SECURITY AND IMPLEMENTATION OF DIFFERENTIAL PHASE SHIFT QUANTUM KEY DISTRIBUTION SYSTEMS

A DISSERTATION
SUBMITTED TO THE DEPARTMENT OF ELECTRICAL
ENGINEERING
AND THE COMMITTEE ON GRADUATE STUDIES
OF STANFORD UNIVERSITY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

Eleni Diamanti

June 2006

I certify that I have read this dissertation and that, in my opinion, it is fully adequate in scope and quality as a dissertation for the degree of Doctor of Philosophy.

Yoshihisa Yamamoto Principal Adviser

I certify that I have read this dissertation and that, in my opinion, it is fully adequate in scope and quality as a dissertation for the degree of Doctor of Philosophy.

David A. B. Miller

I certify that I have read this dissertation and that, in my opinion, it is fully adequate in scope and quality as a dissertation for the degree of Doctor of Philosophy.

Martin M. Fejer (Applied Physics)

Approved for the University Committee on Graduate Studies.

Abstract

Quantum information processing has attracted a lot of attention in recent years because of the promise it holds for faster, better, and more secure future communications. The most advanced field in quantum information processing is quantum cryptography, also referred to as quantum key distribution (QKD), which uses the quantum properties of light to ensure the unconditionally secure transmission of a secret message between two parties. Despite the significant progress achieved in the performance of quantum cryptography systems, the communication distance has been limited to a few tens of kilometers and the communication speed remains very low, preventing the integration of these systems into current telecommunication networks. The main limiting factors are the vulnerability of existing QKD algorithms to powerful eavesdropping attacks, and the characteristics of the single-photon detectors employed in the system.

This work addresses both of these limiting factors. We introduce and prove the security of a new quantum cryptography algorithm, the differential phase shift QKD protocol, which requires a very simple system architecture and only standard telecommunication components, such as lasers, detectors, and linear optics. The security proof against the most general attacks allowed by quantum mechanics reveals that this protocol is very robust to powerful eavesdropping attacks. Furthermore, we develop a new single-photon detector, which combines frequency up-conversion in a periodically poled lithium niobate waveguide and a silicon avalanche photodiode to achieve high speed and efficient single-photon detection in the telecommunication wavelength band. By combining these key elements of a quantum cryptography system, we demonstrate the experimental realization of practical and efficient fiber-optic

QKD systems, with which we achieved communication at a rate of 2 Mbit/s over 10 km, and transmission of secure messages over 100 km of optical fiber. Compared to existing systems, these results represent an improvement of more than two orders of magnitude in communication speed and a factor of two in communication distance. Thus, they demonstrate that high speed and long distance secure quantum communication is possible with currently available technology, and open the way for real-world applications of quantum information processing.

Acknowledgments

The work that I will present in this thesis would not have been possible without the help and support provided in many different ways by many different people, whom I would like to thank below.

First of all, I would like to thank my advisor, Yoshi Yamamoto, for the great advice and guidance that he has given to me throughout these years. I hope that one day I will be able to acquire the unbelievably deep intuition and understanding of physical mechanisms that Yoshi has and that I sincerely admire. I am also very grateful to my thesis committee: David A. B. Miller taught me quantum mechanics when I came to Stanford and he is a great teacher and a great person, I have enjoyed learning from him and talking to him very much; Martin M. Fejer contributed a lot to this thesis work and my discussions with him have significantly increased my knowledge of nonlinear optics; and Leonid Kazovsky brought to the committee the indispensable point of view of a classical optical communications expert. I would also like to thank Steve Harris, who was my Master's advisor, and Jelena Vučković, who has always been very supportive and gave me the opportunity to assist her in teaching quantum mechanics, which was a very rewarding experience.

This thesis work is mainly experimental, and so by definition a product of group effort. Among the colleagues that I was fortunate to work with I would like to particularly thank Edo Waks and Hiroki Takesue. Edo and Hiroki are great experimentalists, from whom I learned practically everything that I know. Most importantly, they are wonderful people, who were always available to answer my questions and respond to my concerns, and made the long hours in the dark lab a lot more enjoyable; I thank them both with all my heart. I would also like to thank Carsten Langrock, who made the best possible waveguides for our experiments, Rosti Roussev, Toshimori Honjo, Kyo Inoue, David Fattal, and George Kalogerakis, who always gave me invaluable advice for solving problems related to fiber-optic systems.

Apart from my close colleagues, I have had the pleasure in these years to discuss various subjects, scientific or not, with all the members of the Yamamoto group, in particular with Thaddeus Ladd, Patrik Recher, Stephan Götzinger, Cyrus Master, Charles Santori, Gregor Weihs, Anne Verhulst, Susan Clark, Hui Deng, Kai-Mei Fu, Na Young Kim, David Press, George Roumpos, as well as Fumiko Yamaguchi, Bingyang Zhang, Katsuya Nozawa, Kaoru Sanaka, Jonathan Goldman, Will Oliver, Matthew Pelton, Jocelyn Plant, Chia-Yu Chen, Kristiaan DeGreve, Shinichi Koseki, Neil Na, and Young Chul Yun. In the Yamamoto group, I have also found the most efficient and friendly administrative support provided by Yurika Peterman, Rieko Sasaki, and Mayumi Hakkaku. Finally, I am grateful to Athina and Nick Arvanitidis for providing financial support through the Stanford Graduate Fellowship program for the first three years of my graduate work.

Although I have spent a considerable time in the past years working in my office and lab with my colleagues, all the rest of my time I have shared happy moments with my friends. I have been lucky enough to have the most wonderful friends from back home in Greece, from Stanford, and from France. In particular I would like to thank Maria for her everlasting invaluable friendship; Iordanis for sharing all our respective thoughts and dreams; Prakash and Joanne for many discussions and precious moments; Fayaz for supporting his fellow electrical engineer in the sea of economists that surrounds us; Enrique and Laura for teaching us basketball and how to always smile; Pedro and Ana-Paula for their unbeatable fezuada; Saumitra and Jessie for their stories about their trips all over the world; Katerina for her true care and support and her movie reviews; Athina for her liveliness; Abdel for all our adventures around the world; and Vangelio, Vangelis, the Yiannis in Athens, Berlin, and Stanford, Markos, Manolis, Lina, Argyro, Ilias, Eleni, Yorgos, Dimitris, Joy, Sanne, Gabriel, François, Julie, Câline, Guillaume, Marie, Seb, Vincent, Charlotte, Raphael, Emma, Olivier, Ludivine for having coffee, playing games, trekking in Patagonia, riding motorbikes in Santorini, and talking for many, many hours. After the end of this thesis, although I will be much closer to some of my friends I will also be far away from some others, and I will miss them very much, but I am sure that we will find ways to meet somewhere around the world many times in the years to come.

Most importantly, I would like to thank my precious family, whose encouragement, love, and support were invaluable throughout the difficult process of finishing a thesis. I have missed my twin sister Kelly very much during these years but we have not stopped being there one for the other for a single moment even from so far away. I know I can rely on my older sister Iliana no matter what happens and she has always given me the best possible advice. My mom, Despina, has cared for me like nobody else in my whole life and especially these years that I have been so far from her. My dad, Dimitris, loves science in all its forms, from biology and geology to chemistry, but he particularly loves physics and astronomy; he taught us how to read the sky when we were little kids and with small experiments he inspired in us the interest in how the world works, so it comes as no surprise that I decided to become a scientist myself. Alexandros, Aris and their families have also been very supportive throughout these years, while in Claude, Josette, Yves, Jean, Marc, Michiko and Michel I have found the most wonderful second family I could have hoped for. Finally, nothing would have been the same without my Emeric, who is by far the best thing that happened to me at Stanford and makes everything else worthwhile; and I know that we will always make each other as happy as we have been in the past years.

Contents

Abstract **v**

Acknowledgments **vii**

1 Introduction **1**

2 Theory of quantum cryptography **7**

2.1 Introduction 7

2.2 Encoding quantum information 9

2.2.1 The photonic qubit 9

2.2.2 Single-photon generation 16

2.2.3 Entangled qubits 18

2.3 A general quantum key distribution algorithm 21

2.3.1 Quantum transmission 22

2.3.2 Sifting 23

2.3.3 Error correction 24

2.3.4 Privacy amplification 25

2.4 The BB84 protocol 30

2.4.1 The standard BB84 protocol 30

2.4.2 The decoy state BB84 protocol 40

2.5 The BBM92 protocol 43

2.6 Summary 47

3 Differential phase shift quantum key distribution 49

3.1 Introduction 49

3.2 The DPS-QKD protocol 51

3.3 Security proof against restricted attacks 53

3.3.1 The beamsplitter attack 54

3.3.2 The intercept and resend attack 56

3.3.3 A small modification 61

3.4 Security proof against general individual attacks 63

3.5 Security proof against sequential attacks 70

3.6 Summary 73

4 The up-conversion single-photon detector 75

4.1 Introduction 75

4.2 InGaAs/InP and Si avalanche photodiodes 76

4.3 The up-conversion single-photon detector 79

4.3.1 Principle of operation 79

4.3.2 1.55 μm single-photon detection experiment 84

4.3.3 1.32 μm single-photon detection experiment 88

4.3.4 Dark counts origin and behavior 91

4.4 Performance of QKD systems with up-conversion detectors 98

4.5 Summary 103

5 Implementation of a 1 GHz differential phase shift QKD system 105

5.1 Introduction 105

5.2 Experimental setup 107

5.3 Experimental results 112

5.3.1 Results for restricted attacks security analysis 112

5.3.2 Results for individual attacks security analysis 117

5.4 Experimental results with low-jitter detectors 121

5.5 Summary 128

6 Implementation of a 10 GHz differential phase shift QKD system 130

6.1 Introduction 130

6.2 Experimental setup 131

6.3 Experimental results 136

6.4 Summary 138

7 Photon-counting optical time domain reflectometry 141

7.1 Introduction 141

7.2 Measurement time calculation 143

7.3 Experimental setup 145

7.4 Experimental results 147

7.5 Summary 149

8 Conclusion 151

References 155

List of Tables

2.1 Benchmark performance of a bidirectional error correction algorithm. 29

4.1 Comparison of InGaAs/InP and Si APD detector characteristics. . . . 79

4.2 Definitions of the dark count quantities for the up-conversion detector and the InGaAs/InP APD. 96

5.1 Summary of fiber transmission experimental conditions and results for the restricted attacks security analysis case. 114

5.2 Summary of fiber transmission experimental conditions and results for the general individual attacks security analysis case. 118

5.3 Summary of fiber transmission experimental conditions and results for the general individual attacks security analysis case and low-jitter up-conversion detectors. 125

6.1 Summary of fiber transmission experimental conditions and results for the 10 GHz DPS-QKD system with low-jitter up-conversion detectors. 137

List of Figures

2.1 Schematic of system for unconditionally secure cryptography. 8

2.2 The Bloch sphere. 10

2.3 (a) Spatial mode, (b) polarization mode, and (c) time slot implementation of a photonic qubit. BS, beamsplitter; DET, detector; HWP, half-wave plate; QWP, quarter-wave plate; PBS, polarizing beamsplitter. 12

2.4 Schematic of a general quantum key distribution algorithm. 22

2.5 (a) Individual, (b) collective, and (c) coherent eavesdropping attacks considered in security proofs for the case of a single qubit quantum key distribution system. 27

2.6 Quantum key distribution system for the implementation of the BB84 protocol. BS, beamsplitter; PBSs, polarizing beamsplitters. 31

2.7 Illustration of the intercept and resend eavesdropping attack in BB84. 32

2.8 Illustration of the general individual eavesdropping attack. 33

2.9 Illustration of the photon number splitting eavesdropping attack. . . . 34

2.10 Secure key generation rate as a function of fiber length for the standard BB84 protocol employing a Poisson or an ideal single-photon source. . 39

2.11 Secure key generation rate as a function of fiber length for the standard BB84 protocol employing a Poisson or an ideal single-photon source, and the vacuum + weak decoy state BB84 protocol. 42

2.12 Comparison of the BB84 and the BBM92 protocols using both ideal and practical sources. 47

3.1 Quantum key distribution system for the implementation of the B92 protocol. PM, phase modulator; UBS, unbalanced beamsplitter; DET, detector. 50

3.2 Quantum key distribution system for the implementation of the DPS-QKD protocol. PM, phase modulator; ATT, attenuator; BS, beamsplitter; DET, detector. 52

3.3 Illustration of the beamsplitter eavesdropping attack in DPS-QKD. . 55

3.4 Illustration of the intercept and resend eavesdropping attack in DPS-QKD. 57

3.5 Secure key generation rate as a function of fiber length for the standard and decoy state BB84 protocol, and the DPS-QKD protocol. 60

3.6 Secure key generation rate as a function of fiber length for the DPS-QKD protocol employing time delay parameters N = 1 or 10 when Eve is equipped with an ideal quantum memory and N = 1, 10 or, 100 when she is not. 63

3.7 Comparison of restricted and general individual attacks in DPS-QKD. 69

3.8 Illustration of the sequential eavesdropping attack in DPS-QKD. . . . 71

3.9 Comparison of sequential and general individual attacks in DPS-QKD. 72

4.1 Comparison of (a) gated and (b) nongated mode operation of single-photon detectors. 77

4.2 Elements of the up-conversion single-photon detector: (a) Basic schematic of the detector; (b) Sum frequency generation nonlinear process; (c) Poling of a lithium niobate crystal; (d) Effective interaction length in a bulk crystal and a waveguide. 80

4.3 Theoretical prediction for the signal conversion and depletion efficiency as a function of the normalized pump power. 82

4.4 Theoretical prediction for the signal conversion efficiency, or else the internal quantum efficiency of the waveguide device, as a function of the normalized pump power. 82

4.5 Experimental setup for single-photon detection at 1.55 μm. VATT, variable attenuator; PC, polarization controller; WDM, wavelength division multiplexer; MO, microscope objective; LPF, long-pass filter; BS, beamsplitter; OSA, optical spectrum analyzer. 85

4.6 Quantum efficiency of the 1.55 μm up-conversion single-photon detector as a function of pump power. The expression for the fitting curve is given by Eq. (4.11). 87

4.7 Dark count rate of the 1.55 μm up-conversion single-photon detector as a function of pump power. The expression for the fitting curve is given by Eq. (4.12). 87

4.8 Experimental setup for single-photon detection at 1.32 μm. VATT, variable attenuator; PC, polarization controller; BPF, band-pass filter; EDFA, erbium-doped fiber amplifier; WDM, wavelength division multiplexer; MO, microscope objective; SPF, short-pass filter; BS, beamsplitter; OSA, optical spectrum analyzer. 88

4.9 Quantum efficiency of the 1.32 μm up-conversion single-photon detector as a function of pump power. The expression for the fitting curve is given by Eq. (4.13). 89

4.10 Dark count rate of the 1.32 μm up-conversion single-photon detector as a function of pump power. The expression for the fitting curve is given by Eq. (4.14). 89

4.11 Spectrum of the SHG of the pump. 92

4.12 Spectrum of the pump diodes. 92

4.13 Spectra of the spurious and SFG output peaks. 93

4.14 Schematic of the (a) Stokes and (b) anti-Stokes spontaneous Raman scattering nonlinear processes. 94

4.15 Ideal communication system employing an up-conversion single-photon detector. 96

4.16 Dark counts per time window for the up-conversion single-photon detector operating at the minimum NEP regime, and a typical InGaAs/InP APD respectively, in an ideal communication system. 97

4.17 Secure key generation rate as a function of fiber length for the standard and decoy state BB84 protocol. 99

4.18 Secure key generation rate as a function of fiber length for the BBM92 protocol employing an ideal or a practical entangled-photon source. . 100

4.19 Secure key generation rate as a function of fiber length for the DPS-QKD protocol for general individual attacks and restricted attacks with time delay parameter $N = 1$ when Eve is equipped with an ideal quantum memory and $N = 10$ when she is not. 101

4.20 Comparison of the performance of QKD systems implementing the BB84, BBM92 and DPS-QKD protocols. In all cases it is assumed that Eve is equipped with an ideal quantum memory and that an optimized up-conversion single-photon detector is used. For the DPS-QKD protocols security against general individual attacks is assumed. . . . 103

5.1 Experimental setup for the 1 GHz DPS-QKD system. PC, polarization controller; IM, intensity modulator; PM, phase modulator; VATT, variable attenuator; PPG, pulse pattern generator; DG, data generator. 108

5.2 Quantum efficiency of the up-conversion single-photon detector as a function of pump power. 110

5.3 Dark count rate of the up-conversion single-photon detector as a function of pump power. 110

5.4 Histograms of the received signal at (a) DET1 and (b) DET2 for a fixed phase modulation pattern. 112

5.5 Secure and sifted key generation rate as a function of fiber length for 3 cases. (a) The dashed and solid curves are theoretical predictions for the sifted and secure rate, respectively, when $\eta = 8.8\%$ and $d = 7.8 \times 10^{-6}$, and security against restricted attacks is taken into account. The clear diamonds and squares are the experimental fiber transmission data for the sifted and secure key generation rate under these conditions. The clear stars and circles are the data taken with attenuation used to simulate additional fiber loss. (b) The dashed and solid curves are the theoretically predicted sifted and secure rate, when $\eta = 2\%$ and $d = 2.7 \times 10^{-7}$. The filled diamonds and squares are the experimental fiber transmission data under these conditions. The filled stars and circles are the simulated attenuation data. A baseline system error rate of 3% is assumed in all theoretical calculations. The effective quantum efficiency factor is 0.67 for (a) and 0.4 for (b). (c) The dash-dot curve is the theoretical prediction and the filled triangles the experimental results for the best experiment employing the BB84 protocol with Poisson light and InGaAs/InP APDs. 115

5.6 Theoretical prediction and experimental results for the bit error rate as a function of fiber length, when $\eta = 2\%$ and $d = 2.7\times10^{-7}$. The squares and circles correspond to fiber transmission and simulated attenuation experiments, respectively. 117

5.7 Secure and sifted key generation rate as a function of fiber length for 3 cases. (a) The dashed and solid curves are theoretical predictions for the sifted and secure rate, respectively, when $\eta = 8.8\%$ and $d = 7.8 \times 10^{-6}$, and security against general individual attacks is taken into account. The clear diamond and square are the experimental fiber transmission data for the sifted and secure key generation rate under these conditions. (b) The dashed and solid curves are the theoretically predicted sifted and secure rate, when $\eta = 2\%$ and $d = 2.7 \times 10^{-7}$. The filled diamond and square are the experimental fiber transmission data under these conditions. For the theoretical calculations we have made the same assumptions as in the case of restricted attacks. (c) The dash-dot curve is the theoretical prediction and the filled triangles the experimental results for the best experiment employing the BB84 protocol with Poisson light and InGaAs/InP APDs. 120

5.8 Typical detection signal from the up-conversion single-photon detector with a low-jitter Si APD when 66 ps pulses are used. This curve corresponds to DET2 and a count rate of 10^5 counts/s. 122

5.9 Timing jitter as a function of count rate for the low-jitter up-conversion detectors when 66 ps pulses are used. 123

5.10 Quantum efficiency of the low-jitter up-conversion single-photon detector as a function of pump power. 124

5.11 Dark count rate of the low-jitter up-conversion single-photon detector as a function of pump power. 124

5.12 Secure and sifted key generation rate as a function of fiber length for 2 cases. (a) The dashed and solid curves are theoretical predictions for the sifted and secure rate, respectively, when $\eta = 6\%$ and $d = 1.95 \times 10^{-5}$, and security against general individual attacks is taken into account. The clear diamond and square are the experimental fiber transmission data for the sifted and secure key generation rate under these conditions. The clear stars and circles are the data taken with attenuation used to simulate additional fiber loss. (b) The dashed and solid curves are the theoretically predicted sifted and secure rate, when $\eta = 0.4\%$ and $d = 3.5 \times 10^{-8}$. The filled diamonds and squares are the experimental fiber transmission data under these conditions. The filled stars and circles are the simulated attenuation data. A baseline system error rate of 1.2% is assumed in all theoretical calculations. The effective quantum efficiency factor is 0.6 for (a) and 0.46 for (b). 127

5.13 Theoretical prediction and experimental results for the bit error rate as a function of fiber length, when $\eta = 0.4\%$ and $d = 3.5 \times 10^{-8}$. The squares and circles correspond to fiber transmission and simulated attenuation experiments, respectively. 128

6.1 Experimental setup for the 10 GHz DPS-QKD system. PC, polarization controller; PM, phase modulator; VATT, variable attenuator; PPG, pulse pattern generator. 132

6.2 Optical pulse train generated from the 10 GHz mode-locked laser. . . 133

6.3 Histogram of the received signal at DET2 for a fixed phase modulation pattern. 134

6.4 Typical detection signal from the up-conversion single-photon detector with a low-jitter Si APD when 10 ps pulses are used. This curve corresponds to DET2 and a count rate of 3×10^5 counts/s. 135

6.5 Timing jitter as a function of count rate for the low-jitter up-conversion detectors when 10 ps pulses are used. 136

6.6 Experimental results for the bit error rate as a function of measurement time window width for the 105 km experiment. 139

6.7 Experimental results for the sifted key generation rate as a function of measurement time window width for the 105 km experiment. 139

7.1 Experimental setup for the 1.55 μm pc-OTDR measurement. IM, intensity modulator; PC, polarization controller; PBS, polarizing beam splitter; HWP, half-wave plate; VATT, variable attenuator; DSF, dispersion-shifted fiber; SMF, single-mode fiber; PPG, pulse pattern generator. . 146

7.2 NEP of the up-conversion single-photon detector as a function of the pump power. The solid curve is derived from the fitting curves of the quantum efficiency and dark counts experimental data. 147

7.3 pc-OTDR measurement result for the link of 11 km, 13 km and 12 m fibers. R is the backscattered signal power normalized by its value at the splice point. 148

7.4 Time interval analyzer data for the 12 m fiber, indicating the 1 m spatial resolution of the pc-OTDR system. 149

Chapter 1

Introduction

The theory of quantum mechanics has profoundly changed our vision and understanding of the physical world that surrounds us. This theory predicts effects that cannot be explained by classical mechanics, and may even run counter to our intuition of physical phenomena. For example, aspects of quantum mechanics such as quantum uncertainty and nonlocal correlations, are extremely difficult to comprehend and have had a radical impact on our conceptual view of the world. However, despite its surprising predictions, the results of numerous elaborate experiments over the last decades have shown that quantum mechanics accurately models physical reality, leaving little doubt about its validity.

Although the quantum mechanical effects were thought provoking, it was thought for many years that they did not have practical applications as they could only be observed in very controlled physical environments. Intense research efforts, however, revealed that the properties of quantum mechanical systems can be harnessed to perform computationally significant tasks. This observation led to the emergence of a new field of research, namely quantum information processing, which investigates the technological applications of quantum mechanics. This research area has attracted a lot of attention both from researchers and the general public due to the promise it holds for faster, better, and more secure future communications. Two very important fields of quantum information processing are quantum computation and quantum cryptography, which we discuss below.

In complex quantum mechanical systems, the information is encoded in the nonlocal correlations between different parts of the system. These correlations have no classical analogue. Quantum information theory, which studies the properties of these correlations between coupled quantum systems, has revolutionized the field of computation, revealing that quantum technology can support entirely news modes of computation. Indeed, quantum computational algorithms have been invented that utilize these properties to achieve exponential speedup of computational tasks, such as prime factorization [1] and database search [2].

In order to implement a quantum computer, a quantum system that serves as the building block for more complex systems is required. This system is referred to as the quantum bit, or qubit. Ideally, a qubit should be easily decoupled from its environment to exhibit quantum properties, but at the same time it should interact with other qubits in a controlled way. The task of achieving a precise and strong control over a system that maintains its quantum nature has proven to be an enormous experimental challenge. This task becomes even harder when decoherence, that is the degradation of quantum information due to the interaction of the system with its environment, becomes significant and prohibits the scaling of the system to larger dimensions. Since the power of quantum computing stems from its scaling properties, a useful quantum technology must be scalable, which imposes even more stringent restrictions on the possible candidates for qubit systems.

Proposals for quantum computation schemes most often use trapped ions [3], atoms in cavities [4], or nuclear spins [5] as qubit systems. Photons, which are a particularly attractive candidate system because they exhibit strong quantum mechanical effects and are very robust to environmental noise, were also shown to be useful for quantum computation when they are combined with linear optics and single-photon detectors [6]. Despite the enormous progress in experimental efforts toward the realization of a quantum computer, however, only simple computational tasks have been performed [7, 8], and a scalable quantum computer capable of performing large computations is beyond reach in the foreseeable future.

The second important field of quantum information processing, quantum cryptography, utilizes quantum properties such as quantum uncertainty, and is some cases nonlocal correlations, to perform unconditionally secure communication. The task of implementing a quantum cryptography system is inherently easier than implementing a quantum computation system. Indeed, quantum cryptography only requires manipulation of simple quantum systems, and, most importantly, qubits only need to be isolated from the environment but not to interact with each other. Consequently, quantum cryptography is today the most advanced field in the area of quantum information processing.

Due to their resilience to environmental noise both in free space and in optical fibers, the photons are the exclusive carriers of information in quantum cryptography. Since the first proposal to use the quantum properties of light to ensure the unconditional security of the transmission of a secret message between two parties by Bennett and Brassard in 1984 [9], and the first demonstration of a quantum cryptography system in 1992, where information was transmitted over 32 cm of free space [10], the field has seen an unprecedented progress. The research efforts during these years have focused both on theoretical and experimental aspects of quantum cryptography.

On the theoretical side, following the quantum cryptography algorithm proposed by Bennett and Brassard, which is called the BB84 protocol, many more protocols were suggested, utilizing different aspects of the theory of quantum mechanics and encoding of the quantum information in various properties of the photons. The need to prove the security of these protocols for practical applications led to a new field in quantum information theory, which has the difficult task of investigating the security requirements of a certain protocol and rigorously proving that it can withstand the most sophisticated attacks allowed by quantum mechanics launched by a potential malevolent eavesdropper. Because of the difficulty of this task, although security of some protocols has been conclusively established, the proof of security of many others remains elusive. This theoretical field has solidified our understanding of quantum cryptography, and in particular of the fundamental concepts of quantum measurement and nonlocality that are required for quantum cryptography. It has also revealed what are the main limiting factors that practical components needed in most protocols, such as single-photon sources and single-photon detectors, impose on quantum cryptography systems and how these affect their performance. For example, we know that nonclassical light generated from a single-photon source is much more suitable for secure communication than classical light generated from a laser source when the BB84 protocol is implemented. However, the engineering of single-photon sources is a hard experimental task, thus an interesting challenge in the field of theoretical quantum cryptography is to invent and prove the security of quantum cryptography protocols that can provide unconditional security using more practical resources.

On the experimental side, the development of better components and the use of more sophisticated techniques, often borrowed from the very advanced field of classical optical communications, has led to a rapid progress in both the speed and the communication distance of quantum cryptography systems. Today, quantum cryptography prototypes are commercially available, quantum cryptography experiments have been performed outside the research laboratory, over installed optical fibers, and efforts toward performing earth to satellite quantum cryptography are underway. Despite these advancements, however, the communication distance of quantum cryptography has been limited to only a few tens of kilometers and the communication speed remains very low, preventing the integration of these systems into current telecommunication networks. Therefore, a very important challenge in the field of experimental cryptography is to invent ways of extending the distance and increasing the speed of quantum cryptography systems, in order to develop practical and implementable systems.

This thesis work concentrates on the field of quantum cryptography, and addresses both of the theoretical and experimental challenges that were previously discussed. The main goal is to achieve a practical and efficient quantum cryptography system that will enable high speed and long-distance secure quantum communication, and will open the way to real-world applications of quantum information processing. Although the focus of this work is quantum cryptography, the concepts and tools developed can be used to enable and enhance the interface between quantum theory and telecommunication technology in other fields of quantum information processing developing in parallel, such as quantum computation.

Chapter 2 provides all the background information required to comprehend the concept of quantum cryptography as a means for two parties to share an unconditionally secure secret message. It discusses the encoding of quantum information in photonic qubits, and shows that the unique properties of quantum mechanics and the results of classical and quantum information theory can be used to perform a quantum cryptography algorithm. We present the most well-known of these algorithms, we discuss their security, and we compare the performance of quantum cryptography systems implementing these protocols with practical components. The concepts and analysis presented in this chapter will be useful for the rest of the thesis.

Chapter 3 introduces a new quantum cryptography protocol, the differential phase shift protocol, which requires a very simple system architecture and only standard telecommunication components, such as lasers, detectors, and linear optics. We prove the security of this protocol against several types of eavesdropping attacks. The security proof reveals that the differential phase shift protocol is robust to powerful eavesdropping attacks, a characteristic that significantly enhances the performance of a quantum cryptography system implementing this protocol in terms of both communication speed and distance. It therefore has a great potential for enabling the implementation of a practical quantum cryptography system.

Chapter 4 studies the main characteristics of single-photon detectors that are commonly implemented in quantum cryptography systems and play a very important role in their performance. It presents the experimental demonstration of a new single-photon detector, the up-conversion single-photon detector, which provides increased speed and efficiency at telecommunication wavelengths compared to current detectors. This detector is based on frequency conversion in a periodically poled lithium niobate waveguide, and a silicon avalanche photodiode. Numerical calculations in this chapter demonstrate that the use of the up-conversion detector can considerably enhance the performance of a quantum cryptography system.

Chapter 5 presents the experimental realization of a quantum cryptography system that implements the differential phase shift protocol with up-conversion single-photon detectors and operates at a repetition rate of 1 GHz. Due to the good characteristics of the two key elements of the system, the protocol and the detectors, we can achieve communication at a practical rate of 1 Mbit/s over 20 km, and transmission of secure information over 75 km of optical fiber, when the security analysis against the most general eavesdropping attacks is taken into account. Furthermore, by using newly developed silicon avalanche photodiodes with improved characteristics, we demonstrate a simple and practical quantum cryptography system capable of achieving communication at a rate of 2 Mbits/s over 10 km, and transmitting secure messages over 100 km of optical fiber. Compared to the best experiments reported to date, these results constitute an improvement of more than two orders of magnitude in communication speed and a factor of two in communication distance.

Chapter 6 presents the experimental realization of a quantum cryptography system that implements the differential phase shift protocol with up-conversion single-photon detectors and operates at a repetition rate of 10 GHz. We show that this system imposes very strict requirements on the characteristics of the single-photon detectors, and thus reaches the limits of today's technological capabilities. Even the best detectors currently available cannot guarantee the secure transmission of information with this system. We explain the limiting factors demonstrated by the experimental results and we discuss possible solutions.

Finally, chapter 7 diverges from the main topic of this thesis, and discusses a classical application of the up-conversion single-photon detector, namely photon-counting optical time domain reflectometry. It explains how this application can benefit from the characteristics of the detector and presents the experimental realization of a photon-counting optical time domain reflectometry system with the up-conversion detector. This system has a very simple control system and achieves a good trade-off between spatial resolution and dynamic range.

