$, $N = 10^{13}$, $N = 10^{14}$ and $N = 10^{16}$.

Figure 6.4 depicts the expected secret key rate corresponding to each pulse (i.e., ℓ/N) in terms of the transmission distance between the participating parties, Alice and Bob, for various amounts of signals N . The simulation result demonstrates the feasibility of our proposed protocol in the finite-key regime. Notably, we obtain a fairly reasonable transmission distance of 90 km with realistic 10^{16} photon signals. For comparison purposes, we provide the plot for key rate against transmission distance for our proposed biphoton MDI QKD and the qubit-based MDI QKD [240] in Figure 6.5. The results indicate that qubit-based MDI-QKD slightly outperforms our proposed biphoton QKD in terms of maximum transmission and achievable key rates. However, it is worth highlighting that the biphoton MDI-QKD provides a higher bit error rate tolerance compared to the qubit-based MDI-QKD. For example, it has previously been demonstrated in Refs. [300, 302] that biphoton-based QKD protocols can tolerate an higher error rate to distill a

secure key in comparison to their qubit-based counterparts. In Figure 6.7, we show the simulation results for the security bounds for the two-dimensional system (qubit based) QKD and for the three-dimensional system (qutrit based) QKD based on the secret key fraction formula derived in [302]. The results show that the qubit based QKD has a lower bound on the error rate of 11% while the qutrit based QKD can tolerate up to 15.95% error rate. Therefore, we highlight that owing to its ability to tolerate a higher quantum bit error rate, the biphoton MDI QKD can still be considered a reliable candidate for key distribution purposes, particularly over short transmission distances with low losses in the channel. Notably, we remark that the means to create and detect biphoton optical fields have long been successfully investigated [152, 303–305]. Furthermore, the experimental results show that the biphoton states can be realized with high fidelity that ranged from 98.3 % to 99.8%, clearly demonstrating the feasibility of biphoton QKD. Most significantly, the advent of superconducting nanowire single-photon detectors has demonstrated detection efficiency of about 93% [306]. Thus, by harnessing these new technologies, the detection inefficiencies contributed by our detection system, which detectors in our scheme could contribute, can be drastically reduced, resulting in improved key rates. In Figure 6.6, we present the performance expected secret key rate (per pulse) ℓ/N given as a function of the number of signals N for various values of the intrinsic error rate: $Q = (0.3\%, 0.6\%, 1\%)$ owing to the misalignment and the optical system's instability at a distance of 50 km. We show that a minimum data size of about 10^{14} signals (attainable current hardware in practical QKD systems) is required to produce a provably secure secret key.

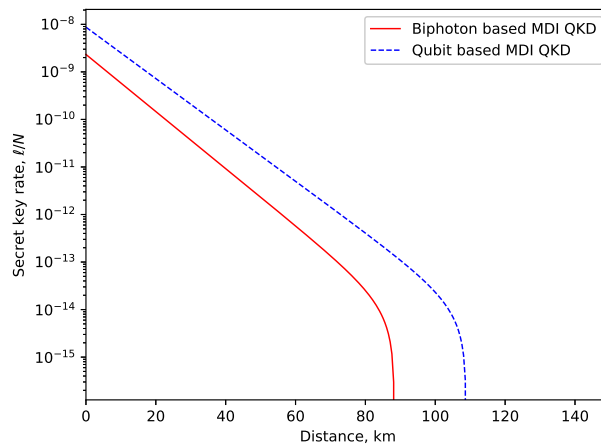


Figure 6.5: Illustration of the secret key rate (in logarithmic scale) in terms of the transmission distance (km) for our proposed biphoton MDI QKD and the qubit-based MDI QKD proposed in Ref. [240] for a fixed amount of signals $N = 10^{16}$.

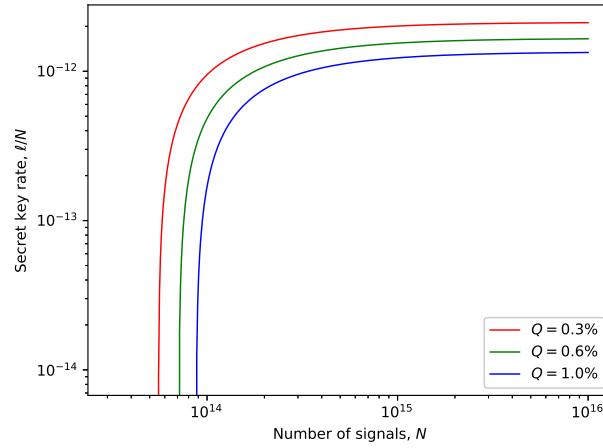


Figure 6.6: The secret key rate (in logarithmic scale) in terms of the number of signals N , for intrinsic misalignment errors 0.3%, 0.6%, and 1%.

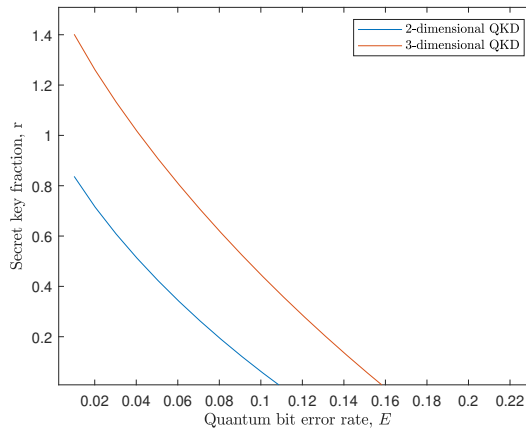


Figure 6.7: Plots of secret key fraction vs quantum bit error rate, E for the 2-dimensional (qubit based) QKD and the 3-dimensional (qutrit based) QKD based on the secret key fraction formula derived in [302].

6.5 Conclusion

We presented a high-dimensional QKD protocol employing biphotons to encode information. The biphotons were exploited as qutrits to improve the secret key rate. This is because qutrits carry more bits of classical information and have improved robustness against eavesdropping compared to qubits. Moreover, the secret key rate for the MDI-QKD proposed protocol was simulated regarding the

transmission distance for different fixed amounts of signals. These results prove that this protocol achieves a considerable secret key rate for a moderate transmission distance of 90 km by using 10^{16} signals. Also, the expected secret key rate was simulated to examine our protocol's performance at various intrinsic error rate values, $Q = (0.3\%, 0.6\%, 1\%)$ caused by misalignment and instability due to the optical system. These results show that reasonable key rates are achieved with a minimum data size of about 10^{14} signals, which are realizable with the current technology. Therefore, the proposed protocol is crucial for realizing practical QKD implementations.

Measurement device independent QKD with vector vortex beams under diverse weather conditions

7.1 Introduction

Real-world deployment of QKD protocols often entails operating in diverse environments, including turbulent weather conditions. Diverse weather conditions cause interference in communication channels, causing fluctuations in the received signal quality, errors and inadvertently enhancing the potential for eavesdropping. Consequently, we introduce an MDI-QKD implemented with vector vortex modes, which have proved resilient against adverse weather conditions. The vector vortex beams are created through a specific combination of OAM and polarization modes (hybrid states). The inherent advantage of these beams is that any perturbation caused by misalignment in the polarization degree of freedom is precisely compensated for by an identical effect caused by misalignment of the OAM modes. This results in rotationally invariant photon states. Another significant contribution is the performance analysis of the proposed MDI-QKD scheme under diverse weather conditions to determine its viability. We do this by evaluating key figures of merit, i.e., secure key rate and transmission distance. This chapter is based on the work in Ref. [200].

7.2 Operation of the OAM-based MDI-QKD protocol

We propose an MDI-QKD scheme implemented with vector vortex and scalar beams. In quantum optics, optical fields can be manipulated to create vector vortex or scalar beams. Vector vortex beams are states of light with spatially varying polarization in the transverse plane, i.e., inhomogeneous polarization states. The spatial and polarization degrees of freedom (DoFs) are coupled non-separable, reminiscent of entanglement in quantum mechanics. Scalar beams, on the other hand, are completely separable in spatial and polarization modes, i.e., the spatial properties are not affected by changes in the polarization state of the photon. Specifically, vector vortex beams are defined by utilizing the notation adopted from quantum mechanics as [307]:

$$|\psi\rangle_{\theta,\ell} = \frac{1}{\sqrt{2}}(|R\rangle|\ell\rangle + e^{i\theta}|L\rangle|-\ell\rangle), \quad (7.1)$$

and the mutually unbiased bases (MUB) scalar beams are expressed as

$$|\phi\rangle_{\theta,\ell} = \frac{1}{\sqrt{2}}(|R\rangle + e^{i\theta}|L\rangle)|\pm\ell\rangle, \quad (7.2)$$

where R and L correspond to the right and left circular polarization states of light, θ denotes the intra modal phase and $|\pm\ell\rangle$ is an OAM state that carries $\pm\ell\hbar$ quanta of OAM. This quantity can be represented as

$$|\ell\rangle = A(r, z)W(r/R)\exp(i\ell\phi), \quad (7.3)$$

where A corresponds to an amplitude of the beam, r and ϕ are the radial and azimuthal coordinates, respectively. The term ℓ denotes an OAM topological charge, and it is an integer, while $W(r/R)$ denotes an aperture function with radius R expressed as [308]

$$W(r/R) = \begin{cases} 1, & \text{if } |r| < R \\ 0, & \text{otherwise.} \end{cases} \quad (7.4)$$

State preparation

The OAM-based MDI-QKD is realized by manipulating the vector vortex and scalar beams in Eqs. (7.1) and (7.2) with intra modal phase $\theta = 0$ or π to generate two mutually unbiased bases (MUB), vector basis $\mathbf{V} \in \{V_0 = \frac{1}{\sqrt{2}}(|R\rangle|\ell\rangle + |L\rangle|-\ell\rangle), V_1 = \frac{1}{\sqrt{2}}(|R\rangle|\ell\rangle - |L\rangle|-\ell\rangle)\}$ and the scalar basis $\mathbf{S} \in \{S_0 = \frac{1}{\sqrt{2}}(|R\rangle + |L\rangle)|\ell\rangle, S_1 = \frac{1}{\sqrt{2}}(|R\rangle - |L\rangle)|-\ell\rangle\}$. The two communication parties, Alice and Bob randomly and independently choose a basis ($\mathbf{V}$ or $\mathbf{S}$), and a bit $r \in \{0, 1\}$ where $r = 0 \in \{V_0, S_0\}$ and $r = 1 \in \{V_1, S_1\}$. Next, they generate optical signals of intensity $\gamma \in \{\mu, \nu, 0\}$ (where μ is the intensity for signal states, ν for decoy states, and ω for vacuum states) prepared in the basis state of $\beta \in \{\mathbf{V}, \mathbf{S}\}$. Alice and Bob send their states to Charlie via the quantum channel.

Measurement

Charlie let the two optical pulses interfere in the symmetric beam-splitter (BS) and performs mode sorting and Bell state measurement. When the photons carrying OAM states from Alice and Bob arrive at 50:50 BS, a Hong–Ou–Mandel (HOM) effect occurs. In particular, according to the HOM effect, two indistinguishable photons incident at each input port of BS will exit at the same output port of BS. However, four distinct possibilities exist with distinguishable photons: the two photons exit the BS together through the same output port, or the photons exit the BS separately through different output arms. Precisely, for the initial state $|\Psi\rangle = |1\rangle_{1,\mathbf{M}}|1\rangle_{2,\mathbf{N}} = |\mathbf{M}\rangle_1|\mathbf{N}\rangle_2 = \hat{a}_{1,\mathbf{M}}^\dagger \hat{b}_{2,\mathbf{N}}^\dagger |0\rangle$, the transformation relations of the two photons incident at the two inputs of BS can be described as

$$\begin{aligned} \hat{a}_{1,\mathbf{M}}^\dagger \hat{b}_{2,\mathbf{N}}^\dagger |0\rangle &\xrightarrow{BS} \frac{1}{2}(\hat{c}_{3,\mathbf{M}}^\dagger + \hat{d}_{4,\mathbf{M}}^\dagger)(\hat{c}_{3,\mathbf{N}}^\dagger - \hat{d}_{4,\mathbf{N}}^\dagger)|0\rangle \\ &= \frac{1}{2}(\hat{c}_{3,\mathbf{M}}^\dagger \hat{c}_{3,\mathbf{N}}^\dagger - \hat{c}_{3,\mathbf{M}}^\dagger \hat{d}_{4,\mathbf{N}}^\dagger + \hat{c}_{3,\mathbf{N}}^\dagger \hat{d}_{4,\mathbf{M}}^\dagger - \hat{d}_{4,\mathbf{N}}^\dagger \hat{d}_{4,\mathbf{M}}^\dagger)|0\rangle, \end{aligned} \quad (7.5)$$

where $\hat{a}^\dagger, \hat{b}^\dagger, \hat{c}^\dagger$ and $\hat{d}^\dagger$ are creation operators at input and output ports 1,2 and 3,4, respectively. The notations $\mathbf{M}$ and $\mathbf{N}$ correspond to the degree of freedom, such as polarization and orbital angular momentum. For the two input photons with identical degrees of freedom, the second and third terms in Eq. (7.5) disappear. For simplicity, for initial states, $|\psi\rangle$ and $|\varphi\rangle$ the action of the beam-splitter can also

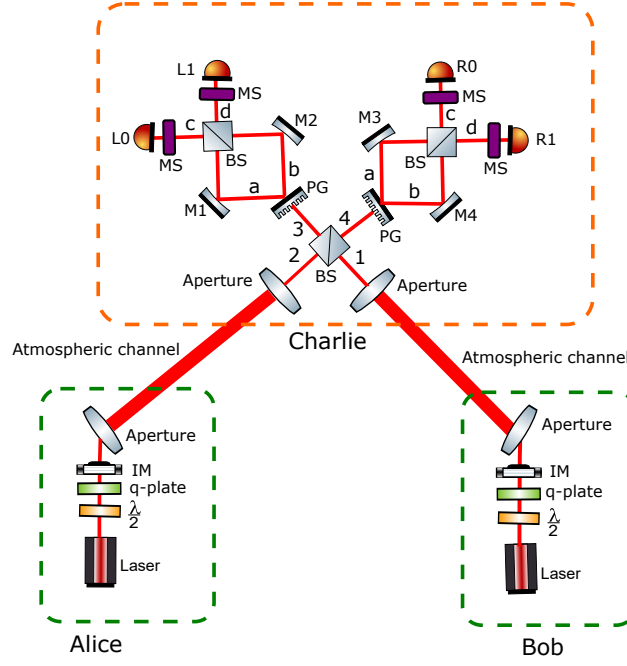


Figure 7.1: An illustration of the proposed OAM-based MDI-QKD. Alice and Bob prepare two mutually unbiased basis states ($\mathbf{V}$, $\mathbf{S}$) and send them to Charlie through the unsecured channel. The $\lambda/2$ plate and the q -plate are used to generate a set of vector and scalar modes, which are then attenuated to intensity $\gamma \in \{\mu, \nu, 0\}$ using intensity modulator IM. Next, the telescope collimates the quantum states with a finite aperture. They are sent through a free atmospheric space link to the measurement site controlled by Charlie. The optical states are then collected by the telescope and allowed to interfere with the symmetric beam-splitter (BS). Next, the photons are passed through the polarization grating that separates the left and right circularly polarized photons, then guided by mirrors (M1, M2, M3, M4) towards a beam-splitter (BS). As a result, the photons are measured using the mode sorters (MS) that map OAM to position and then detected by the detectors (L0, R0, L1, R1).

be illustrated as

$$|\psi\rangle_1|\varphi\rangle_2 \xrightarrow{BS} \frac{1}{2}(|\psi\rangle_3|\bar{\varphi}\rangle_3 - |\psi\rangle_3|\varphi\rangle_4 + |\bar{\psi}\rangle_4|\bar{\varphi}\rangle_3 - |\bar{\psi}\rangle_4|\varphi\rangle_4) \quad (7.6)$$

where $|\bar{x}\rangle$ is the reflected state. Based on the beam-splitter interactions, we describe observations from each basis as follows.

Vector basis Based on a method described in Ref. [307], two vector vortex states are sorted by combining geometric phase control and multipath interference (see Figure 7.1). Once photons exit the first BS, they pass through a polarization grating. This separates left and right circularly polarized photons into

two paths based on their polarization according to

$$|\psi\rangle_{\theta,\ell} = \frac{1}{\sqrt{2}}(|R\rangle_a|\ell\rangle_a + e^{i\theta}|L\rangle_b|-\ell\rangle_b). \quad (7.7)$$

As a result of interference between the photons in paths a and b at the second BS, the resultant state is expressed as follows

$$|\psi'\rangle_{\theta,\ell} = \frac{1 - e^{i\theta}}{2}|\ell\rangle_c + i\frac{1 + e^{i\theta}}{2}|-\ell\rangle_d. \quad (7.8)$$

Note that due to parity differences in the reflections in each input port, the polarisation of the two paths is inherently reconciled in each output port of the beam-splitter. Also, it is worth stating that at this stage, it is not essential to keep the polarisation in the expression of the photon state since the polarisation details are defined in the path. The OAM carrying photons from the outputs c and d are then measured by passing them through the OAM mode sorter and coincidentally detected by two detectors, L0 and L1 or R0 and R1. According to Eq. (7.8), when Alice and Bob prepare the same vector states, we observe a click from one detector along the same path (3 or 4) from the output ports of the first BS. An error corresponds to a click from two detectors within the same path (3 or 4) when the same states are sent by two parties. However, if Alice and Bob prepare vector vortex beams of different states, two detectors are triggered at opposite ends, that is, (L0, R1) or (L1, R0) or within the same path (3 or 4), i.e., (L0, L1) or (R0, R1). For instance, suppose that Alice sent $|\varphi\rangle_2 = \frac{1}{\sqrt{2}}(|R\rangle|\ell\rangle - |L\rangle|-\ell\rangle)$ and Bob sent vector vortex state $|\psi\rangle_1 = \frac{1}{\sqrt{2}}(|R\rangle|\ell\rangle + |L\rangle|-\ell\rangle)$, then based on the first BS interactions we have

$$\begin{aligned} |\psi\rangle_1|\varphi\rangle_2 \xrightarrow{BS} & \frac{1}{2} \left(\left[\frac{1}{\sqrt{2}}(|R\rangle|\ell\rangle + |L\rangle|-\ell\rangle) \right]_3 \otimes \left[\frac{1}{\sqrt{2}}(|R\rangle|\ell\rangle - |L\rangle|-\ell\rangle) \right]_3 \right. \\ & - \left[\frac{1}{\sqrt{2}}(|R\rangle|\ell\rangle + |L\rangle|-\ell\rangle) \right]_3 \otimes \left[\frac{1}{\sqrt{2}}(|R\rangle|\ell\rangle - |L\rangle|-\ell\rangle) \right]_4 \\ & + \left[\frac{1}{\sqrt{2}}(|R\rangle|\ell\rangle + |L\rangle|-\ell\rangle) \right]_4 \otimes \left[\frac{1}{\sqrt{2}}(|R\rangle|\ell\rangle - |L\rangle|-\ell\rangle) \right]_3 \\ & \left. - \left[\frac{1}{\sqrt{2}}(|R\rangle|\ell\rangle + |L\rangle|-\ell\rangle) \right]_4 \otimes \left[\frac{1}{\sqrt{2}}(|R\rangle|\ell\rangle - |L\rangle|-\ell\rangle) \right]_4 \right). \end{aligned} \quad (7.9)$$

From the above result, we observe that there are four distinct probable scenarios; 25% probability that both $|\psi\rangle_1$ and $|\varphi\rangle_2$ will exit at output port 3; 25% probability that $|\psi\rangle_1$ exit at port 3 and $|\varphi\rangle_2$ leaves at port 4; 25% chance that $|\psi\rangle_1$ exit at port 4 and $|\varphi\rangle_2$ exit at output arm 3; 25% probability that both states leave the BS at output arm 4. Without loss of generality, let us consider a case where $|\psi\rangle_1$ exit at

port 4 and $|\varphi\rangle_2$ exit at port 3, which is indicated by the third term in Eq. (7.9). After going through a polarization grating, the states transform as follows

$$\frac{1}{\sqrt{2}}(|R\rangle_3|\ell\rangle_3 + e^{i\theta}|L\rangle_3|-\ell\rangle_3) \xrightarrow{PG} \frac{1}{\sqrt{2}}(|R\rangle_{3,a}|\ell\rangle_{3,a} + e^{i\theta}|L\rangle_{3,b}|-\ell\rangle_{3,b}). \quad (7.10)$$

Note that we have introduced a phase factor $e^{i\theta}$, with $\theta = \pi$. After passing through the second BS we obtain

$$|\psi\rangle_{\theta,\ell} = \frac{1 - e^{i\theta}}{2}|\ell\rangle_{3,c} + i\frac{1 + e^{i\theta}}{2}|-\ell\rangle_{3,d}, \quad (7.11)$$

Now, substituting back $\theta = \pi$ into Eq. (7.11) we obtain

$$|\psi\rangle_{\pi,\ell} = |\ell\rangle_{3,c}. \quad (7.12)$$

For the photon leaving through port 4, we have

$$\frac{1}{\sqrt{2}}(|R\rangle_4|\ell\rangle_4 + e^{i\theta}|L\rangle_4|-\ell\rangle_4) \xrightarrow{PG} \frac{1}{\sqrt{2}}(|R\rangle_{4,a}|\ell\rangle_{4,a} + e^{i\theta}|L\rangle_{4,b}|-\ell\rangle_{4,b}), \quad (7.13)$$

where $\theta = 0$. After passing through the BS, we obtain

$$|\psi\rangle_{\theta,\ell} = \frac{1 - e^{i\theta}}{2}|\ell\rangle_{4,c} + i\frac{1 + e^{i\theta}}{2}|-\ell\rangle_{4,d}, \quad (7.14)$$

Substituting $\theta = 0$ into Eq. (7.14) we obtain

$$|\psi\rangle_{0,\ell} = i|-\ell\rangle_{4,d}. \quad (7.15)$$

Therefore, this scenario will lead to click in detectors L0 and R1. Table 7.1 depicts the results of other probable occurrences.

Scalar basis Scalar modes are sorted analogously to vector modes. As a result, the two states that form the basis can be described as follows

$$|\phi\rangle_{\theta,\ell} = \frac{1}{\sqrt{2}}(|R\rangle_a|\ell\rangle_a + e^{i\theta}|L\rangle_b|\ell\rangle_b) \quad (7.16)$$

and

$$|\phi\rangle_{\theta,-\ell} = \frac{1}{\sqrt{2}}|R\rangle_a|-\ell\rangle_a + e^{i\theta}|L\rangle_b|-\ell\rangle_b. \quad (7.17)$$

The modes are separated into two paths a and b using a polarization grating and then allowed to interfere in the BS. The output state for Eq. (7.16) is given by

$$|\psi'\rangle_{\theta,\ell} = \frac{1 - e^{i\theta}}{2} |R\rangle_c |\ell\rangle_c + i \frac{1 + e^{i\theta}}{2} |L\rangle_d |\ell\rangle_d. \quad (7.18)$$

and the output state for Eq. (7.17) is

$$|\psi'\rangle_{\theta,-\ell} = \frac{1 - e^{i\theta}}{2} |R\rangle_c |-\ell\rangle_c + i \frac{1 + e^{i\theta}}{2} |L\rangle_d |-\ell\rangle_d. \quad (7.19)$$

The intramodal phases are chosen to be $\theta = 0$ and $\theta = \pi$ for states in Eq. (7.18) and Eq. (7.19), respectively. Therefore, the output states can be reduced to $|\psi'\rangle_{\pi,\ell} = |R\rangle |\ell\rangle$ and $|\psi'\rangle_{0,-\ell} = i |L\rangle |-\ell\rangle$. These results indicate that when Alice and Bob prepare the same scalar states, only one detector will be triggered within the relay. Alternatively, suppose two parties prepare scalar states with opposite OAM. In that case, this will result in the click of two detectors in different output paths of the first BS, i.e., a combination of either (L0, R1) or (R0, L1) or the two detectors triggered within the same path from the first BS, that is, (L0, L1) or (R0, R1). There is also an error in this basis if both detectors within the same path (path 3 or 4) are triggered when the same states are sent.

Table 7.1: Probability distribution for Bell state measurement results announced by Charlie when both Alice and Bob choose the same basis.

Basis	Alice	Bob	Charlie's measurement results			
			$ \Psi\rangle^+$		$ \Psi\rangle^-$	
			L0, L1	R0, R1	L0, R1	L1, R0
Vector basis	V_0	V_0	0	0	0	0
	V_0	V_1	0.25	0.25	0.25	0.25
	V_1	V_0	0.25	0.25	0.25	0.25
	V_1	V_1	0	0	0	0
Scalar basis	S_0	S_0	0	0	0	0
	S_0	S_1	0.25	0.25	0.25	0.25
	S_1	S_0	0.25	0.25	0.25	0.25
	S_1	S_1	0	0	0	0

Announcement

Following photon detection, Charlie announces successful measurement events. A successful detection event corresponds to a coincidence click in two detectors (as-

sociated with orthogonal OAM). In the proposed protocol, the detectors L0 and R0 are used to detect OAM state $|\ell\rangle$ while L1 and R1 are used to detect OAM state $|\ell\rangle$. Thus, a combination of (L0, L1), (R0, R1), (L0, R1) and (R0, L1) corresponds to successful detection. We define a click in detectors (L0, L1) or (R0, R1) to indicate projection into Bell state $\Psi^+ = \frac{1}{\sqrt{2}}(|01\rangle_{LL} + |10\rangle_{RR})$, while a click in detectors (L0, R1) or (R0, L1) correspond to Bell state $\Psi^- = \frac{1}{\sqrt{2}}(|01\rangle_{LR} - |10\rangle_{LR})$.

Sifting

When Charlie announces a successful Bell state measurement result, Alice and Bob publish their basis choices and intensity over an authenticated public channel. Bob flips his key bits to match Alice's as illustrated in Table 7.2.

Table 7.2: Post-processing of raw key in the sifting step. Bob flips his bits to ensure a correct correlation with Alice's bit.

Alice and Bob	Charlie's measurement results	
	$ \Psi\rangle^+$	$ \Psi\rangle^-$
Vector basis	Bit flip	Bit flip
Scalar basis	Bit flip	Bit flip

The random bit values $r \in \{0, 1\}$ in each basis are assigned as $r = 0 \in \{V_0, S_0\}$ and $r = 1 \in \{V_1, S_1\}$. The random bits obtained from the vector basis are then exploited by Alice and Bob in order to form a raw key. The random bits from the scalar basis are used to estimate the upper bound in the eavesdropper's information. Then, the two communicating parties perform error correction and privacy amplification to obtain a secret key that can be used for secure communication.

7.3 Security analysis

We provide a security analysis for our scheme along the lines of Ref [309], which makes use of a photon-number channel model and the Gottesman–Lo–Lütkenhaus–Preskill (GLLP) security proof [51]. In particular, the security proof is based on time-reversed EPR-based QKD protocol and the notion of virtual protocol. In this virtual setting, it is assumed that Alice possesses a virtual qubit, and she entangles it with a quantum signal she prepared before sending it to Charlie. Similarly, Bob uses a virtual qubit to prepare an entangled state with the quantum signal he

sends to Charlie. Now, in principle, the two could rather store their virtual qubits in her quantum memory and wait for the announcement of successful Bell state measurements by Charlie. The successful measurements of the signals sent by Alice and Bob automatically imply that their virtual qubits are entangled by virtue of entanglement swapping. After that, Alice and Bob can now perform a measurement on their virtual qubits to determine which state they are sending to Charlie. In such virtual qubits setting, the protocol is directly equivalent to an entanglement-based protocol and its security can be proved following the technique proposed in [259]. The key rate formula for the proposed MDI-QKD is given by

$$K \geq q\{Q_{\mu_a\mu_b}^{\mathbf{V}}f_{\text{EC}}H(E_{\mu_a\mu_b}^{\mathbf{V}}) + Q_{11}^{\mathbf{V}}(1 - H(e_{11}^{\mathbf{S}}))\}, \quad (7.20)$$

where q is the basis sift factor; parameter μ denotes the signal intensity; $Q_{\mu_a\mu_b}^{\mathbf{V}}$ and $E_{\mu_a\mu_b}^{\mathbf{V}}$ are the overall gain and quantum bit error rate (QBER) in the vector basis, respectively. The quantities $Q_{11}^{\mathbf{V}}$ and $e_{11}^{\mathbf{S}}$ indicate the gain and error rate of individual photon components. We evaluate these parameters using the decoy state theory presented in the Appendix F.

7.4 Propagation through perturbing media

We examine how the OAM-carrying optical beams employed in our proposed protocol are affected by various weather conditions during their propagation through the free space link. When OAM beams propagate through atmospheric channels, they undergo aberrations, primarily caused by beam extinction and turbulence effects. Extinction occurs due to absorption and scattering by molecules and aerosols, as opposed to the latter caused by changes in the refractive index of the atmosphere. Atmospheric effects are strongly related to the transmittance, η , defined as the probability of a photon being successfully transmitted through the channel and detected. This is a critical factor in evaluating QKD protocol performance. We use some well-developed atmospheric optical communications models to study the influence of weather conditions on the transmission of OAM signals in the MDI-QKD protocol.

OAM carrying photons through turbulence

As OAM states propagate through free space, their purity is compromised due to the turbulence that occurs in the atmosphere. As a result of fluctuations in the refractive index of the atmosphere caused by turbulence, a propagating optical beam will exhibit random phase aberrations. Based on the methods described in Ref. [308], we investigate the effects of random phase aberrations on the received OAM state. First, the original optical field at the transmitter is assumed to be given by

$$A(\mathbf{r}) = A_0 W(r/R) e^{i\ell\phi}, \quad (7.21)$$

where A_0 is the (spatially uniform) field amplitude, and other parameters are defined as in Eq. (7.3). After undergoing scrambling in the turbulent atmosphere, the field at the receiver aperture can be represented as

$$V(\mathbf{r}) = A_0 W(r/R) e^{i\ell\phi} e^{i\vartheta(\mathbf{r})}, \quad (7.22)$$

where $\vartheta(\mathbf{r})$ represents the turbulence-induced wavefront distortion at the receiver. Notably, the quantity $\exp(i\vartheta(\mathbf{r}))$ can be expanded in the Fourier series as

$$e^{i\vartheta(r,\phi)} = \sum_{k=-\infty}^{\infty} C_k(r) e^{ik\phi}, \quad (7.23)$$

where the expansion coefficients $C_k(r)$ are given by

$$C_k(r) = \frac{1}{2\pi} \int_0^{2\pi} d\phi e^{i\vartheta(r,\phi)} e^{-ik\phi}. \quad (7.24)$$

The received field $V(\mathbf{r})$ can be expanded in a similar manner as $V(r, \phi) = \sum_{n=-\infty}^{\infty} V_n(r) \exp(in\phi)$, where each Fourier component $V_n(r)$ is given by

$$V_n(r) = \frac{1}{2\pi} \int_0^{2\pi} d\phi V(r, \phi) e^{-in\phi}. \quad (7.25)$$

By substituting Eq. (7.22) and Eq. (7.23) into Eq. (7.25) yields

$$V_n(r) = \frac{A_0}{2\pi} W(r/R) \sum_{k=-\infty}^{\infty} C_k(r) \int_0^{2\pi} d\phi e^{-i(n-k-\ell)\phi}. \quad (7.26)$$

The above expression can be further reduced to

$$V_n(r) = \frac{A_0}{2\pi} W(r/R) C_{\Delta}(r), \quad (7.27)$$

by considering that the integral in Eq. (7.25) equals 2π when $n - k - \ell = 0$ and vanishes otherwise. The last expression defines Δ as $\Delta = n - \ell$. The connection between azimuthal Fourier components $C_{\Delta}(r)$ associated with atmospheric turbulence and the OAM state of the received field emanating from Eq. (7.27) allows one to determine the amount of radiation that remains in the initial OAM state based on the spatial component of the azimuthal Fourier spectrum $\exp(i\vartheta(\mathbf{r}))$. Practically, this radiation is determined in terms of power in each OAM state of the received field. The total power collected by the receiver is given by

$$P = \frac{1}{2} \epsilon_0 \int d\mathbf{r} W(r/R) V^*(\mathbf{r}) V(\mathbf{r}) = \frac{1}{2} \epsilon_0 |A_0|^2 \pi R^2, \quad (7.28)$$

Accordingly, this power is constituted by a combination of different (orthogonal) modes of OAM modes of the field according to

$$P = \sum_{\Delta=-\infty}^{\infty} P_{\Delta}, \text{ where } P_{\Delta} = 2\pi |A_0|^2 \int_0^R dr r C_{\Delta}^*(r) C_{\Delta}(r). \quad (7.29)$$

An important parameter of interest is the ratio $\eta_{\text{turb}} = P_{\Delta}/P$ of the power contained in each OAM mode given by

$$\eta_{\text{turb}} = \frac{2}{R^2} \int_0^R dr r C_{\Delta}^*(r) C_{\Delta}(r). \quad (7.30)$$

Using this parameter, we can determine the probability that the OAM quantum number n of the received state differs from that of the transmitted state ℓ by the amount $\Delta = n - \ell$. The result presented in Eq. (7.30) applies to any realization of atmospheric turbulence. Generally, η_{turb} is described as an ensemble average

according to the form

$$\eta_{\text{turb}} = K \int_0^R dr r \int_0^{2\pi} d\phi_1 \int_0^{2\pi} d\phi_2 \langle e^{-[\vartheta(r, \phi_1) - \vartheta(r, \phi_2)]} \rangle \times e^{i\Delta(\phi_1 - \phi_2)}, \quad (7.31)$$

where $K = 1/(2\pi^2 R^2)$. By considering the Kolmogorov turbulence theory, the above expression can be further reduced to

$$\eta_{\text{turb}} = \frac{1}{\pi} \int_0^1 d\rho \rho \int_0^{2\pi} d\phi e^{-3.44(D/r_0)^{5/3}(\rho \sin(\phi/2))^{5/3}} \times \cos(\Delta\phi), \quad (7.32)$$

where $\rho = r/R$. Here D denotes the receiver aperture diameter, and the parameter r_0 corresponds to Fried's coherence diameter, which is described as

$$r_0 = 0.1853 \left(\frac{\lambda^2}{C_n^2 L} \right), \quad (7.33)$$

where λ is the wavelength of the optical beam, L is the transmission distance and C_n^2 is the refractive-index structure parameter, which gives atmospheric turbulence strength.

