Beating Quantum Hackers

by

Feihu Xu

A thesis submitted in conformity with the requirements for the degree of Doctor of Philosophy
Graduate Department of Electrical & Computer Engineering
University of Toronto

Copyright © 2014 by Feihu Xu
Abstract

Beating Quantum Hackers

Feihu Xu
Doctor of Philosophy
Graduate Department of Electrical & Computer Engineering
University of Toronto
2014

Cryptography plays a key role in today’s digital society. The most widely used encryption method is the so-called public-key algorithm, but its security relies on unproven computational assumptions. In contrast, quantum key distribution (QKD) is an unbreakable encryption algorithm. Indeed, in theory, QKD has been proven to provide information-theoretic security rigorously based on the laws of physics and information theory.

Despite the beauty of QKD theory, in practice, QKD still suffers from practical side-channel attacks due to the imperfections of real-life implementations. Such discrepancy between the theory and the practice is fatal to the security of a QKD system. This thesis addresses a number of the discrepancies including the detection, the source and the randomness generation in a standard QKD implementation, and it offers efficient countermeasures to resolve these discrepancies.

(I) Detection security: After reviewing recent quantum hacking activities, I find that the imperfect detectors have become the most important security loophole in conventional QKD implementations. To solve this issue, Lo et al. proposed a novel protocol – measurement-device-independent (MDI) QKD – that can remove all detector side-channel attacks. Nonetheless, before MDI-QKD can be applied in real life, it is important to address a number of practical issues. The first part of my Ph.D. research is to investigate MDI-QKD in real-life applications. I have proposed practical protocols and designed methodologies to optimize parameters for MDI-QKD. Also, my co-workers and I have conducted the first rigorous security proof in the finite-key regime. Moreover, my co-workers and I have experimentally demonstrated a polarization-encoding MDI-QKD by using commercial off-the-shelf components. To further improve the performance of MDI-QKD, I have proposed a long-distance protocol by introducing entanglement photon sources in the middle. These results allow MDI-QKD mature enough to be implemented...
in real-life, and they pave the way for the realization of a future QKD network with an untrusted network server.

(II) **Source security:** Based on the framework of MDI-QKD, the only security issue left is the source. Thus, my second part of Ph.D. research focuses on the source security. Specifically, to solve the security loophole due to the imperfect encoder, I have implemented a recent theoretical protocol, which enables QKD loss-tolerant to source flaws. I have demonstrated both BB84 and the three-state protocol with decoy states on top of a commercial QKD system over 50 km standard telecom fiber. This experiment for the first time shows secure QKD with imperfect state preparations at long distances and achieves rigorous finite-key security bounds for decoy-state QKD against general attacks in the universally composable framework.

(III) **Randomness security:** Besides the imperfect encoders, another vulnerable part in the source is the ability to generate true randomness. My final research topic is to study the generation of true randomness for practical applications. I have experimentally demonstrated an ultrafast quantum random number generator (QRNG) at a rate over 6 Gbit/s based on the quantum phase noise of a laser. Moreover, I have developed a compact and cost-effective prototype, which has a real-time generation rate of 1 Gbit/s with excellent stability. The simplicity and speed of my prototype prove the feasibility of a robust, low-cost, and fast QRNG.

In summary, MDI-QKD enables new scientific developments in the field of quantum cryptography. This thesis solves the major practical issues in the implementation of MDI-QKD, and it allows MDI-QKD mature enough to be implemented in real-life. The combination of MDI-QKD, imperfect sources, and QRNG consists of the foundation of a future practical side-channel-free QKD protocol. This protocol is feasible with current technology. The success of this protocol can substitute current classical cryptosystems by offering people an unconditionally secure infrastructure, which will be the ultimate dream for researchers in secure communication.
Acknowledgements

I would like to take this opportunity to thank various people for making my Ph.D. study in the University of Toronto an exciting experience. First and foremost, I owe my deepest gratitude to my supervisors, Prof. Hoi-Kwong Lo and Prof. Li Qian, who have supported me with their patience and knowledge during my study. I am grateful to them for many useful discussions that motivated me.

I would extend my thanks to Dr. Bing Qi, Prof. M. Curty, and Prof. V. Makarov, who provide many invaluable suggestions for my research as well as for my future career. It has been a great honor to work with them. Special thanks are extended to Prof. Deepa Kundur, Prof. Amr Helmy, Prof. Joyce Poon, Prof. Lacra Pavel for their time and willingness to serve on my thesis committee. Particularly, I am very grateful to Dr. Charles H. Bennett for his time in studying my work and for being my thesis examiner. It is a great honour to have the founder of QKD examining my thesis.

Next, it is a pleasure to thank a friendly and cheerful group of fellow students, including Olinka Bedroya, Viacheslav Burenkov, Kyle Cheng, Dr. Wei Cui, Song Gao, Dongpeng Kang, Dr. Hoi-Kwan Lau, Zhongfa Liao, Jason Ng, Zhiyuan Tang, He Xu, Ke Xu, Dr. Fei Ye, Eric Zhu, Yiwei Zhang for many stimulating discussions. Also, I want to thank the summer students, including David Baik, Shun Kawakami, Piotr Roztocki, Wenyuan Wan, Jeff Zheng, for the help on my research projects. Furthermore, I have largely benefited from the inspiring discussions with many outstanding scientists. In particular, I would like to thank Juan Miguel Arrazola, Dr. Koji Azuma, Prof. Thomas Jennewein, Prof. Norbert Lütkenhaus, Dr. Charles Ci Wen Lim, Prof. Xiongfeng Ma, Prof. Jeffrey Shapiro, Dr. Shihai Sun, Dr. Kiyoshi Tamaki, Dr. Franco Wong, Dr. Christian Weedbrook, and Prof. Hugo Zbinden.

I also thank the Paul Biringer Graduate Scholarship, the Shahid U.H. Qureshi Memorial Scholarship and the OGS VISA award for financial support.

Finally, and most importantly, I am very grateful to my family for their endless encouragement and support. Specially, I thank my mother-in-law for her care in Toronto. This thesis is dedicated to my dear wife, Alice Shan.
Contents

1 Introduction ............................................................. 1
   1.1 Motivation ......................................................... 1
      1.1.1 Quantum Key Distribution (QKD) ......................... 1
      1.1.2 Quantum hacking against practical QKD .............. 2
      1.1.3 Countermeasures against quantum hacking .......... 3
      1.1.4 Security issues in the source ........................ 4
   1.2 Highlight and Outline ........................................... 5
   1.3 Journal publications related to this thesis ............... 7

2 Elements of practical QKD .......................................... 9
   2.1 BB84 protocol .................................................... 9
   2.2 Decoy-state protocol ........................................11
   2.3 Basic QKD components ....................................... 13
      2.3.1 Source ..................................................... 13
      2.3.2 Random number generator .............................. 13
      2.3.3 Quantum channel ....................................... 14
      2.3.4 Detector .................................................. 15
      2.3.5 An example of implementation: plug-and-play ...... 16
   2.4 Quantum hacking ............................................... 16
      2.4.1 Attacks .................................................... 17
      2.4.2 Possible countermeasures ............................... 20

3 Measurement-device-independent QKD (MDI-QKD) ................ 23
   3.1 Time-reversed EPR protocol .................................. 23
   3.2 MDI-QKD protocol ............................................ 25
   3.3 Secure key rate ............................................... 27
   3.4 Summary ....................................................... 27
4 Decoy-state MDI-QKD with finite resources 28
  4.1 Finite number of decoy states ........................................... 28
      4.1.1 Numerical approaches ............................................. 29
      4.1.2 Analytical approaches ........................................... 30
      4.1.3 Simulation .......................................................... 32
  4.2 Finite-key analysis ....................................................... 34
      4.2.1 Security definition .................................................. 35
      4.2.2 Security analysis .................................................. 36
      4.2.3 Parameter estimation .............................................. 37
      4.2.4 Simulation .......................................................... 39
  4.3 Conclusion ................................................................. 42

5 Practical aspects for MDI-QKD 43
  5.1 Practical error sources .................................................. 43
      5.1.1 Polarization misalignment ....................................... 44
      5.1.2 Mode mismatch ..................................................... 45
      5.1.3 Other errors ....................................................... 47
  5.2 Parameter optimization .................................................. 50
      5.2.1 Framework .......................................................... 50
      5.2.2 Local search algorithm .......................................... 51
      5.2.3 Key rate comparison .............................................. 53
  5.3 Asymmetric channel transmission ....................................... 57
      5.3.1 Problem identification ........................................... 57
      5.3.2 Summary of results .............................................. 58
  5.4 Summary ................................................................. 60

6 Experimental polarization-encoding MDI-QKD 62
  6.1 Introduction ............................................................... 62
  6.2 Experimental setup ..................................................... 63
  6.3 Results ................................................................. 65
  6.4 Other related experiments ............................................. 67
  6.5 Conclusion ............................................................... 69

7 Long-distance MDI-QKD with entangled photon sources 70
  7.1 Introduction ............................................................... 70
E  GLLP security analysis with source flaws  119

F  Verify Qubit assumption  121

Bibliography  124
# List of Tables

2.1 List of quantum hacking experiments .............................................. 19
2.2 Assumptions in DI-QKD versus MDI-QKD ........................................ 20
3.1 Post-selection for MDI-QKD ............................................................ 26
4.1 Analytical equations of the two decoy-state protocol for MDI-QKD .... 31
4.2 List of practical parameters for numerical simulations ....................... 32
5.1 Comparison of LSA and exhaustive search ....................................... 52
5.2 Comparison of parameters for a distance of 50 km ............................ 54
5.3 Key rate values with different basis choices .................................... 56
5.4 Optimal intensities for asymmetric MDI-QKD .................................... 60
6.1 Experimental and simulated gains ................................................... 66
6.2 Experimental and simulated QBERs ................................................ 67
6.3 Parameters used to estimate a lower bound of the key rate $R^L$ .......... 67
6.4 Comparison between MDI-QKD demonstrations ............................... 68
7.1 Successful Bell state measurements for Fig. 7.2. ............................... 73
8.1 Parameters measured in ID-500 commercial QKD system .................... 84
8.2 Raw counts and modulation errors for Alice’s phase modulator ............ 84
8.3 Experimental results ................................................................. 87
List of Figures

2.1 A schematic of the BB84 protocol .......................... 10
2.2 Optical setup of commercial plug&play QKD system .......... 17
2.3 Time-shift attack and detector blinding attack ................. 18
2.4 Schematic diagram of device-independent QKD .................. 21

3.1 An equivalent time-reversed EPR based QKD protocol ............. 24
3.2 Schematic diagram of a possible MDI-QKD implementation ..... 25

4.1 Asymptotic key rates with different number of decoy states. .... 33
4.2 Secret key rate in a practical setting with a finite number of signals. 34
4.3 Secret key rate $\ell/N$ as a function of the distance. .......... 40
4.4 Secret key rate as a function of $N$ in zero distance .......... 41

5.1 Model for polarization misalignment .......................... 44
5.2 Polarization misalignment tolerance. .......................... 46
5.3 Model for mode mismatch in the time domain .................. 46
5.4 Mode mismatch tolerance. ...................................... 48
5.5 Background counts tolerance ................................. 49
5.6 Wavelength dependence of a fiber-based beam splitter ........ 49
5.7 Framework for parameter optimization .......................... 51
5.8 Comparison of asymptotic key rates ........................... 53
5.9 Comparison of finite-key rates ................................. 55
5.10 Schematic diagram of asymmetric MDI-QKD .................... 57
5.11 Key rate comparision with 50km channel mismatch ............. 59

6.1 Polarization-encoding MDI-QKD setup .......................... 64

7.1 Schematic diagram of MDI-QKD with heralded quantum memories ... 71
7.2 MDI-QKD with one entangled photon source in the middle ...... 72
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.3</td>
<td>Asymptotic key rate for MDI-QKD with one entangled source</td>
<td>77</td>
</tr>
<tr>
<td>7.4</td>
<td>Key rate with state-of-the-art SPDs</td>
<td>78</td>
</tr>
<tr>
<td>8.1</td>
<td>Experimental raw counts</td>
<td>86</td>
</tr>
<tr>
<td>8.2</td>
<td>Decoy-state QKD with source flaws in a practical setting</td>
<td>88</td>
</tr>
<tr>
<td>9.1</td>
<td>Experimental setup</td>
<td>92</td>
</tr>
<tr>
<td>9.2</td>
<td>Time domain of the raw data</td>
<td>93</td>
</tr>
<tr>
<td>9.3</td>
<td>Noise spectrums</td>
<td>94</td>
</tr>
<tr>
<td>9.4</td>
<td>A simple illustration of min-entropy evaluation</td>
<td>95</td>
</tr>
<tr>
<td>9.5</td>
<td>Autocorrelations of raw-data and post-processed data</td>
<td>96</td>
</tr>
<tr>
<td>9.6</td>
<td>Random test results</td>
<td>97</td>
</tr>
<tr>
<td>9.7</td>
<td>QRNG prototype</td>
<td>98</td>
</tr>
<tr>
<td>10.1</td>
<td>MDI-QKD network</td>
<td>102</td>
</tr>
<tr>
<td>10.2</td>
<td>Commercial QRNG with USB port at a rate of 4 Mbits/s</td>
<td>103</td>
</tr>
<tr>
<td>B.1</td>
<td>Coordinate descent algorithm</td>
<td>111</td>
</tr>
<tr>
<td>B.2</td>
<td>Convexity of key rate function</td>
<td>112</td>
</tr>
<tr>
<td>C.1</td>
<td>Asymptotic key rates of $R_{rig}$ and $R_{est}$</td>
<td>114</td>
</tr>
<tr>
<td>C.2</td>
<td>Optimal $\mu_a$ and $\mu_b$</td>
<td>115</td>
</tr>
<tr>
<td>C.3</td>
<td>Key rate with fixed $x$</td>
<td>116</td>
</tr>
<tr>
<td>F.1</td>
<td>Schematic of an electro-optic phase modulator based on LiNbO$_3$</td>
<td>122</td>
</tr>
</tbody>
</table>
Chapter 1

Introduction

1.1 Motivation

1.1.1 Quantum Key Distribution (QKD)

“A theory is acceptable to us only if it is beautiful.” - Albert Einstein

The introduction of the Internet has enriched many lives by offering users a plethora of information and convenience. However, communication security over the Internet has become an increasingly important issue. The goal of secure communication is to transmit a secret message from the sender (Alice) to the receiver (Bob) such that an eavesdropper (Eve) has no chance to know the message. It is well known that this goal can be achieved using the one-time-pad (OTP) protocol \(1\). This protocol requires that Alice and Bob share a secret key. With such a key, Alice can encrypt the original message (so-called plaintext) into a ciphertext that is unintelligible to Eve. On receiving the ciphertext, Bob can recover the plaintext by using his key. The security of OTP protocol relies solely on the secrecy of the shared key, which renders the task of secure communication equivalent to that of distributing a key securely.

How to distribute a key securely is the duty of quantum key distribution (QKD) \(2, 3\). Unlike the widely used public-key cryptography \(4\), which bases its security on unproven computational assumptions, QKD provides information-theoretically secure key distribu-

\(^1\)The message is represented by a binary string. The key is also a binary string of the same length as the message. For encryption, a bitwise exclusive OR (XOR) is performed between the corresponding bits of the message and the key to generate a ciphertext. Decryption is done by performing a bitwise XOR between the corresponding bits of the ciphertext and the key. For a one-time pad to be secure, the key should not be reused.
Chapter 1. Introduction

2

tion based on the laws of physics. Indeed, if a quantum computer was ever built, many classical public-key schemes, such as the RSA algorithm \[4\], would become insecure \[5\] (see \[6\] for a review on quantum computing). In contrast, QKD will always remain secure, despite the limit of computational and technological power. That is, when combined with the OTP protocol, QKD can be used to achieve perfect secure communication.

The best-known QKD protocol is the BB84 scheme introduced by Bennett and Brassard in 1984 \[2\]. The security of BB84 is based on the quantum no-cloning theorem \[7\]: an unknown quantum state cannot be perfectly copied. This theorem is closely related to Heisenberg’s Uncertainty Principle, which connects the information leaked to Eve with the disturbance observed in Alice’s and Bob’s signals. The larger the amount of information that Eve gains, the larger the disturbance that she causes on the signals. By sacrificing a randomly chosen portion of their data, Alice and Bob can estimate this disturbance (by calculating, for instance, the quantum bit error rate) and thus bound Eve’s information. This bounded information is then removed from the final key by using privacy amplification methods.

In a popular book “The Code Book” \[8\] by Simon Singh, the author suggested that QKD would be the end point of evolution of cryptography. Indeed, in the past two decades, QKD has experienced a dramatic development in both theoretical studies and experimental demonstrations \[9, 10, 11\]. In theory, the principle of QKD has been rigorously proven based on quantum physics and information theory \[10\]. In experiment, QKD has achieved a key generation rate of over 1 Mbits/s \[12, 13\]. The transmission distance has reached over 200 km of optical fibers \[14, 15\]. Various QKD networks have already been built \[13\], and QKD in the 2010 World Cup has been demonstrated. Moreover, commercial QKD products \[16, 17\] have appeared on the market. These products have been used by a number of Swiss banks and Chinese government offices to encrypt critical traffic.

Despite the beauty of QKD theory and the dramatic development of QKD experiment, in practice, QKD still suffers from practical side-channel attacks due to the imperfections of real-life implementations. This security issue will be the major focus of this thesis.

1.1.2 Quantum hacking against practical QKD

In practice, there is a big gap between the assumptions that are typically made in the security proofs of QKD and the actual implementations \[11\]. This gap exists because real devices suffer from inevitable imperfections that can cause them to operate quite
differently from the mathematical models used to prove security. Eve may exploit these imperfections (also called side-channels) and launch quantum hacking that was not covered by the original security proofs.

Is it possible that a small unnoticed imperfection spoils the security of the otherwise carefully designed QKD system? This question has drawn a lot of attention. By exploiting the imperfections in practical QKD, especially those in detectors, researchers have demonstrated various quantum attacks. The first successful quantum hacking against a commercial QKD system was the time-shift attack \cite{18} based on the proposal of \cite{19}. More recently, the phase-remapping attack \cite{20} and the detector-control attack \cite{21, 22} have been implemented against various practical QKD systems. Other attacks have appeared in the literature \cite{23, 24}. These attacks suggest that quantum hacking has become a major problem for real-life security of QKD \cite{11}.

### 1.1.3 Countermeasures against quantum hacking

The first attempt to close the gap between theory and practice was to characterize all specific loopholes and find a countermeasure for each. It is simple to close a known loophole or to prevent a known attack. However, unknown loopholes and unanticipated attacks are difficult to predict and it is impossible to fully characterize real devices and account for all loopholes. Hence, researchers moved to the second approach – device-independent QKD (DI-QKD) \cite{25, 26}. DI-QKD requires no specification of the internal functionality of QKD devices and its security is based on the so-called ‘loophole-free’ Bell inequality test. As long as certain necessary assumptions are satisfied \cite{27}, DI-QKD offers nearly perfect security \cite{28, 29}. Nevertheless, DI-QKD is not practical because it requires near-unity detection efficiency and generates an extremely low key rate \cite{30, 31}. Therefore, no experiment has been demonstrated using DI-QKD.

In this thesis, I focus on the third solution proposed in 2012 \cite{32} (see also \cite{33}). It is called measurement-device-independent QKD (MDI-QKD)\textsuperscript{2}. The security of MDI-QKD is based on the time-reversed EPR QKD protocol \cite{34, 35}. The assumption of MDI-QKD is that both Alice and Bob trust their source. As long as this assumption is satisfied, MDI-QKD can remove all side-channels from the measurement unit, which

\textsuperscript{2}In MDI-QKD, both Alice and Bob are senders, and they transmit signals to an untrusted third party, Charles (or Eve), who is supposed to perform a Bell state measurement. Such a measurement provides post-selected entanglement that can be verified by Alice and Bob. Since the measurement setting is only used to post-select entanglement, it can be treated as an entirely black box. Hence, MDI-QKD can remove all side-channels from the measurement unit, which is the weakest part of a QKD realization.
is the weakest part of a QKD realization [11]. Most importantly, by using the so-called decoy-state protocol [32], MDI-QKD is fully practical with present technology and thus it offers a clear avenue to bridge the gap between theory and practice of QKD.

Nonetheless, in order to apply the proposal of [32] to real-life systems, some loose ends need to be addressed. Specifically, [32] assumes an asymptotic case, where Alice and Bob use an infinite number of decoy-state settings and they have infinite data size. Hence, the open questions include: (i) how many decoy states are needed in practical MDI-QKD? (ii) How can one choose the (optimal) values of the decoy-state intensities? (iii) How does one prove security rigorously in the finite-key case? (iv) How can one implement MDI-QKD experimentally? (v) how can one extend the transmission distance of MDI-QKD?

In Chapter 2–7 of this thesis, I will offer answers for the above questions. I first introduce the basics of QKD and MDI-QKD. Then, I present theoretical proposals about how to implement MDI-QKD with finite resources in practice. Also, some practical aspects related to the implementation will be addressed. Following these theoretical proposals, I present a real experimental demonstration of MDI-QKD. To further improve the performance, I propose a feasible method to extend the transmission distance.

### 1.1.4 Security issues in the source

Based on the framework of MDI-QKD, the only security issue left for Eve is the source. In the source part, until now, former QKD experiments on BB84 [12, 36, 37, 38, 39] have had one important drawback: in the key rate formula, it is commonly assumed that the phase/polarization encoding is done *perfectly*. On one hand, the single-photon components of the four BB84 states are assumed to remain strictly inside a two-dimensional Hilbert space. We call this the *qubit* assumption. In practice, no previous works have verified this assumption. Note that an attack to exploit the higher dimensionality of state preparation has been proposed in [40]. On the other hand, the encoding devices are widely assumed to be perfect without modulation errors. This is a highly unrealistic assumption and may mean that the key generation is actually *not* proven to be secure in previous QKD experiments [12, 36, 37, 38, 39]. What if we use a key rate formula that

---

3Note that this question is highly non-trivial as the requirement of coincidence counts in the original MDI-QKD means that for the same number of signals sent, the raw key rate is lower in MDI-QKD than standard decoy state QKD. Such a lower raw key rate makes the finite size of the transmission a challenge in security proofs.
Chapter 1. Introduction

takes imperfect modulation into account? Standard Gottesman-Lo-Lütkenhaus-Preskill (GLLP) security proof [41] does allow one to do so. Unfortunately, the key rate will be reduced substantially because the GLLP formalism is very conservative and the resulting protocol is not loss-tolerant. Both key rate and distance will suffer greatly from the modulation errors [42]. We remark that source flaw is a serious concern, not only in decoy-state BB84, but also in MDI-QKD [32], quantum coin flipping [43] and blind quantum computing [44].

In Chapter 8 of this thesis, I will address the source-flaw problem by experimentally demonstrating a novel protocol that makes QKD loss-tolerant to source flaws. I present demonstrations on both decoy-state BB84 and three-state protocol on top of a commercial QKD system over 50 km standard telecom fiber. This experiment for the first time shows secure QKD with imperfect state preparations at long distances. The combination of this demonstration and MDI-QKD may incubate the first practical side-channel-free QKD protocol that can be readily implemented with current technology.

1.2 Highlight and Outline

- In Chapter 2, the preliminaries of QKD, including the BB84 protocol, the decoy-state protocol, real-life QKD implementations and quantum hacking are presented.

- In Chapter 3, based on the so-called time-revised EPR QKD protocol, I introduce the basic idea of MDI-QKD, and its implementation setup and secure key formula. This tutorial of MDI-QKD has been published in an invited review article [45]. Some of the contents are based on the original MDI-QKD paper [32].

- In Chapter 4, the decoy-state protocol and the finite-key security analysis for MDI-QKD are discussed. These results have been published in [46, 47]. In [46], I am the first author. I investigated practical decoy-state methods with one, two and three decoy states. Experimentalist can readily implement MDI-QKD by using my decoy-state methods. In [47], I am the second author. My contribution is to apply the decoy-state method into the finite-key security analysis of MDI-QKD, and to perform the numerical simulation to evaluate its performance. Marcos Curty conducted the security proof of MDI-QKD in the finite-key regime. Our decoy-state protocol and finite-key analysis clearly show that even with practical signals (coherent lasers) and a finite size of data, it is possible to perform secure MDI-QKD
over long distances (e.g. up to about 150 km).

- In Chapter 5, some practical aspects of MDI-QKD are presented. These results have been published in [48, 46]. In [48], I am the first author. I studied the physical original of the error in a MDI-QKD system by analyzing various practical error sources. I also investigated MDI-QKD in an asymmetric setting, where the two channels connect Alice to Charles and Bob to Charles have different transmittances. This is an important step towards practical applications of MDI-QKD. In [46], I proposed a method to optimize the implementation parameters for MDI-QKD. This method can be readily used in experiment to significantly boost up the performance.

- In Chapter 6, an experimental demonstration of MDI-QKD over 10 km of optical fibers is presented. This work has been published in [49] and I am the third author. In this work, I designed the overall system, tested the polarization-modulation and polarization-alignment setup, performed the parameter optimization and analyzed the experimental data. Zhiyuan Tang and Zhongfa Liao conducted the whole experiment and measured the raw data. The success of our experiment with only commercial off-the-shelf components clearly demonstrates the practicality of MDI-QKD. In the future, this work can also be extended to free-space polarization encoding MDI-QKD with an untrusted satellite.

- In Chapter 7, a feasible method to extend the transmission distance of MDI-QKD is proposed. This method is called MDI-QKD with entangled photon sources in the middle. This work has been published in [50] and I am the first author. I designed a long-distance MDI-QKD method that is simple and experimentally feasible with current technology. This work is relevant to not only QKD but also general experiments involving entangled photon sources and Bell state measurements.

- In Chapter 8, the first experimental implementation considering source flaws in QKD is presented. It has been published in [49] and I am the first author. I performed a decoy-state QKD experiment that for the first time shows secure QKD with imperfect source at long distances. Our implementation is based on a recent proposal, which allows QKD protocols loss-tolerant to state-preparation flaws. This work is an important step toward QKD with imperfect devices. A combination of this work and MDI-QKD may incubate the first practical side-channel-free QKD.

- In Chapter 9, a fast quantum random number generator (QRNG) is reported.
These results have been published in [51] and [52]. In [51], I am the first author. I demonstrated an ultrafast QRNG based on the quantum phase noise at a rate over 6 Gbits/s. In [52], I developed a compact and cost-effective prototype. The simplicity and speed of this prototype show the feasibility of a robust, low-cost, and fast QRNG.

- In Chapter 10, I conclude my thesis with a summary and an outlook.

1.3 Journal publications related to this thesis


Chapter 2

Elements of practical QKD

In this Chapter, I present a few basics of QKD that are relevant to this thesis. These include the BB84 protocol, the decoy-state protocol, QKD components and quantum hacking. More general theories and experiments on QKD can be found in [9, 10, 11]

2.1 BB84 protocol

BB84 protocol [2] is illustrated in Fig. 2.1. The basic tool of BB84 protocol is a quantum channel (such as optical fiber) connecting Alice and Bob, and an authenticated public classical channel (such as Internet)\(^1\). The quantum channel represents that information through this channel is encoded on the quantum state of photons. Eve is allowed to fully control the quantum channel, but she is not allowed to sneak into Alice’s or Bob’s local laboratory to steal information. For the public channel, everyone including Eve is allowed to listen.

The full procedure of BB84 protocol is stated as follows (see Fig. 2.1).

1. Alice randomly selects a sequence of photons from one of the four polarizations, vertical, horizontal, 45-degrees and 135-degrees, and sends the sequence to Bob.

2. For each photon, Bob randomly chooses one of the two measurement bases (rec-

\(^1\)An authenticated classical channel is essentially required in QKD. In classical cryptography, an information-theoretically secure authentication algorithm does exist, for instance the Wegman-Carter algorithm [56], where authentication can be done with a rather short key. Authentication of an m-bit classical message requires only logarithmic in m-bit of an authentication key. Note that without authentication by a pre-shared secret between Alice and Bob, Eve can disguise herself as Bob, which leads the scheme not secure. Therefore, the goal of QKD is to allow Alice and Bob with a small amount of pre-shared secret to expand it into a much longer one.
Figure 2.1: A schematic of the BB84 protocol [2]. Alice sends Bob a sequence of photons prepared in different polarization states, which are chosen independently at random from two conjugate bases (rectilinear and diagonal basis). Bob measures each incoming photon using one of the two conjugate bases, which he selects independently at random for each signal. Next, Alice and Bob broadcast their basis choices using an authenticated classical channel and discard all data associated with signals prepared and measured in different bases. They sacrifice a randomly chosen portion of the remaining data (Sifted key) to estimate the quantum bit error rate (QBER). If this quantity is larger than some prescribed threshold value, they abort the protocol. Otherwise, Alice and Bob use classical post-processing techniques (such as error correction and privacy amplification) to generate a secret key.

3. Alice and Bob both broadcast their basis of measurements. Alice and Bob discard all events where they use different basis for a signal. The remaining results are called “sifted key”. Alice randomly chooses a fraction of remaining events as testing events, and she publicly broadcasts the testing events’ positions and polarizations. Bob then broadcasts the measured polarizations of the testing events.

4. Alice and Bob compute the quantum bit error rate (QBER) of the testing events. If the computed error rate is larger than some prescribed threshold value, they stop

---

\(^2\)Rectilinear and diagonal are two conjugate basis, where measurement in one basis randomizes the outcome of a measurement in the other basis.
the process. Otherwise, they convert all remaining data into a binary string. They perform classical post-processing such as error correction and privacy amplification to generate a final key.

What happens if Eve attacks the quantum channel? For each photon sent from Alice, Eve performs a measurement in a randomly chosen basis and re-sends a new photon to Bob according to her measurement result. Let us focus on those cases when Alice and Bob happen to use the same basis since they will throw away other cases. If Eve happens to use the correct basis (50%), then both she and Bob will decode Alice’s bit value correctly. No error is introduced by Eve. On the other hand, if Eve uses the wrong basis (50%), then both she and Bob will have random measurement results. This suggests that if Alice and Bob compare a subset of the sifted key, they will see a significant amount of errors, called quantum bit error. Here, for these bits, the photons will be passed on to Bob in the wrong basis, so regardless of Eve’s measurement result, Bob will have a 50% probability of measuring the opposite of Alice’s bit value. In other words, Eve’s attack will introduce 50% QBER for half of the total bits, and thus a total of 25% QBER. This example illustrates the basic principle behind QKD: Eve can only gain information at the cost of introducing errors, which will expose her existence.

2.2 Decoy-state protocol

The aforementioned BB84 protocol relies on single-photon sources, but practical and efficient single-photon sources are still technologically challenging nowadays \[57\]. So far, most implementations of the BB84 protocol are based on phase-randomized weak coherent pulses (WCPs) \[11\]. These states can be easily prepared using standard semiconductor lasers and optical attenuators at a low cost. The output state from a laser is a coherent state, which can be expressed as a Poissonian mixture of the different number states:

$$\rho = \sum_{n=0}^{\infty} \frac{e^{-\mu} \mu^n}{n!} |n\rangle \langle n|,$$

where $n$ is the number state\[^3\], $\mu$ is the mean number of photons in a pulse, and phase-randomization has been assumed. Attenuated lasers were considered to be non-ideal for BB84 as they always have the probability of emitting multi-photon pulses. That is,

\[^3\] In quantum mechanics, a physical state is represented by a state vector in a complex vector space. $|\bullet\rangle$ (called ket) and $\langle \bullet|$(called bra) are two physical-states notations following Dirac in quantum mechanics.
some WCPs may contain more than one photon prepared in the same quantum state \((n \geq 2\) in Eq. (2.1)). If Eve performs, for instance, the so-called photon-number-splitting attack \(^{58}\) on the multi-photon pulses, she could obtain full information about the part of the key generated with them without causing any noticeable disturbance.