Chapter 2

Theory of quantum cryptography

2.1 Introduction

The problem of transmitting securely secret messages between two parties is a very old one. Human imagination has come up with clever ways of overcoming the difficulties associated with this problem, in particular preventing a malevolent eavesdropper from obtaining information about the secret message exchanged over the communication channel.

In today's communications, cryptographic systems are based on codes that ensure computational security. This means that we are mainly concerned with the computational difficulty required to break the code, that is a cryptographic system is secure if it requires the eavesdropper to perform a computationally intractable task in order to break the code. An intractable algorithm is one which scales exponentially in execution time as the size of the problem increases. For example, the factoring problem, i.e., the problem of finding the prime factors of a large composite integer, is generally believed to be intractable and is the basis of the RSA public key cryptography system. The main hurdle of computational security is contained in the phrase 'generally believed' in the previous sentence: it is extremely hard to prove that a mathematical problem is intractable. We need to prove that, even in principle, no algorithm exists that can find a solution. Since this is nearly impossible we often consider the best currently available algorithms for computational security. Thus, if

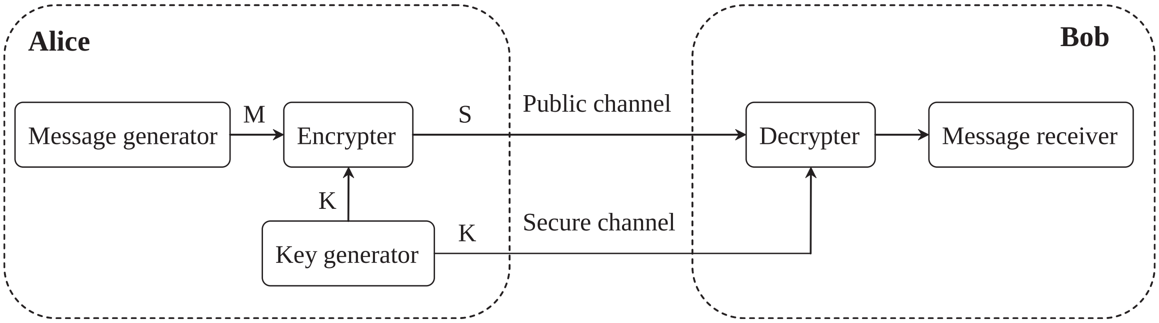

Figure 2.1: Schematic of system for unconditionally secure cryptography.

a new algorithm is discovered that can efficiently break the code all communication over the cryptographic system becomes insecure. The same would be true if a quantum factoring machine, capable of executing Shor's algorithm to efficiently solve the prime factorization problem [1], was developed.

As technology is rapidly advancing, there is a pressing need for a system that can provide unconditional security and not just computational security. A cryptographic system is unconditionally secure when an eavesdropper, often referred to as Eve, cannot obtain enough information from the encrypted message to reconstruct the original message, even if she has infinite computational and time resources. Fig. 2.1 shows the basic model for unconditionally secure cryptography. The sender of the message, referred to as Alice, wants to communicate with the receiver, referred to as Bob, over a public channel that can be potentially eavesdropped. To ensure secrecy of the communication, Alice will also generate a random string of bits, the secret key K, which she uses to encrypt the message M. This generates the encrypted message S, the cryptogram, which is sent over the public channel. Alice must also send a copy of the secret key to Bob, so that he can decrypt the cryptogram. In classical cryptography the exchange of the secret key is only possible using a channel that cannot be eavesdropped or a trusted courier.

One algorithm that provides unconditional security is the Vernam cipher. According to this algorithm, the key has to be as long as the message and the cryptogram is formed by taking the bitwise exclusive (XOR) of each bit of the key with each bit of the message. The key has to be discarded after each transmission, since by reusing it Eve can obtain information about the secret message. This is the reason why the Vernam cipher is often referred to as the one-time pad. The problem of exchanging a secret key, i.e., the key distribution problem, is the reason why this algorithm has not been used in cryptographic systems, especially considering the overhead of a trusted courier needed for the exchange of a new key after each transmission. The advent of quantum cryptography, however, gave a solution to the key distribution problem. The quantum key distribution (QKD) algorithms allow the exchange of secret keys between Alice and Bob without the need of a trusted courier. Security is guaranteed by the laws of quantum mechanics, ensuring that the key can be used afterwards to encrypt and decrypt messages as a one-time pad for unconditionally secure cryptography.

In the following sections, we will first make an introduction to the principles of encoding quantum information, we will then describe the basic elements of a quantum key distribution algorithm, and finally we will discuss the security of the two most well-known QKD protocols and compare their performance.

2.2 Encoding quantum information

2.2.1 The photonic qubit

In quantum communication, information is encoded in quantum bits, which are the quantum mechanical analog of the classical bits used in classical communication. Quantum bits, or qubits, are two-state systems. The two states representing binary 0 and 1 are used to encode information in the same way as classical bits. Qubits have the additional unique property that they can be placed in a superposition state, and can exhibit quantum mechanical coherence properties. Because of this, although all classical information protocols can be implemented with qubits, there are quantum information protocols which cannot be implemented using classical bits. One example is quantum cryptography, which is a method of sharing unconditionally secure secret keys as we discussed in the previous section.

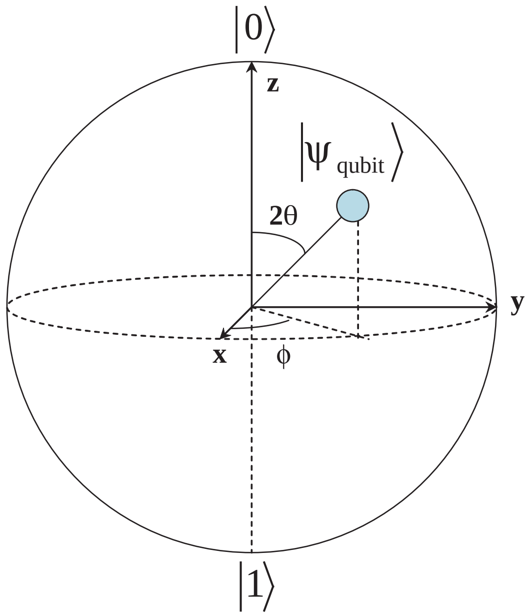

Figure 2.2: The Bloch sphere.

A qubit is a two dimensional quantum system, which means that its Hilbert space is spanned by two basis states. The two orthogonal states of the system, denoted as $|0\rangle$ and $|1\rangle$, form a complete basis for the Hilbert space of the qubit. This basis is referred to as the computational basis. Any other basis can be expressed by linear combinations of the computational basis. All states of the qubit can be expressed in the computational basis as:

$$|\psi_{\text{qubit}}\rangle = \cos\theta\,|0\rangle + e^{i\phi}\sin\theta\,|1\rangle \tag{2.1}$$

The angles θ and ϕ are two independent degrees of freedom and they define a point on the unit sphere in a three dimensional space. Thus, we can visualize the state of a qubit as a vector pointing from the origin to the unit sphere, as shown in Fig. 2.2. This sphere is referred to as the Bloch sphere.

In order for a qubit to be useful, we must be able to perform three fundamental operations on it: prepare it in a well defined state, apply controlled unitary operations on it, and be able to measure it. Physical systems that are suitable as qubits in quantum information and quantum computation applications are primarily atoms, nuclei and photons. One additional requirement especially important for quantum communication is the ability to exchange qubits over long distances. For such applications the photon is the only practical information carrier because it is extremely robust to environmental noise and can be transmitted over long distances in optical fibers. Below we discuss the qubit requirements for the photonic qubit, which interests us in this work.

State preparation: There are several ways to implement a qubit using a single photon. The spatial mode, polarization mode and time slot implementations are illustrated in Fig. 2.3(a)-(c). In the first case, the single photon in mode 1 is split into two spatially separated modes 2 and 3 using a beamsplitter and a phase shifter, hence:

$$|1\rangle_1 \rightarrow |\psi_{\mathrm{qubit}}\rangle = \cos\theta\,|1\rangle_2\,|0\rangle_3 + e^{i\phi}\sin\theta\,|0\rangle_2\,|1\rangle_3 \tag{2.2}$$

Thus, binary information can be encoded in the presence of the photon in one of the modes:

$$\begin{aligned} |0\rangle &= |1\rangle_2\,|0\rangle_3 \\ |1\rangle &= |0\rangle_2\,|1\rangle_3 \end{aligned} \tag{2.3}$$

By properly selecting the beamsplitter ratio and phase shift any qubit state can be prepared. An alternative way to implement a qubit is using the polarization, as shown in Fig. 2.3(b). This is fundamentally equivalent to the first method except that the two spatial modes are replaced by the two polarization states of a single spatial mode. In this case, binary information is encoded in the horizontal or vertical polarization of the single photon:

$$\begin{aligned} |0\rangle &= |H\rangle \\ |1\rangle &= |V\rangle \end{aligned} \tag{2.4}$$

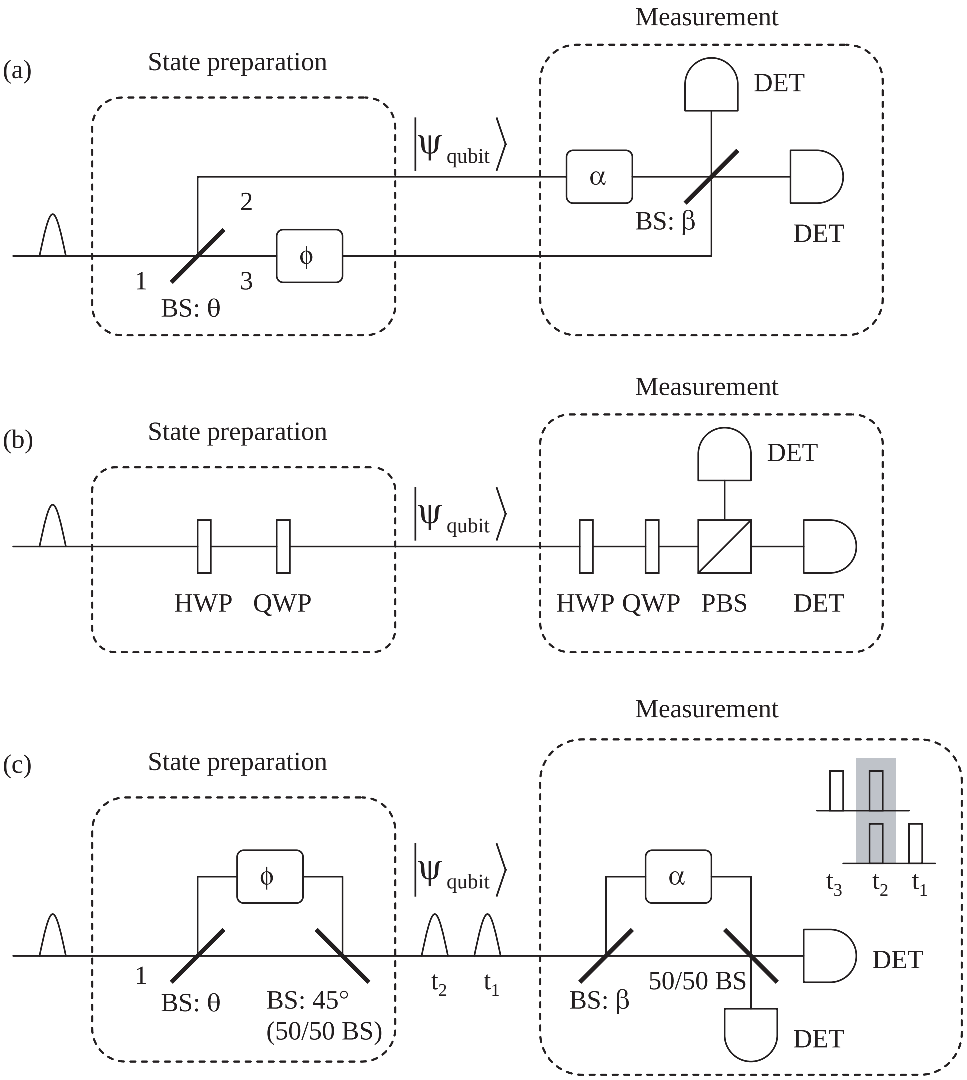

Figure 2.3: (a) Spatial mode, (b) polarization mode, and (c) time slot implementation of a photonic qubit. BS, beamsplitter; DET, detector; HWP, half-wave plate; QWP, quarter-wave plate; PBS, polarizing beamsplitter.

Any qubit state can be prepared by appropriately using a quarter-wave and a half-wave plate. Both implementations are not well suited for long-distance fiber-optic quantum communication systems because they are very sensitive to polarization drifts and phase instability in long optical fibers. A very practical implementation for such systems utilizes time bin encoding [11], and is shown in Fig. 2.3(c). A single photon in mode 1, which defines a transform-limited wavepacket in space and time, is sent through an unbalanced interferometer, which has a short and a long arm. The long arm introduces a delay relative to the short arm, which is greater than the coherence length of the input photon. Thus, the output of the interferometer is two pulses separated in time. Assuming this time separation is sufficiently long so that the two time slots can be treated as orthogonal modes, we can define the modes corresponding to time slots t_1 and t_2. We can then write the qubit state after the unbalanced interferometer as:

$$|\psi_{\text{qubit}}\rangle = \cos\theta\,|\text{t}_1\rangle + e^{i\phi}\sin\theta\,|\text{t}_2\rangle \tag{2.5}$$

The information in this case is encoded in the relative phase of the two time slots. This information remains undisturbed during propagation in an optical fiber because the time separation of the two pulses is usually very short, on the order of a nanosecond, while the phase and polarization drifts occur at long time scales, so the pulses undergo exactly the same distortion in the fiber. This fact makes time slot implementation advantageous for long-distance quantum communication.

Unitary operations: To manipulate quantum information we must be able to perform controlled unitary evolution, which means that we should be able to transform the qubit from its initial state to any other state on the Bloch sphere. This transformation must conserve probability, hence it must be described by unitary operators, which can be thought of as rotations or combinations of rotations on the Bloch sphere. Performing unitary evolution is particularly easy in the case of the photonic qubit because standard optical components such as beamsplitters, quarter-wave plates, half-wave plates, and phase shifters are sufficient to apply all required operations.

Measurement: The ability to observe the qubit and determine its state is essential in any quantum information application. Quantum measurement is a particularly subtle theory, where the differences between classical bits and qubits become strongly pronounced. When a classical bit is observed, it is found to be either 0 or 1, the answer is unambiguous. In contrast, a quantum bit will not give an unambiguous answer unless the basis in which it was prepared is known. More formally, the theory of quantum measurement is described by the following postulates [12]:

- Postulate 1: The wavefunction of a quantum particle is represented by a vector in a normalized Hilbert space which is spanned by an orthonormal basis $|0\rangle$, $|1\rangle$,..., $|n-1\rangle$, where n is the dimensionality of the Hilbert space. Every measurement is represented by a projection onto a complete orthonormal basis which spans the Hilbert space. Define this basis as $|P_0\rangle$, $|P_1\rangle$,..., $|P_{n-1}\rangle$. The probability of measuring the qubit in the state $|P_i\rangle$ is simply given by $|\langle P_i|\psi\rangle|^2$, where $|\psi\rangle$ is the wavefunction of the qubit.

- Postulate 2: Define the wavefunction of a quantum system before a measurement as $|\psi\rangle$. Define the measurement basis as $|P_0\rangle$,..., $|P_{n-1}\rangle$. Given that the system was measured in the state $|P_i\rangle$, the wavefunction of the system after the measurement is also $|P_i\rangle$.

The first postulate states that if the qubit is prepared in one of the states $|P_i\rangle$, the measurement will identify this state with 100% probability. If, however, the state qubit is prepared in a superposition state of the measurement basis, the measurement result will be ambiguous. A qubit repeatedly prepared in the same state and measured in the same basis will yield a different measurement result from shot to shot. The second postulate, known as the projection postulate, states than unless a quantum system is prepared in one of the eigenstates $|P_i\rangle$, the measurement process will destroy the state of the system. The combination of the two postulates reveals one of the most important aspects of quantum measurement, which is fundamental for quantum cryptography: the wavefunction of a single quantum system cannot be determined unless the preparation basis is known. If the system is measured in the wrong basis, an ambiguous answer will be obtained. Furthermore, due to the projection postulate we cannot go back and measure the state again because it has already been destroyed. In quantum communication, any basis can be used for encoding the information. However, error-free communication can only occur if the sender and the receiver use the same basis to encode and measure the qubit.

In Fig. 2.3(a)-(c) the measurement apparatus for the projective measurement on the qubit system in the case of each of the possible implementations of the photonic qubit is shown. Adjustment of the beamsplitter ratio, phase shift or quarter-wave and half-wave plates allows the measurement of the qubit in any desired basis. The measurement result is indicated by a counting event on the photon detectors at each output port of the beamsplitter in the measurement apparatus. In the time slot implementation, the two pulses interfere with each other at time t_2 on the beamsplitter of the second unbalanced interferometer, thus the measurement result is conditional on a detection at this time slot. The main difficulty in the practical implementation of this system is that it requires two unbalanced interferometers whose relative phase shift needs to be stabilized. We will see solutions to this problem in the context of quantum key distribution in Chapter 5.

To conclude the discussion on quantum measurement, we would like to briefly mention a mathematical tool that is very useful for describing general quantum measurements, the Positive Operator Value Measure (POVM) formalism [13]. A POVM measurement on an n-dimensional Hilbert space has n possible measurement outcomes, and each outcome is associated with an operator on the Hilbert space of the measured quantum system. The operators of a POVM for a quantum system are implemented by embedding the system in a larger Hilbert space and making measurements on the total system. It is important to note that POVMs do not represent any new physics relative to the projective measurements discussed before. They are merely a useful mathematical tool, which allows us to generalize the measurement concept to cases where the external environment has an effect on the system. The formalism can also be extended to describe generalized delayed measurements. Such measurements, which involve attaching a probe state to the system state, applying a unitary evolution to the collective system and finally measuring the probe state to obtain information about the system state, can be a very powerful eavesdropping technique, hence they are of interest for the security analysis of quantum key distribution protocols. Because POVMs are simply a convenient mathematical tool allowing the treatment of the most general quantum measurements, it is often not obvious or intuitive what physical systems can be used to apply these operators.

2.2.2 Single-photon generation

In the previous section we discussed extensively the properties of the photonic qubit. A natural question that arises is how to generate the single photons that implement these qubits. The source of single photons is actually of great importance in quantum cryptography with crucial implications in the performance of the system, as we will see in detail in the following sections. Light sources can be generally categorized into two classes, classical and nonclassical. To rigorously define these two classes, we introduce the coherent state, which is defined as the eigenstate of the annihilation operator a:

$$a\left|\alpha\right\rangle = \alpha\left|\alpha\right\rangle \tag{2.6}$$

In the previous expression, $\alpha = |\alpha|e^{i\phi}$, where $|\alpha|$ and ϕ are the amplitude and phase of the coherent state, respectively. An alternative definition of this state is its representation in the Fock state basis:

$$\left|\alpha\right\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n}} \left|n\right\rangle \tag{2.7}$$

where $\left|n\right\rangle$ is the n photon Fock state. Several important properties follow from this expression, for example that the probability of detecting n photons in the field follows a Poisson distribution:

$$P(n) = e^{-\mu}\frac{\mu^n}{n!} \tag{2.8}$$

where $\mu = \left\langle a^{\dagger}a \right\rangle = |\alpha|^2$ is the average number of photons in the field. The set of coherent states forms a complete basis, that is:

$$\int_{\alpha} \left|\alpha\right\rangle \left\langle\alpha\right| = \boldsymbol{I} \tag{2.9}$$

However, two different coherent states are not orthogonal to each other:

$$\langle \alpha | \beta \rangle = e^{-\frac{1}{2}(|\alpha|^2 + |\beta|^2 - 2\alpha^* \beta)} \neq \delta(\alpha - \beta) \tag{2.10}$$

Thus, coherent states form an overcomplete basis, in which the field emitted by a light source can be diagonally decomposed [14]. This is the premise of the coherent state representation of the field, which takes the following form:

$$\rho_{\text{field}} = \int_{\alpha} P(\alpha) \left| \alpha \right\rangle \left\langle \alpha \right| \tag{2.11}$$

where ρ_{field} is the reduced density matrix of a light field spanning the Fock state basis. The function $P(\alpha)$ is known as the distribution function of the emitted field. This function is always real and obeys the normalization condition:

$$\int_{\alpha} P(\alpha) = 1 \tag{2.12}$$

For many sources, such as lasers and LEDs, this function is non-negative, it therefore satisfies all the properties of a probability distribution. Any source whose P distribution function is a valid probability distribution is referred to as classical source. The reason for this name is that all photon counting statistics exhibited by a classical source do not require quantization of the electromagnetic field. We could instead work with classical field amplitudes and use Maxwell's equations to determine their dynamics. The detection statistics can be attributed to the photon counters, which are made of a collection of atoms with quantized energy levels. This type of description, known as the semiclassical theory of photon counting, is adequate in many cases.

Some sources emit fields whose P distribution function becomes negative. Such sources can exhibit effects that cannot be predicted by the semiclassical detection theory. Examples of these effects include photon anti-bunching, negativity of the Wigner function, and nonclassical effects such as violation of Bell's inequality [14].

These sources are referred to as nonclassical sources, because quantization of the electromagnetic field is required to explain the counting statistics they generate. Nonclassical sources play an important role in many quantum information processing applications.

An ideal single-photon source emits exactly one photon, which is a nonclassical field. It has been shown that such a nonclassical source can significantly improve the security of a quantum cryptography system [15, 16, 17, 18]. The engineering of a single-photon source, however, is an experimentally challenging task and although very promising implementations exist [19, 20, 21], they are not yet practical nor are they ideal, which has important effects on the performance of a quantum cryptography system [22]. This is the reason why most quantum cryptography experiments employ attenuated Poisson sources, such as weak laser light, to simulate a single-photon source [23]. As we will see in Sec. 2.4, these implementations are generally vulnerable to certain types of eavesdropping attacks, which significantly compromise the security of a quantum cryptography system [15, 16]. An important part of this thesis work is to show that practical and secure quantum key distribution is in fact possible using Poisson light sources.

2.2.3 Entangled qubits

So far, we have considered the encoding of quantum information in single qubits, as well as their generation, preparation and transmission over a quantum channel. However, quantum information can also be encoded in entangled qubits. Entanglement is one of the most fascinating aspects of quantum mechanics. Considering a system composed of two qubits, the Hilbert space is described by the product space of each individual qubit. This product space is spanned by four basis states, $|0\rangle|0\rangle$, $|0\rangle|1\rangle$, $|1\rangle|0\rangle$, and $|1\rangle|1\rangle$, which represent the computation basis of the two-qubit system. The system can exist in any complex superposition of these basis states. For example, consider the following state:

$$|\psi_{\text{entangled}}\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle) \tag{2.13}$$

This state cannot be factorized into a product state of the two qubits. Any quantum state that satisfies this property is referred to as an entangled state. Such states have the unique property that even if the individual qubits are separated by great distances we cannot describe their behavior independently. Eq. (2.13) may not initially seem counterintuitive, since it simply expresses the fact that both qubits will take the value 0 with 50% probability, otherwise they will both take the value 1. The interesting properties of this state become apparent when the system is measured in a basis other than the computational basis. Define the notation:

$$\begin{aligned} |0_\theta\rangle &= \cos\theta\,|0\rangle + \sin\theta\,|1\rangle \\ |1_\theta\rangle &= \sin\theta\,|0\rangle - \cos\theta\,|1\rangle \end{aligned} \tag{2.14}$$

This change of basis is performed by a rotation of 2θ across the horizontal equator of the Bloch sphere. It is easy to verify that:

$$|\psi_{\text{entangled}}\rangle = \frac{1}{\sqrt{2}}(|0_\theta\rangle\,|0_\theta\rangle + |1_\theta\rangle\,|1_\theta\rangle) \tag{2.15}$$

The above expression shows that the computation basis is not a preferred basis for the system; there is actually a perfect correlation between the two qubits regardless of which value of θ is chosen.

Suppose that two qubits are prepared in an entangled state. One of the qubits is sent to Alice in the North Pole and the other to Bob in the South Pole. Alice picks an angle θ and measures her qubit in the corresponding basis. Eq. (2.15) then indicates that if Alice's qubit is measured in state $|0_\theta\rangle$, Bob's qubit wavefunction becomes $|0_\theta\rangle$ as well. This seemingly counterintuitive action at a distance lies at the heart of quantum entanglement. If two systems are entangled, then measuring one system will have an instantaneous effect on the wavefunction of the other system.

We may speculate from the above discussion that superluminal communication is possible. For example, consider the protocol where Alice encodes a binary 0 by measuring her photonic qubit in the computation basis ($\theta = 0$). This will prepare Bob's qubit in one of the states $|0_0\rangle$ or $|1_0\rangle$, although Alice cannot control which one of these states is generated. To encode binary 1, Alice measures her photon in the basis defined by $\theta = \pi/2$, thus Bob's qubit is prepared in the state $\left|0_{\pi/2}\right\rangle$ or $\left|1_{\pi/2}\right\rangle$ again with equal probability. To decode Alice's transmission, Bob simply needs to determine if his qubit is in the state $|0_0\rangle$ or $|1_0\rangle$ for binary 0, and $\left|0_{\pi/2}\right\rangle$ or $\left|1_{\pi/2}\right\rangle$ for binary 1. But the measurement Bob must perform is physically impossible because any measurement he performs is described by a projection onto an orthonormal basis. Thus, regardless of which basis he chooses to measure, the measurement is completely unaffected by the basis which Alice measures her qubit in. This means that no communication is possible. Bob's inability to decode Alice's message stems from the fundamental principle discussed in Sec. 2.2.1: the wavefunction of a single quantum system cannot be determined unless the preparation basis is known. Alice can instantaneously modify the wavefunction of Bob's qubit but since the wavefunction is not a physical quantity non-locality cannot be used to perform superluminal communication.

Nonlocal states, however, can lead to measurement results which deviate from the natural concept of local realism. These effects become apparent when the correlations between Alice's and Bob's measurement are considered. Suppose, for example, that Alice measures her qubit in the θ basis, while Bob measures his qubit in the ϕ basis. There are four possible measurement results, 00, 01, 10, and 11, which occur with probabilities:

$$\begin{aligned} P(0,0) = P(1,1) &= \frac{1}{2}\cos^2(\theta - \phi) \\ P(0,1) = P(1,0) &= \frac{1}{2}\sin^2(\theta - \phi) \end{aligned} \tag{2.16}$$

If $\theta = \phi$, Alice and Bob's measurement results have perfect correlation, they will both measure either 0 or 1. If instead $\theta - \phi = \pi/4$, there is no correlation between the measurement results. All measurement combinations are equally likely. This behavior is inconsistent with the concept of local reality. The probabilities described in Eq. (2.16) cannot be reproduced by statistical mixtures of qubits whose states are well defined. Theories that restrict the individual qubit states to be well defined are known as local hidden variable theories. All measurement statistics produced by such theories must satisfy a relationship known as Bell's inequality [24]. The measurement statistics in Eq. (2.16), however, predict that this inequality can be violated, thus this inequality gives us a measurable test of the validity of local hidden variable theories. Violations of Bell's inequality have been conclusively demonstrated under many different experimental conditions and using various types of qubits [25, 26, 27].

Except for their use in fundamental tests of basic physical principles such as Bell's inequality, entangled states are an extremely useful tool in quantum information and quantum computation applications. In particular in quantum cryptography, encoding the quantum information in entangled qubits and verifying the security of the transmission using criteria based on Bell's inequality can improve the performance of a system significantly, as we will see in Sec. 2.5. The generation of entangled qubits, however, is a rather difficult task. Although proposals for creating an ideal entangled-photon source, that is a source that emits exactly one pair of photons per clock cycle, exist [28], no successful implementation has been reported to date. A more practical way of generating entangled photons is to use the spontaneous emission of a non-degenerate parametric amplifier. This technique, known as parametric down-conversion, is extensively used to generate entanglement in polarization as well as other degrees of freedom such as energy and momentum, and is employed as a source in entanglement-based quantum cryptography experiments.

2.3 A general quantum key distribution algorithm

In the previous sections we introduced the concept of quantum cryptography, or more accurately quantum key distribution, and discussed the encoding of quantum information in single or entangled photonic qubits. Let us now show how a quantum key distribution (QKD) algorithm can achieve the goal of securely exchanging a random string of bits, referred to as the key, between the sender and the receiver, by using encoded quantum information in conjunction with the results of classical and quantum information theory. Fig. 2.4 illustrates the general steps that a QKD algorithm has to follow. These are the quantum transmission, sifting, error correction, and privacy amplification steps, and they are discussed in the following sections.

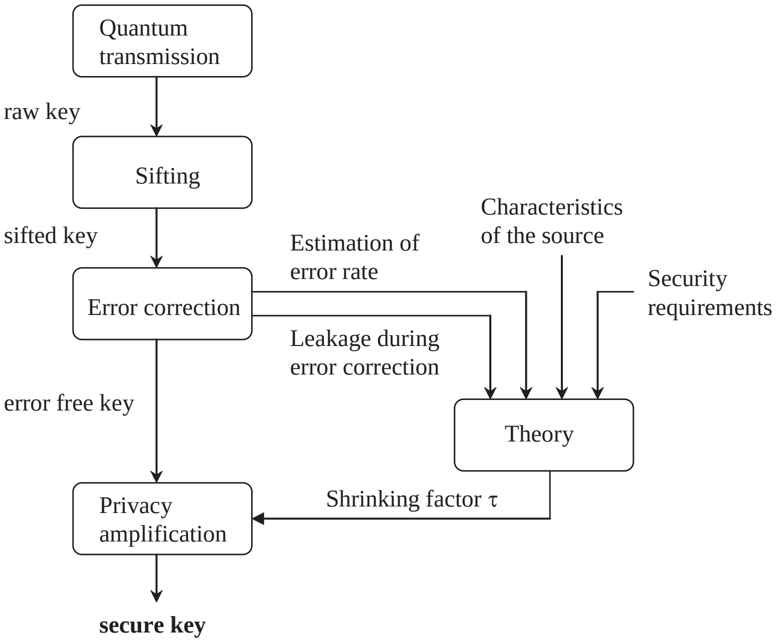

Figure 2.4: Schematic of a general quantum key distribution algorithm.

2.3.1 Quantum transmission

In the quantum transmission step, Alice and Bob share a random string of bits transmitted over a quantum channel. Most quantum key distribution protocols belong to one of two categories, single qubit protocols and entangled qubit protocols.

Single qubit protocols make use of the measurement uncertainty properties discussed in Sec. 2.2.1 to ensure secrecy. Important examples of single qubit protocols are the BB84, B92, Koashi01 and six-state protocols [9, 29, 30, 31]. We are going to focus on the BB84 protocol in Sec. 2.4. In this type of protocol, Alice chooses randomly a basis usually among two nonorthogonal bases as well as the bit value of her single photons and sends them to Bob over a quantum channel. Bob measures each photon also in a randomly chosen basis. This concludes the quantum transmission step.