OAM carrying photons through rain

OAM-carrying beams are also highly susceptible to adverse weather conditions, such as rain. Generally, rain attenuates beam energy in free space link QKD due to the absorption and scattering of rain droplets. The phenomenon is known as rain extinction [310]. An empirical formula has been developed to measure rain extinction in relation to rainfall intensity and is defined as [310, 311]:

$$\alpha_{\text{rain}} = 1.45 I_{\text{rain}}^{0.64}, \quad (7.34)$$

where I_{rain} is the rainfall intensity, and α_{rain} is the rain extinction. Using Law-Parsons raindrop size distribution, rainfall intensity is also related to raindrop size

as [310, 312]:

$$I_{\text{rain}} = 6\pi \times 10^{-4} \int_0^\infty n(D_{\text{rain}}) D_{\text{rain}}^3 v(D_{\text{rain}}) dD_{\text{rain}}. \quad (7.35)$$

The above expression can be further simplified by dropping the integral and expressed analytically as

$$I_{\text{rain}} = \frac{6\pi n(D_{\text{rain}}) D_{\text{rain}}^3 v(D_{\text{rain}})}{10^4 m(D_{\text{rain}})}, \quad (7.36)$$

where D_{rain} denotes diameter of the rain droplet, $n(D_{\text{rain}})$ corresponds to the number of rain-droplets, $v(D_{\text{rain}})$ is terminal velocity of rain-droplets and $m(D_{\text{rain}})$ is percentage of volume. The transmittance associated with rain extinction for horizontal paths with length L is given by

$$\eta = e^{-\alpha_{\text{rain}} L}. \quad (7.37)$$

OAM carrying photons through a foggy atmosphere

This section examines the effects of foggy weather conditions on free space QKD. In general, fog is composed of a large number of small water droplets suspended in the air. Beam degradation caused by fog particles is largely reflected in scattering and absorption contributions, which is known as beam extinction. There are two main factors that influence the extinction effects: the radius of the fog particle and the wavelength of the beam. For modeling the scattering and absorption effect, we consider the Mie scattering theory [313], which is more appropriate for evaluating the scattering of particles approximately the wavelength of a beam of light. The Mie theory uses Maxwell equations to characterize beam extinction induced by fog particles. We consider the case of a beam perturbed by homogeneous spherical particles that are isotropic. According to [314], the relationship between scattered and incident beams is defined as a function of the amplitudes of electric field components as

$$\begin{bmatrix} E_{sca}^V \\ E_{sca}^H \end{bmatrix} = \frac{\exp(ikr)}{-ikr} \begin{bmatrix} S_1 & S_3 \\ S_2 & S_4 \end{bmatrix} \begin{bmatrix} E_V^{inc} \\ E_H^{inc} \end{bmatrix}. \quad (7.38)$$

The subscripts V and H refer to the vertical and polarization components of the electric field, respectively and sca and inc denote scattered and incident beams,

respectively. The parameter k represents the wave number, and the element S_i represents the scattering matrix. Its value is determined by particle diameter, refractive index, beam wavelength, and scattering polar angle. According to the scattering matrix, the value is determined by the particle shape, scale, and refractive index. In the case of spherical particles, $S_3 = 0$, $S_4 = 0$, and the complex solution of the other elements, S_1 and S_2 , can be written as follows

$$\begin{aligned} S_1(\theta) &= \sum_{n=1}^{\infty} \frac{2n+1}{n(n+1)} (a_n \pi_n + b_n \tau_n), \\ S_2(\theta) &= \sum_{n=1}^{\infty} \frac{2n+1}{n(n+1)} (b_n \pi_n + a_n \tau_n), \end{aligned} \quad (7.39)$$

where

$$\pi_n = \frac{P_n^1(\cos \theta)}{\sin \theta} = \frac{dP_n^1(\cos \theta)}{d(\cos \theta)} \quad (7.40)$$

$$\tau_n = \frac{dP_n^1(\cos \theta)}{d(\cos \theta)}. \quad (7.41)$$

According to the above expressions, $P_n^1(\cos \theta)$ is the first kind of Legendre function of order n . The scattering polar angle is defined by the parameter θ . The Mie scattering quantities a_n and b_n defined in Eq. (7.39) are obtained from the Bessel functions as

$$a_n = \frac{\psi_n(x) \psi'_n(mx) - m \psi'_n(x) \psi_n(mx)}{\xi_n(x) \xi'_n(mx) - m \xi'_n(x) \xi_n(mx)}, \quad (7.42)$$

$$b_n = \frac{m \psi_n(x) \psi'_n(mx) - \psi'_n(x) \psi_n(mx)}{m \xi_n(x) \xi'_n(mx) - \xi'_n(x) \xi_n(mx)}, \quad (7.43)$$

where for some variables y , $\psi_n(y) = \sqrt{\frac{\pi y}{2}} J_{n+1/2}(y)$, $\xi_n(y) = \sqrt{\frac{\pi y}{2}} H_{n+1/2}(y)$ and $J_{n+1/2}(X)$, $H_{n+1/2}(X)$ denote the first and second kind of semi-integral order Bessel function and Hankel function, respectively. The parameter m represents the refractive index of fog particles, which is estimated as $m = 1.33 + i0.003$, while the quantity x is related to the particle's circumference and wavelength λ according to

$$x = \frac{2\pi R_{\text{fog}}}{\lambda}, \quad (7.44)$$

where R_{fog} is the particle's radius.

The coefficients a_n and b_n are useful for determining the extinction efficiency factor caused by fog particles, which can be obtained by [313]

$$Q_{\text{ext}} = \frac{\lambda^2}{2\pi} \sum_{n=1}^{\infty} (2n+1) \text{Re}(a_n + b_n). \quad (7.45)$$

Thus, the beam attenuation coefficient of fog can be calculated as follows

$$\alpha_{\text{fog}} = \pi R_{\text{fog}}^2 Q_{\text{ext}} N_{\text{fog}}, \quad (7.46)$$

where N_{fog} denotes the number of particles per unit volume.

7.5 Simulation

Based on the simulation parameters provided in Table 7.3, we analyze the performance of OAM-based MDI-QKD under various weather conditions. To begin with, we examine what impact turbulent atmospheric conditions have on the transmitted OAM states. We evaluate the probabilities of obtaining different OAM measurements, η_{turb} for OAM beams propagating under Kolmogorov turbulence using Eq. (7.32).

According to Figure 7.2, as the receiver aperture diameter D becomes comparable to the Fried parameter r_0 , the probability of obtaining the original OAM states ($\Delta\ell = 0$) at the receiver aperture decreases asymptotically. When $D < r_0$, phase aberrations are weak, and OAM scattering is small. However, as the Fried parameter approaches the receiver aperture diameter, it becomes more likely that OAM scattering will occur. The curves showing the probability of receiving scrambled OAM states, i.e., $\Delta\ell > 0$, initially increase with increasing turbulence levels and ultimately decrease with further increase. Optical power is spread across various OAM modes at high turbulence levels, decreasing the probability of detecting a

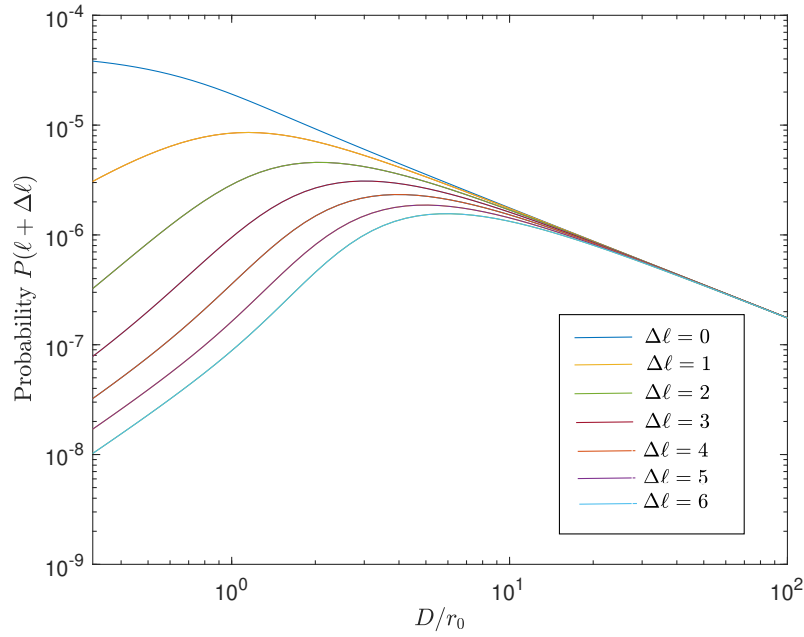


Figure 7.2: This plot illustrates the probability of receiving adjacent OAM states (Transmittance), η_{turb} against the ratio of the aperture diameter D to the Fried parameter r_0 .

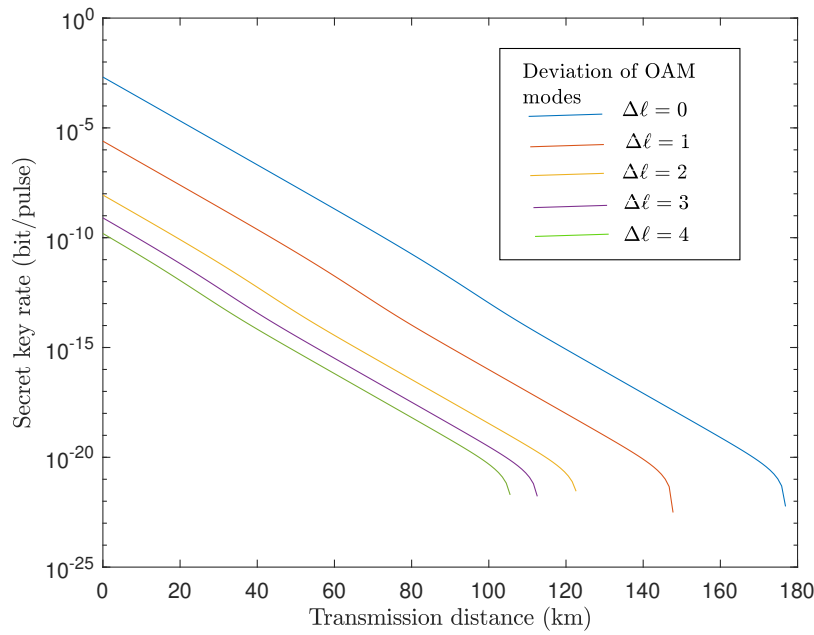


Figure 7.3: A plot of the secret key generation rate, K , versus transmission distance when atmospheric turbulence is varied as measured by the deviation of OAM modes, $\Delta\ell$.

specific OAM value. Figure 7.3 shows a relationship between key rate and transmission distance for different deviations $\Delta\ell$ from original turbulence-induced OAM states. The results demonstrate that the key rate and maximum transmission distance decrease with increasing deviation from originally transmitted OAM states. We observe that the achievable key rate remains comparable to the normal condition without deviation of transmitted OAM states for a lower aberration of OAM states, e.g., for $\Delta\ell = 1$.

Table 7.3: Parameters used for simulation.

Parameters	Values
Background count rate	8×10^{-6}
Error correction efficiency f	1.15
Detector efficiency	14.5%
Aperture diameter, D	15×10^{-2} m
C_n^2	$10^{-14} \text{m}^{-2/3}$
Wavelength of the beam, λ	1550 nm
Terminal velocity of rain, $v(D_{\text{rain}})$	9 m/s
Rain-drop size distribution, $n(D_{\text{rain}})$	10^5
Percentage rain volume, $m(D_{\text{rain}})$	1
Number of particles per unit volume, N_{fog}	10^{15}

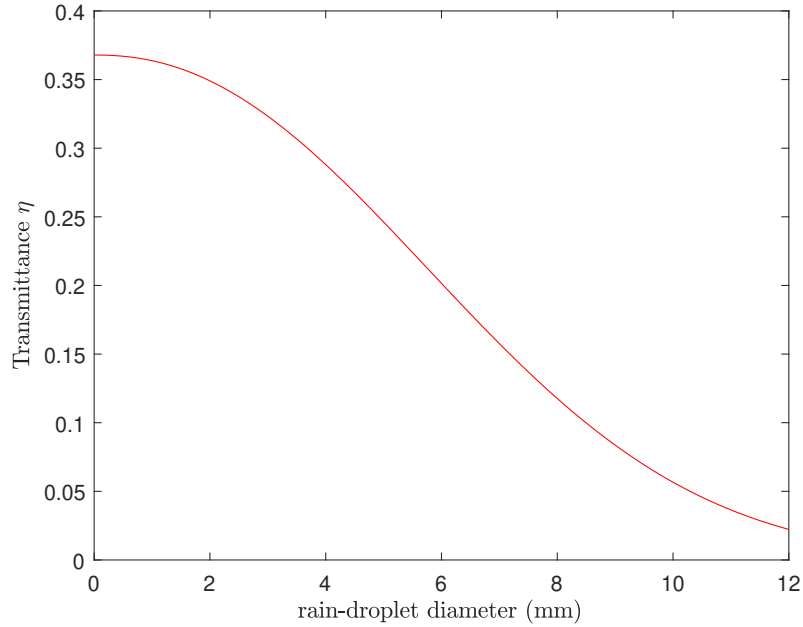


Figure 7.4: A plot of transmittance, η , against the diameter of raindrops, D_{rain} .

In Figure 7.4, we analyze the impact of rain droplet size on transmittance based on the Law-Parson model depicted in Eq. (7.36). The transmittance

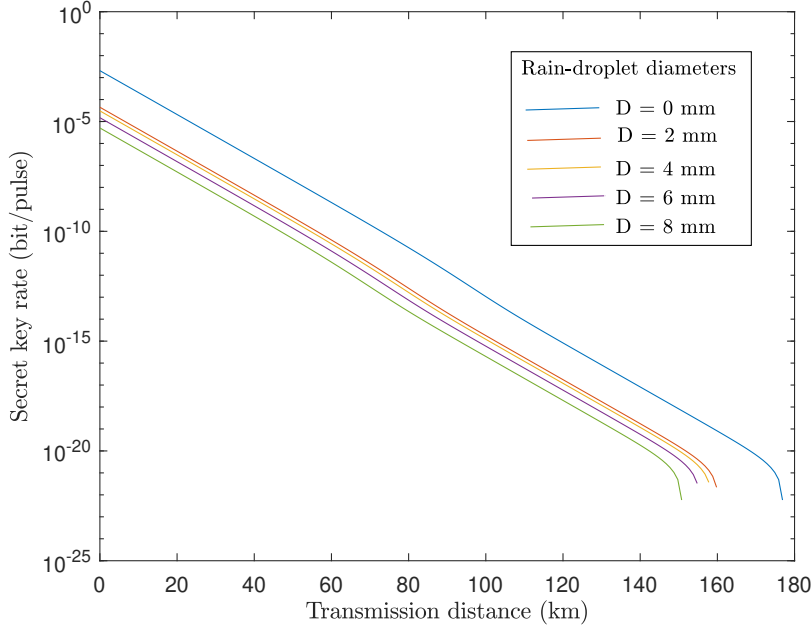


Figure 7.5: Plot of the secret key generation rate, K , against transmission distance in km for a range of raindrop diameters.

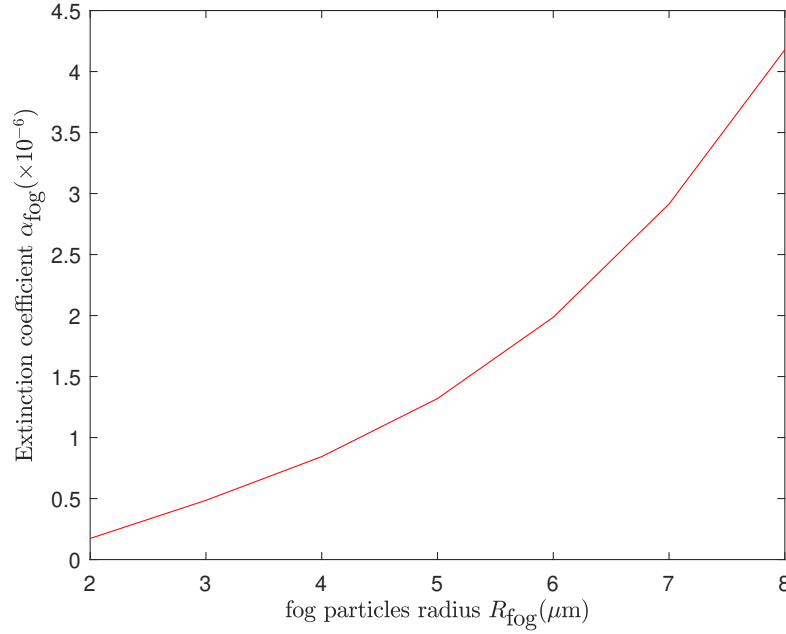


Figure 7.6: An illustration showing the relation between the beam extinction coefficient, α_{fog} , and the radius of the fog particles, R_{fog} .

decreases as the size of the rain droplets increases. As the size of rain droplets increases from 3 mm onwards, a sharp drop in transmittance is observed. In Figure 7.5, we plotted the achievable key rate against the transmission distance for

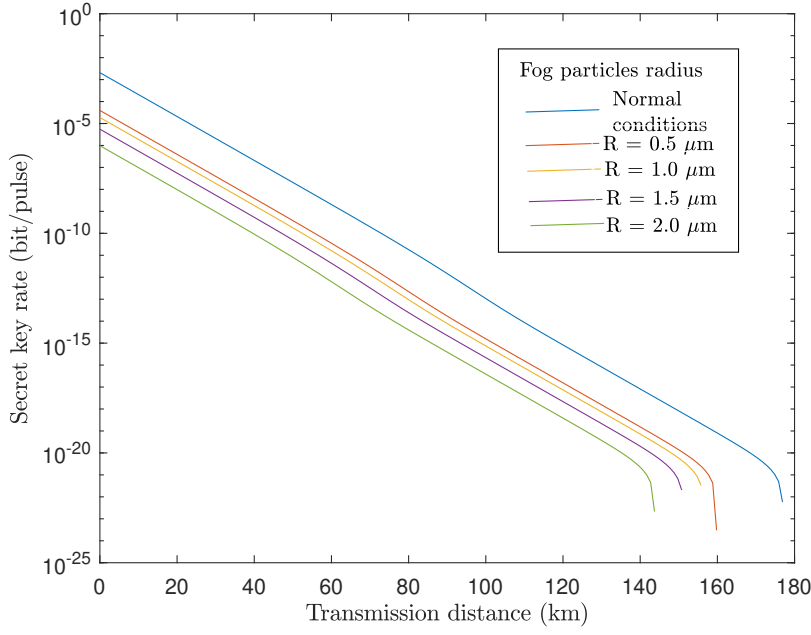


Figure 7.7: A plot of the secret key generation rate, K , against transmission distance in km for various values of the radius of the fog particles.

various sizes of rain droplets. As can be seen from the results, larger rain droplets (which are directly proportional to rainfall intensity) negatively influence key rate and transmission distance. Also, we observe that with a clear atmosphere, the maximum transmission distance is approximately 178 km, while with a rainfall of 2 mm diameter droplets, the maximum distance is 160 km. It should be noted that the distance is further reduced with an increase in the diameter of the rain droplets. A further study was carried out to evaluate the influence of fog particle size on the extinction of optical signals in Figure 7.6 based on Eq. (7.46). Based on the results, the extinction coefficient increases as the fog particle radius increases, indicating an increase in optical absorption and scattering. In Figure 7.7, we generated curves for key rates against transmission distances for different sizes of fog particles. The achievable key rate and maximum transmission distance decrease as the fog particle size increases. However, we discover that the protocol's performance under foggy conditions is still comparable to that under typical atmospheric conditions. For instance, if we set the real-life parameters for the key rate, $R = 10^{-10}$, then the maximum transmission distance under fog particles of size $1\mu\text{m}$ is 80 km. Under normal conditions, the maximum attainable transmission distance is 100 km. Notably, we emphasize that the methods for creating and detecting vector vortex and scalar optical fields have been successfully developed and demonstrated [307]. Furthermore, the experimental results indicate that vector vortex and scalar beams

can be realized with a high fidelity of approximately 97 %, clearly demonstrating the feasibility of the proposed OAM-based MDI-QKD.

7.6 Conclusion

We have demonstrated free space MDI-QKD using vector vortex and scalar beams. Due to the rotational invariance property of the beams, two communicating parties can generate secret keys without having to align the reference frames of the transmitting and receiving units. Additionally, we evaluated the performance of the proposed protocol under a variety of weather conditions that approximate the realistic conditions of everyday communications. We observed that propagation of OAM carrying beam under turbulent conditions may result in scrambling of the OAM state of the beam, and the probability of scrambling increases as the strength of the turbulence increases. Results indicate that large deviations in originally transmitted OAM states of the vortex and scalar beams lead to reduced achievable key rates and maximum transmission distances. In particular, in a weak turbulence regime, i.e., with a small $\Delta\ell$, the achievable distance is comparable to that under normal atmospheric conditions. Notably, we have also demonstrated that, under clear atmospheric conditions, our proposed scheme can transmit signals up to 178 km, whereas with rainfall of 6 mm diameter droplets, the distance to which the signals can be transmitted is 152 km. It should be noted that in foggy conditions with fog particles with a radius of 0.5 μm , the maximum attainable distance is 160 km, which is still comparable to the maximum distance reached under clear conditions. These results demonstrate the robustness of MDI-QKD implementation using vector vortex and scalar beams to generate secure keys over long transmission distances in adverse weather conditions. As a result, this study is of central importance as it opens up the intriguing possibility of utilizing these beams in future QKD applications.

Concluding remarks

This thesis studied the security of several QKD protocols using techniques and models that closely replicate the accuracy of preparation and measurement devices and the environment in which QKD is operated. We reviewed tools used to demonstrate the security of QKD protocols against various classes of attack. We applied the post-selection technique and entropic uncertainty relations to demonstrate the security of our proposed protocols against general attacks with finite resources. In particular, we used the post-selection technique to derive the security bounds for the six-state SARG04 QKD protocol using finite resources. Through this approach, one can derive a secure key from a multi-photon source while also taking into account an optimal coherent attack. We compared the security bounds for the six-state SARG04 protocol under collective attacks with those obtained by applying the post-selection technique when a finite number of resources is available. Our simulation results demonstrate that key rates obtained under optimal coherent attacks assumption do not differ significantly from those obtained under collective attacks.

We also employed the reference frame independence concept to derive the security bounds for several QKD protocols. The approach eliminates the need to align reference frames shared by communicating parties, for instance, the need for active stabilization of interferometers during implementation. Moreover, we derived security bounds for a three-party QKD protocol and demonstrated its performance against general attacks with finite resources using entropic uncertainty relations. Our results indicate that the protocol is robust against noise in the quantum channel based on the realized error rate threshold of 22.7%. This represents an improvement over

the two-party BB84 protocol currently in use. Furthermore, we proposed an RFI twin-field QKD protocol and incorporated the loss-tolerant method in our security analysis. The technique allows us to prove the security of QKD by considering imperfections in the state preparation [52]. The simulation results demonstrate that our protocol can overcome the repeaterless PLOB bound. Moreover, our proposed protocol is capable of extracting a secure key over a transmission distance of $l=505$ km, $l=516$ km and $l=530$ km for encoding flaws $\delta = 0.090$, $\delta = 0.127$ and $\delta = 0.147$, which corresponds to deviations of 5.15° , 7.28° and 8.42° from the desired phase angle, respectively. The results demonstrate that despite the state preparation flaws, key rates achieved are comparable to those for a perfect encoding scenario.

Furthermore, we proposed the various variants of MDI-QKD protocols, which aim to eliminate detector side-channel attacks. To achieve this, we propose a protocol that exploits the polarization state of a biphoton to encode information on a three-level quantum system. Compared to qubits, qutrits carry more classical information and are more resistant to eavesdropping. The results prove that this protocol achieves a considerable secret key rate for a moderate transmission distance of 90 km by using 10^{16} signals. Additionally, the expected secret key rate was simulated to examine our protocol's performance at various intrinsic error rate values, $Q = (0.3\%, 0.6\%, 1\%)$ caused by misalignment and instability due to the optical system. These results show that reasonable key rates are achieved with a minimum data size of about 10^{14} signals, which are realizable with current technology. Moreover, we presented a measurement device-independent (MDI) QKD that employed vector vortex modes [200]. We studied the transmission of vector vortex and scalar beams through a turbulent atmospheric link under diverse weather conditions such as rain or haze. We demonstrated that a maximum secure key transmission distance of 178 km can be achieved under clear conditions by utilizing vector vortex beams, which have largely been ignored in the literature. When raindrops have a diameter of 6 mm and fog particles have a radius of $0.5 \mu\text{m}$, the signals can reach 152 km and 160 km, respectively. Since these distances are comparable, this sheds light on the feasibility of MDI-QKD implemented using vortex vector modes and opens the door to long-distance quantum secure communications.

However, exploring if the SARG04 protocol can be extended to high-dimensional encoding will be interesting. Using high-dimensional systems inherently implies that Eve will require more states to successfully perform unambiguous state discrimination and PNS attacks. For instance, in a three-dimensional system, Eve will need ten photons to perform unambiguous discrimination of the state sent by Alice to

Bob. Thus, high-dimensional encoding is more resistant to PNS attacks, as a secure key can be derived from multi-photon emission scenarios. Additionally, it is worthwhile to extend the three-party RFI QKD to an arbitrary number of participants and derive the generalized security bounds. Additionally, it is desirable to perform a proof of principle experiment to assess the feasibility of the RFI QKD. We can also investigate the possibility of twin-field QKD with vortex beams by considering a discrete-phase randomized source. We realize that in our proposed MDI-QKD protocol with vector vortex modes, when the signal photons are prepared in the same state by two parties, they exit from one output port of the beam-splitter and only one detector is triggered. Therefore, when these signal photons are modulated with the same phase, they will appear as single photons after interfering with the beam-splitter.

Overall, we believe that the results obtained from our proposed protocols will contribute to understanding the influence of preparation and measurement devices in the performance and security of practical QKD. Therefore, our work contributes a giant step towards practical QKD and real-life applications.

Appendix **A**

Fundamental concepts of quantum mechanics and quantum information measures

A.1 Introduction

We define a few useful concepts in quantum mechanics and information theory, which are applied to this thesis. Additionally, this appendix introduces the common notations that are be used in the thesis.

A.2 Quantum mechanics concepts

Here, we introduce some of the fundamental concepts of quantum mechanics. For the following definitions, we use Dirac notation, typically used by physicists. Assumedly, readers are familiar with the linear algebra concepts discussed in this appendix. For further information, refer to Ref. [\[315\]](#).

A.2.1 Hilbert space

According to quantum mechanics, one can relate any isolated physical system to a Hilbert space [315]. The Hilbert space, denoted by $\mathcal{H}$ is a linear algebraic concept, defined as a vector space over the complex numbers $\mathbb{C}$ equipped with an inner product $\langle x|x \rangle$ such that it is a complete normed space, i.e., $\|x\| = \sqrt{\langle x|x \rangle}$ where $\|x\|$ is interpreted as the length of vector $|x\rangle$.

A.2.2 Quantum states

A quantum state is a mathematical object that enables us to determine unambiguously the probability of the outcome of each possible measurement in a system. The quantum states form the basis for quantum communication. Quantum communication is accomplished by encoding classical information in quantum states. Below, we describe different classes of quantum states.

A.2.2.1 Pure states

A pure state is a normalized vector associated with an isolated quantum system in the Hilbert space $\mathcal{H}$. A unit vector $|\psi\rangle \in \mathcal{H}$ is called a pure state such that $\| |\psi\rangle \| = 1$. The fundamental concept for quantum computation and quantum information is a quantum bit (qubit). Qubits are unit vectors in a two-dimensional complex vector space. The qubit can be represented as an actual physical system, for example, the spin of an electron, the polarization of a photon, or a two-level atom with a ground state and an excited state. As a classical bit has a state of 0 or 1, the two possible states for a qubit are $|0\rangle$ and $|1\rangle$. However, unlike the classical bit, a qubit can exist in a state other than 0 or 1. A qubit can exist as a

superposition of the states $|0\rangle$ and $|1\rangle$, i.e.,

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad (\text{A.1})$$

where α and β are complex numbers that satisfy the condition

$$|\alpha|^2 + |\beta|^2 = 1, \quad (\text{A.2})$$

A.2.2.2 Mixed states

Mixed states refer to a probabilistic mixture of pure states. Generally, the arbitrary state of a system is not always pure. The states of that nature form a mixed state. For definiteness, if a quantum system has a probability of p_i to be in the state $|\psi_i\rangle$ for $i = \{1, 2, \dots, n\}$, then the system is represented by a collection of pure states $\{p_i, |\psi_i\rangle\}$ such that $\sum_{i=1}^n p_i$ and $p_i \geq 0$.

A.2.3 Density operators

A more convenient way to represent quantum states is to use density operators or density matrices [316]. Based on the density operator formalism, pure states can be represented as $\rho := |\psi\rangle\langle\psi|$. When a system is in a mixed state defined by an ensemble of pure states $\{p_i : i = 1, 2, \dots, n, |\psi_i\rangle\}$, the density operator for the system is defined as follows:

$$\rho \equiv \sum_i^n p_i |\psi_i\rangle\langle\psi_i| = \sum_{i=1}^n p_i \rho_i \in D(\mathcal{H}), \quad (\text{A.3})$$

where $\rho_i = |\psi_i\rangle\langle\psi_i|$ and $D(\mathcal{H})$ is the bounded algebra on the Hilbert space $\mathcal{H}$.

A.2.4 Linear operators

Linear operators are functions that describe state vector transformations from one vector space to another [315, 317]. A linear operator between vector spaces $\mathbf{X}$ and $\mathbf{Y}$ is defined to be any function $A : \mathbf{X} \rightarrow \mathbf{Y}$ which is linear in its inputs,

$$A \left(\sum_i a_i |x_i\rangle \right) = \sum_i a_i A(|x_i\rangle). \quad (\text{A.4})$$

For definiteness, if $A : \mathbf{X} \rightarrow \mathbf{Y}$ and $|x_1\rangle, \dots, |x_m\rangle$ is a basis of $\mathbf{X}$, $|y_1\rangle, \dots, |y_n\rangle$ form a basis of $\mathbf{Y}$ then for each $j \in \{1, \dots, m\}$ there exists complex numbers $\{A_{1j}, \dots, A_{nj}\}$ such that

$$A|x_j\rangle = \sum_i A_{ij} |y_i\rangle. \quad (\text{A.5})$$

The values A_{ij} constitute a matrix representation of the operator A . The most commonly used linear operators in quantum information processing tasks to represent unitary single-qubit operations are Pauli operators. These are two-dimensional Hermitian and unitary matrices expressed as:

$$\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

$$\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$\sigma_y = -i(|0\rangle\langle 1| - |1\rangle\langle 0|) = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},$$

$$\mathbb{I} = |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Trace of a matrix

Consider a $n \times n$ matrix A . Then, we define the trace of matrix A as the sum of its diagonal elements: $\text{Tr}(A) = \sum_i A_{ii}$, where A_{ii} denotes the entry on the i th row and i th column of A . The trace function obeys the cyclicity property, $\text{Tr}(AB) = \text{Tr}(BA)$, and linearity property, $\text{Tr}(A + B) = \text{Tr}(A) + \text{Tr}(B)$, $\text{Tr}(zA) = z\text{Tr}(A)$, where A and B are arbitrary matrices, and z denotes a complex number.

A.2.5 Tensor Products

The tensor product is a way of creating larger vector spaces from the product of small vector spaces. Suppose $|x_i\rangle$ and $|y_j\rangle$ are two orthogonal bases in vector spaces $\mathbf{X}$ and $\mathbf{Y}$, respectively. Then, the tensor product of two arbitrary state vectors from these vector spaces denoted as $|\psi\rangle = \sum_i \alpha_i |x_i\rangle$ and $|\phi\rangle = \sum_j \beta_j |y_j\rangle$ is given by

$$\begin{aligned} |\psi\rangle \otimes |\phi\rangle &= \left(\sum_i \alpha_i |x_i\rangle \right) \otimes \left(\sum_j \beta_j |y_j\rangle \right) \\ &= \sum_{ij} \alpha_i \beta_j |x_i, y_j\rangle. \end{aligned}$$

The concept of a tensor product can be used to describe composite systems. Composite systems can be described using two classes of state vectors, namely separable and entangled states.

A.2.5.1 Separable states

A system is in a separable state $\rho_{AB} \in D(\mathcal{H}_{AB})$ if it can be expressed as a convex combination of component states:

$$\rho_{AB} = \sum_x^{\infty} p(x) \rho_A^x \otimes \rho_B^x, \quad (\text{A.6})$$

where $p(x)$ is a probability weighting factor and $\rho_A^x \in D(\mathcal{H}_A), \rho_B^x \in D(\mathcal{H}_B) \forall x$.

A.2.5.2 Entangled states

A composite system that cannot be written as the product of its subsystems, i.e., not separable, is said to be in an entangled state. Entanglement forms a valuable resource for quantum computation and communication. The entangled subsystems (particles) exhibit peculiar correlations such that a measurement performed on one of the particles may uniquely reveal the result of a measurement of the state of another particle. This useful property forms a basis for ensuring security in quantum communication, particularly in teleportation and QKD. The most commonly used entangled states are the Bell and Greenberger–Horne–Zeilinger (GHZ) states. Bell states are four maximally entangled quantum states of two qubits. The states are sometimes referred to as EPR (Einstein, Podolsky and Rosen) pairs named after the authors who described the behaviour of the qubits [318, 319]. These states are written as

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle),$$

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),$$

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle),$$

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle).$$

The GHZ state is an entangled quantum state of $N > 2$ subsystems [320]. For two-dimensional subsystems, i.e., qubits, it can be written as

$$|\Psi\rangle = \frac{|0\rangle^{\otimes N} + |1\rangle^{\otimes N}}{\sqrt{2}}.$$

The widely used GHZ states are the three-qubit states given by

$$|\phi^\pm\rangle = \frac{1}{2\sqrt{2}}(|000\rangle \pm |111\rangle),$$

$$|\varphi^\pm\rangle = \frac{1}{2\sqrt{2}}(|011\rangle \pm |100\rangle),$$

$$|\Psi^\pm\rangle = \frac{1}{2\sqrt{2}}(|101\rangle \pm |010\rangle),$$

$$|\Phi^\pm\rangle = \frac{1}{2\sqrt{2}}(|001\rangle \pm |110\rangle).$$

A.2.6 Reduced Density operator

When dealing with bipartite or multipartite systems, it is of particular interest to consider the smaller component state of some parts of a system. A reduced density operator can be obtained by taking a partial trace on a larger system. Let

$\rho_{AB} \in D(\mathcal{H}_{AB})$. The reduced density operator on system A is $\rho_A = \text{Tr}_B(\rho_{AB})$ and the reduced density operator on system B is $\rho_B = \text{Tr}_A(\rho_{AB})$.