Fortunately, the discovery of decoy-state protocol \(^{59, 60, 61}\) made weak coherent lasers much more appealing without significant losses on the performance of a BB84 QKD system. In this protocol, Alice prepares some decoy states in addition to the standard state – signal state – used in initial BB84. The decoy states are the same as the signal state, except for the expected photon number. For instance, if the signal state has an average photon number \(\mu\) of order 1 (e.g. \(\mu = 0.5\)), the decoy states have an average photon number \(\nu_1, \nu_2, \text{etc.}\). Those decoy states are used for the purpose of detecting eavesdropping attacks only, whereas the signal states are used for key generation. Each of Alice’s pulses is assigned to either signal state or decoy state randomly. Alice then modulates the intensity of each pulse and sends it to Bob. After Bob acknowledges the receipt of all the signals, Alice tells Bob over an authenticated classical channel which states are signal states. The statistical characteristics can be analysed. The decoy state idea was first proposed by Hwang \(^{59}\), who suggested using a large \(\nu\) (e.g. \(\nu = 2\)) as a decoy state. Lo et al. and Wang proposed practical protocols. Instead of using a large \(\nu\) as a decoy state, they proposed using small \(\nu\)'s as decoy states \(^{60, 61}\) and found that small \(\nu\)'s could result in a much better estimation. Moreover, \(^{60}\) provided a rigorous proof of security to decoy-state QKD. In the limit of infinitely many decoy states, Alice and Bob can effectively limit Eve’s attack to a simple beam-splitting attack. Notice that the decoy state is a rather general idea that can be applied to other QKD sources. For instance, decoy state protocols have been proposed in \(^{62}\) for parametric down conversion sources. One can refer to \(^{63, 64}\) for the details about practical decoy-state protocols. Remarkably, several experimental groups have demonstrated that decoy-state BB84 is secure and feasible under real-world conditions \(^{36, 37, 38, 39}\). As a result, decoy-state method has become a standard technique in many current QKD implementations\(^{11, 13}\).

\(^{4}\)In this attack, Eve can first perform a quantum non-demolition measurement on each signal and knows the photon number in that signal. She selectively suppresses all the single photon signals and splits all the multi-photon signals by keeping one copy herself and sending the other copy to Bob. In this way, Eve has an identical copy of what Bob possesses. She keeps all the qubits (quantum bits, as to bits in classical communication) in her quantum memory until Alice and Bob reveal the correct basis for each bit. She can then measure her qubits accordingly, thus breaking the security of weak coherent BB84 protocol.
2.3 Basic QKD components

We present some main components used in a typical QKD setup. Besides them, polarizing beam-splitters, beam-splitters, optical filters amplitude modulators, polarization modulators and phase modulators are also widely used in QKD applications.

2.3.1 Source

As aforementioned, attenuated laser sources are the most commonly used sources in QKD experiments. This type of source is essentially the same as the laser source used in classical optical communication except for that heavy attenuation is applied on it (usually attenuated to below 1 photon per pulse). It is simple and reliable, and it can reach Gigahertz with little challenge. It is also a good candidate for another type of QKD protocol – continuous-variable QKD [65], in which the laser source is usually attenuated to around 100 photons per pulse.

Another important class of QKD sources is entangled photon source, which is used in the entanglement-based [3, 66] QKD protocol, and is an essential ingredient in quantum computing [67]. A widely used entangled photon source is based on spontaneous parametric down-conversion (SPDC), where a high energy photon propagates through a highly non-linear crystal, producing two entangled photons with frequency halved [68]. SPDC sources are also used as “triggered single photon sources”, in which Alice possesses a SPDC source and monitor one arm of its outputs. In case that Alice sees a detection, she knows that there is one photon emitted from the other arm.

2.3.2 Random number generator

Random numbers are needed for basis choice, bit value choice, phase randomization, intensity choice in the decoy-state method. Truly random number generation is a key technique in current QKD. Fortunately, quantum mechanics offers true randomness originating from the laws of physics, i.e., quantum random number generator (QRNG). A simple way to build a QRNG is to send a single photon through a 50:50 beam-splitter and put two single-photon detectors on the two outgoing arms [69]. The generated bit value (0 or 1) depends on which detector detects a photon. Several other QRNG schemes have also been demonstrated [70, 71, 72]. Nonetheless, due to the difficulties of measuring quantum effects, most of QRNGs have been limited to a relatively slow rate (typically below 100 Mbits/s). This rate is far from real applications, such as high-speed QKD.
operating over gigahertz [12, 73]. I have solved this difficulty and developed a compact and cost-effective QRNG prototype, which has a real-time generation rate of 1 Gbits/s (see Chapter 9).

2.3.3 Quantum channel

The fundamental requirements for a quantum channel are low-loss and preservation of quantum state. In practice, two types of channels have these desirable properties: single-mode fiber and free-space.

Standard optical fibers have been developed and used in telecommunication for four decades. Currently, standard optical fiber is the most popular choice for QKD implementations, because it can easily connect two arbitrary points and be extended to a network. The loss $\alpha$ of an optical fiber is usually measured in dB/km. The probability for a single photon to be transmitted through an optical fiber of length $l$, is given by the transmittance $t = 10^{-\alpha l/10}$. The losses depend heavily on the wavelength of the photons, and are minimal in the two “telecom window wavelengths”: around 0.35 dB/km at 1330nm, and 0.21 dB/km at 1550nm. In QKD, since loss is critical for the transmission range and key generation rate, the 1550nm wavelength is usually used. The loss in fibers puts an limit on the longest distance that a fiber-based QKD system can reach (typical, less than 400 km). The main disadvantage of optical fiber is its birefringence. The strong polarization dispersion made it hard to implement polarization-coding system. Moreover, it has strong spectral dispersion, which affects the high-speed QKD systems heavily as the pulses are broadened and overlap with each other.

Free-space links have negligible polarization-mode dispersions and negligible chromatic dispersions. There are “atmospheric transmission windows” that have small loss ($\alpha < 0.1$ dB/km) in clear weather. It is an ideal link for the polarization-coding QKD. Recently, free-space QKD has attracted more attention [74, 75]. Nonetheless, over long distance communication, atmospheric fluctuations make it challenging to predict the arrival point of a photon and align the optical beams. Another disadvantage of the free-space link is that it requires a line-of-sight between Alice and Bob. Buildings and mountains are serious obstacles for free-space QKD systems. Furthermore, diffraction is another important factor in free-space communications. Nonetheless, the greatest motivation for open-air QKD scheme is the hope for ground-to-satellite and satellite-to-satellite quantum communications [74, 75]. As there is negligible optical absorption in the outer space, we may be able to achieve an inter-continental quantum communication with free-space
QKD. Indeed, many countries, including USA, Japan, China and Canada, have proposed to build the satellite-based quantum communications.

2.3.4 Detector

In QKD, the most popular type of single-photon detectors is the InGaAs avalanche photodiode (APD) [76]. Single-photon detectors are typically threshold detectors, i.e. the detector output is binary and distinguishes between “0” and “one or more photons”. InGaAs-APD utilizes the avalanche effect of semiconductor diodes. A strong reverse biased voltage is applied on the InGaAs diode. The incident photon will trigger the avalanche effect, generating a voltage pulse. The narrow band gap of InGaAs makes it possible to detect photons at telecom wavelengths. They normally work below -50 °C to lower the dark count rate (i.e. the event that the detector generates a detection click while no actual photon hits it; it is about 1-2 kHz). This temperature can be easily achieved by thermal-electric coolers. During an avalanche, carriers are trapped in impurities in the semiconductor. Hence, there is a high dark count probability due to the decay of trapped carries after an avalanche. This is called the after-pulse effect. To reduce the after-pulse effect, the detector is usually deactivated for a time period, which is called the “dead time”, after a detection event. The dead time should be set to long enough so that when the detector is re-activated, the after-pulse effect is negligible. InGaAs-APDs suffered from low detection efficiencies of around 10% and had rather long dead times after a detection event (about 10 us), which severely limited the detection repetition rate to only a few megahertz. Recently, however, new detector technologies have been developed for QKD applications, including self-differencing avalanche photodiodes [77] and superconducting single-photon detectors (SSPDs). All these approaches enable detection repetition rates on the order of gigahertz. Also, new types of SSPDs with very high detection efficiencies of around 93% have been developed [78]. The main drawback of these novel SSPDs, however, is their operating temperature, which is currently on the order of 1 K. The dark count rate of these high-efficiency SSPDs is of the order of 100 Hz. For more details of single-photon detectors, see Ref. [76].

In a practical QKD system, the APDs are often operated at a gated mode, where the detectors are only activated when the photons are expected to hit them. This activated time period is called a gate. The gates are usually applied at a high repetition rate and a number of gates is deactivated after a detection event, such as the ID Quantique system [16]. Gated mode indeed reduces the dark count rate by several orders and is thus used in
most InGaAs APDs. However, it may open up a security loophole, such as the time-shift attack [19, 18] and the detector-blinding attack [21] (see Section 2.4.1).

2.3.5 An example of implementation: plug-and-play

There are excellent reviews of different QKD implementation schemes [9, 11]. This section only contains an illustration of a specific implementation – Plug-and-Play QKD system – that is commercially available on the market [16].

Besides the polarization-coding BB84 protocol described in Section 2.1, BB84 can be implemented with any two-level quantum system (qubits). Indeed, other coding methods, particularly phase-coding, also exist. In phase-coding BB84, a signal consists of a superposition of two time-separated pulses, known as the reference pulse and the signal pulse. The information is encoded in the relative phase between the two pulses. Hence, the encoded relative phases of \{0, \pi/2, \pi, 3\pi/2\} in the phase-coding BB84 are essentially equivalent to the encoded polarizations of \{Horizon, 45\ degree, Vertical, 135\ degree\} in the polarization-coding BB84. They are simply different embodiments of the same BB84 protocol. The phase-coding BB84 has been practically implemented based on various schemes, and one specific scheme is “Plug-and-Play” QKD implementation, which is widely used in commercial QKD systems [16].

The “Plug-and-Play” schematic is shown in Fig. 2.2. It has only one Mach-Zehnder interferometer and the light propagates through the same channel and interferometer twice due to the Faraday mirror on Alice’s side. This system works as follows. Bob first sends two strong laser pulses (signal pulse and reference pulse) to Alice. Alice uses the reference pulse as a synchronization signal to activate her phase modulator. Then Alice modulates the phase of the signal pulse only, attenuates the two pulses to single-photon level, and sends them back to Bob. Bob randomly chooses his measurement basis by modulating the phase of the returning reference pulse. Owing to the Faraday mirror (in Alice) that can automatically compensate the polarization fluctuations in the channel, this system presents good phase and polarization stability.

2.4 Quantum hacking

As aforementioned, the unconditional security of QKD is based on the laws of quantum mechanics and has been rigorously proven. Nevertheless, owing to the imperfections in the real-life implementations of QKD, there is still a large gap between its theory and
Figure 2.2: Optical setup of commercial plug & play QKD system (manufactured by ID quantique). SPD$_0$/SPD$_1$, single-photon detector; PM$_A$/PM$_B$, phase modulator; BS, beam splitter; PBS, polarization beam splitter; CD, classical photo-detector; FM, Faraday mirror; VOA, variable optical attenuator. This system employs the phase-coding scheme. Bob first sends two strong laser pulses (signal and reference pulse) to Alice. Alice uses the reference pulse as a synchronization signal (detected by her CD) to activate her PM. Then Alice modulates the phase of the signal pulse only, attenuates the two pulses to single photon level, and sends them back to Bob. Bob randomly chooses his measurement basis by modulating the phase of the returning reference pulse and detects the interference signals with his two SPDs.

practice. Eve may try to exploit these imperfections and launch quantum hacking not covered by the original security proofs.

2.4.1 Attacks

The first successful quantum attack against a commercial QKD system was the time-shift attack \cite{18}. It is based on earlier theoretical proposals introduced in \cite{19, 79} (see Fig. 2.3a). As aforementioned, InGaAs avalanche photodiodes, are often operated in a gated mode, i.e., their detection efficiency is time-dependent. Importantly, since every QKD system contains at least two detectors to measure two different bit values, it is usually quite difficult to guarantee that both detectors have precisely the same detection efficiency. Due to finite manufacturing precision of the detectors and the electronics, together with small differences in the optical path lengths coupled to the detectors, the time gates for the two detectors are usually slightly misaligned, thus causing a detector-efficiency mismatch \cite{79}. In this scenario, Eve can simply shift the arrival time of each signal such that one detector has a much higher detection efficiency than the other. As a result, she could obtain partial information about the final key almost without
Figure 2.3: (Color online) (a) Schematic illustration of the typical detection efficiency mismatch between two single-photon detectors (SPD\textsubscript{0} and SPD\textsubscript{1} in the figure). This could be used by Eve to perform a time-shift attack \cite{18}. In this attack, Eve shifts the arrival time of each signal sent by Alice to either \(t_1\) or \(t_2\) such that one detector has a much higher detection efficiency than the other. In so doing, she can obtain information about the final key without being detected. (b) Working principle of the detector blinding attack \cite{21}. First, Eve sends Bob bright light (not shown in the figure) to blind his detectors and make them leave the Geiger mode operation (used in QKD) and enter into linear mode operation. After that, she sends Bob a tailored light pulse that produces a “click” in one of his detector only when Bob uses the same basis employed by Eve to prepare her signal. Otherwise, no detector “clicks”. As a result, Eve can determine which detector generates a “click” at each given time and thus learn the entire secret key without introducing any noticeable disturbance. Fig.\,(b) is adapted from \cite{21} with permission. ©2010 NPG.

Recently, a more powerful attack – detector blinding attack – was introduced in \cite{21}. It allows Eve to learn the entire secret key without being detected. The procedure is as follows (see Fig. 2.3b). Eve shines bright light into the two detectors to make them enter into the so-called linear mode operation \cite{21}. In so doing, the SPDs (including APDs or SSPDs) are not longer sensitive to single-photon pulses but they behave like classical intensity photo-detectors. As a consequence, Eve can now fully control the detector “clicks” just by sending Bob a tailored light pulse. Importantly, this attack has been successfully implemented against both commercial \cite{21} and research \cite{22} QKD setups.
Quantum hacking has attracted a lot of research interest in recent years, and several attacks have been studied in the scientific literature. As an illustration, Table 2.1 contains a list of various attacks that have been successfully demonstrated experimentally. We can see that most of the hacking strategies are actually directed towards Bob’s measurement system, which can be considered as the Achilles heel of conventional QKD implementations. This is so because Alice’s source is usually less likely to be a problem as, in principle, she can prepare her quantum signals in a fully protected environment outside Eve’s influence. This can be achieved, for instance, using optical isolators. It is therefore reasonable to expect that Alice can fully characterise the quantum states emitted using, for example, state tomography techniques, and then include this information in the security analysis [86, 87, 88]. Unfortunately, however, the problem with Bob’s measurement device is more delicate, as Eve is allowed to send in any signal she desires. As a consequence, it is quite hard to protect Bob’s device against hacking attacks.

“Photon detectors have turned out to be an Achilles heel for quantum key distribution, inadvertently opening the door to subtle side-channel attacks.” - Charles H. Bennett

<table>
<thead>
<tr>
<th>Attack</th>
<th>Component</th>
<th>Target</th>
<th>Tested system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time-shift [18]</td>
<td>Detector</td>
<td>Measurement</td>
<td>IDQ</td>
</tr>
<tr>
<td>Detector blinding [21]</td>
<td>Detector</td>
<td>Measurement</td>
<td>IDQ, MagiQ</td>
</tr>
<tr>
<td>Detector blinding [22]</td>
<td>Detector</td>
<td>Measurement</td>
<td>research syst.</td>
</tr>
<tr>
<td>Dead-time [23]</td>
<td>Detector</td>
<td>Measurement</td>
<td>research syst.</td>
</tr>
<tr>
<td>Channel-calibration [24]</td>
<td>Detector</td>
<td>Measurement</td>
<td>IDQ</td>
</tr>
<tr>
<td>Wavelength [80]</td>
<td>Beam-splitter</td>
<td>Measurement</td>
<td>research syst.</td>
</tr>
<tr>
<td>Device-calibration [81]</td>
<td>Local-oscillator</td>
<td>Measurement</td>
<td>research syst.</td>
</tr>
<tr>
<td>Self-differencing [82]</td>
<td>Detector</td>
<td>Measurement</td>
<td>research syst.</td>
</tr>
<tr>
<td>Laser-damaging [83]</td>
<td>Detector</td>
<td>Measurement</td>
<td>research syst.</td>
</tr>
<tr>
<td>Time-information [84]</td>
<td>Detector</td>
<td>Measurement</td>
<td>research syst.</td>
</tr>
<tr>
<td>Phase-information [85]</td>
<td>Phase-modulator</td>
<td>Source</td>
<td>research syst.</td>
</tr>
<tr>
<td>Phase-remapping [20]</td>
<td>Phase-modulator</td>
<td>Source</td>
<td>IDQ</td>
</tr>
</tbody>
</table>

Table 2.1: List of quantum hacking attacks that have been successfully demonstrated against commercial and research QKD systems.
2.4.2 Possible countermeasures

Currently there are four main possible approaches to avoid the problem of quantum hacking and recover the security of QKD implementations.

The first one is called “security patches”. Once a particular attack or loophole is known, it is relatively easy to find an appropriate countermeasure against the attack and to find a method to close the loophole. For instance, the time-shift attack introduced in the previous section can be avoided by simply shifting the gating window of the detectors at random [19]. See also [79] for other possible countermeasures against this attack. Similarly, the detector blinding attack could, in principle, be avoided by monitoring the detector’s photocurrent for anomalously high values. Other techniques can also be used [89, 90]. Nonetheless, the main drawback of this first approach is that it cannot counter unanticipated attacks. This is the case because “patches” can only protect against known hacking strategies. The security of this solution resembles that of classical cryptography in the sense that it abandons the information-theoretic security framework of QKD.

The second approach consists in obtaining “precise mathematical models” for all the physical devices and incorporate this information into the security proof [91, 92]. While this solution is plausible in theory, it is hard to realise in practice. QKD components are complex devices and it is challenging to fully characterise them and then derive a security proof that takes all the relevant information into account. This might be possible for certain components (specially for the ones that can be protected from Eve’s influence), but it seems quite difficult for the whole QKD system.

<table>
<thead>
<tr>
<th></th>
<th>DI-QKD</th>
<th>MDI-QKD</th>
</tr>
</thead>
<tbody>
<tr>
<td>True random number generators</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Trusted classical post-processing</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Authenticated classical channel</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>No unwanted information leakage from the measurement unit</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Characterised source</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Table 2.2: Assumptions in DI-QKD versus MDI-QKD. See [27, 93] for more discussions about the assumptions in DI-QKD.
Figure 2.4: (Color online) Schematic diagram of device-independent QKD (DI-QKD). An untrusted source in the middle distributes entangled photons to Alice and Bob. For each input signal, Alice and Bob select, respectively, a measurement setting (denoted as $X_A$ and $X_B$ in the figure) from a set of possible prescribed values. As a result, they obtain one out of three possible outcomes for each signal received: 0, 1, or no photon is detected (-). From the input data selected and the output data observed, they can prove the security of the protocol based on the violation of Bell inequality, which certifies the presence of quantum correlations. To overcome the detection loophole problem due to channel losses, the system can include a so-called fair sampling device. Examples of such a device are a qubit amplifier [30, 31] or a quantum non-demolition measurement of the number of photons in a pulse. Before Alice and Bob select their measurement settings, this device tells them whether or not the input signal contains precisely one photon. This situation is illustrated in the figure with a flag (Yes/No). Only when the flag is equal to “Yes”, the legitimate users input the setting for the measurement. Other events are discarded. In principle, DI-QKD can remove all side-channels in a QKD implementation. Reproduced from [11] with permission. ©2014 NPG.

The third solution is called device-independent QKD (DI-QKD) [25, 26, 27, 28, 29]. It is illustrated in Fig. 2.4. Alice and Bob do not need to characterise their devices, and they can treat them as two “black boxes”. As long as certain necessary assumptions are satisfied (see Table 2.2 or Ref. [27] for a summary of the assumptions), one can prove the security of QKD based solely on the violation of a Bell inequality, which certifies the presence of quantum correlations. Remarkably, this approach can in principle remove all side-channels from the QKD hardware, if the assumptions listed in Table 2.2 are properly satisfied\(^5\). Its main drawback, however, lies in the fact that it requires a loophole-free

---

\(^5\)DI-QKD requires the assumption that the measurement units of both Alice and Bob do not leak
Bell test which is still unavailable at the moment. Also, the expected secret key rate is limited at practical distances [30, 31]. Still, DI-QKD could be a viable solution for short distance transmission in the future with improved technology.

In summary, the first approach cannot provide information-theoretic security while the second one is challenging to realize in practice. Moreover, DI-QKD cannot be implemented with current technology. In this thesis, I focus on the fourth solution, which is called measurement-device-independent QKD (MDI-QKD) [32] (see also [33]). The key idea of MDI-QKD is that both Alice and Bob are senders. They transmit signals to an untrusted third party, Charles (or Eve), who is supposed to perform a Bell state measurement. This measurement provides post-selected entanglement that can be verified by Alice and Bob. The security of MDI-QKD is based on the time-reversed EPR QKD protocol [34, 35]. The assumption of MDI-QKD is that both Alice and Bob trust their source. As long as this assumption is satisfied, MDI-QKD can remove all side-channels from the measurement unit, which is the weakest part of a QKD realization, as we saw it previously. Most importantly, MDI-QKD is fully practical with present technology and thus it offers a clear avenue to bridge the gap between theory and practice of QKD. Indeed, four research groups have independently demonstrated that MDI-QKD is feasible in the real world [94, 95, 96, 55].

\footnote{Any unwanted information to the outside. An attack exploiting this weakness of DI-QKD has recently been proposed in [93].}
Chapter 3

Measurement-device-independent QKD (MDI-QKD)

In this Chapter, I will discuss the detailed protocol of MDI-QKD, including its implementation set-up and secure key rate formula. This Chapter is largely based on [45].

3.1 Time-reversed EPR protocol

To understand MDI-QKD, let me first introduce an Einstein-Podolsky-Rosen (EPR) based QKD protocol (see Fig. 3.1a), which is a modified version of the original entanglement-based QKD scheme [3, 66]. In this protocol, Alice and Bob each prepare an EPR pair and send half of it to an untrusted third party, Charles. Charles is supposed to perform an entanglement swapping operation on the incoming signals via a Bell state measurement (BSM) and broadcast his measurement results. Next, Alice and Bob measure their halves of the EPR pairs in two conjugate bases (Z or X) that they select at random. Importantly, this allows them to determine whether or not Charles is honest. For this purpose, they can compare a randomly chosen subset of their data in order to test if it satisfies the expected correlations associated with the Bell state declared by Charles.

Interestingly, this protocol can also be implemented in a “time-reversal” fashion (see Fig. 3.1b). This is the case because Charles’ operations commute with those of Alice and Bob. Therefore, one can reverse the order of the measurements. That being said, Alice and Bob don’t need to wait for Charles’ results to measure their halves of the EPR pairs: they can measure them beforehand. Note that Charles’ BSM is only used to check the
Figure 3.1: (Color online) (a) An Einstein-Podolsky-Rosen (EPR) based QKD protocol. Step 1: Alice and Bob each prepare an EPR pair and send half of it to an untrusted third party, Charles. Step 2: On receiving the signals, Charles is supposed to realize an entanglement swapping operation via a Bell state measurement (BSM) and broadcast his measurement results. Step 3: Alice and Bob measure their particles using the X or Z bases, which they select at random. Step 4: Alice and Bob test the honesty of Charles by comparing a randomly chosen portion of their data. (b) An equivalent time-reversed EPR based QKD protocol. Since Charles’ operations commute with those of Alice and Bob, one can reverse the order of the measurements (steps 2 and 3 in subfigure (a)). That being said, Alice and Bob can safely measure their signals before Charles actually implements the BSM.

Parity of Alice’s and Bob’s bits and, as a consequence, it does not reveal any information about the individual bit values. This rephrases the original EPR based QKD protocol into an equivalent prepare-and-measure scheme in which Alice and Bob directly send Charles BB84 states and Charles performs the measurements. Most importantly, like in the original EPR based QKD protocol, Alice and Bob can test the honesty of Charles simply by comparing a random portion of their signals.

This time-reversal scenario has been studied in [34, 35] (see also [33] which discusses the BSM conducted by Charles in QKD). However, these important works offered very limited performance and, therefore, they have been largely forgotten by the QKD community as a result. For instance, the scheme in [34] requires perfect single-photon sources and long-term quantum memories, which renders it unpractical with current technology. Inamori’s scheme [35] uses practical weak coherent pulses (WCPs) but it does not include decoy states, since it was proposed long before the advent of the decoy-state protocol (see Section 2.2).
Figure 3.2: (Color online) (a) Schematic diagram of a possible MDI-QKD implementation. Alice and Bob prepare BB84 polarization states and send them to an untrusted relay Charles/Eve, which can be treated as a “black box”. The relay is supposed to perform a Bell state measurement (BSM) that projects Alice’s and Bob’s signals into a Bell state. (b) Example of a decoy-state BB84 transmitter. The WCPs are generated using four emitting laser diodes. These signals are then phase-randomised with a phase modulator (PM). Decoy states are prepared using an amplitude modulator (AM). In the figure: (M) mirror, (BS) beam-splitter, (QRNG) quantum random number generator, (F) optical filter and (I) optical isolator. (c) Example of a BSM implementation with linear optics. Charles interferes in the incoming pulses at a 50:50 BS, which has a polarising beam-splitter (PBS) on each end that projects the photons into either horizontal (H) or vertical (V) polarization states. A “click” in the single-photon detectors $D_{1H}$ and $D_{2V}$, or in $D_{1V}$ and $D_{2H}$, indicates a projection into the singlet state $|\psi^-\rangle = (|HV\rangle - |VH\rangle)/\sqrt{2}$, while a “click” in $D_{1H}$ and $D_{1V}$, or in $D_{2H}$ and $D_{2V}$, implies a projection into the triplet state $|\psi^+\rangle = (|HV\rangle + |VH\rangle)/\sqrt{2}$. Other detection patterns are considered unsuccessful.

3.2 MDI-QKD protocol

The main merits of the MDI-QKD proposal introduced in [32] are twofold: (i) it identified the importance of the results in [34, 35] to remove all detector side-channels from QKD implementations, (ii) it significantly improved the system performance with practical signals by including decoy states. Hence, it has attracted a lot of scientific attention from the research community in both theoretical [97, 98, 99, 100, 48, 50, 47, 46] and
experimental studies [94, 95, 96, 55]. An example of a possible MDI-QKD implementation is illustrated in Fig. 3.2a [32]. The protocol can be summarized in these three steps:

1. Alice and Bob prepare phase-randomised WCPs (together with decoy signals) in the BB84 states and send them to an untrusted relay, Charles.

2. If Charles is honest, he performs a BSM that projects Alice’s and Bob’s signals into a Bell state. In any case, he announces whether or not his measurements are successful, including the Bell states obtained.

3. Post-processing: Alice and Bob keep the data corresponding to Charles’ successful measurement results and discard the rest. Moreover, they post-select the events where they employ the same basis and, based on the outcomes announced by Charles, for example Alice flips part of her bits to correctly correlate them with those of Bob (see Table 3.1). Finally, they use the decoy-state method to estimate the gain and QBER of the single-photon contributions.

Note that opposed to DI-QKD, there is no need to protect Charles’ measurement unit from unwanted leakage of information to the outside (see Table 2.2). Indeed, this device can be fully controlled or even manufactured by Eve. This is significant because it means that there is no need to certify the detectors in a QKD standardisation process. A pay off of MDI-QKD is that Alice and Bob need to know which states they send to Charles. However, as mentioned previously, it is reasonable to expect that they can indeed characterise their sources and protect their state preparation processes from Eve’s influence. Recent results also show that a full source characterisation is not absolutely necessary for MDI-QKD to work [86, 87, 88].

|                | Singlet state $|\psi^-\rangle$ | Triplet state $|\psi^+\rangle$ |
|----------------|-------------------------------|-------------------------------|
| Coincident clicks | $D_{1H} \& D_{2V}$ or $D_{2H} \& D_{1V}$ | $D_{1H} \& D_{1V}$ or $D_{2H} \& D_{2V}$ |
| Rectilinear basis | Bit flip | Bit flip |
| Diagonal basis | Bit flip | – |

Table 3.1: Alice and Bob post-select the events where the relay (Fig. 3.2c) outputs a successful result and they use the same basis in their transmission. Moreover, either Alice or Bob flips her/his bits, except for the cases where both of them select the diagonal basis and the relay outputs a triplet.
3.3 Secure key rate

In the asymptotic scenario where Alice and Bob send Charles an infinite number of signals, the secret key rate has the form

\[
R \geq Q_{Z11}^Z [1 - H_2(e_{X11}^Z)] - Q_{\mu\mu}^Z f_e(E_{\mu\mu}^Z) H_2(E_{\mu\mu}^Z),
\]

(3.1)

where \(Q_{Z11}^Z\) is the gain (i.e., the probability that Charles declares a successful result) when Alice and Bob send him one single-photon each in the Z basis. This quantity is often written as \(Q_{Z11}^Z = P_{Z11} Y_{Z11}^Z\), where \(P_{Z11}\) denotes the probability that both Alice and Bob send a single photon in the Z basis, and \(Y_{Z11}^Z\) denotes the yield, i.e. a conditional probability that Charles declares a successful event given that Alice and Bob send a single photon. When both Alice and Bob use WCPs with intensity \(\mu\), \(P_{Z11}^Z = \mu^2 e^{-2\mu}\). \(e_{X11}^Z\) is the phase error rate of these single-photon signals; \(Q_{\mu\mu}^Z\) and \(E_{\mu\mu}^Z\) represent, respectively, the gain and the QBER in the Z basis when Alice and Bob send Charles WCPs of intensity \(\mu\); \(f_e \geq 1\) is the error correction inefficiency function, and \(H_2(x) = -x \log_2(x) - (1 - x) \log_2(1 - x)\) is the binary entropy function.

Eq. (3.1) assumes that Alice and Bob use the Z basis for key generation and the X basis for testing only [101]. The term \(Q_{Z11}^Z H_2(e_{X11}^Z)\) corresponds to the information removed from the final key in the privacy amplification step of the protocol, while \(Q_{\mu\mu}^Z f_e(E_{\mu\mu}^Z) H_2(E_{\mu\mu}^Z)\) is the information revealed by Alice in the error correction step. The quantities \(Q_{\mu\mu}^Z\) and \(E_{\mu\mu}^Z\) are directly measured in the experiment, while \(Q_{Z11}^Z\) and \(e_{X11}^Z\) can be estimated using the decoy-state method (see Section 4.1). A model to derive \(Q_{Z11}^Z\), \(e_{X11}^Z\), \(Q_{\mu\mu}^Z\) and \(E_{\mu\mu}^Z\) is shown in Appendix A.

3.4 Summary

In this chapter, we have explained the basic idea of the MDI-QKD protocol. We began by introducing the time-reversed EPR QKD protocol, which is the foundation of MDI-QKD. The main merit of the MDI-QKD proposal is to remove all side channels in the measurement device. MDI-QKD offers a clear avenue to bridge the gap between theory and practice of QKD. This fact has also been noted in Charles H. Bennett’s blog,

“Measurement-device-independent QKD looks like an elegant solution for the untrusted detector problem.” - Charles H. Bennett
Chapter 4

Decoy-state MDI-QKD with finite resources

In the past Chapter, I explained the basic idea of MDI-QKD proposed in [32]. However, in order to apply the results of [32] to real-life systems, there are still some loose ends that need to be addressed. In particular, [32] assumes an asymptotic case, where Alice and Bob use an infinite number of decoy-state settings and they have infinite data size. In this chapter, I will discuss how to overcome these two limitations. Much of this chapter is based on [46, 47]. In [46], I am the first author. I investigated analytical and numerical decoy-state methods with one, two and three decoy states. In [47], I am the second author. My main contribution is to apply the decoy-state method into the finite-key security analysis of MDI-QKD, and to perform the numerical simulation to evaluate its performance. Marcos Curty conducted the rigorous security proof of MDI-QKD in the finite-key regime against general attacks.

4.1 Finite number of decoy states

In MDI-QKD (Fig. 3.2), by performing the measurements for different intensity settings, we can obtain [32]

\[
Q_{qa, qb}^{\lambda} = \sum_{n,m=0} e^{-(qa+qb)} \frac{q_a^n q_b^m}{n! m!} Y_{nm}^{\lambda},
\]

\[
Q_{qa, qb}^{\lambda} E_{qa, qb}^{\lambda} = \sum_{n,m=0} e^{-(qa+qb)} \frac{q_a^n q_b^m}{n! m!} Y_{nm}^{\lambda} e_{nm}^{\lambda},
\]

(4.1)

where \( \lambda \in \{X, Z\} \) denotes the basis choice, \( q_a \) (\( q_b \)) denotes Alice’s (Bob’s) intensity setting, \( Q_{qa, qb}^{\lambda} \) (\( E_{qa, qb}^{\lambda} \)) denotes the gain (QBER), and \( Y_{nm}^{\lambda} \) (\( e_{nm}^{\lambda} \)) denotes the yield (error rate) given...
that Alice and Bob send respectively an \( n \)-photon and \( m \)-photon pulse. Here, following the key rate formula introduced in Eq. (3.1), the key idea of the decoy-state method is to estimate a lower bound for \( Y_{11}^Z \) and an upper bound for \( e_{11}^X \) from the set of linear equations given by Eq. (4.1). We denote these two bounds as \( Y_{11}^{Z,L} \) and \( e_{11}^{X,U} \) respectively. In this section, we focus on the symmetric case where the two channel transmissions from Alice to Charles and from Bob to Charles are equal. The analysis for asymmetric case will be shown in Section 5.3. In symmetric case, the optimal intensities for Alice and Bob are equal (see Appendix A). Hence, to simplify our discussion, we assume that equal intensities are used by Alice and Bob, i.e., \( q_a = q_b = q \) with \( q \in \{\mu, \nu_1, \nu_2, \omega, \ldots\} \), where \( \mu \) denotes the signal state and \( \{\nu_1, \nu_2, \omega, \ldots\} \) denote the decoy states. Our method can be easily extended to the unequal intensities.