Entangled qubit protocols use the nonlocal correlations discussed in Sec. 2.2.3 to achieve security. They rely on the fact that if any local variable exists which can predict the state of an entangled qubit pair, then nonlocal correlations are not observed. Important examples of entangled qubit protocols are the Ekert91 and BBM92 protocols [32, 33]. We are going to discuss the BBM92 protocol in more detail in Sec. 2.5. In this type of protocol, in the quantum transmission step, Alice and Bob each receive a photon from an entangled-photon pair and measure its state in a randomly chosen basis.

The outcome of the first step is an ensemble of bits called the raw key. The raw key generation rate R_{raw} is simply equal to the product of the repetition rate of the transmission and the probability of a photodetection event registered by the detectors in the measurement setup.

2.3.2 Sifting

In the sifting step, Alice and Bob use a public channel to communicate information related to their measurement, in particular what basis they used to prepare or measure their qubits and at what times they registered a detection event. They do not disclose the measurement result. From our discussion in Sec. 2.2 it follows that whenever Alice and Bob used the same basis, they should get perfectly correlated bits. The process of discarding the bits in the cases where they used different bases is called sifting. The ensemble of bits remaining after this basis reconciliation forms the sifted key. The sifted key generation rate is given by:

$$R_{\text{sifted}} = sR_{\text{raw}} \tag{2.17}$$

where s is the sifting parameter, that is the fraction of bits for which the bases were the same.

If the are no errors in the quantum cryptography system, then a potential eavesdropper, referred to as Eve, cannot intercept the transmission and make a measurement that will yield information on the quantum state of the system without causing an unavoidable backaction. This will introduce errors in the transmission and will therefore reveal the presence of the eavesdropper. In this case, the sifted key is unconditionally secure. In any practical communication system, however, errors naturally occur due to imperfections in the individual components, such as the transmission line or the detectors. Errors caused by the system cannot be distinguished from errors due to eavesdropping. Thus, in practical systems, the statement that any eavesdropping will unavoidably cause errors and reveal the eavesdropping, is not a sufficient security proof. There is always a baseline system error rate, so we must take into account that some information about the quantum transmission has been leaked. Consequently, we must be able to put a bound on the amount of information leakage given the error rate. Practical QKD systems handle system errors and eavesdropping by complementing raw quantum transmission and sifting with two important additional steps: error correction and privacy amplification. Processing in both of these steps can be performed using a public channel, it does not require the exchange of additional qubits. These steps are described below.

2.3.3 Error correction

The error correction step serves the dual purpose of correcting all erroneously received bits and giving an estimate of the error rate. In particular, Alice reveals some additional information to Bob about her key that will allow him to find and correct all of the error bits. For example, Alice and Bob can group their bits in segments and check the parity of each segment, optimizing the segment size as the error correction process continues. Because this information is sent over a public channel, error correction unavoidably leaks additional information to an eavesdropper. This information leakage has to be as small as possible. The minimum number κ of bits that Alice and Bob have to exchange publicly to correct their strings is given by a central result of classical information theory, Shannon's noiseless coding theorem [34]. In the case we are interested in, where each bit is transmitted incorrectly with an error probability e independently for each bit transmitted, the theorem asserts that:

$$\lim_{n\to\infty}\frac{\kappa}{n} = -e\log_2 e - (1-e)\log_2(1-e) \equiv h(e) \tag{2.18}$$

where n is the length of the sifted key. Unfortunately, Shannon's theorem has a non-constructive proof, which means that we know there exists an error correction scheme disclosing only κ bits but the theorem does not provide an explicit procedure for this scheme. An error correcting algorithm should ideally operate very close to this limit. At the same time the algorithm should be computationally efficient otherwise the execution time may become prohibitively long.

Error correction algorithms can usually be divided into two classes, unidirectional and bidirectional. In a unidirectional algorithm information flows only from Alice to Bob. Alice provides Bob with an additional string which he uses to try to find his errors. This makes it difficult to design algorithms that are both computationally efficient and operate near the Shannon limit [35, 36]. In a bidirectional algorithm information can flow both ways, and Alice can use the feedback from Bob to determine what additional information she should provide him, which makes it easier to approach the Shannon limit. These two error correction algorithms classes can be further subdivided into algorithms that discard errors and algorithms that correct them. Discarding errors is usually done to prevent additional side information from leaking to Eve. By correcting the errors we allow for this additional flow of side information, which can be accounted for during privacy amplification. Since privacy amplification is typically a very efficient process, algorithms which correct the errors tend to perform better.

In subsequent sections, we will estimate the communication rate of QKD systems based on system parameters such as channel loss and detector dark counts. These estimations strongly depend on how well we assume the error correction algorithm works. In the corresponding calculations we will assume the algorithm given in [35], which is bidirectional and corrects the errors. This algorithm works within 15%-35% of the Shannon limit, even with substantial error rates.

2.3.4 Privacy amplification

In order to account for the information leaked in the raw quantum transmission and during error correction, the final step of privacy amplification is performed. In privacy amplification, the error corrected key is compressed into a final secure key that can be made as secure as desired. The amount of compression required depends on how much information may have leaked to the eavesdropper in the previous phases of the transmission.

For a security proof to be useful, it must bound the amount of information leaked during quantum transmission and error correction, and relate it to how much compression must be applied in privacy amplification. The formulation of a complete security proof of this type is a complex subject with several open questions remaining. For the most well studied protocol, the BB84 protocol, the earliest work on the subject considered the simplest type of attacks, called intercept and resend attacks [37, 38]. Later work considered the problem of the generalized delayed measurements discussed in Sec. 2.2.1. There are three categories of generalized attacks that have been considered: individual, collective, and coherent attacks. Figure 2.5 illustrates these attacks for the case a single qubit QKD system. In an individual attack the eavesdropper is restricted to entangling a quantum probe to each qubit independently. The probes are stored in a quantum memory until the measurements bases are announced, and then each probe is measured independently. Any measurement which is not forbidden by quantum mechanics is allowed. For the BB84 protocol, security against this type of attacks has been proven in [36, 39, 40], and these proofs were extended to practical photon sources in [15]. Collective attacks are similar to individual attacks, but Eve is now allowed to make a global generalized measurement on all probes considered as a single quantum system using a quantum computer. This allows her to take advantage of correlations introduced during error correction and privacy amplification by information exchange. Such correlations can potentially refine an eavesdropper's quantum measurement. Security against collective attacks has been shown for BB84 in [41]. The most general type of attack is the coherent attack where the eavesdropper treats the entire quantum transmission as one system, which she entangles with a probe of very large dimensionality in any initial state. Proofs of security for BB84 against this most general scenario exist for an ideal [42] and a practical qubit source [43]. Security proofs against individual, collective or coherent attacks with several kinds of assumptions also exist for the BBM92 protocol [44, 45, 46, 47, 48] and the B92 protocol [49, 50, 51, 52].

In this work, we are interested in practical quantum communication systems. The ability to perform collective or coherent attacks is well beyond today's technological

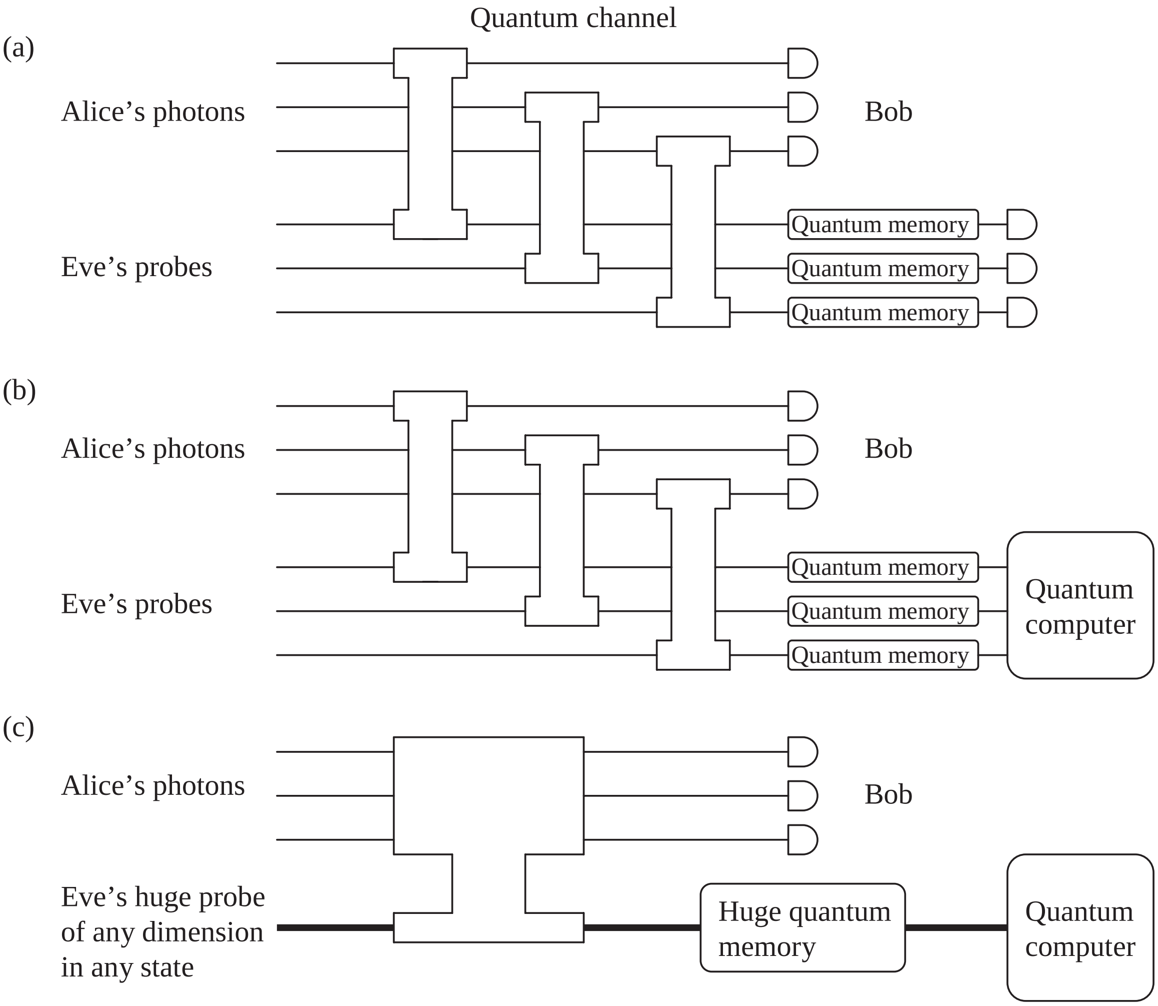

Figure 2.5: (a) Individual, (b) collective, and (c) coherent eavesdropping attacks considered in security proofs for the case of a single qubit quantum key distribution system.

capabilities or even those of the foreseeable future. Since the future technology cannot be used to eavesdrop on today's quantum transmission, we will restrict our discussion in this thesis only to individual attacks. Even these attacks assume very advanced capabilities because Alice and Bob can delay the public bases announcement for an arbitrarily long time, thus Eve is assumed to possess a quantum memory with an infinitely long coherence time, which is not available today. Nevertheless, general individual attacks are close to being realistic so it is very important to prove the security of a quantum key distribution algorithm against these attacks. Thus, in the following, Eve will be restricted to attack individual qubits, and she will not be allowed to perform a coherent attack consisting of collective quantum operations and measurements of many qubits with quantum computers. This not only corresponds to a realistic scenario but it also makes the mathematical treatment of the problems we will consider simpler and more intuitive.

As we mentioned in the beginning of this section, the role of the privacy amplification step is to deduce the shrinking factor τ by which the error corrected key has to be compressed, given the error rate calculated in the error correction step and the bound on the amount of information leaked during the previous phases of the transmission, so that Eve's information about the final key is lower than a specified value. This calculation is performed using the methods of the generalized privacy amplification theory [53], which makes the worst case assumption that all errors are potentially caused by eavesdropping. The result of this theory states that the length of the final key should be set to:

$$r = n\tau - \kappa - t \tag{2.19}$$

where n is the length of the sifted key, κ is the number of bits disclosed during error correction, t is a security parameter, and the shrinking factor τ is given by the expression:

$$\tau = -\frac{\log_2 p_{\mathrm{c}}}{n} \tag{2.20}$$

In the above expression, p_{c} is the average collision probability, an important quantity

Table 2.1: Benchmark performance of a bidirectional error correction algorithm.

e	$f(e)$
0.01	1.16
0.05	1.16
0.1	1.22
0.15	1.35

in the analysis of privacy amplification, which is a measure of Eve's mutual information with Alice and Bob. As we will see in subsequent sections, a security proof for a specific QKD protocol against specific types of attacks finds a bound on p_{c}, and thus determines the shrinking factor τ. This factor is a function of the error rate and the parameters of the quantum cryptography system.

Instead of the length of the final secure key given in Eq. (2.19), it is more useful to calculate the normalized communication rate in units of bits/s. If N is the length of the transmission, then $n = NR_{\text{sifted}} = NsR_{\text{raw}}$, and the communication rate, or else secure key generation rate, is defined as:

$$R = \lim_{N\to\infty} \frac{r}{N} = \lim_{n\to\infty} R_{\text{sifted}} \left(\tau - \frac{\kappa}{n} - \frac{t}{n} \right) \tag{2.21}$$

where Eq. (2.19) was used in the right part of the equation. It can be shown that in the limit of long strings, $t/n = 0$. Furthermore, as we discussed in Sec. 2.3.3, the term κ/n is the fraction of additional information disclosed during error correction. If the error correction algorithm works at the Shannon limit, then Eq. (2.18) is valid. However, an algorithm that is computationally feasible and works at this ideal limit does not exist. All practical algorithms are inefficient to some extent, and this is accounted for by introducing a function $f(e)$, defined as the ratio of the algorithm performance to that of the Shannon limit. Thus,

$$\lim_{n\to\infty} \frac{\kappa}{n} = -f(e)\left[e\log_2 e + (1-e)\log_2(1-e)\right] = f(e)h(e) \tag{2.22}$$

where $f(e) \geq 1$ and $h(e)$ is defined in Eq. (2.18). The function $f(e)$ can be determined by benchmark testing the algorithm under a broad range of strings. In all relevant calculations in this thesis we will assume that the algorithm being used is the bidirectional algorithm proposed in [35]. This algorithm works within 35% of the Shannon limit, even with large error rates. Table 2.1 shows values of $f(e)$ for several different error rates, produced by benchmark tests. These values are linearly interpolated to determine intermediate values of $f(e)$. Putting everything together, the final expression for the secure key generation rate is:

$$R = R_{\text{sifted}} \left\{ \tau + f(e) \left[e \log_2 e + (1-e) \log_2 (1-e) \right] \right\} \tag{2.23}$$

where R_{sifted} and τ depend on the QKD protocol and system parameters.

2.4 The BB84 protocol

2.4.1 The standard BB84 protocol

The previous sections have provided us with all the information necessary to examine a quantum key distribution protocol in more detail. We will start with a protocol that was proposed by Bennett and Brassard in 1984, the BB84 protocol [9]. In this protocol Alice encodes information in single qubits. Although any implementation of the photonic qubit is possible, we will consider in the following discussion the polarization mode implementation illustrated in Fig. 2.3(b). Then, Fig. 2.6 shows a possible way to perform the standard BB84 QKD protocol. In this implementation, Alice uses an electro-optic modulator to encode the information in one of two bases. The first basis is the computational basis, that is Alice uses the states $|0\rangle = |H\rangle$ and $|1\rangle = |V\rangle$ to encode binary 0 and 1, respectively. The second is the basis defined by $\theta = \pi/4$, which is referred to as the diagonal basis and is nonorthogonal to the computational basis. From Eq. (2.14) we see that this means that in this basis Alice uses the states $\left|0_{\pi/4}\right\rangle = \left(|H\rangle + |V\rangle\right)/\sqrt{2}$ and $\left|1_{\pi/4}\right\rangle = \left(|H\rangle - |V\rangle\right)/\sqrt{2}$ to encode binary 0 and 1, respectively. Alice randomly chooses one of the two bases with equal probability for each photon, and then randomly chooses a binary 0 or 1 again with

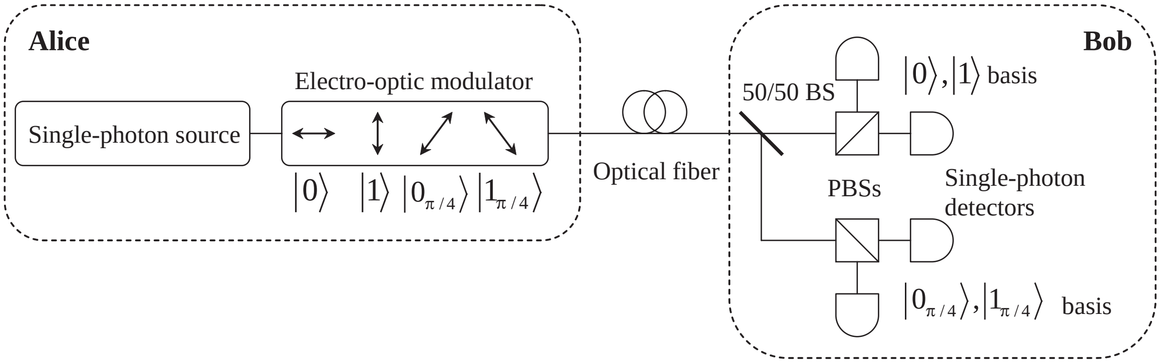
Alice
Electro-optic modulator
Single-photon source
$|0\rangle$ $|1\rangle$ $|0_{\pi/4}\rangle$ $|1_{\pi/4}\rangle$
Optical fiber
Bob
50/50 BS
$|0\rangle,|1\rangle$ basis
PBSs
Single-photon detectors
$|0_{\pi/4}\rangle,|1_{\pi/4}\rangle$ basis

Figure 2.6: Quantum key distribution system for the implementation of the BB84 protocol. BS, beamsplitter; PBSs, polarizing beamsplitters.

equal probability. Thus, she transmits the four possible states $|0\rangle$, $|1\rangle$, $|0_{\pi/4}\rangle$, and $|1_{\pi/4}\rangle$ each with probability 0.25.

Bob receives each qubit and measures it to learn the value of the bit. Because he does not know the preparation basis, he randomly selects one of the computational or diagonal basis with equal probability for each qubit. In the implementation shown in Fig. 2.6, Bob uses a so called passive modulation detection apparatus to randomly select the measurement basis and perform the corresponding measurement in that basis. This setup uses a 50/50 beamsplitter to partition the photons into two different polarization analyzers. An active modulation setup using an electro-optic modulator is also possible but we will consider the passive setup because it is easier to implement and because this setup was assumed in the security analysis of [15], whose results we will use to calculate the communication rate for BB84. When Bob measures in the correct basis, he learns the value of the bit with 100% probability, which means he gets complete information. When he measures in the wrong basis, his result is completely uncorrelated with Alice's transmission, so he obtains no information. After the quantum transmission has concluded, during the sifting process, Alice and Bob reveal the bases they used without disclosing the measurement result and they discard all bits that were measured in the wrong basis. Since Bob chooses the wrong basis with 50% probability, the sifting parameter in this case is $s = 1/2$.

As we discussed in Sec. 2.3.2, if there are no errors in the system, the sifted key

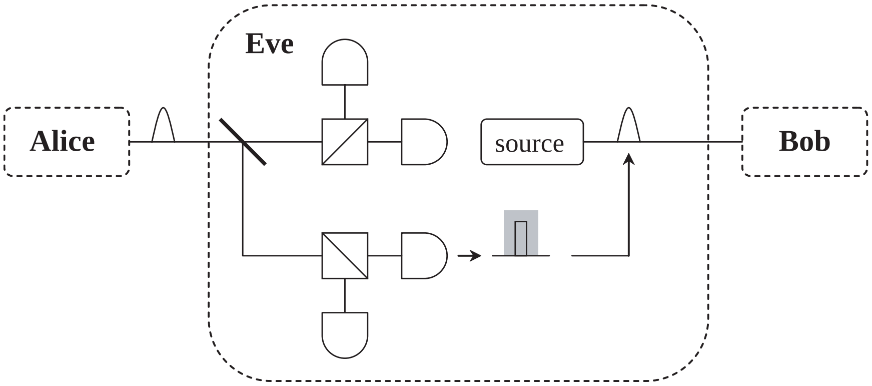

Figure 2.7: Illustration of the intercept and resend eavesdropping attack in BB84.

created by the previous procedure is unconditionally secure. The security relies on the fact that an eavesdropper does not know which basis the qubit was encoded in. She learns this information only after the qubit has been received by Bob, and at that point it is too late to modify her measurement. Consider first the simplest possible attack Eve may perform, known as the intercept and resend attack, which is illustrated in Fig. 2.7. Eve simply intercepts each qubit from the quantum channel, measures its state, and then sends a qubit to Bob prepared in the same state that was measured. But Eve does not know the preparation basis, so she must guess the measurement basis. She can, for example, randomly choose between the computational and diagonal basis, exactly in the same way as Bob. With 50% probability she will have a wrong guess and resend the wrong state to Bob, which will cause a 50% error rate. Thus, the intercept and resend attacks will create an overall 25% error rate in the transmission. This increase in errors can be used to detect the presence of an eavesdropper. Alice and Bob can simply sacrifice a small fraction of their key over the public channel to estimate the error rate. If errors are detected they will discard the key.

Of course, Eve may choose to make her measurement in a basis other than the computational basis, but it is not difficult to show that this would also result in a 25% error rate. Furthermore, the intercept and resend strategy is clearly not the most general attack strategy. In the most general case, the eavesdropper can perform

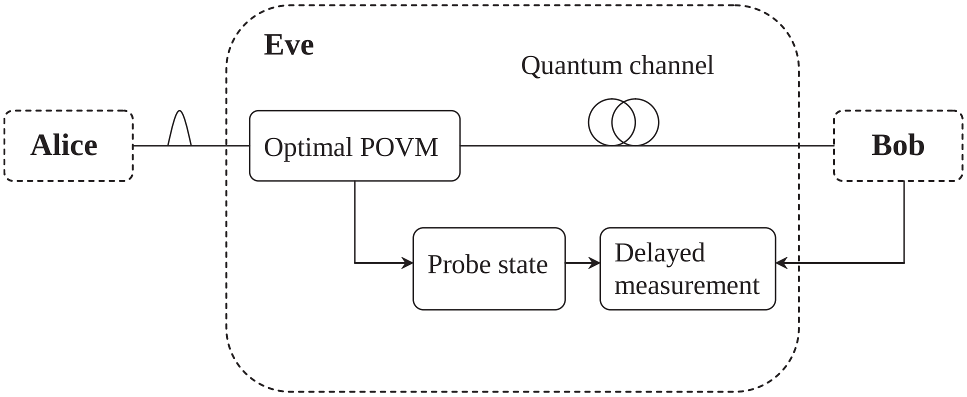

Figure 2.8: Illustration of the general individual eavesdropping attack.

a generalized delayed measurement of the form discussed in Sec. 2.3.4 and illustrated in Fig. 2.8, where she applies an optimal Positive Operator Value Measure (POVM) on the combined system of a single qubit and her probe and subsequently makes a delayed measurement on the probe state to obtain information about the qubit state. Although such a general individual attack is more effective than the intercept and resend attack, it is still true that no such measurement can yield information about the quantum state without causing some amount of error. Any practical communication system, however, has a baseline error rate, so error correction and privacy amplification are in practice absolutely essential.

In the case of the BB84 protocol with an ideal single-photon source, and considering general individual attacks, that is any optimal measurement on single photons allowed by quantum mechanics, it was shown in [15] that the collision probability for each bit p_{c_0} is bounded as follows:

$$p_{c_0} \leq \frac{1}{2} + 2e - 2e^2 \tag{2.24}$$

The above expression shows that when $e = 0$ the collision probability is $1/2$, which means that Eve gets no information about the key, while when $e = 1/2$ the collision probability is 1 and Eve can learn the entire string, for example Eve could intercept each photon Alice sends, store it, and then send an unpolarized photon to Bob.

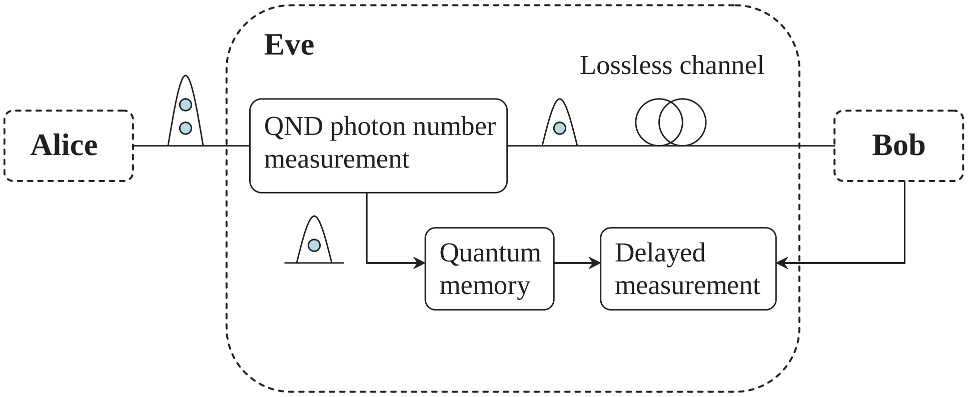

Figure 2.9: Illustration of the photon number splitting eavesdropping attack.

The average collision probability for the n-bit string is calculated from Eq. (2.24) as $p_{\mathrm{c}} = p_{\mathrm{c}_0}^n$, so the shrinking factor in this case is derived using Eq. (2.20):

$$\tau = -\frac{\log_2 p_{\mathrm{c}}}{n} = -\log_2 p_{\mathrm{c}_0} = -\log_2\left(\frac{1}{2} + 2e - 2e^2\right) \tag{2.25}$$

The result of Eq. (2.25) applies only in the case of an ideal single-photon source. In practice, however, all sources sometimes generate vacuum instead of one photon, or, most importantly, multi-photon states. For example, as we saw in Sec. 2.2.2, the light emitted from a classical source such as a laser follows a Poisson distribution, which means that even when the light is highly attenuated and the average photon number is much smaller than 1 there is always a probability that the field will contain more than one photon. Multi-photon states are vulnerable to photon number splitting attacks, which can cause a security loophole in the communication [16]. As illustrated in Fig. 2.9, in a photon number splitting (PNS) attack, Eve performs a quantum non-demolition (QND) measurement of the photon number for each qubit individually, and when she measures for example two photons she splits one photon off and stores it coherently in a quantum memory, letting the second photon reach Bob's detection apparatus undisturbed. After the public bases announcement, Eve measures her photon in the correct basis and therefore learns the value of the bit with 100% probability, without causing any errors in the communication. Even if the probability of a multi-photon state is very small, it can still cause a significant security problem, if the quantum channel used for the transmission is lossy. In this case, Eve can split off one photon at the beginning of the channel, and replace the lossy channel with a lossless one to ensure that the second photon will reach Bob, as shown in Fig. 2.9. She can subsequently block a fraction of the single-photon states to conserve the overall communication rate. This gives her complete information over a large fraction of the key. At some some sufficiently high loss, Eve can resend to Bob only the multi-photon states while blocking all single-photon states. This will render the entire key completely insecure. Thus, the multi-photon states put an upper limit on the amount of channel loss a system can have for secure communication to be possible.

Photon number splitting attacks can be accounted for by appropriately modifying the shrinking factor τ defined in Eq. (2.25). If we define β as the fraction of single-photon states emitted by the source then τ is redefined for the case of practical sources as:

$$\tau = -\beta \log_2 p_{c_0}\left(\frac{e}{\beta}\right) = -\beta \log_2 \left[\frac{1}{2} + 2\frac{e}{\beta} - 2\left(\frac{e}{\beta}\right)^2\right] \tag{2.26}$$

The above expression shows that PNS attacks have two effects on the shrinking factor. First, each multi-photon state reveals one bit of information to Eve, which is accounted for by the outer factor of β in the expression. Second, because Eve learns a fraction of the key without causing errors, she can create a larger error rate on the remainder of the key while maintaining the same overall bit error rate, which is accounted for by normalizing e by β in the above expression.

Eqs. (2.25) and (2.26) give the privacy amplification shrinking factor for the BB84 protocol in the cases of an ideal and a practical single-photon source, respectively. In order to evaluate the performance of the quantum key distribution system in each case we would like to calculate the secure key generation rate given in Eq. (2.23) as a function of several system parameters. For this, we need to define the following quantities.

Let us first define p_{click} as the probability that Bob detects a photon in a given clock cycle. Detection events may be triggered by photons sent from Alice or by dark counts in Bob's detectors. These two sources are assumed independent. Thus,

$$p_{\text{click}} = p_{\text{signal}} + p_{\text{dark}} - p_{\text{signal}} p_{\text{dark}} \tag{2.27}$$

If p_{dark} and p_{signal} are sufficiently small the probability of a simultaneous signal and dark count detection in the same clock cycle is negligible, so we can write:

$$p_{\text{click}} \approx p_{\text{signal}} + p_{\text{dark}} \tag{2.28}$$

Assuming relatively high channel loss, the signal contribution to the detection events is approximately given by the following expression:

$$p_{\text{signal}} \approx \mu T \tag{2.29}$$

In this expression, μ is the average photon number in a clock cycle, which is 1 for an ideal single-photon source while for a Poisson source it becomes a free variable that needs to be optimized, as we will see below. T is the total transmission efficiency of the quantum channel and Bob's detection setup. If the quantum channel is an optical fiber with loss coefficient α dB/km and length L km, the quantum efficiency of Bob's detector is η, and the loss of his detection setup is L_{s} dB, T is given by the expression:

$$T = \eta 10^{-(\alpha L + L_{\text{s}})/10} \tag{2.30}$$

The dark count contribution to the detection events is given by:

$$p_{\text{dark}} = 4d \tag{2.31}$$

where the coefficient 4 is due to the presence of four detectors in the passive modulation setup of Fig. 2.6. The dark counts per measurement time window d are given by:

$$d = Dt_{\text{w}} \tag{2.32}$$

where D is the dark count rate of the detectors and t_{w} is the measurement time window of the system. Defining ν as the repetition rate of the transmission, we can use Eq. (2.17) and the definition of R_{raw} given in Sec. 2.3.1 to write the sifted key generation rate as:

$$R_{\text{sifted}} = \frac{1}{2} R_{\text{raw}} = \frac{1}{2} \nu p_{\text{click}} \tag{2.33}$$

where p_{click} is given by Eqs. (2.28)-(2.32). The error rate e includes contributions from both the signal and dark count components. Errors from the signal component occur because of imperfect state preparation, channel decoherence, and imperfect polarization optics at Bob's detection unit. The baseline system error rate b accounts for all these effects. A second error component comes from the dark counts of Bob's detectors. Each dark count is completely uncorrelated with Alice's signal and thus causes a 50% error rate. Using the above definitions, we can write:

$$e = \frac{\frac{1}{2} p_{\text{dark}} + b p_{\text{signal}}}{p_{\text{click}}} \tag{2.34}$$

Finally, the parameter β, which is the fraction of single-photon states emitted by the source, is given by:

$$\beta = \frac{p_{\text{click}} - p_{\text{multi}}}{p_{\text{click}}} \tag{2.35}$$

where p_{multi} is the probability that the source emits a multi-photon state. For an ideal single-photon source, $p_{\text{multi}} = 0$ (i.e., $\beta = 1$), while for a Poisson source [22]:

$$p_{\text{multi}} \approx \frac{\mu^2}{2} \tag{2.36}$$

Combining Eqs. (2.23) and (2.33), we can write the secure key generation rate as:

$$R_{\text{BB84}} = \frac{1}{2} \nu p_{\text{click}} \{\tau + f(e)[e \log_2 e + (1 - e) \log_2 (1 - e)]\} \tag{2.37}$$

where p_{click} is given by Eqs. (2.28)-(2.32), τ by Eq. (2.25) or Eq. (2.26) depending on the source, e by Eq. (2.34), and β by Eq. (2.35). We have thus expressed the secure key generation rate as a function of the fixed system parameters ν, α, L, L_{s}, η, d, and b. The rate is also a function of the average photon number μ, which is an adjustable parameter in the case of a Poisson source. From the expressions for

p_{signal} and p_{multi} given by Eqs. (2.29) and (2.36) respectively, we can observe that p_{signal} reduces linearly with μ while p_{multi} reduces quadratically. This means that if μ is set too high, the communication rate will drop due to the increase in the probability of multi-photon states. If it is instead set too low, the rate will again drop and secure communication will quickly become impossible due to a decrease in signal counts relative to the dark counts, which will dominate. It turns out that there is a unique optimal μ which maximizes the secure key generation rate. Therefore, for given system parameters the rate must be optimized with respect to μ to achieve the best possible performance of the QKD system.