A.2.7 Schmidt decomposition

The Schmidt decomposition is a mathematical tool used to analyze a pure state and its partial trace [321]. Consider a pure bipartite state $\rho_{AB} = |\psi\rangle\langle\psi| \in D(\mathcal{H}_A \otimes \mathcal{H}_B)$. One can describe the bipartite state using Schmidt decomposition as:

$$|\psi\rangle_{AB} = \sum_{j=1}^n \sqrt{\lambda_j} |\bar{j}\rangle_A |j\rangle_B, \quad (\text{A.7})$$

where $\{|\bar{j}\rangle_A; 1, \dots, n\}$ and $\{|j\rangle_B; j = 1, \dots, n\}$ are orthonormal Schmidt basis in $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. The Schmidt coefficients $\sqrt{\lambda_j}$ are square roots of the eigenvalues of the reduced operators $\rho_A = \text{Tr}_B(\rho_{AB}) = \sum_j \lambda_j |\bar{j}\rangle_A \langle\bar{j}|$ and $\rho_B = \text{Tr}_A(\rho_{AB}) = \sum_j \lambda_j |j\rangle_B \langle j|$, respectively.

A.2.8 Purification

In many practical settings in quantum communication, dealing with pure rather than mixed states is more favorable. One can always find a pure state that resides in a large space such that its reduced density operator gives back the original mixed state. Purification is a mathematical procedure that allows one to associate pure states and mixed states [322]. Suppose the state ρ_A on system A can be represented as $\rho_A = \sum_i p_i |i\rangle_A \langle i|$. Then there exists an additional system R and a pure state $|\psi\rangle_{AR}$ on the joint system AR such that $\rho_A = \text{Tr}_R |\psi\rangle_{AR} \langle\psi|$. The pure state $|\psi\rangle_{AR}$ is called a purification of ρ_A . If $\{|i\rangle_R\}_i$ is an orthonormal basis on the system R which has the same dimension as A meaning $\langle i_A | j_R \rangle = \delta_{ij}$ then the purification can be

constructed as

$$|\psi\rangle_{AR} = \sum_i \sqrt{p_i} |i\rangle_A |i\rangle_R. \quad (\text{A.8})$$

A.2.9 Quantum operations

Quantum operations are crucial in several aspects of quantum information and communication tasks. For instance, they explain any physical process a quantum mechanical system undergoes. These include, among others, the evolution of the state of a closed system with time and a description of what transpires to quantum information when it is sent from point A to point B through a noisy quantum channel.

A.2.9.1 Unitary Transformations

A unitary transformation can characterize the evolution of a closed quantum system. Suppose the state $|\psi\rangle$ of the system at time t_0 is associated to the state $|\tilde{\psi}\rangle$ of the system at time t_1 by a unitary operator $\mathcal{U}$ which specifically depends on the times t_0 and t_1 [323]. The time evolution of the system can be described by the Schrödinger representation [315]

$$\begin{aligned} |\tilde{\psi}\rangle &= \exp\left(\frac{-iH(t_1 - t_0)}{\hbar}\right) |\psi\rangle \\ &= \mathcal{U}(t_1 - t_0) |\psi\rangle, \end{aligned} \quad (\text{A.9})$$

where H refers to the Hamiltonian of the physical system. If we have prior knowledge of the system's Hamiltonian, we understand its dynamics completely. In general, a closed quantum system evolves according to a unitary operator $\mathcal{U}$ which

satisfies the condition:

$$\mathcal{U}^\dagger \mathcal{U} = \mathbb{1}. \quad (\text{A.10})$$

A.2.10 Quantum measurement

A.2.10.1 Projective Measurements

Define an observable given by a Hermitian operator $\hat{A}$ whose eigenvalues are $\{a_1, a_2, \dots, a_n\}$ and corresponding eigenstates given by $\{|a_1\rangle, |a_2\rangle, \dots, |a_n\rangle\}$. Suppose a measurement is performed on state $|\psi\rangle$ described by Hermitian operator $\hat{A}$. A projective measurement is defined by an observable $\hat{A}$ on the state space of the system being observed [322]. The spectral decomposition of the observable $\hat{A}$ is given by

$$\hat{A} = \sum_n q_n P_n, \quad (\text{A.11})$$

where $P_n = |q_n\rangle\langle q_n|$ is the projector on the eigenspace of $\hat{A}$ with eigenvalue q_n . The probability of obtaining an eigenvalue q_n , which corresponds to possible outcomes of the measurement of $|\psi\rangle$ is given by

$$p(q_n) = \langle \psi | P_n | \psi \rangle. \quad (\text{A.12})$$

If the result q_n is obtained, the post-measurement state is expressed as

$$\frac{P_n |\psi\rangle}{\sqrt{p(q_n)}}.$$

A.2.10.2 Positive Operator Valued Measure (POVM)

Projective measurements give us the postulates for describing the measurement statistics and the post-measurement state of the system. Various quantum information and communication applications are primarily concerned with the probability of measurement outcomes. POVM formalism becomes handy in such instances. Define a set of measurement operators A_n acting on a quantum system in the state $|\psi\rangle$. The possible outcome n of the measurement on $|\psi\rangle$ is given by $p(n) = \langle\psi|A_n^\dagger A_n|\psi\rangle$. Consider a set of operators given by

$$E_n = A_n^\dagger A_n. \quad (\text{A.13})$$

From elementary linear algebra, E_n is a positive operator which satisfies the completeness relation $\sum_n E_n = I$ and $p(n) = \langle\psi|E_n|\psi\rangle$. The operators E_n are defined as POVM elements associated with the measurement [323]. This set of operators enables us to determine the probabilities of the different measurement outcomes.

A.3 Information theory

This section examines a key element of information processing: quantification of information. Information can be quantified as a measure of the uncertainty in determining the outcome of a random event, i.e., if an event is highly probable, then we gain less information in learning that it eventually occurred and the reverse is true. All this leads us to the concept of entropy [324, 325]. Entropy is an essential tool in information theory since it has operational meaning for numerous information-processing tasks. It is often a necessity for quantitative analyses. In this thesis, we exploit entropic quantities for proving QKD security and calculating secret key rates. We review those necessary entropic quantities in both the classical

and quantum domains.

A.3.1 Classical information theory

A.3.1.1 Shannon Entropy

Shannon entropy measures how much information we gain when we learn the contents of a message [326]. Consider X a discrete random variable whose value x is drawn from a finite set $\mathbf{X}$. Let each possible value x of the random variable X be drawn with probability distribution $p_X(x)$. The Shannon entropy $H(X)$ of X is expressed as

$$H(X) = \sum_{x \in X} p_X(x) \log_2(p_X(x)). \quad (\text{A.14})$$

The Shannon entropy for a random variable with two possible outcomes is called binary entropy function [327] and is given by

$$H(p) = -p \log_2 p - (1 - p) \log_2(1 - p), \quad (\text{A.15})$$

where p and $1 - p$ are the probabilities of the outcomes.

A.3.1.2 Joint Entropy

Suppose we have two random variables X and Y whose possible values x and y , respectively, are drawn with the joint probability distribution $p(x, y)$, then their joint entropy $H(X, Y)$ which quantifies the combined uncertainty of the two is given by [325]

$$H(X, Y) = - \sum_{x, y} p(x, y) \log_2 p(x, y). \quad (\text{A.16})$$

A.3.1.3 Conditional Entropy

Consider two random variables X and Y with realizations x and y . The two random variables share correlations if they are not statistically independent. The conditional entropy $H(X|Y)$ is the measure of uncertainty about X given that one already has access to Y . Thus, if we know the value of the variable, Y , then we can calculate the uncertainty of X from joint entropy of the two variables as

$$\begin{aligned} H(X|Y) &= - \sum_{y \in Y} p(y) \sum_{x \in X} p(x|y) \log p(x|y) \\ &= - \sum_{x,y} p(x,y) \log \frac{p(x,y)}{p(y)}. \end{aligned} \quad (\text{A.17})$$

Conditional information can also be interpreted as

$$H(X|Y) = H(X,Y) - H(Y). \quad (\text{A.18})$$

A.3.1.4 Mutual Information

The mutual information between the two random variables X and Y quantifies the information contained in both variables. It reduces uncertainty about a random variable X due to the knowledge of the random variable Y . The knowledge of Y gives an information gain of $H(X|Y)$ bits about X , and consequently, the overall uncertainty $H(X)$ about X is reduced. Therefore, the mutual information of two random variables X and Y , selected with a joint probability distribution function $p_{X,Y}(x,y)$, is given by

$$I(X : Y) = \sum_{x,y} p_{X,Y}(x,y) \log \frac{p_{X,Y}(x,y)}{p_X(x)p_Y(y)}. \quad (\text{A.19})$$

Mutual information can also be represented as

$$I(X : Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) = I(Y : X). \quad (\text{A.20})$$

A.3.2 Quantum information theory

A.3.2.1 von Neumann Entropy

Classical information theory deals with Shannon entropy, quantifying the degree of uncertainty associated with the random variables. In quantum information theory, we deal with quantum systems defined by an ensemble of quantum states (density operator). Therefore, we employ a quantum analog of information measure called the von Neumann entropy [328]. It is defined as

$$S(\rho) = -\text{tr} \rho \log_2 \rho, \quad (\text{A.21})$$

where the density operator ρ is given by $\rho = \sum_i \lambda_i |i\rangle\langle i|$. Here, λ_i denotes the eigenvalues and $|i\rangle$ correspond to orthonormal basis for which ρ is diagonal.

A.3.2.2 Accesible Information

The accessible information $I_{\text{acc}}(\mathcal{E})$ of an ensemble $\mathcal{E}$ refers to the maximum mutual information between a random variable encoded into quantum states and the probabilistic outcome of a quantum measurement [325, 328]. Consider two communicating parties, Alice and Bob, who wish to exchange classical information encoded in quantum states through a quantum channel. Let ρ_x be the state prepared by Alice from an ensemble $\mathcal{E} := \{\rho_x, p_X(x) : x = 0, \dots, n\}$ according to some random variable X . Note that x is the classical index encoded in the quantum states ρ . If

we define Bob's measurements by POVM elements $\Lambda_y := \{E_y : E_0, \dots, E_n\}$ on the state, with the measurement outcome defined by some random variable Y , then the maximal information gain is given by

$$I_{\text{acc}}(\mathcal{E}) = \max_{\Lambda_y} I(X : Y). \quad (\text{A.22})$$

This quantity is called the accessible information of the ensemble $\mathcal{E}$. The accessible information of an ensemble of mixed states $\{\rho_x, p_X(x)\}$ satisfies

$$I_{\text{acc}}(\mathcal{E}) \leq \chi(\varepsilon), \quad (\text{A.23})$$

and this is known as the Holevo bound [329]. This bound is not tight in general, though it holds with equality for ensembles of mutually orthogonal mixed states. It asserts that for any such measurement, Bob may execute

$$H(X : Y) \leq S(\rho) - \sum_x p_X(x) S(\rho_x), \quad (\text{A.24})$$

where $\rho = \sum_x p_X(x) \rho_x$ is the statistical operator describing Alice's signals. This density operator describes the state from Bob's point of view since he does not have prior knowledge of the classical index x .

Estimation of key rate parameters and derivation of finite key rate for three-party RFI QKD

B.1 Decoy parameters estimation

In this appendix, we derive parameters that are used in determination of the finite key rate in chapter 4. In practice, the signal pulses are generated using a spontaneous parametric down-conversion (SPDC) source, which occasionally emits more than one photon. The signals produced by this source contain photons whose probability distribution is given by

$$p(k|\gamma) = \frac{(k+1)(\frac{\gamma}{2})^k}{(1+\frac{\gamma}{2})^{k+2}}, \quad (\text{B.1})$$

where k is the number of photons and γ is the average intensity of the laser source [330]. Therefore, to combat the PNS attack, Alice randomly prepares the photons using three different intensities (μ, ν, ω) where μ is the intensity for signal

states, ν for decoy states, and ω for vacuum states [223]. The three intensities are selected with the probabilities $P_\mu > P_\nu > P_\omega$ where P_μ, P_ν and P_ω correspond to the probabilities for signal, decoy and vacuum states respectively. The photons are sent to Bob and Charlie, who measure the received pulses in three bases $\{Z, X, Y\}$. The signal states obtained with intensity μ are used for generating the final key, while decoy states acquired from the intensity ν are for bounding Eve's knowledge to the key. In the proposed protocol, Alice measures all the signal pulses, (μ) in the Z basis, and weak decoy pulses, ν in all bases $\{X, Y, Z\}$. The parameters are estimated using the decoy theory as follows. First, we highlight that these parameters are generally derived under two-party communication scenarios, but here, we extend our analysis to accommodate the third party. In our analysis, we assume that the detection probabilities of photons are independently determined by the channel transmittance, $t = 10^{-0.02l}$ where l is the channel length, and detection efficiencies, η_B and η_C of Bob and Charlie's detection systems, respectively. The overall background gain is calculated as

$$\begin{aligned} Q_0 &= Q_{0,B}Q_{0,C} \\ &= Y_0 \left(1 + \frac{\mu}{2}\right)^{-2} Y_0 \left(1 + \frac{\mu}{2}\right)^{-2} = Y_0^2 \left(1 + \frac{\mu}{2}\right)^{-4}, \end{aligned} \quad (\text{B.2})$$

where $Q_{0,B}$ and $Q_{0,C}$ are the background gains for Bob and Charlie, respectively and Y_0 is the background count rate. Following the method used in Ref. [331], the gain of signal or decoy states of intensity γ prepared by Alice in basis Γ_A and measured by Bob and Charlie in basis Γ_B and Γ_C , respectively, can be expressed as

$$\begin{aligned} Q_{\gamma, \Gamma_A \Gamma_B \Gamma_C} &= \frac{1}{2} \left[Y_{\gamma, \Gamma_A^0 \Gamma_B^0 \Gamma_C^0} + Y_{\gamma, \Gamma_A^0 \Gamma_B^1 \Gamma_C^1} + Y_{\gamma, \Gamma_A^1 \Gamma_B^0 \Gamma_C^0} + Y_{\gamma, \Gamma_A^1 \Gamma_B^1 \Gamma_C^1} + Y_{\gamma, \Gamma_A^0 \Gamma_B^0 \Gamma_C^1} + Y_{\gamma, \Gamma_A^0 \Gamma_B^1 \Gamma_C^0} \right. \\ &\quad \left. + Y_{\gamma, \Gamma_A^1 \Gamma_B^0 \Gamma_C^1} + Y_{\gamma, \Gamma_A^1 \Gamma_B^1 \Gamma_C^0} \right], \end{aligned} \quad (\text{B.3})$$

with $\gamma \in \{\mu, \nu\}$, $\Gamma_A, \Gamma_B, \Gamma_C \in \{X, Y, Z\}$. The orthonormal states $\Gamma_{A(B)(C)}^0$ and $\Gamma_{A(B)(C)}^1$ belong to the basis $\Gamma_{A(B)(C)}$. The parameter $Y_{\gamma, \Gamma_A^0 \Gamma_B^0 \Gamma_C^0}$ corresponds to the probability of Bob and Charlie measuring Γ_B^0 and Γ_C^0 , respectively, conditional on Alice preparing the two states Γ_A^0 with intensity γ . The other conditional probabilities can be described in a similar manner. The factor $\frac{1}{2}$ in Eq. (B.3) represents the probability of Alice preparing the qubits in state Γ_A^0 or Γ_A^1 . Eq. (B.3) is a generalised expression for different gains, so we evaluate $Q_{\gamma, X_A X_B X_C}$ as an example to demonstrate how to explicitly obtain these gains. First, we define $Y_{\gamma, X_A^0 X_B^0 X_C^0}$ as follows

$$\begin{aligned}
Y_{\gamma, X_A^0 X_B^0 X_C^0} &= \sum_{k=0}^{\infty} p(k|\gamma) \sum_{j=0}^k C_j^k (\eta_B t)^j (1 - \eta_B t)^{k-j} (\langle X_A^0 | X_B^0 \rangle)^2 \chi(k) \sum_{k=0}^{\infty} p(k|\gamma) \\
&\quad \times \sum_{j=0}^k C_j^k (\eta_C t)^j (1 - \eta_C t)^{k-j} (\langle X_A^0 | X_C^0 \rangle)^2 \chi(k) \\
&= e^{-2\gamma \eta_B t \eta_C t} (1 - Y_0)^2 \left(e^{\gamma \eta_B t \frac{1+\cos \beta}{2}} + Y_0 - 1 \right) \left(e^{\gamma \eta_C t \frac{1+\cos \beta}{2}} + Y_0 - 1 \right),
\end{aligned} \tag{B.4}$$

where

$$\chi(k) = \begin{cases} 1 - Y_0 & \text{if } k > 0 \\ Y_0(1 - Y_0) & \text{if } k = 0 \end{cases}$$

denotes the probability of valid detection events conditional on k -photon states.

The other conditional probabilities are analogously obtained as

$$Y_{\gamma, X_A^0 X_B^1 X_C^1} = e^{-2\gamma\eta_B t \eta_C t} (1 - Y_0)^2 \left(e^{\gamma\eta_B t \frac{1-\cos\beta}{2}} + Y_0 - 1 \right) \left(e^{\gamma\eta_C t \frac{1-\cos\beta}{2}} + Y_0 - 1 \right), \quad (\text{B.5})$$

$$Y_{\gamma, X_A^1 X_B^0 X_C^0} = e^{-2\gamma\eta_B t \eta_C t} (1 - Y_0)^2 \left(e^{\gamma\eta_B t \frac{1-\cos\beta}{2}} + Y_0 - 1 \right) \left(e^{\gamma\eta_C t \frac{1-\cos\beta}{2}} + Y_0 - 1 \right), \quad (\text{B.6})$$

$$Y_{\gamma, X_A^1 X_B^1 X_C^1} = e^{-2\gamma\eta_B t \eta_C t} (1 - Y_0)^2 \left(e^{\gamma\eta_B t \frac{1+\cos\beta}{2}} + Y_0 - 1 \right) \left(e^{\gamma\eta_C t \frac{1+\cos\beta}{2}} + Y_0 - 1 \right), \quad (\text{B.7})$$

$$Y_{\gamma, X_A^0 X_B^0 X_C^1} = e^{-2\gamma\eta_B t \eta_C t} (1 - Y_0)^2 \left(e^{\gamma\eta_B t \frac{1+\cos\beta}{2}} + Y_0 - 1 \right) \left(e^{\gamma\eta_C t \frac{1-\cos\beta}{2}} + Y_0 - 1 \right), \quad (\text{B.8})$$

$$Y_{\gamma, X_A^0 X_B^1 X_C^0} = e^{-2\gamma\eta_B t \eta_C t} (1 - Y_0)^2 \left(e^{\gamma\eta_B t \frac{1-\cos\beta}{2}} + Y_0 - 1 \right) \left(e^{\gamma\eta_C t \frac{1+\cos\beta}{2}} + Y_0 - 1 \right), \quad (\text{B.9})$$

$$Y_{\gamma, X_A^1 X_B^0 X_C^1} = e^{-2\gamma\eta_B t \eta_C t} (1 - Y_0)^2 \left(e^{\gamma\eta_B t \frac{1-\cos\beta}{2}} + Y_0 - 1 \right) \left(e^{\gamma\eta_C t \frac{1+\cos\beta}{2}} + Y_0 - 1 \right), \quad (\text{B.10})$$

$$Y_{\gamma, X_A^1 X_B^0 X_C^0} = e^{-2\gamma\eta_B t \eta_C t} (1 - Y_0)^2 \left(e^{\gamma\eta_B t \frac{1+\cos\beta}{2}} + Y_0 - 1 \right) \left(e^{\gamma\eta_C t \frac{1-\cos\beta}{2}} + Y_0 - 1 \right). \quad (\text{B.11})$$

Here, we assume that the degree of misalignment β is the same for Bob and Charlie's channels. The overall gain, $Q_{\gamma, X_A X_B X_C}$ is obtained by combining the results of Eqs. (B.4) to (B.11). The overall quantum bit error rate is described as follows

$$E_{\gamma, \Gamma_A \Gamma_B \Gamma_C} = \frac{Y_{\gamma, \Gamma_A^0 \Gamma_B^1 \Gamma_C^1} + Y_{\gamma, \Gamma_A^1 \Gamma_B^0 \Gamma_C^0} + Y_{\gamma, \Gamma_A^0 \Gamma_B^0 \Gamma_C^1} + Y_{\gamma, \Gamma_A^0 \Gamma_B^1 \Gamma_C^0} + Y_{\gamma, \Gamma_A^1 \Gamma_B^0 \Gamma_C^1} + Y_{\gamma, \Gamma_A^1 \Gamma_B^1 \Gamma_C^0}}{Q_{\gamma, \Gamma_A \Gamma_B \Gamma_C}}. \quad (\text{B.12})$$

The gain for single photon components is expressed as

$$\begin{aligned}
Q_{\mu,ZZZ}^1 &= Y_{\mu,ZZZ}^1 (p(1|\mu))^2 \\
&= [1 - (1 - Y_{0B})(1 - \eta_B t)][1 - (1 - Y_{0C})(1 - \eta_C t)] \frac{\mu}{(1 + \frac{\mu}{2})^3}. \quad (\text{B.13})
\end{aligned}$$

The upper bound, I_E^U dependent on the parameters C and E_{ZZZ} is obtained from the lower bound C_1^L and upper bound for error rate in the Z basis, $e_{ZZZ}^{1,U}$ for single photon components. The latter parameter is expressed as

$$e_{ZZZ}^{1,U} = \frac{E_{\mu,ZZZ} Q_{\mu,ZZZ} - e_0 Y_0 p(\mu|0)}{Y_{1,L} p(\mu|1)} \quad (\text{B.14})$$

where

$$Y_{1,L} = \frac{p(\mu|2)[Q_{\nu,\Gamma_A\Gamma_B\Gamma_C} - p(\nu|0)Y_0] - p(\nu|2)[Q_{\mu,\Gamma_A\Gamma_B\Gamma_C} - p(\mu|0)Y_0]}{p(\mu|2)p(\nu|1) - p(\mu|1)p(\nu|2)}. \quad (\text{B.15})$$

In the above equation, $p(\gamma|k)$ is the probability that signals generated with intensity $\gamma \in \{\mu, \nu\}$ contain k photons. The lower bound of C for single-photon states can be obtained in terms of error rates from measurements in the complementary bases as

$$\begin{aligned}
C_1^L &= (1 - 2e_{XX}^{1,U})^2 + (1 - 2e_{XY}^{1,U})^2 + (1 - 2e_{YX}^{1,U})^2 + (1 - 2e_{YY}^{1,U})^2 + (1 - 2e_{XX}^{1,U})^2 \\
&\quad + (1 - 2e_{XY}^{1,U})^2 + (1 - 2e_{YX}^{1,U})^2 + (1 - 2e_{YY}^{1,U})^2. \quad (\text{B.16})
\end{aligned}$$

The upper bound on error rates $e_{\alpha\beta\delta}$ with α, β and $\delta \in \{X, Y\}$ obtained from the

signals produced using the decoy intensity are given by

$$E_{\nu, \Gamma_A \Gamma_B \Gamma_C} Q_{\nu, \Gamma_A \Gamma_B \Gamma_C} = \frac{1}{2} \left(1 + \frac{\nu}{2}\right)^{-2} Y_0 + e_{\alpha\beta\delta}^1 \frac{\nu}{(1 + \frac{\nu}{2})^3} Y_1 + \sum_{k \geq 2} e_{\alpha\beta\delta}^k \frac{(1+k)(\frac{\nu}{2})^k}{(1 + \frac{\nu}{2})^{k+2}} Y_k;$$

$$e_{\alpha\beta\delta}^{1,U} \leq \frac{E_{\nu, \Gamma_A \Gamma_B \Gamma_C} Q_{\nu, \Gamma_A \Gamma_B \Gamma_C} - e_0 Y_0 (1 + \frac{\nu}{2})^{-2}}{Y_{1,L} \frac{\nu}{(1 + \frac{\nu}{2})^3}}.$$
(B.17)

Finally, the upper bound of I_E based on $e_{ZZZ}^{1,U}$ and C_1^L is determined using the following equations

$$I_E^U = (1 - e_{ZZZ}^{1,U}) h\left(\frac{1 + u_{\max}}{2}\right) - e_{ZZZ}^{1,U} h\left(\frac{1 + v(u_{\max})}{2}\right) + e_{ZZZ}^{1,U} \log_2 7, \quad (\text{B.18})$$

where

$$u_{\max} = \min \left[\frac{1}{1 - e_{ZZZ}^{1,U}} \sqrt{C_1^L/4}, 1 \right],$$

$$v(u_{\max}) = \sqrt{\frac{49}{19} \left[C_1^L/4 - (1 - e_{ZZZ}^{1,U})^2 u_{\max}^2 \right]} / e_{ZZZ}^{1,U}. \quad (\text{B.19})$$

B.2 Secrecy

We provide details for deriving key length and security bounds presented in Chapter 4. We use the entropic uncertainty relations to establish bounds on the smooth-min entropy of the raw key conditioned on Eve's information. Let system $\hat{\mathbf{E}}$ be information that Eve gains on $\mathbf{Z}_A$, $\mathbf{Z}_B$ and $\mathbf{Z}_C$, i.e., the raw key for Alice, Bob, and Charlie up to the error correction step. If Alice, Bob, and Charlie apply a privacy amplification scheme based on two universal hashing [210] to extract shorter key

strings of length ℓ from Z measurement statistics, the protocol is Δ -secret if

$$\Delta \leq 2\varepsilon + \frac{1}{2}\sqrt{2^{\ell - H_{\min}^{\varepsilon}(\mathbf{Z}_A|\dot{\mathbf{E}})}}, \quad (\text{B.20})$$

where $H_{\min}^{\varepsilon}(\mathbf{Z}_A|\dot{\mathbf{E}})$ is the smooth-min entropy [217, 218]. It measures the maximum probability that an eavesdropper with access to $\dot{\mathbf{E}}$ can guess correctly Alice's bit string, $\mathbf{Z}_A$ by using the optimal attacking strategy. Let $v = \frac{1}{2}\sqrt{2^{\ell - H_{\min}^{\varepsilon}(\mathbf{Z}_A|\dot{\mathbf{E}})}}$ then,

$$\ell = H_{\min}^{\varepsilon}(\mathbf{Z}_A|\dot{\mathbf{E}}) - 2\log_2\left(\frac{1}{2v}\right). \quad (\text{B.21})$$

By applying chain rule inequality for smooth entropies and using the fact that the amount of information leaked to an eavesdropper during the error correction step is $\text{leak}_{EC} + \log_2\left(\frac{2}{\varepsilon_{\text{cor}}}\right)$ we have

$$H_{\min}^{\varepsilon}(\mathbf{Z}_A|\dot{\mathbf{E}}) \geq H_{\min}^{\varepsilon}(\mathbf{Z}_A|\mathbf{E}) - \text{leak}_{EC} + \log_2\left(\frac{2}{\varepsilon_{\text{cor}}}\right), \quad (\text{B.22})$$

where $\mathbf{E}$ is the remaining information available to Eve. Since we are considering the implementation with decoy states, it is important to note that $\mathbf{Z}_A$ can be decomposed into $\mathbf{Z}_A^v \mathbf{Z}_A^s \mathbf{Z}_A^m$ which corresponds to bit strings due to vacuum, single photon and multi-photon events. By applying the generalized chained rule according to Ref. [240] we have

$$H_{\min}^{\varepsilon}(\mathbf{Z}_A|\mathbf{E}) \geq H_{\min}^{\delta_1}(\mathbf{Z}_A^s|\mathbf{Z}_A^v \mathbf{Z}_A^m|\mathbf{E}) + H_{\min}^{\delta_3+2\delta_4+\delta_5}(\mathbf{Z}_A^v \mathbf{Z}_A^m|\mathbf{E}) - 2\log_2\left(\frac{1}{\delta_2}\right) - 1, \quad (\text{B.23})$$

where $\epsilon = 2\delta_1 + \delta_2 + (\delta_3 + \delta_4 + \delta_5)$ for all $\delta_i > 0$. Further, we can apply the chain rule on the second term on the r.h.s to obtain

$$\begin{aligned} H_{\min}^{\delta_3+2\delta_4+\delta_5}(\mathbf{Z}_A^v \mathbf{Z}_A^m | \mathbf{E}) &\geq H_{\min}^{\delta_4}(\mathbf{Z}_A^m | \mathbf{Z}_A^v | \mathbf{E}) + H_{\min}^{\delta_5}(\mathbf{Z}_A^v | \mathbf{E}) - 2 \log_2 \left(\frac{1}{\delta_3} \right) - 1 \\ &\geq N_\mu p_z^3 Q_0 - 2 \log_2 \left(\frac{1}{\delta_3} \right) - 1, \end{aligned} \quad (\text{B.24})$$

where N_μ is the number of signals sent with intensity μ , p_z is the probability of selecting the Z basis and Q_0 is the gain vacuum events. The second inequality results from these two conditions; $H_{\min}^{\delta_4}(\mathbf{Z}_A^m | \mathbf{Z}_A^v | \mathbf{E}) \geq 0$ and $H_{\min}^{\delta_5}(\mathbf{Z}_A^v | \mathbf{E}) = H_{\min}(\mathbf{Z}^v) = \log_2 2^{N_\mu p_z^3 Q_0} = N_\mu p_z^3 Q_0$. The former stems from the fact that all multi-photon events are considered to be insecure due to PNS attack. The latter is due to the fact that vacuum contributions do not carry any information on bit encodings.

We now provide the bound for smooth min-entropy $H_{\min}^{\delta_1}(\mathbf{Z}_A^s | \mathbf{Z}_A^v \mathbf{Z}_A^m | \mathbf{E})$ with restriction to single photon events based on the uncertainty relations for smooth entropies [217]. We consider a gedankenexperiment in which all measurements are done in the Y and X bases by the communicating parties: Alice, Bob and Charlie. They have to extract n raw keys from single photon events using compatible measurements, i.e., $X_A \otimes X_B \otimes X_C$ and $Y_A \otimes Y_B \otimes Y_C$. The bound obtained from the max-entropy between Alice, Bob and Charlie is given by

$$\begin{aligned} H_{\min}^{\delta_1}(\mathbf{Z}_A^s | \mathbf{Z}_A^v \mathbf{Z}_A^m | \mathbf{E}) &\geq n - H_{\max}^\epsilon(\mathbf{C}_A | \dot{\mathbf{C}}) \\ &= n[1 - I_E^U(C, e)]. \end{aligned} \quad (\text{B.25})$$

Here, $n = N_\mu p_z^3 Q_{\mu, ZZZ}^1$ is the size of a sifted raw key from single-photon events, $\mathbf{C}_A$ is Alice's key bit string obtained from complementary bases, (X, Y) and similarly $\dot{\mathbf{C}}$ is key bit string for either Bob or Charlie. The term $I_E^U(C, e)$ is determined in terms of C and e . The statistical quantity C is obtained from average values of incompatible measurement results from the hypothetical experiment. Lastly, e is

the bit error rate of bit strings $\mathbf{C}_A$ and $\hat{\mathbf{C}}$ which is equivalent to the error rate e_{ZZZ} in the real QKD protocol as described in the previous section.