Various decoy-state methods have been proposed for MDI-QKD. Ref. [97] proposed a numerical method using two and three decoy states. Refs. [98, 99, 100] presented analytical approaches by assuming that Alice and Bob can prepare a perfect vacuum state. I [47, 46], however, designed an analytical approach with two general decoy states, i.e., without the assumption of vacuum. This is particularly important for the practical implementations, as it is usually difficult to create a vacuum state in decoy-state QKD experiments [102]. The different intensities are usually generated with an intensity modulator, which has a finite extinction ratio (e.g., around 30 dB).

Given the existing decoy-state methods, a natural open question is: how many types of decoy states are essentially needed for MDI-QKD in practice? In the following of this section, we summarize both analytical and numerical decoy-state methods with one, two and three decoy states. By clearly comparing these methods, we find that two decoy states, combined with a parameter optimization (see Section 5.2), is already close to the optimal estimation, and more decoy states cannot improve the key rate much in both asymptotic and finite-data cases.

4.1.1 Numerical approaches

Ignoring statistical fluctuations temporally, the estimations on \( Y_{11}^{Z,L} \) and \( e_{11}^{X,U} \) from Eq. (4.1) are constrained optimisation problems, which is linear and can be efficiently
solved by linear programming. The numerical routine can be written as:

\[ \begin{align*}
    &\min_Y : Y^{Z}_{11}, \\
    &\text{s.t.} : 0 \leq Y^{Z}_{nm} \leq 1, \text{ with } n, m \in S_{\text{cut}}, \\
    &Q^{Z}_{qaqb} - (1 - \sum_{n, m \in S_{\text{cut}}} e^{-(q_a + q_b)} \frac{q^n_a q^m_b}{n! m!}) \leq \sum_{n, m \in S_{\text{cut}}} e^{-(q_a + q_b)} \frac{q^n_a q^m_b}{n! m!} Y^{Z}_{nm} \leq Q^{Z}_{qaqb}
\end{align*} \]

Max : \( X^{X}_{11} \),

\[ \begin{align*}
    &\text{s.t.} : 0 \leq Y^{X}_{nm} \leq 1, 0 \leq Y^{X}_{nm} e^{X}_{nm} \leq 1, \text{ with } n, m \in S_{\text{cut}}, \\
    &Q^{X}_{qaqb} - (1 - \sum_{n, m \in S_{\text{cut}}} e^{-(q_a + q_b)} \frac{q^n_a q^m_b}{n! m!}) \leq \sum_{n, m \in S_{\text{cut}}} e^{-(q_a + q_b)} \frac{q^n_a q^m_b}{n! m!} Y^{X}_{nm} \leq Q^{X}_{qaqb} \\
    &Q^{X}_{qaqb} E^{X}_{qaqb} - (1 - \sum_{n, m \in S_{\text{cut}}} e^{-(q_a + q_b)} \frac{q^n_a q^m_b}{n! m!}) \leq \sum_{n, m \in S_{\text{cut}}} e^{-(q_a + q_b)} \frac{q^n_a q^m_b}{n! m!} Y^{X}_{nm} e^{X}_{nm} \leq Q^{X}_{qaqb} E^{X}_{qaqb}
\end{align*} \]

where \( S_{\text{cut}} \) denotes a finite set of indexes \( n \) and \( m \), with \( S_{\text{cut}} = \{ n, m \in \mathbb{N} \text{ with } n \leq N_{\text{cut}} \text{ and } m \leq M_{\text{cut}} \} \), for prefixed values of \( N_{\text{cut}} \geq 2 \) and \( M_{\text{cut}} \geq 2 \). In our simulations presented below, we choose \( N_{\text{cut}} = 7 \) and \( M_{\text{cut}} = 7 \), as larger \( N_{\text{cut}} \) and \( M_{\text{cut}} \) have negligible effect on decoy-state estimation. More discussions can be seen in [97]. Here, \( q \in \{ \mu, \nu \} \) for one decoy-state estimation; \( q \in \{ \mu, \nu, \omega \} \) for two decoy-state estimation; \( q \in \{ \mu, \nu_1, \nu_2, \omega \} \) for three decoy-state estimation. Notice that statistical fluctuations can be easily conducted by adding constraints on the experimental measurements of \( Q^{\lambda}_{qaqb} \) and \( E^{\lambda}_{qaqb} \). These additional constraints can be analyzed by using statistical estimation methods, such as standard error analysis [97] or Chernoff bound [47] (see next Section).

### 4.1.2 Analytical approaches

We discuss the analytical approaches based on Gaussian elimination.

**Two decoy states**

We consider an estimation method with two general decoy states \( \nu, \omega \) satisfying \( \mu > \nu > \omega \geq 0 \). The final results are summarized in Table 4.1. The method to estimate \( Y^{Z, L}_{11} \) from Eq. (4.1) can be divided into two steps:

1. Cancel out the terms \( Y^{Z}_{0m} \) and \( Y^{Z}_{n0} \) using Gaussian elimination.
2. Cancel out the terms \( Y^{Z}_{12} \) and \( Y^{Z}_{21} \) using the results in the first step.
Analytical equations for the two decoy-state protocol. See the main text for details. Ignoring the finite-key effect, these results can be directly used by experimentalists to obtain an estimation of the expected system performance.

For the first step, we choose the gains \( \{Q_{\nu\nu}^Z, Q_{\omega\omega}^Z, Q_{\nu\omega}^Z, Q_{\omega\nu}^Z\} \) and \( \{Q_{\mu\mu}^Z, Q_{\omega\omega}^Z, Q_{\mu\omega}^Z, Q_{\omega\mu}^Z\} \) from Eq. (4.1), and generate two quantities \( Q_{M1}^Z \) and \( Q_{M2}^Z \) given by

\[
\begin{align*}
Q_{M1}^Z &= Q_{\nu\nu}^Z e^{2\nu} + Q_{\omega\omega}^Z e^{2\omega} - Q_{\nu\omega}^Z e^{\nu + \omega} - Q_{\omega\nu}^Z e^{\omega + \nu}, \\
Q_{M2}^Z &= Q_{\mu\mu}^Z e^{2\mu} + Q_{\omega\omega}^Z e^{2\omega} - Q_{\mu\omega}^Z e^{\mu + \omega} - Q_{\omega\mu}^Z e^{\omega + \mu}.
\end{align*}
\]

Next, we cancel out \( Y_{11}^{12} \) and \( Y_{Z}^{21} \) by using \( (\mu^2 - \omega^2)(\mu - \omega) \) (4.2) to minus \( (\nu^2 - \omega^2)(\nu - \omega) \) \( Q_{M1}^Z \), and obtain:

\[
Y_{11}^Z \geq Y_{11}^{Z,L} = \frac{(\mu^2 - \omega^2)(\mu - \omega)Q_{M1}^Z - (\nu^2 - \omega^2)(\nu - \omega)Q_{M2}^Z}{(\mu - \omega)^2(\nu - \omega)^2(\mu - \nu)}.
\]

Similarly, the strategy to estimate \( e_{11}^{X,U} \) requires to cancel out \( Y_{0m}^X e_{0m}^X \) and \( Y_{n0}^X e_{n0}^X \). We have

\[
e_{11}^X \leq e_{11}^{X,U} = \frac{1}{(\nu - \omega)^2 Y_{11}^{XL}} \times \left( e^{2\nu} Q_{\nu\nu}^X E_{\nu\nu}^X + e^{2\omega} Q_{\omega\omega}^X E_{\omega\omega}^X - e^{\nu + \omega} Q_{\nu\omega}^X E_{\nu\omega}^X - e^{\omega + \nu} Q_{\omega\nu}^X E_{\omega\nu}^X \right)
\]

where \( Y_{11}^{X,L} \) can be estimated using a similar method to that for \( Y_{11}^Z \) in Eq. 4.2.

One decoy state

We consider an estimation method with only one decoy state \( \nu \) satisfying \( \mu > \nu \). To estimate \( Y_{11}^{Z,L} \), firstly, we simultaneously cancel out all the third order terms \( Y_{12}, Y_{21}, Y_{30}, Y_{03} \):

\[
\mu^3 \times Q_{\nu\nu}^Z e^{2\nu} - \nu^3 \times Q_{\mu\mu}^Z e^{2\mu} = \mu^2 \nu^2 (\mu - \nu) Y_{11}^Z + \mu^3 (Y_{00}^Z + \nu Y_{01}^Z + \nu^2 Y_{02}^Z/2 + \nu^2 Y_{20}^Z/2) - \nu^3 (Y_{00}^Z + \mu Y_{01}^Z + \mu^2 Y_{02}^Z/2 + \mu^2 Y_{20}^Z/2) + \sum_{n+m>3} \frac{\nu^{n+m} \mu^3 - \mu^{n+m} \nu^3}{n!m!} Y_{nm}^Z \leq \mu^3 \nu^2 (\mu - \nu) Y_{11}^Z + \nu^3 (Y_{00}^Z + \nu Y_{01}^Z + \nu Y_{10}^Z + \nu^2 Y_{02}^Z/2 + \nu^2 Y_{20}^Z/2),
\]

(4.3)
where the inequality comes from the fact that \((\nu^{n+m} - \mu^{n+m}) < 0\) for \(n + m > 3\). Next, from \(Q_{\nu\nu}^{Z}E_{\nu\nu}^{Z}e^{2\nu} = \sum_{n,m=0}^{\infty} \frac{\nu^{n+m}}{n!m!} Y_{nm}^{Z}e_{nm}^{Z} \geq Y_{00}^{Z}e_{00}^{Z} + \nu Y_{01}^{Z}e_{01}^{Z} + \nu Y_{10}^{Z}e_{10}^{Z} + \nu^{2} Y_{02}^{Z}e_{02}^{Z}/2 + \nu^{2} Y_{20}^{Z}e_{20}^{Z}/2 \geq (Y_{00}^{Z} + \nu Y_{01}^{Z} + \nu Y_{10}^{Z} + \nu^{2} Y_{02}^{Z}/2 + \nu^{2} Y_{20}^{Z}/2)/2\), \(4.5\) where the final equality is from \(e_{0m} = e_{m0} = 1/2\). This is a standard assumption in QKD descending from the fact that the error rate cause by 0-photon pulse is 1/2. Therefore, by combining Eq. \((4.4)\) and Eq. \((4.5)\), we have a lower bound for \(Y_{11}^{Z}\)

\[
Y_{11}^{Z} \geq Y_{11}^{Z,L} = \frac{\mu^{3} Q_{\nu\nu}^{Z}e^{2\nu}(1 - 2E_{\nu\nu}^{Z}) - \nu^{3} Q_{\mu\mu}^{Z}e^{2\mu}}{\mu^{2}\nu^{2}(\mu - \nu)} \tag{4.6}
\]

To estimate \(e_{11}^{X,U}\), we use the same method as Eq. \((4.3)\) and obtain an upper bound:

\[
e_{11}^{X,U} \leq e_{11}^{X,U} = \frac{1}{(\mu - \nu)^{2}Y_{11}^{X,L}} \times (e^{2\mu}Q_{\mu\mu}^{X}E_{\mu\mu}^{X} + e^{2\nu}Q_{\nu\nu}^{X}E_{\nu\nu}^{X} - e^{\mu+\nu}Q_{\mu\nu}^{X}E_{\mu\nu}^{X} - e^{\nu+\mu}Q_{\nu\mu}^{X}E_{\nu\mu}^{X}) \tag{4.7}
\]

### 4.1.3 Simulation

<table>
<thead>
<tr>
<th>(\eta_{d})</th>
<th>(e_{d})</th>
<th>(Y_{0})</th>
<th>(f_{e})</th>
<th>(\epsilon)</th>
<th>(N)</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.5%</td>
<td>1.5%</td>
<td>6.02 \times 10^{-6}</td>
<td>1.16</td>
<td>10^{-10}</td>
<td>10^{12}</td>
</tr>
</tbody>
</table>

Table 4.2: List of practical parameters for numerical simulations. These experimental parameters, including the detection efficiency \(\eta_{d}\), the total misalignment error \(e_{d}\) and the background rate \(Y_{0}\), are from the 144 km QKD experiment reported in [103]. Since two SPDs are used in [103], the background rate of each SPD here is roughly half of the value there. We assume that the four SPDs in MDI-QKD have identical \(\eta_{d}\) and \(Y_{0}\). \(\epsilon\) is the security bound considered in our finite-data analysis. \(N\) denotes the total number of signals (WCPs) sent by Alice and Bob.

In all the simulations presented below, we use the experimental parameters, listed in Table 4.2, mostly from the long-distance QKD experiment reported in [103]. Moreover, we use a rather generic channel model that includes an intrinsic error rate which simulates the misalignment and instability of the optical system (see Section 5.1).

The simulation results using numerical methods for different number of decoy states are shown in Figs. 4.1, 4.2. In the asymptotic case (Fig. 4.1), the key rate with two
Chapter 4. Decoy-state MDI-QKD with finite resources

Figure 4.1: (Color online) Asymptotic key rates with different number of decoy states. The solid curve is the one with infinitely many decoy states. The dashed, dashed-dotted, dotted curves are respectively the one, two, three decoy-state results using numerical methods (Section 4.1.1). The signal state $\mu$ is optimized in all cases, while some reasonable values of decoy states are adopted: for one decoy state, $\nu=0.0005$; for two decoy states, $\nu=0.01$ and $\omega=0.0005$; for three decoy states, $\nu_1=0.1$, $\nu_2=0.01$ and $\omega=0.0005$. We emphasize that the key rates with analytical methods are almost overlapped with the ones presented in this figure, which shows that the analytical approaches provide a highly good estimation. The estimation using two decoy states gives a nearly similar key rate to the one with three decoy states and is higher than one decoy-state case. Therefore, two decoy states can already result in a near optimal estimation and more decoy states cannot improve the key rate. Reproduced from [46] with permission. ©2014 APS.

de decoy states is close to the one with three decoy states as well as infinitely many decoy states and it is also larger than that with one decoy state. In a practical setting with finite data-set (Figs. 4.2), for simplicity, the statistical fluctuations are simulated using the standard error analysis method [63]. A more rigorous finite-key analysis will be presented in next Section. A full parameter optimization is conducted (see Section 5.2). Our results show that after a full parameter optimization, two decoy states can give an almost optimal key rate, which is much higher than the one with one decoy state. Three decoy states cannot improve the key rates much. Notice that the key rates using the analytical methods are almost overlapped with the ones using numerical methods. This shows that the analytical approaches provide a good decoy-state estimation. Therefore,
4.2 Finite-key analysis

As mentioned before, another question that needs to be solved is related with the fact that any QKD realization only produces a finite amount of data. Of course, a real-life QKD experiment is always completed in finite time, which means that the length of the output secret key is obviously finite. Thus, the parameter estimation procedure in QKD needs to take the statistical fluctuations of the different parameters into account. In this Section, we present a rigorous finite-key analysis for MDI-QKD. In contrast to existing heuristic results [97, 104], we provide, for the first time, a security proof in the finite-key regime that is valid against general attacks, and satisfies the composability definition [105].
of QKD. Moreover, we apply large deviation theory, specifically a multiplicative form of Chernoff bound, to perform the parameter estimation step. This Section is based on [47].

4.2.1 Security definition

Let us first review the security framework [105] that we are considering here. A general QKD protocol (executed by Alice and Bob) generates either a pair of bit strings $S_A$ and $S_B$, or a symbol $\perp$ to indicate the abort of the protocol. In general, the string of Alice, $S_A$, can be quantum mechanically correlated with a quantum state that is held by the adversary. Mathematically, this situation is described by the classical-quantum state

$$\rho_{AE} = \sum_s |s\rangle\langle s| \otimes \rho_E^s,$$

where \{\ket{s}\}_s denotes an orthonormal basis for Alice’s system, and the subscript E indicates the system of the adversary.

Ideally, we say that a QKD protocol is secure if it satisfies two conditions, namely the correctness and the secrecy. The correctness condition is met if $S_A = S_B$, i.e., Alice’s and Bob’s bit strings are identical. The secrecy condition is met if $\rho_{AE} = U_A \otimes \rho_E$, where $U_A = \sum_s \frac{1}{2^{|S|}} |s\rangle\langle s|$ is the uniform mixture of all possible values of the bit string $S_A$. That is, the system of the adversary is completely decoupled from that of Alice.

Owing to the presence of errors, however, these two conditions can never be perfectly met. For example, in the finite-key regime it is impossible to guarantee $S_A = S_B$ with certainty. In practice, this implies that we need to allow for some minuscule errors. That is, we say that a QKD scheme is $\epsilon_{\text{cor}}$-correct if $\Pr[S_A \neq S_B] \leq \epsilon_{\text{cor}}$, i.e., the probability that Alice’s and Bob’s bit strings are not identical is not greater than $\epsilon_{\text{cor}}$. Similarly, we say that a protocol is $\epsilon_{\text{sec}}$-secret if

$$\frac{1}{2} \| \rho_{AE} - U_A \otimes \rho_E \|_1 \leq \epsilon_{\text{sec}},$$

where $\| \cdot \|_1$ denotes the trace norm. That is, the state $\rho_{AE}$ is $\epsilon_{\text{sec}}$-close to the ideal situation described by $U_A \otimes \rho_E$. Thereby a QKD protocol is said to be $\epsilon$-secure if it is both $\epsilon_{\text{cor}}$-correct and $\epsilon_{\text{sec}}$-secret, with $\epsilon_{\text{cor}} + \epsilon_{\text{sec}} \leq \epsilon$. With this security definition we are able to guarantee that the security of the protocol holds even when combined with other protocols, i.e., the protocol is secure in the so-called universally composable framework [105].
4.2.2 Security analysis

To prove the finite-key security for MDI-QKD, it is convenient to introduce some parameters, and to define the protocol in the practical setting with finite resources. We recap the MDI-QKD protocol as follows.

1. **State Preparation** Alice and Bob repeat the first four steps of the protocol for \(i = 1, \ldots, N\) till the conditions in the Sifting step are met. For each \(i\), Alice chooses an intensity \(a \in \{a_0, a_1, \ldots, a_{d_a}\}\), a basis \(\lambda \in \{Z, X\}\), and a random bit \(r \in \{0, 1\}\) with probability \(p_{a, \lambda}/2\). Here \(a_s = \mu (a_d = \nu)\) is the intensity of the signal (decoy) states. Next, she generates a quantum signal of intensity \(a\) prepared in the basis state of \(\lambda\) given by \(r\). Likewise, Bob does the same.

2. **Distribution** Alice and Bob send their states to Charles via the quantum channel.

3. **Measurement** If Charles is honest, he measures the signals received with a Bell state measurement. In any case, he informs Alice and Bob (via a public channel) of whether or not his measurement was successful. If he succeeds, he reveals the Bell state obtained.

4. **Sifting** If Charles reports a successful result, Alice and Bob broadcast (via an authenticated channel) their intensity and basis settings. For each Bell state \(k\), we define two groups of sets: \(Z_k^{a,b}\) and \(\lambda_k^{a,b}\). The first (second) one identifies signals where Charles declared the Bell state \(k\) and Alice and Bob selected the intensities \(a\) and \(b\) and the basis \(Z\) (\(X\)). The protocol repeats these steps until \(|Z_k^{a,b}| \geq \Lambda^{a,b}_k\) and \(|\lambda_k^{a,b}| \geq M^{a,b}_k \forall a, b, k\). Next, say Bob flips part of his bits to correctly correlate them with those of Alice (see Table 3.1). Afterwards, they execute the last steps of the protocol for each \(k\).

5. **Parameter Estimation** Alice and Bob use \(n_k\) random bits from \(Z_k^{a,b}\) to form the code bit strings \(Z_k\) and \(Z_k'\), respectively. The remaining \(R_k\) bits from \(Z_k^{a,b}\) are used to compute the error rate \(E_k^{a,b} = \frac{1}{R_k} \sum_i r_i \oplus r'_i\), where \(r'_i\) are Bob’s bits. If \(E_k^{a,b} > E_{\text{tol}}\), Alice and Bob assign an empty string to \(S_k\) and abort steps 6 and 7 for this \(k\). The protocol only aborts if \(E_k^{a,b} > E_{\text{tol}} \forall k\). If \(E_k^{a,b} \leq E_{\text{tol}}\), Alice and Bob use \(Z_k^{a,b}\) and \(\lambda_k^{a,b}\) to estimate \(n_{k,0}, n_{k,1}\) and \(e_{k,1}\). The parameter \(n_{k,0} (n_{k,1})\) is a lower bound for the number of bits in \(Z_k\) where Alice (Alice and Bob) sent a vacuum (single photon) state. \(e_{k,1}\) is an upper bound for the single photon phase error rate. If \(e_{k,1} > e_{\text{tol}}\), an empty string is assigned to \(S_k\) and steps 6 and 7 are aborted for this \(k\), and the protocol only aborts if \(e_{k,1} > e_{\text{tol}} \forall k\).

6. **Error Correction** For those \(k\) that passed the parameters estimation step, Bob obtains an estimate \(\hat{Z}_k\) of \(Z_k\) using an information reconciliation scheme. For this, Alice sends him leakEC,\(k\) bits of error correction data. Next, Alice computes a hash of \(Z_k\) of length \(\lceil \log_2(4/e_{\text{cor}}) \rceil\) using a random universal2 hash function, which she sends to Bob together with the hash [105]. If \(\text{hash}(\hat{Z}_k) \neq \text{hash}(Z_k)\), Alice and Bob assign an empty string to \(S_k\) and abort step 7 for this \(k\). The protocol only aborts if \(\text{hash}(\hat{Z}_k) \neq \text{hash}(Z_k) \forall k\).

7. **Privacy Amplification** If \(k\) passed the error correction step, Alice and Bob apply a random universal2 hash function to \(Z_k\) and \(\hat{Z}_k\) to extract two shorter strings of length \(\ell_k\) [105]. Alice obtains \(S_k\) and Bob \(\hat{S}_k\). The concatenation of \(S_k (\hat{S}_k)\) form the secret key \(S_A (S_B)\).
The MDI-QKD protocol is both $\epsilon_{\text{cor}}$-correct and $\epsilon_{\text{sec}}$-secret, given that the length $\ell$ of the secret key $S_A$ is selected appropriately for a given set of observed values. The correctness of the protocol is guaranteed by its error correction step, where, for each possible Bell state $k$, Alice sends a hash of $Z_k$ to Bob, who compares it with the hash of $\hat{Z}_k$. If both hash values are equal, the protocol gives $S_k = \hat{S}_k$ except with error probability $\epsilon_{\text{cor}}/4$. If hash($\hat{Z}_k$) $\neq$ hash($Z_k$), it outputs the empty string (i.e., the protocol is trivially correct). Moreover, if the protocol aborts, the result is $\perp$, i.e., it is also correct. This guarantees that $S_A = S_B$ except with error probability less or equal than $\epsilon_{\text{cor}}$. Alternatively to this method, note that Alice and Bob may also guarantee the correctness of the protocol by exploiting properties of the error correcting code employed.

The protocol is $\epsilon_{\text{sec}}$-secret, with $\epsilon_{\text{sec}} \leq \sum_k \epsilon_{k,\text{sec}}$, if the length $\ell_k$ of each bit string $S_k$, which forms the secret key $S_A$, satisfies

$$\ell_k \leq n_{k,0} + n_{k,1} \left[ 1 - h(e_{k,1}) \right] - \text{leak}_{EC,k} - \log_2 \frac{8}{\epsilon_{\text{cor}}} - 2 \log_2 \frac{2}{e_k e_k} - 2 \log_2 \frac{1}{2 \epsilon_{k,PA}},$$

with $\epsilon_{k,\text{sec}} = 2(\epsilon'_k + 2\epsilon_{k,e} + \epsilon_k) + \epsilon_{k,b} + \epsilon_{k,0} + \epsilon_{k,1} + \epsilon_{k,PA}$, and where $h(x) = -x \log_2(x) - (1 - x) \log_2(1 - x)$ is the binary Shannon entropy. Here, the parameters $\epsilon_{k,0}$, $\epsilon_{k,1}$, and $\epsilon_{k,e}$ quantity, respectively, the probability that the estimation of the terms $n_{k,0}$, $n_{k,1}$ and $e_{k,1}$ is incorrect. A sketch of the proof of Eq. (4.8) can be found in Ref. [47]. There it is also explained the meaning of all the epsilons contained in the term $\epsilon_{k,\text{sec}}$, which we omit here for simplicity. In the asymptotic limit of very large data blocks, the terms reducing the length of $S_A$ due to statistical fluctuations may be neglected, and thus $\ell$ satisfies $\ell \leq \sum_k \max \{ n_{k,0} + n_{k,1} \left[ 1 - h(e_{k,1}) \right] - \text{leak}_{EC,k}, 0 \}$, as previously obtained in [32]. That is, $n_{k,0}$ and $n_{k,1}$ provide a positive contribution to the secret key rate, while $n_{k,1} h(e_{k,1})$ and $\text{leak}_{EC,k}$ reduce it. The term $n_{k,1} h(e_{k,1})$ corresponds to the information removed from $Z_k$ in the privacy amplification step of the protocol, while $\text{leak}_{EC,k}$ is the information revealed by Alice in the error correction step.

### 4.2.3 Parameter estimation

We present an estimation method to obtain the relevant parameters $n_{k,0}$, $n_{k,1}$ and $e_{k,1}$. This method is basically the same as that of Section 4.1, while the only difference is that in a finite-data setting, we should take the statistical fluctuations into account. We solve this problem using techniques in large deviation theory. More specifically, we employ Chernoff bound [106]. Remarkably, Chernoff bound takes advantage of the property of the distribution and provides good bounds even in a high-loss regime.
To simplify the discussion, let us consider the estimation of the parameter $n_{k,0}$. The method to obtain $n_{k,1}$ and $e_{k,1}$ follows similar arguments. The procedure can be divided into two steps. First, we calculate a lower bound for the number of indexes in $Z_{k}^{a_{k},b_{k}}$ where Alice sent a vacuum state. This quantity is denoted as $m_{k,0}$. Second, we compute $n_{k,0}$ from $m_{k,0}$ using Serfling inequality [107] for random sampling without replacement.

In the first step we use a multiplicative form of Chernoff bound [106] for independent random variables, which does not require the prior knowledge on the population mean. More precisely, we have the following claim.

**Claim 1.** Let $X_1, X_2, \ldots, X_n$, be a set of independent Bernoulli trials that satisfy $\Pr(X_i = 1) = p_i$. And, let $X = \sum_{i=1}^{n} X_i$ and $\mu = E[X] = \sum_{i}^{n} p_i$, where $E[\cdot]$ is the mean value. Then, we have that

$$X = \mu + \delta,$$

except with error probability $\gamma = \varepsilon + \hat{\varepsilon}$, where the parameter $\delta \in [-\Delta, \hat{\Delta}]$, with $\Delta = g(X, \varepsilon^4)$ and $\hat{\Delta} = g(X, \hat{\varepsilon}^2)$, and the function $g(x, y) = \sqrt{x \ln (y^{-2})}$, given that $(\hat{\varepsilon}^{-1})^{1/X} \leq \exp [2/ \log_2 (e)]^2$ and $(\varepsilon^{-1})^{1/X} \leq \exp (1/4)$.

To apply this statement and be able to obtain the parameter $m_{k,0}$, we rephrase the protocol described in Section 4.2.2 as follows. For each signal, we consider that Alice (Bob) first chooses a photon number $n$ ($m$) and sends the signal to Charles, who declares whether his measurement is successful or not. After, Alice decides the intensity setting $a$, and Bob does the same. This virtual protocol is equivalent to the original one because the essence of decoy-state QKD is precisely that Alice and Bob could have postponed the choice of which states are signals or decoys after Charles’ declaration of the successful events. This is possible because Alice’s and Bob’s observable commute with those of Charles. This result shows that for each combination $n$ and $m$, the signal and decoy states provide a random sample of the population of all signals containing $n$ and $m$ photons respectively. Therefore, one can apply random sampling theory in classical statistics to the quantum problem.

Let $\mathcal{S}_{k,nm}$ denote the set that identifies those signals sent by Alice and Bob with $n$ and $m$ photons respectively, when they select the Z basis and Charles announces the Bell state $k$. And, let $|\mathcal{S}_{k,nm}| = S_{k,nm}$, and $p_{a,b|nm,Z}$ be the conditional probability that Alice and Bob have selected the intensity settings $a$ and $b$, given that their signals contain, respectively, $n$ and $m$ photons prepared in the Z basis. Then, if we apply the above equivalence, independently of each other and for each signal Alice and Bob assign to each element in $\mathcal{S}_{k,nm}$ the intensity setting $a, b$, with probability $p_{a,b|nm,Z}$. 
Let $X_{i[k, nm]}^{a, b}$ be 1 if the $i$th element of $S_{k, nm}$ is assigned to the intensity setting combination $a, b$, and otherwise 0. And, let

$$X_k^{a, b} = \sum_{n, m} \sum_{i=1}^{S_{k, nm}} X_{i[k, nm]}^{a, b} = |Z_k^{a, b}|,$$

where $\mu = E[X_k^{a, b}] = \sum_{n, m} p_{a, b|nm} Z_{S_{k, nm}}$. Then, Claim 1 implies that

$$|Z_k^{a, b}| = \sum_{n, m} p_{a, b|nm} Z_{S_{k, nm}} + \delta_{a, b},$$

except with error probability $\gamma_{a, b} = \varepsilon_{a, b} + \hat{\varepsilon}_{a, b}$, where $\delta_{a, b} \in [-\Delta_{a, b}, \hat{\Delta}_{a, b}]$, with $\Delta_{a, b} = g(|Z_k^{a, b}|, \varepsilon_{a, b}^1)$ and $\hat{\Delta}_{a, b} = g(|Z_k^{a, b}|, \varepsilon_{a, b}^2)$.

Using similar arguments, we find that the parameter $m_{k, 0}$ can be written as

$$m_{k, 0} = \sum_{m} p_{a, b|0m, Z_{S_{k, 0m}}} - \Delta_0,$$

except with error probability $\varepsilon_{0, 0}$, where $\Delta_0 = g(\sum_{m} p_{a, b|0m, Z_{S_{k, 0m}}}, \varepsilon_{0, 0})$. Now, it is easy to find a lower bound for $m_{k, 0}$. One only needs to minimise Eq. (4.11) given the linear constraints imposed by Eq. (4.11) for all $a, b$. This problem can be solved using the methods presented in Section 4.1.

The second step of the procedure is quite direct. Note that Alice forms her bit string $Z_k$ using $n_k$ random indexes from $Z_k^{a, b_k}$. Using [107] we obtain

$$n_{k, 0} = \max \left\{ \left\lfloor n_{k} \frac{m_{k, 0}}{|Z_k^{a, b_k}|} - n_k \Lambda(|Z_k^{a, b_k}|, n_k, \varepsilon_{k, 0}^\eta) \right\rfloor, 0 \right\},$$

except with error probability

$$\varepsilon_{k, 0} \leq \varepsilon_{k, 0}^0 + \varepsilon_{k, 0}^\eta,$$

where $\varepsilon_{k, 0}^0$ corresponds to the total error probability in the estimation of $m_{k, 0}$, and the function $\Lambda(x, y, z)$ is defined as $\Lambda(x, y, z) = \sqrt{(x - y + 1) \ln (z^{-1})/(2xy)}$.

The method to obtain $n_{k, 1}$ and $\epsilon_{k, 1}$ is similar by following the decoy-state methods in Section 4.1 [47].

### 4.2.4 Simulation

In this section we analyse the behaviour of the secret key rate provided in Eq. (4.8). We use experimental parameters from Table 4.2, and the system model of Appendix A. In addition, we fix the security bound to $\epsilon = 10^{-10}$. 