Before continuing with numerical calculations and comparison of the various cases, we would like to make an initial estimation of the difference in the performance of a QKD system employing the BB84 protocol with an ideal single-photon source and an attenuated Poisson source. For the case of negligible error rate and $p_{\text{dark}} \ll p_{\text{signal}} \ll 1$, Eq. (2.37) becomes:

$$R_{\text{poisson}} \approx \frac{1}{2}\nu\left(p_{\text{click}} - p_{\text{multi}}\right) \tag{2.38}$$

The average photon number that maximizes this expression is given by:

$$\mu_{\text{opt}} \sim T \tag{2.39}$$

This leads to:

$$R_{\text{poisson}} \approx \frac{1}{4}\nu T^2 \tag{2.40}$$

This calculation simply expresses the fact that in order for Alice and Bob to overcome the hybrid attack launched by Eve, in which she blocks more and more single-photon states as the channel loss increases, the average photon number must be reduced along with the fiber loss. As a result, the secure key generation rate decreases quadratically with the transmission of the quantum channel, as Eq. (2.40) shows. On the contrary, for an ideal single-photon source implementation, under the same conditions we find:

$$R_{\text{ideal}} \approx \frac{1}{2}\nu T \tag{2.41}$$

which means that the rate decreases only linearly with the fiber transmission due to

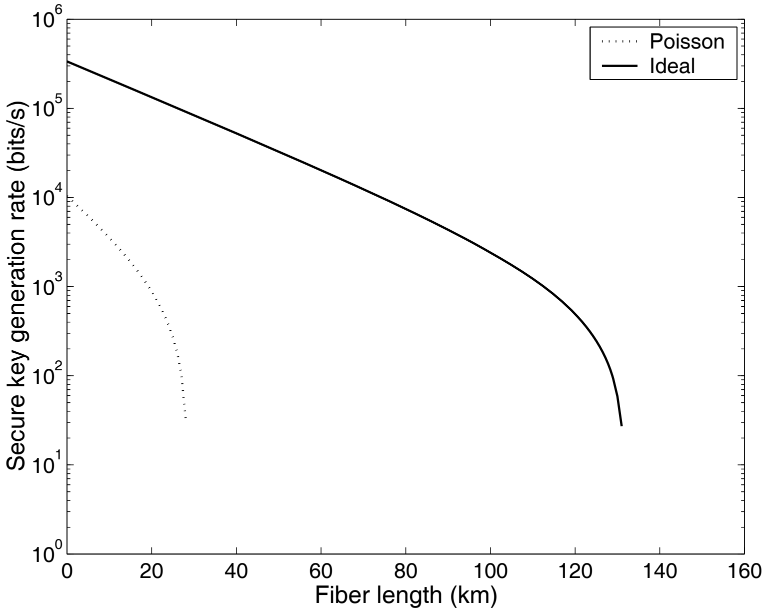

Figure 2.10: Secure key generation rate as a function of fiber length for the standard BB84 protocol employing a Poisson or an ideal single-photon source.

the absence of PNS attacks in this case.

Fig. 2.10 shows the communication rate for fiber-optic implementations of the standard BB84 QKD protocol employing an ideal single-photon source or an attenuated Poisson source, as a function of fiber length. For these calculations, the loss coefficient of the optical fiber is set to $\alpha = 0.2$ dB/km for the telecommunication window around 1.55 μm that is of interest for long-distance QKD, the baseline system error rate is set to $b = 0.01$, and in addition to the fiber losses we assume an extra loss of $L_{\mathrm{s}} = 1$ dB at the receiver site. The choice of the single-photon detector is extremely important because the detector's characteristics, namely the quantum efficiency and dark counts, play a crucial role in the performance of the QKD system. This will become very clear in Chapter 4, where we will describe different single-photon detectors. In the calculations of the remainder of this chapter and in Chapter 3, we will consider an InGaAs/InP avalanche photodiode (APD), which is usually employed in fiber-optic QKD experiments. The typical characteristics of this single-photon detector at 1.55 μm are a quantum efficiency of $\eta = 10\%$ and a dark count rate of $D = 10^4$ counts/s [54]. The measurement time window t_w is ultimately limited by the timing jitter of the detector, and it is set to 1 ns, thus from Eq. (2.32) we have $d = 10^{-5}$ counts/time window. The repetition rate of the experiment is set to $\nu = 10$ MHz, which is the best rate achieved with these detectors to date [55]. Finally, in the case of a Poisson source the average photon number μ is numerically optimized for each value of the fiber length.

As we observe in Fig. 2.10, each curve features a cut-off distance, beyond which secure communication is no longer possible. This is due to the increasing contribution of the dark counts with fiber length. Furthermore, in the case of a Poisson source, we see that the quadratic decrease of the rate with the fiber length predicted by Eq. (2.40) is a dominant factor, making this implementation of the standard BB84 protocol unsuitable for long-distance quantum cryptography. On the contrary, the use of an ideal single-photon source allows for a significantly better performance in terms of both communication distance and secure key generation rate.

2.4.2 The decoy state BB84 protocol

Recent studies have shown that modifications of the BB84 protocol, such as changing the sifting procedure [56] or introducing decoy states [54, 57, 58, 59, 60], can make the protocol a lot more robust against the photon number splitting attacks and, consequently, extend the secure key distribution distance of BB84 with Poisson sources significantly. Although a detailed analysis of these variations is beyond the scope of this work, we will briefly discuss the vacuum + weak decoy state protocol described in [59] and compare it with the standard BB84 protocol, due to its importance as an alternative for a practical quantum key distribution system.

The basic idea of the decoy state BB84 protocol is that in addition to the single-photon pulse sequence that Alice uses to encode the quantum information, she also sends a decoy state pulse sequence which contains no useful information. Because Alice chooses randomly whether to send a decoy or a signal state, Eve has no way of distinguishing the two types of states. Alice and Bob can then use the decoy states to test the quality of the transmission and derive a lower bound for the gain and an upper bound for the error rate of the signal single-photon states, which are the only states used for the formation of the secret key. This procedure significantly increases the robustness of the protocol against PNS attacks. It can be shown that the optimal signal average photon number is in this case independent of the quantum channel transmission, contrary to the case of the standard BB84 protocol with a Poisson source. This means that the secure key generation rate decreases only linearly with the fiber length, as in the case of the standard BB84 protocol with an ideal single-photon source.

The vacuum + weak decoy state protocol uses two decoy pulse sequences, a vacuum decoy state that is used to estimate the background detection rate, and a weak decoy state that is used to derive the appropriate bounds. The security of this protocol against general attacks is proven in [59], where it is shown that the secure key generation rate is given by the following expression:

$$R_{\text{decoy}} = \frac{1}{2}\nu \left\{ -Q_\mu f(e_\mu) h(e_\mu) + Q_1[1 - h(e_1)] \right\} \tag{2.42}$$

where Q_μ, Q_1 and e_μ, e_1 are the gain and the error rate due to all signal states and only the single-photon states, respectively. The values for $f(e)$ are given in Table 2.1 and $h(e)$ is defined in Eq. (2.18). Defining q as the average photon number of the decoy states and T as in Eq. (2.30), the following equations relate the quantities in Eq. (2.42) with the system parameters, assuming that Bob's detection setup is the one shown in Fig. 2.6 [59]:

$$\begin{aligned}
Q_\mu &= 1 - e^{-\mu T} + 4d & (2.43)\\
Q_q &= 1 - e^{-qT} + 4d & (2.44)\\
e_\mu &= \frac{2d + b\left(1 - e^{-\mu T}\right)}{Q_\mu} & (2.45)\\
e_q &= \frac{2d + b\left(1 - e^{-qT}\right)}{Q_q} & (2.46)\\
Y_1 &= \frac{\mu}{\mu q - q^2}\left(Q_q e^q - Q_\mu e^\mu \frac{q^2}{\mu^2} - \frac{\mu^2 - q^2}{\mu^2} 4d\right) & (2.47)\\
Q_1 &= Y_1 \mu e^{-\mu} & (2.48)
\end{aligned}$$

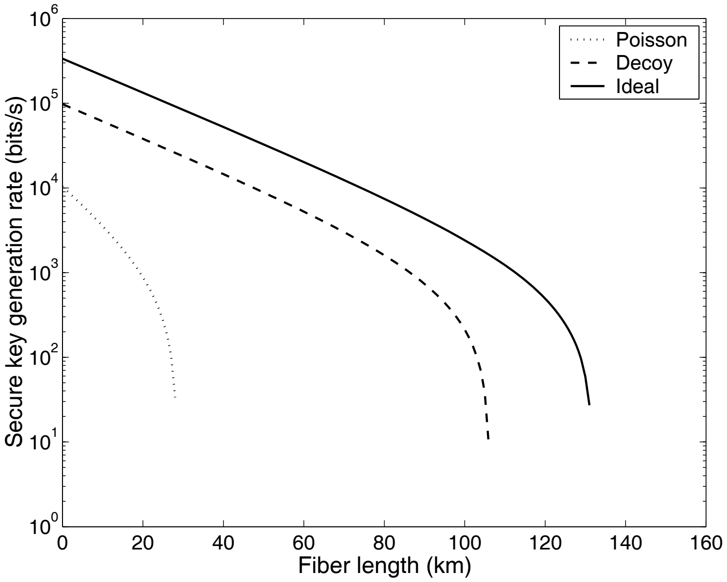

Figure 2.11: Secure key generation rate as a function of fiber length for the standard BB84 protocol employing a Poisson or an ideal single-photon source, and the vacuum + weak decoy state BB84 protocol.

$$e_1 = \frac{e_q Q_q e^q - 2d}{Y_1 q} \tag{2.49}$$

The optimal signal average photon number is only a function of the baseline system error rate and is determined by the equation:

$$(1 - \mu_{\text{opt}})e^{-\mu_{\text{opt}}} = \frac{f(b)h(b)}{1 - h(b)} \tag{2.50}$$

For example, for $b = 0.01$, which is the value we used in our calculation in Sec. 2.4.1, we find $\mu_{\text{opt}} = 0.77$. This value is much higher than the average photon number corresponding to the BB84 with a Poisson source in Fig. 2.10, which ranges between 0.02 and 0.07. This is a direct consequence of the use of decoy states to increase the robustness to PNS attacks, and leads to a higher communication rate.

In Fig. 2.11 we compare the performance of a QKD system implementing the standard BB84 protocol with an ideal single-photon source or a Poisson source, and the vacuum + weak decoy state BB84 protocol, which uses a Poisson source to produce signal states with $\mu = 0.77$ and weak decoy states with $q = 0.05$. The parameters ν, α, L_s, η, d, and b are the same as in Sec. 2.4.1. Clearly, the decoy state protocol achieves a much better performance than the standard BB84 protocol with a Poisson source, the result actually closely follows the performance achieved with an ideal single-photon source. This protocol is therefore a promising candidate for the implementation of a practical quantum cryptography system.

2.5 The BBM92 protocol

The most well studied entangled qubit quantum key distribution protocol is the BBM92 protocol, which was proposed by Bennett, Brassard, and Mermin in 1992 [33]. This protocol is the two-photon variant of BB84. To describe it, we consider again the polarization mode implementation of the photonic qubit. Alice and Bob each share a photon of an entangled photon pair, in the ideal case described by Eq. (2.13), and generated by a source presumed to be somewhere between the two parties. Subsequently, they measure the polarization state of their photon in a randomly chosen basis, either the computational basis $\{|0\rangle, |1\rangle\}$ or the diagonal basis $\{|0_{\pi/4}\rangle, |1_{\pi/4}\rangle\}$, with equal probability for each qubit, using the detection apparatus shown in Fig. 2.6. When Alice and Bob measure their qubits in the same basis, their results should be perfectly correlated and in the absence of errors they share an identical bit. When they choose different bases, their results are uncorrelated, so they discard the bits that correspond to these cases during the sifting process. This happens with probability 50%, that is the sifting parameter is $s = 1/2$, as in BB84.

If there are no errors in the transmission, the sifted key is unconditionally secure. In this case, Eve cannot gain information about the key without inducing some errors that can be detected by Alice and Bob and reveal her presence. In a practical communication system, however, there is always a baseline error rate, so privacy amplification is required to derive a bound on the information that may have leaked to an eavesdropper and thus calculate the shrinking factor τ. The security proof of the BBM92 protocol, which considers general individual attacks and allows Eve to have full control of the entangled qubit source, is presented in [48], and shows that the collision probability for each bit p_{c_0} is bounded as follows:

$$p_{\mathrm{c}_0} \leq \frac{1}{2} + 2e - 2e^2 \tag{2.51}$$

This result is exactly the same as for the case of the BB84 protocol with an ideal single-photon source, as shown in Eq. (2.24). Thus, as in Eq. (2.25), the privacy amplification shrinking factor becomes:

$$\tau = -\log_2\left(\frac{1}{2} + 2e - 2e^2\right) \tag{2.52}$$

This indicates that there is no analog to a photon number splitting attack in BBM92. The error rate is sufficient to calculate the privacy amplification factor. In order to compare the performance of a QKD system implementing the BB84 and BBM92 protocols, we need to express the secure key generation rate given by Eq. (2.23) for BBM92 as a function of the system parameters.

Defining p_{coin} as the probability of a coincidence in the detections between Alice and Bob, p_{true} and p_{false} as the probability of a true and a false coincidence, respectively, assuming that the sources of true and false coincidences are independent, and that the probability of simultaneous detections in one clock cycle is negligible, we can write:

$$p_{\mathrm{coin}} = p_{\mathrm{true}} + p_{\mathrm{false}} \tag{2.53}$$

In [48] it is shown that p_{false} is minimized if the entangled-photon source is placed halfway between Alice and Bob. Thus, if L is the total distance between them, the transmission efficiency for each party is defined similarly to Eq. (2.30) as:

$$T_{L/2} = \eta 10^{-(\alpha L + 2L_{\mathrm{s}})/20} \tag{2.54}$$

Then, for an ideal entangled-photon source, that is a source that deterministically generates one pair of entangled photons per clock cycle, we can write the following expressions:

$$
\begin{aligned}
p_{\text{true}} &= T_{L/2}^2 && (2.55)\\
p_{\text{false}} &= 16d^2 + 8dT_{L/2} && (2.56)
\end{aligned}
$$

where the last expression shows that in the case of an ideal source a false coincidence can only occur from a photon and a dark count or from two dark counts.

In the case of a practical entangled-photon source such as the parametric down-converter (PDC) that we discussed in Sec. 2.2.3, we need to take into account additional factors related to the parametric down-conversion process. The expressions for p_{true} and p_{false} are thus modified as follows [48]:

$$
\begin{aligned}
p_{\text{true}} &= c_1 && (2.57)\\
p_{\text{false}} &= 16d^2c_2 + 8dc_3 + c_4 && (2.58)
\end{aligned}
$$

where

$$
\begin{aligned}
c_1 &= \frac{1}{\cosh^4\chi}\frac{2T_{L/2}^2\tanh^2\chi}{\left[1-\tanh^2\chi(1-T_{L/2})^2\right]^4} && (2.59)\\
c_2 &= \frac{1}{\cosh^4\chi}\frac{1}{\left[1-\tanh^2\chi(1-T_{L/2})^2\right]^2} && (2.60)\\
c_3 &= \frac{1}{\cosh^4\chi}\frac{2T_{L/2}(1-T_{L/2})\tanh^2\chi}{\left[1-\tanh^2\chi(1-T_{L/2})^2\right]^3} && (2.61)\\
c_4 &= \frac{1}{\cosh^4\chi}\frac{4T_{L/2}^2(1-T_{L/2})^2\tanh^4\chi}{\left[1-\tanh^2\chi(1-T_{L/2})^2\right]^4} && (2.62)
\end{aligned}
$$

In the above equations, c_1 is the probability that Alice and Bob share an entangled photon pair, c_2 is the probability that neither receives a photon, either because the source failed to generate a pair or because all photons were lost, c_3 is the probability that one receives a photon while the other does not, and c_4 is the probability that they both receive a photon but these photons are unpolarized and uncorrelated. The parameter χ is a function of the nonlinear coefficient, the pump energy, and the interaction time of the down-conversion process, and determines the average number of photon pairs per clock cycle. This adjustable parameter plays the same role as the average number of photons μ in BB84 with a Poisson source. As we see from Eqs. (2.59) and (2.62), c_1 which is the probability of a real coincidence increases with χ, and c_4 which contributes to false coincidences also increases with χ, but is of higher order. Thus, we cannot make c_1 arbitrarily large without getting an increased contribution from c_4. This leads to an optimum value for χ for given system parameters.

Finally, similarly to Eq. (2.34) the error rate is given by the expression:

$$e = \frac{\frac{1}{2}p_{\mathrm{false}} + b p_{\mathrm{true}}}{p_{\mathrm{coin}}} \tag{2.63}$$

Putting everything together, we can write the secure key generation rate as:

$$R_{\mathrm{BBM92}} = \frac{1}{2}\nu p_{\mathrm{coin}}\{\tau + f(e)[e\log_2 e + (1-e)\log_2(1-e)]\} \tag{2.64}$$

where p_{coin} is given by Eqs. (2.53)-(2.62) depending on the source, τ by Eq. (2.52), and e by Eq. (2.63).

For the case of negligible error rate and $p_{\mathrm{false}} \ll p_{\mathrm{true}}$, the above expression shows that the secure key generation rate of BBM92 decreases linearly with the transmission of the quantum channel, similarly to the case of the BB84 protocol with an ideal single-photon source, as we see from Eq. (2.41). Eqs. (2.37) and (2.64) are used to compare the performance of a quantum key distribution system implementing the BB84 and BBM92 protocols using both ideal and practical sources. The result is shown in Fig. 2.12. The parameters ν, α, L_{s}, η, d, and b are assumed the same as in the calculations of Sec. 2.4, while in the case of a parametric down-conversion source the parameter χ is numerically optimized for each value of the fiber length. As we observe in Fig. 2.12, the curves for BBM92 feature a much longer cut-off distance than their BB84 counterparts, albeit at a lower communication rate. This is due to the absence of photon number splitting attacks in BBM92, as well as the inherent robustness of this protocol. For example, BBM92 is less vulnerable to errors

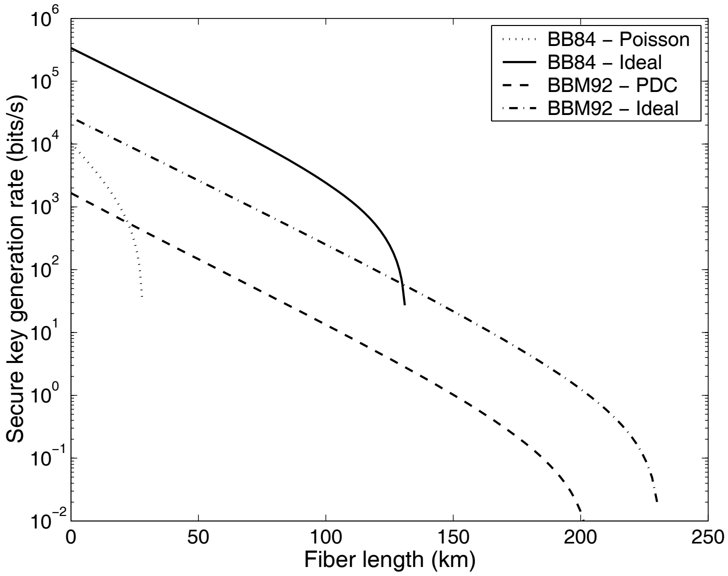

Figure 2.12: Comparison of the BB84 and the BBM92 protocols using both ideal and practical sources.

caused by dark counts, since one dark count alone cannot produce an error in this entanglement-based protocol.

2.6 Summary

In this chapter, we introduced the concept of quantum cryptography as a means for two parties to share an unconditionally secure secret message. We discussed how we can encode quantum information in single and entangled photons, and we then showed that we can cleverly use the unique properties of quantum measurement together with the results of classical and quantum information theory to perform a quantum key distribution algorithm. Finally, we discussed in detail two prominent algorithms, the standard and decoy state versions of the BB84 protocol, and the BBM92 protocol. We showed the limits that practical components impose on the performance of a quantum cryptography system implementing these protocols, and we compared such systems. Efforts toward the experimental realization of these systems will be discussed in Chapter 5.

In the next chapter, we will introduce a new quantum key distribution algorithm, the differential phase shift QKD protocol. We will prove the security of this protocol against several types of attacks, we will compare it with the BB84 protocol, and we will show that it opens the way to the implementation of a simple and practical quantum cryptography system.

Chapter 3

Differential phase shift quantum key distribution

3.1 Introduction

The quantum key distribution protocols that we described in Chapter 2 use encoding of quantum information in two nonorthogonal bases, or else four nonorthogonal single-photon states, as in BB84, or in entangled two-photon states, as in BBM92. The security relies on the fact that an eavesdropper does not know the basis the qubits were encoded in, so in principle she cannot perform a measurement without causing disturbance in the communication system.

The possibility that encoding quantum information in only two nonorthogonal quantum states may be sufficient to perform secure quantum key distribution was first discussed by Bennett in 1992, who proposed the B92 protocol [29]. A system that implements the B92 protocol using attenuated Poisson light is shown in Fig. 3.1. In this implementation, Alice uses an unbalanced interferometer to divide a bright coherent pulse into two pulses: a bright reference pulse that travels through the short path of the interferometer, and a weak signal pulse that travels through the long path and is randomly phase modulated by 0 or π. Bob receives each pair of sequential pulses and measures it using an unbalanced interferometer identical to the one on Alice's site, that is an interferometer that introduces a time delay equal to the separation of

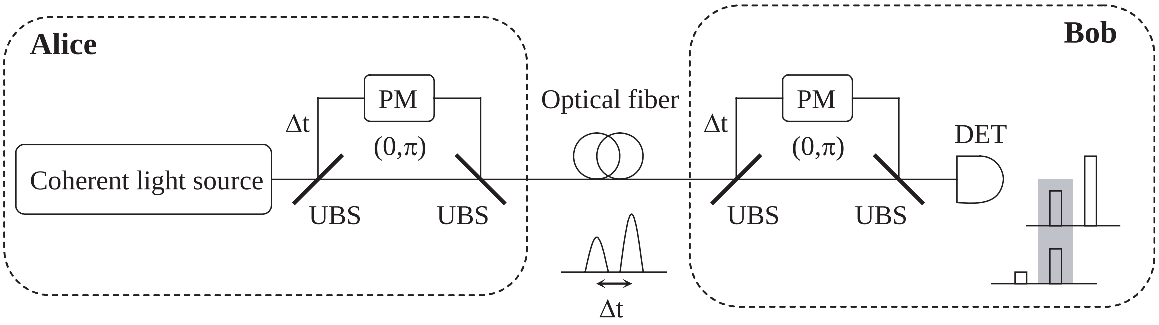

Figure 3.1: Quantum key distribution system for the implementation of the B92 protocol. PM, phase modulator; UBS, unbalanced beamsplitter; DET, detector.

the two pulses as well as a random phase modulation of 0 or π to the pulse that goes through the long path. A single-photon detector is placed at one of the interferometer output ports. As shown in Fig. 3.1, the detector can record an event at 3 time slots. The first slot corresponds to the bright reference pulse, which has taken the short path in both Alice's and Bob's interferometers. The second slot corresponds either to the attenuated pulse taking the short path in Bob's interferometer or the bright pulse taking the long path in Bob's interferometer. Finally, the third slot corresponds to a very weak pulse that has been attenuated twice, and is of no interest for the protocol.

The security of this protocol is based on the fact that Alice randomly prepares and sends to Bob two nonorthogonal states. In particular, coherent states of light with an average photon number less than 1 are highly nonorthogonal when they have opposite phases. This is shown from Eq. (2.10), which becomes in this case:

$$\langle\alpha|-\alpha\rangle = e^{-2|\alpha|^2} \tag{3.1}$$

where $|\alpha|^2 = \mu \ll 1$ is the average photon number per pulse. The information is encoded in the phase between the weak signal pulse and the accompanying reference pulse, for example phase differences 0 and π are used to encode binary 0 and 1, respectively. When Bob applies his measurement on the two pulses, the second time slot corresponds to the interference between the reference pulse taking the long path and the signal pulse taking the short path in his interferometer. If the phases of the interferometers of Alice and Bob are matched, constructive interference occurs and the detector records an event, while in the opposite case destructive interference leads to no detection event. Subsequently, Bob announces the time instances at which he recorded an event. From her modulation data, Alice knows which phase value he has applied, so they share in this way an identical bit string. Clearly, only the second slot contains important key information in this protocol. The first time slot contains no phase information, but serves to confirm that the reference pulse has actually arrived. Therefore, it protects against an intercept and resend type of attack, in which Eve measures each pulse pair using an apparatus similar to Bob, resends a pair in the case of a successful measurement result, and suppresses both signal and reference pulses in the case of an unsuccessful result, thereby eavesdropping on the transmission without creating errors. Due to the existence of the bright reference pulse, Eve is obliged to send a signal pulse together with the reference pulse even when her measurement was unsuccessful. She thus creates errors which reveal her presence. The security of the B92 protocol against more elaborate attacks, such as general individual and coherent attacks has been studied [49, 50, 51, 52].

In the following sections, we will describe and prove the security of the differential phase shift quantum key distribution protocol (DPS-QKD), which was proposed by Inoue, Waks, and Yamamoto in 2002 [61, 62]. Similarly to the B92 protocol, in the DPS-QKD protocol quantum information is encoded in the differential phase of attenuated coherent states of light. However, this protocol does not require a bright reference pulse, and it is a simpler and more efficient protocol compared to the B92 protocol.

3.2 The DPS-QKD protocol

A quantum key distribution system that implements the DPS-QKD protocol using attenuated Poisson light is shown in Fig. 3.2. Alice generates a train of coherent pulses, which are attenuated such that the average photon number per pulse is less than 1, randomly phase modulated by 0 or π, and sent over the quantum channel

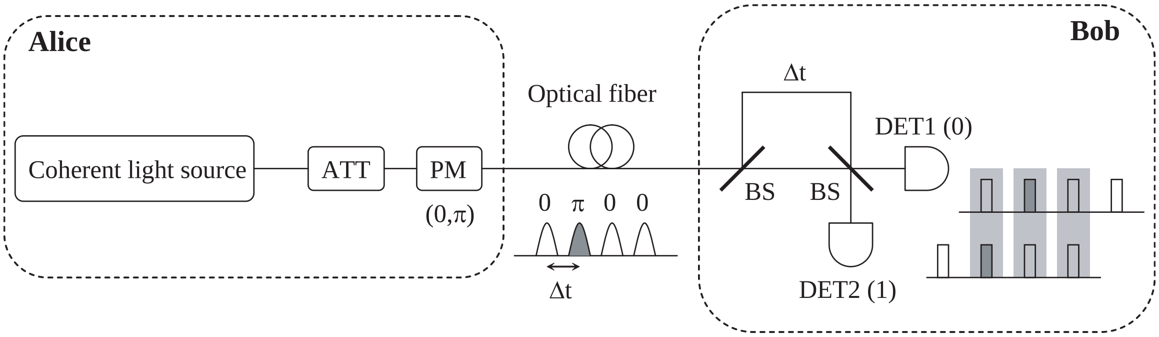

Figure 3.2: Quantum key distribution system for the implementation of the DPS-QKD protocol. PM, phase modulator; ATT, attenuator; BS, beamsplitter; DET, detector.

to Bob. Each photon coherently spreads over many pulses with a fixed phase modulation pattern. In the receiver side, Bob divides the incoming pulses into two paths and recombines them using 50/50 beamsplitters. The time delay introduced by his interferometer is equal to the inverse of the clock frequency, or else equal to the time separation between the sequential pulses. Single-photon detectors are placed at the output ports of the second beamsplitter. After passing through Bob's interferometer, consecutive pulses interfere at the output beamsplitter, and which detector records a detection event depends on the phase difference of the two pulses. If the interferometer is appropriately adjusted, detector 1 in Fig. 3.2 records an event when the phase difference is 0 and detector 2 records an event when the phase difference is π. Because the average photon number per pulse is less than one, Bob observes detection events only occasionally and at random time instances. Bob announces publicly the time instances at which a photon was detected, but he does not reveal which detector detected it. From her modulation data, Alice knows which detector in Bob's site recorded the event. Thus, by designating detection events recorded by detector 1 and 2 as bits 0 and 1, respectively, they can share an identical bit string. Since all bits are used during the key formation, the sifting parameter in the case of the DPS-QKD protocol is $s = 1$.

If there are no errors in the system, the sifted key created by the described procedure is unconditionally secure. However, as we discussed in Chapter 2, all practical systems have a baseline error rate, and therefore error correction and privacy amplification are essential. For a QKD protocol to be useful, it is crucial to prove its security against several types of eavesdropping attacks, that is to derive the privacy amplification shrinking factor that ensures the generation of a secure key. Such a security analysis for the DPS-QKD protocol is the subject of the remainder of this chapter, and it is extremely important, since from Fig. 3.2 it is clear that this protocol requires a very simple system architecture and mainly components that are extensively used in current telecommunication systems. It therefore has a great potential for enabling the implementation of a simple and practical QKD system.

3.3 Security proof against restricted attacks

In general terms, the security of the DPS-QKD protocol stems from the nondeterministic collapse of a wavefunction in a quantum measurement. In particular, if the number of pulses in the coherence time of Alice's source is n_p, then each of Alice's photons is in a superposition of all the states that correspond to the n_p time instances with the appropriate phase applied to each one of them. The overall wavefunction is a product state of these individual photon states. At Bob's site, a detection event at a certain time instance n reveals the phase difference between the pulses in time instances n and $n+1$, which corresponds to one bit of information. However, these detection events occur completely randomly, so an eavesdropper cannot deterministically collapse the wavefunction in the same time instance and obtain the same bit of information as Bob.