Finally, we compose the error terms from statistical fluctuations due to finite sample sizes as described in chapter 4. In chapter 4, we found out that there is error probability, ε_1 due to the estimation of expected error rate, e_{ZZZ} by using Lemma 1 of Ref. [267]. The expected error rates in the complementary bases $e_{\alpha\beta\delta}$ with $\alpha, \beta, \delta \in \{X, Y\}$ are obtained analogously applying Lemma 1 with failure probability, ε_1 . The error rates from the incompatible measurements in the complementary bases are eight, bringing the sum of error probabilities to $8\varepsilon_1$. We also estimated the observed number of signals with single photon components using Lemma 2 of Ref. [267] with failure probability, ε_2 . Lemma 3 was used to estimate the expected values, $\bar{n}_\mu$ and $\bar{n}_\nu$ with failure probability, ε_3 for each. Therefore, combining all the error terms for min-entropies and estimation of expected and observed values, the secrecy is given by

$$\varepsilon_{\text{sec}} = 2\varepsilon + 2(\delta_1 + \delta_2 + \delta_3) + v + 9\varepsilon_1 + \varepsilon_2 + 3\varepsilon_3. \quad (\text{B.26})$$

In this case, $\delta_4, \delta_5 = 0$ and we set every error term to a common value ε and $\varepsilon_{\text{sec}} = 22\varepsilon$. The final key length ℓ is obtained by substituting the results of Eq. (B.22) up to Eq. (B.25) and secrecy condition from Eq. (B.26) into Eq. (B.21). The formula is expressed as

$$\ell = N_\mu p_z^3 \left[Q_0 + Q_{ZZZ}^{1,\mu} (1 - I_E^U) - \text{leak}_{EC} - \log_2 \frac{2}{\varepsilon_{\text{cor}}} - 2 \log_2 \frac{11}{\varepsilon_{\text{sec}}} \right]. \quad (\text{B.27})$$

Determination of yields in the virtual and actual protocols

C.1 Determination of yield for virtual states

This section provides an explicit derivation of the yield for virtual states, which are used to deduce error rates for bounding Eve's information. We demonstrate how to concisely represent the joint probabilities of these states in terms of the transmission rate of identity and Pauli operators. The yields for virtual states as defined by Eq. (5.15) in the main text are given by

$$\begin{aligned}
 Y_{\Phi^+;0_X0_X}^{Z,\text{vir}} &= \frac{1}{8} \text{Tr}(\hat{D}_{\Phi^+} \hat{\sigma}_{C;0_X0_X}^{\text{vir}}) \\
 &= \frac{1}{32} \left[\left(\frac{3}{16} + \frac{1}{4\sqrt{2}} \right) q_{\Phi^+|\mathbb{1},\mathbb{1}} + \left(\frac{1}{8} + \frac{1}{8\sqrt{2}} \right) q_{\Phi^+|\mathbb{1},Z} + \frac{1}{16} \left(\frac{7}{2} + \frac{5}{\sqrt{2}} \right) q_{\Phi^+|\mathbb{1},X} \right. \\
 &\quad + \left(\frac{1}{8} + \frac{1}{8\sqrt{2}} \right) q_{\Phi^+|Z,\mathbb{1}} + \frac{1}{8} q_{\Phi^+|Z,Z} + \frac{1}{16} \left(\frac{3}{2 + \sqrt{2}} \right) q_{\Phi^+|Z,X} \\
 &\quad \left. + \frac{1}{16} \left(\frac{7}{2} + \frac{5}{\sqrt{2}} \right) q_{\Phi^+|X,\mathbb{1}} + \frac{1}{16} \left(\frac{3}{2 + \sqrt{2}} \right) q_{\Phi^+|X,Z} + \frac{1}{16} \left(\frac{6}{\sqrt{2}} + \frac{17}{4} \right) q_{\Phi^+|X,X} \right],
 \end{aligned} \tag{C.1}$$

$$\begin{aligned}
Y_{\Phi^+;0_X 1_X}^{Z,\text{vir}} &= \frac{1}{8} \text{Tr}(\hat{D}_{\Phi^+} \hat{\sigma}_{C;0_X 1_X}^{\text{vir}}) \\
&= \frac{1}{32} \left[\frac{1}{8\sqrt{2}} q_{\Phi^+|\mathbb{1},\mathbb{1}} - \frac{1}{16} q_{\Phi^+|\mathbb{1},Z} - \frac{1}{16} q_{\Phi^+|\mathbb{1},X} + \frac{1}{16} \left(\frac{4}{\sqrt{2}-2} \right) q_{\Phi^+|Z,\mathbb{1}} \right. \\
&\quad + \frac{1}{16} \left(\frac{2}{\sqrt{2}} - 2 \right) q_{\Phi^+|Z,Z} + \frac{1}{16} \left(\frac{2}{\sqrt{2}} - 2 \right) q_{\Phi^+|Z,X} + \frac{1}{16} \left(\frac{1}{\sqrt{2}} + 1 \right) q_{\Phi^+|X,\mathbb{1}} \\
&\quad \left. - \frac{1}{16} \left(\frac{1}{\sqrt{2}} + \frac{1}{2} \right) q_{\Phi^+|X,Z} - \frac{1}{16} \left(\frac{1}{\sqrt{2}} + \frac{1}{2} \right) q_{\Phi^+|X,X} \right], \tag{C.2}
\end{aligned}$$

$$\begin{aligned}
Y_{\Phi^+;1_X 0_X}^{Z,\text{vir}} &= \frac{1}{8} \text{Tr}(\hat{D}_{\Phi^+} \hat{\sigma}_{C;1_X 0_X}^{\text{vir}}) \\
&= \frac{1}{32} \left[\frac{1}{8\sqrt{2}} q_{\Phi^+|\mathbb{1},\mathbb{1}} + \frac{1}{16} \left(\frac{4}{\sqrt{2}} - 2 \right) q_{\Phi^+|\mathbb{1},Z} + \frac{1}{16} \left(\frac{1}{\sqrt{2}} + 1 \right) q_{\Phi^+|\mathbb{1},X} \right. \\
&\quad - \frac{1}{16} q_{\Phi^+|Z,\mathbb{1}} + \frac{1}{16} \left(\frac{2}{\sqrt{2}} - 2 \right) q_{\Phi^+|Z,Z} - \frac{1}{16} \left(\frac{1}{\sqrt{2}} + \frac{1}{2} \right) q_{\Phi^+|Z,X} - \frac{1}{16} q_{\Phi^+|X,\mathbb{1}} \\
&\quad \left. + \frac{1}{16} \left(\frac{2}{\sqrt{2}} - 2 \right) q_{\Phi^+|X,Z} - \frac{1}{16} \left(\frac{1}{\sqrt{2}} + \frac{1}{2} \right) q_{\Phi^+|X,X} \right], \tag{C.3}
\end{aligned}$$

$$\begin{aligned}
Y_{\Phi^+;1_X 1_X}^{Z,\text{vir}} &= \frac{1}{8} \text{Tr}(\hat{D}_{\Phi^+} \hat{\sigma}_{C;1_X 1_X}^{\text{vir}}) \\
&= \frac{1}{32} \left[\frac{1}{16} \left(6 - \frac{8}{\sqrt{2}} \right) q_{\Phi^+|\mathbb{1},\mathbb{1}} + \frac{1}{16} \left(4 - \frac{6}{\sqrt{2}} \right) q_{\Phi^+|\mathbb{1},Z} + \frac{1}{16} \left(4 - \frac{6}{\sqrt{2}} \right) q_{\Phi^+|\mathbb{1},X} \right. \\
&\quad + \frac{1}{16} \left(4 - \frac{6}{\sqrt{2}} \right) q_{\Phi^+|Z,\mathbb{1}} + \frac{1}{16} \left(3 - \frac{4}{\sqrt{2}} \right) q_{\Phi^+|Z,Z} + \frac{1}{16} \left(3 - \frac{4}{\sqrt{2}} \right) q_{\Phi^+|Z,X} \\
&\quad \left. + \frac{1}{16} \left(4 - \frac{6}{\sqrt{2}} \right) q_{\Phi^+|X,\mathbb{1}} + \frac{1}{16} \left(3 - \frac{4}{\sqrt{2}} \right) q_{\Phi^+|X,Z} + \frac{1}{16} \left(3 - \frac{4}{\sqrt{2}} \right) q_{\Phi^+|X,X} \right]. \tag{C.4}
\end{aligned}$$

Let the coefficients of transmission rates be given by a row vector $\mathbf{V}_{\Phi^+;j\mathbf{X}k\mathbf{X}}$ and the transmission rate of identity and Pauli operators be denoted by a column vector $\mathbf{q}$ such that

$$Y_{\Phi^+;j_X k_X}^{Z,\text{vir}} = \mathbf{V}_{\Phi^+;j\mathbf{X}k\mathbf{X}} \mathbf{q}, \tag{C.5}$$

where

$$\mathbf{q} = [q_{\Phi^+|\mathbb{1},\mathbb{1}}, q_{\Phi^+|\mathbb{1},X}, q_{\Phi^+|\mathbb{1},Y}, q_{\Phi^+|\mathbb{1},Z}, q_{\Phi^+|X,\mathbb{1}}, q_{\Phi^+|X,X}, q_{\Phi^+|X,Y}, q_{\Phi^+|X,Z}, q_{\Phi^+|Y,\mathbb{1}}, \\ q_{\Phi^+|Y,X}, q_{\Phi^+|Y,Y}, q_{\Phi^+|Y,Z}, q_{\Phi^+|Z,\mathbb{1}}, q_{\Phi^+|Z,X}, q_{\Phi^+|Z,Y}, q_{\Phi^+|Z,Z}]^T. \quad (\text{C.6})$$

Then, the vectors $\mathbf{V}_{\Phi^+;j\mathbf{X}k\mathbf{X}}$ for different yields become

$$\mathbf{V}_{\Phi^+;0\mathbf{X}0\mathbf{X}} = \left[\left(\frac{3}{16} + \frac{1}{4\sqrt{2}} \right), \frac{1}{16} \left(\frac{7}{2} + \frac{5}{\sqrt{2}} \right), 0, \left(\frac{1}{8} + \frac{1}{8\sqrt{2}} \right), \frac{1}{16} \left(\frac{7}{2} + \frac{5}{\sqrt{2}} \right), \right. \\ \left. \frac{1}{16} \left(\frac{6}{\sqrt{2}} + \frac{17}{4} \right), 0, \frac{1}{16} \left(\frac{3}{2 + \sqrt{2}} \right), 0, 0, 0, 0, \left(\frac{1}{8} + \frac{1}{8\sqrt{2}} \right), \frac{1}{16} \left(\frac{3}{2 + \sqrt{2}} \right), 0, \frac{1}{8} \right] \quad (\text{C.7})$$

$$\mathbf{V}_{\Phi^+;0\mathbf{X}1\mathbf{X}} = \left[\frac{1}{8\sqrt{2}}, -\frac{1}{16}, 0, -\frac{1}{16}, \frac{1}{16} \left(\frac{1}{\sqrt{2}} + 1 \right), -\frac{1}{16} \left(\frac{1}{\sqrt{2}} + \frac{1}{2} \right), 0, -\frac{1}{16} \left(\frac{1}{\sqrt{2}} + \frac{1}{2} \right), \right. \\ \left. 0, 0, 0, 0, \frac{1}{16} \left(\frac{4}{\sqrt{2} - 2} \right), \frac{1}{16} \left(\frac{2}{\sqrt{2}} - 2 \right), 0, \frac{1}{16} \left(\frac{2}{\sqrt{2}} - 2 \right) \right] \quad (\text{C.8})$$

$$\mathbf{V}_{\Phi^+;1\mathbf{X}0\mathbf{X}} = \left[\frac{1}{8\sqrt{2}}, \frac{1}{16} \left(\frac{1}{\sqrt{2}} + 1 \right), 0, \frac{1}{16} \left(\frac{4}{\sqrt{2}} - 2 \right), -\frac{1}{16}, -\frac{1}{16} \left(\frac{1}{\sqrt{2}} + \frac{1}{2} \right), 0, \right. \\ \left. \frac{1}{16} \left(\frac{2}{\sqrt{2}} - 2 \right), 0, 0, 0, 0, -\frac{1}{16}, -\frac{1}{16} \left(\frac{1}{\sqrt{2}} + \frac{1}{2} \right), 0, \frac{1}{16} \left(\frac{2}{\sqrt{2}} - 2 \right) \right] \quad (\text{C.9})$$

$$\mathbf{V}_{\Phi^+;1\mathbf{X}1\mathbf{X}} = \left[\frac{1}{16} \left(6 - \frac{8}{\sqrt{2}} \right), \frac{1}{16} \left(4 - \frac{6}{\sqrt{2}} \right), 0, \frac{1}{16} \left(4 - \frac{6}{\sqrt{2}} \right), \frac{1}{16} \left(4 - \frac{6}{\sqrt{2}} \right), \right. \\ \left. \frac{1}{16} \left(3 - \frac{4}{\sqrt{2}} \right), 0, \frac{1}{16} \left(3 - \frac{4}{\sqrt{2}} \right), 0, 0, 0, 0, \frac{1}{16} \left(4 - \frac{6}{\sqrt{2}} \right), \frac{1}{16} \left(3 - \frac{4}{\sqrt{2}} \right), \right. \\ \left. 0, \frac{1}{16} \left(3 - \frac{4}{\sqrt{2}} \right) \right] \quad (\text{C.10})$$

Furthermore, if we denote yields as a vector

$$\mathbf{Y}_{\Phi^+;j\mathbf{X}k\mathbf{X}}^{\mathbf{Z},\text{vir}} = [Y_{\Phi^+;0\mathbf{X}0\mathbf{X}}^{\mathbf{Z},\text{vir}}, Y_{\Phi^+;0\mathbf{X}1\mathbf{X}}^{\mathbf{Z},\text{vir}}, Y_{\Phi^+;1\mathbf{X}0\mathbf{X}}^{\mathbf{Z},\text{vir}}, Y_{\Phi^+;1\mathbf{X}1\mathbf{X}}^{\mathbf{Z},\text{vir}}]^T \quad (\text{C.11})$$

and $\mathbf{V}$ as a matrix

$$\mathbf{V} = [\mathbf{V}_{\Phi^+;0\mathbf{X}0\mathbf{X}}, \mathbf{V}_{\Phi^+;0\mathbf{X}1\mathbf{X}}, \mathbf{V}_{\Phi^+;1\mathbf{X}0\mathbf{X}}, \mathbf{V}_{\Phi^+;1\mathbf{X}1\mathbf{X}}], \quad (\text{C.12})$$

the joint probabilities can succinctly be written as

$$\mathbf{Y}_{\Phi^+, \mathbf{j} \mathbf{k} \mathbf{x}}^{\mathbf{Z}, \text{vir}} = \mathbf{V} \mathbf{q}. \quad (\text{C.13})$$

C.2 Determination of yield of states used in the actual protocol

We compute the joint probabilities for sending the four states used in the actual protocol and show that by using the transmission rate for these states, one can obtain the yield of virtual states described above and subsequently estimate the error rate E_{XX} . From the actual experiment, we have the following constraints,

$$\begin{aligned} Y_{\Phi^+, 0_Z 0_Z} &= \frac{1}{8} \text{Tr}(\hat{D}_{\Phi^+} \sigma_{C; 0_Z 0_Z}^Z) \\ &= (q_{\Phi^+ | \mathbf{1}, \mathbf{1}} + q_{\Phi^+ | \mathbf{1}, Z} + q_{\Phi^+ | Z, \mathbf{1}} + q_{\Phi^+ | Z, Z})/32, \end{aligned} \quad (\text{C.14})$$

where

$$\begin{aligned} \sigma_{C; 0_Z 0_Z}^Z &= \text{Tr}[\hat{P}(|0_Z\rangle) \otimes \hat{P}(|0_Z\rangle) \otimes \mathbb{1}_C \hat{P}(|\Psi_Z\rangle_{AC} \otimes |\Psi_Z\rangle_{BC})] \\ &= \frac{1}{4} |\phi_{0Z}\rangle \langle \phi_{0Z}| \otimes |\phi_{0Z}\rangle \langle \phi_{0Z}|, \end{aligned}$$

$$\begin{aligned} Y_{\Phi^+, 0_Z 1_Z} &= \frac{1}{8} \text{Tr}(\hat{D}_{\Phi^+} \sigma_{C; 0_Z 1_Z}^Z) \\ &= \frac{1}{8} \left(\frac{1}{4} q_{\Phi^+ | \mathbf{1}, \mathbf{1}} + \frac{1}{4} q_{\Phi^+ | \mathbf{1}, X} + \frac{1}{4} q_{\Phi^+ | Z, \mathbf{1}} + \frac{1}{4} q_{\Phi^+ | Z, X} \right), \end{aligned} \quad (\text{C.15})$$

$$\begin{aligned}
 Y_{\Phi^+;1_Z 0_Z} &= \frac{1}{8} \text{Tr}(\hat{D}_{\Phi^+} \sigma_{C;1_Z 0_Z}^Z) \\
 &= \frac{1}{8} \left(\frac{1}{4} q_{\Phi^+|\mathbb{1},\mathbb{1}} + \frac{1}{4} q_{\Phi^+|\mathbb{1},Z} + \frac{1}{4} q_{\Phi^+|X,\mathbb{1}} + \frac{1}{4} q_{\Phi^+|X,Z} \right), \quad (\text{C.16})
 \end{aligned}$$

$$\begin{aligned}
 Y_{\Phi^+;1_Z 1_Z} &= \frac{1}{8} \text{Tr}(\hat{D}_{\Phi^+} \sigma_{C;1_Z 1_Z}^Z) \\
 &= \frac{1}{8} \left(\frac{1}{4} q_{\Phi^+|\mathbb{1},\mathbb{1}} + \frac{1}{4} q_{\Phi^+|\mathbb{1},X} + \frac{1}{4} q_{\Phi^+|X,\mathbb{1}} + \frac{1}{4} q_{\Phi^+|X,X} \right), \quad (\text{C.17})
 \end{aligned}$$

$$\begin{aligned}
 Y_{\Phi^+;0_X 0_Z} &= \frac{1}{8} \text{Tr}(\hat{D}_{\Phi^+} \sigma_{C;0_X 0_Z}^Z) \\
 &= \frac{1}{8} \left(\frac{1}{4} q_{\Phi^+|\mathbb{1},\mathbb{1}} + \frac{1}{4} q_{\Phi^+|\mathbb{1},Z} + \frac{1}{4} \cos(\delta_1) q_{\Phi^+|X,\mathbb{1}} + \frac{1}{4} \cos(\delta_1) q_{\Phi^+|X,Z} \right), \quad (\text{C.18})
 \end{aligned}$$

$$\begin{aligned}
 Y_{\Phi^+;0_X 1_Z} &= \frac{1}{8} \text{Tr}(\hat{D}_{\Phi^+} \sigma_{C;0_X 1_Z}^Z) \\
 &= \frac{1}{8} \left(\frac{1}{4} q_{\Phi^+|\mathbb{1},\mathbb{1}} - \frac{1}{4} q_{\Phi^+|\mathbb{1},X} + \frac{1}{4} \cos(\delta_1) q_{\Phi^+|X,\mathbb{1}} + \frac{1}{4} \cos(\delta_1) q_{\Phi^+|X,X} \right), \quad (\text{C.19})
 \end{aligned}$$

$$\begin{aligned}
 Y_{\Phi^+;0_X 0_X} &= \frac{1}{8} \text{Tr}(\hat{D}_{\Phi^+} \sigma_{C;0_X 0_X}^Z) \\
 &= \frac{1}{8} \left(\frac{1}{4} q_{\Phi^+|\mathbb{1},\mathbb{1}} + \frac{1}{4} \cos(\delta_1) q_{\Phi^+|\mathbb{1},X} + \frac{1}{4} \cos(\delta_1) q_{\Phi^+|X,\mathbb{1}} + \frac{1}{4} \cos^2(\delta_1) q_{\Phi^+|X,X} \right), \quad (\text{C.20})
 \end{aligned}$$

$$\begin{aligned}
 Y_{\Phi^+;0_X 0_Y} &= \frac{1}{8} \text{Tr}(\hat{D}_{\Phi^+} \sigma_{C;0_X 0_Y}^Z) \\
 &= \frac{1}{8} \left(\frac{1}{4} q_{\Phi^+|\mathbb{1},\mathbb{1}} + \frac{1}{4} \sin(2\Theta) q_{\Phi^+|\mathbb{1},X} + \frac{1}{4} \cos(\delta_1) q_{\Phi^+|X,\mathbb{1}} + \frac{1}{4} \cos(\delta_1) \right. \\
 &\quad \left. \times \sin(2\Theta) q_{\Phi^+|X,X} \right), \quad (\text{C.21})
 \end{aligned}$$

$$\begin{aligned}
 Y_{\Phi^+;0_Y 0_Y} &= \frac{1}{8} \text{Tr}(\hat{D}_{\Phi^+} \sigma_{C;0_Y 0_Y}^Z) \\
 &= \frac{1}{8} \left(\frac{1}{4} q_{\Phi^+|\mathbb{1},\mathbb{1}} + \frac{1}{4} \sin(2\Theta) q_{\Phi^+|\mathbb{1},X} + \frac{1}{4} \sin(2\Theta) q_{\Phi^+|X,\mathbb{1}} + \right. \\
 &\quad \left. \frac{1}{4} \sin^2(2\Theta) q_{\Phi^+|X,X} \right), \tag{C.22}
 \end{aligned}$$

$$\begin{aligned}
 Y_{\Phi^+;0_Y 0_Z} &= \frac{1}{8} \text{Tr}(\hat{D}_{\Phi^+} \sigma_{C;0_Y 0_Z}^Z) \\
 &= \frac{1}{8} \left(\frac{1}{4} q_{\Phi^+|\mathbb{1},\mathbb{1}} + \frac{1}{4} q_{\Phi^+|\mathbb{1},Z} + \frac{1}{4} \sin(2\Theta) q_{\Phi^+|X,\mathbb{1}} + \frac{1}{4} \sin(2\Theta) q_{\Phi^+|X,Z} \right), \tag{C.23}
 \end{aligned}$$

$$\begin{aligned}
 Y_{\Phi^+;0_Y 1_Z} &= \frac{1}{8} \text{Tr}(\hat{D}_{\Phi^+} \sigma_{C;0_Y 1_Z}^Z) \\
 &= \frac{1}{8} \left(\frac{1}{2\sqrt{2}} q_{\Phi^+|\mathbb{1},\mathbb{1}} - \frac{1}{2\sqrt{2}} q_{\Phi^+|\mathbb{1},X} + \frac{1}{2\sqrt{2}} \sin(2\Theta) q_{\Phi^+|X,\mathbb{1}} \right. \\
 &\quad \left. - \frac{1}{2\sqrt{2}} \sin(2\Theta) q_{\Phi^+|X,X} \right), \tag{C.24}
 \end{aligned}$$

$$\begin{aligned}
 Y_{\Phi^+;0_Y 0_X} &= \frac{1}{8} \text{Tr}(\hat{D}_{\Phi^+} \sigma_{C;0_Y 0_X}^Z) \\
 &= \frac{1}{8} \left(\frac{1}{4} q_{\Phi^+|\mathbb{1},\mathbb{1}} + \frac{1}{4} \cos(\delta_1) q_{\Phi^+|\mathbb{1},X} + \frac{1}{4} \sin(2\Theta) q_{\Phi^+|X,\mathbb{1}} \right. \\
 &\quad \left. + \frac{1}{4} \cos(\delta_1) \sin(2\Theta) q_{\Phi^+|X,X} \right), \tag{C.25}
 \end{aligned}$$

$$\begin{aligned}
 Y_{\Phi^+;0_Z 0_X} &= \frac{1}{8} \text{Tr}(\hat{D}_{\Phi^+} \sigma_{C;0_Z 0_X}^Z) \\
 &= \frac{1}{8} \left(\frac{1}{4} q_{\Phi^+|\mathbb{1},\mathbb{1}} + \frac{1}{4} \cos(\delta_1) q_{\Phi^+|\mathbb{1},X} + \frac{1}{4} q_{\Phi^+|Z,\mathbb{1}} + \frac{1}{4} \cos(\delta_1) q_{\Phi^+|Z,X} \right), \tag{C.26}
 \end{aligned}$$

$$\begin{aligned}
 Y_{\Phi^+;0_Z 0_Y} &= \frac{1}{8} \text{Tr}(\hat{D}_{\Phi^+} \sigma_{C;0_Z 0_Y}^Z) \\
 &= \frac{1}{8} \left(\frac{1}{4} q_{\Phi^+|\mathbb{1},\mathbb{1}} + \frac{1}{4} \sin(2\Theta) q_{\Phi^+|\mathbb{1},X} + \frac{1}{4} q_{\Phi^+|Z,\mathbb{1}} + \frac{1}{4} \sin(2\Theta) q_{\Phi^+|Z,X} \right), \tag{C.27}
 \end{aligned}$$

$$\begin{aligned}
 Y_{\Phi^+;1_Z0_X} &= \frac{1}{8} \text{Tr}(\hat{D}_{\Phi^+} \sigma_{C;1_Z0_X}^Z) \\
 &= \frac{1}{8} \left(\frac{1}{4} q_{\Phi^+|\mathbb{1},\mathbb{1}} + \frac{1}{4} \cos(\delta_1) q_{\Phi^+|\mathbb{1},X} - \frac{1}{4} q_{\Phi^+|X,\mathbb{1}} - \frac{1}{4} \cos(\delta_1) q_{\Phi^+|X,X} \right), \quad (\text{C.28})
 \end{aligned}$$

$$\begin{aligned}
 Y_{\Phi^+;1_Z0_Y} &= \frac{1}{8} \text{Tr}(\hat{D}_{\Phi^+} \sigma_{C;1_Z0_Y}^Z) \\
 &= \frac{1}{8} \left(\frac{1}{4} q_{\Phi^+|\mathbb{1},\mathbb{1}} + \frac{1}{4} \sin(2\Theta) q_{\Phi^+|\mathbb{1},X} - \frac{1}{4} q_{\Phi^+|X,\mathbb{1}} - \frac{1}{4} \sin(2\Theta) q_{\Phi^+|X,X} \right). \quad (\text{C.29})
 \end{aligned}$$

Similar to the virtual protocol, the joint probabilities can be concisely written in terms of vector $\mathbf{q}$ and row vector $\mathbf{V}_{\Phi^+;\mathbf{j}\alpha\mathbf{k}\beta}$ corresponding to the coefficients of the transmission rate of Pauli operators as follows

$$Y_{\Phi^+;\mathbf{j}\alpha\mathbf{k}\beta} = \mathbf{V}_{\Phi^+;\mathbf{j}\alpha\mathbf{s}\beta} \mathbf{q}. \quad (\text{C.30})$$

Hence, the vector $\mathbf{Y}_{\Phi^+;\mathbf{j}\alpha\mathbf{k}\beta}$ can be represented as

$$\begin{aligned}
 \mathbf{Y}_{\Phi^+;\mathbf{j}\alpha\mathbf{k}\beta} &= [Y_{\Phi^+;0_Z0_Z}, Y_{\Phi^+;0_Z1_Z}, Y_{\Phi^+;1_Z0_Z}, Y_{\Phi^+;1_Z1_Z}, Y_{\Phi^+;0_X0_Z}, Y_{\Phi^+;0_X1_Z}, Y_{\Phi^+;0_X0_X}, \\
 &Y_{\Phi^+;0_X0_Y}, Y_{\Phi^+;0_Y0_Y}, Y_{\Phi^+;0_Y0_Z}, Y_{\Phi^+;0_Y1_Z}, Y_{\Phi^+;0_Y0_X}, Y_{\Phi^+;0_Z0_X}, Y_{\Phi^+;0_Z0_Y}, Y_{\Phi^+;1_Z0_X}, \\
 &Y_{\Phi^+;1_Z0_Y}]^T \quad (\text{C.31})
 \end{aligned}$$

and matrix $\mathbf{V}$ obtained from vectors $\mathbf{V}_{\Phi^+;\mathbf{j}\alpha\mathbf{k}\beta}$ is expressed as

$$\begin{aligned}
 \mathbf{V} &= [\mathbf{V}_{\Phi^+;0_Z0_Z}, \mathbf{V}_{\Phi^+;0_Z1_Z}, \mathbf{V}_{\Phi^+;1_Z0_Z}, \mathbf{V}_{\Phi^+;1_Z1_Z}, \mathbf{V}_{\Phi^+;0_X0_Z}, \mathbf{V}_{\Phi^+;0_X1_Z}, \mathbf{V}_{\Phi^+;0_X0_X}, \\
 &\mathbf{V}_{\Phi^+;0_X0_Y}, \mathbf{V}_{\Phi^+;0_Y0_Y}, \mathbf{V}_{\Phi^+;0_Y0_Z}, \mathbf{V}_{\Phi^+;0_Y1_Z}, \mathbf{V}_{\Phi^+;0_Y0_X}, \mathbf{V}_{\Phi^+;0_Z0_X}, \mathbf{V}_{\Phi^+;0_Z0_Y}, \\
 &\mathbf{V}_{\Phi^+;1_Z0_X}, \mathbf{V}_{\Phi^+;1_Z0_Y}]^T. \quad (\text{C.32})
 \end{aligned}$$

Finally, we obtain an expression for the joint probabilities,

$$\mathbf{Y}_{\Phi^+; \mathbf{j} \alpha \mathbf{k} \beta} = \mathbf{V} \mathbf{q}. \quad (\text{C.33})$$

The above result can be rewritten in terms of the transmission rate vector, $\mathbf{q}$ as follows

$$\mathbf{q} = \mathbf{V}^{-1} \mathbf{Y}_{\Phi^+; \mathbf{j} \alpha \mathbf{k} \beta}. \quad (\text{C.34})$$

Combining the above equation with Eq. (C.13) we can obtain the yield for virtual states from the transmission rate of actual states and thus deduce the error rate E_{XX} .

Security proof of the TF-QKD and the channel model

D.1 Security proof against coherent attacks

In this section, we provide security proof using a virtual protocol. The protocol generates measurement statistics that are the same as those obtained in the actual protocol. Moreover, the classical communication between Alice and Bob is precisely the same for actual and virtual protocols. Therefore, our security claim stems from the fact that the two protocols are indistinguishable from Eve’s viewpoint. The security proof of our protocol is based on the complementarity principle proposed by Koashi in [332, 333]. This technique exploits a virtual protocol that uses an observable, which is conjugate of the key generation basis. More precisely, in the actual protocol, Alice and Bob generate a key from measurements performed in the Z basis, whereas, in the virtual protocol, two parties prepare their signals in an eigenstate of the X basis. In doing so, the two parties can accurately estimate the phase error rate, which is the bit error rate that Alice and Bob would have observed if they had measured their Z basis state in the X basis. We have shown in Chapter 5

how to use the complementarity formalism to estimate this phase error rate. Here, we provide a more detailed description of the virtual protocol used for security proof and consider coherent attacks by Eve using Azuma's inequality [334]. Most importantly, we consider a general case where Alice and Bob prepare mixed states, which can be attributed to the inherent deficiencies in their sources of photons. Note that in the main text, we considered only the pure states for the simplicity of our analysis. The mixed states can be represented as

$$\hat{\rho}_{jZ} = P_{jZ}^0 |\phi_{jZ}^0\rangle\langle\phi_{jZ}^0| + P_{jZ}^1 |\phi_{jZ}^1\rangle\langle\phi_{jZ}^1|, \quad j \in \{0, 1\} \quad (\text{D.1})$$

$$\hat{\rho}_{0X} = P_{0X}^0 |\phi_{0X}^0\rangle\langle\phi_{0X}^0| + P_{0X}^1 |\phi_{0X}^1\rangle\langle\phi_{0X}^1|, \quad (\text{D.2})$$

$$\hat{\rho}_{0Y} = P_{0Y}^0 |\phi_{0Y}^0\rangle\langle\phi_{0Y}^0| + P_{0Y}^1 |\phi_{0Y}^1\rangle\langle\phi_{0Y}^1|, \quad (\text{D.3})$$

where P_{jZ}^0 , P_{jZ}^1 , P_{0X}^0 , P_{0X}^1 , P_{0Y}^0 and P_{0Y}^1 are the probabilities that satisfy $P_{jZ}^0 + P_{jZ}^1 = 1$, $P_{0X}^0 + P_{0X}^1 = 1$ and $P_{0Y}^0 + P_{0Y}^1 = 1$. These probabilities are given by

$$P_{j\beta}^i = \frac{1}{2} \left(1 - (-1)^i \sqrt{(\mathbf{n}_x^{j\beta})^2 + (\mathbf{n}_z^{j\beta})^2} \right). \quad (\text{D.4})$$

The states $\{|\phi_{jZ}^0\rangle, |\phi_{jZ}^1\rangle\}$, $\{|\phi_{0X}^0\rangle, |\phi_{0X}^1\rangle\}$ and $\{|\phi_{0Y}^0\rangle, |\phi_{0Y}^1\rangle\}$ form orthonormal bases. Also, the explicit form of these eigenstates is given by

$$|\phi_{j\beta}^i\rangle = \begin{cases} \frac{1}{N} \left(\frac{\mathbf{n}_z^{j\beta} - (-1)^i \sqrt{(\mathbf{n}_x^{j\beta})^2 + (\mathbf{n}_z^{j\beta})^2}}{\mathbf{n}_x^{j\beta}} |0_Z\rangle + |1_Z\rangle \right) & (\mathbf{n}_x^{j\beta} \neq 0) \\ |i_Z\rangle & (\mathbf{n}_x^{j\beta} = 0 \wedge \mathbf{n}_z^{j\beta} < 0) \\ |i \oplus 1_Z\rangle & (\mathbf{n}_x^{j\beta} = 0 \wedge \mathbf{n}_z^{j\beta} > 0) \end{cases} \quad (\text{D.5})$$

for $i, j \in \{0, 1\}$, $\beta \in \{X, Y, Z\}$ and N denoting the normalization factor while $\mathbf{n}_x^{j\beta}$ and $\mathbf{n}_z^{j\beta}$ represent the coefficients of Pauli operators σ_x and σ_z , respectively. In our security proof, we consider purifications of these mixed states, which is realized by

introducing Alice and Bob's ancilla systems. Thus, we get the following expressions

$$|\tilde{\psi}_{jZ}\rangle_{A_1C} = \sqrt{P_{jZ}^0}|0_Z\rangle_{A_1}|\phi_{jZ}^0\rangle_C + \sqrt{P_{jZ}^1}|1_Z\rangle_{A_1}|\phi_{jZ}^1\rangle_C, \quad (\text{D.6})$$

$$|\tilde{\psi}_{0X}\rangle_{A_1C} = \sqrt{P_{0X}^0}|0_X\rangle_{A_1}|\phi_{0X}^0\rangle_C + \sqrt{P_{0X}^1}|1_X\rangle_{A_1}|\phi_{0X}^1\rangle_C, \quad (\text{D.7})$$

$$|\tilde{\psi}_{0Y}\rangle_{A_1C} = \sqrt{P_{0Y}^0}|0_Y\rangle_{A_1}|\phi_{0Y}^0\rangle_C + \sqrt{P_{0Y}^1}|1_Y\rangle_{A_1}|\phi_{0Y}^1\rangle_C, \quad (\text{D.8})$$

where the index A_1 represents Alice's ancilla system that purifies the state and C corresponds to the system sent to Charlie. Similarly, for Bob, the purifications are given by

$$|\tilde{\psi}_{jZ}\rangle_{B_1C} = \sqrt{P_{jZ}^0}|0_Z\rangle_{B_1}|\phi_{jZ}^0\rangle_C + \sqrt{P_{jZ}^1}|1_Z\rangle_{B_1}|\phi_{jZ}^1\rangle_C, \quad (\text{D.9})$$

$$|\tilde{\psi}_{0X}\rangle_{B_1C} = \sqrt{P_{0X}^0}|0_X\rangle_{B_1}|\phi_{0X}^0\rangle_C + \sqrt{P_{0X}^1}|1_X\rangle_{B_1}|\phi_{0X}^1\rangle_C, \quad (\text{D.10})$$

$$|\tilde{\psi}_{0Y}\rangle_{B_1C} = \sqrt{P_{0Y}^0}|0_Y\rangle_{B_1}|\phi_{0Y}^0\rangle_C + \sqrt{P_{0Y}^1}|1_Y\rangle_{B_1}|\phi_{0Y}^1\rangle_C. \quad (\text{D.11})$$

To proceed with our analysis, we define the entangled states initially prepared by Alice and Bob by incorporating the purified states. For Alice, these states are expressed as

$$|\Psi_Z\rangle_{A_1A_2C} = \frac{1}{\sqrt{2}}(|0_Z\rangle_{A_2}|\tilde{\psi}_{0Z}\rangle_{A_1C} + |1_Z\rangle_{A_2}|\tilde{\psi}_{1Z}\rangle_{A_1C}), \quad (\text{D.12})$$

$$|\Psi_X\rangle_{A_1A_2C} = |0_X\rangle_{A_2}|\tilde{\psi}_{0X}\rangle_{A_1C}, \quad (\text{D.13})$$

$$|\Psi_Y\rangle_{A_1A_2C} = |0_Y\rangle_{A_2}|\tilde{\psi}_{0Y}\rangle_{A_1C}. \quad (\text{D.14})$$

Likewise, Bob prepares the states

$$|\Psi_Z\rangle_{B_1B_2C} = \frac{1}{\sqrt{2}}(|0_Z\rangle_{B_2}|\tilde{\psi}_{0Z}\rangle_{B_1C} + |1_Z\rangle_{B_2}|\tilde{\psi}_{1Z}\rangle_{B_1C}), \quad (\text{D.15})$$

$$|\Psi_X\rangle_{B_1B_2C} = |0_X\rangle_{B_2}|\tilde{\psi}_{0X}\rangle_{B_1C}, \quad (\text{D.16})$$

$$|\Psi_Y\rangle_{B_1B_2C} = |0_Y\rangle_{B_2}|\tilde{\psi}_{0Y}\rangle_{B_1C}, \quad (\text{D.17})$$

where A_2 and B_2 in the above equations represent the systems Alice and Bob used to generate key bits. Recall that in the virtual protocol, as explained in Chapter 5, Alice and Bob prepare the states in Eqs. (D.12) and (D.15) and measure their subsystems A_2 and B_2 in the X basis rather than Z basis. Therefore, to simplify our analysis we rewrite the state in Eq. (D.12) in the X basis form as

$$\begin{aligned} |\Psi_Z\rangle_{A_1 A_2 C} = & \sqrt{\frac{1 + \langle \tilde{\psi}_{0Z} | \tilde{\psi}_{1Z} \rangle_{A_1 C}}{2}} |0_X\rangle_{A_2} |\tilde{\psi}_{0X}^{\text{vir}}\rangle_{A_1 C} + \sqrt{\frac{1 - \langle \tilde{\psi}_{0Z} | \tilde{\psi}_{1Z} \rangle_{A_1 C}}{2}} |1_X\rangle_{A_2} \\ & \otimes |\tilde{\psi}_{1X}^{\text{vir}}\rangle_{A_1 C}, \end{aligned} \quad (\text{D.18})$$

with the normalized virtual states given by

$$|\tilde{\psi}_{jX}^{\text{vir}}\rangle_{A_1 C} = \frac{|\tilde{\psi}_{0Z}\rangle_{A_1 C} + (-1)^j |\tilde{\psi}_{1Z}\rangle_{A_1 C}}{\sqrt{2[1 + (-1)^j \langle \tilde{\psi}_{0Z} | \tilde{\psi}_{1Z} \rangle_{A_1 C}]}}. \quad (\text{D.19})$$

The same results are obtained for states prepared by Bob. In what follows, we present a virtual protocol that employs two virtual states, $|\tilde{\psi}_{jX}^{\text{vir}}\rangle_{A_1(B_1)C}$ and four actual states, $|\tilde{\psi}_{jZ}\rangle_{A_1(B_1)C}$, $|\tilde{\psi}_{0X}\rangle_{A_1(B_1)C}$, $|\tilde{\psi}_{0Y}\rangle_{A_1(B_1)C}$ that are sent by Alice (Bob) to Charlie. The preparation, selection, and measurement process of these states can be defined in a more compact form as

$$|\varphi\rangle_{sh_A A_1 C} = \sum_{c_A=1}^6 \sqrt{P(c_A)} |c_A\rangle_{sh_A} |\phi^c\rangle_{A_1 C} \quad (\text{D.20})$$

and

$$|\varphi\rangle_{sh_B B_1 C} = \sum_{c_B=1}^6 \sqrt{P(c_B)} |c_B\rangle_{sh_B} |\phi^c\rangle_{B_1 C}, \quad (\text{D.21})$$

for Alice and Bob, respectively. Here the shield systems sh_A and sh_B remain with

Alice and Bob. The states $|\phi^c\rangle_{A_1(B_1)C}$ prepared by Alice (Bob) correspond to

$$|\phi^1\rangle_{A_1(B_1)C} = |\tilde{\psi}_{0X}^{\text{vir}}\rangle_{A_1(B_1)C} \quad (\text{D.22})$$

$$|\phi^2\rangle_{A_1(B_1)C} = |\tilde{\psi}_{1X}^{\text{vir}}\rangle_{A_1(B_1)C} \quad (\text{D.23})$$

$$|\phi^3\rangle_{A_1(B_1)C} = |\tilde{\psi}_{0Z}\rangle_{A_1(B_1)C} \quad (\text{D.24})$$

$$|\phi^4\rangle_{A_1(B_1)C} = |\tilde{\psi}_{1Z}\rangle_{A_1(B_1)C} \quad (\text{D.25})$$

$$|\phi^5\rangle_{A_1(B_1)C} = |\tilde{\psi}_{0X}\rangle_{A_1(B_1)C} \quad (\text{D.26})$$

$$|\phi^6\rangle_{A_1(B_1)C} = |\tilde{\psi}_{0Y}\rangle_{A_1(B_1)C}, \quad (\text{D.27})$$

with probabilities given by

$$P(1) = P_Z(1 + \langle \tilde{\psi}_{0Z} | \tilde{\psi}_{1Z} \rangle_{A_1(B_1)C}) \quad (\text{D.28})$$

$$P(1) = P_Z(1 - \langle \tilde{\psi}_{0Z} | \tilde{\psi}_{1Z} \rangle_{A_1(B_1)C}) \quad (\text{D.29})$$

$$P(3) = P(4) = P_Z \quad (\text{D.30})$$

$$P(5) = P_X \quad (\text{D.31})$$

$$P(6) = P_Y. \quad (\text{D.32})$$

We now present comprehensive steps of a virtual protocol as follows.