Figure 4.3: Secret key rate $\ell/N$ as a function of the distance. The dotted line represent the asymptotic case with $N=\infty$. The solid lines correspond to different values for the total number of signals $N$ sent by Alice and Bob. The overall misalignment in the channel is 1.5%, and the security bound $\epsilon = 10^{-10}$, which is a conservative bound typically used in the security proof of QKD [10] (this level of security dictates a much wider confidence interval drawn from the measurements). For simulation purposes we consider the experimental parameters listed in Table 4.2. Our results show clearly that even with a realistic finite size of data, say $N = 10^{12}$ to $10^{14}$, it is possible to achieve secure MDI-QKD at long distances. In comparison, the dotted line represents a lower bound on the secret key rate for the asymptotic case where Alice and Bob send Charles infinitely many signals and use an infinite number of decoy settings. Reproduced from [47] with permission. ©2014 NPG.

The results are shown in Figs. 4.3 and 4.4 for the situation where Alice and Bob use two decoy states each. In this scenario, we obtain the parameters $n_{k,0}$, $n_{k,1}$ and $\epsilon_{k,1}$ using the analytical estimation procedure introduced in Section 4.1.2. The first figure illustrates the secret key rate (per pulse) $\ell/N$ as a function of the distance between Alice and Bob for different values of the total number of signals $N$ sent. We fix $\epsilon_{cor} = 10^{-15}$; this corresponds to a realistic hash tag size in practice [105]. Also, we fix the intensity of the weakest decoy states to $a_{d_2} = b_{d_2} = 5 \times 10^{-4}$. Moreover, we assume an error correction leakage of $\text{leak}_{EC,k} = n_s f_e h(E_k^{a,b})$. For a given distance, we optimise numerically $\ell/N$ over all the free parameters of the protocol (See Section 5.2). Our simulation result shows clearly that MDI-QKD is feasible with current technology and does not require high detection efficiency detectors for its implementation. If Alice and Bob use laser diodes operating at 1 GHz repetition rate, and each of them sends $N = 10^{13}$ signals, we find, for instance,
Figure 4.4: The plot shows the secret key rate $\ell/N$ in logarithmic scale as a function of the total number of signals $N$ sent by Alice and Bob in the limit of zero distance. The security bound $\epsilon = 10^{-10}$. The solid lines correspond to different values for the intrinsic error rate due to the misalignment and instability of the optical system. The horizontal dotted lines show the asymptotic rates. The experimental parameters are the ones described in Table 4.2. Our results show that, even for a finite size of signals sent by Alice and Bob, MDI-QKD is robust to intrinsic errors due to basis misalignment and instability of the optical system. Reproduced from [47] with permission. ©2014 NPG.

that they can distribute a 1 Mb secret key over a 75 km fiber link in less than 3 hours. This scenario corresponds to the red line shown in Fig. 4.3. Notice that, at telecom wavelengths, standard InGaAs detectors have modest detection efficiency of about 15%. Since MDI-QKD requires two-fold coincidence rather than single-detection events, as is the case in the standard decoy state protocol, the key rate of MDI-QKD is lower than that of the standard decoy state scheme. However, with high-efficiency detectors [78], the key rate of MDI-QKD can be made comparable to that of the standard decoy state protocol.

The second figure illustrates $\ell/N$ as a function of $N$ for different values of the misalignment in the limit of zero distance. For comparison, this figure also includes the asymptotic secret key rate when Alice and Bob send an infinite number of signals and use an infinite number of decoy states. Our results show that significant secret key rates are already possible with $10^{11}$ signals, given that the error rate is not too large.
4.3 Conclusion

To sum up, we have presented analytical and numerical decoy-state methods with one, two and three decoy states. By clearly comparing these methods, we find that two decoy states combined with a full parameter optimization is already close to the optimal estimation and more decoy states cannot improve the key rate much in both asymptotic and finite-data cases. Experimentalist can readily implement MDI-QKD by using our two decoy-state (analytical or numerical) approach. We have also proved the security of MDI-QKD in the finite-key regime against general attacks. Our results clearly demonstrate that even with practical signals (WCPs) and a finite size of data (say $10^{12}$ to $10^{14}$ signals) it is possible to perform secure MDI-QKD over long distances (up to about 150 km).
Chapter 5

Practical aspects for MDI-QKD

Besides the decoy-state method and finite-key analysis discussed in the past chapter, there are still other practical issues related to the implementations of MDI-QKD. These include, the error sources in the system, the methodologies to optimize parameters and MDI-QKD in an asymmetric setting, where the two channels connect Alice to Charles and Bob to Charles have different transmittances. All these practical aspects will be addressed in this Chapter. This Chapter is based on [48, 46].

5.1 Practical error sources

In this section, we consider the practical errors in a MDI-QKD setting [32]. To model the practical error sources, we focus on the fiber-based polarization-encoding MDI-QKD system proposed in [32] and demonstrated in [95, 55]. Notice, however, that with some modifications, our analysis can also be applied to other implementations such as free-space transmission, the phase-encoding scheme and the time-bin-encoding scheme. See also [108] and [109] respectively for models of phase-encoding and time-bin-encoding schemes.

A comprehensive list of practical error sources is as follows.

1. Polarization misalignment (or rotation).

2. Mode mismatch including time-jitter, spectral mismatch, etc.

3. Fluctuations of the intensities (modulated by Alice and Bob) at the source.

4. Background rate.
5. Asymmetry of the beam splitter.

Here, we primarily analyze the first two error sources, i.e., polarization misalignment and mode mismatch. The other error sources present minor contributions to the QBER in practice.

5.1.1 Polarization misalignment

Polarization misalignment (or rotation) is one of the most significant factors contributing to the QBER in not only the polarization-encoding BB84 system [2] but also the polarization-encoding MDI-QKD system. Since MDI-QKD requires two transmitting channels and one BSM (instead of one channel and a simple measurement as in the BB84 protocol), it is cumbersome to model its polarization misalignment. Here, we solve this problem by proposing a simple model in Fig. 5.1. One of the polarization beam splitters (e.g. PBS2 in Fig. 5.1) is defined as the fundamental measurement basis. Three unitary operators, \{U_1, U_2, U_3\}, are considered to model the polarization misalignment of each channel [6]. The operator \(U_1 (U_2)\) represents the misalignment of Alice’s (Bob’s) channel transmission, while \(U_3\) models the misalignment of the other measurement setting, PBS1.
For simplicity, we consider a simplified model with a 2-dimensional unitary matrix:

\[
U_k = \begin{pmatrix}
\cos \theta_k & -\sin \theta_k \\
\sin \theta_k & \cos \theta_k
\end{pmatrix},
\]

(5.1)

where \(k = 1, 2, 3\) and \(\theta_k\) (polarization-rotation angle) is in the range of \([-\pi, \pi]\). For each value of \(k\), we define the polarization misalignment error \(e_k = \sin^2 \theta_k\) and the total error \(e_d = \sum_{k=1}^{3} e_k\). Note that \(e_d\) is equivalent to the systematic QBER in a polarization-encoding BB84 system.

From the model of Fig. 5.1, we can analyze the effect of polarization misalignment by evaluating the secure key rate given by Eq. (3.1). By using the practical parameters listed in Table 4.2, we perform a numerical simulation of the asymptotic key rates for different values of polarization misalignment, \(e_d\). The result is shown in Fig. 5.2. In this simulation, we temporarily ignore mode mismatch (i.e., set \(e_m = 0\) in Table 4.2) and make two practical assumptions for the polarization misalignment: a) each polarization-rotation angle, \(\theta_k\), follows a Gaussian distribution with a standard deviation of \(\theta_{\text{std}}^k = \arcsin(\sqrt{e_k})\); and b) the probability distribution of \(e_k\) is selected as \(e_1 = e_2 = 0.475e_d\) and \(e_3 = 0.05e_d^2\). Fig. 5.2 shows that a polarization-encoding system can tolerate up to about 6.7% polarization misalignment at 0 km, while at 120 km it can only tolerate up to 5% misalignment. It also shows that MDI-QKD is moderately robust to errors due to polarization misalignment.

5.1.2 Mode mismatch

In practice, due to the imperfections of experimental devices, it is inevitable that the two modes interfering at the BS of Charles have mismatch. This involves, for instance, time jitter, spectral mismatch, spatial mismatch and so forth. Such mode mismatch results in an imperfect interference between Alice’s pulse and Bob’s pulse, and thus it introduces QBER. Here, I primarily use the model of mismatch in the time domain, called time-jitter, to discuss our method to analyze mode mismatch. Time-jitter is defined here as

\[\text{That is, if we denote the two incoming modes in the horizontal and vertical polarization by the creation operators } a_h^\dagger \text{ and } a_v^\dagger, \text{ and the outgoing modes by } b_h^\dagger \text{ and } b_v^\dagger, \text{ then the unitary operator yields an evolution of the form } b_h^\dagger = \cos \theta_k a_h^\dagger - \sin \theta_k a_v^\dagger \text{ and } b_v^\dagger = \sin \theta_k a_h^\dagger + \cos \theta_k a_v^\dagger. \text{ This unitary matrix is a simple form rather than the general one (see Section I.A in [6]). Nonetheless, we believe that the result for a more general unitary transformation will be similar to our simulation results.}

\[\text{Two remarks for the distribution of the three unitary operators: a) We assume that the two channel transmissions, i.e., } U_1 \text{ and } U_2, \text{ introduce much larger polarization misalignments than the other measurement basis, } U_3 \text{ (PBS1 in Fig. 5.1), because PBS1 is located in Charles’s local station and can be carefully aligned (in principle). Hence, we choose } e_1 = e_2 = 0.475e_d \text{ and } e_3 = 0.05e_d. \text{ b) Notice that the simulation result is more or less independent of the distribution of } e_k.\]
Figure 5.2: Polarization misalignment tolerance. Following the model illustrated in Fig. 5.1, we incorporate the polarization misalignment into the derivation of the asymptotic key rate given by Eq. (3.1). We find that MDI-QKD is robust against practical errors due to polarization misalignment. Reproduced from [48] with permission. ©2013 IOP.

Figure 5.3: Model for mode mismatch in the time domain (time-jitter). Alice’s state is defined as the reference basis, while Bob’s state is a superposition of Alice’s fundamental mode $|T_a\rangle$ and the orthogonal mode $|\overline{T}_a\rangle$ (see Eq. (5.2)). Reproduced from [48] with permission. ©2013 IOP.

the variance in arrival times of Alice’s and Bob’s packets at Charles’s station. My model is shown in Fig. 5.3. We describe Alice’s and Bob’s quantum states in the time domain as

$$
\begin{align*}
Alice & : |\phi_a\rangle = |T_a\rangle \\
Bob & : |\phi_b\rangle = \alpha|T_a\rangle + \beta|\overline{T}_a\rangle,
\end{align*}
$$

(5.2)

where $|\overline{T}_a\rangle$ is the orthogonal time mode of $|T_a\rangle$, $\beta=\sqrt{e_t}$, $\alpha=\sqrt{1-e_t}$, and $e_t$ is defined as the time-jitter that represents the probability of Alice’s state not overlapping with that
This model is a very general method that can be used to study the mode mismatch problem in other domains for a variety of quantum optics experiments involving quantum interference. For instance, a similar discussion can be applied to the spectral (wavelength) mismatch if we write Eq. (5.2) in the frequency domain. One can also refer to [110] for a general discussion about the spectral mismatch. Considering Eq. (5.2) in the form of Alice’s and Bob’s pulse shapes, we can also analyze the pulse-shape mismatch. Here we define the total mode mismatch in all domains as $e_m$.

Next, let us discuss how $e_m$ affects the key rate given by Eq. (3.1). As illustrated in Fig. 5.1, the overlapping modes between Alice’s and Bob’s pulses experience a HOM interference at the beam splitter (BS), while the non-overlapping modes transmit through the BS without interference. Assuming that $\eta_d \gg Y_0$ and ignoring the polarization misalignment for the moment, we find that the mode mismatch only affects the gains and the error rates in the X basis rather than those in the Z basis. Hence, in Eq. (3.1), $e_m$ mainly affects $e^{X}_{11}$. In practice, $e^{X}_{11}$ is estimated from the gains ($Q^{Z}_{\mu \mu}$) and QBERs ($E^{Z}_{\mu \mu}$) in the X basis. Similar to the analysis of the polarization misalignment in last section, we can incorporate $e_m$ into the derivations of $Q^{Z}_{\mu \mu}$ and $E^{Z}_{\mu \mu}$ following the model presented in Appendix A.

Using the parameters of Table 4.2, we simulate the asymptotic key rates for different values of $e_m$. The results are shown in Fig. 5.4. In this simulation, we temporarily ignore polarization misalignment (i.e., we set $e_d=0$) and only focus on mode mismatch. At 0 km, we find that the system can tolerate up to 80% mode mismatch and at 120 km, the tolerable value is about 50%. Hence, a polarization-encoding MDI-QKD system is less sensitive to mode mismatch than to polarization misalignment. Notice also that we have quantified the value of $e_m$ (see Table 4.2) by using the experimental parameters from [55] and find that $e_m$ is usually small in practice (e.g., below 5%). Therefore, mode mismatch does not appear to be a major problem in a MDI-QKD implementation.

### 5.1.3 Other errors

We discuss other practical error sources in MDI-QKD and show that their contribution to the QBER is not very significant in a practical MDI-QKD system.

---

3In experiment, the value of $e_t$ can be quantified from the fidelity between the two pulses in time domain. This fidelity can be obtained by measuring the pulse width and the time-jitter value between the two pulses. From the experimental values of [55], $e_t$ is below 1.5%.
Figure 5.4: Mode mismatch tolerance. In the asymptotic case, a polarization-encoding MDI-QKD system can tolerate up to 80% mode mismatch at 0 km. Mode mismatch does not appear to be a major problem in a polarization-encoding implementation of MDI-QKD. Reproduced from [48] with permission. ©2013 IOP.

**Intensity fluctuations at the source**

The intensity fluctuations of the signal and decoy states at the source are relatively small ($\sim 0.1$ dB) [102]. Additionally, Alice and Bob can in principle locally and precisely quantify their own intensities. Therefore, this error source can be mostly ignored in the theoretical model that analyzes the performance of practical MDI-QKD (but one could easily include it in the analysis).

**Threshold detector with background counts**

The threshold single photon detector (SPD) can be modeled by a beam splitter with $\eta_d$ transmission and $(1-\eta_d)$ reflection. The transmission part is followed by a unity efficiency detector, while the reflection part is discarded. $\eta_d$ is defined as the detector efficiency. Background counts can be treated to be independent of the incoming signals. For simplicity, the system model discussed in Appendix A assumes that the four SPDs (see Fig. 5.1) are identical and have a detection efficiency $\eta_d$ and a background rate $Y_0$. Note, however, that if this condition is not satisfied (i.e., there is some detection efficiency mismatch) our system model can be adapted to take care of this case.

All the simulations reported in the main text already consider a background rate of $Y_0=6.02 \times 10^{-6}$ (see Table 4.2). Fig. 5.5 simulates more general cases of the asymptotic key rates at different background count rates. At 0 km, the MDI-QKD system can tolerate up to $10^{-3}$ (per pulse) background counts before key generation rate drops to
Figure 5.5: Background counts tolerance. Following the model discussed in Section..., we simulate the asymptotic key rates at different background count rates. MDI-QKD is robust to background counts. Reproduced from [48] with permission. ©2013 IOP.

Figure 5.6: Wavelength dependence of a fiber-based beam splitter. If the laser wavelength is 1542 nm [55], the beam splitter ratio is 0.5007, which introduces negligible QBER (below 0.01%) in a typical MDI-QKD system. Reproduced from [48] with permission. ©2013 IOP.

zero.

**Beam splitter ratio**

In practice, for telecom wavelengths, the asymmetry of the beam splitter (BS) (i.e., not 50:50) is usually small. For instance, the wavelength dependence of the fiber-based BS in our lab (Newport-13101550-5050 fiber coupler) is experimentally quantified in Fig. 5.6. If the laser wavelength is 1542 nm [55], the BS ratio is 0.5007, which introduces negligible
QBER (below 0.01%) in a MDI-QKD system. Hence, this error source can also be ignored in the theoretical model of MDI-QKD.

5.2 Parameter optimization

An implementation of MDI-QKD requires the optimal parameters to optimize the system performance. In practical applications, the changes on channel loss and data size lead to different optimal parameters. Thus, a real-time optimization process for arbitrary inputs of channel loss and data size is required. However, some previous theoretical studies [97, 98, 99] and experimental implementations [95, 96] simply choose empirical parameters without optimization. Hence, an important question is: how can one optimize the parameters used in MDI-QKD? This question is non-trivial, given the large number of parameters involved. Another question is: how much will a careful parameter optimization improve performance? In this Section, I will discuss the methodologies to optimize the parameters in MDI-QKD.

5.2.1 Framework

We develop a general framework to optimize the parameters. This framework is shown in Fig. 5.7, and is composed of five steps.

1. Quantify the parameters and errors of the system. For simulation purposes, we will consider the parameters shown in Table 4.2.

2. Model the system using the techniques presented in Section 5.1. A complete model for a polarization-encoding MDI-QKD can be found in Appendix A.

3. Implement the finite decoy-state method discussed in Section 4.1.

4. Apply the finite-key analysis discussed in Section 4.2.

5. Perform the numerical optimization. In our simulation, we use a local search algorithm (see discussions below) to maximize the secure key rate and thus obtain the optimal parameters under different channel transmittances.

Our approach has already been applied to the experimental demonstration reported in [55], where the polarization misalignment is around 0.7% and the total mode mismatch is below 2%. Owing to the low operation rate there, the value of $\omega$ is set to 0.01. The optimal intensities in this scenario are $\mu_{opt} \approx 0.3$ and $\nu_{opt} \approx 0.1$. 
Figure 5.7: Framework for parameter optimization. Step 1 is to quantify the practical parameters and errors of the system (see Table 4.2 for some representative values). Step 2 is to model the system, i.e., derive the gain and QBER by incorporating the practical error sources (see Appendix A). Step 3 is to implement the finite decoy-state method (see Section 4.1). Step 4 is to apply the finite-key analysis (see Section 4.2). Step 5 is to perform the numerical optimization to get the optimal parameters for implementation. Reproduced from [48] with permission. ©2013 IOP.

5.2.2 Local search algorithm

Based on the above framework, a full optimization requires the search on many operating parameters (e.g., signal/decoy state intensities, basis probabilities and signal/decoy state probabilities). In all previous works on MDI-QKD [45], it is commonly assumed that the basis choice is independent of the intensity choice. We called it simplified choice (or partial optimization). If Z is used as the majority basis for key generation, the simplified choice will modulate most of signals (over 90%) on Z for all signal and decoy states. Nonetheless, the key parameter in a decoy-state estimation is the bit error rate in X, i.e., $e_{11}^X$, which requires a large amount of detection counts for the decoy states in X. The simplified choice, in contrast, results in a small number of such detection counts and thus increases the estimation error of $e_{11}^X$ due to large statistical fluctuations. Therefore, the optimal choice (or full optimization) refers to the basis choice dependent on the intensity choice.

To perform this optimal choice in BB84 and MDI-QKD in the case of two decoy states, we are required to optimize two sets of parameters: intensities of signal and decoy states $\mu, \nu, \omega$, and the probabilities to choose different intensities and bases
Table 5.1: Comparison of local search local search algorithm (LSA) and exhaustive search. The simulation is conducted on MDI-QKD with two decoy-state numerical approach (Appendix 4.1.1) using a standard desktop computer. A full optimization on eight dimensions including intensity and probability choices is performed. To reduce the computational complexity of exhaustive search, the intensity of $\omega$ is fixed at a near optimal value $\omega=0.0005$. Exhaustive search applies 10 points on seven other dimensions and thus it requires $10^7$ iterations for optimization. LSA uses the coordinate descent and backtrack search algorithm. LSA can not only maintain the accuracy of parameter optimization, but can also significantly reduce the computational complexity. The time needed for LSA is four orders of magnitude shorter than an exhaustive search.

$P_\mu, P_\nu, P_{Z|\mu}, P_{Z|\nu}, P_{Z|\omega}$, where $P_\mu$ denotes the probability to choose intensity $\mu$ and $P_{Z|\mu}$ denotes the conditional probability to choose Z basis conditional on $\mu$. Essentially, it requires a search over eight dimensions. Suppose that a trivial exhaustive search with 10 points on each dimension is conducted, it requires $10^8$ iterations to obtain the optimal parameters, which requires over 5000 hours on a standard desktop with 4-core CPUs (see Table 5.1). At first sight, it might appear to be a hard problem to perform full optimization. However, there is no need to perform an exhaustive search.

Here, we introduce a local search algorithm (LSA) in the field of computer science, to QKD for this optimization problem. In particular, we adopt the coordinate descent and backtrack search algorithm in our implementation. Coordinate descent can effectively transform a multi-dimensional optimization problem to a one-dimensional line search problem along the direction of one coordinate. This one-dimensional line search problem can be solved by backtrack search algorithm. As a consequence, the LSA enables one to perform a full optimization on all experimental parameters efficiently. We implement this LSA on MDI-QKD and show the comparison results to the trivial exhaustive search in Table 5.1. LSA can be four orders of magnitude shorter than an exhaustive search.

---

4In the case of Vacuum + weak decoy-state protocol, the search can be reduced to six dimensions.

5Even though a monte carlo optimization is conducted on a high-performance computer such as the one with 16-core CPUs, it still requires a few days to complete such optimization.
Figure 5.8: (Color online) Key rate with infinite number of data-set. The dotted black curve is the perfect key rate with infinitely many decoy states. The blue solid curve is our optimized key rate using the numerical approach with two decoy states, where the intensities are $\omega = 0.0005$, $\nu = 0.01$ and optimized $\mu$. For comparison purpose, we present the non-optimized and partially-optimized key rates using the methods and parameters of Refs. [97, 100, 99]: the black dashed curve is using Sun et al. [100] with $\omega = 0$, $\nu = 0.01$ and optimized $\mu$; the red dashed curve is using Yu et al. [99] with $\omega = 0.01$, $\nu = 0.1$ and $\mu = 0.3$; the green dashed curve is using Ma et al. [97] with $\omega = 0$, $\nu = 0.1$ and $\mu = 0.5$. Notice that if the parameter optimization is also applied to Refs. [97, 99], all the key rates are almost the same. In the asymptotic case, parameter optimization is simple, as only the intensities are required to be optimized and a smaller value of decoy-state intensity can result in a better estimation. Parameter optimization can still increase the key rate and extend the secure distance. Reproduced from [46] with permission. ©2014 APS.

5.2.3 Key rate comparison

For previous works on decoy-state MDI-QKD, Refs. [97, 99] used some typical parameters without optimization and Ref. [100] performed a partial optimization only on intensity choice. Here, we first compare our optimized key rate to those using the parameters and methods presented in Refs. [97, 99, 100]. Fig. 5.8 shows the comparison results in...
the asymptotic case with system parameter in Table 4.2. The dotted black curve is the perfect key rate with infinitely many decoy states. The blue solid curve is the key rate using our numerical method with two decoy states (see Section 4.1.1), where we choose the near optimal intensities by maximizing the key rate \(^6\). The black, red and green dashed curves are respectively using the method and parameters of [100], [99] and [97]. We can see that the key rates without parameter optimization in Refs [97, 99] are much lower than ours and Ref. [100]. Hence, parameter optimization both increases the key rate and extends the secure distance in the asymptotic case.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Optimal</th>
<th>Ref. [97]</th>
<th>Ref. [100]</th>
</tr>
</thead>
<tbody>
<tr>
<td>(\mu)</td>
<td>0.25</td>
<td>0.5</td>
<td>0.21</td>
</tr>
<tr>
<td>(\nu)</td>
<td>0.05</td>
<td>0.1</td>
<td>0.06</td>
</tr>
<tr>
<td>(\omega)</td>
<td>(10^{-6})</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(P_\mu)</td>
<td>0.58</td>
<td>0.33</td>
<td>0.33</td>
</tr>
<tr>
<td>(P_\nu)</td>
<td>0.30</td>
<td>0.33</td>
<td>0.33</td>
</tr>
<tr>
<td>(P_{X</td>
<td>\mu})</td>
<td>0.03</td>
<td>0.5</td>
</tr>
<tr>
<td>(P_{X</td>
<td>\nu})</td>
<td>0.71</td>
<td>0.5</td>
</tr>
<tr>
<td>(P_{X</td>
<td>\omega})</td>
<td>0.83</td>
<td>0.5</td>
</tr>
<tr>
<td>(R)</td>
<td>(1.68 \times 10^{-6})</td>
<td>(1.01 \times 10^{-7})</td>
<td>(1.64 \times 10^{-7})</td>
</tr>
</tbody>
</table>

Table 5.2: Comparison of parameters at a distance of 50 km standard fiber. More general comparison results are shown in Fig. 5.9. The 2nd column is the optimal parameters after a full parameter optimization. The 3rd and 4th columns are respectively the parameters from Refs. [97] and [100]. We can see that full optimization can improve the key rate \(R\) over one order of magnitude over the non-full-optimization of Refs. [97, 100]. This improvement mainly comes from optimizing the choices of intensities and probabilities. Notice that for the smallest decoy-state \(\omega\), modulating the optimal value of around \(10^{-6}\) is usually difficult in decoy-state QKD experiments [36, 37, 12]. However, we find that as long as the intensity of \(\omega\) is below \(1 \times 10^{-3}\), the key rate is very close to the optimum [46]. Reproduced from [46] with permission. ©2014 APS.

Fig. 5.9 shows the practical key rates, i.e., with statistical fluctuations, in the case of data-size \(N=10^{12}\). The optimal parameters and key rate for the distance of 50km (stan-

---

\(^6\)Notice that in the asymptotic case, the key rate increases with the decrease of the intensity values of decoy states and the probability choice of intensities and basis is not required. To have a fair comparison to [100], we choose the same value of decoy state \(\nu\) as \(\nu = 0.01\) and optimize \(\mu\). These intensity values can already give a key rate close to the perfect key rate with infinitely many decoy state.
Figure 5.9: (Color online) Practical key rate comparison (with statistical fluctuations). The optimal parameters and key rate in the distance of 50km (standard fiber) are shown in Table 5.2. All the key rates are simulated with $N=10^{12}$. The blue solid and red dashed-dotted curves (almost overlapped) are respectively our optimized key rates (after a full optimization) using the numerical (Appendix 4.1.1) and analytical (Appendix 4.1.2) methods with two decoy states. The black dashed curve is using the method of Ref. [100], where only partial parameters (i.e., the intensities) are optimized. The green dashed curve is using the method of Ref. [97], where some typical parameters are assumed without optimization. Without full parameter optimization, the key rates in Refs [97, 100] are around one order of magnitude lower than ours across different distances. Our method can enable secure MDI-QKD over 25km longer than [97, 100]. These results highlight the importance of parameter optimization in practical decoy-state MDI-QKD. Reproduced from [46] with permission. ©2014 APS.
light the importance of full parameter optimization in the practical implementation of
decoy-state MDI-QKD.

<table>
<thead>
<tr>
<th>Distance</th>
<th>0km</th>
<th>0km</th>
<th>0km</th>
<th>50km</th>
<th>50km</th>
<th>50km</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data-size</td>
<td>$10^{12}$</td>
<td>$10^{14}$</td>
<td>$10^{18}$</td>
<td>$10^{12}$</td>
<td>$10^{14}$</td>
<td>$10^{18}$</td>
</tr>
<tr>
<td>Unbiased</td>
<td>$1.50 \times 10^{-5}$</td>
<td>$3.98 \times 10^{-5}$</td>
<td>$6.37 \times 10^{-5}$</td>
<td>$3.21 \times 10^{-7}$</td>
<td>$2.39 \times 10^{-6}$</td>
<td>$5.71 \times 10^{-6}$</td>
</tr>
<tr>
<td>Simplified</td>
<td>$2.05 \times 10^{-5}$</td>
<td>$6.27 \times 10^{-5}$</td>
<td>$2.03 \times 10^{-4}$</td>
<td>$3.36 \times 10^{-7}$</td>
<td>$3.97 \times 10^{-6}$</td>
<td>$1.66 \times 10^{-5}$</td>
</tr>
<tr>
<td>Optimal</td>
<td>$6.83 \times 10^{-5}$</td>
<td>$1.72 \times 10^{-4}$</td>
<td>$2.72 \times 10^{-4}$</td>
<td>$1.68 \times 10^{-6}$</td>
<td>$1.05 \times 10^{-5}$</td>
<td>$2.24 \times 10^{-5}$</td>
</tr>
</tbody>
</table>

Table 5.3: Key rate values with different basis choices. The key rates are simulated with
two decoy states and numerical approach. Unbiased denotes the standard protocol with
equal basis choice; Simplified denotes the simplified choice with the (biased) basis choice
independent of intensity choice; Optimal denotes the optimal choice with the (biased)
basis choice depending on intensity choice. In a large data-set of $10^{18}$ (approaching
asymptotic case), the key rates with optimal choice are around 300% higher than those
of unbiased choice and close to those of simplified choice. In a reasonable data-set ($10^{12}$ to
$10^{14}$), the key rates with optimal choice are around 300% higher than those of unbiased
choice and around 200% higher than those of simplified choice. This shows that the
optimal choice can significantly increase the key rates in a practical setting with finite
data-set. Reproduced from [46] with permission. ©2014 APS.

Table 5.3 shows the comparison results for different choices of bases. The key rates
are simulated using the numerical method with two decoy states. Unbiased denotes
the standard protocol with equal basis choice; Simplified denotes the simplified choice
with basis choice independent of intensity choice; Optimal denotes the optimal choice
with basis choice depending on intensity choice. In a larger data-set of $10^{18}$ (approaching
asymptotic case), the key rates with optimal choice are around 300% higher than those
of unbiased choice and close to those of simplified choice. In a reasonable data-set ($N=10^{12}$
to $10^{14}$), the key rates with optimal choice are around 300% higher than those of unbiased
choice and around 200% higher than those of simplified choice. Therefore, the optimal
choice of parameters can significantly increase the key rates in a practical setting with
finite data-set.
Figure 5.10: Asymmetric MDI-QKD. The two channels connecting Alice to Charles and Bob to Charles have different transmittances. In real-life MDI-QKD, asymmetry appeared naturally in two field-test experiments [94, 113]. Reproduced from [48] with permission. ©2013 IOP.

5.3 Asymmetric channel transmission

A schematic diagram of the asymmetric MDI-QKD is shown in Fig. 5.10. Note that this asymmetric scenario appeared naturally in two recent field-test experiments performed in Calgary [94] and China [113]. Another concrete illustration can be found at the Tokyo QKD network [13], in which the asymmetric case occurs if Koganei-1 (Alice) and Koganei-3 (Bob) use Koganei-2 (Charles) as the quantum relay to perform MDI-QKD, where the two fiber links are respectively 90 km and 1 km.

Here we define a parameter $x$ to quantify the ratio of the two channel transmittances, i.e., $x = t_a/t_b$, where $t_a$ ($t_b$) represents the channel transmittance between Alice (Bob) and Charles. In the Calgary’s (China’s) system, $x=0.752$ ($x=0.21$), while in the Tokyo QKD network $x=0.017$.

5.3.1 Problem identification

The main question here is how to choose the optimal intensities in this asymmetric situation. In the asymptotic case, these optimal intensities refer to the two signal states $\mu_a^{\text{opt}}$ and $\mu_b^{\text{opt}}$. Let us discuss two possible options.

The first option is to choose $\mu_a^{\text{opt}}=\mu_b^{\text{opt}}$ with both in $O(1)$. If we ignore the system imperfections such as background counts and other practical errors, the error rates ($e_{11}^X$ and $E_{\mu\nu}^Z$ in Eq. (3.1)) will be zero, while $P_{11}^Z Y_{11}^Z$ can be maximized with $\mu_a^{\text{opt}}=\mu_b^{\text{opt}}=1$ (see Appendix A.1 for the details). However, in practice, it is inevitable to have some
practical errors such as the polarization misalignment discussed above. A relatively large intensity in the short channel will significantly increase the QBER due to the misalignment of the short channel. Moreover, owing to the intensity mismatch on Charles’s side ($\mu_{\text{opt}}^a t_a \neq \mu_{\text{opt}}^b t_b$), the quantum interference known as the HOM dip, will be imperfect. As a consequence, this option leads to a relatively large QBER, which decreases the key rate due to the cost of error correction.