The above argument will become more clear in the next section where we consider the beamsplitter attack. In this attack, Eve obtains coherent copies of the quantum state of the pulses sent by Alice by inserting a beamsplitter in the transmission line. As we will see, this attack does not introduce any errors in the transmission and cannot be distinguished from channel loss. Along with the beamsplitter attack, Eve can also undertake an intercept and resend attack as long as the bit error rate induced by this attack is kept smaller than the baseline system error rate. In the following, we analyze the security of the DPS-QKD protocol against this set of restricted eavesdropping attacks, where we only allow Eve to perform specific actions and measurements. In order to derive the secure key generation rate for the DPS-QKD protocol in this case, we calculate the privacy amplification shrinking factor τ, defined in Eq. (2.20) as a function of the average collision probability p_{c}, for the hybrid beamsplitter and intercept and resend attack.

3.3.1 The beamsplitter attack

In the beamsplitter attack, which is illustrated in Fig. 3.3, Eve uses a beamsplitter to obtain coherent copies of the quantum state of the pulses that Alice sends to Bob. She also replaces the lossy quantum channel with a lossless one, and the imperfect detectors at Bob's receiver unit with perfect ones. The assumption that Eve can replace Bob's imperfect detectors with perfect ones may seem unrealistic. However, there are some ways that Eve can improve the characteristics of Bob's detectors. For example, Eve can change the wavelength of the photons to a region of higher detection efficiency. A similar argument can be applied to the dark count rate. In order to account for this, this security analysis is based on the conservative assumption that Eve has control of the quantum efficiency and dark count rate of Bob's detectors. Without Eve's intervention, Bob's probability of detecting a signal photon is identical to the one given in Eq. (2.29) and repeated here:

$$p_{\mathrm{signal}} \approx \mu T \tag{3.2}$$

where μ is the average number of photons per pulse and T is the total transmission efficiency of the quantum channel and Bob's detection setup. As in Eq. (2.30), if the quantum channel is an optical fiber with loss coefficient α dB/km and length L km, the quantum efficiency of Bob's detector is η, and the loss of his detection setup is L_{s} dB, T is given by the expression:

$$T = \eta 10^{-(\alpha L + L_{\mathrm{s}})/10} \tag{3.3}$$

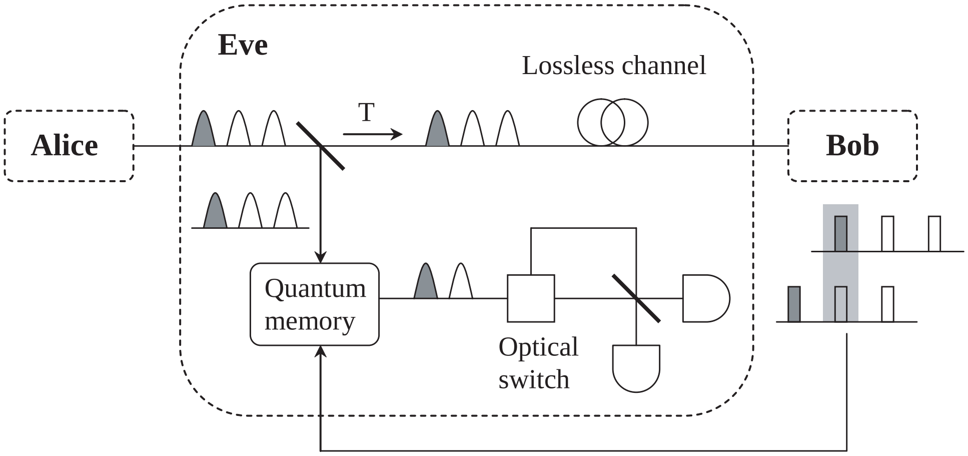

Figure 3.3: Illustration of the beamsplitter eavesdropping attack in DPS-QKD.

In order for Eve to avoid being revealed due to a decrease in the count rate, she has to leave the probability of signal detection unaltered, so she has to set the beamsplitter transmission equal to T. Then, one beam with an average photon number of $n_p\mu T$, where n_p is again the number of pulses in the coherence time of the source, is sent to Bob through her lossless fiber, while the other beam with an average photon number of $n_p\mu(1-T)$ is used by Eve. One possibility for Eve is to measure the pulses that she picks up with an interferometer identical to Bob's. Each photon in her n_p-slot wavefunction is detected completely randomly at one of n_p different time instances. Thus, the probability that she obtains the phase modulation data at a desired time instance, that is the probability that she obtains the value of a bit at a certain time given that Bob has detected a photon at that time is equal to $\mu(1-T)$.

The above result gives Eve's information gain relative to Bob when we assume that Eve is not equipped with a quantum memory with an infinitely long coherence time. However, if we allow Eve to have such a quantum memory, her strategy can be changed in order to increase her information gain. In this case, she stores the pulses in her quantum memory, as shown in Fig. 3.3, and waits for Bob's announcement. It is important to note that Alice and Bob can delay the public announcement for an arbitrarily long time, so Eve's quantum memory must have an infinitely long coherence time. After Bob announces the time instances at which he recorded detection events, Eve applies her measurement using an interferometer with an optical switch instead of a 50/50 beamsplitter at the input side, which allows her to interfere only the pulses for which she is aware that Bob has obtained the differential phase information. This strategy increases Eve's probability of gaining bit information to $2\mu(1-T)$.

It is clear from this analysis that the beamsplitter attack does not cause any error in the communication between Alice and Bob. Hence, it gives full information, which corresponds to a collision probability for each bit of $p_{c_0}=1$, to Eve for a fraction of bits equal to $2\mu(1-T)$. For the remaining $1-2\mu(1-T)$ fraction of the bits, Eve does not obtain any information, which means that $p_{c_0}=1/2$ for these bits. This result shows that the mutual information between Eve and Bob is independent of the system transmission efficiency T, if $T \ll 1$. Therefore, in the case of $T \ll 1$, the mutual information between Eve and Bob can be made small simply by choosing a small μ that is independent of T.

3.3.2 The intercept and resend attack

Taking advantage of the system's inherent error rate, Eve can also apply an intercept and resend attack to some of the pulses that are sent to Bob after her beamsplitter. In this attack, which is illustrated in Fig. 3.4, Eve intercepts some pulses, lets them pass through an interferometer identical to Bob's, measures the phase differences, and according to her measurement result she resends an appropriate state to Bob. In the case of an inconclusive or vacuum outcome she sends the vacuum state, while when she measures a single photon she sends a photon split into two pulses with the correct phase difference 0 or π applied between them. When this photon arrives at Bob's site, he counts the photon possibly at three time instances, as shown in Fig. 3.4. When Bob measures the central time instance, he does not detect the eavesdropping because he obtains the correct phase difference. However, with 50% probability he measures the side time instances, which yield random, uncorrelated results, and with 50% probability these lead in error. Consequently, this attacks induces an overall 25% bit error rate in the communication between Alice and Bob. This means that if the error rate of the system is e, Eve can apply her attack to a fraction $4e$ of the photons

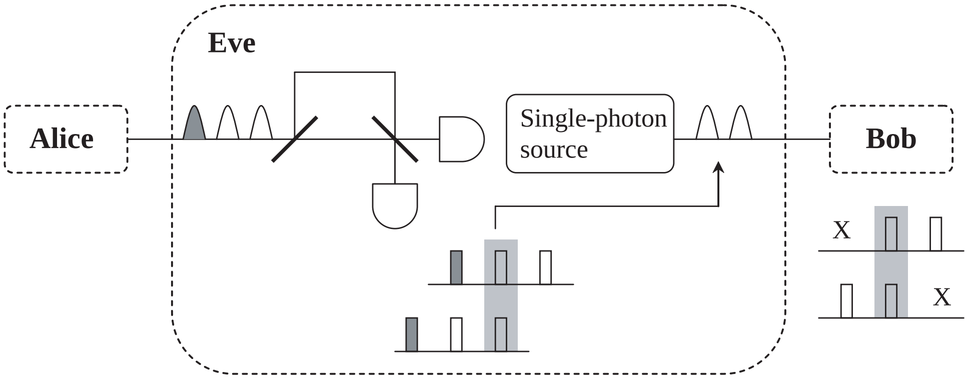

Figure 3.4: Illustration of the intercept and resend eavesdropping attack in DPS-QKD.

in order not to exceed this error rate. With 50% probability, which is the probability that Bob measures the central time instance for a resent photon, Eve obtains full information for these intercepted photons, which means that $p_{c_0} = 1$ for a fraction $2e$ of the bits. Eve does not obtain any information on the remaining bits.

To summarize the above arguments, taking into account the hybrid attack consisting of the beamsplitter and intercept and resend attacks, we find that the fraction of bits for which Eve has no information, that is for which $p_{c_0} = 1/2$, is equal to $1 - 2\mu(1-T) - 2e$, while she obtains full information for the rest of the bits. Thus, if n is the length of the sifted key, the average collision probability between bits owned by Bob and Eve is given by the expression:

$$p_c = p_{c_0}^n = \left(\frac{1}{2}\right)^{n[1-2\mu(1-T)-2e]} \tag{3.4}$$

Then, the privacy amplification shrinking factor in this case is derived using Eq. (2.20):

$$\tau = -\frac{\log_2 p_c}{n} = 1 - 2\mu(1-T) - 2e \tag{3.5}$$

This result concludes the security analysis of the DPS-QKD protocol against the beamsplitter and intercept and resend attacks. Before continuing with a comparison of the DPS-QKD and BB84 protocols, we would like to briefly mention a security concern that was pointed out in [63], where it was reported that the security of a QKD system implementing the BB84 protocol with an attenuated Poisson source without phase randomization is seriously compromised if Eve obtains phase reference information of the source. Although a careful analysis in the case of the DPS-QKD protocol is required, such an attack is possibly inefficient for this protocol for two reasons. First, in most implementations of the phase-encoded BB84 protocol a strong pulse is required [64, 65, 66], so the phase reference can be easily obtained by measuring the phase of this pulse. However, the retrieval of the phase reference for homodyne detection is hard for the DPS-QKD protocol, which employs a weak binary PSK signal, because of the intrinsic quantum noise of a local oscillator. Second, even if such a reference local oscillator wave is reconstructed, adaptive homodyne detection has a lower bound of bit error rate due to the intrinsic overlap of two coherent states with an average photon number of 0.2 or less.

After completing the derivation of the privacy amplification shrinking factor in Eq. (3.5), we would now like to express the secure key generation rate given in Eq. (2.23) as a function of the system parameters for the DPS-QKD protocol, as we did for the BB84 and BBM92 protocols in Chapter 2. Following the discussion in Sec. 2.4, the probability that Bob detects a photon in a given clock cycle is given by the expression:

$$p_{\mathrm{click}} \approx p_{\mathrm{signal}} + p_{\mathrm{dark}} \tag{3.6}$$

where the signal contribution the detection events is given by Eq. (3.2), while the dark count contribution is given by the expression:

$$p_{\mathrm{dark}} = 2d \tag{3.7}$$

In the above equation, the coefficient 2 is due to the presence of two detectors in the receiver unit of Fig. 3.2, and the dark counts per measurement time window d are given by Eq. (2.32). If ν is the repetition rate of the transmission, because the sifting parameter is 1 in the DPS-QKD protocol as we discussed in Sec. 3.2, similarly to

Eq. (2.33) we can write the sifted key generation rate as follows:

$$R_{\text{sifted}} = \nu p_{\text{click}} \tag{3.8}$$

Finally, the error rate is given by the expression:

$$e = \frac{\frac{1}{2}p_{\text{dark}} + bp_{\text{signal}}}{p_{\text{click}}} \tag{3.9}$$

where b is the baseline system error rate. Based on the above definitions, we can write the equation for the secure key generation rate of the DPS-QKD protocol against the hybrid beamsplitter and intercept and resend attack as:

$$R_{\text{DPS-QKD}} = \nu p_{\text{click}}\{\tau + f(e)[e\log_2 e + (1-e)\log_2(1-e)]\} \tag{3.10}$$

where τ is given by Eq. (3.5) and $f(e)$ characterizes the performance of the error correction algorithm.

For the case of negligible error rate and $p_{\text{dark}} \ll p_{\text{signal}} \ll 1$, Eq. (3.10) becomes:

$$R_{\text{DPS-QKD}} \approx \nu\mu T(1-2\mu) \tag{3.11}$$

This means that the secure key generation rate for the DPS-QKD protocol decreases linearly with the fiber transmission. This characteristic illustrates the robustness of this protocol to the photon number splitting attacks, and is identical to the cases of the standard BB84 protocol with an ideal single-photon source and the decoy state BB84 protocol as we discussed in Sec. 2.4, as well as a slightly modified B92 protocol [52].

In Fig. 3.5 we compare the performance of a fiber-optic QKD system implementing the standard BB84 protocol with an ideal or a Poisson source, the decoy state BB84 protocol, and the DPS-QKD protocol. The calculations for the BB84 protocol are based on the analysis of Sec. 2.4, while for the DPS-QKD protocol we use Eq. (3.10). All the fixed parameters of the system are assumed the same as in Sec. 2.4, that is $\nu = 10$ MHz, $\alpha = 0.2$ dB/km for 1.55 μm, $L_s = 1$ dB, $\eta = 10\%$, $d = 10^{-5}$ counts/time

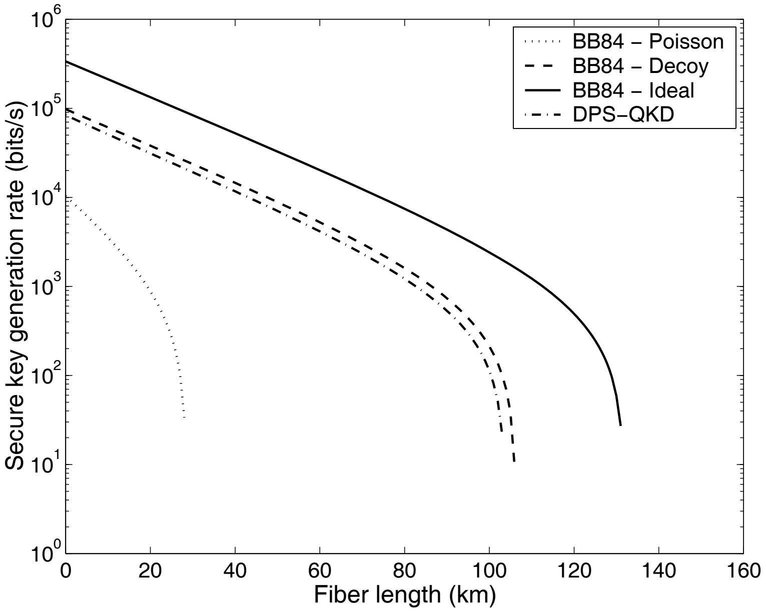

Figure 3.5: Secure key generation rate as a function of fiber length for the standard and decoy state BB84 protocol, and the DPS-QKD protocol.

window, and $b = 0.01$. For the decoy state protocol the average number of photons per pulse is set to $\mu = 0.77$, while the rate is numerically optimized with respect to μ for each value of the fiber length in the case of the BB84 protocol with a Poisson source and the DPS-QKD protocol in order to achieve the best possible performance of the QKD system. As we expect from the security analysis of the DPS-QKD protocol, this protocol features characteristics very similar to the standard BB84 protocol with an ideal single-photon source and the decoy state BB84 protocol, and significantly outperforms the standard BB84 protocol with Poisson light. This is a very important conclusion because the DPS-QKD protocol can be implemented with conventional lasers, detectors and linear optics, and has a very simple system architecture. This protocol is therefore a very practical and appealing candidate for a long-distance quantum cryptography system. Indeed, we will describe the implementation of such a system in Chapter 5.

3.3.3 A small modification

An interesting improvement in the performance of the DPS-QKD protocol, especially in the realistic case where Eve is not allowed to possess a quantum memory with an infinitely long coherence time, occurs when we consider a slight modification to the protocol. In particular, let us assume that Bob does not use an interferometer that introduces a time delay equal to the time separation between sequential pulses Δt as shown in Fig. 3.2, but rather he randomly modulates the delay time $N\Delta t$ in his interferometer by randomly choosing a positive integer N. In this case, after passing through Bob's interferometer, the pulses interfere at Bob's output beam splitter, and which detector clicks depends on the phase difference of the two pulses separated by a time $N\Delta t$ and not on the phase difference between two consecutive pulses. During the sifting phase, Bob announces the time instances at which a photon was detected as well as the randomly chosen positive integer N. When this modification is assumed, the beamsplitter and intercept and resend attacks are also modified as follows.

When Eve is not equipped with a quantum memory with an infinitely long coherence time, we calculated in Sec. 3.3.1 that the probability that she obtains the phase modulation data at a desired time instance by applying the beamsplitter attack is equal to $\mu(1-T)$. But because of the modification in the protocol, Eve also has to choose independently from Bob a positive integer M so that the delay time in her interferometer is equal to $M\Delta t$. Then, the probability that Eve's randomly chosen M matches Bob's N is equal to $1/N$. Thus, in this case the probability that Eve gains bit information relative to Bob is $\mu(1-T)/N$. On the other hand, when Eve is equipped with an ideal quantum memory, the modification in the protocol does not give Bob any advantage over Eve, and so in this case the information gain is the one calculated in Sec. 3.3.1, that is $2\mu(1-T)$. In summary, Eve does not obtain any information for a fraction $1-\mu(1-T)/N$ of the bits when she does not possess a quantum memory, and a fraction $1-2\mu(1-T)$ of the bits when she does.

In the modified intercept and resend attack, Eve intercepts pulses with a time interval $M\Delta t$, lets them pass through an interferometer with a delay $M\Delta t$, measures the differential phase, and according to her measurement result she sends an appropriate state to Bob, as described in Sec. 3.3.2. In this case, when Bob picks up an identical delay, $N = M$, and measures the central time instance, he does not detect the eavesdropping. However, with probability $1 - 1/2N$ he chooses another delay, $N \neq M$, or measures the side time instances, which yield uncorrelated results, and with probability $1/2$ these lead in error. Hence, this attack causes a bit error of $(1 - 1/2N)/2$ in the communication between Alice and Bob. If the error rate of the system is e, Eve is allowed to apply her attack to a fraction $2e/(1 - 1/2N)$ of the photons in order not to exceed this error rate. With probability $1/2N$, which is the probability that Bob chooses the same delay as Eve and measures the central time instance, Eve obtains full bit information for these intercepted photons. Thus, she obtains full information for a fraction $e/(N - 1/2)$ of the bits.

Summarizing the above discussion, we find that taking into account the modified hybrid beamsplitter and intercept and resend attack the fraction of bits for which Eve has no information, that is for which $p_{c_0} = 1/2$, is equal to $1-\mu(1-T)/N-e/(N-1/2)$ when she is not equipped with an ideal quantum memory, and $1-2\mu(1-T)-e/(N-1/2)$ when she is. Thus, similarly to Eqs. (3.4) and (3.5) we have derived the privacy amplification shrinking factor:

$$\tau = \begin{cases} 1 - \frac{\mu(1-T)}{N} - \frac{e}{N-1/2} & \text{without quantum memory} \\ 1 - 2\mu(1-T) - \frac{e}{N-1/2} & \text{with quantum memory} \end{cases} \tag{3.12}$$

The above result and Eq. (3.10) are used to compare the performance of a QKD system implementing the DPS-QKD protocol under the assumptions that Eve does and does not possess a quantum memory with an infinitely long coherence time, and with various values for the time delay parameter N. The parameters for the numerical calculations are exactly the same as in the previous section, and the result is shown in Fig. 3.6. The curve for the case of a quantum memory and $N = 1$ corresponds to the curve for the DPS-QKD protocol in Fig. 3.5. As we observe in Fig. 3.6, when Eve is equipped with an ideal quantum memory introducing a time delay parameter N does not have a significant effect on the performance of the system. The beamsplitter attack term in Eq. (3.12), which is independent of N in this case, dominates. However, when a realistic scenario is assumed, where Eve does not possess a quantum memory with an infinitely long coherence time, we observe a significant

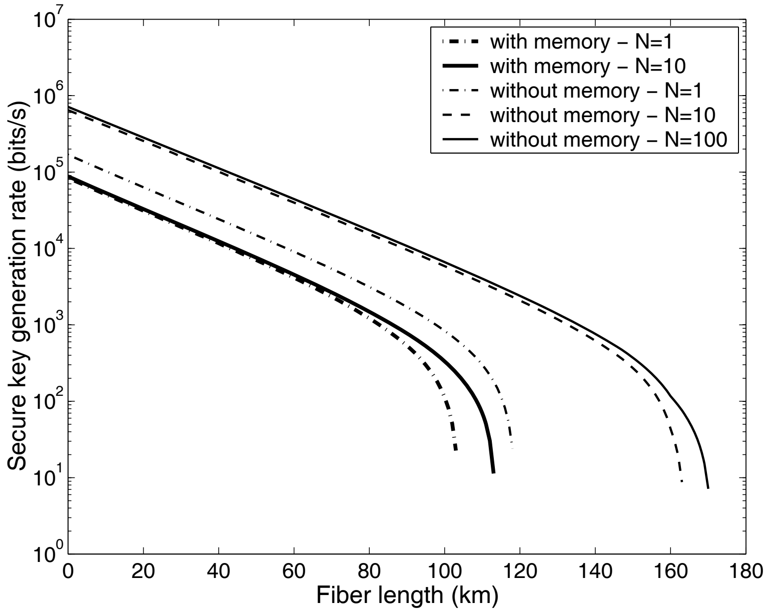

Figure 3.6: Secure key generation rate as a function of fiber length for the DPS-QKD protocol employing time delay parameters N = 1 or 10 when Eve is equipped with an ideal quantum memory and N = 1, 10 or, 100 when she is not.

effect on the performance of the system. Indeed, in this case introducing a time delay parameter N greater than 1 enhances both the secure key generation rate and the communication distance of the system considerably. Nevertheless, the advantage becomes comparatively smaller as N increases to values greater than 10. This result complements the conclusion of the previous section that the DPS-QKD protocol offers the prospect of a simple and practical quantum cryptography system.

3.4 Security proof against general individual attacks

The security proof for the DPS-QKD protocol against restricted attacks gave us all the basic information and intuition required to comprehend the nature of this protocol and the reason why it is secure. However, it is important to prove the security of the protocol against a more general set of eavesdropping attacks. As we discussed in Sec. 2.3.4, in this work we are interested in practical communication systems, we will therefore restrict our discussion only to individual attacks, such as the ones illustrated in Figs. 2.5(a) and 2.8. In these attacks, Eve is assumed to attack individually each photon, which in the DPS-QKD protocol spreads over many pulses with a fixed phase modulation pattern.

We start our analysis by giving a mathematical description of individual attacks. In the DPS-QKD protocol, Alice prepares a state, denoted as $|\psi\rangle$, which is a train of coherent pulses. These pulses are phase modulated by 0 or π, and we denote ϕ_n the phase induced by the phase modulator on a pulse in time slot n. Then, if Alice sends n_p coherent pulses, state $|\psi\rangle$ is written as:

$$|\psi\rangle = \bigotimes_{n=0}^{n_p-1} \left|\alpha e^{i(\phi+\phi_n)}\right\rangle \tag{3.13}$$

where ϕ is the initial phase of the coherent state. In order to rewrite this state so that it describes a series of photons generated at certain time instances rather than a series of coherent state pulses, we define the operator:

$$\hat{\psi}^\dagger = \frac{1}{\sqrt{n_p}} \sum_{n=0}^{n_p-1} e^{i\phi_n} \hat{a}_n^\dagger \tag{3.14}$$

where $\hat{a}_n^\dagger$ is the creation operator for a photon in time slot n. We assume that the time slots do not overlap, so these operators commute with each other. Then, using the representation of the coherent state in the Fock state basis shown in Eq. (2.7) and the properties of the creation operators [14] we can rewrite Eq. (3.13) as follows:

$$|\psi\rangle = \sum_{j=0}^{\infty} \sqrt{P(j)} e^{ij\phi} \frac{\left(\hat{\psi}^\dagger\right)^j}{\sqrt{j!}} |0\rangle = \sum_{j=0}^{\infty} \sqrt{P(j)} e^{ij\phi} |\psi_j\rangle \tag{3.15}$$

In the second part of the above equation we have defined $|\psi_j\rangle = \left(\hat{\psi}^\dagger\right)^j / \sqrt{j!}$. $P(j)$ is a Poisson distribution such as in Eq. (2.8) with an average photon number $n_p\mu$, where $\mu = |\alpha|^2$:

$$P(j) = e^{-n_p\mu} \frac{(n_p\mu)^j}{j!} \tag{3.16}$$

Because we assume that Eve does not possess the phase reference of the source, the state that she actually observes is the state in Eq. (3.15) averaged over the different values of the phase ϕ, which results in the mixed state:

$$\rho_{eve} = \sum_{j=0}^{\infty} P(j) \left|\psi_j\right\rangle \left\langle\psi_j\right| \tag{3.17}$$

We consider now the following eavesdropping strategy. Eve measures the photon number in the n_p-slot wavefunction using a quantum non-demolition (QND) measurement. Then, she sends to Bob $n_p\mu T$ photons, where T is the total transmission efficiency of the quantum channel and Bob's detection setup, and she stores $n_p\mu(1-T)$ photons coherently to be measured after Alice and Bob have revealed all classical information. In the presence of system errors, Eve can also attack the fraction of photons that she has transmitted to Bob by entangling the photons with a probe state. The first component of the eavesdropping strategy corresponds to the photon number splitting attacks in the BB84 protocol, and we will formally show below that the information that Eve can extract from this attack is exactly the same as the one we derived using simple arguments for the beamsplitter attack in Sec. 3.3.1. The second component of the strategy is equivalent to the general optimal measurement attack on single-photon states illustrated in Fig. 2.8 for the BB84 protocol. One simplified attack in this category is the intercept and resend attack we discussed in Sec. 3.3.2. The amount of information that Eve can gain from the general optimal measurement attack was studied in [67], and we will use the result of this study to complete our discussion of the security of the DPS-QKD protocol against general individual attacks.

Our analysis for the photon splitting attack assumes that Eve attacks each photon individually, that is the photons that she has kept are individually stored and measured. This assumption implies that Eve cannot use the measurement result of one photon to refine her measurement on the rest of the photons. Thus, since she has kept $n_p\mu(1-T)$ photons, she has $n_p\mu(1-T)$ copies of the state $\hat{\psi}^\dagger |0\rangle$, which she stores coherently until the detection time instance information is publicly disclosed by Bob. Then, if B is the set of all time instances in which a detection event was observed, and $\bar{B}$ is the set of all other time instances, we can write the state $\hat{\psi}^\dagger |0\rangle$ using Eq. (3.14) as follows:

$$\begin{aligned}\hat{\psi}^\dagger |0\rangle &= \frac{1}{\sqrt{n_p}}\sum_{n=0}^{n_p-1} e^{i\phi_n}\hat{a}_n^\dagger |0\rangle \\ &= \frac{1}{\sqrt{n_p}}\left[\sum_{m\in B} e^{i\phi_m}\left(\hat{a}_m^\dagger + e^{i\Delta\phi_m}\hat{a}_{m+1}^\dagger\right) + \sum_{n\in\bar{B}, n\neq m+1} e^{i\phi_n}\hat{a}_n^\dagger\right]|0\rangle \qquad (3.18)\end{aligned}$$

In the above equation, $\Delta\phi_m$ is the phase difference between two pulses that is revealed from the time instance announcement and can either take the value 0, which corresponds to the detection event recorded by detector 1 and encodes bit 0, or the value π, which corresponds to the event recorded by detector 2 and encodes bit 1. Subsequently, we assume that Eve can apply the unitary transformation $\hat{a}_m^\dagger \rightarrow \left(\hat{0}_m^\dagger + \hat{1}_m^\dagger\right)/\sqrt{2}$ and $\hat{a}_{m+1}^\dagger \rightarrow \left(\hat{0}_m^\dagger - \hat{1}_m^\dagger\right)/\sqrt{2}$, where $\hat{0}_m^\dagger$ and $\hat{1}_m^\dagger$ are orthogonal modes. In this case, the term in parentheses in the first summation of Eq. (3.18) becomes:

$$\begin{aligned}\hat{a}_m^\dagger + e^{i\Delta\phi_m}\hat{a}_{m+1}^\dagger &\rightarrow \frac{1}{\sqrt{2}}\left(\hat{0}_m^\dagger + \hat{1}_m^\dagger\right) + e^{i\Delta\phi_m}\frac{1}{\sqrt{2}}\left(\hat{0}_m^\dagger - \hat{1}_m^\dagger\right) \\ &\rightarrow \frac{1}{\sqrt{2}}\left(1+e^{i\Delta\phi_m}\right)\hat{0}_m^\dagger + \frac{1}{\sqrt{2}}\left(1-e^{i\Delta\phi_m}\right)\hat{1}_m^\dagger \\ &\rightarrow \begin{cases}\sqrt{2}\ \ \hat{0}_m^\dagger & \text{when}\ \ \Delta\phi_m = 0\ \ \text{(bit 0)} \\ \sqrt{2}\ \ \hat{1}_m^\dagger & \text{when}\ \ \Delta\phi_m = \pi\ \ \text{(bit 1)}\end{cases} \qquad (3.19)\end{aligned}$$

Then, the state of each of the photons that Eve has kept is given by the expression:

$$\hat{\psi}^\dagger |0\rangle = \frac{1}{\sqrt{n_p}}\left[\sum_{m\in B} e^{i\phi_m}\hat{x}_m^\dagger + \sum_{n\in\bar{B}, n\neq m+1} e^{i\phi_n}\hat{a}_n^\dagger\right]|0\rangle$$

$$= \frac{1}{\sqrt{n_p}} \left[\sum_{m \in B} e^{i\phi_m} \left| x_m \right\rangle + \sum_{n \in \bar{B}, n \neq m+1} e^{i\phi_n} \left| a_n \right\rangle \right] \tag{3.20}$$

In this equation $\hat{x}^\dagger_m$ is equal to $\hat{0}^\dagger_m$ when Alice has sent bit 0 and $\hat{0}^\dagger_m$ when she has sent bit 1. Also, in the second part we have defined $\left| x_m \right\rangle = \hat{x}^\dagger_m \left| 0 \right\rangle$ and $\left| a_n \right\rangle = \hat{a}^\dagger_n \left| 0 \right\rangle$. This expression shows that Eve's photons are in a superposition of all the bits of the secret key, plus some irrelevant time instances where no photons were detected. Because Eve does not have a phase reference, her state is actually the state in Eq. (3.20) averaged over the different values of the phases ϕ_m, which similarly to Eq. (3.17) leads in the mixed state:

$$\rho_{eve} = \frac{1}{n_p} \left[2 \sum_{m \in B} \left| x_m \right\rangle \left\langle x_m \right| + \sum_{n \in \bar{B}, n \neq m+1} \left| a_n \right\rangle \left\langle a_n \right| \right] \tag{3.21}$$

From the above result, we see that each of the photons that Eve has kept reveals bit information to Eve for each of Bob's detection events with probability $2/n_p$. Then, given that she has kept $n_p\mu(1-T)$ photons and she has transmitted to Bob $n_p\mu T$ photons, we find that Eve's information gain relative to Bob is equal to $(2/n_p) \times n_p\mu(1-T) \times n_p\mu T / n_p\mu T = 2\mu(1-T)$. We have therefore derived the result that using the photon splitting attack Eve gains bit information for a fraction $2\mu(1-T)$ of the bits, which is exactly the same result we found for the beamsplitter attack in Sec. 3.3.1. As we noted in the discussion of that section, for small T the amount of information that Eve gains with the photon splitting attack is independent of the quantum channel loss, contrary to the case of the BB84 protocol with a Poisson source. This indicates robustness of the DPS-QKD protocol to photon number splitting attacks. In other words, this protocol is a lot less sensitive to the photon statistics of the source.