Virtual protocol

Before starting the protocol, Alice and Bob set a fixed number of rounds (say N trials) needed to complete key generation.

1. Preparation

Alice and Bob prepare the states $|\varphi\rangle_{sh_A A_1 C}$ and $|\varphi\rangle_{sh_B B_1 C}$ defined in Eqs. (D.20) and (D.21), respectively, and send the systems C to Charlie through a quantum channel. They delay their measurements until the announcement

by Charlie.

2. *Detection announcement*

Charlie performs single-photon interference followed by threshold detection in two detectors and announces successful detection results.

3. *Measurement and classical communication*

Steps 1-2 are repeated until N trials agreed on by the two parties are completed. After that, for the case where Charlie declares detection results from $|\Phi^+\rangle$, Alice and Bob measure their shield systems $|c_A\rangle, |c_B\rangle$ and announce Z (X, Y) basis choice when the results of their measurements are $c = 1, 2, 3, 4$ ($c = 5, 6$). This ensures that classical information in the actual protocol is identical to the virtual protocol.

4. *Estimation of the number of phase errors*

Alice and Bob use the events $c = 3, 4, 5, 6$, corresponding to actual states to estimate the number of phase errors.

The virtual protocol described above is equivalent to the actual protocol because quantum states sent by Alice and Bob in the two protocols are the same, and classical communication by the two parties is precisely identical. To elucidate this argument, when Alice and Bob prepare the virtual states ($c = 1, 2$), they measure their subsystems in the X basis and announce the Z basis instead. The announcement is made in this manner to make the virtual protocol indistinguishable from the actual protocol in which the events ($c = 1, 2$) are used for key generation, i.e., In these events, Alice and Bob measure their systems in the Z basis and also declares the same basis. Such being the case, both protocols are equivalent from Eve's viewpoint.

Now, we present a method used to estimate observed phase errors in N measurements performed by Alice and Bob in their systems c_A and c_B and consider

coherent attacks where Eve interacts with all signals sent by the two parties and executes a joint measurement after classical communication is completed. For this kind of attack, it suffices to use Azuma's inequality [334], which considers any random variables, including correlated ones, provided that a Martingale and Bounded difference condition (BDC) are satisfied. Azuma's inequality is described as follows.

A sequence of random variables $X^{(0)}, X^{(1)}, \dots$ is called Martingale if and only if $E[X^{(m+1)} | X^{(0)}, X^{(1)}, \dots, X^{(m)}] = X^{(m)} \forall m \geq 0$ with $E[\cdot]$ denoting the expectation value. In addition, $X^{(0)}, X^{(1)}, \dots$ is considered to satisfy BDC if there exists $c^{(m)} > 0$ such that $|X^{(m+1)} - X^{(m)}| \leq c^{(m)} \forall m \geq 0$. Consider a case of N trials described by random variable $X^{(m)}$, where m corresponds to the m^{th} trial. If $X^{(m)}$ is a Martingale and fulfils the BDC with $c^{(m)} = 1$ then Azuma's inequality asserts that

$$\Pr[|X^{(N)} - X^{(0)}| > N\delta] \leq 2e^{-\frac{N\delta^2}{2}} \quad (\text{D.33})$$

for any $\delta \in (0, 1)$. For m^{th} trial the random variable $X^{(m)}$ is defined as

$$X^{(m)} := \Lambda^{(m)} - \sum_{j=1}^m P(\xi_j = 1 | \xi_0, \dots, \xi_{j-1}), \quad (\text{D.34})$$

where $\Lambda^{(m)}$ is a random variable that corresponds to the actual number of events ($\Lambda^{(m)} = \sum_{j=1}^m \xi_j$) observed in the first m trials and ξ_j is a Bernoulli random variable. Furthermore, $P(\xi_j = 1 | \xi_0, \dots, \xi_{j-1})$ is probability of having event $\xi_j = 1$ in the j^{th} run conditioned on the first $j - 1$ outcomes, $\xi_0, \dots, \xi_{j-1}$. It can be easily shown that the random variables in Eq. (D.34) are Martingale and fulfill BDC. Thus, by applying Azuma's inequality, we obtain

$$\Pr[|\Lambda^{(N)} - \sum_{j=1}^N P(\xi_j = 1 | \xi_0, \dots, \xi_{j-1})| > N\delta] \leq 2e^{-\frac{N\delta^2}{2}} \quad (\text{D.35})$$

where $X^{(0)} = 0$. This essentially implies that

$$\sum_{j=1}^N P(\xi_j = 1 | \xi_0, \dots, \xi_{j-1}) - N\delta \leq \Lambda^{(N)} \leq P(\xi_j = 1 | \xi_0, \dots, \xi_{j-1}) + N\delta \quad (\text{D.36})$$

holds at least with probability $P = 1 - 2e^{-\frac{N\delta^2}{2}}$. Hence,

$$\Lambda^{(N)} = \sum_{j=1}^N P(\xi_j = 1 | \xi_0, \dots, \xi_{j-1}) + \delta_A \quad (\text{D.37})$$

except with error probability $\varepsilon_A + \hat{\varepsilon}_A$ where parameter δ_A is bounded by an interval $\delta_A \in [-\Delta_A, \hat{\Delta}_A]$ with $\Delta_A = f_A(N, \varepsilon_A)$, and where $f_A(x, y) = \sqrt{2x \ln \frac{1}{y}}$.

Now, applying Azuma's inequality to our scenario, from the N trials by Alice and Bob in the virtual protocol, if we consider the j^{th} run of the protocol and once we obtain the probability for measuring systems c_A and c_B for that particular run conditioned on previous measurement outcomes, then we can find the actual number of events observed. Precisely, for random variables $X_{c_A c_B}^l$ with $l = 1, \dots, N$ Azuma's inequality states that

$$X_{c_A c_B}^l = \Lambda_{c_A c_B}^l - \sum_{j=1}^l P_{c_A c_B}(\xi_j | \xi_0, \dots, \xi_{j-1}), \quad (\text{D.38})$$

where $\Lambda_{c_A c_B}^l$ is a random variable that corresponds to the actual number of events during l trials ($l = 1, \dots, N$). Moreover, $P_{c_A c_B}(\xi_j | \xi_0, \dots, \xi_{j-1})$ is the probability of Alice and Bob obtaining the values c_A and c_B in their measurements performed in the j^{th} , conditioned on the previous $j-1$ measurement outcomes, $\xi_j | \xi_0, \dots, \xi_{j-1}$. To determine this conditional probability in the j^{th} run, we use the joint state prepared

by Alice and Bob for N trials

$$\begin{aligned}
|\Phi\rangle_{sh_A A_1 C_A sh_B B_1 C_B} &= |\varphi\rangle_{sh_A A_1 C_A} \otimes |\varphi\rangle_{sh_B B_1 C_B} \\
&= |\phi_{j-1}\rangle_{sh_A A_1 C_A} |\phi_j\rangle_{sh_A A_1 C_A} |\phi_{N-j}\rangle_{sh_A A_1 C_A} \\
&\quad \otimes |\phi_{j-1}\rangle_{sh_B B_1 C_B} |\phi_j\rangle_{sh_B B_1 C_B} |\phi_{N-j}\rangle_{sh_B B_1 C_B}
\end{aligned} \tag{D.39}$$

where $|\phi_{j-1}\rangle_{sh_{A(B)} A(B)_1 C_{A(B)}}$, $|\phi_j\rangle_{sh_{A(B)} A(B)_1 C_{A(B)}}$ and $|\phi_{N-j}\rangle_{sh_{A(B)} A(B)_1 C_{A(B)}}$ represent states prepared by Alice (Bob) in the first $j-1$ runs, j^{th} run and the remaining $N-j$ runs, respectively.

Let us define the evolution of the joint state after Eve's action by

$$\mathcal{U}_{\mathbf{C}E} |\Phi\rangle_{sh_A A_1 sh_B B_1 \mathbf{C}} |0\rangle_E = \sum_t \hat{C}_{t,\mathbf{C}} |\Phi\rangle_{sh_A A_1 sh_B B_1 \mathbf{C}} |t\rangle_E, \tag{D.40}$$

where $\mathcal{U}_{\mathbf{C}E}$ is Eve's unitary transformation on $\mathbf{C}E$ and $\hat{C}_{t,\mathbf{C}}$ corresponds to the Kraus operator which acts on system $\mathbf{C}$ according to Eve's measurement results on her ancilla. Here, we denote Charlie's system with index $\mathbf{C}$, which essentially corresponds to a joint system constituted by subsystems C_A and C_B received from Alice and Bob, respectively. Now, taking into consideration measurement outcomes prior to the j^{th} run, we define the joint measurement operator for the $j-1$ systems as

$$\hat{O}_{j-1, sh_A sh_B \mathbf{C}} = \otimes_{i=1}^{j-1} \hat{M}_{sh_A^i sh_B^i \mathbf{C}_i} \tag{D.41}$$

where $\hat{M}_{sh_A^i sh_B^i \mathbf{C}_i}$ represents the Kraus operator associated with i^{th} measurement outcome of Alice and Bob's systems sh_A , sh_B and Charlie's system $\mathbf{C}$. From this joint measurement operation on $j-1$ systems, we define the measurement outcomes of $j-1$ runs as O_{j-1} . After Eve's interaction, the joint state of the j^{th} run conditioned on the measurement results of the first $j-1$ runs can be expressed

as

$$\hat{\rho}_{j|O_{j-1}}^{sh_A sh_B \mathbf{C}} = \frac{\sigma_{j|O_{j-1}}^{sh_A sh_B \mathbf{C}}}{\text{Tr}(\sigma_{j|O_{j-1}}^{sh_A sh_B \mathbf{C}})} \quad (\text{D.42})$$

where the state $\sigma_{j|O_{j-1}}^{sh_A sh_B \mathbf{C}}$ is defined as

$$\sigma_{j|O_{j-1}}^{sh_A sh_B \mathbf{C}} = \sum_t \text{Tr}_{\bar{j}}(\hat{P}[\hat{\mathcal{O}}_{j-1, sh_A sh_B \mathbf{C}} \hat{C}_{t, \mathbf{C}} |\Phi\rangle_{sh_A A_1 sh_B B_1 \mathbf{C}}]). \quad (\text{D.43})$$

Here Tr is the trace over all systems sh_A , sh_B , A_1 , B_1 and $\mathbf{C}$ for all events except for the j^{th} run. This precisely means taking trace with basis $\{|\vec{x}_{j-1}\rangle, |\vec{x}_{N-j}\rangle\}$ where $|\vec{x}_{j-1}\rangle$ and $|\vec{x}_{N-j}\rangle$ correspond to systems in the first $j-1$ runs and remaining $N-j$ runs, respectively. Then Eq. (D.43) can be equivalently rewritten as

$$\sigma_{j|O_{j-1}}^{sh_A sh_B \mathbf{C}} = \sum_t \sum_{\vec{x}_{j-1}, \vec{x}_{N-j}} \text{Tr}_{A_1 B_1}^j(\hat{P}[\hat{A}_{t, \mathbf{C}|O_{j-1}}^{(\vec{x}_{j-1}, \vec{x}_{N-j})} |\phi_j\rangle_{sh_A A_1 sh_B B_1 \mathbf{C}}]) \quad (\text{D.44})$$

where $\text{Tr}_{A_1 B_1}^j$ denotes trace over A_1 and B_1 in the j^{th} run and $\hat{A}_{t, \mathbf{C}|O_{j-1}}^{(\vec{x}_{j-1}, \vec{x}_{N-j})}$ is the Kraus operator acting on the j^{th} system conditioned on the previous measurement outcomes O_{j-1} , and it is given by

$$\hat{A}_{t, \mathbf{C}|O_{j-1}}^{(\vec{x}_{j-1}, \vec{x}_{N-j})} = \langle \vec{x}_{N-j} | \langle \vec{x}_{j-1} | \hat{\mathcal{O}}_{j-1, sh_A sh_B \mathbf{C}} \hat{C}_{t, \mathbf{C}} | \phi_{j-1} \rangle_{sh_A A_1 sh_B B_1 \mathbf{C}} | \phi_{N-j} \rangle_{sh_A A_1 sh_B B_1 \mathbf{C}}. \quad (\text{D.45})$$

By substituting Eq. (D.20) and (D.21) into Eq. (D.44) we obtain

$$\begin{aligned} \sigma_{j|O_{j-1}}^{sh_A sh_B \mathbf{C}} &= \sum_{c_A, c_B, c_A^*, c_B^*} \sqrt{P(c_A)P(c_B)P(c_A^*)P(c_B^*)} \sum_t \sum_{\vec{x}_{j-1}, \vec{x}_{N-j}} \text{Tr}_{A_1 B_1}^j(\hat{P}[\hat{A}_{t, \mathbf{C}|O_{j-1}}^{(\vec{x}_{j-1}, \vec{x}_{N-j})} \\ &\quad |c_A\rangle_{sh_A} \otimes |c_B\rangle_{sh_B} (|\phi^{(c)}\rangle_{A_1} \otimes |\phi^{(c)}\rangle_{B_1} \mathbf{C}]). \end{aligned} \quad (\text{D.46})$$

Now the probability that Alice and Bob obtains outcomes c_A and c_B , and Charlie announces detection result $|\Phi^+\rangle$ after measuring his system $\mathbf{C}$ conditioned on the

first $j - 1$ measurement outcomes is given by

$$\begin{aligned}
Y_{\Phi^+ c_A c_B | O_{j-1}} &= \frac{P(c_A)P(c_B)}{\text{Tr}(\sigma_{j|O_{j-1}}^{sh_A sh_B \mathbf{C}})} \sum_t \sum_{\vec{x}_{j-1}, \vec{x}_{N-j}} \text{Tr}(\hat{P}[\hat{A}_{t, \mathbf{C} | O_{j-1}}^{(\vec{x}_{j-1}, \vec{x}_{N-j})} \text{Tr}_{A_1 B_1}(|\phi^{(c)}\rangle_{A_1} \\
&\quad \otimes |\phi^{(c)}\rangle_{B_1}) \mathbf{C} \hat{M}_{\Phi^+}]) \\
&= \frac{P(c_A)P(c_B)}{\text{Tr}(\sigma_{j|O_{j-1}}^{sh_A sh_B \mathbf{C}})} \text{Tr}(\hat{D}_{\Phi^+ | O_{j-1}} \hat{P}[\text{Tr}_{A_1 B_1}(|\phi^{(c)}\rangle_{A_1} \otimes |\phi^{(c)}\rangle_{B_1}) \mathbf{C}]) \quad (\text{D.47})
\end{aligned}$$

where $\hat{D}_{\Phi^+ | O_{j-1}} = \hat{A}_{t, \mathbf{C} | O_{j-1}}^{(\vec{x}_{j-1}, \vec{x}_{N-j})} \hat{M}_{\Phi^+} \hat{A}_{t, \mathbf{C} | O_{j-1}}^{(\vec{x}_{j-1}, \vec{x}_{N-j})\dagger}$ and $\hat{M}_{\Phi^+}$ represent Charlie's measurement operation.

Note that for $c_A(c_B) = 3, 4, 5, 6$ the probability $Y_{\Phi^+ c_A c_B | O_{j-1}}$ corresponds to the actual yields $Y_{\phi^+ j \alpha s \beta}$ ($\alpha, \beta \in \{X, Y, Z\}$, $s, j \in \{0, 1\}$) described in Chapter 5. From experimental results we know the actual events $\Lambda_{c_A c_B}$ (for different combinations $c_A(c_B) \in \{3, 4, 5, 6\}$). Thus, using Eq. (D.37) of Azuma's inequality, we can calculate the conditional probabilities that correspond to the yields $Y_{\phi^+ j \alpha s \beta}$. We have shown in the Chapter 5 and C.1 that we can determine the transmission rate of operators from the actual yields and, in turn, determine the yields of virtual states $Y_{\Phi^+ j X s X}^{\text{Zvir}}$ from those transmission rates. These virtual yields corresponds to the conditional probabilities $Y_{\Phi^+ c_A c_B | O_{j-1}}$ for $c_A(c_B) = 1, 2$. Again, we employ Azuma's inequality to determine the actual number of events $\Lambda_{c_A c_B}$ where $c_A(c_B) = 1, 2$, which represent the number of phase errors.

D.2 Channel model

Here, we introduce a channel model to simulate the quantities observed in an actual experiment. We consider a symmetric lossy channel that links Alice and Bob through Charlie with transmittance η . We assume that the dark count rate, p_d , is measured from the transmission of optical pulses.

D.2.1 Estimation of gain and error rate from Z basis

In the Z basis, states sent by Alice and Bob are in four possible combinations; $|0\rangle_A \otimes |0\rangle_B$, $|\sqrt{\mu}e^{i\chi_a}\rangle_A \otimes |0\rangle_B$, $|0\rangle_A \otimes |\sqrt{\mu}e^{i\chi_b}\rangle_B$ and $|\sqrt{\mu}e^{i\chi_a}\rangle_A \otimes |\sqrt{\mu}e^{i\chi_b}\rangle_B$ where $|0\rangle$ represents the vacuum state (when intensity 0 is selected). After going through the beam-splitter, the resultant states are

$$\begin{aligned}
& |0\rangle_A |0\rangle_B \xrightarrow{BS} |0\rangle_L |0\rangle_R \\
& |0\rangle_A |\sqrt{\mu}e^{i\chi_b}\rangle_B \xrightarrow{BS} \left| e^{i\chi_b} \sqrt{\frac{\mu\eta}{2}} \right\rangle_L \left| -e^{i\chi_b} \sqrt{\frac{\mu\eta}{2}} \right\rangle_R \\
& |\sqrt{\mu}e^{i\chi_a}\rangle_A |0\rangle_B \xrightarrow{BS} \left| e^{i\chi_a} \sqrt{\frac{\mu\eta}{2}} \right\rangle_L \left| e^{i\chi_a} \sqrt{\frac{\mu\eta}{2}} \right\rangle_R \\
& |\sqrt{\mu}e^{i\chi_a}\rangle_A |\sqrt{\mu}e^{i\chi_b}\rangle_B \xrightarrow{BS} \left| e^{i\chi_a} \sqrt{\frac{\mu\eta}{2}} + e^{i\chi_b} \sqrt{\frac{\mu\eta}{2}} \right\rangle_L \left| e^{i\chi_a} \sqrt{\frac{\mu\eta}{2}} - e^{i\chi_b} \sqrt{\frac{\mu\eta}{2}} \right\rangle_R. \quad (D.48)
\end{aligned}$$

The detection probabilities are given by

$$\begin{aligned}
p_0 &= 1 - \eta \\
p_L &= \eta \cos^2 \left(\frac{\chi}{2} \right) \\
p_R &= \eta \sin^2 \left(\frac{\chi}{2} \right), \quad (D.49)
\end{aligned}$$

where p_0 , p_L , and p_R denote the probabilities for no click, click in L-detector and click in R-detector, respectively. Taking into consideration the effects caused by dark counts p_d , we have that

$$P_0 = (1 - p_d)^2 (1 - \eta)^2, \quad (D.50)$$

$$\begin{aligned}
P_L &= (1 - p_d)^2 \exp \left(-\mu\eta \cos^2 \left(\frac{\chi}{2} \right) \right) + p_d(1 - p_d) \left[(1 - \eta) \exp \left(-\mu\eta \cos^2 \left(\frac{\chi}{2} \right) \right) \right] \\
&= p_d(1 - p_d)(1 - \eta) + (1 - p_d) \exp \left(-\mu\eta \cos^2 \left(\frac{\chi}{2} \right) \right), \quad (D.51)
\end{aligned}$$

$$\begin{aligned}
P_R &= (1 - p_d)^2 \exp\left(-\mu\eta \sin^2\left(\frac{\chi}{2}\right)\right) + p_d(1 - p_d) \left[(1 - \eta) \exp\left(-\mu\eta \sin^2\left(\frac{\chi}{2}\right)\right)\right] \\
&= p_d(1 - p_d)(1 - \eta) + (1 - p_d) \exp\left(-\mu\eta \sin^2\left(\frac{\chi}{2}\right)\right), \tag{D.52}
\end{aligned}$$

$$\begin{aligned}
P_{LR} &= 1 - P_0 - P_L - P_R \\
&= (1 - p_d)^2 [1 + (1 - \eta) - [(1 - \eta) + \exp(-\mu\eta \cos^2(\frac{\chi}{2}))] - [(1 - \eta) \\
&\quad + \exp(-\mu\eta \sin^2(\frac{\chi}{2}))]] + p_d(1 - p_d) [\exp(-\mu\eta \cos^2(\frac{\chi}{2})) + \exp(-\mu\eta \sin^2(\frac{\chi}{2}))] \\
&\quad + p_d^2 \\
&= (1 - p_d)^2 [1 + (1 - \eta)e^{-\mu\eta}] + p_d(1 - p_d)e^{-\mu\eta} + p_d^2 \tag{D.53}
\end{aligned}$$

where P_0 , P_{LR} , P_L and P_R correspond to the probabilities that n -photon coherent states from Alice and Bob results in no click in both detectors, click in both detectors, click in L-detector only and click in R-detector only, respectively. The gain Q_μ^Z is therefore estimated from detection probabilities as

$$\begin{aligned}
Q_\mu^Z &= P_0 + P_L + P_R + P_{LR} \\
&= (1 - p_d)^2 (1 - \eta)^2 + p_d(1 - p_d)(1 - \eta) + (1 - p_d) \exp\left(-\mu\eta \cos^2\left(\frac{\chi}{2}\right)\right) \\
&\quad + p_d(1 - p_d)(1 - \eta) + (1 - p_d) \exp\left(-\mu\eta \sin^2\left(\frac{\chi}{2}\right)\right) \\
&\quad + (1 - p_d)^2 [1 + (1 - \eta)e^{-\mu\eta}] + p_d(1 - p_d)e^{-\mu\eta} + p_d^2 \\
&\approx (1 - p_d)^2 (1 - \eta)e^{-\mu\eta} + 1 + (1 - \eta) - 2(1 - p_d)^2 (1 - \eta)e^{-\mu\eta} \\
&\approx (1 - p_d)^2 (1 - \eta)e^{-\mu\eta} + 1 - (1 - 2p_d)(1 - \eta)e^{-\mu\eta} \tag{D.54}
\end{aligned}$$

The quantum bit error rate E_μ^Z is estimated as

$$\begin{aligned}
 E_\mu^Z &= \frac{P_0^n + P_{LR}}{P_0 + P_L + P_R + P_{LR}} \\
 &= \frac{1}{Q_\mu} (1 - p_d)^2 (1 - \eta)^2 + (1 - p_d)^2 [1 + (1 - \eta)e^{-\mu\eta}] + p_d(1 - p_d)e^{-\mu\eta} + p_d^2
 \end{aligned} \tag{D.55}$$

D.2.2 Estimation of gain in the X and Y bases

We adopt the channel model developed in Ref. [296] to estimate the gain used for simulation for the states prepared in the complementary bases. For simplicity, we study the case where Alice and Bob select the same state and same phase slices according to the phase post-selection method ($j_a = j_b$). The states sent by Alice and Bob are $|\sqrt{\mu_a}e^{i\chi_a}\rangle$ and $|\sqrt{\mu_b}e^{i\chi_b}\rangle$, respectively where $\mu_a = \mu_b = \mu/2$. Due to channel losses and detection inefficiencies, the states transform into $|\sqrt{\eta\mu_a}e^{i\chi_a}\rangle$ and $|\sqrt{\eta\mu_b}e^{i\chi_b}\rangle$. After going through the beam-splitter, the resultant states are

$$|\alpha_L\rangle = \left| \frac{\sqrt{\eta\mu}}{2} (e^{i\chi_a} + e^{i\chi_b}) \right\rangle = \left| \frac{\sqrt{\eta\mu}}{2} e^{i\chi_a} (1 + e^{i\chi_\omega}) \right\rangle, \tag{D.56}$$

$$|\alpha_R\rangle = \left| \frac{\sqrt{\eta\mu}}{2} (e^{i\chi_a} - e^{i\chi_b}) \right\rangle = \left| \frac{\sqrt{\eta\mu}}{2} e^{i\chi_a} (1 - e^{i\chi_\omega}) \right\rangle, \tag{D.57}$$

where χ_ω is the fixed phase difference between the global phases χ_a and χ_b . The detection probabilities are

$$\begin{aligned}
 P_\mu(\bar{L}) &= (1 - p_d) \exp(-|\alpha_L|^2) \\
 &= (1 - p_d) \exp(-\eta\mu \cos^2(\frac{\chi_\omega}{2})),
 \end{aligned} \tag{D.58}$$

$$P_\mu(L) = 1 - P_\mu(\bar{L}), \quad (\text{D.59})$$

$$\begin{aligned} P_\mu(\bar{R}) &= (1 - p_d) \exp(-|\alpha_R|^2) \\ &= (1 - p_d) \exp(-\eta\mu \sin^2(\frac{\chi_\omega}{2})), \end{aligned} \quad (\text{D.60})$$

$$P_\mu(R) = 1 - P_\mu(\bar{R}), \quad (\text{D.61})$$

where $P_\mu(L)$ and $P_\mu(\bar{L})$ are the probabilities of L click and no click events, respectively, and $P_\mu(R)$ and $P_\mu(\bar{R})$ are defined similarly for R -detector. The total gain is approximated as

$$\begin{aligned} Q_\mu &= P(L)P(\bar{R}) + P(\bar{L})P(R) \\ &= (1 - p_d) \exp(-\eta\mu \sin^2(\frac{\chi_\omega}{2})) [1 - (1 - p_d) \exp(-\eta\mu \cos^2(\frac{\chi_\omega}{2}))] \\ &\quad + (1 - p_d) \exp(-\eta\mu \cos^2(\frac{\chi_\omega}{2})) [1 - (1 - p_d) \exp(-\eta\mu \sin^2(\frac{\chi_\omega}{2}))] \\ &\approx (1 - p_d) [1 - (1 - p_d) \exp(-\eta\mu_b)] + p_d (1 - p_d) \exp(-\eta\mu_b) \\ &= (1 - p_d) [1 - (1 - 2p_d) e^{-\eta\mu}] \\ &\approx 1 - e^{-\eta\mu} + 2p_d e^{-\eta\mu}. \end{aligned} \quad (\text{D.62})$$

Estimation of key rate parameters and derivation of key rate formula for the MDI-QKD based on biphotons

E.1 Estimation of key rate parameters

We evaluate gains and quantum bit error rates by considering the conditional probabilities for the coincidence detection of n -photon pairs in the Brown Twiss scheme. In terms of the basis state $|\alpha\rangle$, the yield is given by

$$Y_{n,n}^{\alpha} = [1 - (1 - Y_{0D_{H1A}})(1 - \eta_{D_{H1A}}t)^n][1 - (1 - Y_{0D_{H1B}})(1 - \eta_{D_{H1B}}t)^n] \\ \times [1 - (1 - Y_{0D_{H2A}})(1 - \eta_{D_{H2A}}t)^n][1 - (1 - Y_{0D_{H2B}})(1 - \eta_{D_{H2B}}t)^n], \quad (\text{E.1})$$

where Y_0 is the background count rate, D_{H1A} , D_{H1B} , D_{H2A} and D_{H2B} correspond to detectors for measuring horizontally polarized states in the Brown Twiss scheme. The terms t and η represent channel transmittance and detection efficiencies. The

yield for photon pairs that correspond to state $|\beta\rangle$ is given by

$$Y_{n,n}^\beta = [1 - (1 - Y_{0D_{H3A}})(1 - \eta_{D_{H3A}}t)^n][1 - (1 - Y_{0D_{H3B}})(1 - \eta_{D_{H3B}}t)^n] \\ \times [1 - (1 - Y_{0D_{V4A}})(1 - \eta_{D_{V4A}}t)^n][1 - (1 - Y_{0D_{V4B}})(1 - \eta_{D_{V4B}}t)^n], \quad (\text{E.2})$$

where D_{H3A} , D_{H3B} , D_{V4A} , and D_{V4B} correspond to detectors for measuring horizontal and vertical polarized states, respectively, in the Brown Twiss scheme. Similarly, the detection probability for the n -photon pair corresponding to $|\gamma\rangle$ is

$$Y_{n,n}^\gamma = [1 - (1 - Y_{0D_{V5A}})(1 - \eta_{D_{V5A}}t)^n][1 - (1 - Y_{0D_{V5B}})(1 - \eta_{D_{V5B}}t)^n] \\ \times [1 - (1 - Y_{0D_{V6A}})(1 - \eta_{D_{V6A}}t)^n][1 - (1 - Y_{0D_{V6B}})(1 - \eta_{D_{V6B}}t)^n], \quad (\text{E.3})$$

D_{V5A} , D_{V5B} , D_{V6A} , and D_{V6B} correspond to detectors for measuring vertically polarized states in the Brown Twiss scheme. Therefore, the overall yield is given by

$$Y_{n,n} = Y_{n,n}^\alpha Y_{n,n}^\beta Y_{n,n}^\gamma. \quad (\text{E.4})$$

From these results, the gain for states prepared from a key basis comprising of n -photon pairs is given by

$$Q_{\mu_a\mu_b, \mathcal{M}_1}^{n,n} = Y_{n,n} P(n_a) P(n_b), \quad (\text{E.5})$$

where $P(n_a)$ and $P(n_b)$ denotes the probabilities for Alice and Bob's SPDC sources to emit n_a -photon and n_b -photon pairs. This probability is expressed as

$$P(n) = \frac{(n+1)\left(\frac{\mu}{2}\right)^n}{\left(1 + \frac{\mu}{2}\right)^{n+2}}. \quad (\text{E.6})$$

The gain corresponding to single-photon contributions is then given by

$$Q_{\mu_a\mu_b,\mathcal{M}_1}^{1,1} = \frac{4Y_{1,1}\mu_a\mu_b}{(2 + \mu_a + \mu_b)^3}. \quad (\text{E.7})$$

In addition, we have the overall gain expressed as

$$Q_{\mu_a\mu_b,\mathcal{M}_1} = \sum_n^{\infty} Q_{\mu_a\mu_b,\mathcal{M}_1}^{n,n}, \quad (\text{E.8})$$

and the QBER, $E_{\mu_a\mu_b,\mathcal{M}_1}$ is expressed as

$$E_{\mu_a\mu_b,\mathcal{M}_1} Q_{\mu_a\mu_b,\mathcal{M}_1} = \sum_{n=0}^{\infty} e_{n,n} Q_{\mu_a\mu_b,\mathcal{M}_1}^{n,n}, \quad (\text{E.9})$$

where the error rate of the n -photon pairs from Alice and Bob, $e_{n,n}$ is expressed as

$$e_{n,n} = e_{n,n}^{\alpha} + e_{n,n}^{\beta} + e_{n,n}^{\gamma}. \quad (\text{E.10})$$

The error rate for the n -photon pair corresponding to the state $|\alpha\rangle$ given by

$$\begin{aligned} e_{n,n}^{\alpha} = & [e_0(Y_{0D_{H1A}}Y_{0D_{H1B}} + Y_{0D_{H1A}}\eta_{D_{H1B}} + Y_{0D_{H1B}}\eta_{D_{H1A}} + Y_{0D_{H2A}}Y_{0D_{H2B}} \\ & + Y_{0D_{H2A}}\eta_{D_{H2B}} + Y_{0D_{H2B}}\eta_{D_{H2A}}) + e_d(\eta_{D_{H1A}}\eta_{D_{H1B}} + \eta_{D_{H2A}}\eta_{D_{H2B}})] \div Y_{n,n}^{\alpha} \end{aligned} \quad (\text{E.11})$$

The error rates e_n^{β} and e_n^{γ} associated with the detection of states $|\beta\rangle$ and $|\gamma\rangle$, respectively are analogously obtained as

$$\begin{aligned} e_{n,n}^{\beta} = & [e_0(Y_{0D_{H3A}}Y_{0D_{H3B}} + Y_{0D_{H3A}}\eta_{D_{H3B}} + Y_{0D_{H3B}}\eta_{D_{H3A}} + Y_{0D_{V4A}}Y_{0D_{V4B}} \\ & + Y_{0D_{V4A}}\eta_{D_{V4B}} + Y_{0D_{V4B}}\eta_{D_{V4A}}) + e_d(\eta_{D_{H3A}}\eta_{D_{H3B}} + \eta_{D_{V4A}}\eta_{D_{V4B}})] \div Y_{n,n}^{\beta} \end{aligned} \quad (\text{E.12})$$

$$\begin{aligned}
e_{n,n}^\gamma = & [e_0(Y_{0D_{V5A}}Y_{0D_{V5B}} + Y_{0D_{V5A}}\eta_{D_{V5B}} + Y_{0D_{V5B}}\eta_{D_{V5A}} + Y_{0D_{V6A}}Y_{0D_{V6B}} \\
& + Y_{0D_{V6A}}\eta_{D_{V6B}} + Y_{0D_{V6B}}\eta_{D_{V6A}}) + e_d(\eta_{D_{V5A}}\eta_{D_{V5B}} + \eta_{D_{V6A}}\eta_{D_{V6B}})] \div Y_{n,n}^\gamma
\end{aligned} \tag{E.13}$$

Finally, the upper bound on the error rate measured in the complimentary basis used to approximate the phase error rate on the key basis is given by

$$e_{\mathcal{M}_2}^{1,1U} = \frac{E_{\nu_a\nu_b,\mathcal{M}_2}Q_{\nu_a\nu_b,\mathcal{M}_2}e^{2\nu} - e_0Y_0}{Y_{1,1}^L\nu^2}, \tag{E.14}$$

where

$$\begin{aligned}
Y_{1,1}^L = & (P(\mu_a|2)P(\mu_b|2)[Q_{\nu_a\nu_b,\mathcal{M}_2} - P(\nu_a|0)P(\nu_b|0)Y_0] - P(\nu_a|2)P(\nu_b|2)[Q_{\mu_a\mu_b,\mathcal{M}_1} \\
& - P(\mu_a|0)P(\mu_b|0)Y_0]) \div (P(\mu_a|2)P(\mu_b|2)P(\nu_a|1)P(\nu_b|1) \\
& - P(\mu_a|1)P(\mu_b|1)P(\nu_a|2)P(\nu_b|2)).
\end{aligned} \tag{E.15}$$

In above equation $P(\lambda|n) = \frac{(n+1)(\frac{\lambda}{2})^n}{(1+\frac{\lambda}{2})^{n+2}}$ with $\lambda \in \{\mu, \nu\}$ and n denotes number of photons.