To minimize the QBER, a second option is to choose $\mu_{\text{opt}}^a t_a = \mu_{\text{opt}}^b t_b$ regardless of $x$. We denote this situation as the symmetric choice (indicated by Symmetry in Fig. 5.11 and Table 5.4). An equivalent implementation scheme for this option is to add a tailored length of fiber in the local station of the sender with the short channel transmission (i.e., Bob in Fig. 5.10) in order to balance the two channel transmittances. In fact, such a scheme was recently implemented in a proof-of-principle MDI-QKD experiment [94]. However, when $x$ is far from 1, to satisfy $\mu_a t_a = \mu_b t_b$, either $\mu_a$ or $\mu_b$ needs to be relatively small. Hence, we cannot derive good bounds for $P_{11}^{z} Y_{11}^z$ and $e_{11}^X$. In particular, the increase of $e_{11}^X$ results in the decrease of the key rate due to the cost of privacy amplification.

In summary, we find that both of the above two options are sub-optimal. We present the optimal choice below.

5.3.2 Summary of results

The optimal choice (indicated by Optimum in Fig. 5.11 and Table 5.4) can be determined from numerical optimizations. Here we perform such optimizations and also analyze the properties of asymmetric MDI-QKD. Our main results are:

1. In the asymptotic case, the optimal choice for $\mu_a$ and $\mu_b$ does not always satisfy $\mu_{\text{opt}}^a t_a = \mu_{\text{opt}}^b t_b$, but the ratio $\mu_{\text{opt}}^a t_a / \mu_{\text{opt}}^b t_b$ is near 1. That is, if $x < 1$, then $\mu_{\text{opt}}^a t_a / \mu_{\text{opt}}^b t_b \in [0.3, 1]$. This result can be seen from Fig. C.2. In the practical case with the two decoy-state protocol and finite-key analysis, $\{\mu_{\text{opt}}^a, \mu_{\text{opt}}^b\}$ and $\{\nu_{\text{opt}}^a, \nu_{\text{opt}}^b\}$ satisfy a similar condition with the ratio $\mu_{\text{opt}}^a t_a / \mu_{\text{opt}}^b t_b$ (or $\nu_{\text{opt}}^a t_a / \nu_{\text{opt}}^b t_b$) near 1, while $\{\omega_{\text{opt}}^a, \omega_{\text{opt}}^b\}$ are optimized at their smallest value. See Table 5.4 for further details.

2. In an asymmetric system with $x = 0.1$ (50 km length difference for two standard fiber links), the advantage of the optimal choice is shown in Fig. 5.11, where the key rate with the optimal choice is around 80% larger than that with the symmetric
Figure 5.11: Key rate comparison with 50km channel mismatch. We assume a fixed channel mismatch, $x=0.1$ ($L_{ac}-L_{bc}=50$km). In the symmetric choice (Symmetry in figure), we set $\mu_a t_a = \mu_b t_b$, while in the optimal choice (Optimum in figure), we non-trivially determine the optimal intensities by numerical simulation. The red curves are evaluated by the two decoy-state protocol (Section 4.1) combined with the finite-key analysis of [47]. Note that in each curve, all the intensities of the signal and decoy states are optimized by maximizing the key rate. On average, the key rate with the optimal choice is around 80% larger than that with the symmetric choice in both asymptotic and two decoy-state cases. Reproduced from [48] with permission. ©2013 IOP.

In the asymptotic case, at a short distance where background counts can be ignored: $\mu_a^{opt}$ and $\mu_b^{opt}$ are only determined by $x$ instead of $t_a$ or $t_b$ (see the optimal intensities in Table 5.4 and Theorem 1 in Appendix C); assuming a fixed $x$, $\mu_a^{opt}$ and $\mu_b^{opt}$ can be analytically derived and the optimal key rate is quadratically proportional to $t_b$ (see Appendix C).

Finally, notice that the channel transmittance ratio in Calgary’s asymmetric system is near 1 ($x=0.752$), hence the optimal choice can slightly improve the key rate compared to the symmetric choice (around 2% improvement). However, in Tokyo’s asymmetric
Table 5.4: Optimal intensities of an asymmetric MDI-QKD system. The channel mismatch is fixed at $x=0.1$ and thus $L_{ac} = \{50\text{km}, 60\text{km}, 70\text{km}\}$. In the asymptotic case, the ratio $\mu_a^{\text{opt}}/\mu_b^{\text{opt}}$ for the optimal choice is around 4. In the symmetric choice, this ratio is 10. The parameters $\mu_a^{\text{opt}}$ and $\mu_b^{\text{opt}}$ are fixed regardless of $t_a$ and $t_b$ (see Theorem 1 in C.1). In the two decoy-state case (with different $L_{bc}$), the optimal intensities for the decoy state $\nu$ are about $\{\nu_a=0.10, \nu_b=0.01\}$ for the symmetric choice and $\{\nu_a^{\text{opt}}=0.07, \nu_b^{\text{opt}}=0.01\}$ for the optimal choice. The optimal value for the weakest decoy state is $\omega_a^{\text{opt}}=\omega_b^{\text{opt}}=5 \times 10^{-4}$ for both choices. From the intensity values in this table, we find that the optimal choice for $\mu_a$ and $\mu_b$ does not always satisfy $\mu_a^{\text{opt}}t_a=\mu_b^{\text{opt}}t_b$, but the ratio $\mu_a^{\text{opt}}t_a/\mu_b^{\text{opt}}t_b$ is near 1. Also, in the asymptotic case, $\mu_a^{\text{opt}}$ and $\mu_b^{\text{opt}}$ are only determined by $x$ instead of $t_a$ or $t_b$. Reproduced from [48] with permission. ©2013 IOP.

5.4 Summary

We have presented an analysis for practical aspects of MDI-QKD. To understand the physical origin of the QBER, we have investigated various practical error sources. In a polarization-encoding system, polarization misalignment is the major source contributing to the QBER. Hence, in practice, an efficient polarization management scheme such as polarization feedback control [95] can significantly improve the polarization stabilization and thus generate a higher key rate. Moreover, we have shown the importance of full parameter optimization in practical decoy-state MDI-QKD and presented a novel LSA to realize such optimization. Full parameter optimization can increase the key rate around 200% over the simplified choice. LSA can be four orders of magnitude faster than a trivial exhaustive search to achieve a similar optimal key rate. In practice, implementing full parameter optimization requires slightly complex modulation schemes, as the sender’s two
modulators on the intensities and the bit information are dependent. However, one can in principle jointly modulate the two modulators using a single QRNG, which is similar to the setup in [94]. Furthermore, we have studied the properties of the asymmetric MDI-QKD protocol and discussed how to optimize its performance. Our work is relevant to both QKD and general experiments on quantum interference.
Chapter 6

Experimental polarization-encoding MDI-QKD

In this Chapter, I discuss how to apply the theoretical proposals presented in the past two chapters into a real implementation of MDI-QKD. This implementation uses polarization encoding in telecom optical fiber. This chapter is based heavily on [55], and I am the third author. In this work, I designed the overall system, tested the polarization-modulation and polarization-alignment setup, performed the parameter optimization and analyzed the experimental data. Zhiyuan Tang and Zhongfa Liao conducted the whole experiment and measured the raw data.

6.1 Introduction

The main experimental challenge of MDI-QKD is to perform a high-fidelity BSM between photons from different light sources [32], which is not required in conventional QKD schemes. Indeed, to obtain high-visibility two-photon interference, Alice’s photons should be indistinguishable from those of Bob\(^1\). Furthermore, if one implements MDI-QKD over telecom fibres, it is necessary to include feedback controls to compensate the time-dependent polarization rotations and propagation delays caused by the fibres.

Before our experiment, various experimental attempts of MDI-QKD with time-bin encoding [94, 96] and polarization encoding [95] have been reported. In [94, 95], only

\(^1\)In principle, one may suggest that first Charles sends strong light pulses (from the same laser) to both Alice and Bob, who then encode their bit values, attenuate the pulses, and send them back to Charles. However, note that this design could compromise the security of the whole system, as now Charles could try to interfere with Alice’s and Bob’s state preparation processes.
Chapter 6. Experimental polarization-encoding MDI-QKD

Bell state measurements with different BB84 states and intensities were conducted, and in fact no real MDI-QKD, which requires both Alice and Bob to modulate their qubits’ states and intensity levels randomly and independently. A time-bin encoding MDI-QKD was performed in [96]. However, intensity levels and probability distribution of the signal and decoy states were not optimized. Additionally, phase randomization of weak coherent pulses, a crucial assumption in security proofs of decoy state QKD, was neglected in former implementations, leaving the system vulnerable to attacks on the imperfect weak coherent sources [85].

We report an experimental demonstration of polarization encoding MDI-QKD over 10 km of optical fibers. While time-bin encoding MDI-QKD has the advantage of easier polarization management in optical fiber, it requires expensive and bulky equipment for phase stabilization in interferometers at the users’ (Alice and Bob) sites. On the other hand, polarization qubits can be easily prepared by the users using standard optoelectronic devices, which can be miniaturized using state-of-the-art micro-fabrication processes at a low cost [114]. Those more expensive polarization stabilization systems, if required, can be placed with other expensive equipments (e.g., detectors) at the service centre. This makes polarization encoding more favourable in a network setting. Moreover, there is an increasing interest in implementing QKD in free space, particularly ground-to-satellite QKD, in which polarization is a preferred encoding scheme.

6.2 Experimental setup

Figure 6.1 shows the schematic of our polarization encoding MDI-QKD experiment. Alice and Bob each possesses a CW frequency-locked laser (Clarity-NLL-1542-HP, wavelength \( \sim 1542 \) nm). The laser light is attenuated and modulated by a LiNbO\(_3\) based intensity modulator (IM) to generate weak coherent pulses at a repetition rate of 500 KHz. Phases of pulses are uniformly randomized in the range of \([0, 2\pi]\) by a phase modulator (PM). To implement the decoy state protocol, intensities of the pulses are randomly modulated by an acousto-optic modulator (AOM). Key bits are encoded into polarization states of the weak coherent pulses by a polarization modulator (Pol-M). The schematic of the polarization modulator, consists of an optical circulator, a phase modulator (labelled as PM-pol), and a Faraday mirror [115]. Optical pulses are launched via the optical circulator into the phase modulator with polarization at 45° from the optical axis of the phase modulator’s waveguide. By modulating the relative phase between the two principal
Figure 6.1: (Color online) Polarization-encoding MDI-QKD setup. Each of the two CW frequency-locked lasers is attenuated by an optical attenuator (Attn) and modulated by an intensity modulator (IM), which is driven by an electrical pulse generator (PG), to prepare weak coherent pulses. The phases of these pulses are uniformly modulated by a phase modulator (PM) for active phase randomisation. Next, an acousto-optic modulator (AOM) randomly modulates their intensities to implement the decoy-state protocol. Key bits are encoded into polarization states of the WCPs using a polarization modulator (Pol-M). Alice and Bob send their signals to Charles through a 5 km fibre spool. On receiving the transmission, Charles performs a BSM on the incoming pulses using a beam-splitter (BS) and a polarising beam-splitter (PBS) together with two commercial SPDs. Synchronisation is done with an electrical delay generator (DG). In the figure: (PC) polarization controller, (RNG) random number generator and (TIA) time interval analyser.

modes of the waveguide, four BB84 polarization states can be generated. Polarization mode dispersion and temperature-induced variation of polarization states inside the Pol-M setup can be compensated when pulses are reflected by a Faraday mirror with a 90° rotation in polarization, thus stable polarization modulation can be achieved.

Alice and Bob need to ensure that they have a shared reference frame of polarization. Their rectilinear bases are first aligned manually using fiber polarization controllers (PCs). Bob’s horizontal polarization state is also aligned to either the fast or slow axis of one of the fiber squeezers (driven by piezoelectric actuators) in an electrical polarization controller (E-PC, General Photonics PolaRITE III, in Bob’s setup). A DC voltage is then applied on this squeezer to change the phase retardation between the components
with polarizations along the fast and slow axes. This corresponds to a unitary transformation in which Bob’s polarization states in the rectilinear basis remain unchanged, while polarization states in the diagonal basis are rotated about the horizontal-vertical axis on the Poincaré sphere. The voltage is properly adjusted such that Bob’s diagonal basis is aligned to Alice’s. The misalignment is around 1% in our experiment.

All the modulators (PMs, AOMs, and Pol-Ms) are independently driven by random number generators (function generators with pre-stored random numbers generated by a QRNG [51, 52]). An electrical delay generator (DG) located in Charlie’s setup synchronizes all the RNGs and the electrical pulse generators (PGs) driving the IMs. As aforementioned, it is critical to assure that the weak coherent pulses independently prepared by Alice and Bob are indistinguishable at Charlie’s beam splitter in terms of spectrum and arrival time. The wavelengths of the lasers used by Alice and Bob are independently locked to one molecular absorption line of a gas cell (integrated in the laser by the manufacturer) at around 1542.38 nm. This guarantees the frequency difference between Alice and Bob’s lasers is within 10 MHz, while the temporal width of the pulse is about 1 ns (FWHM), corresponding to a bandwidth of about 1 GHz. The arrival time of the pulses can be independently controlled by the DG with a resolution of 50 ps, and the timing jitter of the electronic devices is about 100 ps (RMS). Therefore, we can guarantee that the two independently prepared pulses have sufficient overlap in both time and spectrum.

Alice and Bob send their pulses through a 5 km fiber spool to Charlie, who performs Bell state measurements on the incoming pulses. Charlie’s measurement setup consists of a 50:50 beam splitter (BS), a polarizing beam splitter (PBS), and two commercial InGaAs/InP single photon detectors (SPDs, detection efficiency \( \sim 10\% \), dark count rate \( \sim 5 \times 10^{-5} \)). Due to the limited number of available detectors, we choose to detect photons at the outputs of one PBS only. A coincidence between the two detectors (defined as when both SPDs click within 10 ns, measured by a time-interval analyser in this setup), corresponds to a successful projection into the triplet state \( |\psi^+\rangle \).

### 6.3 Results

We implement MDI-QKD with two decoy states. Using the method in Section 5.2, we perform a numerical simulation to optimize the performance: average photon numbers are chosen to be \( \mu = 0.3 \) for the signal state, \( \nu = 0.1 \) and \( \omega = 0.01 \) for the two decoy
Table 6.1: Experimental and simulated (in bracket) gains $Q^{\lambda}_{q_aq_b} \times 10^{-4}$ with intensities $q_a$ and $q_b$ in basis $\lambda$.

<table>
<thead>
<tr>
<th>$q_b$</th>
<th>$q_a$</th>
<th>rectilinear (Z) basis</th>
<th>diagonal (X) basis</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mu$</td>
<td>$\mu$</td>
<td>0.4660 0.1597 0.0225</td>
<td>0.9030 0.4100 0.2540</td>
</tr>
<tr>
<td></td>
<td>(0.4643)</td>
<td>(0.1596)</td>
<td>(0.0215)</td>
</tr>
<tr>
<td>$\nu$</td>
<td>$\nu$</td>
<td>0.1550 0.0531 0.0070</td>
<td>0.397 0.1015 0.0312</td>
</tr>
<tr>
<td></td>
<td>(0.1596)</td>
<td>(0.0539)</td>
<td>(0.0066)</td>
</tr>
<tr>
<td>$\omega$</td>
<td>$\omega$</td>
<td>0.0214 0.0067 0.0009</td>
<td>0.2460 0.0317 0.0014</td>
</tr>
<tr>
<td></td>
<td>(0.0215)</td>
<td>(0.0066)</td>
<td>(0.0007)</td>
</tr>
</tbody>
</table>

states\(^2\); the ratio of numbers of pulses sent out with intensities $\mu$, $\nu$, and $\omega$ is set to be 4 : 9 : 7. The experiment run for about 94 hours\(^3\) and a total number of $N = 1.69 \times 10^{11}$ pulses are sent out. The gains and QBERs with different intensities in the rectilinear and diagonal bases can be measured from the sifted key and the results are listed in Tables 6.1 and 6.2, respectively.

We used the following measured experimental parameters for the simulation: quantum efficiency of the detectors $\eta=10\%$, 0.8 dB of insertion loss in Charlie’s measurement setup, 1% of misalignment, and 0.2 dB/km for the loss in the 5 km fiber spools. The simulation model is based on Section 5.1 and the results are presented in Tables 6.1 and 6.2 with the values in bracket. By comparing the simulation results to the experiment results, we can see that they are consistent.

To extract a secure key, Alice and Bob need to estimate $Y_{11}^{Z,L}$ and $\epsilon_{11}^{X,U}$ from the decoy-state protocol. Here we use the analytical method with two decoy states, presented in Section 4.1. Given the short data set obtained in experiment (mainly due to the low repetition rate of the system), we use the method proposed in [97] for statistical

\(^2\)Ideally the decoy state $\omega$ should be set to vacuum in order to optimize the performance. Since the extinction ratios of our acousto-optic modulators are finite, it is impossible to generate perfect vacuum state in practice. A low (but non-zero) $\omega$ (e.g., $\omega = 0.001$) would give a key rate close to that when $\omega$ is vacuum. However, given the data size in our experiment, it is difficult to measure the gain $Q^{X,Z}_{\omega}$ and the error rate $E^{X,Z}_{\omega}$ for such a small $\omega$. Although the choice of $\omega = 0.01$ slightly compromises the performance, it is more practical for our system.

\(^3\)Polarizations in our system can remain stable for about one hour without active polarization feedback control. The QKD experiment is stopped every hour for polarization realignment. The realignment process can be automated by adding a polarization compensation system to the setup in the future.
Table 6.2: Experimental and simulated (in bracket) QBERs $E_{q_{a_{b}}}$.

<table>
<thead>
<tr>
<th>$I_B$</th>
<th>$I_A$</th>
<th>rectilinear (Z) basis</th>
<th>diagonal (X) basis</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$\mu$</td>
<td>$\nu$</td>
<td>$\omega$</td>
</tr>
<tr>
<td>$\mu$</td>
<td>0.0178</td>
<td>0.0320</td>
<td>0.1670</td>
</tr>
<tr>
<td>$\nu$</td>
<td>0.0306</td>
<td>0.0402</td>
<td>0.1610</td>
</tr>
<tr>
<td>$\omega$</td>
<td>0.1560</td>
<td>0.1570</td>
<td>0.2300</td>
</tr>
</tbody>
</table>

Table 6.3: Parameters used to estimate a lower bound of the key rate $R^L$.

<table>
<thead>
<tr>
<th>$q$</th>
<th>$p_{11}$</th>
<th>$Y_{11}^{Z,L}$</th>
<th>$e_{11}^{X,U}$</th>
<th>$Q_{\mu\mu}$</th>
<th>$E_{\mu\mu}^{Z}$</th>
<th>$f$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.011</td>
<td>0.0494</td>
<td>$4.1 \times 10^{-4}$</td>
<td>0.151</td>
<td>$4.66 \times 10^{-5}$</td>
<td>0.0178</td>
<td>1.16</td>
</tr>
</tbody>
</table>

fluctuations and assume a secure bound of $\epsilon = 1 \times 10^{-3}$ (three standard deviations). We find $Y_{11}^{Z,L} = 4.1 \times 10^{-4}$ and $e_{11}^{X,U} = 15.1\%$. We can estimate a lower bound of the secure key rate $R^L = 9.8 \times 10^{-9}$ and the parameters summarized in Table 6.3. Therefore, a secure key of length $L = 1600$ bits can be generated between Alice and Bob.

### 6.4 Other related experiments

Up to date, four successful independent MDI-QKD experimental realisations have already been reported [94, 95, 96, 55]. Table 6.4 includes a brief summary of their main features. In the POP (proof-of-principle) demonstrations [94, 95], both Alice and Bob send the same quantum state repeatedly without random selection of the encoding states or bases. In [96, 55], two real demonstrations with key exchange have been performed.

In the first POP MDI-QKD demonstration [94], an HOM interference experiment was conducted with photons generated by independent sources that travel through separate field-deployed fibres of lengths 6.2 km and 12.4 km, respectively. By performing automatic polarization stabilisation, manual adjustment of the photons arrival time, and manual adjustment of the lasers frequency, a high interference visibility was obtained even under a real-world environment. The two light pulses constructing a time-bin sig-
### Table 6.4: Comparison between MDI-QKD demonstrations

<table>
<thead>
<tr>
<th>Encoding</th>
<th>Implementation</th>
<th>Condition</th>
<th>Fiber length</th>
<th>Asymp-key rate(^\dagger)</th>
<th>Finite-key rate(^\ddagger)</th>
<th>Repetition rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time-bin</td>
<td>POP(^*)</td>
<td>Field test</td>
<td>28.8 km</td>
<td>(~10^{-6})</td>
<td>N.A.</td>
<td>2 MHz</td>
</tr>
<tr>
<td>Polarization</td>
<td>POP</td>
<td>Lab</td>
<td>17 km</td>
<td>(~10^{-6})</td>
<td>N.A.</td>
<td>1 MHz</td>
</tr>
<tr>
<td>Time-bin</td>
<td>Real(^{**})</td>
<td>Lab</td>
<td>50 km</td>
<td>N.A.</td>
<td>(~10^{-7})</td>
<td>1 MHz</td>
</tr>
<tr>
<td>Polarization</td>
<td>Real</td>
<td>Lab</td>
<td>10 km</td>
<td>(~10^{-6})</td>
<td>(~10^{-8})</td>
<td>0.5 MHz</td>
</tr>
</tbody>
</table>

*POP represents “proof-of-principle” experiment, i.e., no key exchange.

**Real: there is true key exchange.

***N.A. represents “not available”

\(^\dagger\)The key rate (bits/pulse) under the assumption of infinitely long keys.

\(^\ddagger\)The key rate (bits/pulse) after finite-key corrections.

A similar time-bin encoding MDI-QKD scheme was investigated in [96]. The authors performed a real MDI-QKD demonstration with random selection of encoding states and bases. They made use of custom-made and specialised devices including high-efficiency up-conversion single-photon detectors. Here, the time-bin signals were generated by sending a laser pulse through an unbalanced fibre interferometer. Compared to [94], this approach relaxes the requirement on the frequency stability of two lasers but it needs phase stabilisation of the fibre interferometers. For polarization encoding MDI-QKD, besides our experiment, [95] performed a POP implementation and demonstrated that the polarization rotation due to a long fibre could be compensated using conventional polarization feedback control.

All these four experiments, when taken together, complete the cycle needed to demonstrate the feasibility of using off-the-shelf optoelectronic devices to build a QKD system that is immune to all detector side-channel attacks. Very recently, a new MDI-QKD implementation over 200 km of optical fibre using a system clock of 75 MHz has been reported in [116], and a follow-up field test has also been conducted in the city of Hefei, China [113]. These impressive results, once again, show that MDI-QKD is highly practical with current technology.
6.5 Conclusion

We have demonstrated a polarization encoding MDI-QKD experiment over 10 km of optical fibers. Our work shows that, with commercial off-the-shelf optoelectronic devices, it is feasible to build a QKD system immune to detector side-channel attack. In particular, the practicability of polarization encoding MDI-QKD indicates the potential to build a detector side-channel free QKD network, in which users only need to possess handy hardware to prepare polarization qubits. Our work can also be extended to free space polarization encoding MDI-QKD with an untrusted satellite in the future.
Chapter 7

Long-distance MDI-QKD with entangled photon sources

The above chapters discussed the basic idea of MDI-QKD together with its practical aspects. To further improve its performance, in this Chapter, I propose a method to extend the transmission distance of the initial MDI-QKD proposal (Chapter 3). This method is called MDI-QKD with entangled photon sources in the middle. This scheme is simple, experimentally feasible, and most importantly, it enables us to implement QKD over significantly longer distance than what is possible with any existing proposal in the literature. This Chapter is based heavily on [50].

7.1 Introduction

The global quantum Internet is believed to be the next-generation information processing platform promising an exponentially speed-up computation and a secure means of communication. The long-distance distribution of quantum states is a key ingredient for such a global platform, and recently, it has attracted significant scientific attention [117]. Tremendous effort has been dedicated to creating a global QKD network, but long-distance QKD remains challenging. Indeed, for the initial proposal of MDI-QKD [32], even in the asymptotic case, the protocol can only tolerate a maximal loss of 50 dB, which imposes a limit on the transmission distance within 238km for standard telecom fiber. 50 dB is also not suitable for a global QKD network, because the minimal loss of ground-satellite QKD is about 60 dB [118]. Therefore, a key question is: how to extend the transmission distance for MDI-QKD?
Figure 7.1: (Color online) Schematic diagram of MDI-QKD with heralded quantum memories [119, 120]. Charles first stores the incoming photons in two heralded quantum memories, one for Alice and one for Bob. Then, he performs a Bell state measurement only between those photons that have been successfully stored in the memories. This significantly increases the success probability of his measurement unit and, therefore, also the covered distance and achievable secret key rate are increased. In the figure: (QM) quantum memory, and (BSM) Bell state measurement.

One possible way is to include quantum memories in Charles’s measurement device [119, 120] (see Fig. 7.1). Instead of performing a BSM between each pair of signals received from Alice and Bob, Charles firstly stores the incoming photons in two heralded quantum memories, one for Alice’s signals and one for Bob’s signals. After that, he performs a BSM only between those photons that have been successfully stored in the memories. By doing so, he can increase the success probability of the measurement unit, which results in a significant increase of both the covered distance and the secret key rate. Unfortunately, however, obtaining an efficient quantum memory is very challenging with current technology [121]. A complete quantum repeater (even with two segments) has still not been realized yet.

7.2 MDI-QKD with one entangled photon source in the middle

We propose a long-distance MDI-QKD method without the necessity of quantum memories. This method is called MDI-QKD with entangled photon sources in the middle. Fig. 7.2 illustrates the diagram of MDI-QKD with one entangled photon source in the middle. This entangled photon source can be based on parametric-down-conversion
Figure 7.2: MDI-QKD with one entangled photon source in the middle. WCP: weak coherent pulse; EPR: Type II parametric-down-conversion (PDC) entanglement source; M: polarization and intensity modulators; BS: beam splitter; D: single photon detector; PBS: polarization beam splitter. Reproduced from [50] with permission. ©2013 AIP.

(PDC). Note that a practical PDC entanglement source operating at telecom wavelength has already been demonstrated by many research groups [122] (such as the one based on periodically poled lithium niobate) and the commercial product has already available on the market [16]. Thus, our proposal is highly feasible with current technology. This method is also similar to the original MDI-QKD in that David, Ethan and Charles together can be treated as an untrusted relay. Hence, the model and security analysis are nearly equivalent. Note that this analysis is also applicable to the case of multiple entangled photon sources combined with multiple BSMs in the middle.

The protocol is as follows. Each of Alice and Bob prepares phase-randomized weak coherent pulses (WCP) in one of the four BB84 polarization states [2] randomly and independently. They also randomly modulate the average photon number in each pulse to implement the decoy-state method [59, 60, 61]. Meanwhile, an untrusted source, Charles, prepares polarization entangled photon pairs using a Type II parametric-down-conversion (PDC) entanglement source (ideally, producing Singlet $|\psi^-\rangle$). All three parties send quantum signals to two untrusted relays, David and Ethan, each of whom is supposed to perform a BSM that projects the incoming signals into a Bell state (either Singlet $|\psi^-\rangle$)
or Triplet $|\psi^+\rangle$). Here, by using the method in Section 4.1, Alice and Bob can use the decoy-state method to estimate the counts and the error rates when both Alice and Bob send out single-photon pulses and both David and Ethan report successful events.

In the classical communication phase, each of David and Ethan uses a classical channel to broadcast their measurement results. Alice and Bob keep the successful events (i.e., the event when both David and Ethan achieve successful BSMs), discard the rest and post-select the events where they use the same basis. Finally, as shown in Table 7.1, either Alice or Bob applies a bit flip to her or his data according to their basis and the BSM results.

For post-processing, Alice and Bob evaluate the data sent in two bases separately [101]. The $Z$-basis (rectilinear) is used for key generation, while the $X$-basis (diagonal) is used for testing against tampering and the purpose of quantifying the amount of privacy amplification needed. In the $Z$-basis, an error corresponds to a successful event when Alice and Bob prepare the same quantum states; in the $X$-basis, an error corresponds to a projection into $|\psi^-\psi^-\rangle$ or $|\psi^+\psi^+\rangle$ when they prepare the same states, or, into $|\psi^+\psi^-\rangle$ or $|\psi^-\psi^+\rangle$ when they prepare orthogonal states (see Table 7.1). The secure key rate in the asymptotic case is the same as Eq. (3.1).

| David&Ethan | $|\psi^+\psi^+\rangle$ | $|\psi^-\psi^-\rangle$ | $|\psi^+\psi^-\rangle$ | $|\psi^-\psi^+\rangle$ |
|-------------|-----------------|-----------------|-----------------|-----------------|
| Alice/Bob   | flip            | flip            | flip            | flip            |
| Alice/Bob   | flip            | flip            | non-flip        | non-flip        |

Table 7.1: Successful Bell state measurements for Fig. 7.2.

### 7.3 Modelling system

To evaluate the performance of our protocol, we provide a general approach to model the system. Although the model is proposed to study MDI-QKD, it is also useful for other non-QKD experiments involving entanglement and BSMs [6, 121].

1. **Source.** *WCP:* The output from an attenuated laser is a weak-coherent state $|\alpha\rangle$ that is a superposition of number states (Fock states). The density matrix $\rho$ of the weak-coherent state has already been shown in Eq. (2.1).

   *EPR:* The state emitted from a type-II PDC entanglement source can be written as [123]

   $|\Psi\rangle = (\cosh \chi)^{-2} \sum_{n=0}^{\infty} \sqrt{n+1} \tanh^n \chi |\Phi_n\rangle,$

   (7.1)
where \(|\Phi_n\rangle\) is the state of an \(n\)-photon pair, given by

\[
|\Phi_n\rangle = \frac{1}{\sqrt{n+1}} \sum_{m=0}^{n} (-1)^m |n-m, m\rangle_d \otimes |m, n-m\rangle_e,
\]

where \(d=d\)-mode and \(e=e\)-mode in Fig. 7.2. The probability of an \(n\)-photon pair is \(P(n)=\frac{(n+1)^{\lambda^2}}{(1+\lambda)^{n+1}}\), where \(\lambda=\sinh^2 \chi\). The expected number (brightness) of photon pairs per pump pulse is \(\mu=2\lambda\). Here, we use the polarization modes as the qubit basis. Specifically, in Z-basis, \(|m, n\rangle\) represents \(m\) photons in \(|H\rangle\) mode (horizontal) and \(n\) photons in \(|V\rangle\) mode (vertical); while in X-basis, \(|m, n\rangle\) represents \(m\) photons in \(|+\rangle\) mode (45) and \(n\) photons in \(|-\rangle\) mode (135).

2. Transmission. Suppose Alice, Bob, and Charles send out states \(|\alpha_a\rangle\), \(|\alpha_b\rangle\) and \(|\Psi_c\rangle\) respectively. After channel transmission, the source states evolve to

\[
|\alpha_a\rangle \rightarrow |\alpha'_a\rangle = \sum_{x_a=0}^{\infty} \sum_{y_a=0}^{\infty} C_a |x_a, y_a\rangle
\]

\[
|\alpha_b\rangle \rightarrow |\alpha'_b\rangle = \sum_{x_b=0}^{\infty} \sum_{y_b=0}^{\infty} C_b |x_b, y_b\rangle
\]

\[
|\Psi_c\rangle \rightarrow |\phi_c\rangle = \sum_{x_d=0}^{\infty} \sum_{y_d=0}^{\infty} \sum_{x_e=0}^{\infty} \sum_{y_e=0}^{\infty} C_c |x_d, y_d, x_e, y_e\rangle
\]

where \(x\) and \(y\) denote the number of photons in \(|H\rangle\) and \(|V\rangle\) mode respectively and \(C\) denotes the final coefficient associated with channel loss and misalignment. In the following, we discuss how one can derive \(C_a\), \(C_b\) and \(C_c\).

WCP: Suppose Alice and Bob send out coherent states both in \(|H\rangle\) mode, after channel transmission with transmittance \(\{t_a, t_b\}\) and misalignment angle \(\{\theta_1, \theta_4\}\), the resulting density matrices can be written as

\[
|\rho'_a\rangle = e^{-\mu t_a} \sum_{n_a=0}^{\infty} \sum_{m_a=0}^{n_a} \frac{(\mu t_a)^{n_a}}{n_a!} \left( \frac{n_a}{m_a} \right) (\cos^2 \theta_1)^{m_a} \times (\sin^2 \theta_1)^{n_a-m_a} |m_a, n_a - m_a\rangle\langle m_a, n_a - m_a|
\]

\[
|\rho'_b\rangle = e^{-\mu t_b} \sum_{n_b=0}^{\infty} \sum_{m_b=0}^{n_b} \frac{(\mu t_b)^{n_b}}{n_b!} \left( \frac{n_b}{m_b} \right) (\cos^2 \theta_4)^{m_b} \times (\sin^2 \theta_4)^{n_b-m_b} |m_b, n_b - m_b\rangle\langle m_b, n_b - m_b|
\]

where \(m (n-m)\) denotes the number of photons in \(|H\rangle\ (|V\rangle\) mode. Hence, we can derive the coefficients \(C_a\) and \(C_b\) (Eq. (7.2)).