We showed that due to photon splitting Eve can obtain complete information for a fraction $2\mu(1-T)$ of the sifted key. When $T \ll 1$ and μ is small this attack is relatively ineffective for the DPS-QKD protocol. However, as we discussed earlier, in the presence of channel loss Eve can also apply an optimal measurement attack on some of the photons transmitted to Bob. This case was analyzed in [67], where only individual attacks were considered, that is Eve is assumed to attach an individual probe state to each single photon, and then measures the probes independently after all classical information has been revealed. In this analysis, it was shown that the collision probability for each bit p_{c_0} is bounded as follows:

$$p_{\mathrm{c}_0} \leq 1 - e^2 - \frac{(1-6e)^2}{2} \tag{3.22}$$

This equation applies when the error rate is in the range $[0, 6/38]$. The value $e = 6/38$ is the point at which the equation is maximized. When the error rate exceeds this value the collision probability saturates, which means that there is no attack that allows Eve to have complete information on the key. This is in contrast to the BB84 protocol, where from Eq. (2.24) we see that Eve can learn the entire string for example by intercepting each photon Alice sends, storing it and then sending an unpolarized photon to Bob, simultaneously inducing an error rate of $e = 1/2$.

Taking into account the results of the photon splitting and general individual attacks analysis, we find that the average collision probability for the n-bit string is given by the expression:

$$p_{\mathrm{c}} = p_{\mathrm{c}_0}^n = \left[1 - e^2 - \frac{(1-6e)^2}{2}\right]^{n[1-2\mu(1-T)]} \tag{3.23}$$

The privacy amplification shrinking factor in this case is derived using Eq. (2.20):

$$\tau = -\frac{\log_2 p_{\mathrm{c}}}{n} = -\left[1 - 2\mu(1-T)\right]\log_2\left[1 - e^2 - \frac{(1-6e)^2}{2}\right] \tag{3.24}$$

As we observe in the above equation, the factor due to the photon number splitting attack does not enter into the expression due to the optimal measurement attack. This is in contrast to the BB84 protocol, where as we see in Eq. (2.26), the error rate in the optimal measurement attack term is normalized by the fraction of single-photon states β to account for the fact that Eve obtains bit information for the multi-photon states without creating any errors. In the case of the DPS-QKD protocol, however, detection events due to the photon splitting attack occur probabilistically, so Eve cannot increase the error rate on the remainder of the key because she only knows

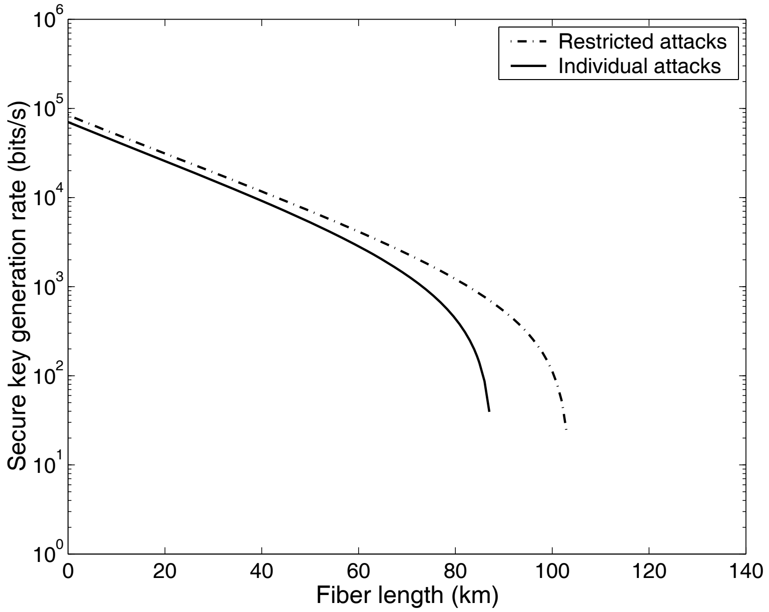

Figure 3.7: Comparison of restricted and general individual attacks in DPS-QKD.

which detection events have given her bit information after the quantum transmission has ended.

The result of Eq. (3.24) completes the security proof of the DPS-QKD protocol against general individual attacks. Using this equation for the general individual attacks, Eq. (3.5) for the restricted attacks, and Eq. (3.10) for the secure key generation rate as a function of the system parameters, we can compare the performance of a QKD system implementing the DPS-QKD protocol for the two types of attacks we have considered. All the system parameters for the numerical calculations are assumed the same as in the previous sections, and the result is shown in Fig. 3.7. This figure shows that the communication rate is always lower for the general individual attacks than it is for the restricted attacks. This is expected because the security proof for the first type of attacks allows Eve to use more sophisticated measurement techniques and gives her the full advantages that quantum mechanics allows; she therefore obtains more bit information and Alice and Bob need to compress their key by a larger fraction in order to guarantee the security of the transmission. Nevertheless, the difference in the performance is not very large. This is due to the fact that the system performance is mostly determined by the robustness of the DPS-QKD protocol to the photon number splitting attacks, which was accounted for in the security analysis against both restricted and general individual attacks.

3.5 Security proof against sequential attacks

In this last section of our security analysis of the DPS-QKD protocol, we consider another type of eavesdropping attack, which we call sequential attack. This type of attack is not an individual attack, that is it does not satisfy the major assumption of the previous section that Eve measures each photon individually and does not use the measurement result on one photon to refine her measurement on the other photons. Thus, the sequential attacks are not accounted for in the security analysis of Sec. 3.4. However, it is a conceptually simple attack and raises a security concern for the DPS-QKD protocol especially at high channel losses, so it is important to analyze the security of the protocol against this type of attack.

The sequential attack is an extension of the intercept and resend attack shown in Fig. 3.4. In this attack, which is illustrated in Fig. 3.8, Eve uses an interferometer identical to Bob's to intercept the pulses that Alice sends to Bob. But now instead of waiting until she measures a single photon and then sending the appropriately prepared state to Bob as she did in the intercept and resend attack, she waits for k consecutive detection events. Whenever such an event occurs, Eve can reconstruct a $k+1$ time-slot state with the correct phase differences applied between the pulses and send it to Bob, as shown in Fig. 3.8 for the case of $k = 3$ consecutive detection events. Of course, the probability of observing k consecutive detection events decreases exponentially with k. If μ is the average number of photons per pulse, then the probability of k consecutive events is μ^k. In order for Eve to avoid being revealed due to a decrease in the count rate, she has to keep this probability as large as Bob's detection probability μT, so:

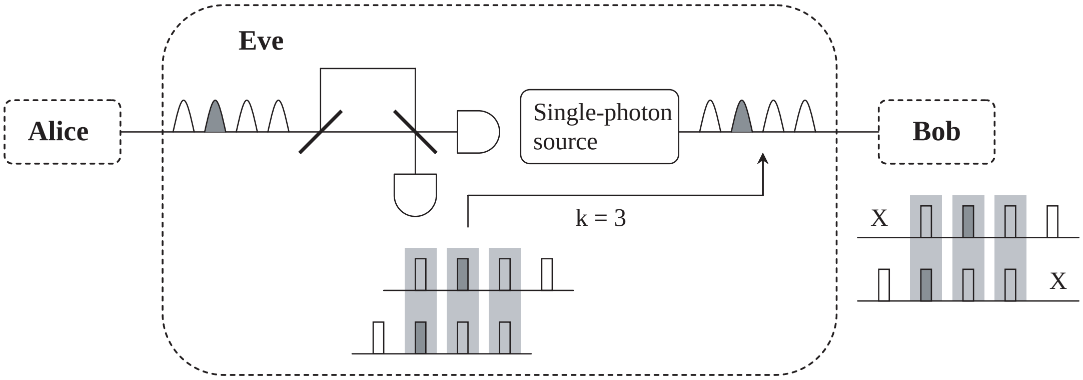

Figure 3.8: Illustration of the sequential eavesdropping attack in DPS-QKD.

$$\mu^k = \mu T \tag{3.25}$$

which means that the following condition must be satisfied:

$$k = \log_\mu T + 1 \tag{3.26}$$

When the reconstructed state arrives at Bob's site, he counts photons possible at $k+2$ time instances, as shown in Fig. 3.8. When Bob measures the central time instances, he does not observe the eavesdropping because he obtains the correct phase difference results. However, with a probability of $1/(k+1)$ he measures the side time instances, which yield uncorrelated results and lead in error with probability $1/2$. Consequently, this attacks induces an overall error rate of:

$$e_{\text{seq}} = \frac{1}{2(k+1)} \tag{3.27}$$

This means that if the system error rate is e, Eve can apply her attack to a fraction $e/e_{\text{seq}} = 2(k+1)e$ of the bits in order not to exceed this error rate. With probability $k/(k+1)$, which is the probability that Bob measures the central time instances, she obtains full information for these intercepted bits, hence $p_{c_0} = 1$ for a fraction $2ke$ of the bits. On the other hand, Eve does not gain any information on the remaining

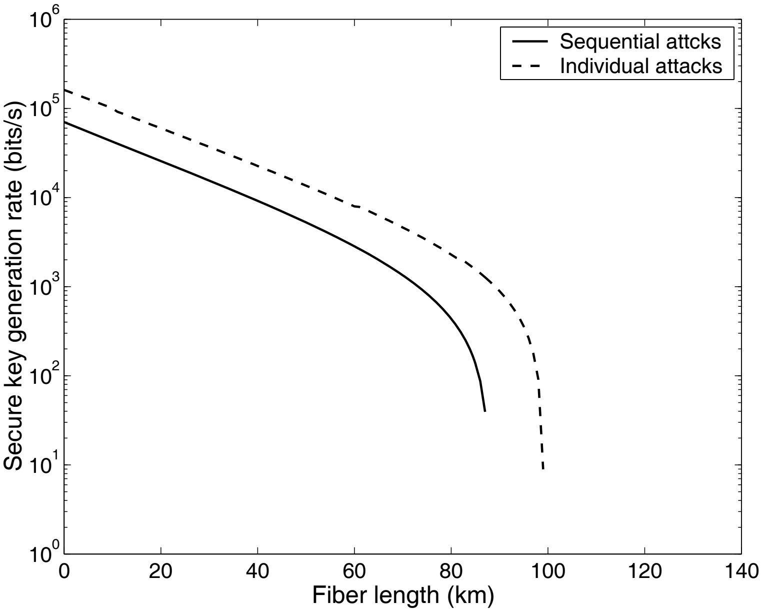

Figure 3.9: Comparison of sequential and general individual attacks in DPS-QKD.

bits, that is $p_{c_0} = 1/2$ for a fraction $1 - 2ke$ of the bits. Thus, the average collision probability for the n-bit long sifted key is given by the expression:

$$p_c = p_{c_0}^n = \left(\frac{1}{2}\right)^{n(1-2ke)} \tag{3.28}$$

Then, the privacy amplification shrinking factor in the case of the sequential attack is derived using Eq. (2.20):

$$\tau = -\frac{\log_2 p_c}{n} = 1 - 2ke = 1 - 2e\left(\log_\mu T + 1\right) \tag{3.29}$$

where for the second part of the above equation we have used the condition of Eq. (3.26). In Fig. 3.9 we compare the performance of a QKD system implementing the DPS-QKD protocol for the cases of general individual and sequential attacks, based on Eqs. (3.24), (3.29), and (3.10). We use the same values for the system parameters as in the previous sections. For the individual attacks, the average photon number per pulse μ is optimized as before for each value of the fiber length. Then, the same optimal value of μ is used to evaluate the secure key generation rate for sequential attacks, in order to compare the effectiveness of the two types of attacks under the same operating conditions. As we can see in Fig. 3.9, the rate for general individual attacks is always lower than the one for sequential attacks, indicating that it is more advantageous for Eve to perform individual attacks rather than sequential attacks. This means that the security against individual attacks implies security against sequential attacks as well. Of course, we do not know if the sequential attacks are optimal, or if a more sophisticated eavesdropping scheme could produce better results for Eve. To answer this question, a more general security proof will be required.

3.6 Summary

In this chapter, we introduced the differential phase shift quantum key distribution protocol, and we discussed the security of this protocol against a set of restricted attacks, general individual attacks including photon splitting attacks, and sequential attacks. The security proofs revealed that the most crucial characteristic of the DPS-QKD protocol is its robustness to photon number splitting attacks. This feature significantly enhances the performance of a QKD system implementing this protocol in terms of both secure key generation rate and communication distance. Most importantly, the DPS-QKD protocol achieves this using a very simple system architecture and practical telecommunication components such as lasers, detectors and linear optics. Thus, it opens the way to the implementation of a simple and practical quantum cryptography system. We will describe the implementation of such systems in Chapters 5 and 6.

The security analysis of the different protocols that we have considered has clearly highlighted the important role that the characteristics of the components of the QKD system play in its performance. On the sender side, we have seen that using an ideal single-photon source can improve the performance of a QKD system implementing the standard BB84 protocol considerably, while a Poisson source such as a laser is sufficient for security in the case of the DPS-QKD protocol. On the receiver side, the dark counts and the quantum efficiency of the single-photon detectors determine the cut-off distance, beyond which secure communication is no longer possible. The single-photon detectors also determine the repetition rate of the experiment, and so the achievable communication rate as well. In all the numerical calculations of Chapters 2 and 3 we have assumed the characteristics of the InGaAs/InP avalanche photodiode (APD), which is usually employed in fiber-optic QKD systems. In the next chapter, we will introduce a new single-photon detector, the up-conversion single-photon detector, and will we show that it presents characteristics more favorable for quantum cryptography than the InGaAs/InP APD.

Chapter 4

The up-conversion single-photon detector

4.1 Introduction

Fast and efficient single-photon detection is essential in many quantum information processing applications that use photonic qubits. Especially in quantum cryptography systems, as we demonstrated in the previous chapters, in addition to the QKD protocol that is being implemented and the photon statistics of the light source, the characteristics of the single-photon detectors, namely the quantum efficiency, the dark counts and the operation mode of the detectors, play a crucial role in determining the performance of the system.

A single-photon detector absorbs a single photon and via an avalanche process produces a macroscopic current that can be detected by subsequent digital circuits. Photomultiplier tubes (PMTs) are often used as single-photon detectors but avalanche photodiodes (APDs) in Geiger mode are the most commonly used detectors. In this mode, the APD is operated with a reverse bias above the device's breakdown voltage in order to achieve very high gain, which enables the detection of single photons. In this case, the signal current of the APD needs to be quickly limited and diminished to control the avalanche and achieve a stable gain. Passive or active current quenching circuits are employed in the device for this purpose. Depending on the semiconductor material used to create the *pn* junction of the photodiode, the detector is sensitive to different wavelength regions. For example, Si has an appropriate bandgap for detection of light in the visible and near-infrared, while Ge and InGaAs/InP are appropriate for detection in the infrared wavelength band.

In the following sections, we will first discuss and compare the characteristics of the most commonly used single-photon detectors, the InGaAs/InP and Si APDs. We will then show that we can use nonlinear optical frequency conversion in waveguides to take advantage of the good characteristics of the Si APDs and achieve fast and efficient single-photon detection in the infrared communication band. We will demonstrate the implementation of the resulting device, the up-conversion single-photon detector, we will discuss its characteristics, and we will show that the use of this detector can considerably enhance the performance of a quantum key distribution system.

4.2 InGaAs/InP and Si avalanche photodiodes

InGaAs/InP avalanche photodiodes are sensitive to light in the infrared wavelength region around 1.5 μm and 1.3 μm, where the standard optical fiber presents its minimum loss and all current telecommunication networks operate. Thus, because of their importance as single-photon detectors in long-distance fiber-optic quantum key distribution systems, these detectors have been the subject of thorough investigation over the last decade.

Although considerable progress has been achieved in the performance of these detectors [55, 68, 69, 70, 71, 72], they present several drawbacks. One such drawback is that they exhibit low quantum efficiency, which is typically on the order of 10%. This number indicates the external quantum efficiency of the device, that is it does not correspond to the percentage of photons generating an electron-hole pair inside the device, which can be very high for InGaAs, but to the percentage of photons triggering a detected avalanching event and so a measurable current outside the device. Therefore, the quantum efficiency depends on both the absorption of light and the collection of charge carriers. In addition to the low quantum efficiency, a serious drawback of InGaAs/InP APDs is that they suffer from after-pulse effects caused by

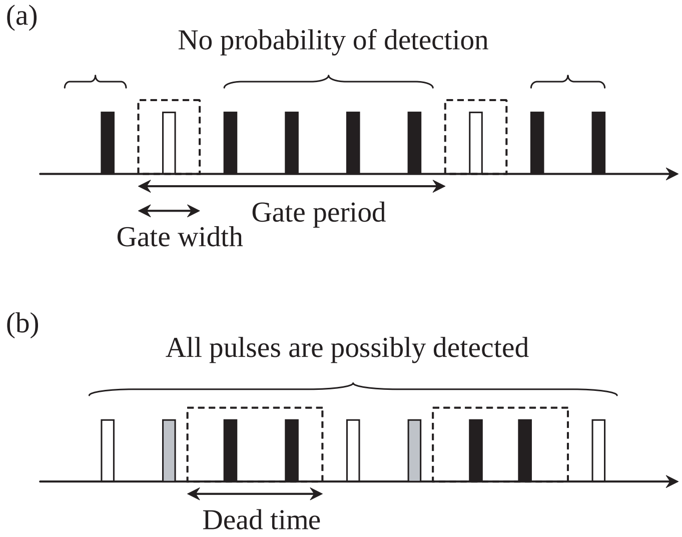

Figure 4.1: Comparison of (a) gated and (b) nongated mode operation of single-photon detectors.

trapped charge carriers, which produce large dark count rates during a relatively long time. The high dark count probability imposes gated Geiger mode operation, which is schematically illustrated in Fig. 4.1(a). When operated in gated mode, the APD device is raised above breakdown threshold for a few nanoseconds, which ensures low probability of a dark count and high efficiency for detecting light. Subsequently, the device is returned to below breakdown for a time long enough for any trapped charge carrier to leak away. Given that the trapping lifetime is on the order of a microsecond, this mode allows operation at megahertz rates. The maximum gate frequency that has been achieved to date with these detectors is 10 MHz [55]. In a QKD application, this gate frequency, or else the inverse of the gate period, determines the repetition rate of the signal pulses. In particular, the detection rate, which is the raw key generation rate in a QKD system, is given by the expression:

$$R_{\mathrm{raw}} = f_{\mathrm{g}} p_{\mathrm{click}} \tag{4.1}$$

where, as in Chapters 2 and 3, p_{click} is defined as the probability of a detection event in a given clock cycle, and f_{g} is the gate frequency. Thus, f_{g} is the repetition rate of the transmission ν that appears for example in Eqs. (2.37) and (3.10), and so it limits the attainable secure key generation rate.

With gated mode operation of the InGaAs/InP APDs, the after-pulse probability is reduced by the ratio of the gate width to the gate period. Even with this improvement, however, the dark count rate remains high in these devices with a typical value of 10^4 counts/s. The dark count rate per measurement time window, a critical parameter for the communication distance in QKD systems, is determined by the gate width, which is limited by the response time of the semiconductor material. Typically, gate widths of 1 ns are used with resulting dark counts on the order of 10^{-5} counts/time window.

Contrary to single-photon detection in the infrared communication band, conventional single-photon detection at visible and near-infrared wavelengths is a very mature technology. Commercially available Si APDs feature very high quantum efficiencies and low dark count rates, typically on the order of 70% at 700 nm and 50 counts/s, respectively. Most importantly, these detectors have very small after-pulse effects, which enables free-running or nongated Geiger mode operation. This operation mode is illustrated in Fig. 4.1(b). In this case, the detection rate of the device, and thus the attainable secure key generation rate in a QKD system, is limited by the dead time of the Si APD, which is on the order of 50 ns for commercial devices. During this time period that follows a detection event, the photodiode cannot respond to subsequent events, and, eventually, a very large photon flux saturates the device. If t_d is the dead time of the detector, the raw key generation rate is written in this case as:

$$R_\mathrm{raw} = \nu p_\mathrm{click} e^{-\nu p_\mathrm{click} t_\mathrm{d}} \tag{4.2}$$

In the above equation, we have assumed that the photodetection events follow a Poisson process, so the probability of two events occurring in a time period larger than t_d is given by the exponential term in the expression. As we will see in the numerical calculations in Sec. 4.4, this saturation factor limits the secure key generation rate at low fiber losses. The nongated mode operation, however, does not impose any severe limitation on the clock frequency ν of the QKD system, which is now only determined

Table 4.1: Comparison of InGaAs/InP and Si APD detector characteristics.

	InGaAs/InP APD	Si APD
Wavelength	1300-1600 nm	500-900 nm
Quantum efficiency (η)	$\sim$ 10%	$\sim$ 70%
Dark count rate (D)	$\sim 10^4$ counts/s	$\sim$ 50 counts/s
After-pulse probability	Large → gated mode	Small → nongated mode

by the speed of the electronic equipment and the Si APD timing jitter. The use of this detector therefore offers the potential of very fast communication.

The basic characteristics of the two types of single-photon detectors we discussed are summarized in Table 4.1. It is clear that Si APD is much more suitable as a single-photon detector in a quantum key distribution system. Unfortunately, this device is not sensitive to light in the wavelength region of interest for long-distance quantum cryptography, so instead InGaAs/InP APDs have been invariably used in such applications. In the next section, we will describe a new detector, the up-conversion single-photon detector, which achieves fast and efficient single-photon detection at telecommunication wavelengths by combining guided-wave frequency up-conversion in a nonlinear crystal and detection by a Si APD.

4.3 The up-conversion single-photon detector

4.3.1 Principle of operation

The idea of using highly efficient nonlinear optical frequency converters in order to achieve single-photon detection in the infrared while taking advantage of the good properties of near-infrared single-photon detectors is the basic principle of the up-conversion single-photon detector. A schematic of this detector for the case of 1.5 μm single-photon detection is shown in Fig. 4.2(a). In this figure we see that a single-photon signal at 1.5 μm interacts with a strong laser beam at 1.3 μm in a waveguide device to produce a 700 nm single-photon idler, which is subsequently detected by a Si APD. The frequency conversion is achieved by the nonlinear process of sum

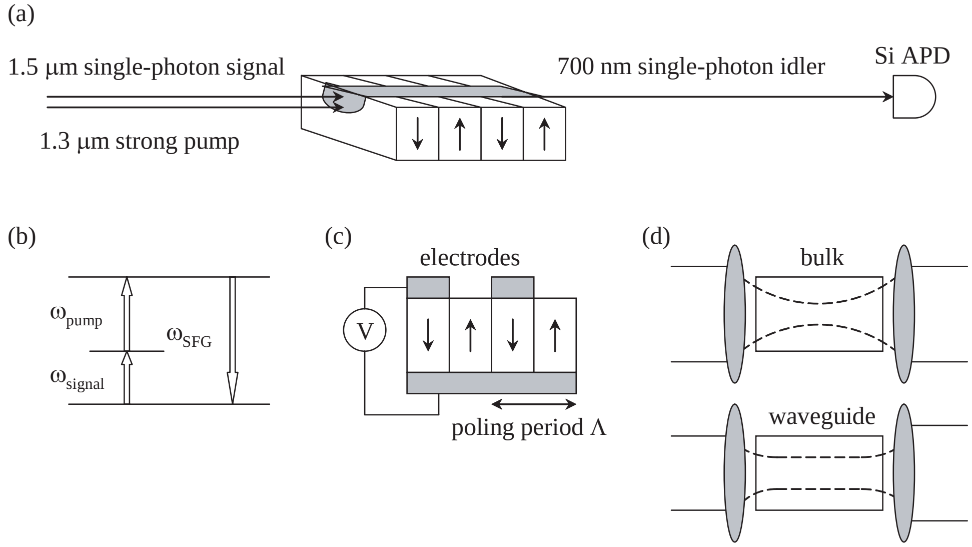

Figure 4.2: Elements of the up-conversion single-photon detector: (a) Basic schematic of the detector; (b) Sum frequency generation nonlinear process; (c) Poling of a lithium niobate crystal; (d) Effective interaction length in a bulk crystal and a waveguide.

frequency generation (SFG). As shown in Fig. 4.2(b), this frequency up-conversion process converts a signal at low frequency ω_{signal} to an idler at high frequency ω_{SFG} by mixing it with a strong pump at a convenient frequency ω_{pump} in a crystal with a $\chi^{(2)}$ nonlinearity. Then, the conservation of energy gives:

$$\omega_{\text{signal}} + \omega_{\text{pump}} = \omega_{\text{SFG}} \tag{4.3}$$

which is satisfied by the wavelengths shown in Fig. 4.2(a). In addition to the energy, the momentum of the interacting fields also has to be conserved during this nonlinear process, which leads to the momentum conservation or phase-matching condition:

$$\boldsymbol{k}_{\text{signal}} + \boldsymbol{k}_{\text{pump}} = \boldsymbol{k}_{\text{SFG}} \tag{4.4}$$

where the bold symbols represent vectors. In most nonlinear crystals, this condition is typically achieved by employing different polarizations for the pump, signal and idler fields. This is called birefrigent phase-matching. A much more interesting way to achieve phase-matching, however, is by using the quasi-phase-matching (QPM) technique [73]. This technique corrects the relative phases of the fields involved in the nonlinear interaction at regular intervals by means of a structural periodicity built into the nonlinear medium. In other words, the phase is reset periodically so that, on average, the proper relationship is satisfied for the growth of the desired field. The required inversion of the phase can be accomplished by changing the sign of the nonlinear coefficient of the material. In ferroelectric materials, such as lithium niobate ($LiNbO_3$), this sign is linked to the direction of the spontaneous electric polarization. Thus, modulation of the nonlinear coefficient and therefore QPM can be achieved by forming regions of periodically reversed electric polarization, which is possible by periodically applying high electric field. This process, called poling, is shown in Fig. 4.2(c). The phase-matching condition in a periodically poled crystal becomes:

$$\boldsymbol{k}_{\text{signal}} + \boldsymbol{k}_{\text{pump}} + \boldsymbol{K} = \boldsymbol{k}_{\text{SFG}} \tag{4.5}$$

where

$$|\boldsymbol{K}| = \frac{2\pi}{\Lambda} \tag{4.6}$$

and Λ is the poling period. The above equation shows that with an appropriate choice of Λ, we can achieve quasi-phase-matching practically for any desired nonlinear interaction between the signal, pump, and idler fields. The major advantage of this technique is that it allows the use of nonlinear coefficients which couple waves of the same polarization and may be much stronger than coefficients used in birefrigent phase-matching. Thus, QPM offers the potential of very efficient nonlinear interactions in crystals.

In addition to quasi-phase-matching, another way to increase the efficiency of the frequency conversion process is to use a guiding structure rather than a bulk crystal. As shown in Fig. 4.2(d), the use of a waveguide permits the tight confinement of the interacting modes over the entire length of the crystal, which can be several centimeters [74], and eliminates diffraction effects. Thus, since the strength of the nonlinear process is proportional to the effective interaction length, a much higher

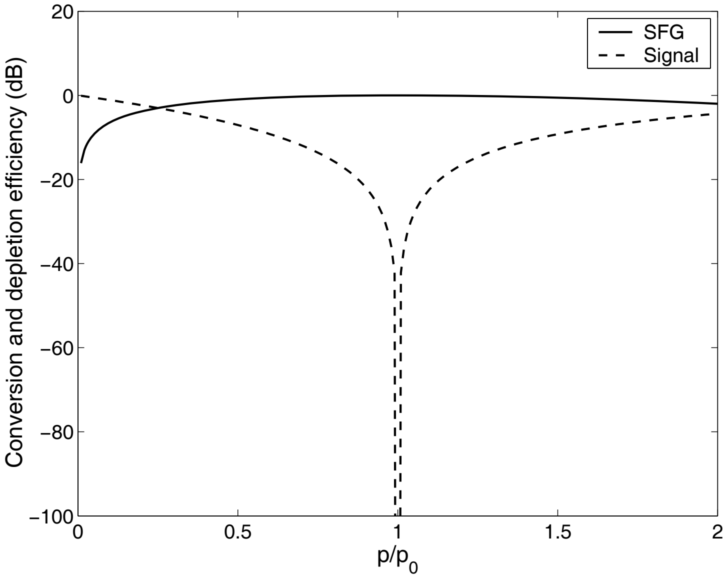

Figure 4.3: Theoretical prediction for the signal conversion and depletion efficiency as a function of the normalized pump power.

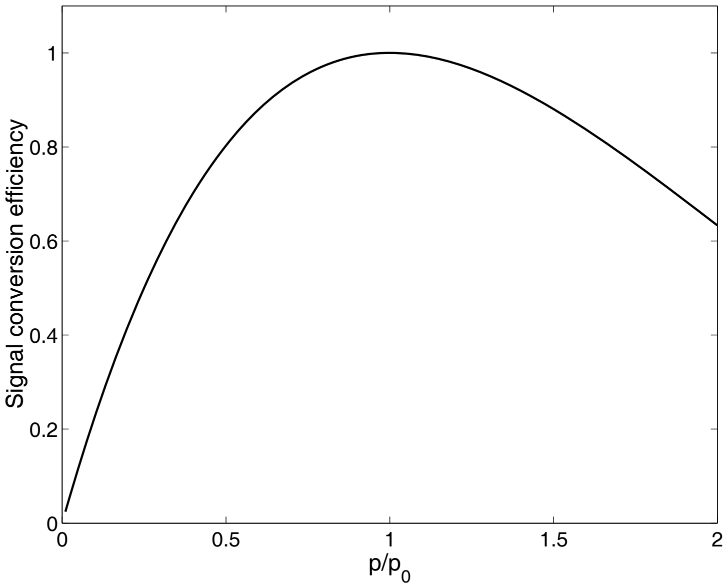

Figure 4.4: Theoretical prediction for the signal conversion efficiency, or else the internal quantum efficiency of the waveguide device, as a function of the normalized pump power.

signal conversion efficiency can be achieved in a waveguide than in a bulk nonlinear crystal.