E.1.1 Statistical fluctuation analysis

This section studies the effects of statistical fluctuations on single-photon occurrences and the phase error rates.

E.1.1.1 Estimation of $Q_{\mu_a\mu_b,\mathcal{M}_1}^{1,1}$

From the value directly observed from the experiment, $n_{\mu_a\mu_b} = Q_{\mu_a\mu_b}N_{\mu_a\mu_b}$ (where we omitted basis choice for simplicity), which corresponds to the number of detected signal states, we can use variant multiplicative Chernoff bound presented in Lemma

3 of Ref. [267] to estimate the lower and upper bounds of the expected detection events. For simplicity we use notation μ in place of $\mu_a\mu_b$ in the next discussion. To determine the bounds, we rewrite n_μ in terms of photon number statistics as

$$n_{k_a, k_b, \mu} = \sum_{l=1}^n \chi_{k_a, k_b, l}^\mu, \quad (\text{E.16})$$

where

$$\chi_{k_a, k_b, l}^\mu = \begin{cases} 1 & \text{with probability } p_{(a,b)} \\ 0 & \text{with probability } (1 - p_{(a,b)}) \end{cases}, \quad l = 1, \dots, n \quad (\text{E.17})$$

are independent Bernoulli random variables. Here $p_{(a,b)} = p(k_a|\mu_a)p(k_b|\mu_b)$. In particular, $\chi_{k_a, k_b, l}^\mu = 1$ means that k_a -photon signal state sent by Alice and k_b -photon signal state sent by Bob have resulted in the l th detection event while $\chi_{k_a, k_b, l}^\mu = 0$ means either vacuum or decoy state has been used. The term $p(k|\mu)$ is the conditional probability that a source set at signal intensity μ produces a k -photon state. It then follows that for a set of Bernoulli random variables, $\chi_{k_a, k_b, 1}^\mu, \chi_{k_a, k_b, 2}^\mu, \dots, \chi_{k_a, k_b, n}^\mu$, the expected value of $n_{k_a, k_b, \mu}$ is $\bar{n}_{k_a, k_b, \mu} = \mathbb{E}[n_{k_a, k_b, \mu}] = \sum_{l=1}^n p_{(a,b)}$. Let an observed outcome, $n_{k_a, k_b, \mu}$ be denoted by x for a given trial. Then, for any $\varepsilon_3 > 0$ we have that

$$\begin{aligned} \bar{n}_{k_a, k_b, \mu} &\geq \max\{0, x - \Delta(x, \varepsilon_3)\} \\ \bar{n}_{k_a, k_b, \mu}^L &:= \max\{0, x - \Delta(x, \varepsilon_3)\}, \end{aligned} \quad (\text{E.18})$$

holds with failure probability ε_3 , where $\bar{n}_{k_a, k_b, \mu}^L$ is the lower bound and $\Delta(x, \varepsilon_3)$ is the positive root of the equation $\Delta(x, \varepsilon_3) - [x + \Delta(x, \varepsilon_3)] \ln[1 + \Delta(x, \varepsilon_3)/x] - \ln x = 0$. Also, for any $\varepsilon_3 > 0$, we have that

$$\begin{aligned}\bar{n}_{k_a, k_b, \mu} &\leq x + \Delta(x, \varepsilon_3) \\ \bar{n}_{k_a, k_b, \mu}^U &:= x + \Delta(x, \varepsilon_3),\end{aligned}\tag{E.19}$$

holds with failure probability ε_3 , where $\bar{n}_{k_a, k_b, \mu}^U$ is the upper bound of $\bar{n}_{k_a, k_b, \mu}$ and $\Delta(x, \varepsilon_3)$ is the positive root of equation $\Delta(x, \varepsilon_3) + x \ln(x/[x + \Delta(x, \varepsilon_3)]) + \ln \varepsilon_3 = 0$. The same argument can be applied to determine the lower and upper bounds of expected value $\bar{n}_\nu$ from observed detection events $n_\nu = Q_\nu N_\nu$ for decoy states. Next, the lower and upper bounds of $\bar{n}_\mu$ and $\bar{n}_\nu$ are used to calculate the lower and upper bounds of gains, $\bar{Q}_\mu^L = \bar{n}_{k_a, k_b, \mu}^L/N_\mu$, $\bar{Q}_\mu^U = \bar{n}_{k_a, k_b, \mu}^U/N_\mu$, $\bar{Q}_\nu^L = \bar{n}_{k_a, k_b, \nu}^L/N_\nu$ and $\bar{Q}_\nu^U = \bar{n}_{k_a, k_b, \nu}^U/N_\nu$ which are in turn used to calculate $\bar{Y}_{1,1}^L$ and $\bar{Y}_{1,1}^U$, respectively as follows

$$\begin{aligned}\bar{Y}_{1,1}^L &= (P(\mu_a|2)P(\mu_b|2)[\bar{Q}_{\nu_a \nu_b, \mathcal{M}_2}^L - P(\nu_a|0)P(\nu_b|0)Y_0] - P(\nu_a|2)P(\nu_b|2)[Q_{\mu_a \mu_b, \mathcal{M}_1}^U \\ &\quad - P(\mu_a|0)P(\mu_b|0)Y_0]) \div (P(\mu_a|2)P(\mu_b|2)P(\nu_a|1)P(\nu_b|1) \\ &\quad - P(\mu_a|1)P(\mu_b|1)P(\nu_a|2)P(\nu_b|2)),\end{aligned}\tag{E.20}$$

$$\begin{aligned}\bar{Y}_{1,1}^U &= (P(\mu_a|2)P(\mu_b|2)[\bar{Q}_{\nu_a \nu_b, \mathcal{M}_2}^U - P(\nu_a|0)P(\nu_b|0)Y_0] - P(\nu_a|2)P(\nu_b|2)[Q_{\mu_a \mu_b, \mathcal{M}_1}^L \\ &\quad - P(\mu_a|0)P(\mu_b|0)Y_0]) \div (P(\mu_a|2)P(\mu_b|2)P(\nu_a|1)P(\nu_b|1) \\ &\quad - P(\mu_a|1)P(\mu_b|1)P(\nu_a|2)P(\nu_b|2)).\end{aligned}\tag{E.21}$$

Estimation of bounds for $n_{1,1,\mu}$ The parameters $\bar{Y}_{1,1}^U$ and $\bar{Y}_{1,1}^L$ are used to evaluate the upper and lower bounds on the observed yield for single photon components. We use multiplicative Chernoff bound (Lemma 2) of Ref. [267] to deduce the upper and lower bounds of observed yield from expected values $\bar{Y}_{1,1}^U$ and $\bar{Y}_{1,1}^L$ as follows. According to results of Lemma 2, if $g(\bar{Y}_{1,1}^U, \delta) = [e^\delta / (1 + \delta)^{1+\delta}]^{\bar{Y}_{1,1}^U}$, for any $\delta > 0$, then upper tail is defined as

$$\Pr[Y_{1,1}^U \geq (1 + \delta)\bar{Y}_{1,1}^U] < g(\bar{Y}_{1,1}^U, \delta) = \varepsilon_2, \quad (\text{E.22})$$

where δ is the positive root of the equation $\bar{Y}_{1,1}^U[\delta - (1 + \delta)\ln(1 + \delta)] - \ln \varepsilon_2 = 0$. For any $0 < \hat{\delta} \leq 1$, we have the lower tail given by

$$\Pr[Y_{1,1}^L \leq (1 - \hat{\delta})\bar{Y}_{1,1}^L] < g(\bar{Y}_{1,1}^L, -\hat{\delta}) = \hat{\varepsilon}_2, \quad (\text{E.23})$$

where $\hat{\delta}$ is the positive root of equation $\bar{Y}_{1,1}^L[\hat{\delta} + (1 - \hat{\delta})\ln(1 - \hat{\delta})] + \ln \hat{\varepsilon}_2 = 0$. From these results, the observed lower bound of single photon detection events is given by $n_{1,1,\mu}^L = Y_{1,1}^L N_\mu p_{(a,b)}$. The detection events are used to compute the gain for single photon events as $Q_\mu^{1,1} = n_{1,1,\mu}^L / N_\mu$.

E.1.1.2 Estimation of $e_{\mathcal{M}_\epsilon}^{1,1U}$

The tail inequality for random sampling without replacement described in Lemma 1 of [267] is exploited to provide an upper bound for the expected error rates from the observed error rates in the sampled data. We can use Lemma 1 to estimate the upper bound on expected error rate in the $\mathcal{M}_1$ basis by considering a thought experiment picture where an $n + m$ string of bits correspond to compatible measurements made by Alice, Bob and Charlie in the $\mathcal{M}_1$ basis. If the observed average error rate obtained from m random bit strings is $E_{\mu_a \mu_b, \mathcal{M}_1} = \sum_{i=1}^m r_{\mathcal{M}_1, A} \oplus r_{\mathcal{M}_1, B}$ ($r_{\mathcal{M}_1, A}$ and $r_{\mathcal{M}_1, B}$ are Alice and Bob's bits) then by using the upper tail inequality, the remaining

n bits give upper bound for error rate in the $\mathcal{M}_1$ basis under the condition that

$$\bar{E}_{\mu_a \mu_b, \mathcal{M}_1}^U \leq E_{\mu_a \mu_b, \mathcal{M}_1} + \xi(n, m, E_{\mu_a \mu_b, \mathcal{M}_1}, \varepsilon_1), \quad (\text{E.24})$$

with probability $1 - \varepsilon_1$. We leverage this result and the outcome of (E.21) to compute the upper on error rate for single photon events as

$$e_{\mathcal{M}_1}^{1,1U} = \frac{\bar{E}_{\mu_a \mu_b, \mathcal{M}_1}^U \bar{Q}_\mu^U - e_0 Y_0 p(\mu|0)}{\bar{Y}_{1,1}^L}. \quad (\text{E.25})$$

E.2 Secrecy

Let the system $\tilde{\mathbf{E}}$ represent information collected by Eve on Alice and Bob's bit strings $\mathbf{K}_A$ and $\mathbf{K}_B$, respectively, up to the error correction step. By applying the privacy amplification based on the universal class-two hash function, we generate a Δ -secret key of length ℓ and

$$\Delta \leq 2\varepsilon + \frac{1}{2} \sqrt{2^{\ell - H_{\min}^\varepsilon(\mathbf{K}_A | \tilde{\mathbf{E}})}}, \quad (\text{E.26})$$

where $H_{\min}^\varepsilon(\mathbf{K}_A | \tilde{\mathbf{E}})$ represents the smooth min-entropy, which corresponds to the average probability which an adversary guesses $\mathbf{K}_A$ correctly using an optimal strategy through having access to $\tilde{\mathbf{E}}$. Let $v = \frac{1}{2} \sqrt{2^{\ell - H_{\min}^\varepsilon(\mathbf{K}_A | \tilde{\mathbf{E}})}}$, then the secret key length, ℓ is given by

$$\ell = H_{\min}^\varepsilon(\mathbf{K}_A | \tilde{\mathbf{E}}) - 2 \log_2 \left(\frac{1}{2v} \right). \quad (\text{E.27})$$

During error correction, Alice and Bob reveal bits of information equal to $\text{leak}_{EC} + \log_2 \left(\frac{2}{\varepsilon_{\text{cor}}} \right)$ to an eavesdropper. Therefore, we have that

$$H_{\min}^{\varepsilon}(\mathbf{K}_A | \tilde{\mathbf{E}}) \geq H_{\min}^{\varepsilon}(\mathbf{K}_A | \mathbf{E}) - \text{leak}_{EC} + \log_2 \left(\frac{2}{\varepsilon_{\text{cor}}} \right), \quad (\text{E.28})$$

where $\mathbf{E}$ is Eve's information prior to the error correction step. Since our analysis is based on decoy states, $\mathbf{K}_A$ can be written in terms of $\mathbf{K}_A^1 \mathbf{K}_A^m$ and this represents the bit strings owing to single photons and multi-photons events. By using the generalized chain rule for smooth entropies, we have that

$$\begin{aligned} H_{\min}^{\varepsilon}(\mathbf{K}_A | \mathbf{E}) &\geq H_{\min}^{\delta_1}(\mathbf{K}_A^1 | \mathbf{K}_A^m \mathbf{E}) + H_{\min}^{\delta_3}(\mathbf{K}_A^m | \mathbf{E}) - 2 \log_2 \left(\frac{1}{\delta_2} \right) - 1 \\ &\geq H_{\min}^{\delta_1}(\mathbf{K}_A^1 | \mathbf{K}_A^m \mathbf{E}) - 2 \log_2 \left(\frac{1}{\delta_2} \right) - 1, \end{aligned} \quad (\text{E.29})$$

Furthermore, the second inequality is based on the fact that $H_{\min}^{\delta_3}(\mathbf{K}_A^m | \mathbf{E}) \geq 0$. Next, we provide bound for $H_{\text{Twissmin}}^{\delta_1}(\mathbf{K}_A^1 | \mathbf{K}_A^m \mathbf{E})$ by using the uncertainty relations for the smooth entropies. To achieve this, we use a gedankenexperiment where Alice and Bob prepare all their states in the basis $\mathcal{M}_2$ even when they choose the $\mathcal{M}_1$ basis. In this hypothetical protocol, the bit strings obtained from measurements in the complementary basis, $\mathbf{C}_A$ and $\mathbf{C}_B$ of length ℓ replace the keys $\mathbf{K}_A$ and $\mathbf{K}_B$. The smooth min-entropy is expressed as

$$\begin{aligned} H_{\min}^{\delta_1}(\mathbf{K}_A^1 | \mathbf{K}_A^m \mathbf{E}) &\geq n_{1,1\mu} - H_{\max}^{\varepsilon}(\mathbf{C}_A | \mathbf{C}_B) \\ &= n_{1,1\mu} [1 - h(e_{\mathcal{M}_2}^{1,1})], \end{aligned} \quad (\text{E.30})$$

where $n_{1,1\mu} = N_{\mu} p_{\kappa}^2 Q_{\mu_a \mu_b \mathcal{M}_1}^{1,1}$ denotes the sifted raw key size obtained from the single photon occurrences.

Finally, we combine all the terms representing errors for min-entropies and error probabilities due to parameter estimation discussed in the previous section. Thus,

the secrecy is given by

$$\varepsilon_{\text{sec}} = 2\varepsilon + 2\delta_1 + \delta_2 + v + \varepsilon_1 + \varepsilon_2. \quad (\text{E.31})$$

Here, ε_1 and ε_2 represent error probabilities for estimating the single photon events and the phase error rate. The error term is set to a common value ε and $\varepsilon_{\text{sec}} = 8\varepsilon$. The final key length ℓ is obtained using the results from Eq. (E.28) to Eq. (E.30) and invoking the secrecy requirement from Eq. (E.31) in Eq. (E.27). Then, the final derived formula is written as

$$\ell = N_\mu p_\kappa^2 \left[Q_{\mu_a \mu_b, \mathcal{M}_1}^{1,1} (\log_2 3 - h_3(e_{\mathcal{M}_2}^{1,1U})) - \text{leak}_{EC} - \log_2 \frac{2}{\varepsilon_{\text{cor}}} - 2 \log_2 \frac{4}{\varepsilon_{\text{sec}}} \right]. \quad (\text{E.32})$$

Derivation of decoy-state parameters for MDI-QKD with vector vortex beams

This appendix presents the derivation of the parameters used to estimate the MDI-QKD secret key rate. The gain for single photon states $Q_{11}^{\mathbf{V}}$, which represents the probability of Alice and Bob sending out single photon states on a vector basis and obtaining successful detection results, is expressed as follows

$$Q_{11}^{\mathbf{V}} = \mu_a \mu_b e^{-\mu_a - \mu_b} Y_{11}^{\mathbf{V}}. \quad (\text{F.1})$$

The quantity $Y_{11}^{\mathbf{V}}$ corresponds to the yield of single photons in the vector basis and is given by

$$Y_{11}^{\mathbf{V}} = Y_{11}^{\text{L0R1}} + Y_{11}^{\text{L1R0}} + Y_{11}^{\text{L0L1}} + Y_{11}^{\text{R0R1}} + Y_{11}^{\text{L0R0}} + Y_{11}^{\text{L1R1}}. \quad (\text{F.2})$$

Without a loss of generality, here we show how to obtain Y_{11}^{L0R1} , and owing to symmetry, other terms are deduced similarly. After propagating through a lossy channel modeled by transmittance η_a, η_b , the initial state of Alice and Bob can be

described as a mixed state

$$\begin{aligned} & \frac{\eta_a \eta_b}{4} |\psi_{11}\rangle \langle \psi_{11}| + \frac{\eta_a(1-\eta_b)}{2} |\psi_{10}\rangle \langle \psi_{10}| + \frac{(1-\eta_a)\eta_b}{2} |\psi_{01}\rangle \langle \psi_{01}| \\ & + (1-\eta_a)(1-\eta_b) |\psi_{00}\rangle \langle \psi_{00}| \end{aligned} \quad (\text{F.3})$$

where $|\psi_{00}\rangle = |00\rangle_{ab}$, $|\psi_{01}\rangle = |01\rangle_{ab}$, $|\psi_{10}\rangle = |10\rangle_{ab}$, $|\psi_{11}\rangle = |11\rangle_{ab}$ and $|0\rangle$, $|1\rangle$ represent vacuum and one photon states. After passing through a BS, the states in Eq. (F.3) transform to

$$\begin{aligned} |11\rangle_{12} &\mapsto \frac{1}{\sqrt{2}}(|0\rangle_3|2\rangle_4 - |2\rangle_3|0\rangle_4), \\ |10\rangle_{12} &\mapsto \frac{1}{\sqrt{2}}(|0\rangle_3|1\rangle_4 - |1\rangle_3|0\rangle_4), \\ |01\rangle_{12} &\mapsto \frac{1}{\sqrt{2}}(|1\rangle_3|0\rangle_4 - |0\rangle_3|1\rangle_4), \\ |00\rangle_{12} &\mapsto |0\rangle_3|0\rangle_4, \end{aligned} \quad (\text{F.4})$$

where we assume the case of indistinguishable photons. For distinguishable photons the state $|11\rangle$ can also be represented by the transformations

$$|11\rangle_{12} \mapsto |1\rangle_3|1\rangle_4 \quad (\text{F.5})$$

$$|11\rangle_{12} \mapsto \frac{1}{\sqrt{2}}(|0\rangle_3|2\rangle_4 - |2\rangle_3|0\rangle_4). \quad (\text{F.6})$$

The Bell state measurement is considered successful when exactly one of the two detectors is triggered in each OAM mode. By taking into account the effects of detector dark counts p_d , we obtain the photon detection probabilities by conditioning on the following events;

Dark counts In a case where no photons reach the input ports of the beam-splitter, detection events can only result from detector noise. In this case, the detection probability is given by

$$P_{\text{det}}(|00\rangle) = (1 - \eta_a)(1 - \eta_b)p_d^2(1 - p_d)^2. \quad (\text{F.7})$$

One-photon case Consider a case where only one photon from the two parties reaches the input port of the beam-splitter, then detection probability is given by

$$P_{\text{det}}(|01\rangle) = (1 - \eta_a)\eta_b(1 - p_d)p_d(1 - p_d)^2 \quad (\text{F.8})$$

$$P_{\text{det}}(|10\rangle) = \eta_a(1 - \eta_b)(1 - p_d)p_d(1 - p_d)^2 \quad (\text{F.9})$$

Two-photon case We now determine detection events emanating from two photons entering the beam-splitter. The two photons can leave the BS at different ports, or they may exit from the same port, and the detection probabilities are respectively given by

$$P_{\text{det}}(|11\rangle) = \eta_a\eta_b(1 - p_d)^2(1 - p_d)^2 \quad (\text{F.10})$$

$$P_{\text{det}}(|11\rangle) = \eta_a\eta_b(1 - p_d)p_d(1 - p_d)^2. \quad (\text{F.11})$$

Thus, the yield Y_{11}^{LOR1} is given by

$$Y_{11}^{\text{LOR1}} = (1 - p_d)^2[\eta_a\eta_b + (\eta_b + \eta_a - 4\eta_a\eta_b)p_d + (1 - 2\eta_a - 2\eta_b + 4\eta_a\eta_b)p_d^2]. \quad (\text{F.12})$$

An error is obtained in the cases where L0 and R0 or L1 and R1 click. The detection probabilities for these events are given by

$$Y_{11}^{\text{L0R0(L1R1)}} = (1 - p_d)^2 [(\eta_b + \eta_a - \eta_a \eta_b) p_d + (1 - 2\eta_a - 2\eta_b + 2\eta_a \eta_b) p_d^2] \quad (\text{F.13})$$

Thus, an error rate $e_{11}^{\mathbf{S}}$ is given by

$$\begin{aligned} e_{11}^{\mathbf{S}} Y_{11} &= Y_{11}^{\text{L0R0}} + Y_{11}^{\text{L1R1}} \\ &= 2(1 - p_d)^2 [(\eta_a + \eta_b - \eta_a \eta_b) p_d + (1 - 2\eta_a - 2\eta_b + 2\eta_a \eta_b) p_d^2] \\ &= e_0 (1 - p_d)^2 [(\eta_a + \eta_b - \eta_a \eta_b) p_d + (1 - 2\eta_a - 2\eta_b + 2\eta_a \eta_b) p_d^2] \end{aligned} \quad (\text{F.14})$$

where $e_0 = \frac{1}{2}$ corresponds to the random erroneous detection error rate. The overall gain $Q_\mu^{\mathbf{V}}$ and the QBER, $E_\mu^{\mathbf{V}}$ are evaluated in accordance with the method in Ref. [309] with modifications as follows

$$\begin{aligned} Q_\mu^{\mathbf{V}} &= [D_{\text{L0}}(1 - D_{\text{L1}}) + (1 - D_{\text{L0}})D_{\text{L1}}][D_{\text{R1}}(1 - D_{\text{R0}}) + (1 - D_{\text{R1}})D_{\text{R0}}] \\ &\quad + [D_{\text{L0}}D_{\text{L1}}(1 - D_{\text{R0}})(1 - D_{\text{R1}})] + [D_{\text{R0}}D_{\text{R1}}(1 - D_{\text{L0}})(1 - D_{\text{L1}})]. \end{aligned} \quad (\text{F.15})$$

Here, the detection probabilities for the four detectors are given by

$$D_{\text{L0(R0)}} = 1 - (1 - p_d) \exp \left(- \left| e^{i\theta_a} \frac{\sqrt{\eta_a \mu_a}}{2} + e^{i\theta_b} \frac{\sqrt{\eta_b \mu_b}}{2} \right| \right), \quad (\text{F.16})$$

$$D_{\text{L1(R1)}} = 1 - (1 - p_d) \exp \left(- \left| e^{i\theta_a} \frac{\sqrt{\eta_a \mu_a}}{2} - e^{i\theta_b} \frac{\sqrt{\eta_b \mu_b}}{2} \right| \right). \quad (\text{F.17})$$

We adopt the following notation to simplify our analysis;

$$\begin{aligned}\lambda &= \eta_a \mu_a + \eta_b \mu_b, \\ \Delta\theta &= \theta_b - \theta_a, \\ x &= \sqrt{\eta_a \mu_a \eta_b \mu_b}/2, \\ y &= (1 - p_d)e^{-\lambda/4},\end{aligned}$$

where λ denotes the average number of photons after interference in the BS, and $\Delta\theta$ corresponds to the difference between Alice's and Bob's random overall phases. As a result, the probability of detection simplifies as follows

$$D_{L0(R0)} = 1 - ye^{-x \cos \Delta\theta}, \quad (\text{F.18})$$

$$D_{L1(R1)} = 1 - ye^{x \cos \Delta\theta}. \quad (\text{F.19})$$

The QBER, $E_\mu^{\mathbf{V}}$ is expressed as

$$E_\mu^{\mathbf{V}} Q_\mu^{\mathbf{V}} = 2D_{L0}(1 - D_{L1})(1 - D_{R1})D_{R0}. \quad (\text{F.20})$$

Bibliography

- [1] V. Scarani, H. Bechmann-Pasquinucci, N. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, “The security of practical quantum key distribution,” *Reviews of Modern Physics*, vol. 81, no. 3, pp. 1301–1350, 2009.
- [2] C. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, vol. 175, Bangalore, India, 1984.
- [3] A. K. Ekert, “Quantum cryptography based on Bell’s theorem,” *Physical Review Letters*, vol. 67, no. 6, p. 661, 1991.
- [4] L. Rivest, Ronald, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.
- [5] P. W. Shor, “Algorithms for quantum computation: discrete logarithms and factoring,” in *Proceedings 35th annual symposium on foundations of computer science*, pp. 124–134, IEEE, 1994.
- [6] H.-K. Lo, M. Curty, and K. Tamaki, “Secure quantum key distribution,” *Nature Photonics*, vol. 8, no. 8, p. 595, 2014.
- [7] V. Zapatero, T. van Leent, R. Arnon-Friedman, W.-Z. Liu, Q. Zhang, H. Weinfurter, and M. Curty, “Advances in device-independent quantum key distribution,” *npj Quantum Information*, vol. 9, no. 1, p. 10, 2023.
- [8] W. K. Wootters and W. H. Zurek, “A single quantum cannot be cloned,” *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.

- [9] C. H. Bennett, “Quantum cryptography using any two nonorthogonal states,” *Physical Review Letters*, vol. 68, no. 21, p. 3121, 1992.
- [10] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, “Limitations on practical quantum cryptography,” *Physical Review Letters*, vol. 85, no. 6, p. 1330, 2000.
- [11] N. Lütkenhaus and M. Jahma, “Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack,” *New Journal of Physics*, vol. 4, no. 1, p. 44, 2002.
- [12] 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*, vol. 92, no. 5, p. 057901, 2004.
- [13] C. Bennett, “Quantum cryptography using any two non-orthogonal states,” *Physical Review Letters*, vol. 68, no. 21, pp. 3121–3124, 1992.
- [14] F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, “Continuous-variable quantum key distribution with gaussian modulation—the theory of practical implementations,” *Advanced Quantum Technologies*, vol. 1, no. 1, p. 1800011, 2018.
- [15] Y. Zhang, Y. Bian, Z. Li, S. Yu, and H. Guo, “Continuous-variable quantum key distribution system: Past, present, and future,” *Applied Physics Reviews*, vol. 11, no. 1, 2024.
- [16] N. Jain, H.-M. Chin, H. Mani, C. Lupo, D. S. Nikolic, A. Kordts, S. Pirandola, T. B. Pedersen, M. Kolb, B. Ömer, *et al.*, “Practical continuous-variable quantum key distribution with composable security,” *Nature Communications*, vol. 13, no. 1, p. 4740, 2022.
- [17] Y. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, “Long-distance continuous-variable quantum key distribution over 202.81 km of fiber,” *Physical Review Letters*, vol. 125, no. 1, p. 010502, 2020.
- [18] S. Ghorai, P. Grangier, E. Diamanti, and A. Leverrier, “Asymptotic security of continuous-variable quantum key distribution with a discrete modulation,” *Physical Review X*, vol. 9, no. 2, p. 021059, 2019.

- [19] J. Lin, T. Upadhyaya, and N. Lütkenhaus, “Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution,” *Physical Review X*, vol. 9, no. 4, p. 041064, 2019.
- [20] T. Matsuura, K. Maeda, T. Sasaki, and M. Koashi, “Finite-size security of continuous-variable quantum key distribution with digital signal processing,” *Nature Communications*, vol. 12, no. 1, p. 252, 2021.
- [21] S. Bäuml, C. Pascual-García, V. Wright, O. Fawzi, and A. Acín, “Security of discrete-modulated continuous-variable quantum key distribution,” *Quantum*, vol. 8, p. 1418, 2024.
- [22] P. Wang, Y. Zhang, Z. Lu, X. Wang, and Y. Li, “Discrete-modulation continuous-variable quantum key distribution with a high key rate,” *New Journal of Physics*, vol. 25, no. 2, p. 023019, 2023.
- [23] L. Li, T. Wang, X. Li, P. Huang, Y. Guo, L. Lu, L. Zhou, and G. Zeng, “Continuous-variable quantum key distribution with on-chip light sources,” *Photonics Research*, vol. 11, no. 4, pp. 504–516, 2023.
- [24] K. Inoue, E. Waks, and Y. Yamamoto, “Differential phase shift quantum key distribution,” *Physical Review Letters*, vol. 89, no. 3, p. 037902, 2002.
- [25] A. Mizutani, Y. Takeuchi, and K. Tamaki, “Finite-key security analysis of differential-phase-shift quantum key distribution,” *Physical Review Research*, vol. 5, no. 2, p. 023132, 2023.
- [26] Y. Hatakeyama, A. Mizutani, G. Kato, N. Imoto, and K. Tamaki, “Differential-phase-shift quantum-key-distribution protocol with a small number of random delays,” *Physical Review A*, vol. 95, no. 4, p. 042301, 2017.
- [27] A. Mizutani and T. Tsurumaru, “Tight scaling of key rate for differential-phase-shift quantum key distribution,” *Physical Review Research*, vol. 6, no. 4, p. 043300, 2024.
- [28] H. Endo, T. Sasaki, M. Takeoka, M. Fujiwara, M. Koashi, and M. Sasaki, “Line-of-sight quantum key distribution with differential phase shift keying,” *New Journal of Physics*, vol. 24, no. 2, p. 025008, 2022.
- [29] K. Inoue and T. Honjo, “Quantum conference key agreement based on differential-phase-shift quantum key distribution,” *Quantum Information Processing*, vol. 23, no. 7, p. 253, 2024.