EPR: Let us start from a general state \(|\Psi\rangle\) emitted by Charles. After channel transmission
\{t_d, t_e\}, the resulting state is

\[
(cosh \chi)^{-2} \sum_{n_c=0}^{\infty} \tanh^{n_c} \chi \sum_{m_c=0}^{n_c} (-1)^{m_c} \left[ \sum_{k_d=0}^{m_c} \sum_{(l_d-k_d)=0}^{n_c-m_c} \left( \frac{m_c}{l_d-k_d} \right) \left( \frac{k_d}{l_d-k_d} \right) \times (\sqrt{t_d})^{l_d} (\sqrt{1-t_d})^{n_c-l_d} |l_d-k_d, k_d\rangle_d \right]
\]

\[
\otimes \sum_{k_e=0}^{m_c} \sum_{(l_e-k_e)=0}^{n_c-m_c} \left( \frac{m_c}{l_e-k_e} \right) \left( \frac{k_e}{l_e-k_e} \right) \times (\sqrt{t_e})^{l_e} (\sqrt{1-t_e})^{n_c-l_e} |k_e, l_e-k_e\rangle_e \right]
\]

where \(l_d\) and \(l_e\) denote the number of photons passing the channel and finally arriving at David and Ethan. Afterwards, combined with channel misalignment \(\{\theta_2, \theta_3\}\), the above joint state, i.e., \(|l_d-k_d, k_d\rangle_d \otimes |k_e, l_e-k_e\rangle_e\), is given by

\[
\sum_{i_d=0}^{k_d} \sum_{j_d=0}^{l_d-k_d} \left( \frac{e^{i_d}}{i_d} \right) \left( \frac{k_d}{j_d} \right) (-1)^{l_d-k_d-j_d} \times (\cos \theta_2)^{k_d+j_d-i_d} (\sin \theta_2)^{l_d+i_d-k_d-j_d} \times (\cos \theta_3)^{i_e+j_e-k_e-j_e} (\sin \theta_3)^{k_e+j_e-i_e} |l_d-i_d-j_d\rangle_d
\]

\[
\otimes \sum_{i_e=0}^{k_e} \sum_{j_e=0}^{l_e-k_e} \left( \frac{e^{i_e}}{i_e} \right) \left( \frac{k_e}{j_e} \right) (-1)^{k_e-i_e} \times (\cos \theta_3)^{i_e+j_e-k_e-j_e} (\sin \theta_3)^{k_e+i_e-l_e-j_e} |l_e-i_e-j_e\rangle_e
\]

By combining the above two equations, we can derive the coefficient \(C_c\) in Eq. (7.2).

3. Detection. \(|\alpha'_d\rangle\), \(|\alpha'_e\rangle\), and \(|\phi_c\rangle\) will finally interfere (HOM interference) at David and Ethan. In Eq. (7.2), each one is a superposition of number states. Hence, the overall HOM interference is the superposition of the interference between all number states. Let us focus on one specific input number state, interfering at David and Ethan:

\[
\left\{ |x_a, y_a\rangle \otimes |x_d, y_d\rangle \right\}_{David} \otimes \left\{ |x_e, y_e\rangle \otimes |x_b, y_b\rangle \right\}_{Ethanol}
\]

(7.3)

In Z basis, considering \(|H\rangle\) and \(|V\rangle\) mode separately, we can derive the interference results (output of the two beam splitters) using the method of Ref. [124]. For instance, on David’s side, the interference for \(|H\rangle\) mode is between \(|x_a\rangle_{port1-h}\) and \(|x_d\rangle_{port2-h}\), where the interference result is given by a binomial distribution

\[
\sum_{q_a=0}^{x_a} \sum_{q_d=0}^{x_d} \left( \frac{x_a}{q_a} \right) \left( \frac{x_d}{q_d} \right) \sqrt{\binom{q_a+q_d}{t} (x_a+q_a-x_d) \cdot (x_a+q_d-x_d) \cdot (x_d+q_d-x_a) \cdot (x_d+q_a-x_a) \cdot (x_a+q_a+q_d)} \times \sqrt{\binom{q_a+q_d}{r} (q_a+q_d-x_a) \cdot (q_a+q_d-x_d) \cdot (x_d+q_d-x_a) \cdot (x_d+q_d-x_d) \cdot (q_a+q_d+q_a)}
\]

\[
|q_a+q_d\rangle_{port3-h} \otimes |x_a+x_d-q_a-q_d\rangle_{port4-h}
\]

where \(t\) (\(r\)) is the transmission (reflection) coefficient of BS satisfying \(r^2 + t^2 = 0\) and \(|r|^2 + |t|^2 = 1\). Hence, the coefficient of \(z\) photons in \(|H\rangle\) mode populating out from port3 of David’s BS, \(C_{port3-h}(z)\), is given by

\[
\sum_{k=0}^{x_k} \left( \frac{x_k}{z-k} \right) \sqrt{\binom{z}{t} (x_k+z-x_d) \cdot (x_k+z-x_d) \cdot (x_d+z-x_k) \cdot (x_d+z-x_d) \cdot (z-2k)}
\]
where $k \leq z$, $(z-k) \leq (x_d)$, and $z \in \{0, 1, \ldots, (x_a+x_d)\}$. Note that $C_{port3-h}(z)$ is also the coefficient of $x_a + x_d - z$ photons populating out from port4 of David’s BS. Similarly, we can get the interference result for $|V\rangle$ mode, i.e., between $|y_a\rangle_{port1-v}$ and $|y_d\rangle_{port2-v}$. At the same time, we can also derive the interference result between $|x_e, y_e\rangle_c$ and $|x_b, y_b\rangle_b$ on Ethan’s side and thus the joint interference result (4-fold coincidence) for a given number state given by Eq. (7.3).

By summing over all the number states given by Eq. (7.2), we can calculate the overall inference results. In our simulation, for each number state given by Eq. (7.3), we create a table to store the coefficients of different interference outputs. By adding the tables for all number states (Eq. (7.2)), we can have the summation table containing the final coefficients of all interference outputs. In the end, we can have the coincident detection probabilities by considering the detection efficiency $\eta_d$ of a threshold SPD. Finally, based on the detection probabilities, we can derive the gains and the errors for different encodings by Alice/Bob.

### 7.4 Simulation

In simulation, the polarization misalignments of the four quantum channels are assumed to be identical$^1$, and the four channel transmittances are optimized by maximizing the key rates. Firstly, we simulate the key rate in the asymptotic case using the practical parameters from the entanglement based QKD experiment reported in Ref. [103]. This result is shown by the red solid curve in Fig. 7.3. As a comparison, we also present the simulation result of the original MDI-QKD [32] in this figure (see the blue dashed curve). It is interesting that MDI-QKD with one PDC source in the middle can tolerate significantly higher loss, up to 77 dB. Notice that with the same practical parameters, the decoy-state BB84 protocol, however, can only tolerate around 30 dB [125]. Without other losses, a 77 dB loss corresponds to a channel transmission of 367km standard telecom fiber (0.21 dB/km) or 481km ultra-low loss telecom fiber (0.16 dB/km [126]).

It is worth noting that in Fig. 7.3, the optimal key rate of MDI-QKD with one PDC source at 0km is about $2.39 \times 10^{-8}$ bits per pulse. Why is this key rate lower than the original MDI-QKD? It is due to two factors: 1) MDI-QKD with one PDC source requires 4-fold coincidence, whereas the original MDI-QKD requires only 2-fold coincidence, whereas the original MDI-QKD requires only 2-fold coincidence, whereas the original MDI-QKD requires only 2-fold coincidence, whereas the original MDI-QKD requires only 2-fold coincidence, whereas the original MDI-QKD requires only 2-fold coincidence.

---

$^1$We found that unequal transmissions could not increase the key rate too much. The key reason is that when $t_a > t_d$, the multi-photon pulse of WCP combined with the channel misalignment of $L_{ad}$ will take turns to contribute significantly to the QBER.
Chapter 7. Long-distance MDI-QKD with entangled photon sources

Figure 7.3: Asymptotic key rate. Asymptotic limit means that Alice and Bob have an infinite number of signals and decoy states. Most of the practical parameters are the same as Table 4.2, while the only difference is the misalignment error $e_d$. Owing to 4-channel links in Fig. 7.2 instead of 2 links in [103], the total misalignment error is assumed to be roughly twice as that in [103], i.e., $e_d = 3\%$. In the low and medium channel loss regions, since MDI-QKD with one PDC source requires 4-fold coincident detections instead of 2-fold coincident detections required by the original MDI-QKD, its key rate is lower than that of the original MDI-QKD. However, MDI-QKD with one PDC source can tolerate significantly higher losses up to 77 dB (367km standard telecom fiber). Reproduced from [50] with permission. ©2013 AIP.

...dence; Hence, the low detector efficiency here (14.5%) inherently decreases the key rate by around two orders of magnitude. 2) If the PDC source in the middle presents a large brightness, its multi-photon pairs contribute significantly to the QBER. Consequently, the optimal brightness of this PDC source is on the order of $10^{-3}$.

The result in Fig. 7.3 can be significantly improved if we consider state-of-the-art single-photon detectors (SPD). For instance, using the practical parameters of Ref. [78] with detector efficiency of 93% and dark-count rate (per gating window) of $1 \times 10^{-6}$, the simulation result is shown in Fig. 7.4. Remarkably, it shows that our scheme can tolerate 140 dB loss (667km standard fiber) in the asymptotic limit. The optimal brightness of PDC is still on the order of $10^{-3}$. To address the finite-key effect, we simulate the finite-key rate by blue dash-dotted and red solid curves in this figure. Here we use the method presented in Section 4.2 for a rigorous finite-key analysis including an analytical...
Figure 7.4: Key rate with state-of-the-art SPDs. We consider better SPDs with detector efficiency of 93% and dark count rate of $1 \times 10^{-6}$. The other experimental parameters are the same as those used in Fig. 7.3. In the asymptotic limit, MDI-QKD with one PDC source can tolerate significantly higher losses, up to 140 dB (667km standard fiber). With the method presented in Section 4.2, the finite-key analysis is conducted on a data-size of $N=10^{15}$. MDI-QKD with one PDC source can tolerate 60 dB loss (286km standard fiber) in the finite-key case. Reproduced from [50] with permission. ©2013 AIP.

approach with two decoy states for the finite decoy-state protocol, a data-size of $N=10^{15}$ and a security bound of $\epsilon=10^{-10}$ for the finite-key analysis. In this case, our scheme can tolerate up to 60 dB channel loss (286km standard fiber or 375km ultra-low loss fiber).

The ultimate transmission distance is limited by the low system operation rate, i.e., the speed of experimental devices. For instance, at 100 dB, even in the asymptotic case, the optimal key rate is only $3 \times 10^{-15}$. Thus, to get one secure bit requires 30 hours of continuous experiment with a high-speed QKD system working at 10 GHz. Note that achieving such high-speed system is currently one of the primary goals of experimental quantum communication community. Also, a high-fidelity on-demand-photon-pair source [127] can increase the key rate by about two orders of magnitude. On the other hand, similar to classical optical communication, a quantum repeater [121] can be helpful for an ultra-long distance quantum communication.
7.5 Conclusion

In summary, we have presented a method of MDI-QKD with an entangled photon source in the middle to extend the transmission distance of initial MDI-QKD proposal. Our method only requires an additional PDC entanglement source together with linear optics, which does not require any quantum memories. Note that a practical PDC entanglement source operating at telecom wavelength has already been demonstrated by many research groups [122] (such as the one based on periodically poled lithium niobate) and the commercial product has already available on the market [16]. Thus our method can be readily demonstrated in experiment. Our work is relevant to not only QKD but also general experiments involving entangled photon sources and BSMs.
Chapter 8

Experimental QKD with source flaws

In addition to the improvement of the performance of MDI-QKD, the most important issue is its security. As mentioned previously, a key assumption in MDI-QKD is that the source is trusted, i.e. with MDI-QKD, the only potential security issue left for Eve is the source. How can one guarantee the source security? In this Chapter, I will discuss one general security issue – source flaws – in the source part, and propose an efficient countermeasure to resolve this issue. Particularly, I perform a decoy-state QKD experiment that shows secure QKD with imperfect source over long distances for the first time. Our implementation is based on a novel proposal [86]. This proposal allows QKD protocols loss-tolerant to state-preparation flaws. This Chapter is largely based on [49].

8.1 Introduction

Until now, former QKD experiments on BB84 [12, 36, 37, 38, 39] and MDI-QKD [94, 95, 96, 55] have had three important drawbacks in the source part. First, in the key rate formula of all existing experiments, it is commonly assumed that the phase/polarization encoding is done perfectly. On one hand, the single-photon components of the four BB84 states are assumed to remain strictly inside a two-dimensional Hilbert space. We call this the qubit assumption. In practice, no previous works have verified this assumption. Note that an attack to exploit the higher dimensionality of state preparation has been proposed in [40]. On the other hand, the encoding devices are widely assumed to be perfect without modulation errors. This is a highly unrealistic assumption and may mean that
Chapter 8. Experimental QKD with source flaws

the key generation is actually *not* proven to be secure in a real QKD experiment. What if we use a key rate formula that takes imperfect modulation into account? Standard Gottesman-Lo-Lütkenhaus-Preskill (GLLP) security proof [41] does allow one to do so. Unfortunately, the key rate will be reduced substantially because the GLLP formalism is very conservative and the resulting protocol is not *loss-tolerant*. Both key rate and distance will suffer greatly from the modulation errors [42]. This might be the major reason why previous experiments commonly ignored source flaws. We remark that source flaw is a serious concern, not only in decoy-state BB84, but also in measurement-device-independent QKD [32], quantum coin flipping [43] and blind quantum computing [44].

Second, the security claims in most (if not all) of the experiments were made with the assumption that the eavesdropper (Eve) was restricted to particular types of attacks (e.g., collective attacks) or that the finite-key analysis was not rigorous (e.g., the security did not satisfy the universally composable security definition [105]). Unfortunately, such assumptions cannot be guaranteed in practice. While [128] has reported an attempt at implementing the rigorous finite-key analysis proposed in [129], a slight drawback is that both the theory and experiment assume a perfect single-photon source without decoy states. Very recently, Lim et al. have provided tight and rigorous security bounds against general attacks for decoy-state QKD for the first time [112]. This analysis is built on a combination of the rigorous finite-key analysis of [129], and the novel finite-data analysis for the MDI-QKD (see Section 4.2). A QKD experiment that implements such a rigorous security analysis has yet to be completed.

Third, the security analysis of previous experiments often relies on rotational symmetries [130, 131, 41]. Hence, four BB84 states are required for the estimation of the bit error rate and phase error rate. QKD protocols with three states, i.e., three-state protocols, have been proposed [132, 133] but, to our knowledge, a decoy-state implementation of a three-state protocol has not been reported in the literature.

We perform a decoy-state QKD experiment that shows secure QKD with an imperfect source at long distances. Our implementation is based on a novel proposal [86], which allows QKD protocols loss-tolerant to state-preparation flaws. We call it a *loss-tolerant protocol*. The key insight of loss tolerant protocol is that, as long as the single-photon component remains a qubit (though, the devices that manipulate them can have modulation errors), Eve *cannot* enhance state-preparation flaws by exploiting the channel loss. This is a reasonable assumption, given the fact that the source can be placed in Alice’s protected environment outside of Eve’s influence and Alice can, in principle, guarantee
this assumption by quantifying her devices locally (see Appendix F).

8.2 Theory

Three-state QKD:

The loss-tolerant protocol works for both BB84 and three-state QKD. The three-state QKD [132, 133] runs almost in the same way as BB84, except that: i) Alice sends only three pure states to Bob, i.e. \{0_z, 0_x, 1_z\}, where \(|i_j\rangle\) (\(i \in \{0,1\}\) and \(j \in \{Z,X\}\)) denotes the state associated with bit “i” in j basis; ii) the rejected data (i.e., basis mismatch events) are used for the estimation of the phase error rate [134]. Based on the security analysis with a biased basis choice, Alice and Bob can generate a secret key only from those instances where both of them select the Z basis [86].

The qubit assumption and its verification:

The key point of the loss-tolerant protocol is the qubit assumption. If it holds, Eve can’t exploit any side-channels to enhance the source flaws through channel loss [86, 40]. To guarantee this assumption, a phase-encoding system needs to have (almost) the same temporal, spatial, spectral and polarization mode for different encoding states. For a standard one-way phase-encoding system based on the LiNbO_3 phase modulator [12, 37, 94, 96], we find that temporal and spatial information can be easily guaranteed without any additional devices, while spectral and polarization information can also be guaranteed with standard low-cost optical devices such as a wavelength filter and a polarizer (see Appendix F for the details). In the case of a two-way system, Alice can monitor the source and verify this assumption locally by using, for instance, the scheme proposed in [135].

Finite-key analysis:

So far, the loss-tolerant protocol was only proven in the asymptotic case with infinitely long keys and an infinite number of types of decoy states, which means that the legitimate users have unlimited resources [86]. Such an asymptotic case is impossible in practice. Here, in order to implement the loss-tolerant protocol, we extend it to a general practical setting with finite keys and finite decoy states. Our finite-key analysis is based on [129,
The $\epsilon_{\text{sec}}$-secret key length in the $Z$ basis is given by \cite{129, 112}

$$\ell \geq s_{z,0}^L + s_{z,1}^L q - s_{z,1}^L h\left(e^U_{x,1}\right) - \text{leak}_{\text{EC}} - 6 \log_2 \frac{21}{\epsilon_{\text{sec}}} - \log_2 \frac{2}{\epsilon_{\text{cor}}}, \quad (8.1)$$

where $h(y) = -y \log_2 y - (1-y) \log_2 (1-y)$ is the binary entropy function. Given the qubit assumption, $q$ characterizes the quality of the state preparation with the fidelity between states prepared in the $Z$ basis and states prepared in the $X$ basis \cite{129}; $s_{z,0}^L$, $s_{z,1}^L$ and $e^U_{x,1}$ are the lower bound of vacuum events, the lower bound of single-photon events, and the upper bound of the phase error rate, associated with the single-photon events in $Z$ basis, respectively; $\text{leak}_{\text{EC}} = n_{z,\mu} f_e h(e_z)$ is the size of the information exchanged during error-correction, where $n_{z,\mu}$ and $e_z$ denote respectively the gain counts for signal state and QBER and $f_e \geq 1$ is the error correction inefficiency function; $6 \log_2 \frac{21}{\epsilon_{\text{sec}}}$ and $\log_2 \frac{2}{\epsilon_{\text{cor}}}$ are respectively the secrecy and correctness parameters. $\ell$ quantifies the lower bound of final key length and the key rate is given by $R = \ell / N$ with $N$ denoting the total number of signals (optical pulses) sent by Alice. This key formula uses a security proof that is based on an uncertainty relation for smooth entropies \cite{129} and it fulfills the composable security definition \cite{105}.

Finite decoy-state protocol:

In practice, $s_{z,0}^L$, $s_{z,1}^L$ and $e^U_{x,1}$ are estimated using the decoy-state method. Here, we propose a novel method for the estimation of the phase error rate $e^U_{x,1}$. In our analysis, besides the signal state $\mu$, we consider two additional decoy states, $\nu$ and $\omega$, where $\mu$, $\nu$ and $\omega$ are the mean photon numbers of weak coherent pulses and they satisfy $\mu > \nu > \omega \geq 0$. Hence, the intensity setting $k \in \{\mu, \nu, \omega\}$. The key novelty to estimate $e^U_{x,1}$ consists in using the rejected detection counts \cite{134}, i.e., considering the detection events associated with single photons when Alice and Bob use different bases. The estimation result is shown in Eq. (D.3) of Appendix D. $s_{z,0}^L$ and $s_{z,1}^L$ can be estimated using a method similar to \cite{112}, from the detection events $n_{z,k}$ (see Appendix D for details).

8.3 Experiment

System description:

We perform a proof-of-principle experiment on top of a commercial ID-500 (manufactured by id Quantique) plug&play QKD system. The system setup has already been discussed in Section 2.3.5. To implement the decoy-state protocol, we use the variable optical
Table 8.1: Parameters measured in ID-500 commercial QKD system, including laser wavelength $\lambda$, optical misalignment error $e_d$ (the probability that a photon hits the erroneous detector), Bob’s overall quantum efficiency $\eta_{Bob}$, dark count rate per pulse $Y_0$ for each detector and system repetition rate $f$.

<table>
<thead>
<tr>
<th>$\lambda$ (nm)</th>
<th>$e_d$</th>
<th>$\eta_{Bob}$</th>
<th>$Y_0$ (Hz)</th>
<th>$f$ (MHz)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1551.71</td>
<td>1.65%</td>
<td>5.05%</td>
<td>4.01 x 10^{-5}</td>
<td>5</td>
</tr>
</tbody>
</table>

Quantifying modulation error:

<table>
<thead>
<tr>
<th>System</th>
<th>$\theta$</th>
<th>$D_{1,\theta}$</th>
<th>$D_{2,\theta}$</th>
<th>$\delta_{\theta}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID-500</td>
<td>0</td>
<td>630</td>
<td>867678</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>$\pi/2$</td>
<td>456735</td>
<td>444336</td>
<td>0.015</td>
</tr>
<tr>
<td></td>
<td>$\pi$</td>
<td>856245</td>
<td>3894</td>
<td>0.127</td>
</tr>
<tr>
<td></td>
<td>$3\pi/2$</td>
<td>464160</td>
<td>436962</td>
<td>0.032</td>
</tr>
</tbody>
</table>

Table 8.2: Raw counts and modulation errors for Alice’s phase modulator in ID-500 plug&play system. $D_{1,\theta}$ ($D_{2,\theta}$) represents the detections counts of SPD$_1$ (SPD$_2$). $\delta_{\theta}$, given by Eq. (8.3), is the upper bound of modulation error for a given phase $\theta$.

We discuss the calibration methods and measurement results for the modulation error $\delta$ of Alice’s phase modulator (PM) in two ID Quantique commercial plug&play systems. $\delta$ is defined as the difference between expected phase and actual phase. Alice’s PM is a LiNbO$_3$ waveguide based electro-optical modulator. We find that in our ID-500 system, the voltage value $\{0, 0.77, 1.59, 2.36\}$ V is used for the phase modulation $\{0, \pi/2, \pi, 3\pi/2\}$.

The calibration process is as follows: Alice is directly connected to Bob with a short fiber (about 1 m); Bob keeps sending optical pulses out and Alice scans the voltages applied to her PM; Bob sets his own PM at a fixed unmodulated phase $\{0\}$ and records the detection counts of his two SPDs$^1$. The counts for Alice’s different phase modulations are denoted by $D_{1,\theta}$ and $D_{2,\theta}$. We find that in ID-500 system, the voltages $\{0, 0.30V_m,$

$^1$In our calibration, we assume that phase $\{0\}$ modulation is error-free. Our method could easily be generalised to the case when $\{0\}$ phase modulation has an error.
0.62V_m, 0.92V_m} give the phase modulations \{0, \pi/2, \pi, 3\pi/2\}, where \(V_m \approx 2.57\) V is a maximal value allowed on Alice’s PM. The detections counts of ten measurements for \(\theta \in \{0, \pi/2, \pi, 3\pi/2\}\) are shown in Table 8.2.

In the ID-500 system, to quantify the modulation errors \(\delta_{\theta}\) for \(\theta \in \{\pi/2, \pi, 3\pi/2\}\), we first determine the detector efficiency and dark counts for Bob’s two SPDs and find that \(\eta_{d1} = 5.05\%\) and \(\eta_{d2} = 4.99\%\) and the dark count rate for the two SPDs are almost the same as \(Y_{0,d1} = Y_{0,d2} = 4.01 \times 10^{-5}\). Notice that when Alice’s PM applies a \{0\} phase, \(D_{1,0}\) (i.e., 630 in Table 8.2) quantifies the summation of the dark counts and imperfect visibility of the system (due to imperfect optical alignment). Ignoring finite data statistics temporarily, the modulation error can be written as:

\[
\delta_{\theta} = |\theta - 2\arctan\sqrt{(D_{1,\theta} - D_{1,0})/\eta_{d1}}|/\eta_{d2},
\]

where \(\theta \in \{\pi/2, \pi, 3\pi/2\}\).

In our analysis of the statistics, we use standard error analysis following [63]. The upper bound of \(\delta_{\theta}\) is thus given by:

\[
\delta_{\theta} \leq \bar{\delta}_{\theta} = |\theta - 2\arctan\sqrt{(D_{1,\theta} + n_\alpha\sqrt{D_{1,0}}) - (D_{1,0} - n_\alpha\sqrt{D_{1,0}})/\eta_{d1}}|/\eta_{d2},
\]

where \(n_\alpha\) denotes the number of standard deviations one chooses for statistical fluctuation analysis. Here, we choose \(n_\alpha = 7\), which corresponds to a failure probability of about \(\epsilon = 10^{-10}\). The upper bounds of \(\delta_{\theta}\) are shown in Table 8.2. From this table, the error \(\delta\) in ID-500 system is upper bounded by the case of \(\delta_{\pi}\), i.e., \(\delta \leq \bar{\delta}_{\pi} = 0.127\).

Using the same method in Clavis2, we find that \(\delta\) is upper bounded by \(\delta \leq \bar{\delta}_{\pi} = 0.147\).

**Implementation of the loss-tolerant protocol:**

In our demonstration, we first implement the three-state decoy-state protocol over a 50 km standard telecom fiber. The ID-500 system allows one to freely modify (via a software) the four voltage values applied on Alice’s PM. In our implementation, we set Alice’s modulation voltage values to be \{0, 0.77, 1.59, 0.77\} V and thus operate Alice to send three encoding phases \{0, \pi/2, \pi\}, where the probability ratio for these three phases is 1 : 2 : 1 (with equal basis probability for the simplicity of implementation). We chose to operate the system for about 3 hours and send a total number of pulses \(N=5 \times 10^{10}\). Before the experiment, we performed a numerical simulation to optimize the implementation parameters. Our optimization routine is similar to [63], with the
difference being we use the rigorous finite-key security bounds (see Eq. (8.1)) to predict the key rate. The optimal parameters are: intensities $\mu=0.55$, $\nu=0.06$, $\omega=0.001$ and probabilities $P_\mu=0.74$, $P_\nu=0.18$, $P_\omega=0.08$.

Our measurement and post-processing are different from previous demonstrations in the sense that we directly measure the detection counts instead of detection probabilities (so-called gains in former experiments [36, 37, 38, 39, 12]) and we record the basis-mismatch counts as well. These experimental counts are shown in Fig. 8.1(a), 8.1(b), and 8.1(c). By plugging them into the decoy-state estimations (see Appendix D) and using Eq. (8.1), we obtain the experimental results listed in the middle column of Table 8.3. In our analysis of experimental data, we consider a conservative security parameter (the

\[ Z \] 

\[ X \] 

\[ 0 \] 

\[ 5 \] 

\[ 10 \] 

\[ 15 \] 

\[ 20 \] 

\[ 25 \] 

\[ \mu \] 

\[ \nu \] 

\[ \omega \] 

2To simplify our implementation, we adopt equal basis probability, i.e., $P_Z = P_X=0.5$, and assume that the basis choice is independent of the intensities.
summation of all failure probabilities) $\epsilon = 10^{-10}$. Finally, based on the three-state protocol, we get a QBER $e_z = 2.98\%$ and a lower bound of secure key generation rate $R^L = 5.21 \times 10^{-5}$ per pulse. About 2603 kbit of unconditionally secure keys are exchanged between Alice and Bob. The security of these keys considers source flaws and satisfies the composable security definition, and it can be used against general attacks by Eve.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Three-state</th>
<th>BB84</th>
</tr>
</thead>
<tbody>
<tr>
<td>$s_{z,0}^L$</td>
<td>$3.22 \times 10^5$</td>
<td>$3.21 \times 10^5$</td>
</tr>
<tr>
<td>$s_{z,1}^L$</td>
<td>$1.30 \times 10^7$</td>
<td>$1.31 \times 10^7$</td>
</tr>
<tr>
<td>$e_z$</td>
<td>$2.98%$</td>
<td>$2.89%$</td>
</tr>
<tr>
<td>$e_u^{x,1}$</td>
<td>$11.49%$</td>
<td>$6.01%$</td>
</tr>
<tr>
<td>$l$</td>
<td>$2.60 \times 10^6$</td>
<td>$7.70 \times 10^6$</td>
</tr>
<tr>
<td>$R^L$</td>
<td>$5.21 \times 10^{-5}$</td>
<td>$1.54 \times 10^{-4}$</td>
</tr>
</tbody>
</table>

Table 8.3: Experimental results. These values are obtained by plugging the raw counts (Fig. 8.1) into the estimation equations shown in Appendix D and the key rate formula of Eq. (8.1).

Next, we perform a similar experiment based on decoy-state BB84. Alice modulates her PM with a voltage value selected from $\{0, 0.77, 1.59, 2.36\}$ V for each pulse, i.e., she randomly sends a state from $\{0, \pi/2, \pi, 3\pi/2\}$ for each pulse. We also send a total number of signals $5 \times 10^{10}$ and use the same intensities and probabilities as the three-state implementation. We measure the raw counts in Fig. 8.1(d) and 8.1(e) and obtain the experimental results shown in the right column of Table 8.3. Based on the loss-tolerant protocol (see Appendix E), the final secure key rate is $R^L = 1.54 \times 10^{-4}$ per pulse. The key rate differences between BB84 and three-state protocol are mainly due to the finite-data statistics, which affects the estimation error on $e_u^{x,1}$. We numerically find that if operating the experiment longer, for instance generating $N=10^{12}$, the key rate with three states is close to that with BB84. Notice that $10^{12}$ signals can be easily achieved within 20 min by using a relatively high speed system such as 1 GHz repetition rate [12].

As a comparison to previous security analysis (e.g., GLLP), with the source flaws $\delta = 0.127$, no matter how many decoy states we choose or how big the data we use is, the key generation rate will hit zero at only about 10 km based on GLLP [41, 42]. In other words, at 50 km, not even a single bit could be shared between Alice and Bob with guaranteed security following the previous GLLP security proof. This means that if we consider the source flaws in previous long-distance decoy-state experiments [36, 37, 38,
Figure 8.2: Decoy-state QKD with source flaws in a practical setting. The simulation is conducted with parameters in Table 8.1, \(N = 5 \times 10^{10}\) and \(\epsilon = 10^{-10}\). The main figure is for the three-state protocol based on our security analysis, while the inserted figure is for the decoy-state BB84 protocol based on GLLP security analysis (see Appendix E for the model). The power of our security analysis is explicitly shown by the fact that GLLP delivers a key rate that decreases rapidly when \(\delta\) increases. The maximal tolerant distance is about 9 km for our QKD system (green dashed-dotted curve in the inserted figure). In contrast, our analysis can substantially outperform GLLP and it is loss-tolerant to source flaws. Our QKD set-up can be made secure over 60 km and the secure key rate is almost the same as the case without considering source flaws (i.e., assuming \(\delta = 0\)).

39, 12\], the key generation might not be proven to be secure. In contrast, our analysis with the loss-tolerant protocol can easily achieve a high secure key generation rate over long distances even in the presence of source flaws.

### 8.4 Simulation

With \(\delta\) and the parameters in Table 8.1, we perform a simulation to numerically study our security analysis in a practical setting. Fig. 8.2 shows the simulation results, where similar to our experiment, we use \(N = 5 \times 10^{10}\) and \(\epsilon = 10^{-10}\). For comparison purpose, this figure also includes the key rate for the decoy-state BB84 based on the GLLP security analysis (See Appendix E for the model). The power of our security analysis is explicitly shown by the fact that GLLP delivers a key rate that decreases rapidly when \(\delta\) increases.
The maximal tolerant distance is about 9 km for our QKD system. This is due to the fact that GLLP considers the worst case scenario where losses can increase the fidelity flaw \[41, 42\]. Our security analysis, however, can substantially outperform GLLP and it is loss-tolerant to source flaws. Our QKD set-up can be made secure over 60 km and the secure key rate is almost the same as in the case without source flaws.