The above discussion demonstrates that very efficient frequency up-conversion is possible in periodically poled nonlinear waveguides. In more quantitative terms, the analytical solution of the coupled-mode equations describing three-wave interactions inside waveguides in the absence of propagation losses and pump-wave depletion is given in [74]. Under these assumptions, the signal conversion efficiency, which is the internal quantum efficiency of the waveguide device, can be expressed as:

$$\eta_{\text{internal}} = \frac{N_{\text{SFG}}(L_{\text{WG}})}{N_{\text{signal}}(0)} = \sin^2\left(\sqrt{\eta_{\text{nor}} p} L_{\text{WG}}\right) \tag{4.7}$$

where N is the photon number, η_{nor} the normalized power efficiency in the low-gain limit, L_{WG} the effective interaction length, and p the pump power. Maximum conversion is achieved when the pump power is equal to:

$$p_0 = \frac{\pi^2}{4\eta_{\text{nor}} L_{\text{WG}}^2} \tag{4.8}$$

The signal conversion efficiency as well as the signal depletion efficiency, which is simply equal to $1 - \eta_{\text{internal}}$, are plotted as a function of the normalized pump power p/p_0 in Fig. 4.3 in logarithmic scale, while Fig. 4.4 shows the signal conversion efficiency in linear scale. It is clear from these figures that a waveguide structure allows 100% signal conversion efficiency. This means that the internal quantum efficiency of the waveguide device is limited only by propagation losses, while the external quantum efficiency is further reduced by coupling and reflection losses. Finally, the overall quantum efficiency of the up-conversion single-photon detector has to take the optical collection efficiency and the Si APD's intrinsic quantum efficiency into account. Assuming that the propagation losses are equal to α_{WG} for both the signal and SFG wavelengths, the overall quantum efficiency is given by the expression:

$$\eta_{\text{up}} = \eta_{\text{internal}} T_{\text{WG}} T_{\text{CS}} \eta_{\text{Si APD}} \tag{4.9}$$

where

$$T_{\mathrm{WG}} = T_{\mathrm{in}}^{\mathrm{signal}} e^{-\alpha_{\mathrm{WG}} L_{\mathrm{WG}}} T_{\mathrm{out}}^{\mathrm{SFG}} \tag{4.10}$$

is the signal power transmission efficiency through the waveguide of length L_{WG}, and T_{CS} is the SFG transmission efficiency through the optical collection system. These transmission efficiencies, ideally unity, are reduced by the nonunity coupling $T_{\mathrm{in}}^{\mathrm{signal}}$ of the signal wavelength at the waveguide input owing to Fresnel reflections and modal mismatch and at the waveguide output by Fresnel reflections $T_{\mathrm{out}}^{\mathrm{SFG}}$ at the sum frequency wavelength, as well as propagation losses.

The above expressions show that the quantum efficiency of the up-conversion single-photon detector is determined by the Si APD, the frequency conversion efficiency, which is a function of the pump power as shown in Eq. (4.7), and the losses of the optical setup and the waveguide. On the other hand, the dark count rate is determined by the Si APD and parasitic nonlinear interactions inside the nonlinear crystal, which we will discuss in detail in Sec. 4.3.4. Finally, the use of the Si APD allows for nongated mode operation of the up-conversion detector, which makes this detector suitable for high speed fiber-optic quantum cryptography systems.

4.3.2 1.55 μm single-photon detection experiment

The experimental setup for the implementation of a 1.55 μm up-conversion single-photon detector is shown in Fig. 4.5. A highly attenuated continuous wave signal at 1.55 μm generated by an external-cavity tunable diode laser (ECDL) is combined with a strong pump at 1.32 μm generated by a fiber-coupled nonplanar ring oscillator (NPRO), in a wavelength division multiplexer (WDM), and injected into a fiber-pigtailed periodically poled lithium niobate (PPLN) waveguide device. The integration of the waveguide on the PPLN substrate is achieved using the reverse proton exchange (RPE) procedure [75]. The waveguide is 5 cm long and designed for sum frequency generation at the appropriate wavelengths of 1.55 μm and 1.32 μm [74]. In order to avoid beam distortion due to photorefractive damage [76], the waveguide is heated to 75°C in a temperature-controlled oven. Because the nonlinear coefficient of the waveguide material and so the condition for which maximum conversion

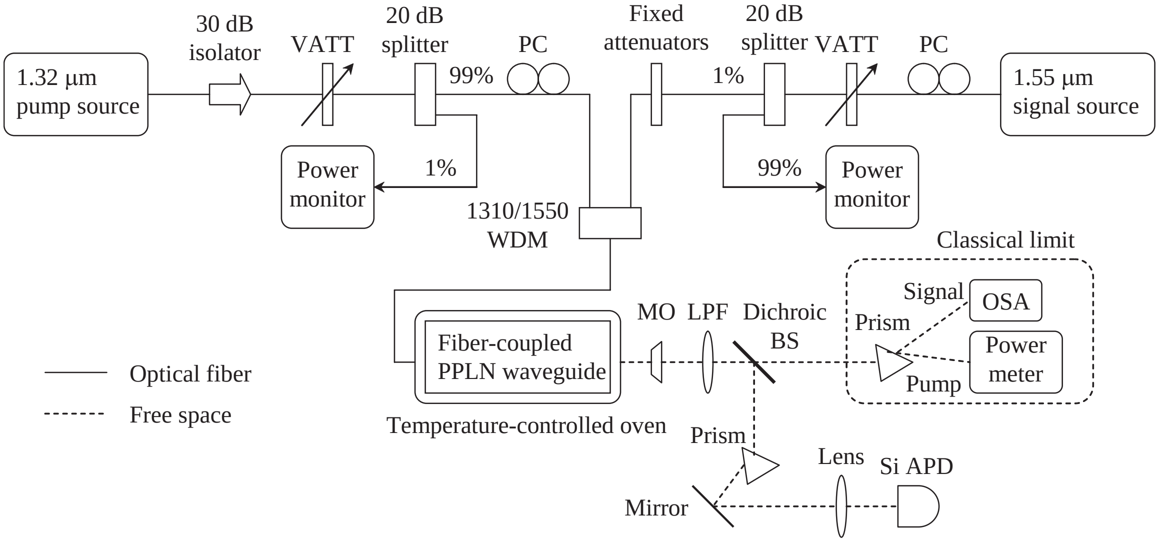

Figure 4.5: Experimental setup for single-photon detection at 1.55 μm. VATT, variable attenuator; PC, polarization controller; WDM, wavelength division multiplexer; MO, microscope objective; LPF, long-pass filter; BS, beamsplitter; OSA, optical spectrum analyzer.

efficiency is achieved depends on the waveguide temperature, this temperature control also serves the purpose of slightly adjusting the performance of the waveguide device when necessary. After the waveguide, the 715 nm SFG single-photon output goes through a series of filters, which are used to suppress the noise photons such as the residual pump and second harmonic generation (SHG) of the pump light. More specifically, a dichroic beamsplitter is used to separate the residual pump and signal light from the SFG output. These beams are directed to a setup used only in the high-power classical limit in order to determine the specific signal wavelength and pump power conditions where maximum signal depletion is achieved. In the path of the SFG light, a long-pass filter and a prism are used to suppress the SHG of the pump. Finally, the SFG single-photon signal is detected by a single-photon counting module (SPCM) based on a Si APD.

The experimental results for the main characteristics of the 1.55 μm up-conversion single-photon detector, namely the quantum efficiency η_{up} and the dark count rate D_{up}, are shown in Figs. 4.6 and 4.7, respectively, as a function of the coupled pump power. To calculate the values for the quantum efficiency, the loss of the fixed attenuators in Fig. 4.5 is carefully calibrated using a 20 dB splitter and a fiber-coupled power meter so that the number of signal photons that enter the WDM coupler is known. Then, the number of counts detected by the SPCM after substraction of the dark counts and correction for the nonlinearity of the device at high count rates, is divided by the number of signal photons before the WDM to give the quantum efficiency values shown in Fig. 4.6. Thus, these values include all loss terms and the intrinsic Si APD quantum efficiency, and they correspond to the overall quantum efficiency of the up-conversion single-photon detector. The signal conversion efficiency of the infrared light to the SFG output, that is the internal quantum efficiency of the waveguide device, exceeds 99.9% with a coupled pump power of about 100 mW, which corresponds to p_0 of Eq. (4.8). This efficiency drops to 83% when propagation losses are included, and further to 65% when input coupling, output coupling, fiber pigtail, reflection, and optical setup losses are taken into account. Finally, including the Si APD quantum efficiency, the maximum overall up-conversion single-photon detector quantum efficiency achieved is 46%, as shown in Fig. 4.6. In agreement with the coupled mode theory for three-wave interactions in a waveguide, which predicts a $\sin^2$ dependence of η_{up} on the pump power p as shown from Eqs. (4.7) and (4.9), the fitting curve of the experimental results is given by the following expression:

$$\eta_{\mathrm{up}}(p) = a_1 \sin^2\left(\sqrt{a_2 p}\right) \tag{4.11}$$

where $a_1 = 0.465, a_2 = 79.75$, and p is given in mW.

As we can see in Fig. 4.7, the dark count rate at the maximum quantum efficiency is 8×10^5 counts/s. The dark counts increase approximately quadratically with the pump power, and they are dominated by spurious nonlinear interactions inside the waveguide that we will describe in Sec. 4.3.4. A more accurate polynomial fitting curve for the experimental results shown in Fig. 4.7 is given by the following expression:

$$D_{\mathrm{up}}(p) = b_0 + b_1 p + b_2 p^2 + b_3 p^3 + b_4 p^4 \quad \text{(counts/s)} \tag{4.12}$$

where $b_0 = 50$, $b_1 = 826.4$, $b_2 = 110.3$, $b_3 = -0.403$, $b_4 = 0.00065$.

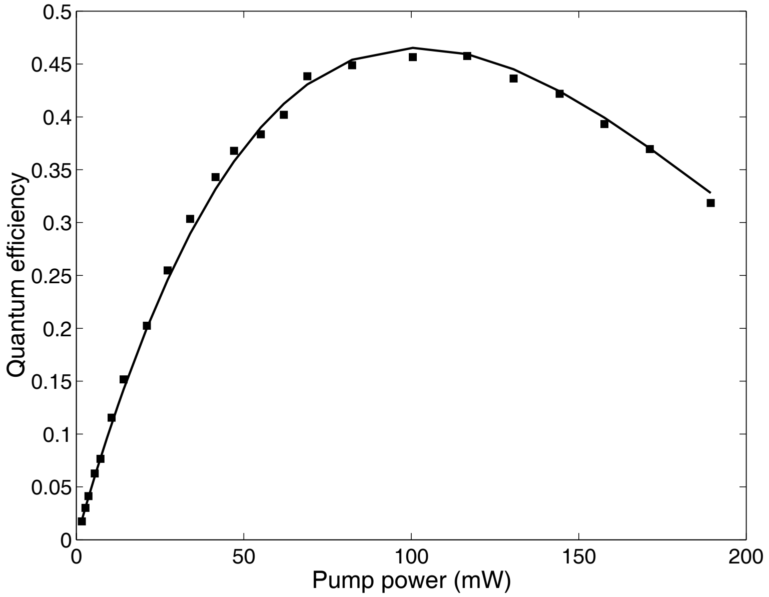

Figure 4.6: Quantum efficiency of the 1.55 μm up-conversion single-photon detector as a function of pump power. The expression for the fitting curve is given by Eq. (4.11).

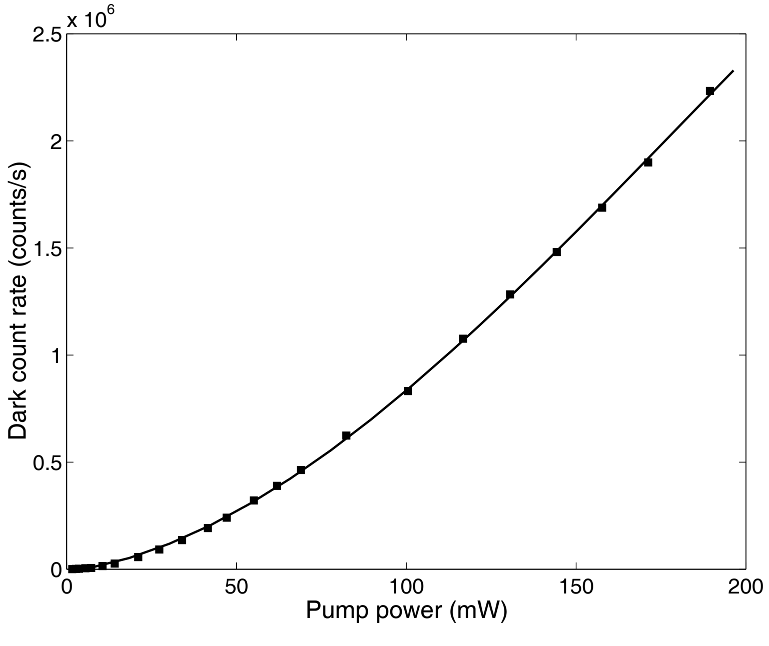

Figure 4.7: Dark count rate of the 1.55 μm up-conversion single-photon detector as a function of pump power. The expression for the fitting curve is given by Eq. (4.12).

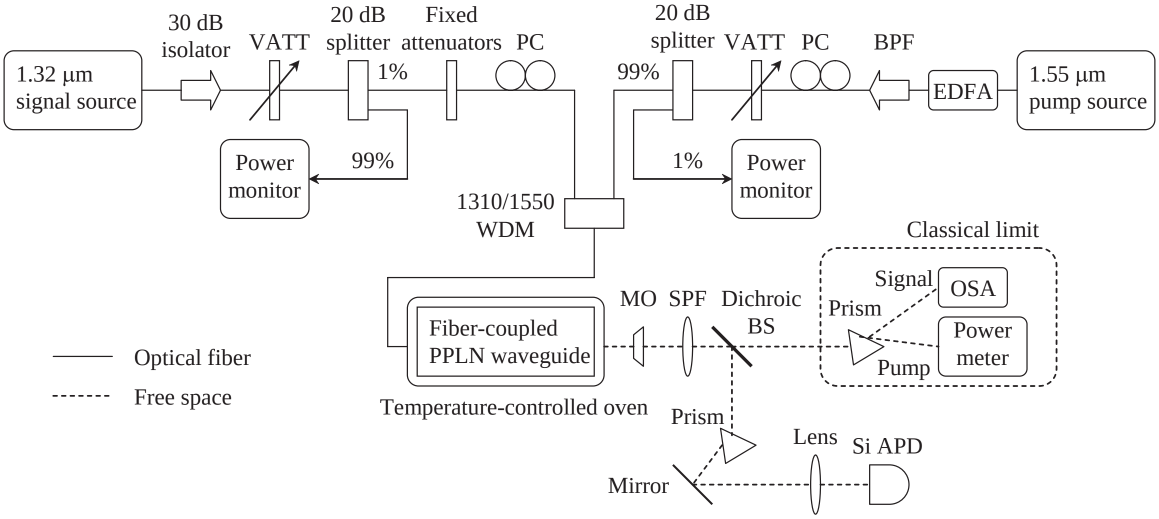

Figure 4.8: Experimental setup for single-photon detection at 1.32 μm. VATT, variable attenuator; PC, polarization controller; BPF, band-pass filter; EDFA, erbium-doped fiber amplifier; WDM, wavelength division multiplexer; MO, microscope objective; SPF, short-pass filter; BS, beamsplitter; OSA, optical spectrum analyzer.

4.3.3 1.32 μm single-photon detection experiment

The experimental setup employed for single-photon detection at 1.55 μm can be slightly modified to enable single-photon detection at the second telecommunication window around 1.32 μm. The corresponding experimental setup is shown in Fig. 4.8. In this case, the ECDL is combined with an erbium doped fiber amplifier (EDFA) to produce sufficient pump power at 1.55 μm, while the 1.32 μm is highly attenuated to serve as the single-photon signal light. Furthermore, the long-pass filter is replaced by a short-pass filter to suppress the SHG of the pump light.

The experimental results for the quantum efficiency and dark count rate of the 1.32 μm up-conversion single-photon detector are shown in Figs. 4.9 and 4.10, respectively, as a function of the coupled pump power. The values for the quantum efficiency are calculated as before, and the fitting curve is given in this case by the expression:

$$\eta_{\mathrm{up}}(p) = a_1 \sin^2\left(\sqrt{a_2 p}\right) \tag{4.13}$$

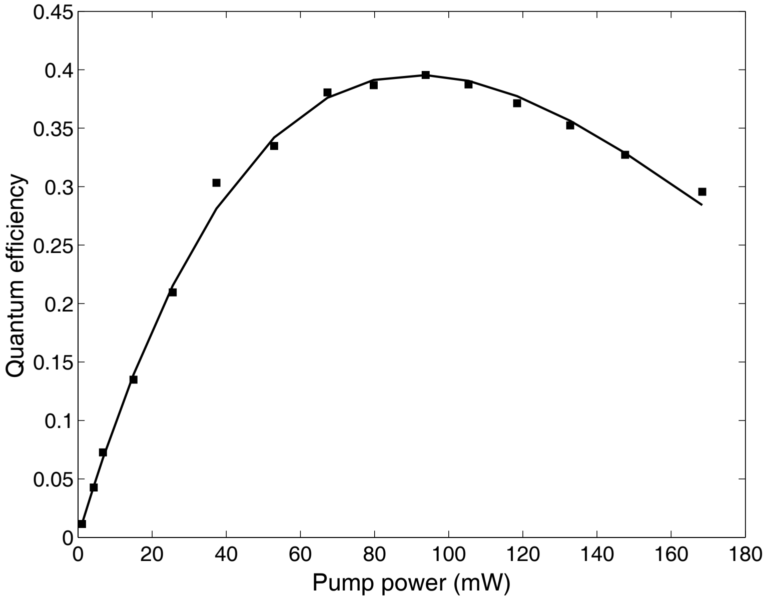

Figure 4.9: Quantum efficiency of the 1.32 μm up-conversion single-photon detector as a function of pump power. The expression for the fitting curve is given by Eq. (4.13).

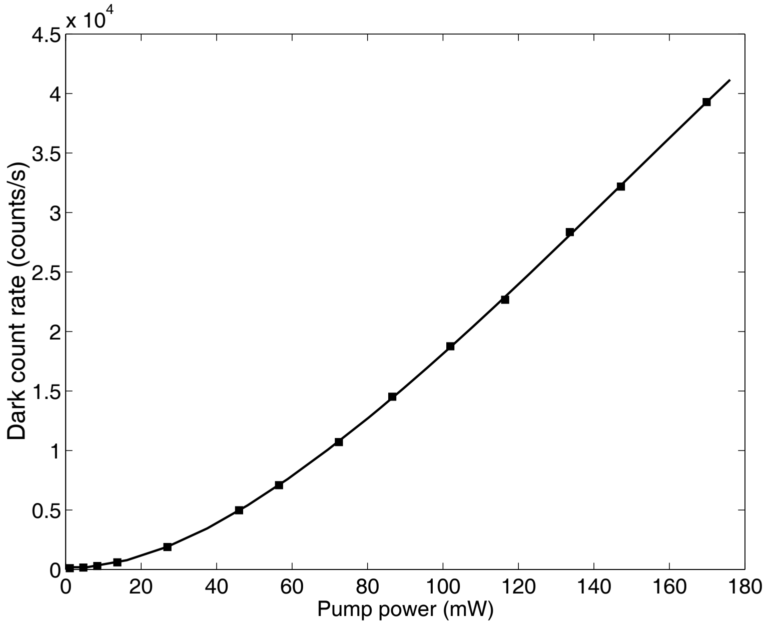

Figure 4.10: Dark count rate of the 1.32 μm up-conversion single-photon detector as a function of pump power. The expression for the fitting curve is given by Eq. (4.14).

where $a_1 = 0.396, a_2 = 88.46$, and p is given in mW. The maximum overall quantum efficiency achieved is 40%. The difference in quantum efficiency with the 1.55 μm case can be explained by the transmission characteristics of the filters used in the two setups. In particular, the transmission of the short-pass filter at the SFG wavelength used in the 1.32 μm detection setup is 8% lower than the transmission of the long-pass filter used in the 1.55 μm detection setup.

As we can see in Fig. 4.10, the dark count rate at the maximum quantum efficiency is 2×10^4 counts/s. The dark counts increase again approximately quadratically with the pump power, but in general their values are smaller in this experiment than in the 1.55 μm case. This will be explained in the discussion about the dark counts origin in Sec. 4.3.4. A polynomial fitting curve for the experimental results shown in Fig. 4.10 is given by the following expression:

$$D_{\mathrm{up}}(p) = b_0 + b_1 p + b_2 p^2 + b_3 p^3 + b_4 p^4 \quad \text{(counts/s)} \tag{4.14}$$

where $b_0 = 80$, $b_1 = 4.45$, $b_2 = 2.65$, $b_3 = -0.01$, $b_4 = 0.00002$.

The implementations of the up-conversion single-photon detector that we described show that very efficient single-photon detection in high speed nongated mode is possible at the standard communication wavelength bands around 1.5 μm and 1.3 μm using this device. Improvements of the up-conversion single-photon detector in order to achieve even better performance include use of antireflection coatings to reduce the Fresnel reflections off the waveguide end facets, and better design and fabrication of the PPLN waveguide device to reduce the propagation and coupling losses, as well as the required pump power for maximum signal conversion. Since the dark count rate strongly depends on the pump power, as we see from Figs. 4.7 and 4.10, the latter improvement will also greatly reduce the dark counts, which is very important for QKD applications.

Other experimental implementations of the up-conversion detector scheme use a different wavelength configuration for sum frequency generation, and a bulk PPLN crystal inserted into a cavity in order to achieve the required pump power level for efficient signal conversion [77, 78]. The quantum efficiencies and dark counts achieved in these experiments are similar to the results presented in this and the previous section. The up-conversion single-photon detector that we described, however, has the advantage of a very compact and robust design with single-pass operation that requires low pump power. Finally, in addition to the InGaAs/InP APD that we described extensively in Sec. 4.2, another important candidate for single-photon detection in the infrared is the superconducting transition-edge sensor (TES) [79]. This detector features extremely low dark count rates, limited only by the background light, but its operation requires cryogenic cooling and the maximum count rate it can withstand is 20 kHz. These characteristics limit the detector's usefulness for practical implementations, although further improvements can make it a promising alternative single-photon detector for long-distance quantum cryptography systems.

4.3.4 Dark counts origin and behavior

Figs. 4.7 and 4.10 reveal that the dark count rate of the up-conversion single-photon detector is not determined by the dark count rate of the Si APD as was initially expected but rather by a parasitic process strongly dependent on the pump power. In order to determine the nature of this process, the output of the waveguide when only the pump light enters the device is spectrally resolved using a spectrometer.

One spectral feature that is clearly present is generated by the SHG of the pump and appears at about 660 nm in the case of the 1.55 μm single-photon detector, which uses a pump at 1.32 μm. The spectrum of this peak is shown in Fig. 4.11. In the up-conversion single-photon detector the potential dark counts due to this peak are eliminated with the use of the long-pass filter or short-pass filter for the 1.32 μm single-photon detection case, and the prism shown in Figs. 4.5 and 4.8. Another spectral feature appears at about 808 nm and is due to the pump diodes of the 1.32 μm pump laser for the 1.55 μm detector. These peaks, shown in Fig. 4.12, are eliminated with the use of the optical isolator shown in Fig. 4.5. Finally, the spectral analysis of the output reveals a third spurious peak that is present at exactly the same wavelength as the SFG output, so it cannot be eliminated by external filtering and appears to be intrinsic to the device. The spectrum of this peak as well as the

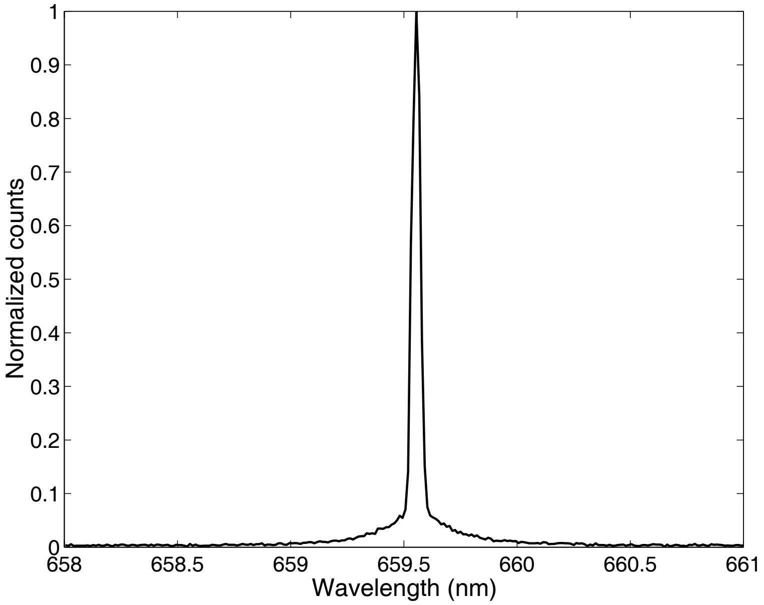

Figure 4.11: Spectrum of the SHG of the pump.

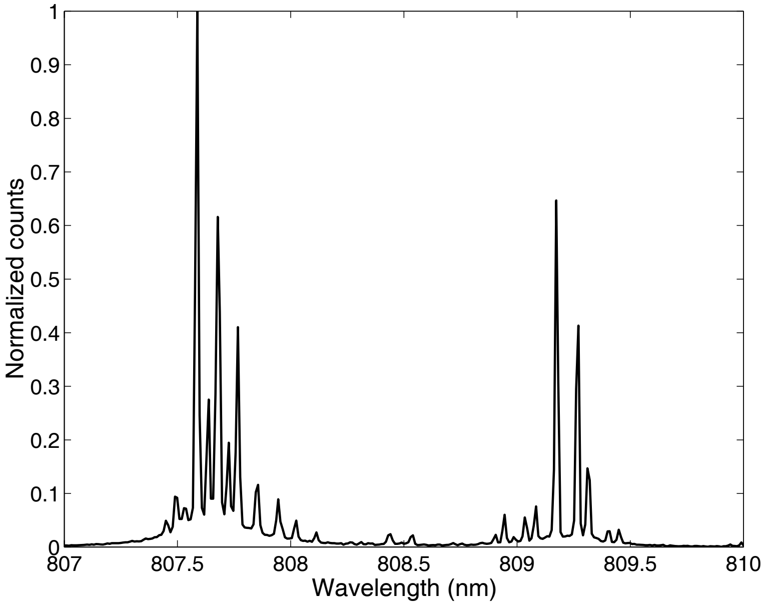

Figure 4.12: Spectrum of the pump diodes.

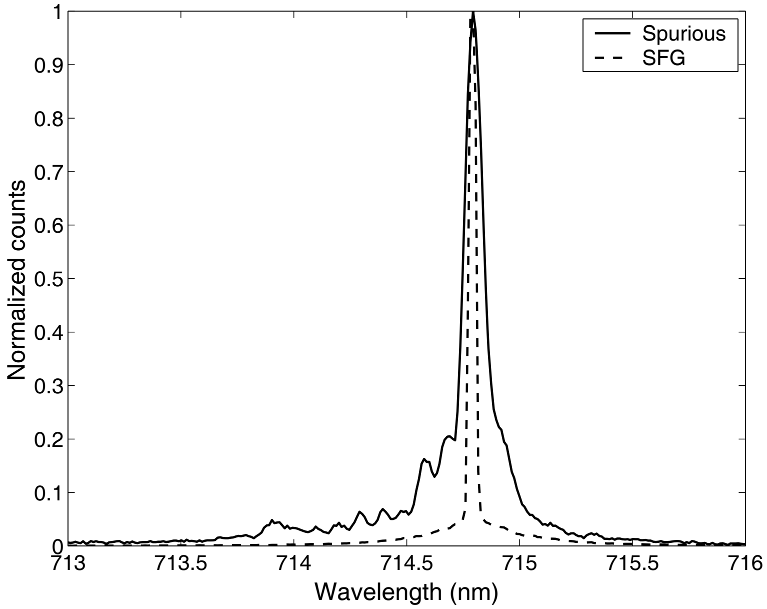

Figure 4.13: Spectra of the spurious and SFG output peaks.

SFG spectrum are shown in Fig. 4.13.

One possible origin of the spurious peak that causes the high dark count rate is the following combined nonlinear process. Initially, the pump photons are scattered by the phonons of both the PPLN waveguide and the fiber pigtail leading to the waveguide via a spontaneous Ramam scattering (SRS) process. A schematic illustration of the SRS process is shown in Fig. 4.14, where two cases have been considered, namely the Stokes and anti-Stokes cases. The first case is relevant for the 1.55 μm up-conversion detector, since in this scenario the pump photons at a high frequency interact with the phonons of the material, and the SRS process generates a spectrum of Stokes photons, which includes the lower frequency of the signal photons. Subsequently, the noise photons interact with the pump photons in the PPLN waveguide via the phase-matched sum frequency generation process, and create dark counts. On the other hand, in the case of the 1.32 μm detector, the pump photons at a low frequency interact with the phonons to generate a spectrum of anti-Stokes photons, which includes the higher frequency of the signal photons. Again, the noise photons are up-converted through the SFG process and create dark counts. In this scenario,

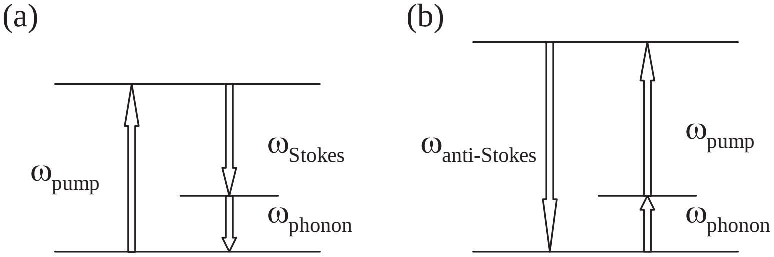

Figure 4.14: Schematic of the (a) Stokes and (b) anti-Stokes spontaneous Raman scattering nonlinear processes.

however, for the nonlinear process to occur the phonons have to be in an excited vibrational state, which make this process less efficient. More specifically, if N_{pump} is the number of pump photons, B_{d} the detection bandwidth, L the length of the medium where the SRS process occurs, and g the gain of the SRS nonlinear process, the number of generated SRS noise photons is given by the expression:

$$N_{\text{SRS}} = B_{\text{d}} N_{\text{pump}} g L \tag{4.15}$$

The scattering gains for the Stokes and anti-Stokes case are related as follows:

$$g_{\text{anti-Stokes}} = g_{\text{Stokes}} e^{-\frac{h\Delta f}{k_B T}} \tag{4.16}$$

where the exponential term is simply the thermal occupation factor for the excited vibrational state. For $T = 75$°C and $\Delta f = 35$ THz, which corresponds to the frequency difference between the pump and signal wavelengths, this occupation factor is approximately equal to 10^{-2}, which means that the number of noise photons is reduced in the anti-Stokes case by two orders of magnitude. This is actually the difference in the dark count rates that we observe in the corresponding experimental results for the 1.55 μm and 1.32 μm up-conversion detectors in Figs. 4.7 and 4.10. Therefore, the experimental data support the theory that we have described for the origin of the dark counts. Furthermore, Eq. (4.15) shows that the SRS process scales linearly with the pump power, so the quantity N_{signal} in Eq. (4.7), which now corresponds to the noise signal photons generated by spontaneous Raman scattering, is a linear function of p. Therefore, in the low gain limit, the number of SFG photons due to this parasitic combined nonlinear process scales approximately quadratically with the pump power. This dependence is observed in Figs. 4.7 and 4.10, while more accurate polynomial fitting curves are given in Eqs. (4.12) and (4.14).