- [30] M. Sandfuchs, M. Haberland, V. Vilasini, and R. Wolf, “Security of differential phase shift qkd from relativistic principles,” *Quantum*, vol. 9, p. 1611, 2025.
- [31] K. Inoue and T. Honjo, “Modified general individual attack against differential-phase-shift quantum key distribution,” *Physical Review A*, vol. 110, no. 4, p. 042626, 2024.
- [32] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, “Fast and simple one-way quantum key distribution,” *Applied Physics Letters*, vol. 87, no. 19, p. 194108, 2005.
- [33] M.-Y. Li, X.-Y. Cao, Y.-M. Xie, H.-L. Yin, and Z.-B. Chen, “Finite-key analysis for coherent one-way quantum key distribution,” *Physical Review Research*, vol. 6, no. 1, p. 013022, 2024.
- [34] R.-Q. Gao, Y.-M. Xie, J. Gu, W.-B. Liu, C.-X. Weng, B.-H. Li, H.-L. Yin, and Z.-B. Chen, “Simple security proof of coherent-one-way quantum key distribution,” *Optics Express*, vol. 30, no. 13, pp. 23783–23795, 2022.
- [35] E. Lavie and C. C.-W. Lim, “Improved coherent one-way quantum key distribution for high-loss channels,” *Physical Review Applied*, vol. 18, no. 6, p. 064053, 2022.
- [36] J. González-Payo, R. Trényi, W. Wang, and M. Curty, “Upper security bounds for coherent-one-way quantum key distribution,” *Physical Review Letters*, vol. 125, no. 26, p. 260510, 2020.
- [37] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, “Time-shift attack in practical quantum cryptosystems,” *Quantum Information & Computation*, vol. 7, no. 1, pp. 73–82, 2007.
- [38] A. Lamas-Linares and C. Kurtsiefer, “Breaking a quantum key distribution system through a timing side channel,” *Optics Express*, vol. 15, no. 15, pp. 9388–9393, 2007.
- [39] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, “Hacking commercial quantum cryptography systems by tailored bright illumination,” *Nature Photonics*, vol. 4, no. 10, pp. 686–689, 2010.
- [40] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter, “Quantum eavesdropping without interception: an attack exploiting the dead

- time of single-photon detectors,” *New Journal of Physics*, vol. 13, no. 7, p. 073024, 2011.
- [41] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, “Full-field implementation of a perfect eavesdropper on a quantum cryptography system,” *Nature Communications*, vol. 2, no. 1, p. 349, 2011.
- [42] R. Trényi and M. Curty, “Zero-error attack against coherent-one-way quantum key distribution,” *New Journal of Physics*, vol. 23, no. 9, p. 093005, 2021.
- [43] J. Rey-Domínguez, Á. Navarrete, P. van Loock, and M. Curty, “Hacking coherent-one-way quantum key distribution with present-day technology,” *Quantum Science and Technology*, vol. 9, no. 3, p. 035044, 2024.
- [44] J.-Z. Huang, S. Kunz-Jacques, P. Jouguet, C. Weedbrook, Z.-Q. Yin, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, “Quantum hacking on quantum key distribution using homodyne detection,” *Physical Review A*, vol. 89, no. 3, p. 032304, 2014.
- [45] S. Sun and A. Huang, “A review of security evaluation of practical quantum key distribution system,” *Entropy*, vol. 24, no. 2, p. 260, 2022.
- [46] X.-L. Pang, A.-L. Yang, C.-N. Zhang, J.-P. Dou, H. Li, J. Gao, and X.-M. Jin, “Hacking quantum key distribution via injection locking,” *Physical Review Applied*, vol. 13, no. 3, p. 034008, 2020.
- [47] F.-Y. Lu, P. Ye, Z.-H. Wang, S. Wang, Z.-Q. Yin, R. Wang, X.-J. Huang, W. Chen, D.-Y. He, G.-J. Fan-Yuan, *et al.*, “Hacking measurement-device-independent quantum key distribution,” *Optica*, vol. 10, no. 4, pp. 520–527, 2023.
- [48] A. Huang, Á. Navarrete, S.-H. Sun, P. Chaiwongkhot, M. Curty, and V. Makarov, “Laser-seeding attack in quantum key distribution,” *Physical Review Applied*, vol. 12, no. 6, p. 064043, 2019.
- [49] W.-Y. Hwang, “Quantum key distribution with high loss: toward global secure communication,” *Physical Review Letters*, vol. 91, no. 5, p. 057901, 2003.
- [50] H.-K. Lo, X. Ma, and K. Chen, “Decoy state quantum key distribution,” *Physical Review Letters*, vol. 94, no. 23, p. 230504, 2005.

- [51] D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, “Security of quantum key distribution with imperfect devices,” in *International Symposium on Information Theory, 2004. ISIT 2004. Proceedings.*, p. 136, IEEE, 2004.
- [52] K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, “Loss-tolerant quantum cryptography with imperfect sources,” *Physical Review A*, vol. 90, no. 5, p. 052314, 2014.
- [53] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, *et al.*, “Advances in quantum cryptography,” *Advances in Optics and Photonics*, vol. 12, no. 4, pp. 1012–1236, 2020.
- [54] E. Hänggi, “Device-independent quantum key distribution,” *arXiv preprint arXiv:1012.3878*, 2010.
- [55] U. Vazirani and T. Vidick, “Fully device independent quantum key distribution,” *Communications of the ACM*, vol. 62, no. 4, pp. 133–133, 2019.
- [56] W. Zhang, T. van Leent, K. Redeker, R. Garthoff, R. Schwonnek, F. Fertig, S. Eppelt, W. Rosenfeld, V. Scarani, C. C.-W. Lim, *et al.*, “A device-independent quantum key distribution system for distant users,” *Nature*, vol. 607, no. 7920, pp. 687–691, 2022.
- [57] F. Xu, Y.-Z. Zhang, Q. Zhang, and J.-W. Pan, “Device-independent quantum key distribution with random postselection,” *Physical Review Letters*, vol. 128, no. 11, p. 110506, 2022.
- [58] W.-Z. Liu, Y.-Z. Zhang, Y.-Z. Zhen, M.-H. Li, Y. Liu, J. Fan, F. Xu, Q. Zhang, and J.-W. Pan, “Toward a photonic demonstration of device-independent quantum key distribution,” *Physical Review Letters*, vol. 129, no. 5, p. 050502, 2022.
- [59] I. W. Primaatmaja, K. T. Goh, E. Y.-Z. Tan, J. T.-F. Khoo, S. Ghorai, and C. C.-W. Lim, “Security of device-independent quantum key distribution protocols: a review,” *Quantum*, vol. 7, p. 932, 2023.
- [60] H.-K. Lo, M. Curty, and B. Qi, “Measurement-device-independent quantum key distribution,” *Physical Review Letters*, vol. 108, no. 13, p. 130503, 2012.
- [61] G.-J. Fan-Yuan, F.-Y. Lu, S. Wang, Z.-Q. Yin, D.-Y. He, Z. Zhou, J. Teng, W. Chen, G.-C. Guo, and Z.-F. Han, “Measurement-device-independent

- quantum key distribution for nonstandalone networks,” *Photonics Research*, vol. 9, no. 10, pp. 1881–1891, 2021.
- [62] Y. Cao, Y.-H. Li, K.-X. Yang, Y.-F. Jiang, S.-L. Li, X.-L. Hu, M. Abulizi, C.-L. Li, W. Zhang, Q.-C. Sun, *et al.*, “Long-distance free-space measurement-device-independent quantum key distribution,” *Physical Review Letters*, vol. 125, no. 26, p. 260503, 2020.
- [63] R. Valivarthi, P. Umesh, C. John, K. A. Owen, V. B. Verma, S. W. Nam, D. Oblak, Q. Zhou, and W. Tittel, “Measurement-device-independent quantum key distribution coexisting with classical communication,” *Quantum Science and Technology*, vol. 4, no. 4, p. 045002, 2019.
- [64] H.-T. Zhu, Y. Huang, H. Liu, P. Zeng, M. Zou, Y. Dai, S. Tang, H. Li, L. You, Z. Wang, *et al.*, “Experimental mode-pairing measurement-device-independent quantum key distribution without global phase locking,” *Physical Review Letters*, vol. 130, no. 3, p. 030801, 2023.
- [65] W. Wang, K. Tamaki, and M. Curty, “Measurement-device-independent quantum key distribution with leaky sources,” *Scientific Reports*, vol. 11, no. 1, p. 1678, 2021.
- [66] C. Jiang, Z.-W. Yu, X.-L. Hu, and X.-B. Wang, “Higher key rate of measurement-device-independent quantum key distribution through joint data processing,” *Physical Review A*, vol. 103, no. 1, p. 012402, 2021.
- [67] Y. Tian, P. Wang, J. Liu, S. Du, W. Liu, Z. Lu, X. Wang, and Y. Li, “Experimental demonstration of continuous-variable measurement-device-independent quantum key distribution over optical fiber,” *Optica*, vol. 9, no. 5, pp. 492–500, 2022.
- [68] J. E. Bourassa, A. Gnanapandithan, L. Qian, and H.-K. Lo, “Measurement-device-independent quantum key distribution with passive time-dependent source side channels,” *Physical Review A*, vol. 106, no. 6, p. 062618, 2022.
- [69] R. I. Woodward, Y. Lo, M. Pittaluga, M. Minder, T. K. Paraïso, M. Lucamarini, Z. Yuan, and A. Shields, “Gigahertz measurement-device-independent quantum key distribution using directly modulated lasers,” *npj Quantum Information*, vol. 7, no. 1, p. 58, 2021.

- [70] Y.-H. Li, S.-L. Li, X.-L. Hu, C. Jiang, Z.-W. Yu, W. Li, W.-Y. Liu, S.-K. Liao, J.-G. Ren, H. Li, *et al.*, “Free-space and fiber-integrated measurement-device-independent quantum key distribution under high background noise,” *Physical Review Letters*, vol. 131, no. 10, p. 100802, 2023.
- [71] R. C. Berrevoets, T. Middelburg, R. F. Vermeulen, L. D. Chiesa, F. Broggi, S. Piciaccia, R. Pluis, P. Umesh, J. F. Marques, W. Tittel, *et al.*, “Deployed measurement-device independent quantum key distribution and bell-state measurements coexisting with standard internet data and networking equipment,” *Communications Physics*, vol. 5, no. 1, p. 186, 2022.
- [72] Y.-M. Xie, J.-L. Bai, Y.-S. Lu, C.-X. Weng, H.-L. Yin, and Z.-B. Chen, “Advantages of asynchronous measurement-device-independent quantum key distribution in intercity networks,” *Physical Review Applied*, vol. 19, no. 5, p. 054070, 2023.
- [73] A. Laing, V. Scarani, J. G. Rarity, and J. L. O’Brien, “Reference-frame-independent quantum key distribution,” *Physical Review A*, vol. 82, no. 1, p. 012304, 2010.
- [74] V. D’ambrosio, E. Nagali, S. P. Walborn, L. Aolita, S. Slussarenko, L. Marrucci, and F. Sciarrino, “Complete experimental toolbox for alignment-free quantum communication,” *Nature Communications*, vol. 3, no. 1, pp. 1–8, 2012.
- [75] P. Zhang, K. Aungskunsiri, E. Martín-López, J. Wabnig, M. Lobino, R. Nock, J. Munns, D. Bonneau, P. Jiang, H. Li, *et al.*, “Reference-frame-independent quantum-key-distribution server with a telecom tether for an on-chip client,” *Physical Review Letters*, vol. 112, no. 13, p. 130501, 2014.
- [76] C. Wang, S.-H. Sun, X.-C. Ma, G.-Z. Tang, and L.-M. Liang, “Reference-frame-independent quantum key distribution with source flaws,” *Physical Review A*, vol. 92, no. 4, p. 042319, 2015.
- [77] X. Fang, C. Wang, Y.-G. Han, Z.-Q. Yin, W. Chen, and Z.-F. Han, “Tomographic approach in reference-frame-independent measurement-device-independent quantum key distribution,” *Communications in Theoretical Physics*, vol. 66, no. 5, p. 496, 2016.
- [78] C.-M. Zhang, J.-R. Zhu, and Q. Wang, “Decoy-state reference-frame-independent measurement-device-independent quantum key distribution with

- biased bases,” *Journal of Lightwave Technology*, vol. 35, no. 20, pp. 4574–4578, 2017.
- [79] H.-L. Yin and Y. Fu, “Measurement-device-independent twin-field quantum key distribution,” *Scientific Reports*, vol. 9, no. 1, pp. 1–13, 2019.
- [80] H. Liu, J. Wang, H. Ma, and S. Sun, “Reference-frame-independent quantum key distribution using fewer states,” *Physical Review A*, vol. 12, no. 3, p. 034039, 2019.
- [81] Q. Li, C. Zhu, S. Ma, K. Wei, and C. Pei, “Reference-frame-independent and measurement-device-independent quantum key distribution using one single source,” *International Journal of Theoretical Physics*, vol. 57, no. 7, pp. 2192–2202, 2018.
- [82] K. Liu, J. Li, J.-R. Zhu, C.-M. Zhang, and Q. Wang, “Decoy-state reference-frame-independent quantum key distribution with both source errors and statistical fluctuations,” *Chinese Physics B*, vol. 26, no. 12, p. 120302, 2017.
- [83] J.-R. Zhu, R. Wang, and C.-M. Zhang, “Improved reference-frame-independent quantum key distribution,” *Optics Letters*, vol. 47, no. 16, pp. 4219–4222, 2022.
- [84] Y.-F. Nie and C.-M. Zhang, “Afterpulse analysis for reference-frame-independent quantum key distribution,” *Quantum Information Processing*, vol. 21, no. 9, p. 340, 2022.
- [85] S. Sun, “Security of reference-frame-independent quantum key distribution with source flaws,” *Physical Review A*, vol. 104, no. 2, p. 022423, 2021.
- [86] A. Jin, P. Zeng, R. V. Penty, and X. Ma, “Reference-frame-independent design of phase-matching quantum key distribution,” *Physical Review Applied*, vol. 16, no. 3, p. 034017, 2021.
- [87] L.-G. She and C.-M. Zhang, “Reference-frame-independent quantum key distribution with modified coherent states,” *Quantum Information Processing*, vol. 21, no. 5, p. 161, 2022.
- [88] J.-R. Zhu, C.-M. Zhang, R. Wang, and H.-W. Li, “Reference-frame-independent quantum key distribution with advantage distillation,” *Optics Letters*, vol. 48, no. 3, pp. 542–545, 2023.

- [89] Y. Zhou, H.-J. Ding, J.-Y. Liu, C.-H. Zhang, X.-Y. Zhou, and Q. Wang, “Finite-key security analysis against the trojan-horse attack on practical reference-frame-independent measurement-device-independent quantum key distribution,” *Physical Review Applied*, vol. 23, no. 2, p. 024007, 2025.
- [90] Z. Sun, J. Wang, Z. Li, W. Qu, T. Dou, F. Zhou, and H. Ma, “Performance of reference-frame-independent quantum key distribution in underwater channel,” *International Journal of Quantum Information*, vol. 19, no. 01, p. 2150011, 2021.
- [91] W.-J. Wang, X.-Y. Zhou, C.-H. Zhang, H.-J. Ding, and Q. Wang, “Performance influence on reference-frame-independent quantum key distributions with detection imperfections,” *Quantum Information Processing*, vol. 21, no. 8, p. 283, 2022.
- [92] Y. Li, Z. Sun, X. Liu, Z. Li, J. Li, H. Wang, K. Shi, C. Liu, and H. Ma, “Reference-frame-independent mode-pairing quantum key distribution with advantage distillation,” *Advanced Quantum Technologies*, vol. 7, no. 4, p. 2300387, 2024.
- [93] C. Wang, X.-T. Song, Z.-Q. Yin, S. Wang, W. Chen, C.-M. Zhang, G.-C. Guo, and Z.-F. Han, “Phase-reference-free experiment of measurement-device-independent quantum key distribution,” *Physical Review Letters*, vol. 115, no. 16, p. 160502, 2015.
- [94] W.-Y. Liang, S. Wang, H.-W. Li, Z.-Q. Yin, W. Chen, Y. Yao, J.-Z. Huang, G.-C. Guo, and Z.-F. Han, “Proof-of-principle experiment of reference-frame-independent quantum key distribution with phase coding,” *Scientific Reports*, vol. 4, p. 3617, 2014.
- [95] J. Wang, H. Liu, H. Ma, and S. Sun, “Experimental study of four-state reference-frame-independent quantum key distribution with source flaws,” *Physical Review A*, vol. 99, no. 3, p. 032309, 2019.
- [96] X.-Y. Zhou, H.-J. Ding, M.-S. Sun, S.-H. Zhang, J.-Y. Liu, C.-H. Zhang, J. Li, and Q. Wang, “Reference-frame-independent measurement-device-independent quantum key distribution over 200 km of optical fiber,” *Physical Review Applied*, vol. 15, no. 6, p. 064016, 2021.
- [97] B.-Y. Tang, H. Chen, J.-P. Wang, H.-C. Yu, L. Shi, S.-H. Sun, W. Peng, B. Liu, and W.-R. Yu, “Free-running long-distance reference-frame-

- independent quantum key distribution,” *npj Quantum Information*, vol. 8, no. 1, p. 117, 2022.
- [98] Z. Tian, Z. Xie, R. Wang, C. Zhang, and S. Sun, “Experimental demonstration of improved reference-frame-independent quantum key distribution over 175km,” *Optics Express*, vol. 32, no. 13, pp. 22460–22469, 2024.
- [99] X. Liu, D. Luo, Z. Luo, S. Li, Z. Zhang, and K. Wei, “Reference-frame-independent quantum key distribution over 250 km of optical fiber,” *Physical Review Applied*, vol. 22, no. 6, p. 064018, 2024.
- [100] R. Tannous, Z. Ye, J. Jin, K. B. Kuntz, N. Lütkenhaus, and T. Jennewein, “Demonstration of a 6 state-4 state reference frame independent channel for quantum key distribution,” *Applied Physics Letters*, vol. 115, no. 21, 2019.
- [101] Z. Xie, Z. Tian, X. Fan, Y. Chen, and S. Sun, “Four-state reference-frame-independent quantum key distribution over 200 km,” *Physical Review Applied*, vol. 22, no. 6, p. 064037, 2024.
- [102] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, “Fundamental limits of repeaterless quantum communications,” *Nature Communications*, vol. 8, no. 1, pp. 1–15, 2017.
- [103] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, “Quantum repeaters: the role of imperfect local operations in quantum communication,” *Physical Review Letters*, vol. 81, no. 26, p. 5932, 1998.
- [104] L.-M. Duan, M. Lukin, J. I. Cirac, and P. Zoller, “Long-distance quantum communication with atomic ensembles and linear optics,” *Nature*, vol. 414, no. 6862, p. 413, 2001.
- [105] R. Van Meter, *Quantum networking*. John Wiley & Sons, 2014.
- [106] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, “Overcoming the rate–distance limit of quantum key distribution without quantum repeaters,” *Nature*, vol. 557, no. 7705, p. 400, 2018.
- [107] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, W. Chen, *et al.*, “Twin-field quantum key distribution over 830-km fibre,” *Nature Photonics*, vol. 16, no. 2, pp. 154–161, 2022.

- [108] Y. Liu, W.-J. Zhang, C. Jiang, J.-P. Chen, C. Zhang, W.-X. Pan, D. Ma, H. Dong, J.-M. Xiong, C.-J. Zhang, *et al.*, “Experimental twin-field quantum key distribution over 1000 km fiber distance,” *Physical Review Letters*, vol. 130, no. 21, p. 210801, 2023.
- [109] L. Zhou, J. Lin, Y. Jing, and Z. Yuan, “Twin-field quantum key distribution without optical frequency dissemination,” *Nature Communications*, vol. 14, no. 1, p. 928, 2023.
- [110] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W.-J. Zhang, Z.-Y. Han, S.-Z. Ma, X.-L. Hu, Y.-H. Li, H. Liu, *et al.*, “Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas,” *Nature Photonics*, vol. 15, no. 8, pp. 570–575, 2021.
- [111] W. Li, L. Zhang, Y. Lu, Z.-P. Li, C. Jiang, Y. Liu, J. Huang, H. Li, Z. Wang, X.-B. Wang, *et al.*, “Twin-field quantum key distribution without phase locking,” *Physical Review Letters*, vol. 130, no. 25, p. 250802, 2023.
- [112] Y. Liu, W.-J. Zhang, C. Jiang, J.-P. Chen, D. Ma, C. Zhang, W.-X. Pan, H. Dong, J.-M. Xiong, C.-J. Zhang, *et al.*, “1002 km twin-field quantum key distribution with finite-key analysis,” *Quantum Frontiers*, vol. 2, no. 1, p. 16, 2023.
- [113] X. Zhong, W. Wang, R. Mandil, H.-K. Lo, and L. Qian, “Simple multiuser twin-field quantum key distribution network,” *Physical Review Applied*, vol. 17, no. 1, p. 014025, 2022.
- [114] C. Clivati, A. Meda, S. Donadello, S. Virzì, M. Genovese, F. Levi, A. Mura, M. Pittaluga, Z. Yuan, A. J. Shields, *et al.*, “Coherent phase transfer for real-world twin-field quantum key distribution,” *Nature Communications*, vol. 13, no. 1, p. 157, 2022.
- [115] Y.-M. Xie, C.-X. Weng, Y.-S. Lu, Y. Fu, Y. Wang, H.-L. Yin, and Z.-B. Chen, “Scalable high-rate twin-field quantum key distribution networks without constraint of probability and intensity,” *Physical Review A*, vol. 107, no. 4, p. 042603, 2023.
- [116] C. H. Park, M. K. Woo, B. K. Park, Y.-S. Kim, H. Baek, S.-W. Lee, H.-T. Lim, S.-W. Jeon, H. Jung, S. Kim, *et al.*, “ $2 \times n$ twin-field quantum key distribution network configuration based on polarization, wavelength, and time division multiplexing,” *npj Quantum Information*, vol. 8, no. 1, p. 48, 2022.

- [117] J.-P. Chen, F. Zhou, C. Zhang, C. Jiang, F.-X. Chen, J. Huang, H. Li, L.-X. You, X.-B. Wang, Y. Liu, *et al.*, “Twin-field quantum key distribution with local frequency reference,” *Physical Review Letters*, vol. 132, no. 26, p. 260802, 2024.
- [118] H. Bechmann-Pasquinucci and A. Peres, “Quantum cryptography with 3-state systems,” *Physical Review Letters*, vol. 85, no. 15, pp. 3313–3316, 2000.
- [119] J. C. Howell, R. S. Bennink, S. J. Bentley, and R. Boyd, “Realization of the Einstein-Podolsky-Rosen paradox using momentum-and position-entangled photons from spontaneous parametric down conversion,” *Physical Review Letters*, vol. 92, no. 21, p. 210403, 2004.
- [120] M. Mafu, A. Dudley, S. Goyal, D. Giovannini, M. McLaren, M. J. Padgett, T. Konrad, F. Petruccione, N. Lütkenhaus, and A. Forbes, “Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases,” *Physical Review A*, vol. 88, no. 3, p. 032305, 2013.
- [121] A. Sit, F. Bouchard, R. Fickler, J. Gagnon-Bischoff, H. Larocque, K. Heshami, D. Elser, C. Peuntinger, K. Günthner, B. Heim, *et al.*, “High-dimensional intracity quantum cryptography with structured photons,” *Optica*, vol. 4, no. 9, pp. 1006–1010, 2017.
- [122] M. Mirhosseini, O. S. Magaña-Loaiza, M. N. O’Sullivan, B. Rodenburg, M. Malik, M. P. J. Lavery, M. J. Padgett, D. J. Gauthier, and R. W. Boyd, “High-dimensional quantum cryptography with twisted light,” *New Journal of Physics*, vol. 17, no. 3, p. 033033, 2015.
- [123] F. Wang, P. Zeng, X. Wang, H. Gao, F. Li, and P. Zhang, “Towards practical high-speed high dimensional quantum key distribution using partial mutual unbiased basis of photon’s orbital angular momentum,” *arXiv preprint arXiv:1801.06582*, 2018.
- [124] F. Bouchard, K. Heshami, D. England, R. Fickler, R. W. Boyd, B.-G. Englert, L. L. Sánchez-Soto, and E. Karimi, “Experimental investigation of high-dimensional quantum key distribution protocols with twisted photons,” *Quantum*, vol. 2, p. 111, 2018.
- [125] Z. Tao, Y. Ren, A. Abdukirim, S. Liu, and R. Rao, “Mitigating the effect of atmospheric turbulence on orbital angular momentum-based quantum key

- distribution using real-time adaptive optics with phase unwrapping,” *Optics Express*, vol. 29, no. 20, pp. 31078–31098, 2021.
- [126] K. Yao, W. O. Krawec, and J. Zhu, “Quantum sampling for finite key rates in high dimensional quantum cryptography,” *IEEE Transactions on Information Theory*, vol. 68, no. 5, pp. 3144–3163, 2022.
- [127] D. Cozzolino, D. Bacco, B. Da Lio, K. Ingerslev, Y. Ding, K. Dalgaard, P. Kristensen, M. Galili, K. Rottwitt, S. Ramachandran, *et al.*, “Orbital angular momentum states enabling fiber-based high-dimensional quantum communication,” *Physical Review Applied*, vol. 11, no. 6, p. 064058, 2019.
- [128] H.-H. Li, L.-H. Gong, and N.-R. Zhou, “New semi-quantum key agreement protocol based on high-dimensional single-particle states,” *Chinese Physics B*, vol. 29, no. 11, p. 110304, 2020.
- [129] Q.-K. Wang, F.-X. Wang, J. Liu, W. Chen, Z.-F. Han, A. Forbes, and J. Wang, “High-dimensional quantum cryptography with hybrid orbital-angular-momentum states through 25 km of ring-core fiber: A proof-of-concept demonstration,” *Physical Review Applied*, vol. 15, no. 6, p. 064034, 2021.
- [130] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, “Quantum cryptography using entangled photons in energy-time bell states,” *Physical Review Letters*, vol. 84, no. 20, p. 4737, 2000.
- [131] R. T. Thew, A. Acin, H. Zbinden, and N. Gisin, “Bell-type test of energy-time entangled qutrits,” *Physical Review Letters*, vol. 93, no. 1, p. 010503, 2004.
- [132] I. Ali-Khan, C. J. Broadbent, and J. C. Howell, “Large-alphabet quantum key distribution using energy-time entangled bipartite states,” *Physical Review Letters*, vol. 98, no. 6, p. 060503, 2007.
- [133] J. Mower, Z. Zhang, P. Desjardins, C. Lee, J. H. Shapiro, and D. Englund, “High-dimensional quantum key distribution using dispersive optics,” *Physical Review A*, vol. 87, no. 6, p. 062322, 2013.
- [134] J. Nunn, L. Wright, C. Söller, L. Zhang, I. Walmsley, and B. Smith, “Large-alphabet time-frequency entangled quantum key distribution by means of time-to-frequency conversion,” *Optics Express*, vol. 21, no. 13, pp. 15959–15973, 2013.

- [135] D. Bunandar, Z. Zhang, J. H. Shapiro, and D. R. Englund, “Practical high-dimensional quantum key distribution with decoy states,” *Physical Review A*, vol. 91, no. 2, p. 022336, 2015.
- [136] M. Y. Niu, F. Xu, J. H. Shapiro, and F. Furrer, “Finite-key analysis for time-energy high-dimensional quantum key distribution,” *Physical Review A*, vol. 94, no. 5, p. 052323, 2016.
- [137] Y. Jo and W. Son, “Key-rate enhancement using qutrit states for quantum key distribution with askew aligned sources,” *Physical Review A*, vol. 94, no. 5, p. 052316, 2016.
- [138] W.-Y. Hwang, H.-Y. Su, and J. Bae, “N-dimensional measurement-device-independent quantum key distribution with N+1 un-characterized sources: zero quantum-bit-error-rate case,” *Scientific Reports*, vol. 6, no. 1, p. 30036, 2016.
- [139] L. Dellantonio, A. S. Sørensen, and D. Bacco, “High-dimensional measurement-device-independent quantum key distribution on two-dimensional subspaces,” *Physical Review A*, vol. 98, no. 6, p. 062301, 2018.
- [140] K. Sulimany, G. Pelc, R. Dudkiewicz, S. Korenblit, H. S. Eisenberg, Y. Bromberg, and M. Ben-Or, “High-dimensional coherent one-way quantum key distribution,” *npj Quantum Information*, vol. 11, no. 1, p. 16, 2025.
- [141] Y. Zhou, C. Zhou, Y. Wang, Y.-F. Lu, M.-S. Jiang, X.-X. Zhang, and W.-S. Bao, “Finite-key analysis of practical time-bin high-dimensional quantum key distribution with afterpulse effect,” *Chinese Physics B*, vol. 31, no. 8, p. 080303, 2022.
- [142] I. Vagniluca, B. Da Lio, D. Rusca, D. Cozzolino, Y. Ding, H. Zbinden, A. Zavatta, L. K. Oxenløwe, and D. Bacco, “Efficient time-bin encoding for practical high-dimensional quantum key distribution,” *Physical Review Applied*, vol. 14, no. 1, p. 014051, 2020.
- [143] H. Iqbal and W. O. Krawec, “High-dimensional semiquantum cryptography,” *IEEE Transactions on Quantum Engineering*, vol. 1, pp. 1–17, 2020.
- [144] J. C. Chapman, C. C. Lim, and P. G. Kwiat, “Hyperentangled time-bin and polarization quantum key distribution,” *Physical Review Applied*, vol. 18, no. 4, p. 044027, 2022.

- [145] B. Da Lio, D. Cozzolino, N. Biagi, Y. Ding, K. Rottwitt, A. Zavatta, D. Bacco, and L. K. Oxenløwe, “Path-encoded high-dimensional quantum communication over a 2-km multicore fiber,” *npj Quantum Information*, vol. 7, no. 1, p. 63, 2021.
- [146] K.-C. Chang, M. C. Sarihan, X. Cheng, Z. Zhang, and C. W. Wong, “Large-alphabet time-bin quantum key distribution and einstein–podolsky–rosen steering via dispersive optics,” *Quantum Science and Technology*, vol. 9, no. 1, p. 015018, 2023.
- [147] B. Courme, P. Cameron, D. Faccio, S. Gigan, and H. Defienne, “Manipulation and certification of high-dimensional entanglement through a scattering medium,” *PRX Quantum*, vol. 4, no. 1, p. 010308, 2023.
- [148] J. Liu, Z. Lin, D. Liu, X. Feng, F. Liu, K. Cui, Y. Huang, and W. Zhang, “High-dimensional quantum key distribution using energy-time entanglement over 242 km partially deployed fiber,” *Quantum Science and Technology*, vol. 9, no. 1, p. 015003, 2023.
- [149] H. Hajji and M. El Baz, “Qutrit-based semi-quantum key distribution protocol,” *Quantum Information Processing*, vol. 20, no. 1, p. 4, 2021.
- [150] X. Liu, X. Yao, H. Wang, H. Li, Z. Wang, L. You, Y. Huang, and W. Zhang, “Energy-time entanglement-based dispersive optics quantum key distribution over optical fibers of 20 km,” *Applied Physics Letters*, vol. 114, no. 14, 2019.
- [151] Ö. Erkiş, L. Conlon, B. Shajilal, S. Kish, S. Tserkis, Y.-S. Kim, P. K. Lam, and S. M. Assad, “Surpassing the repeaterless bound with a photon-number encoded measurement-device-independent quantum key distribution protocol,” *npj Quantum Information*, vol. 9, no. 1, p. 29, 2023.
- [152] Y. I. Bogdanov, M. Chekhova, S. Kulik, G. Maslennikov, A. Zhukov, C. Oh, and M. Tey, “Qutrit state engineering with biphotons,” *Physical Review Letters*, vol. 93, no. 23, p. 230503, 2004.
- [153] A. V. Burlakov and M. V. Chekhova, “Polarization optics of biphotons,” *Journal of Experimental and Theoretical Physics Letters*, vol. 75, no. 8, pp. 432–438, 2002.
- [154] G. Maslennikov, A. Zhukov, M. Chekhova, and S. Kulik, “Practical realization of the quantum cryptography protocol exploiting polarization encoding in the qutrits,” *arXiv preprint quant-ph/0305115*, 2003.

- [155] P. Sibson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan, *et al.*, “Chip-based quantum key distribution,” *Nature Communications*, vol. 8, no. 1, p. 13984, 2017.
- [156] K. Wei, W. Li, H. Tan, Y. Li, H. Min, W.-J. Zhang, H. Li, L. You, Z. Wang, X. Jiang, *et al.*, “High-speed measurement-device-independent quantum key distribution with integrated silicon photonics,” *Physical Review X*, vol. 10, no. 3, p. 031030, 2020.
- [157] H. Semenenko, P. Sibson, A. Hart, M. G. Thompson, J. G. Rarity, and C. Erven, “Chip-based measurement-device-independent quantum key distribution,” *Optica*, vol. 7, no. 3, pp. 238–242, 2020.
- [158] L. Cao, W. Luo, Y. Wang, J. Zou, R. Yan, H. Cai, Y. Zhang, X. Hu, C. Jiang, W. Fan, *et al.*, “Chip-based measurement-device-independent quantum key distribution using integrated silicon photonic systems,” *Physical Review Applied*, vol. 14, no. 1, p. 011001, 2020.
- [159] L.-C. Kwek, L. Cao, W. Luo, Y. Wang, S. Sun, X. Wang, and A. Q. Liu, “Chip-based quantum key distribution,” *AAPPS Bulletin*, vol. 31, pp. 1–8, 2021.
- [160] Q. Liu, Y. Huang, Y. Du, Z. Zhao, M. Geng, Z. Zhang, and K. Wei, “Advances in chip-based quantum key distribution,” *Entropy*, vol. 24, no. 10, p. 1334, 2022.
- [161] A. Orioux and E. Diamanti, “Recent advances on integrated quantum communications,” *Journal of Optics*, vol. 18, no. 8, p. 083002, 2016.
- [162] C. Ma, W. D. Sacher, Z. Tang, J. C. Mikkelsen, Y. Yang, F. Xu, T. Thiessen, H.-K. Lo, and J. K. Poon, “Silicon photonic transmitter for polarization-encoded quantum key distribution,” *Optica*, vol. 3, no. 11, pp. 1274–1278, 2016.
- [163] F. Raffaelli, G. Ferranti, D. H. Mahler, P. Sibson, J. E. Kennard, A. Santamato, G. Sinclair, D. Bonneau, M. G. Thompson, and J. C. Matthews, “A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers,” *Quantum Science and Technology*, vol. 3, no. 2, p. 025003, 2018.