8.5 Conclusion

We have demonstrated decoy-state QKD with imperfect state preparations and employed tight finite-key security bounds in our implementation. Our work constitutes an important step towards secure QKD with imperfect devices. In this Chapter, we ignore certain imperfections in the source such as the intensity fluctuations of signal/decoy states, which have a small effect and can be accounted for using previous result [136]. Also, we assume that there is no unwanted information leakage from the source. How to protect the source outside of Eve’s active influence will be a subject for future investigations. Moreover, a device-independent dimension witness could be used to verify the dimension of the source [137, 138]. Furthermore, it will be interesting to work out a refined security proof that would include all possible (small) imperfections and side channels in the source and to extend our results to MDI-QKD [32]. Thus, one can not only solve the problem of imperfect sources but also remove all loopholes in the detection system. MDI-QKD with imperfect source may incubate the first practical side-channel-free QKD.

\[\text{Note that most of previous works could only test the lower bound of the dimension of a quantum system in a device-independent manner. It will be interesting to investigate a device-independent method to test the upper bound of the dimension.}\]
Chapter 9

Fast quantum random number generator (QRNG)

“Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin.” - J. von Neumann

The above chapters discuss the framework to connect the theory and practice of QKD. This framework is based on MDI-QKD with imperfect sources. Meanwhile, an important element in the source of this framework is the random number generator used for creating secure keys. The ability to generate truly random numbers is highly demanded. In this Chapter, I present an ultrafast quantum random number generator (QRNG) to generate truly random numbers. My approach is by measuring the quantum phase fluctuations of a laser, which is operated near its threshold. Moreover, I have developed a compact and cost-effective prototype, which has a real-time generation rate of 1 Gbits/s with excellent stability. The content of this chapter is largely based on Refs. [51, 52]. More details about this prototype can be seen in [53].

9.1 Introduction

Random numbers play a crucial role in the areas ranging from computer simulations, on-line gambling, to secure communications. While computer generated pseudo-random numbers can be used for many applications, they remain fundamentally deterministic and thus experience various problems [139]. To address this pseudo-randomness issue, the probabilistic characteristic of quantum physics offers a natural way to generate true randomness, i.e. quantum random number generator (QRNG).
As a simple example, we consider the polarization measurement of a polarization quantum state, $\frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$, in the rectilinear basis of $\{|H\rangle, |V\rangle\}$. It will yield the unbiased and thus completely unpredictable outcomes $|H\rangle$ and $|V\rangle$. Then by assigning the classical bit values “0” and “1” to these outcomes, a sequence of truly random numbers can be generated. This scheme can be easily realized by a single-photon source followed by a polarization beam splitter (PBS), and two single-photon detectors (SPDs), one for each output arm of the PBS. Indeed, this scheme has drawn much scientific attention [69], where commercial QRNGs, like ID Quantique system [16], have already appeared on the market.

Unfortunately, due to the difficulties of measuring quantum effects in real experiments, previous implementations of QRNG have been limited to a relatively slow rate (typically below 20 Mbits/s). In 2009, my group proposed and built a fast QRNG by measuring the quantum phase fluctuations of a laser, which yields a speed of 500 Mbits/s [140]. Nonetheless, the key point is, the generation rates of all previous QRNGs are still too low for many applications ¹, such as high-speed QKD working at 1GHz [12] or 10 GHz [73].

Here, I substantially improved the previous work [140] on both the hardware design and post-processing algorithm, and demonstrated an ultrafast QRNG with a rate over 6 Gbits/s. Moreover, we have developed a compact and cost-effective prototype, which can stably generate real-time quantum random numbers at a rate of 1 Gbits/s with excellent immunity to external perturbations. On the post-processing side, we remove the contamination of classical noise by implementing an information-theoretically provable randomness-extractor. The simplicity and speed of our prototype show the feasibility of a robust, low-cost, and fast QRNG. It can be readily commercialized for practical applications.

### 9.2 QRNG based on quantum phase noise

It is well known that the fundamental phase fluctuations (or noise) of a laser can be attributed to spontaneous emission, which is quantum mechanical by nature [141]. The quantum phase fluctuations are inversely proportional to the laser output power [141]. By operating the laser at a low intensity level, the quantum phase fluctuations can be

---

¹Notice that in a decoy-state BB84 system, the random numbers are required for both decoy-state randomization and state preparation. Thus, a high-speed QRNG is highly demanding so that it can generate real-time random numbers for different parts of the implementation.
dominant over classical phase noise and is readily extracted to generate truly random numbers.

We have developed a delayed self-heterodyning system to measure the phase fluctuations. The schematic diagram of the experimental setup is shown in Fig. 9.1. A 1.55 µm single mode cw DFB diode laser (ILX lightwave) operating at a low intensity level is the source of quantum phase fluctuations. A PLC-MZI with a 500ps delay difference (manufactured by NTT) is employed to convert the phase fluctuations to intensity fluctuations, which is subsequently detected by a 5GHz InGaAs photodetector (Thorlab). Note that to achieve a high interference visibility, a polarization maintaining fiber is used to connect the laser and the PLC-MZI. A temperature controller (TC) is used to stabilize the phase difference of PLC-MZI. The photodetector output is further digitized by an 8-bit analog-to-digital convertor (ADC) to generate random bits.

The experimental procedures for random number generation are as follows. The laser output power is set to an optimal working point of 0.95 mW [51] by adjusting its driving current. The TC is carefully adjusted to stabilize the phase difference of PLC-MZI at \([2m\pi + \pi/2]\). The photodetector output is sampled by an 8-bit ADC at a sampling rate of 1 GSample/s\(^2\). Fig. 9.2 shows the sampling results acquired in 5 ms. As a comparison,

\(^2\)The sampling time (1 ns) is larger than the addition of MZI time difference (500 ps) and detector response time (200 ps), which reduces the correlations between adjacent samples.
in the same figure, we also show the background noise acquired when the laser is turned off. The histograms (Gaussian fit) of the sampling results are shown in Fig. 9.2(b).

We also perform measurements in the frequency domain by using an RF spectrum analyzer. Three different power spectra have been acquired: (1) the total phase fluctuations spectrum under the normal working conditions (0.95 mW); (2) the background noise spectrum acquired by turning off the laser; (3) the intensity noise spectrum acquired by connecting the laser (at 0.95 mW) output directly to the photodetector. The measurement results are shown in Fig. 9.3. We can see that under the normal operating condition, the intensity noise is negligible comparing to the phase fluctuations. This result supports our previous assumption. As we expect from a perfect white noise source, the spectrum of phase fluctuations itself is flat over the whole measurement frequency range. There are a few spectral lines in the spectrum of background noise which could be environmental EM noise picked up by our detector\textsuperscript{3}.

\textsuperscript{3}There are mainly five spikes around 0, 100, 200, 500, and 650 MHz. These frequencies are all within practical broadcast radio bands (see http://www.fcc.gov/oet/spectrum).
Chapter 9. Fast quantum random number generator (QRNG)

The raw random bits from our QRNG are contributed by both the quantum signal and the classical noise. In order to remove the correlation between the random bits and the classical noise (and thus extract pure quantum randomness), we apply a post-processing scheme that is composed of two main parts - quantum min-entropy (or randomness) evaluation and randomness extraction.

Min-entropy is defined as

\[ H_{\infty}(X) = -\log_2 \left( \max_{x \in \{0,1\}^n} Pr[X = x] \right) \]  

(9.1)

It quantifies the amount of randomness of a distribution \( X \) on \{0,1\}^n. From Eqn. 9.1, the min-entropy of a given sequence \( X \) is determined by the sample point \( x \) with maximal probability \( P_{\text{max}} = \max_{x \in \{0,1\}^n} Pr[X = x] \). A simple illustration of the evaluation process is shown in Fig 9.4, where the raw-data follows a Gaussian distribution and is digitized by a 3-bit ADC. Hence, the raw-data will be mapped to a binary sequence \( X \) with 3 dimensions (\( n=3 \) in Eqn. 9.1). The sample point (one of the 8 bins in Fig 9.4) with maximal probability is ‘011’ (or ‘100’) and its corresponding probability \( P_{\text{max}} \) can be calculated from its bin area. Note that in Fig 9.4, three key parameters to determine \( P_{\text{max}} \) (thus min-entropy) are the standard deviation of Gaussian distribution (\( \sigma \)), the ADC sampling range (\( a \)) and the resolution of ADC (3-bit in Fig 9.4).

In our experiment, a physical model is derived to evaluate the quantum min-entropy of
Figure 9.4: A simple illustration of min-entropy evaluation (toy model). The raw-data follows a Gaussian distribution ($\mu = 0$ and $\sigma = 7$) and is digitized by a 3-bit ADC (sampling range is defined as [-a, a] with a=15 here). From Eqn. 9.1, the min-entropy is determined by the sample point $x$ with the maximal probability $P_{\text{max}}$. Here, $x$ equals to the bin of ‘100’ (or ‘011’) and $P_{\text{max}}$ can be calculated from its bin area. Reproduced from [51] with permission. ©2012 OSA.

the raw-data. Our main assumptions are: (1) Quantum signal is independent of classical noise when the laser is operating above threshold; (2) Quantum signal follows a Gaussian distribution [142]; (3) The sequence of the raw-data is independent and identically distributed (iid, see discussion below). With these assumptions, we can calculate the quantum min-entropy of the raw-data by following the procedures proposed in [51]. We obtain that the quantum min-entropy of our raw-data is 6.7 bits per sample (8 raw bits from the ADC). This means that we can generate 6.7 information-theoretically random bits from each sample. To extract the 6.7 perfect-random bits and improve the randomness quality of our raw-data, randomness extractor is implemented. Roughly speaking, a randomness extractor is a function as

$$\{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\}^m$$

(9.2)

which means that for a raw and non-perfect-random sequence $X$ on $\{0,1\}^n$ with min-entropy $H_\infty(X) \geq m$, the extracted output sequence $Y$ is a nearly uniform distribution on $\{0,1\}^m$. In other words, a randomness extractor takes a small random seed ($d$ bits) and a raw random source ($n$ bits) and outputs a near perfect-random bit-string ($m$ bits). A more rigorous discussion of randomness extractor can be found in [54]. We implement two randomness extractors (see Eq. 9.2 for definition), Toeplitz-hashing extractor [56]
and Trevisan’s extractor [143]. Both are proven to be information-theoretically secure and take finite-size effects into account. The details of our implementation are discussed in Ref. [54].

Figure 9.5: (a) Autocorrelation of the raw-data. The raw-data is obtained by sampling the output a.c. voltage (output from the photodetector) with an ADC (see Fig. 9.1). Each sample consists of 8 bits and the correlation between samples cannot reach zero for a practical detector with finite bandwidth. (b) Autocorrelation of the Toeplitz-hashing output. Data size is $1 \times 10^7$ bits and the average value within 100 bit-delay is $-1.0 \times 10^{-5}$. In theory, for a truly random $1 \times 10^7$ bit string, the average normalized correlation is 0 and the standard deviation is $3 \times 10^{-4}$. In practice, due to the inevitable presence of bias and finite data size, the autocorrelation of data sequence can never reach 0. Reproduced from [51] with permission. ©2012 OSA.

The output from both extractors successfully passes all the standard statistic tests of Diehard, NIST, and TestU01. The autocorrelations of the raw-data and the Toeplitz-hashing output are shown in Fig. 9.5(a) and Fig. 9.5(b). Here, the autocorrelation coefficient $R$ of a sequence $X$ is defined as $R(j) = \frac{E[(X_i-\mu)(X_{i+j}-\mu)]}{\sigma^2}$, where $E[\bullet]$ is the expected value operator, $j$ is the sample delay (or shift), $\mu$ and $\sigma$ are the mean and the standard deviation of $X$. Fig. 9.5(a) shows the autocorrelation results of our raw-data. The low values of the autocorrelation between raw samples (8-bit per sample) verify the iid assumption of our physical model for min-entropy evaluation. A slightly large coefficient at the 2nd delay sample is attributed to the finite bandwidth of our photodetector. After post-processing, the autocorrelation is substantially reduced as shown in Fig. 9.5(b). Some test results of the extracted data are given in Fig. 9.6(a) and Fig. 9.6(b). With the sampling rate of 1 GHz, the corresponding random bit generation rate is over 6 Gb/s. We finally remark that our implementations of randomness extractors
Figure 9.6: (a) NIST results of the Toeplitz-hashing output. Data size is 3.25 Gbits (500 sequences with each sequence around 6.5 Mbits). To pass the test, P-value should be larger than the lowest significant level $\alpha = 0.01$, and the proportion of sequences satisfying $P > \alpha$ should be greater than 0.976. Where the test has multiple P-values, the worst case is selected. (b) Diehard results of the Trevisan’s extractor output. Data size is 240Mbits. A Kolmogorov-Smirnov (KS) test is used to obtain a final P-value from the case of multiple P-values. Successful P-value is $0.01 \leq P \leq 0.99$. Reproduced from [51] with permission. ©2012 OSA.

with Matlab on a standard PC are not fast enough for a real-time QRNG. In practice, this might restrict the random bit generation speed. It will be interesting for future investigations to create a real-time extractor for our high-speed QRNG.

### 9.4 QRNG prototype

Recently, we have further improved our system of Fig. 9.1 towards moving outside the physics laboratory. A robust and low-cost prototype generating real-time random bits has been developed in a standard 19” rack-mount enclosure (Fig. 9.7(a)) [52]. The schematic diagram of prototype is shown in Fig. 9.7(b). The source of quantum phase noise is a distributed feedback diode laser (Sumitomo Electric SLT5411F290), which is operated at a low intensity level by adjusting its driving current from an OEM laser driver. A temperature controller is coupled to the laser driver to stabilize diode temperature. The diode output is fed into a compact Mach-Zehnder interferometer (PLC-MZI from NTT) for interference. After that, the interfered signal is detected and converted to an electrical signal by a 5GHz photo-detector (Thorlabs SIR5FC). Finally, a differential amplifier (National Semiconductor LMH6554) divides the electrical signal into two differential
Figure 9.7: (a) Quantum random number generator prototype in a standard 19” rack-mount enclosure. (b) Schematic diagram of the prototype (See the main text for details). (c) Temporal waveform of the prototype outputs recorded by an Oscilloscope. Channel 1 (yellow signal) is the monitor of quantum phase noise, while Channel 2 (green signal) is the random sequence output. (d) Autocorrelation of the raw random sequence.

beams, which is further digitized by a comparator (Comp2 in Fig. 9.7(b), ADCMP572 from Analog Devices). The comparator2 is triggered by a master clock that consists of another comparator (Comp1 in Fig. 9.7(b)) and a voltage-control oscillator. The real-time random sequence from comparator2 outputs through a BNC connector. The overall system is supported by a power-supply printed circuit board together with an alternative current (AC) adapter.

The binary signals are obtained by comparing the differential logic inputs of the comparator, where the speed is determined by the master clock frequency, i.e. the Oscillator in Fig. 9.7(b). In our prototype, we set the clock frequency at 1 GHz, which corresponds to a random bit generation rate of 1 Gbits/s. The temporal waveforms of the quantum phase noise and the random sequence output are observed and recorded on an oscilloscope (Agilent DSO81204A) as shown in Fig. 9.7(c). The autocorrelation of the random sequence is depicted in Fig. 9.7(d), where the low correlation coefficient indicates its good randomness quality. We remark that thanks to the differential amplifier generating two DC-balanced differential beams, the system is robust against external
perturbations. To further improve the randomness quality, the random sequence is post-
processed by a randomness extractor - Universal hashing with Toeplitz matrix. The
extraction efficiency is over 80%, which is determined by the quantum min-entropy of
the raw random sequence. The details of randomness evaluation and extractor imple-
mentation are discussed in Refs. [54]. A key advantage of our processing approach is
that the output randomness is information-theoretically provable. Finally, the extracted
results successfully pass standard statistic tests of Diehard and NIST.

9.5 Conclusion

We have successfully demonstrated a high-speed QRNG at a generation rate of over 6
Gb/s. In the above work, I performed the whole experimental demonstration of high-
speed QRNG and built up the QRNG prototype. Prof. Xiongfeng Ma implemented
the randomness extractor. Our work not only highlights the importance on the rigorous
quantification and distillation of the quantum randomness in a practical QRNG, but
also demonstrates the large potential for random number generations by quantum phase
fluctuations as the true entropy source.
Chapter 10

Conclusion and outlook

10.1 Conclusion

My Ph.D. research was primarily motivated by an important question: How can code-makers resolve the existing/potential attacks efficiently in QKD? To answer this question, I have studied the security issues in the detection, the source and the randomness generation.

**Detection security:** MDI-QKD removes all detector side-channel attacks. To make it suitable for real-life implementations, I have proposed practical protocols and designed methodologies to optimize parameters. My co-workers and I have conducted a rigorous security proof against general attacks in the finite-data regime. Moreover, to extend the transmission distance, I have proposed a long-distance protocol by introducing entanglement photon sources in the middle. Furthermore, my co-workers and I have demonstrated a polarization-encoding MDI-QKD by using commercial off-the-shelf components. My theoretical and experimental results show that MDI-QKD is mature enough to be implemented in real-life. My research on MDI-QKD paves the way for the realization of a future QKD network with an untrusted network server.

**Source security:** To solve the security loophole due to the imperfect encoder in the source, I have implemented a recent protocol [86], which is loss-tolerant to source flaws. I have implemented both decoy-state BB84 and three-state protocol on top of a commercial QKD system over 50 km telecom fiber. This experiment for the first time shows secure QKD with imperfect state preparations at long distances and achieves tight finite-key security bounds against general attacks in the universally composable framework. This research constitutes an important step towards secure QKD with imperfect devices.
Randomness security: To generate true randomness in high speed, I have proposed and experimentally demonstrated an ultrafast QRNG at a rate over 6 Gbits/s based on the quantum phase noise of a laser. Moreover, I have developed a compact and cost-effective prototype, which has a real-time generation rate of 1 Gbits/s with excellent stability. The simplicity and speed of my prototype show the feasibility of a robust, low-cost, and fast QRNG.

In conclusion, I have shown that while quantum hacking has threatened the security of QKD, MDI-QKD has now appeared to be an important counter-measure against it. MDI-QKD constitutes a major step towards the unconditional security in communication. More importantly, MDI-QKD with imperfect sources may incubate the first practical side-channel-free QKD. In contrast to the previous research on the impractical proposal of DI-QKD, MDI-QKD with imperfect sources can be readily implemented with current technology, and thus it may change the research scope on side-channel-free QKD from ideal proposals to practical implementations. This protocol can also substitute current classical cryptosystems by offering people an unconditionally secure infrastructure, which will be the ultimate dream for researchers in quantum communication.

The main contributions of this thesis are twofold: (i) I have resolved (almost) all the major practical issues in the implementation of MDI-QKD. This for the first time allows MDI-QKD mature enough to be implemented in real-life. (ii) I have proposed a practical side-channel-free QKD framework – MDI-QKD with imperfect source. This framework provides a clear venue to connect the theory and practice of QKD. To study this framework, I have completed two foundation steps by implementing both MDI-QKD and QKD (BB84) with imperfect source. These results will motivate future research to fully realize this framework and apply it into practical applications for unconditionally secure communications.

10.2 Outlook

10.2.1 MDI-QKD

On the experimental side of MDI-QKD, it would be necessary to improve the performance of the implementations realized so far. For instance, current experimental demonstrations consider short-distance transmission (i.e., below 50 km) only and their system clock rate is relatively low (below 2 MHz). For practical applications, it would be desirable to achieve longer distances (say around 100-200 km) and to use higher system clock rates
Figure 10.1: (Color online) Example of a QKD network with an untrusted node based on MDI-QKD. The users have low-cost and compact transmitters that send quantum signals to the network server, which contains all the expensive and complex calibration and measurement devices. This scenario can be easily extended to the case with several servers.

(say 100MHz-1GHz)\(^1\). Using state-of-the-art SPDs [78] could also help to substantially increase the key generation rate.

It would be interesting as well to prove the feasibility of MDI-QKD over free-space communications. Such implementation would constitute the first step towards future satellite-based MDI-QKD networks, in which an untrusted satellite can be shared by many users. Moreover, continuous-variable MDI-QKD demonstrations using standard telecom devices are still missing. Furthermore, in the long term, MDI-QKD could be used to build a fibre-based QKD network, in which the users possess low cost, compact devices to transmit quantum states, while all the expensive calibration and measurement apparatuses are located within the network servers. This scenario is illustrated in Fig. 10.1.

Much work needs to be done as well on the theoretical side. For instance, as already discussed, a key assumption in MDI-QKD is that Alice’s and Bob’s sources can be trusted. It would be therefore necessary to further investigate how this essential requirement could be guaranteed in practice, or to design new protocols to relax the requirements [88]. Also, as aforementioned, it would be important to take both source flaws and detector flaws into account by combining MDI-QKD with the loss-tolerant protocol. Such result, and its experimental demonstration, would bring QKD a big step closer to the unconditional security. In addition, it would be beneficial to derive tighter finite-key security bounds.

\(^1\)After the completion of a preliminary version of this thesis, a new MDI-QKD implementation over 200 km of optical fibre using a system clock of 75 MHz has been reported in [116].
for MDI-QKD such that the post-processing data block sizes needed to achieve good performance could be reduced.

Very recently, a new QKD protocol, aiming at bridging the strong security of MDI-QKD with the high efficiency of conventional QKD, was proposed by three groups simultaneously [144, 145, 146]. Two important advantages of this approach are: (i) the high key generation rate, which is comparable with that of a conventional QKD protocol; (ii) the relatively simple implementation, which does not require the photon interference from two separate photon sources. This is achieved by replacing the two-photon BSM scheme (which is required in the original MDI-QKD protocol) by a single-photon BSM scheme [144, 145, 146]. However, the price to pay is that additional assumptions on the measurement device are required for the security proof. Note that a specific attack to comprise the security of this protocol has been proposed in [147]. A countermeasure to prevent the attack of [147] is to make other additional assumptions about the BSM devices [144]. In practice, the difficulty to guarantee these additional assumptions is still an open question for future research.

10.2.2 QRNG

We can improve the prototype of Fig. 9.7 by making it more compact and robust. For instance, a feed-back control can be realized to automatically stabilize the system. It is also important to create a real-time hardware-based randomness extractor at a high speed. Moreover, it is expected to build a compact, low-cost, high-speed, and robust QRNG system with USB port in the future. A commercial QRNG with USB port and a generation rate of 4 Mbits/s has already appeared on the market (see Fig. 10.2 for an example [16]).

![Figure 10.2: Commercial QRNG with USB port at a rate of 4 Mbits/s [16].](image)
Besides the development of the prototype, it will be interesting to further investigate the physical source for randomness generation. Based on a different type of laser and system design, the intensity fluctuations of a laser have been studied to generate fast random bits [148]. An improved system with a super-luminescent LED has also been demonstrated [149]. Since the fundamental physical origin of both the phase fluctuations and the intensity fluctuations of a laser is amplified spontaneous emissions, it will be interesting to demonstrate a QRNG exploiting both fluctuations. Very recently, a study on the feasibility of QRNG on mobile photon has also been reported in [150]. It will be interesting to integrate our QRNG prototype on a photonic chip. This can make the widespread use of quantum random numbers a reality, with an important impact on information security.
Appendix A

System model of MDI-QKD

In this section, we discuss an analytical method to model a polarization-encoding MDI-QKD system. That is, we calculate $Y^Z_{11}$, $e^X_{11}$, $Q^Z_{\mu\mu}$ and $E^Z_{\mu\mu}$ and thus estimate the expected key rate from Eq. (3.1). Note that $Q^Z_{11} = P^Z_{11}Y^Z_{11}$.

To simplify our calculation, we make two assumptions about the practical error sources: a) since most practical error sources do not contribute significantly to the system performance (see Section 5.1), we only consider the polarization misalignment $e_d$, the background count rate $Y_0$ and the detector efficiency $\eta_d$; b) for the model of the polarization misalignment, we consider only two unitary operators, $U_1$ and $U_2$, to represent respectively the polarization misalignment of Alice’s and Bob’s channel transmission, i.e., set $U_3 = I$ in the generic model of Sec. 5.1.1. For simplicity, a more rigorous derivation with $U_3 \neq I$ is not shown here, but it can be easily completed following our procedures discussed below.

A.1 $Y^Z_{11}$ and $e^X_{11}$

In the asymptotic case, we assume that $Y^Z_{11}$, $e^X_{11}$ in Eq. (3.1) can be perfectly estimated with an infinite number of signals and decoy states. Thus, they are given by

$$e^X_{11} = \frac{1}{2} - \frac{t_at_b\eta_d^2(1 - e_d)^2(1 - Y_0)^2}{4Y^X_{11}},$$

$$Y^Z_{11} = (1 - Y_0)^2[4Y_0^2(1 - t_a\eta_d)(1 - t_b\eta_d) + 2Y_0(t_a\eta_d + t_b\eta_d - \frac{3t_at_b\eta_d^2}{2}) + \frac{t_at_b\eta_d^2}{2}],$$

where $Y^X_{11} = Y^Z_{11}$. Importantly, we can see that ignoring the imperfections of polarization misalignment and background counts (i.e., $e_d = 0$, $Y_0 = 0$), $e^X_{11}$ is zero, while $Q^Z_{11} = P^Z_{11}Y^Z_{11}$ ($P^Z_{11} = \mu_a\mu_be^{-(\mu_a + \mu_b)}$) can be maximized with $\mu_a = \mu_b$. Thus, the optimal choice of
Appendix A. System model of MDI-QKD

106

intensities is $\mu_a = \mu_b = 1$. However, in practice, it is inevitable to have certain practical errors, which result in this optimal choice being a function of the practical errors.

A.2 $Q_{\mu\mu}^Z$ and $E_{\mu\mu}^Z$

Now, let us calculate $Q_{\mu\mu}^Z$ and $E_{\mu\mu}^Z$, which are eventually given by Eq. (A.10). To further simplify our discussion, we use \{H, V, D, A\} to represent the BB84 polarization states. Also, \{HH, HV, DD, DA\} will denote Alice’s and Bob’s encoding modes. We define the following notations: $\gamma_a = \sqrt{\mu_a t_a \eta_d}$, $\gamma_b = \sqrt{\mu_b t_b \eta_d}$, $\beta = \gamma_a \gamma_b$, $\gamma = \gamma_a^2 + \gamma_b^2$, $\lambda = \gamma_a \gamma_b \sqrt{e_{d1}} (1 - e_{d1})$, $\omega = \gamma_a^2 + e_{d1} (\gamma_b^2 - \gamma_a^2)$

Derivation of $Q_{Z}^{HH}$

First, both Alice and Bob encode their states in the H mode (symmetric to V mode). We assume that $U_1$ and $U_2$ (see Eq. (5.1)) rotate the polarization in the same direction, i.e. $\theta_1 \theta_2 > 0$. The discussion regarding rotation in the opposite direction (i.e. $\theta_1 \theta_2 < 0$) is similar. Note that in a practical polarization-encoding MDI-QKD system, the polarization rotation angle of each quantum channel ($\theta_1$ or $\theta_2$) can be modeled by a Gaussian distribution with a standard deviation of $\theta_{std}^k = \arcsin(\sqrt{e_k})$ ($k = 1, 2$), which means that both $\theta_1$ and $\theta_2$ (mostly) distribute in the range of $[-3\theta_{std}^k, 3\theta_{std}^k]$ and the relative direction between them also randomly distributes between $\theta_1 \theta_2 > 0$ and $\theta_1 \theta_2 < 0$.

The effect of the polarization misalignment is the same for $R^{\psi^-}$ and $R^{\psi^+}$, i.e., both $R^{\psi^-}$ and $R^{\psi^+}$ are independent of the total polarization misalignment. We can experimentally choose to measure either the Singlet or the Triplet by using only two detectors (but sacrificing half of the total key rate), such as in the experiments of [94, 96, 55].

In Charles’s lab, after the BS and PBS (see Fig. 5.1), the optical intensities received by each SPD are given by

\[
D_{ch} : |A|^2 = \frac{(1 - e_{d1}) (\gamma_a^2 + \gamma_b^2) - 2 \gamma_a \gamma_b \cos(\phi) (1 - e_{d1})}{2},
\]

\[
D_{dh} : |C|^2 = \frac{(1 - e_{d1}) (\gamma_a^2 + \gamma_b^2) + 2 \gamma_a \gamma_b \cos(\phi) (1 - e_{d1})}{2},
\]

\[
D_{cv} : |B|^2 = \frac{e_{d1} (\gamma_a^2 + \gamma_b^2) - 2 \gamma_a \gamma_b \cos(\phi) e_{d1}}{2},
\]

\[
D_{dv} : |D|^2 = \frac{e_{d1} (\gamma_a^2 + \gamma_b^2) + 2 \gamma_a \gamma_b \cos(\phi) e_{d1}}{2},
\]

where $\phi$ denotes the relative phase between Alice’s and Bob’s weak coherent states. Thus,
the detection probability of each threshold SPD is

\[ P_V = 1 - (1 - Y_0) e^{-|V|^2}, \]  
\[ (A.3) \]

where \( V = A, B, C, D \). Then, the coincident counts are

\[ Q_{Z}^{HH, \psi^+} = 2P_A P_B (1 - P_C)(1 - P_D), \]
\[ Q_{Z}^{HH, \psi^-} = 2P_A P_D (1 - P_B)(1 - P_C), \]

where \( Q_{Z}^{HH, \psi^+} \) and \( Q_{Z}^{HH, \psi^-} \) denote, respectively, the probability of the projection on the Triplet \( |\psi^+) = \frac{1}{\sqrt{2}}(|H, V) + |V, H) \) and the Singlet \( |\psi^-) = \frac{1}{\sqrt{2}}(|H, V) - |V, H) \). Here from Fig. 5.1, Triplet means the coincident detections of \{ch & cv\} or \{dh & dv\}; Singlet means the coincident detections of \{ch & dv\} or \{cv & dh\}. After averaging over the relative phase \( \phi \) (integration over \([0, 2\pi]\)), we have

\[ Q_{Z}^{HH, \psi^+} = 2e^{-\frac{\gamma^2}{2}}(1 - Y_0)^2[I_0(\beta) + (1 - Y_0)^2 e^{-\frac{\beta^2}{2}} - (1 - Y_0)e^{-\frac{(1 - e_{d1})}{2}} I_0(\beta - e_{d1} \beta)], \]
\[ Q_{Z}^{HH, \psi^-} = 2e^{-\frac{\gamma^2}{2}}(1 - Y_0)^2[I_0(\beta) - 2\beta e_{d1} + (1 - Y_0)^2 e^{-\frac{\beta^2}{2}} - (1 - Y_0)e^{-\frac{(1 - e_{d1})}{2}} I_0(\beta - e_{d1} \beta)], \]

where \( I_0(\cdot) \) is the modified Bessel function. Therefore, \( Q_{Z}^{HH} \) is given by

\[ Q_{Z}^{HH} = Q_{Z}^{HH, \psi^+} + Q_{Z}^{HH, \psi^-}. \]  
\[ (A.5) \]

Here, to simplify Eq. (A.2), we ignore background counts, i.e., \( Y_0 = 0 \), and use a 2nd order approximation (as both \( \beta \) and \( \gamma \) are typically on the order of 0.01) such that

\[ I_0(\beta) = 1 + \frac{\beta^2}{4} + O(\beta^4), \]
\[ e^{\gamma} = 1 + \gamma + \frac{\gamma^2}{2} + O(\gamma^3), \]

then, Eq. (A.2) can be estimated as

\[ Q_{Z}^{HH, \psi^+} = \frac{\gamma^2 e_{d1}(1 - e_{d1})}{2} + \beta^2 e_{d1}(1 - e_{d1}), \]  
\[ (A.6) \]
\[ Q_{Z}^{HH, \psi^-} = \frac{\gamma^2 e_{d1}(1 - e_{d1})}{2} - \beta^2 e_{d1}(1 - e_{d1}), \]

and \( Q_{Z}^{HH} \) is given by

\[ Q_{Z}^{HH} = \gamma^2 e_{d1}(1 - e_{d1}). \]
Derivation of $Q_{Z}^{HV}$

Alice (Bob) encodes her (his) state in the H (V) mode (symmetric to V (H)). We also assume $\theta_1 \theta_2 > 0$. At Charles’s side, the optical intensities received by each SPD are given by

$$|A'|^2 = \frac{(1 - e_{d1}) \gamma_a^2 + e_{d1} \gamma_b^2 - 2 \lambda \cos(\phi)}{2},$$

$$|B'|^2 = \frac{e_{d1} \gamma_a^2 + (1 - e_{d1}) \gamma_b^2 - 2 \lambda \cos(\phi)}{2},$$

$$|C'|^2 = \frac{(1 - e_{d1}) \gamma_a^2 + e_{d1} \gamma_b^2 + 2 \lambda \cos(\phi)}{2},$$

$$|D'|^2 = \frac{e_{d1} \gamma_a^2 + (1 - e_{d1}) \gamma_b^2 + 2 \lambda \cos(\phi)}{2}.$$

The detection probability of each SPD is described by Eq. (A.3). $Q_{Z}^{HV,\psi^+}$ and $Q_{Z}^{HV,\psi^-}$ can be calculated similarly to Eq. (A.4). After averaging over $\phi$, the results are

$$Q_{Z}^{HV,\psi^+} = 2e^{-\frac{\gamma}{2}}(1 - Y_0)^2[I_0(2\lambda) + (1 - Y_0)^2e^{-\frac{\gamma}{2}} - (1 - Y_0)e^{-\frac{\gamma}{2}}I_0(\lambda)],$$

$$Q_{Z}^{HV,\psi^-} = 2e^{-\frac{\gamma}{2}}(1 - Y_0)^2[1 + (1 - Y_0)^2e^{-\frac{\gamma}{2}} - (1 - Y_0)e^{-\frac{\gamma}{2}}I_0(\lambda)].$$

Therefore, $Q_{Z}^{HV}$ is given by

$$Q_{Z}^{HV} = Q_{Z}^{HV,\psi^+} + Q_{Z}^{HV,\psi^-}. \quad (A.8)$$

To simplify Eq. (A.7) we once again ignore the background counts and take a 2nd order approximation. Eq. (A.7) can be estimated as

$$Q_{Z}^{HV,\psi^+} = \frac{\omega(\gamma - \omega)}{2} + \lambda^2, \quad (A.9)$$

$$Q_{Z}^{HV,\psi^-} = \frac{\omega(\gamma - \omega)}{2} - \lambda^2,$$

and $Q_{Z}^{HV}$ is given by

$$Q_{Z}^{HV} = \omega(\gamma - \omega).$$

**Derivation of $Q_{\mu\mu}^{Z}$ and $E_{\mu\mu}^{Z}$**

Finally, $Q_{\mu\mu}^{Z}$ and $E_{\mu\mu}^{Z}$ can be expressed as

$$Q_{\mu\mu}^{Z} = \frac{Q_{Z}^{HH} + Q_{Z}^{HV}}{2}, \quad (A.10)$$

$$E_{\mu\mu}^{Z} = \frac{Q_{Z}^{HH}}{Q_{Z}^{HH} + Q_{Z}^{HV}}.$$
where the different terms on the r.h.s. of this equation are given by Eqs. (A.2, A.5, A.7, A.8). Therefore, together with Eq. (A.1), we could derive the analytical key rate of Eq. (3.1).

If we ignore background counts and take the 2nd order approximation from Eqs. (A.6, A.9), $Q_{\mu\mu}^{Z}$ and $E_{\mu\mu}^{Z}$ can be written as

\[
Q_{\mu\mu}^{Z} = \frac{\beta^2 + e_d(1 - \frac{e_d}{2})(\gamma^2 - 2\beta^2)}{2}, \quad (A.11)
\]

\[
E_{\mu\mu}^{Z} = \frac{\gamma^2 e_d(1 - \frac{e_d}{2})}{4Q_Z}.
\]
Appendix B

Local search algorithm

The optimal key rate is achieved via numerical optimization on many dimensions (parameters). To reduce both computational time and storage space of this optimization process, local search algorithm (LSA), a combination of coordinate descent (CD) and backtrack search (BS) algorithm, is adopted in lieu of the conventional exhaustive search algorithm. There are salient drawbacks of exhaustive search. If the search is too fine, the computational time and space are challenging. If the search is too coarse, we will miss finer details. In contrast, CD is a non-derivative approximation to the well-known steepest descent (SD) algorithm [151]. This approximation is necessary from the facts that our key rate is an implicit function (a linear program) of the parameters and the actual finding of gradients and hessians of SD cannot be done easily. CD converges to the same optimal point as SD, even though it requires more iterations. CD can fix low-speed by making large progress at the start, and it can also fix in-accuracy by re-defining how close to the optimal point the algorithm can stop. Table 5.1 compares the speed and accuracy of exhaustive search versus LSA.

CD is based on the idea that the minimization of a multivariate function (key rate $R$) can be achieved by minimizing it along one direction at a time (see Fig. B.1). Instead of varying descent direction according to gradient, one fixes descent directions at the outset [152]. These directions are usually the cartesian bases, i.e., $e_i$ with $i=1,2,3,....$ In the two decoy-state case, $e_1=\mu$, ..., $e_4=\mu$, ..., $e_7=P_{X|\mu}$, $e_8=P_{X|\nu}$, and this basis is iterated through one at a time, minimizing the objective function with respect to the current coordinate direction. Mathematically, to optimize $\mu$, if $\mu^k$ (optimized $\mu$ in the $k$th iteration) is given, the minimization of key rate $R$ (see Eq. 3.1) along $\mu$ coordinate
Figure B.1: Coordinate descent (CD). CD algorithm searches along one coordinate direction in each iteration, and it uses different coordinate directions cyclically. For instance, on the equiv-error contour of two-dimensional subspace, CD starts at point A (arbitrarily) and descents vertically along the direction $e_1$ to B, then horizontally along the direction $e_2$ toward C. After cyclic iterations of vertical and horizontal descent, the algorithm stops at D where it is very close to the optimal. This simplified two-dimensional example illustrates how generalized search in any dimensional space can be done analogously.

In the $k+1$th iteration is:

$$
\mu^{k+1} = \arg \max_{y \in \mathbb{R}} R(P_{\mu}^{k+1}, P_{\nu}^{k+1}, P_{X|\mu}^{k+1}, P_{X|\nu}^{k+1}, P_{X|\omega}^{k+1}, y, \nu^k, \omega^k)
$$

By doing line search in each iteration, we automatically have a sequence of vectors $x_0, x_1, x_2, ...$, where $x_i = ((P_{\mu})_i, (P_{\nu})_i, ..., (P_{X|\mu})_i, ..., (\nu)_i, (\omega)_i)$ and the sequence of key rate: $R(x_0) \geq R(x_1) \geq R(x_2) \geq ...$. The demonstration of convexity in Fig. B.2 will make the result of LSA a global optimum. Although CD requires an intelligent guess to start with, the starting point in convex topologies can be in theory any non-zero objective (key rate) point in the search space. In practice, prior research can shed light on the choices of initial parameters, and these parameters often are good candidates for the starting guess.

After a direction along a coordinate chosen in CD, we still have to do a one-dimensional line search problem to compute how far the search can move along a given coordinate. This is realized via the BS algorithm. BS starts at the end of previous iterations, and makes progress toward a minima along the chosen coordinate direction. With a step from one side to the minima to the other side, the algorithm found a turning point. From there, BS searches backward again toward the minima until the same turning point is found with greater accuracy. The procedure is iterated until converged.
Figure B.2: (Color online) Convexity of key rate function. The key rate is simulated by sweeping $\mu$ and $\nu$, and optimizing other parameters at 0km with $N=10^{12}$.

to the minima. At this point in the search space, the CD algorithm restarts with a new direction of line-search.
Appendix C

Asymmetric MDI-QKD

Here we discuss the properties of a practical asymmetric MDI-QKD system. For this, we derive an analytical expression for the estimated key rate and we optimize the system performance numerically.

C.1 Estimated key rate

The estimated key rate $R_{\text{est}}$ is defined under the condition that background counts are ignored. Note that this is a reasonable assumption for a short distance transmission.

**Theorem 1** $\mu_a^{opt}$ and $\mu_b^{opt}$ only depend on $x$ rather than on $t_a$ or $t_b$; Under a fixed $x$, $R_{\text{est}}$ is quadratically proportional to $t_b$.

**Proof:** When $Y_0$ is ignored, $Y_{11}^Z$ and $e_{11}^X$ are given by (see Eq. (A.1))

\[
e_{11}^X = e_d - \frac{e_d^2}{2},
\]

\[
P_{11}Y_{11}^Z = \mu_a t_a \mu_b t_b e^{-(\mu_a + \mu_b)\eta_d^2}.
\]

If we take the 2nd order approximation, $Q_Z$ and $E_Z$ are estimated as (see Eq. (A.11))

\[
Q_{\mu \mu}^Z = \frac{t_b^2 \eta_d^2 [2x\mu_a \mu_b + (\mu_b^2 + x^2 \mu_a^2)(2e_d - e_d^2)]}{4}, \tag{C.1}
\]

\[
E_{\mu \mu}^Z = \frac{(\mu_b + x\mu_a)^2(2e_d - e_d^2)}{2[2x\mu_a \mu_b + (\mu_b^2 + x^2 \mu_a^2)(2e_d - e_d^2)]}.
\]

By combining the above two equations with Eq. (3.1), the overall key rate can be written as

\[
R_{\text{est}} = \frac{t_b^2 \eta_d^2}{2} G(x, \mu_a, \mu_b), \tag{C.2}
\]
Figure C.1: Asymptotic key rates of $R_{\text{rig}}$ and $R_{\text{est}}$. $R_{\text{rig}}$ and $R_{\text{est}}$ denote respectively the rigorous key rate (Eq. (3.1)) and the estimated key rate (Eq. (C.2)). At short distances, the overlap between $R_{\text{rig}}$ and $R_{\text{est}}$ demonstrates the accuracy of our estimation model, while at long distances, background counts affect its accuracy. An asymmetric system can tolerate a maximal channel mismatch of $x=0.004$ (120 km length difference for two standard fiber links).

where $G(x, \mu_a, \mu_b)$ has the form

$$G(x, \mu_a, \mu_b) = x\mu_a\mu_be^{-(\mu_a+\mu_b)}[1 - H_2(e_d - \frac{e_d^2}{2})]$$

$$- \frac{2x\mu_a\mu_b+\mu_a^2+\mu_b^2}{2(2e_d-e_d^2)} \times f_eH_2(E_{\mu\mu}^Z),$$

where $E_{\mu\mu}^Z$ is given by Eq. (C.1) and is also a function of $(x, \mu_a, \mu_b)$. Therefore, optimizing $R_{\text{est}}$ is equivalent to maximizing $G(x, \mu_a, \mu_b)$ and the optimal values, $\mu_a^{\text{opt}}$ and $\mu_b^{\text{opt}}$, are only determined by $x$. Under a fixed $x$, the optimal key rate is quadratically proportional to $t_b$. For a given $x$, the maximization of $G(x, \mu_a, \mu_b)$ can be done by calculating the derivatives over $\mu_a$ and $\mu_b$ and verified using the Jacobian matrix.

### C.2 Properties of asymmetric MDI-QKD

We numerically study the properties of an asymmetric MDI-QKD system. In our simulations below, the asymptotic key rate, denoted by $R_{\text{rig}}$, is rigorously calculated from the key rate formula given by Eq. (3.1) in which each term is shown in Appendix A. $R_{\text{est}}$ denotes the estimated key rate from Eq. (C.2). The practical parameters are listed in Table 4.2. We used the method of [47] for the finite-key analysis.
Figure C.2: Optimal $\mu_a$ and $\mu_b$. At short distances (i.e., $x$ is around 1 or bigger), $\mu_a^{\text{opt}}$ and $\mu_b^{\text{opt}}$ depend only on $x$, while at long distances (i.e., $x<0.5$), background counts contribute significantly. The non-smooth behaviors here are mainly due to background counts and numerical errors.

Firstly, Fig. C.1 simulates the key rates of $R_{\text{rig}}$ and $R_{\text{est}}$ at different channel lengths. For short distances (i.e., total length $L_{ac} + L_{bc} < 100$ km), the overlap between $R_{\text{est}}$ and $R_{\text{rig}}$ demonstrates the accuracy of our estimation model of Eq. (C.2). Therefore, in the short distance range, we could focus on $R_{\text{est}}$ to understand the behaviors of the key rate. Moreover, from the curve of $L_{bc}=1m$, we have that this asymmetric system can tolerate up to $x=0.004$ (120 km length difference for standard fiber links).

Secondly, Fig. C.2 shows $\mu_a^{\text{opt}}$ and $\mu_b^{\text{opt}}$, when both $L_{bc}$ and $L_{ac}$ are scanned from 1 m to 100 km. These parameters numerically verify Theorem 1: at short distances ($x\geq0.5$), $\mu_a^{\text{opt}}$ and $\mu_b^{\text{opt}}$ depend only on $x$, while at long distances ($x<0.5$), background counts contribute significantly and result in non-smooth behaviors. $\mu_a^{\text{opt}}$ and $\mu_b^{\text{opt}}$ are both in $O(1)$.

Finally, we simulate the optimal key rates under two fixed $x$ in Fig. C.3.

1. Solid curves are the asymptotic keys: at short distances ($L_{bc}+L_{ac}<120$ km), the maximal $G(x,\mu_a,\mu_b)$ is fixed with a fixed $x$ (see Eq. (C.3)). Taking the logarithm with base 10 of $R_{\text{est}}$ and writing $t_b=10^{-\alpha L_{bc}}$, Eq. (C.2) can be expressed as

$$\log_{10} R_{\text{est}} = -2\alpha L_{bc} + \log_{10} \frac{\eta^2 G(x,\mu_a,\mu_b)}{2}. \quad (C.4)$$

Hence, the scaling behavior between the logarithm (base 10) of the key rate and the channel distance is linear, which can be seen in the figure. Here, $\alpha = 0.2 \text{ dB/km}$ (standard fiber link) results in a slope of -0.4.
Figure C.3: Key rate with fixed $x$. Solid curves are the asymptotic key rates: as shown in Eq. (C.4), $\log_{10} R_{\text{est}}$ is linearly proportional to $L_{bc}$. Dashed curves are the two decoy-state key rates without the finite-key effect, i.e., with an infinite number of signals. Dotted curves are the two decoy-state key rates with the finite-key analysis: we consider a total number of signals $N = 10^{14}$ and a security bound of $\epsilon = 10^{-10}$; for the dotted curve with $x=0.1$, the optimal intensities satisfy $\mu_a^{\text{opt}}/\mu_b^{\text{opt}} = \nu_a^{\text{opt}}/\nu_b^{\text{opt}} \approx 7$, which means that the ratios for the optimal $\mu$ and $\nu$ are roughly the same and this ratio is mainly determined by $x$. Even taking the finite-key effect into account, the system can still tolerate a total fiber link of 110 km.
Appendix D

Decoy states for three-state protocol

Our decoy-state analysis builds on [112], which discusses the decoy-state BB84. Our new contribution is estimating the phase error rate \( e_{x,1}^U \). In decoy-state BB84, \( e_{x,1}^U \) is estimated from the counts in X basis [112]. In three-state protocol, however, \( e_{x,1}^U \) is estimated from the rejected counts, i.e., considering the detection events associated with single photons when Alice and Bob use different bases. Notice also that our estimation focuses directly on the detection counts announced by Bob, which is different from previous analysis that is based on detection probabilities [60, 61].

In original decoy-state method [60, 61], Alice first randomly chooses an intensity setting (signal state or decoy state) to modulate each laser pulse and then she announces her intensity choices after Bob’s detections. One can imagine a virtual but equivalent protocol: Alice has the ability to first send \( n \)-photon states and then she only decides on the choice of intensity after Bob has a detection. Let \( s_{z,n} \) be the number of detection counts observed by Bob given that Alice sends \( n \)-photon states in Z basis. Note that \( \sum_{n=0}^{\infty} s_{z,n} = n_z \) is the total number of detections (gain counts). In the asymptotic limit with two decoy states, we have

\[
\hat{n}_{z,k} = \sum_{n=0}^{\infty} P_{k|n}s_{z,n}, \quad \forall k \in \{\mu, \nu, \omega\},
\]

where \( P_{k|n} \) is the conditional probability of choosing the intensity \( k \) given that Alice prepares an \( n \)-photon state. For finite-data size, from Hoeffding’s inequality [153], the experimental measurement \( n_{z,k} \) satisfies

\[
|\hat{n}_{z,k} - n_{z,k}| \leq \delta(n_z, \epsilon_1),
\]

with probability at least \( 1 - 2\epsilon_1 \), where \( \delta(n_z, \epsilon_1) = \sqrt{n_z/2 \log(1/\epsilon_1)} \) and \( \hat{n}_{z,k} \) is the expected value of \( n_{z,k} \). Note that our analysis considers the most general type of attack –
Appendix D. Decoy states for three-state protocol

joint attack – consistent with quantum memories. The above equation allows us to establish a relation between the asymptotic values and the observed statistics. Specifically,

\[ \hat{n}_{z,k} \leq n_{z,k} + \delta(n_{z}, \epsilon_1) = n_{z,k}^U, \]

\[ \hat{n}_{z,k} \geq n_{z,k} - \delta(n_{z}, \epsilon_1) = n_{z,k}^L, \]

are respectively the upper and lower bound of the gain counts \( n_{z,k} \) for a given intensity setting \( k \in \{\mu, \nu, \omega\} \).

An analytical lower-bound on \( s_{z,0} \) can be established by exploiting the structure of the conditional probabilities \( P_{k|n} \) based on Bayes’ rule: \( P_{k|n} = \frac{P_k \ e^{-k \ k_n}}{\tau_n} \), where \( \tau_n = \sum_{k \in \{\mu, \nu, \omega\}} P_k e^{-k \ k_n} / n! \) is the probability that Alice prepares an \( n \)-photon state. Based on an estimation method in [63], we have

\[ s_{z,0}^L = \frac{\tau_0}{(\nu - \omega)} \left( \frac{\nu e^\omega n_{z,\omega}^L}{P_\omega} - \frac{\omega e^\nu n_{z,\nu}^U}{P_\nu} \right), \quad (D.1) \]

\[ s_{z,1}^L = \frac{\mu \tau_1}{\mu (\nu - \omega) - (\nu^2 - \omega^2)} \left[ \frac{e^\nu n_{z,\nu}^U}{P_\nu} - \frac{e^\omega n_{z,\omega}^L}{P_\omega} + \frac{\nu^2 - \omega^2}{\mu^2} \left( \frac{s_{z,0}^L}{\tau_0} - \frac{e^\mu n_{z,\mu}^U}{P_\mu} \right) \right]. \quad (D.2) \]

Different from [112], the phase error rate \( e_{x,1}^U \) in a three-state protocol is estimated using the rejected data analysis [86]:

\[ e_{x,1}^U = \frac{2P_{x} s_{0|z,1}^U + P_{z} (s_{1|z,1}^U - s_{0|z,1}^L)}{2P_{x} s_{z,1}^L}, \quad (D.3) \]

where \( P_x \) (\( P_z \)) is the probability that Alice/Bob selects \( X \) (\( Z \)) basis; \( s_{0|z,1}^U \) denotes the upper bound of single-photon events when Bob has detections associated with bit “0” in \( X \) basis, given that Alice sends a state in \( Z \) basis; \( s_{1|z,1}^U, s_{0|z,1}^L, s_{z,1}^L \) has the similar meaning. \( s_{0|z,1}^L \) and \( s_{z,1}^L \) can be estimated equivalently by plugging \( n_{0|z,k}^L (n_{0|z,k}^U) \) and \( n_{z|z,k}^L (n_{z|z,k}^U) \) into Eqs. (D.1) and (D.2) to replace \( n_{z,k}^L (n_{z,k}^U) \). \( s_{0|z,1}^U \) and \( s_{1|z,1}^U \) can be estimated by

\[ s_{0|z,1}^U = \tau_1 \frac{n_{0|z,\nu}^U - n_{0|z,\omega}^L}{\nu - \omega}, \]

\[ s_{1|z,1}^U = \tau_1 \frac{n_{1|z,\nu}^U - n_{1|z,\omega}^L}{\nu - \omega}. \]
Appendix E

GLLP security analysis with source flaws

We discuss the standard GLLP security analysis for BB84 with source flaws [41, 42], which is used for our simulation of Fig. 8.2. We focus on phase encoding BB84 and assume \( \{ \delta_1, \delta_2, \delta_3 \} \) to be Alice’s phase modulation errors for \( \{ \pi/2, \pi, 3\pi/2 \} \), thus the four BB84 imperfect states sent by Alice are given by

\[
\begin{align*}
|\phi_{0z}\rangle &= |0z\rangle \\
|\phi_{1z}\rangle &= \sin \delta_2 |0z\rangle + \cos \delta_2 |1z\rangle \\
|\phi_{0x}\rangle &= \cos \delta_1 |0x\rangle + \sin \delta_1 |1x\rangle \\
|\phi_{1x}\rangle &= \sin \delta_3 |0x\rangle + \cos \delta_3 |1x\rangle
\end{align*}
\]  
(E.1)

Based on GLLP for imperfect sources, the \( \epsilon_{\text{sec}} \)-secret key length is similar to Eqn. 8.1, except for the phase error rate, which includes the correction due to basis-dependent flaws and is revised to [41]

\[
\bar{e}_{x,1}^U \leq e_{x,1}^U + 4\Delta' + 4\sqrt{\Delta'e_{x,1}^U} + \epsilon_{pb}
\]  
(E.2)

Here, \( \Delta' \), called the balance of a quantum coin [41, 42], quantifies the basis-dependent flaws of Alice signals associated with single-photons events. \( \Delta' \) is given by [41]

\[
\Delta' \leq \frac{\Delta}{Y_1}
\]
(E.3)

\[
\Delta = \frac{1 - F(\rho_z, \rho_x)}{2}
\]

where \( Y_1 = \frac{N_{P_{x,1}}}{N_{P_{z,1}}} \) (typically called the yield of single photons [60]) is the frequency of successful detections associated with single-photons; \( F(\rho_z, \rho_x) \) is the fidelity of the density
matrices for the $Z$ and $X$ basis. Using Eq. (E.1), we can easily calculate $F(\rho_z, \rho_x)$ given \{\delta_1, \delta_2, \delta_3\}. In our QKD system, with \{\delta_1, \delta_2, \delta_3\} upper bounded by 0.127, we have $F(\rho_z, \rho_x)=1 - 1.9 \times 10^{-3}$. So, from Eq. (E.3), $\Delta = 9.45 \times 10^{-4}$.

In GLLP analysis, the imperfect fidelity $F(\rho_z, \rho_x)$ can in principle be enhanced by Eve via exploiting the channel loss, which is clearly shown in Eq. (E.3), i.e., $\Delta$ is enhanced to $\Delta'$. Combined with the decoy-state estimations discussed in [112], we can derive the key length and obtain the insert curves in Fig. 8.2.
Appendix F

Verify Qubit assumption

We verify the qubit assumption, i.e., that the four BB84 states remain in two dimensions. This assumption is commonly made in various QKD protocols including decoy-state BB84 and MDI-QKD. We focus on a standard one-way phase-encoding system, which has been widely implemented in experiments [12, 37, 154]. In this system, LiNbO$_3$ waveguide-based phase modulator (PM) is commonly used to encode/decode phase information. Fig. F.1 illustrates the schematic of such PM [155]. To guarantee the qubit assumption, Alice’s PM is supposed to have the same timing, spectral, spatial and polarization mode information for different BB84 states. We find that timing and spatial information can be easily guaranteed without any additional devices, while spectral and polarization information can also be guaranteed with standard low-cost optical devices such as wavelength filter and polarizer. Therefore, based on standard devices, we can verify the qubit assumption with high accuracy. In the following, we discuss timing, spectral, spatial and polarization properties for different encoding phases.

Temporal-spectral mode

Temporal mode: Fig. F.1 shows the schematic of the phase modulation based on LiNbO$_3$ crystal. When phase modulator (PM) modulates different phases, the electrical-optical effect inside the LiNbO$_3$ waveguide changes the principal refractive index $n_z$. At first sight, it might appear that the timing information is indeed changed for different phase modulations. However, we will show that such change is so small that it can be neglected.

According to the EM theory in LiNbO$_3$ waveguide, the relations among the principal refractive index $n_z$, the group refractive index $n_g$ and the extraordinary refractive index
Appendix F. Verify Qubit assumption

Figure F.1: Schematic of an electro-optic phase modulator based on LiNbO$_3$ crystal [155]. The double-headed arrows show the direction of polarization of the optical beam. The crystal is cut in a configuration so that the applied electrical field (voltage) is along the direction of the principal ($z$) axis. To take the advantage of the largest electro-optical coefficient in the $z$ axis, an optical beam is propagating along the $x$ axis, with the direction of polarization parallel to the $z$ axis.

$n_e$ are given by [155]

\[
\begin{align*}
n_g &= n_z + \omega_0 \frac{dn_z(\omega)}{d\omega} |_{\omega_0} \\
n_z &= n_e - \frac{1}{2} n_e^2 r_z V \frac{d}{d}
\end{align*}
\]

where $\omega_0$ is the central frequency of the optical field, $r_z$ is the electro-optical coefficient along $z$ axis, $V$ is the voltage applied onto the crystal, and $d$ is the thickness of the crystal. Thus the timing difference $\Delta t$ between $\{0\}$ and phase modulation $\{\pi\}$ is given by

\[
\Delta t = \left[ \frac{1}{2} n_e^3 r_z V_{\pi} + 3 \frac{n_e^2 r_z V_{\pi}}{2} \omega_0 \frac{dn_e(\omega)}{d\omega} |_{\omega_0} \right] \frac{l_0}{c}
\]

where $V_{\pi} = \frac{\lambda_0 d}{n_e^2 r_z l_0}$ is the half-wave voltage that provides a phase modulation $\{\pi\}$ [155], $l_0$ is the length of the crystal and $c$ is the speed of light.

For a typical LiNbO$_3$ crystal working in the telecom wavelength $\lambda_0 \sim 1550$ nm, it is well known that the relation between $n_e$ and $\lambda_0$ is given by [156]

\[
n_e^2 = 1 + \frac{2.980\lambda_0^2}{\lambda_0^2 - 0.020} + \frac{0.598\lambda_0^2}{\lambda_0^2 - 0.067} + \frac{8.954\lambda_0^2}{\lambda_0^2 - 416.08}
\]

Notice that in a waveguide based PM, one has to use the effective index, i.e., $n_{eff}$, to include the waveguide effect. We remark however that, for LiNbO$_3$ material, $n_{eff}$ and $n_e$ are almost the same [157]. Hence, by plugging Eq. (F.3) into Eq. (F.2), we have $\Delta t \approx 4 \times 10^{-6}$ ns. In a QKD implementation, the optical pulse is typically around 1 ns width [37, 38, 39] or 0.1 ns [12, 154], thus $\Delta t \ll 0.1$ ns. Assuming that the optical pulse is Gaussian, $\Delta t$ corresponds to a fidelity of $F(\rho^0, \rho^\pi) \approx 1 - 10^{-8}$ between $\{0\}$ and $\{\pi\}$. Therefore, timing remains (almost) the same for different phase modulations.
Appendix F. Verify Qubit assumption

**Spectral mode:** First, in a standard one-way system, Alice can locally synchronize the devices so that the optical pulse passes through Alice’s PM in the middle of the electrical modulation signal (flat response). Hence, the optical pulse experiences a correct modulation *without* spectral change [20, 158]. In a two-way system, Alice can monitor the timing information between the signal and reference pulse to guarantee the correct modulation and defend against side-channel attacks [20, 158]. Second, to guarantee single spectral mode from the output of a laser, one can use a standard wavelength filter. For instance, a recent QKD experiment used an off-the-shelf wavelength filter with a full-width at the half maximum (FWHM) of $\Delta \nu = 15$ GHz for a different purpose [154]. In this case, given a Gaussian pulse with FWHM $\Delta t = 0.1$ ns in the time domain [154], it is quite close to the lower bound of time-bandwidth product [155], i.e., $\Delta t \times \Delta \nu \geq \frac{2ln2}{\pi}$. Wavelength filters with narrow bandwidth have already been widely available on the market. Hence, single spectral mode can be guaranteed with high accuracy by using a wavelength filter.

**Spatial mode**

For a standard single-mode fiber (SMF), the core diameter is around 10 um. Theory and experiments have already confirmed that a SMF in the telecom wavelength rejects all high-order modes and conducts only one fundamental mode [159]. Using the software of BeamPROP, we have also performed a numerical simulation with a standard multi-mode fiber propagating into a SMF. The results show that after only about one millimeter, SMF rejects almost all high-order modes. The high-order modes decay exponentially, thus after about ten millimeters, there is no high-order component left (less than $10^{-10}$ proportion). Notice that, the input of a standard commercial PM usually has a certain length of pigtail fiber (about one meter). Therefore, the single mode assumption on spatial mode can be easily guaranteed in practice.

**Polarization mode**

The input of a commercial PM is normally a pigtail of polarization maintaining fiber, which can ensure that the input polarization is perfectly aligned with the principal axis of PM. Experimentally, before this polarization maintaining fiber, one can use a fiber polarization beam splitter (PBS) to reject other polarization modes. A standard PBS has about 30 dB extinction ratio. In the following, we discuss the error due to this finite extinction ratio (30 dB). Ideally, if the PBS has infinitely large extinction ratio, the input
Appendix F. Verify Qubit assumption

The state is perfectly aligned with the principal axis (z axis in Fig. F.1) and Alice modulates the four BB84 states as

$$|\phi_j\rangle = \frac{1}{\sqrt{2}} (e^{i\frac{\pi}{4}} |S_z\rangle + |R_z\rangle),$$

where $j \in \{0, 1, 2, 3\}$ denotes the four BB84 states and $|S_z\rangle$ ($|R_z\rangle$) denotes the signal (reference) pulse with polarization along z axis. However, due to the finite extinction ratio of PBS, the signal and reference pulse are expressed as

$$|S\rangle = \alpha |S_y\rangle + \beta |S_z\rangle,$$
$$|R\rangle = \alpha |R_y\rangle + \beta |R_z\rangle,$$

where $|S_y\rangle$ denotes the polarization component along y axis. For 30 db extinction ratio, $\alpha^2 \approx 0.001$. Thus Alice’s imperfect modulations can be described by

$$|\phi'_j\rangle = \frac{1}{\sqrt{2}} (\alpha e^{i\frac{\pi}{4}} |S_y\rangle + \beta e^{i\frac{\pi}{4}} |S_z\rangle + \alpha |R_y\rangle + \beta |R_z\rangle),$$

where we assume that the relative modulation magnitude ratio between the polarization aligned with the principal axis (z axis) and the orthogonal polarization (y axis in Fig. F.1) is 1:3 [155, 20]. Using three new bases $\{|e_1\rangle, |e_2\rangle, |e_3\rangle\}$, Eq. (F.4) can be written as (similar to [40])

$$|\phi'_j\rangle = \frac{1}{\sqrt{2}} (\alpha \beta (e^{i\frac{\pi}{4}} - e^{i\frac{\pi}{4}}) |e_1\rangle + (\alpha^2 e^{i\frac{\pi}{4}} + \beta^2 e^{i\frac{\pi}{4}}) |e_2\rangle + |e_3\rangle),$$

Hence, the four imperfect states is spanned to three dimensions in Hilbert space, i.e., the information encoded by Alice is not only in the time-phase mode but also in the polarization mode. However, for 30 dB extinction ratio, we find that it is almost impossible for Eve to attack the system, because the fidelity between $|\phi_j\rangle$ and $|\phi'_j\rangle$, $F(\rho|\phi_j\rangle, \rho|\phi'_j\rangle) = tr\sqrt{\sqrt{\rho|\phi_j\rangle \rho|\phi'_j\rangle} \sqrt{\rho|\phi'_j\rangle \rho|\phi_j\rangle}}$, is about $1 - 10^{-7}$ for $j \in \{0, 1, 2, 3\}$. This shows that the imperfect states are highly close to the perfect BB84 states. Most importantly, one can derive a refined security proof to include this small imperfection into the secure key rate formula, which will be a subject of future investigation.
Bibliography


[67] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. O’Brien,

[68] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih,

compact quantum random number generator,” Review of Scientific Instruments,

[70] J. Dynes, Z. Yuan, A. Sharpe, and A. Shields, “A high speed, postprocessing free,
quantum random number generator,” Applied Physics Letters, vol. 93, no. 031109,
2008.

[71] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich,
P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, “Rand-
don numbers certified by bell’s theorem.,” Nature, vol. 464, no. 7291, p. 1021,
2010.

[72] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. Andersen, C. Mar-
quardt, and G. Leuchs, “A generator for unique quantum random numbers based

[73] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and
Y. Yamamoto, “Quantum key distribution over a 40-db channel loss using super-
conducting single-photon detectors,” Nature photonics, vol. 1, no. 6, pp. 343–348,
2007.

[74] R. Hughes, W. Buttler, P. Kwiat, S. Lamoreuax, G. Morgan, J. Nordholt, and
C. Peterson, “Quantum cryptography for secure satellite communications,” in IEEE

Yang, H. Jiang, Y.-L. Tang, et al., “Direct and full-scale experimental verifications