- [164] S. Gyger, J. Zichi, L. Schweickert, A. W. Elshaari, S. Steinhauer, S. F. Covre da Silva, A. Rastelli, V. Zwiller, K. D. Jöns, and C. Errando-Herranz, “Reconfigurable photonics with on-chip single-photon detectors,” *Nature Communications*, vol. 12, no. 1, p. 1408, 2021.
- [165] F. Beutel, H. Gehring, M. A. Wolff, C. Schuck, and W. Pernice, “Detector-integrated on-chip qkd receiver for ghz clock rates,” *npj Quantum Information*, vol. 7, no. 1, p. 40, 2021.
- [166] F. Beutel, F. Brückerohoff-Plückelmann, H. Gehring, V. Kovalyuk, P. Zolotov, G. Goltsman, and W. H. Pernice, “Fully integrated four-channel wavelength-division multiplexed qkd receiver,” *Optica*, vol. 9, no. 10, pp. 1121–1130, 2022.
- [167] L. Feng, M. Zhang, J. Wang, X. Zhou, X. Qiang, G. Guo, and X. Ren, “Silicon photonic devices for scalable quantum information applications,” *Photonics Research*, vol. 10, no. 10, pp. A135–A153, 2022.
- [168] P. Ye, W. Chen, Z.-H. Wang, G.-W. Zhang, Y.-Y. Ding, G.-Z. Huang, Z.-Q. Yin, S. Wang, D.-Y. He, W. Liu, *et al.*, “Transmittance-invariant phase modulator for chip-based quantum key distribution,” *Optics Express*, vol. 30, no. 22, pp. 39911–39921, 2022.
- [169] J. A. Dolphin, T. K. Paraíso, H. Du, R. I. Woodward, D. G. Marangon, and A. J. Shields, “A hybrid integrated quantum key distribution transceiver chip,” *npj Quantum Information*, vol. 9, no. 1, p. 84, 2023.
- [170] J. Chang, J. Gao, I. Esmail Zadeh, A. W. Elshaari, and V. Zwiller, “Nanowire-based integrated photonics for quantum information and quantum sensing,” *Nanophotonics*, vol. 12, no. 3, pp. 339–358, 2023.
- [171] L. Labonté, O. Alibart, V. D’Auria, F. Dautre, J. Etesse, G. Sauder, A. Martin, É. Picholle, and S. Tanzilli, “Integrated photonics for quantum communications and metrology,” *PRX Quantum*, vol. 5, no. 1, p. 010101, 2024.
- [172] D. Bunandar, A. Lentine, C. Lee, H. Cai, C. M. Long, N. Boynton, N. Martinez, C. DeRose, C. Chen, M. Grein, *et al.*, “Metropolitan quantum key distribution with silicon photonics,” *Physical Review X*, vol. 8, no. 2, p. 021009, 2018.
- [173] T. K. Paraíso, I. De Marco, T. Roger, D. G. Marangon, J. F. Dynes, M. Lucamarini, Z. Yuan, and A. J. Shields, “A modulator-free quantum key dis-

- tribution transmitter chip,” *npj Quantum Information*, vol. 5, no. 1, p. 42, 2019.
- [174] M. Avesani, L. Calderaro, M. Schiavon, A. Stanco, C. Agnesi, A. Santamato, M. Zahidy, A. Scriminich, G. Foletto, G. Contestabile, *et al.*, “Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics,” *npj Quantum Information*, vol. 7, no. 1, p. 93, 2021.
- [175] G. Zhang, Z. Zhao, J. Dai, S. Yang, X. Fu, and L. Yang, “Polarization-based quantum key distribution encoder and decoder on silicon photonics,” *Journal of Lightwave Technology*, vol. 40, no. 7, pp. 2052–2059, 2021.
- [176] X. Li, L.-L. Wang, J.-s. Zhang, W. Chen, Y. Wang, D. Wu, and J.-M. An, “Quantum key distribution transmitter chip based on hybrid-integration of silica and lithium niobates,” *Chinese Physics B*, vol. 31, no. 6, p. 064212, 2022.
- [177] K. Wei, X. Hu, Y. Du, X. Hua, Z. Zhao, Y. Chen, C. Huang, and X. Xiao, “Resource-efficient quantum key distribution with integrated silicon photonics,” *Photonics Research*, vol. 11, no. 8, pp. 1364–1372, 2023.
- [178] Y. Ding, D. Bacco, K. Dalgaard, X. Cai, X. Zhou, K. Rottwitt, and L. K. Oxenløwe, “High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits,” *npj Quantum Information*, vol. 3, no. 1, p. 25, 2017.
- [179] M. Zahidy, Y. Liu, D. Cozzolino, Y. Ding, T. Morioka, L. K. Oxenløwe, and D. Bacco, “Photonic integrated chip enabling orbital angular momentum multiplexing for quantum communication,” *Nanophotonics*, vol. 11, no. 4, pp. 821–827, 2022.
- [180] G. Zhang, J. Y. Haw, H. Cai, F. Xu, S. Assad, J. F. Fitzsimons, X. Zhou, Y. Zhang, S. Yu, J. Wu, *et al.*, “An integrated silicon photonic chip platform for continuous-variable quantum key distribution,” *Nature Photonics*, vol. 13, no. 12, pp. 839–842, 2019.
- [181] W. Li, V. Zapatero, H. Tan, K. Wei, H. Min, W.-Y. Liu, X. Jiang, S.-K. Liao, C.-Z. Peng, M. Curty, *et al.*, “Experimental quantum key distribution secure against malicious devices,” *Physical Review Applied*, vol. 15, no. 3, p. 034081, 2021.

- [182] X. Zheng, P. Zhang, R. Ge, L. Lu, G. He, Q. Chen, F. Qu, L. Zhang, X. Cai, Y. Lu, *et al.*, “Heterogeneously integrated, superconducting silicon-photonic platform for measurement-device-independent quantum key distribution,” *Advanced Photonics*, vol. 3, no. 5, pp. 055002–055002, 2021.
- [183] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. Dynes, *et al.*, “The secoqc quantum key distribution network in vienna,” *New Journal of Physics*, vol. 11, no. 7, p. 075001, 2009.
- [184] J. Qiu *et al.*, “Quantum communications leap out of the lab.,” *Nature*, vol. 508, no. 7497, pp. 441–442, 2014.
- [185] J. Yang, Z. Jiang, F. Benthin, J. Hanel, T. Fandrich, R. Joos, S. Bauer, S. Kolatschek, A. Hreibi, E. P. Rugeramigabo, *et al.*, “High-rate intercity quantum key distribution with a semiconductor single-photon source,” *Light: Science & Applications*, vol. 13, no. 1, p. 150, 2024.
- [186] Z.-Q. Yin, F.-Y. Lu, J. Teng, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, “Twin-field protocols: Towards intercity quantum key distribution without quantum repeaters,” *Fundamental Research*, vol. 1, no. 1, pp. 93–95, 2021.
- [187] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng, and L. Hanzo, “The evolution of quantum key distribution networks: On the road to the qinternet,” *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 839–894, 2022.
- [188] A. Hreibi, A.-K. Kniggeendorf, A. Kuhl, J. Kronjäger, H. Schnatz, and S. Kück, “Entanglement-based intercity quantum key distribution: metrology and implementation,” *Measurement: Sensors*, p. 101777, 2025.
- [189] Y.-H. Yang, P.-Y. Li, S.-Z. Ma, X.-C. Qian, K.-Y. Zhang, L.-J. Wang, W.-L. Zhang, F. Zhou, S.-B. Tang, J.-Y. Wang, *et al.*, “All optical metropolitan quantum key distribution network with post-quantum cryptography authentication,” *Optics Express*, vol. 29, no. 16, pp. 25859–25867, 2021.
- [190] H.-T. Zhu, Y. Huang, W.-X. Pan, C.-W. Zhou, J. Tang, H. He, M. Cheng, X. Jin, M. Zou, S. Tang, *et al.*, “Field test of mode-pairing quantum key distribution,” *Optica*, vol. 11, no. 6, pp. 883–888, 2024.
- [191] M. Stanley, Y. Gui, D. Unnikrishnan, S. Hall, and I. Fatadin, “Recent progress in quantum key distribution network deployments and standards,” in *Journal of Physics: Conference Series*, vol. 2416, p. 012001, IOP Publishing, 2022.

- [192] T.-Y. Chen, X. Jiang, S.-B. Tang, L. Zhou, X. Yuan, H. Zhou, J. Wang, Y. Liu, L.-K. Chen, W.-Y. Liu, *et al.*, “Implementation of a 46-node quantum metropolitan area network,” *npj Quantum Information*, vol. 7, no. 1, p. 134, 2021.
- [193] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, *et al.*, “Satellite-to-ground quantum key distribution,” *Nature*, vol. 549, no. 7670, p. 43, 2017.
- [194] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, *et al.*, “Satellite-relayed intercontinental quantum network,” *Physical Review Letters*, vol. 120, no. 3, p. 030501, 2018.
- [195] R. Bedington, J. M. Arrazola, and A. Ling, “Progress in satellite quantum key distribution,” *npj Quantum Information*, vol. 3, no. 1, p. 30, 2017.
- [196] C. Sekga and M. Mafu, “Security of quantum-key-distribution protocol by using the post-selection technique,” *Physics Open*, vol. 7, p. 100075, 2021.
- [197] C. Sekga and M. Mafu, “Three-party reference frame independent quantum key distribution protocol,” *Chinese Physics B*, vol. 30, no. 12, p. 120301, 2021.
- [198] C. Sekga and M. Mafu, “Reference frame independent twin field quantum key distribution with source flaws,” *Journal of Physics Communications*, vol. 5, no. 4, p. 045008, 2021.
- [199] C. Sekga, M. Mafu, and M. Senekane, “High-dimensional quantum key distribution implemented with biphotons,” *Scientific Reports*, vol. 13, no. 1, p. 1229, 2023.
- [200] C. Sekga and M. Mafu, “Measurement device-independent quantum key distribution with vortex vector modes under diverse weather conditions,” 2023.
- [201] R. Renner, “Security of quantum key distribution,” *International Journal of Quantum Information*, vol. 6, no. 01, pp. 1–127, 2008.
- [202] W. Heisenberg, *The physical principles of the quantum theory*. Courier Corporation, 1949.
- [203] G. S. Vernam, “Cipher printing telegraph systems: For secret wire and radio telegraphic communications,” *Journal of the AIEE*, vol. 45, no. 2, pp. 109–115, 1926.

- [204] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim, “The universal composable security of quantum key distribution,” in *Theory of Cryptography: Second Theory of Cryptography Conference, TCC 2005, Cambridge, MA, USA, February 10-12, 2005. Proceedings 2*, pp. 386–406, Springer, 2005.
- [205] R. Renner and R. König, “Universally composable privacy amplification against quantum adversaries,” in *Theory of Cryptography Conference*, pp. 407–425, Springer, 2005.
- [206] J. Müller-Quade and R. Renner, “Composability in quantum cryptography,” *New Journal of Physics*, vol. 11, no. 8, p. 085006, 2009.
- [207] V. Scarani and R. Renner, “Security bounds for quantum cryptography with finite resources,” in *Workshop on Quantum Computation, Communication, and Cryptography*, pp. 83–95, Springer, 2008.
- [208] I. Devetak and A. Winter, “Distillation of secret key and entanglement from quantum states,” in *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 461, pp. 207–235, The Royal Society, 2005.
- [209] R. Y. Cai and V. Scarani, “Finite-key analysis for practical implementations of quantum key distribution,” *New Journal of Physics*, vol. 11, no. 4, p. 045024, 2009.
- [210] R. Renner, “Security of quantum key distribution,” *International Journal of Quantum Information*, vol. 6, no. 01, pp. 1–127, 2008.
- [211] R. Renner and J. I. Cirac, “de finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography,” *Physical Review Letters*, vol. 102, no. 11, p. 110504, 2009.
- [212] M. Christandl, R. König, and R. Renner, “Postselection technique for quantum channels with applications to quantum cryptography,” *Physical Review Letters*, vol. 102, no. 2, p. 020504, 2009.
- [213] R. Renner, “Simplifying information-theoretic arguments by post-selection,” in *Quantum Cryptography and Computing*, pp. 66–75, IOS Press, 2010.
- [214] P. J. Coles, M. Berta, M. Tomamichel, and S. Wehner, “Entropic uncertainty relations and their applications,” *Reviews of Modern Physics*, vol. 89, no. 1, p. 015002, 2017.

- [215] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, “The uncertainty principle in the presence of quantum memory,” *Nature Physics*, vol. 6, no. 9, pp. 659–662, 2010.
- [216] P. J. Coles, L. Yu, V. Gheorghiu, and R. B. Griffiths, “Information-theoretic treatment of tripartite systems and quantum channels,” *Physical Review A*, vol. 83, no. 6, p. 062338, 2011.
- [217] M. Tomamichel and R. Renner, “Uncertainty relation for smooth entropies,” *Physical Review Letters*, vol. 106, no. 11, p. 110506, 2011.
- [218] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, “Tight finite-key analysis for quantum cryptography,” *Nature Communications*, vol. 3, no. 1, pp. 1–6, 2012.
- [219] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, “Leftover hashing against quantum side information,” *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 5524–5535, 2011.
- [220] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” *Reviews of Modern Physics*, vol. 74, pp. 145–195, 2002.
- [221] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, “New high-intensity source of polarization-entangled photon pairs,” *Physical Review Letters*, vol. 75, no. 24, p. 4337, 1995.
- [222] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, “The security of practical quantum key distribution,” *Rev. Mod. Phys.*, vol. 81, pp. 1301–1350, 2009.
- [223] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, “Practical decoy state for quantum key distribution,” *Physical Review A*, vol. 72, no. 1, p. 012326, 2005.
- [224] K. Tamaki and H.-K. Lo, “Unconditionally secure key distillation from multiphotons,” *Physical Review A*, vol. 73, no. 1, p. 010302, 2006.
- [225] H.-L. Yin, Y. Fu, and Z.-B. Chen, “Practical quantum digital signature,” *Physical Review A*, vol. 93, no. 3, p. 032316, 2016.
- [226] H.-L. Yin, Y. Fu, H. Liu, Q.-J. Tang, J. Wang, L.-X. You, W.-J. Zhang, S.-J. Chen, Z. Wang, Q. Zhang, *et al.*, “Experimental quantum digital signature over 102 km,” *Physical Review A*, vol. 95, no. 3, p. 032334, 2017.

- [227] X. Fang-Xing, W. Shuang, H. Zheng-Fu, and G. Guang-Can, “Passive decoy state SARG04 quantum-key-distribution with practical photon-number resolving detectors,” *Chinese Physics B*, vol. 19, no. 10, p. 100312, 2010.
- [228] L. Jing-Bo and F. Xi-Ming, “Non-orthogonal decoy-state quantum key distribution,” *Chinese Physics Letters*, vol. 23, no. 4, p. 775, 2006.
- [229] H.-P. Hu, J.-D. Wang, Y.-X. Huang, S.-H. Liu, and W. Lu, “Non-orthogonal decoy-state quantum key distribution based on conditionally prepared down-conversion source,” *Acta Physica Sinica*, vol. 59, no. 1, pp. 287–292, 2010.
- [230] H.-L. Yin, Y. Fu, Y. Mao, and Z.-B. Chen, “Security of quantum key distribution with multiphoton components,” *Scientific Reports*, vol. 6, no. 1, p. 29482, 2016.
- [231] K. Karabo, C. Sekga, C. Kissack, M. Mafu, and F. Petruccione, “A novel quantum key distribution resistant against large-pulse attacks,” *IET Quantum Communication*, vol. 5, no. 3, pp. 282–290, 2024.
- [232] B. Djaouida and S. Ali, “Theoretical and simulation investigation of practical qkd for both bb84 and sarg04 protocols,” *International Journal of Quantum Information*, vol. 22, no. 04, p. 2350050, 2024.
- [233] H. Nian, Y.-F. Nie, C.-M. Zhang, and L.-L. Lu, “Analysis of the one-decoy-state sarg04 quantum cryptography protocol in the presence of afterpulse effects,” *Communications in Theoretical Physics*, vol. 76, no. 6, p. 065101, 2024.
- [234] Y.-C. Jeong, Y.-S. Kim, and Y.-H. Kim, “Effects of depolarizing quantum channels on BB84 and SARG04 quantum cryptography protocols,” *Laser Physics*, vol. 21, no. 8, pp. 1438–1442, 2011.
- [235] Y.-C. Jeong, Y.-S. Kim, and Y.-H. Kim, “An experimental comparison of BB84 and SARG04 quantum key distribution protocols,” *Laser Physics Letters*, vol. 11, no. 9, p. 095201, 2014.
- [236] T. Meyer, H. Kampermann, M. Kleinmann, and D. Bruß, “Finite key analysis for symmetric attacks in quantum key distribution,” *Physical Review A*, vol. 74, no. 4, p. 042340, 2006.
- [237] V. Scarani and R. Renner, “Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way post-processing,” *Physical Review Letters*, vol. 100, no. 20, p. 200501, 2008.

- [238] L. Sheridan, T. P. Le, and V. Scarani, “Finite-key security against coherent attacks in quantum key distribution,” *New Journal of Physics*, vol. 12, no. 12, p. 123019, 2010.
- [239] M. Mafu, K. Garapo, and F. Petruccione, “Finite-size key in the Bennett 1992 quantum-key-distribution protocol for rényi entropies,” *Physical Review A*, vol. 88, no. 6, p. 062306, 2013.
- [240] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, “Finite-key analysis for measurement-device-independent quantum key distribution,” *Nature Communications*, vol. 5, no. 1, pp. 1–7, 2014.
- [241] M. Mafu, K. Garapo, and F. Petruccione, “Finite-key-size security of the Phoenix-Barnett-Chefles 2000 quantum-key-distribution protocol,” *Physical Review A*, vol. 90, no. 3, p. 032308, 2014.
- [242] M. Lucamarini, K. Patel, J. Dynes, B. Fröhlich, A. Sharpe, A. Dixon, Z. Yuan, R. Pentty, and A. Shields, “Efficient decoy-state quantum key distribution with quantified security,” *Optics Express*, vol. 21, no. 21, pp. 24550–24565, 2013.
- [243] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, “Concise security bounds for practical decoy-state quantum key distribution,” *Physical Review A*, vol. 89, no. 2, p. 022307, 2014.
- [244] C. Zhou, W.-S. Bao, H.-W. Li, Y. Wang, Y. Li, Z.-Q. Yin, W. Chen, and Z.-F. Han, “Tight finite-key analysis for passive decoy-state quantum key distribution under general attacks,” *Physical Review A*, vol. 89, no. 5, p. 052328, 2014.
- [245] Y. Wang, W.-S. Bao, C. Zhou, M.-S. Jiang, and H.-W. Li, “Tight finite-key analysis of a practical decoy-state quantum key distribution with unstable sources,” *Physical Review A*, vol. 94, no. 3, p. 032335, 2016.
- [246] Y. Wang, W.-S. Bao, C. Zhou, M.-S. Jiang, and H.-W. Li, “Finite-key analysis of practical decoy-state measurement-device-independent quantum key distribution with unstable sources,” *Journal of the Optical Society of America B*, vol. 36, no. 3, pp. B83–B91, 2019.
- [247] H.-L. Yin, M.-G. Zhou, J. Gu, Y.-M. Xie, Y.-S. Lu, and Z.-B. Chen, “Tight security bounds for decoy-state quantum key distribution,” *Scientific Reports*, vol. 10, no. 1, pp. 1–10, 2020.

- [248] V. Zapatero and M. Curty, “Finite-key security of passive quantum key distribution,” *Physical Review Applied*, vol. 21, no. 1, p. 014018, 2024.
- [249] W. Wang and N. Lütkenhaus, “Numerical security proof for the decoy-state bb84 protocol and measurement-device-independent quantum key distribution resistant against large basis misalignment,” *Physical Review Research*, vol. 4, no. 4, p. 043097, 2022.
- [250] J. S. Sidhu, T. Brougham, D. McArthur, R. G. Pousa, and D. K. Oi, “Finite key effects in satellite quantum key distribution,” *npj Quantum Information*, vol. 8, no. 1, p. 18, 2022.
- [251] G. Foletto, F. Picciariello, C. Agnesi, P. Villoresi, and G. Vallone, “Security bounds for decoy-state quantum key distribution with arbitrary photon-number statistics,” *Physical Review A*, vol. 105, no. 1, p. 012603, 2022.
- [252] D. Bunandar, L. C. Govia, H. Krovi, and D. Englund, “Numerical finite-key analysis of quantum key distribution,” *npj Quantum Information*, vol. 6, no. 1, p. 104, 2020.
- [253] A. Leverrier, F. Grosshans, and P. Grangier, “Finite-size analysis of a continuous-variable quantum key distribution,” *Physical Review A*, vol. 81, no. 6, p. 062343, 2010.
- [254] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, “Continuous variable quantum key distribution: finite-key analysis of composable security against coherent attacks,” *Physical Review Letters*, vol. 109, no. 10, p. 100502, 2012.
- [255] A. Leverrier, R. García-Patrón, R. Renner, and N. J. Cerf, “Security of continuous-variable quantum key distribution against general attacks,” *Physical Review Letters*, vol. 110, no. 3, p. 030502, 2013.
- [256] F. Kanitschar, I. George, J. Lin, T. Upadhyaya, and N. Lütkenhaus, “Finite-size security for discrete-modulated continuous-variable quantum key distribution protocols,” *PRX Quantum*, vol. 4, no. 4, p. 040306, 2023.
- [257] T. Moroder, M. Curty, C. C. W. Lim, H. Zbinden, N. Gisin, *et al.*, “Security of distributed-phase-reference quantum key distribution,” *Physical Review Letters*, vol. 109, no. 26, p. 260501, 2012.

- [258] H.-K. Lo, “Proof of unconditional security of six-state quantum key distribution scheme,” *Quantum Information and Computation*, vol. 1, no. 2, pp. 81–94, 2001.
- [259] P. W. Shor and J. Preskill, “Simple proof of security of the BB84 quantum key distribution protocol,” *Physical Review Letters*, vol. 85, no. 2, p. 441, 2000.
- [260] A. Chefles, “Unambiguous discrimination between linearly dependent states with multiple copies,” *Physical Review A*, vol. 64, no. 6, p. 062305, 2001.
- [261] A. Acin, N. Gisin, and V. Scarani, “Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks,” *Physical Review A*, vol. 69, no. 1, p. 012309, 2004.
- [262] A. Chefles, “Unambiguous discrimination between linearly independent quantum states,” *Physics Letters A*, vol. 239, no. 6, pp. 339–347, 1998.
- [263] R. Renner, “Symmetry of large physical systems implies independence of subsystems,” *Nature Physics*, vol. 3, no. 9, pp. 645–649, 2007.
- [264] S. Ali and B. Djaouda, “Optimizing quantum key distribution protocols using decoy state techniques and experimental validation,” *Engineering, Technology & Applied Science Research*, vol. 14, no. 4, pp. 15133–15140, 2024.
- [265] J. Wabnig, D. Bitauld, H. Li, A. Laing, J. O’Brien, and A. Niskanen, “Demonstration of free-space reference frame independent quantum key distribution,” *New Journal of Physics*, vol. 15, no. 7, p. 073001, 2013.
- [266] J. Ribeiro, G. Murta, and S. Wehner, “Fully device-independent conference key agreement,” *Physical Review A*, vol. 97, no. 2, p. 022307, 2018.
- [267] H.-L. Yin and Z.-B. Chen, “Finite-key analysis for twin-field quantum key distribution with composable security,” *Scientific Reports*, vol. 9, no. 1, pp. 1–9, 2019.
- [268] C.-H. F. Fung, X. Ma, and H. Chau, “Practical issues in quantum-key-distribution postprocessing,” *Physical Review A*, vol. 81, no. 1, p. 012318, 2010.
- [269] H.-K. Lo, H. F. Chau, and M. Ardehali, “Efficient quantum key distribution scheme and a proof of its unconditional security,” *Journal of Cryptology*, vol. 18, no. 2, pp. 133–165, 2005.

- [270] S. Pironio, A. Acin, N. Brunner, N. Gisin, S. Massar, and V. Scarani, “Device-independent quantum key distribution secure against collective attacks,” *New Journal of Physics*, vol. 11, no. 4, p. 045021, 2009.
- [271] Z. Wei, W. Wang, Z. Zhang, M. Gao, Z. Ma, and X. Ma, “Decoy-state quantum key distribution with biased basis choice,” *Scientific Reports*, vol. 3, no. 1, p. 2453, 2013.
- [272] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, *et al.*, “Entanglement-based quantum communication over 144 km,” *Nature Physics*, vol. 3, no. 7, pp. 481–486, 2007.
- [273] F. Wong, J. Shapiro, and T. Kim, “Efficient generation of polarization-entangled photons in a nonlinear crystal,” *Laser Physics*, vol. 16, pp. 1517–1524, 2006.
- [274] X. Li, P. L. Voss, J. E. Sharping, and P. Kumar, “Optical-fiber source of polarization-entangled photons in the 1550 nm telecom band,” *Physical Review Letters*, vol. 94, no. 5, p. 053601, 2005.
- [275] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, “Quantum cryptography with entangled photons,” *Physical Review Letters*, vol. 84, no. 20, p. 4729, 2000.
- [276] X. Guo, C.-l. Zou, C. Schuck, H. Jung, R. Cheng, and H. X. Tang, “Parametric down-conversion photon-pair source on a nanophotonic chip,” *Light: Science & Applications*, vol. 6, no. 5, pp. e16249–e16249, 2017.
- [277] J. W. Silverstone, D. Bonneau, K. Ohira, N. Suzuki, H. Yoshida, N. Iizuka, M. Ezaki, C. M. Natarajan, M. G. Tanner, R. H. Hadfield, *et al.*, “On-chip quantum interference between silicon photon-pair sources,” *Nature Photonics*, vol. 8, no. 2, pp. 104–108, 2014.
- [278] R. Horn, P. Abolghasem, B. J. Bijlani, D. Kang, A. Helmy, and G. Weihs, “Monolithic source of photon pairs,” *Physical Review Letters*, vol. 108, no. 15, p. 153605, 2012.
- [279] J. Wang, X. Qin, Y. Jiang, X. Wang, L. Chen, F. Zhao, Z. Wei, and Z. Zhang, “Experimental demonstration of polarization encoding quantum key distribution system based on intrinsically stable polarization-modulated units,” *Optics Express*, vol. 24, no. 8, pp. 8302–8309, 2016.

- [280] Y. Du, X. Zhu, X. Hua, Z. Zhao, X. Hu, Y. Qian, X. Xiao, and K. Wei, “Silicon-based decoder for polarization-encoding quantum key distribution,” *Chip*, vol. 2, no. 1, p. 100039, 2023.
- [281] C. Agnesi, M. Avesani, L. Calderaro, A. Stanco, G. Foletto, M. Zahidy, A. Scriminich, F. Vedovato, G. Vallone, and P. Villoresi, “Simple quantum key distribution with qubit-based synchronization and a self-compensating polarization encoder,” *Optica*, vol. 7, no. 4, pp. 284–290, 2020.
- [282] N. K. Pathak, S. Chaudhary, Sangeeta, and B. Kanseri, “Phase encoded quantum key distribution up to 380 km in standard telecom grade fiber enabled by baseline error optimization,” *Scientific Reports*, vol. 13, no. 1, p. 15868, 2023.
- [283] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, “Twin-field quantum key distribution with large misalignment error,” *Physical Review A*, vol. 98, no. 6, p. 062323, 2018.
- [284] Z.-W. Yu, X.-L. Hu, C. Jiang, H. Xu, and X.-B. Wang, “Sending-or-not-sending twin-field quantum key distribution in practice,” *Scientific Reports*, vol. 9, no. 1, pp. 1–8, 2019.
- [285] M. Curty, K. Azuma, and H.-K. Lo, “Simple security proof of twin-field type quantum key distribution protocol,” *npj Quantum Information*, vol. 5, no. 1, pp. 1–6, 2019.
- [286] M. Minder, M. Pittaluga, G. Roberts, M. Lucamarini, J. Dynes, Z. Yuan, and A. Shields, “Experimental quantum key distribution beyond the repeaterless secret key capacity,” *Nature Photonics*, vol. 13, no. 5, pp. 334–338, 2019.
- [287] S. Wang, D.-Y. He, Z.-Q. Yin, F.-Y. Lu, C.-H. Cui, W. Chen, Z. Zhou, G.-C. Guo, and Z.-F. Han, “Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system,” *Physical Review X*, vol. 9, no. 2, p. 021046, 2019.
- [288] Y. Liu, Z.-W. Yu, W. Zhang, J.-Y. Guan, J.-P. Chen, C. Zhang, X.-L. Hu, H. Li, C. Jiang, J. Lin, *et al.*, “Experimental twin-field quantum key distribution through sending or not sending,” *Physical Review Letters*, vol. 123, no. 10, p. 100505, 2019.

- [289] H. Liu, C. Jiang, H.-T. Zhu, M. Zou, Z.-W. Yu, X.-L. Hu, H. Xu, S. Ma, Z. Han, J.-P. Chen, *et al.*, “Field test of twin-field quantum key distribution through sending-or-not-sending over 428 km,” *Physical Review Letters*, vol. 126, no. 25, p. 250502, 2021.
- [290] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, “Device calibration impacts security of quantum key distribution,” *Physical Review Letters*, vol. 107, no. 11, p. 110501, 2011.
- [291] J.-Y. Liu, H.-J. Ding, C.-M. Zhang, S.-P. Xie, and Q. Wang, “Practical phase-modulation stabilization in quantum key distribution via machine learning,” *Physical Review A*, vol. 12, no. 1, p. 014059, 2019.
- [292] X. Ma, “Quantum cryptography: theory and practice,” *arXiv preprint arXiv:0808.1385*, 2008.
- [293] S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, and Z. Wang, “Multichannel SNSPD system with high detection efficiency at telecommunication wavelength,” *Optics Letters*, vol. 35, no. 13, pp. 2133–2135, 2010.
- [294] Y. Nambu, S. Takahashi, K. Yoshino, A. Tanaka, M. Fujiwara, M. Sasaki, A. Tajima, S. Yoroze, and A. Tomita, “Efficient and low-noise single-photon avalanche photodiode for 1.244-GHz clocked quantum key distribution,” *Optics Express*, vol. 19, no. 21, pp. 20531–20541, 2011.
- [295] 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*, vol. 19, no. 11, pp. 10387–10409, 2011.
- [296] X. Ma, P. Zeng, and H. Zhou, “Phase-matching quantum key distribution,” *Physical Review X*, vol. 8, no. 3, p. 031043, 2018.
- [297] K. Tamaki, H.-K. Lo, C.-H. F. Fung, and B. Qi, “Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw,” *Physical Review A*, vol. 85, no. 4, p. 042307, 2012.
- [298] K. Tamaki, H.-K. Lo, W. Wang, and M. Lucamarini, “Information theoretic security of quantum key distribution overcoming the repeaterless secret key capacity bound,” *arXiv preprint arXiv:1805.05511*, 2018.

- [299] J. Lin and N. Lütkenhaus, “Simple security analysis of phase-matching measurement-device-independent quantum key distribution,” *Physical Review A*, vol. 98, no. 4, p. 042332, 2018.
- [300] I. Bregman, D. Aharonov, M. Ben-Or, and H. Eisenberg, “Simple and secure quantum key distribution with biphotons,” *Physical Review A*, vol. 77, no. 5, p. 050301, 2008.
- [301] H. Chernoff, “A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations,” *The Annals of Mathematical Statistics*, vol. 23, no. 4, pp. 493–507, 1952.
- [302] L. Sheridan and V. Scarani, “Security proof for quantum key distribution using qudit systems,” *Physical Review A*, vol. 82, no. 3, p. 030301, 2010.
- [303] E. Moreva, G. Maslennikov, S. Straupe, and S. Kulik, “Realization of four-level qudits using biphotons,” *Physical Review Letters*, vol. 97, no. 2, p. 023602, 2006.
- [304] A. Z. Goldberg, “Quantum polarimetry,” in *Progress in Optics*, vol. 67, pp. 185–274, Elsevier, 2022.
- [305] P.-C. Ma, G.-B. Chen, X.-W. Li, and Y.-B. Zhan, “Cyclic controlled remote state preparation in the three-dimensional system,” *Laser Physics Letters*, vol. 19, no. 11, p. 115204, 2022.
- [306] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, *et al.*, “Detecting single infrared photons with 93% system efficiency,” *Nature Photonics*, vol. 7, no. 3, pp. 210–214, 2013.
- [307] B. Ndagano, I. Nape, B. Perez-Garcia, S. Scholes, R. I. Hernandez-Aranda, T. Konrad, M. P. Lavery, and A. Forbes, “A deterministic detector for vector vortex states,” *Scientific Reports*, vol. 7, no. 1, p. 13882, 2017.
- [308] G. A. Tyler and R. W. Boyd, “Influence of atmospheric turbulence on the propagation of quantum states of light carrying orbital angular momentum,” *Optics Letters*, vol. 34, no. 2, pp. 142–144, 2009.
- [309] X. Ma and M. Razavi, “Alternative schemes for measurement-device-independent quantum key distribution,” *Physical Review A*, vol. 86, no. 6, p. 062319, 2012.

- [310] R. Uijlenhoet, J.-M. Cohard, and M. Gosset, “Path-average rainfall estimation from optical extinction measurements using a large-aperture scintillometer,” *Journal of Hydrometeorology*, vol. 12, no. 5, pp. 955–972, 2011.
- [311] C. W. Ulbrich and D. Atlas, “Extinction of visible and infrared radiation in rain: Comparison of theory and experiment,” *Journal of Atmospheric and Oceanic Technology*, vol. 2, no. 3, pp. 331–339, 1985.
- [312] D. A. de Wolf, “On the laws-parsons distribution of raindrop sizes,” *Radio Science*, vol. 36, no. 4, pp. 639–642, 2001.
- [313] C. F. Bohren and D. R. Huffman, *Absorption and scattering of light by small particles*. John Wiley & Sons, 2008.
- [314] H. C. Hulst and H. C. van de Hulst, *Light scattering by small particles*. Courier Corporation, 1981.
- [315] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2002.
- [316] U. Fano, “Description of states in quantum mechanics by density matrix and operator techniques,” *Reviews of Modern Physics*, vol. 29, no. 1, p. 74, 1957.
- [317] T. F. Jordan, *Linear operators for quantum mechanics*. Courier Corporation, 2012.
- [318] A. Einstein, B. Podolsky, and N. Rosen, “Can quantum-mechanical description of physical reality be considered complete?,” *Physical Review A*, vol. 47, no. 10, p. 777, 1935.
- [319] J. S. Bell, “On the Einstein Podolsky Rosen paradox,” *Physics Physique Fizika*, vol. 1, no. 3, p. 195, 1964.
- [320] D. M. Greenberger, M. A. Horne, and A. Zeilinger, “Going beyond Bell’s theorem,” in *Bell’s theorem, quantum theory and conceptions of the universe*, pp. 69–72, Springer, 1989.
- [321] J. Preskill, “Lecture notes for physics 229: Quantum information and computation,” *California Institute of Technology*, vol. 16, no. 1, pp. 1–8, 1998.
- [322] J. Audretsch, *Entangled systems: new directions in quantum physics*. John Wiley & Sons, 2008.

- [323] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*. Cambridge University, 2000.
- [324] T. Cover and J. Thomas, *Elements of Information Theory*. John Wiley and Sons, 1991.
- [325] M. M. Wilde, “From classical to quantum Shannon theory,” *arXiv preprint arXiv:1106.1445*, 2011.
- [326] C. E. Shannon, “A mathematical theory of communication,” *The Bell system technical journal*, vol. 27, no. 3, pp. 379–423, 1948.
- [327] D. J. MacKay, *Information theory, inference and learning algorithms*. Cambridge university press, 2003.
- [328] J. Preskill, *Lecture Notes for Ph219/CS219: Quantum Information*, ch. 10. California Institute of Technology, 2015.
- [329] A. S. Holevo, “Bounds for the quantity of information transmitted by a quantum communication channel,” *Problemy Peredachi Informatsii*, vol. 9, no. 3, pp. 3–11, 1973.
- [330] X. Ma, C.-H. F. Fung, and H.-K. Lo, “Quantum key distribution with entangled photon sources,” *Physical Review A*, vol. 76, no. 1, p. 012307, 2007.
- [331] C.-M. Zhang, J.-R. Zhu, and Q. Wang, “Practical reference-frame-independent quantum key distribution systems against the worst relative rotation of reference frames,” *Journal of Physics Communications*, vol. 2, no. 5, p. 055029, 2018.
- [332] M. Koashi, “Complementarity, distillable secret key, and distillable entanglement,” *arXiv preprint arXiv:0704.3661*, 2007.
- [333] M. Koashi, “Simple security proof of quantum key distribution based on complementarity,” *New Journal of Physics*, vol. 11, no. 4, p. 045018, 2009.
- [334] K. Azuma, “Weighted sums of certain dependent random variables,” *Tohoku Mathematical Journal, Second Series*, vol. 19, no. 3, pp. 357–367, 1967.