Another possible origin of dark counts that has been discussed as a potential source of large dark counts in other implementations of the up-conversion single-photon detector [77, 78] is a potentially phase-matched parametric fluorescence process, followed by up-conversion of the noise signal photons. In this process, in the case of the 1.55 μm detector, the 1.32 μm pump photons convert spontaneously to photons at the signal wavelength of 1.55 μm, which are subsequently up-converted via sum frequency generation and create dark counts, and idler photons at an appropriate wavelength that satisfies the energy conservation condition, which in this case is equal to 8.9 μm. This parametric fluorescence process also invokes an approximately quadratic dependence of the dark counts on the pump power. However, the strong absorption in lithium niobate of the 8.9 μm idler photons associated with this process suggests that the efficiency of such a process is negligible, and so the combined process involving spontaneous Raman scattering described above most probably dominates the generation of dark counts. This conclusion suggests that a significant reduction in the dark count rate of the 1.55 μm up-conversion single-photon detector can be achieved by minimizing the spurious nonlinear effects inside the device, for example by choosing a pump wavelength longer than the signal wavelength.

An important feature of the up-conversion detector stems from the fact that the dark counts depend on the bandwidth of the waveguide, which determines the number of noise photons, as we can see from Eq. (4.15). In order to illustrate this feature, let us define the following quantity:

$$D_{\mathrm{up\ Hz}} = \frac{D_{\mathrm{up}}}{B_{\mathrm{d}}} \tag{4.17}$$

for a detector with bandwidth B_{d} and dark count rate D_{up}. This quantity has units counts/(s Hz), and corresponds to the optical dark counts per mode. Then, we can think of the ideal communication system employing the up-conversion detector shown

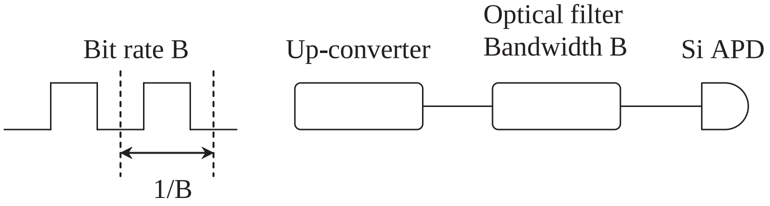

Figure 4.15: Ideal communication system employing an up-conversion single-photon detector.

Table 4.2: Definitions of the dark count quantities for the up-conversion detector and the InGaAs/InP APD.

	Up-converter	InGaAs/InP APD
Dark count rate (counts/s)	D_{up}	D_{APD}
Dark counts per mode [counts/(s Hz)]	$D_{\mathrm{up\ Hz}} = \frac{D_{\mathrm{up}}}{B_{\mathrm{d}}}$	–
Dark counts per time window	$d_{\mathrm{up}} = D_{\mathrm{up\ Hz}}$	$d_{\mathrm{APD}} = D_{\mathrm{APD}} \frac{1}{B}$

in Fig. 4.15, which operates at a bit rate B, and uses a matched filter with bandwidth equal to B that follows the up-converter, and a measurement time window equal to $1/B$. In such a system, the dark counts per time window d_{up}, a parameter of great importance in QKD applications as we have seen in Chapters 2 and 3, is equal to:

$$d_{\mathrm{up}} = B D_{\mathrm{up\ Hz}} \frac{1}{B} = D_{\mathrm{up\ Hz}} \tag{4.18}$$

The above equation shows that d_{up} is independent of the bit rate B (or measurement time window $1/B$) under this optimum filtering. On the other hand, in the case of an InGaAs/InP APD operated in gated mode, the gate width is equal to $1/B$ and so the dark counts per time window d_{APD} is given by:

$$d_{\mathrm{APD}} = D_{\mathrm{APD}} \frac{1}{B} \tag{4.19}$$

where D_{APD} (counts/s) is the dark count rate of the InGaAs/InP APD.

Table 4.2 summarizes the definitions of the dark count quantities that we have introduced. In Fig. 4.16 the quantities d_{up} and d_{APD} are plotted as a function of the bit rate. For the InGaAs/InP APD, the typical value $D_{\mathrm{APD}} = 10^4$ counts/s is used.

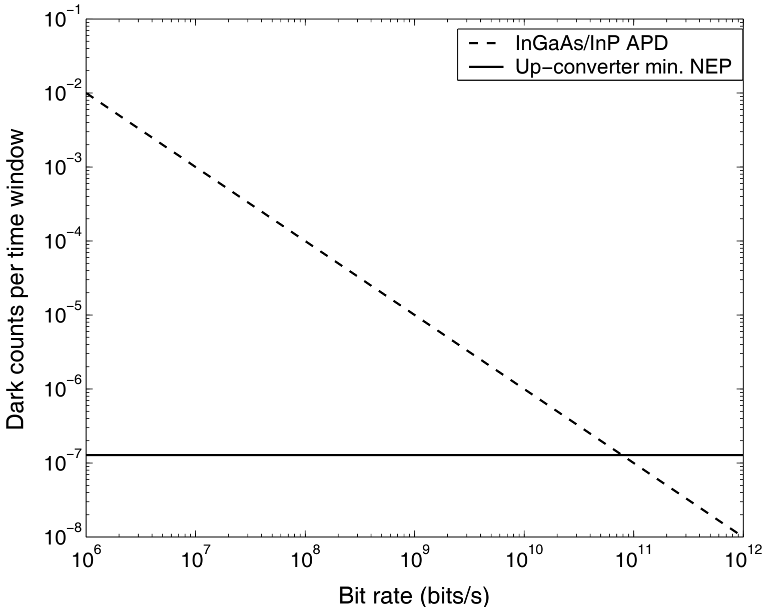

Figure 4.16: Dark counts per time window for the up-conversion single-photon detector operating at the minimum NEP regime, and a typical InGaAs/InP APD respectively, in an ideal communication system.

For the up-conversion detector, we calculate the quantity $D_{\mathrm{up\ Hz}}$ at the operating point of the detector, where the Noise Equivalent Power (NEP) is minimized. NEP is defined as $h\nu\sqrt{2D}/\eta$, where $h\nu$ is the energy of the signal photon, and it characterizes the sensitivity of a detector, so it is often used as a figure of merit for photodetectors in optical communications. The normalized NEP is defined as $\sqrt{2D}/\eta$, and for the 1.55 μm up-conversion detector it takes its minimum value for $D_{\mathrm{up}} = 6.4 \times 10^3$ counts/s and $\eta_{\mathrm{up}} = 0.075$. Then, given a bandwidth of $B_{\mathrm{d}} = 50$ GHz for the up-converter, we find from Eqs. (4.17) and (4.18) that the optimum d_{up} is $\sim 1.3 \times 10^{-7}$, as shown in Fig. 4.16. This result illustrates the significant advantage of the up-conversion detector over the InGaAs/InP APD in terms of reduced dark counts per time window, for most practical system bit rates.

The dependence of the dark counts on the waveguide bandwidth, together with the nongated mode operation of the Si APD and the pump power dependence of the detector characteristics, have a significant effect on the performance of a quantum cryptography system employing up-conversion detectors, as we will see in the next section.

4.4 Performance of QKD systems with up-conversion detectors

To illustrate the advantage that the up-conversion detector characteristics present for quantum cryptography, we compare the performance of fiber-optic quantum key distribution systems implementing the BB84, BBM92, and DPS-QKD protocols, when these systems employ the 1.55 μm up-conversion single-photon detector described in Sec. 4.3. Similarly to the calculations of Chapters 2 and 3, the comparison is based on the secure key generation rate as a function of fiber length. For these calculations, the loss coefficient of the optical fiber is set to $\alpha = 0.2$ dB/km, the baseline system error rate is set to $b = 0.01$, and an additional loss of $L_{\mathrm{s}} = 1$ dB in the receiver side is assumed. These parameters are exactly the same as in the calculations of Chapters 2 and 3.

On the other hand, we now use different values for the parameters that are determined by the single-photon detector employed in the QKD system, that is the quantum efficiency η, the dark counts per time measurement window d, and the repetition rate of the transmission ν. As we discussed in Sec. 4.2, in the case of the up-conversion single-photon detector, due to the nongated mode operation of the Si APD, there is no severe limitation on the repetition rate of the experiment. In practice, the limit is set by the speed of the electronic equipment as well as by the timing jitter of the Si APD, which is typically on the order of 0.5 ns. A realistic value, compatible with currently available components, is $\nu = 1$ GHz. This is the value used in Eq. (4.2) to determine the raw key generation rate, which is limited by the dead time of the Si APD that we set to 50 ns. The saturation factor in this equation becomes rather small at rates greater than a few megahertz, limiting the final rate at small fiber losses.

Figs. 4.6 and 4.7 show that both the quantum efficiency and the dark count rate

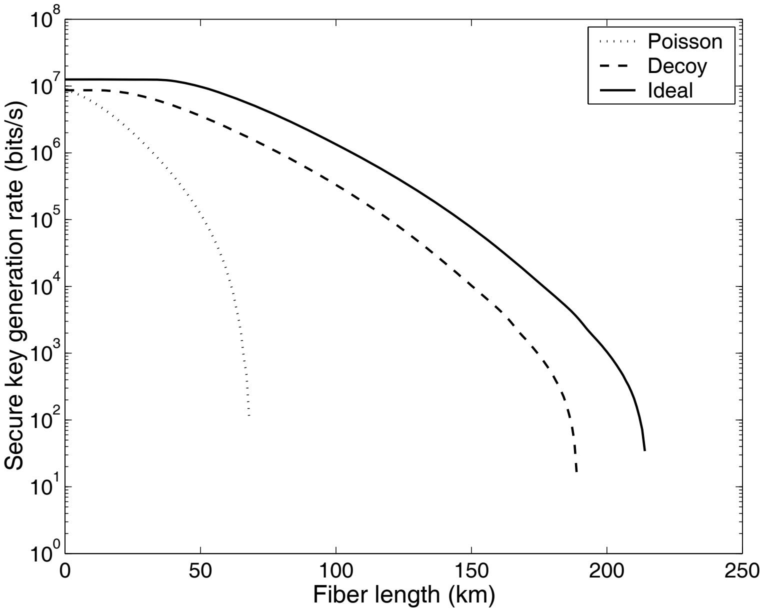

Figure 4.17: Secure key generation rate as a function of fiber length for the standard and decoy state BB84 protocol.

of the up-conversion detector depend on the pump power. This gives us a convenient tuning tool for determining the optimal operation regime of the detector depending on the application and the system parameters. Thus, in all calculations we numerically optimize the secure key generation rate with respect to the pump power p at each fiber length using Eqs. (4.11) and (4.12). Such optimization is necessary because depending on the communication distance an equilibrium between the values of the quantum efficiency and the dark counts of the up-conversion detector has to be established. The result of this optimization indicates the optimal operation regime of the detector at each fiber length. Finally, assuming the optimum filtering configuration shown in Fig. 4.15, we set the measurement time window equal to the inverse of the clock frequency, that is 1 ns.

The result of the calculation for the standard BB84 protocol employing an ideal or a Poisson single-photon source, and the decoy state B884 protocol, is shown in Fig. 4.17. For the standard BB84 protocol the calculation is based on Eq. (2.37) with the privacy amplification factors given in Eqs. (2.25) and (2.26), while for the decoy

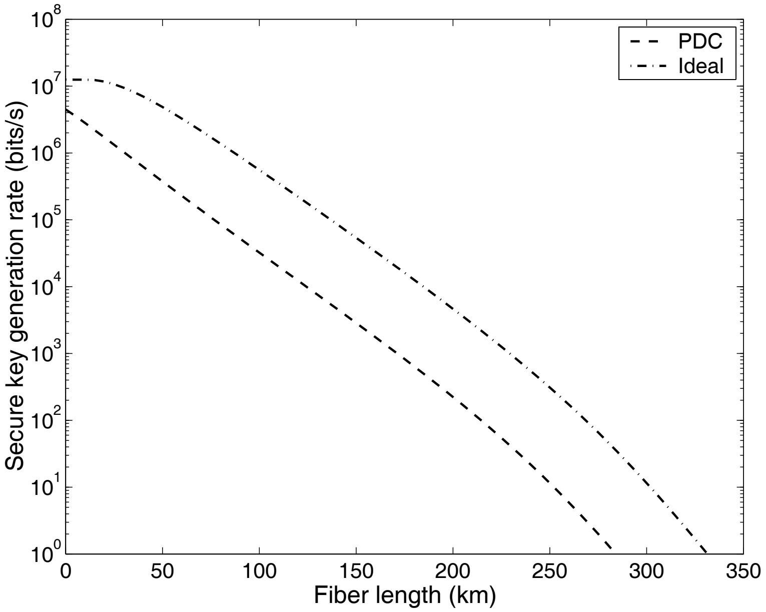

Figure 4.18: Secure key generation rate as a function of fiber length for the BBM92 protocol employing an ideal or a practical entangled-photon source.

state BB84 protocol Eq. (2.42) is used. As was discussed in Sec. 2.4, in the case of a weak laser pulse implementation of the BB84 protocol, the average number of photons per pulse μ is an adjustable parameter, with respect to which the rate is numerically optimized at each fiber length. On the other hand, for the decoy state protocol μ is determined by the baseline system error rate, and is set to 0.77. The saturation effect caused by the dead time of the Si APD is apparent for small fiber losses and high bit rates in Fig. 4.17. We also observe that, despite the improvement in the performance of the QKD system employing a Poisson source due to the use of the up-conversion detector, this system is clearly not well suited for long-distance quantum cryptography, as we had also concluded from Fig. 2.10. On the contrary, the use of an ideal single-photon source or decoy states allows for a significantly longer communication distance with high communication rates because of the increased robustness to photon number splitting attacks that these systems offer.

Fig. 4.18 shows the result of the numerical calculation for the BBM92 protocol employing an ideal entangle-photon source or a practical parametric down-conversion

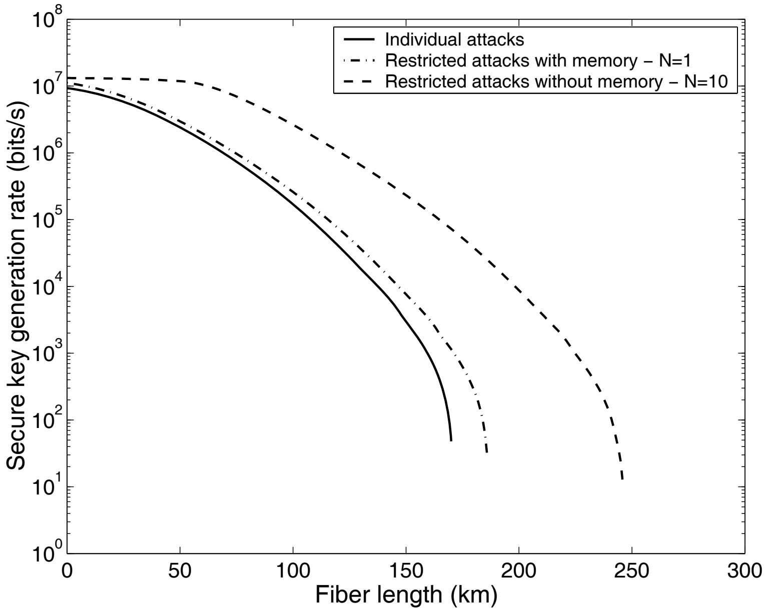

Figure 4.19: Secure key generation rate as a function of fiber length for the DPS-QKD protocol for general individual attacks and restricted attacks with time delay parameter $N = 1$ when Eve is equipped with an ideal quantum memory and $N = 10$ when she is not.

source of entangled photons. The calculation is based on Eqs. (2.64) and (2.52). In the case of the PDC source the adjustable parameter that optimizes the rate is the parameter χ, which depends on properties of the down-conversion process. As we observe in Fig. 4.18, the inherently more robust BBM92 protocol allows for longer communication distances than the BB84 protocol, having the capability to achieve a practical 1 bit/s secure key generation rate at more than 300 km with an ideal entangled-photon source and the up-conversion single-photon detector.

The results of the calculation for the DPS-QKD protocol when security against general individual attacks is assumed, or when security against restricted attacks is assumed and Eve is equipped with an ideal quantum memory and the time delay parameter defined in Sec. 3.3.3 is $N = 1$, or Eve is not equipped with a quantum memory and $N = 10$, are shown in Fig. 4.19. The calculations are based on Eqs. (3.10), (3.12), and (3.24), and in all cases the secure key generation rate is numerically optimized with respect to μ at each fiber length. As we expect from the analysis and conclusions of Chapter 3, the curves for the DPS-QKD protocol feature characteristics very similar to the standard BB84 protocol with an ideal single-photon source and the decoy state BB84, due to its robustness to PNS attacks. Fig. 4.19 shows that this protocol can be used in a simple and practical QKD system, with the potential of 1 kbit/s secure key generation rate over distances longer than 150 km.

For all the QKD protocols that we have considered, if we compare the results of this section with the corresponding figures in Chapters 2 and 3, which have assumed an InGaAs/InP APD with $\eta = 10\%$, $d = 10^{-5}$ counts/time window, and $\nu = 10$ MHz, we see that the maximum communication distance is about half of the one achieved with an up-conversion detector, while the secure key generation rate is two orders of magnitude lower than with the up-conversion detector, due to the gated mode operation of the InGaAs/InP APD. Clearly, the up-conversion single-photon detector offers a great advantage over the InGaAs/InP APD as a single-photon detector in a QKD system, in terms of both secure key generation rate and communication distance.

In order to determine the ultimate capabilities of a QKD system employing the up-conversion detector, in Fig. 4.20 we compare the performance of quantum key distribution systems implementing the three protocols, under the assumptions that Eve is equipped with an ideal quantum memory and that the dark counts of the up-conversion detector, which are dominated by parasitic nonlinear processes in the PPLN waveguide as we saw in Sec. 4.3.4, are eliminated. This means that the detector's performance is ideally limited by the Si APD characteristics, which corresponds to $d = 5 \times 10^{-8}$ with a dark count rate of 50 counts/s and a time window equal to 1 ns. Operation at the maximum quantum efficiency regime is also assumed, which means that $\eta = 46\%$. We observe that, ultimately, 250 km of secure communication distance is possible with the DPS-QKD protocol and the BB84 protocol with decoy states. An ideal single-photon source implementation of BB84 can extend this distance even more, while BBM92 has the potential of reaching 350 km of secure key distribution with an ideal entangled-photon source.

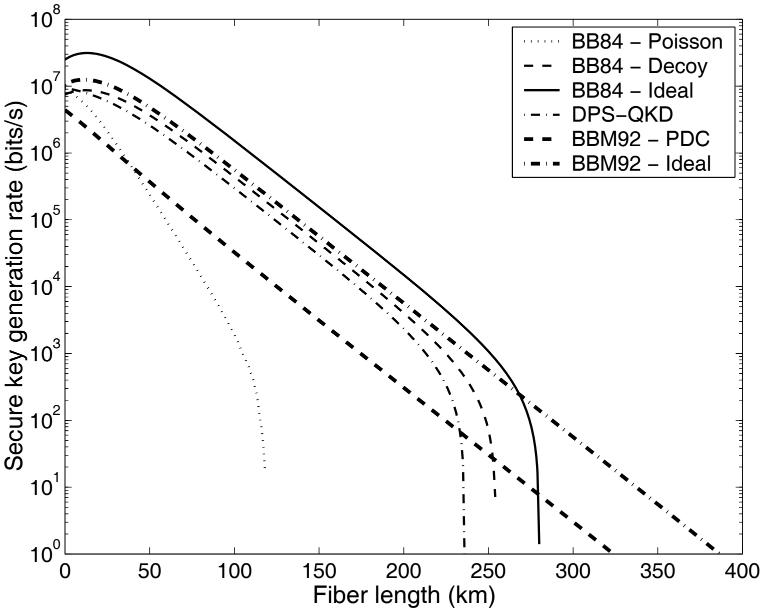

Figure 4.20: Comparison of the performance of QKD systems implementing the BB84, BBM92 and DPS-QKD protocols. In all cases it is assumed that Eve is equipped with an ideal quantum memory and that an optimized up-conversion single-photon detector is used. For the DPS-QKD protocols security against general individual attacks is assumed.

4.5 Summary

In this chapter, we studied the main characteristics of two types of single-photon detectors, the InGaAs/InP APDs and the Si APDs, and we discussed how we can use frequency conversion in a periodically poled lithium niobate waveguide device in conjunction with a Si APD to achieve high speed and efficient single-photon detection at telecommunication wavelengths that are of interest for long-distance quantum cryptography systems. We presented experimental realizations of the resulting up-conversion single-photon detector operating at 1.55 μm and 1.32 μm, and discussed the nature of the dark counts observed in these implementations. Finally, we demonstrated that the use of the up-conversion detector can considerably enhance the performance of a quantum key distribution system.

Although the calculations of Sec. 4.4 have assumed rather realistic experimental conditions, there are several factors that come into play when we try to experimentally implement a QKD system rather than predict its performance using the known parameters and the theoretical calculations. In the next chapter, we will present an experimental realization of a QKD system implementing the DPS-QKD protocol with up-conversion single-photon detectors. We will show how the characteristics of the protocol that we described in Chapter 3 and the detector that we described in this chapter successfully combine to enable the implementation of a practical and robust quantum cryptography system capable of transmitting secure keys at high rates over 100 km of optical fiber.

Chapter 5

Implementation of a 1 GHz differential phase shift QKD system

5.1 Introduction

Since the first demonstration of a quantum key distribution system in 1992 [10], there have been numerous efforts toward the implementation of such systems with the goal of making quantum cryptography practical by achieving the longest possible communication distance and the highest possible communication rate. Among these efforts, almost all of the fiber-optic QKD experiments that have been conducted have implemented the standard BB84 protocol with Poisson photon sources and InGaAs/InP APDs [55, 64, 65, 66, 71, 80, 81, 82]. The most advanced systems use the phase-encoding BB84 protocol in the so called "plug and play" configuration. More specifically, these systems employ the time slot implementation of the photonic qubit shown in Fig. 2.3(c) except that all beamsplitters are balanced and Alice and Bob randomly modulate the phase of their single-photon pulses by values that belong to two nonorthogonal bases, namely $\{0, \pi\}$ and $\{\pi/2, 3\pi/2\}$. This protocol is completely equivalent to the polarization-encoded BB84 protocol that we discussed in Sec. 2.4.1, and it has the additional advantage of being more suitable for fiber-optic long-distance quantum communication. The problem associated with the relative phase stabilization of the two interferometers has been cleverly solved with the use of the "plug and play" configuration. This configuration uses only one interferometer for dividing the pulse on Alice's site and interfering the pulses on Bob's site, and a Faraday polarization rotating mirror which ensures robustness to birefringence fluctuation in the optical fiber. However, in this two-way scheme the Rayleigh backscattered light from the fiber is a considerable source of noise, and limits the repetition rate of the system. An alternative one-way scheme successfully solved the stability problem by active compensation of the QKD system for temporal drifts in the photon phase and polarization [83]. Other fiber-optic QKD experiments have used superconducting single-photon detectors that have very low dark counts to increase the communication distance [84], or near-infrared operation with Si APDs to increase the key generation rate at the expense of limited key distribution distance [85, 86].

Although the experimental progress that has led to the above results is extremely valuable, most of the experiments have not been able to produce secure keys, either because the experimental conditions were not sufficient to guarantee security especially against Eve's photon number splitting attack, or because the implemented protocol was inherently insecure as in the case of the B92 protocol without a bright phase reference pulse. Secure key distribution was achieved in an experiment implementing the BB84 protocol with an attenuated Poisson source and InGaAs/InP APDs with particularly small dark count rates over 50 km of optical fiber, but with a very small secure key generation rate of about 0.1 bits/s [71]. As we discussed in Sec. 2.4.2, the secure key distribution distance of the BB84 protocol with Poisson sources can be significantly extended by employing decoy states. Although this scheme is promising, experimental realization is still at an early stage with a reported distance of 15 km [87]. We have also seen that the use of a single photon source can significantly enhance the performance of a QKD system. However, an ideal single-photon source does not exist today for the 1.5 μm telecommunication band, although efforts toward this goal are underway [21]. Entanglement-based QKD systems implementing the BBM92 protocol [88, 89, 90, 91, 92] are more robust than systems implementing the BB84 protocol, but the maximum key distribution distance has not exceeded 30 km so far [88], mainly due to the difficulty involved in the generation and coincidence detection of an entangled photon pair in the 1.5 μm band. Finally, the use of quantum repeaters based on nested entanglement purification and swapping [93] constitutes another candidate for long-distance quantum communication. However, to realize such a system, we need to overcome a number of technological challenges. These challenges include capturing entangled photon pairs in quantum memories either by the cavity QED technique [94] or the electromagnetically induced transparency technique [95, 96], and storing qubits of information in quantum memories with a long coherence time of typically $1 - 10$ s, requirements far beyond today's capabilities.

This review of experimental efforts for implementing a practical and secure quantum key distribution system has highlighted the main limiting factors in such systems, which are due either to the vulnerability of the QKD protocol to eavesdropping attacks or the limited capabilities of the system components. In the following sections, we will present a simple, practical and secure QKD system implementing the DPS-QKD protocol with up-conversion single-photon detectors operating in nongated mode at 1.55 μm. We will first explain the experimental setup, and we will then show that the use of the DPS-QKD protocol allows for longer communication distance while the use of the up-conversion detector allows for higher secure key generation rate, the combination resulting in a system that significantly outperforms previous experimental efforts. We will present the experimental results when the security analysis against restricted attacks only is taken into account, and how they are modified when security against general individual attacks is considered instead. Finally, by using Si APDs with very low timing jitter, we will present experimental results for a QKD system that achieves secure exchange of secret keys at high rates over 100 km of optical fiber.

5.2 Experimental setup

The experimental setup for the quantum key distribution experiments that were conducted at a repetition rate of 1 GHz and implemented the DPS-QKD protocol with

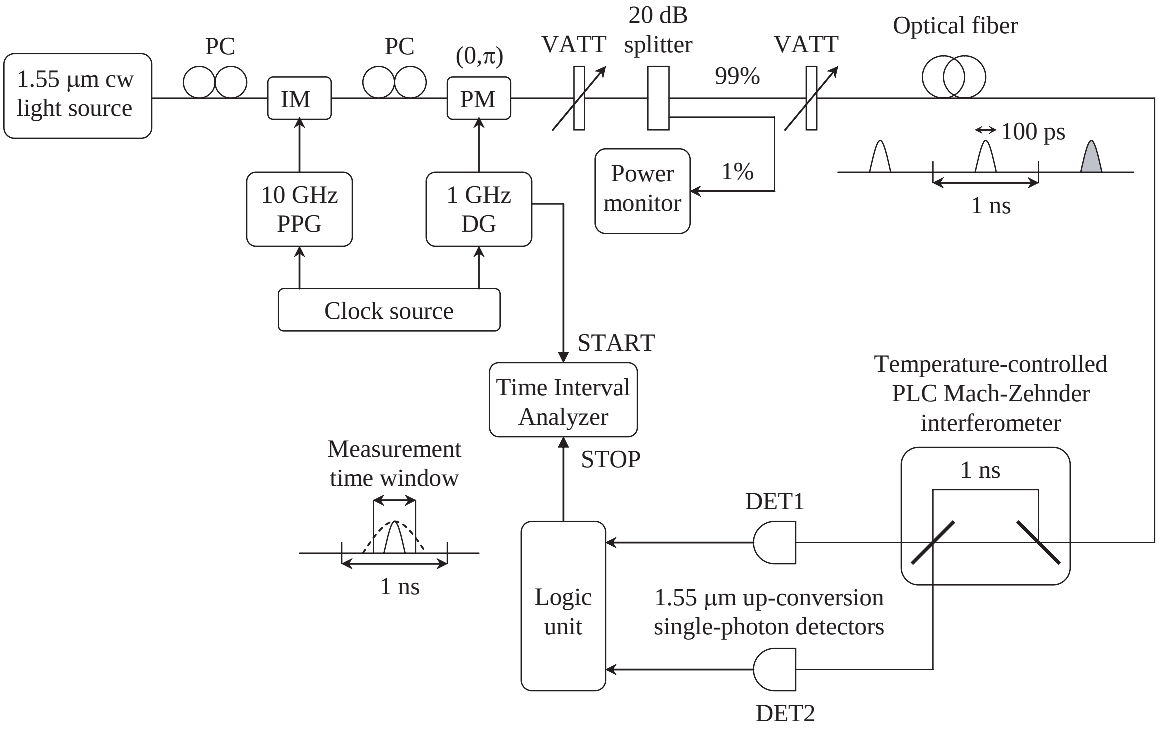

Figure 5.1: Experimental setup for the 1 GHz DPS-QKD system. PC, polarization controller; IM, intensity modulator; PM, phase modulator; VATT, variable attenuator; PPG, pulse pattern generator; DG, data generator.

up-conversion single-photon detectors is shown in Fig. 5.1. At Alice's site, a continuous wave light at 1.55 μm generated from an external cavity semiconductor laser is modulated into a coherent pulse train with a 1 GHz clock frequency using a $LiNbO_3$ intensity modulator. The modulator is driven by a 10 GHz pulse pattern generator, so the pulse width is 100 ps. Subsequently, following the DPS-QKD protocol that is illustrated in Fig. 3.2, the phase of each pulse is modulated by 0 or π with a $LiNbO_3$ phase modulator. The phase modulation signal is a 1 Gbit/s pseudo-random bit sequence with a length of $2^7 - 1$ bits, which is generated by a data generator. This sequence is used to generate a 10 μs long bit pattern, which corresponds to 10,000 bits for 1 GHz repetition rate, and is used for the QKD experiments described below. After appropriate attenuation, the pulse train is sent to Bob's site through an optical fiber, where a Mach-Zehnder interferometer based on planar lightwave circuit (PLC) technology [97] is installed. The interferometer has a path length difference of 20 cm, and so it introduces a 1-bit delay of 1 ns to the incoming pulses. The PLC technology offers stability of operation and very small polarization dependence [98]. The insertion loss of the interferometer is 2.5 dB, and the extinction ratio is greater than 20 dB. One 1.55 μm up-conversion single-photon detector is connected to each of the output ports of the interferometer. In particular, the output of each port of the interferometer enters the WDM coupler shown in Fig. 4.5, and is combined with the 1.32 μm pump light to generate the single-photon SFG output, which is subsequently detected by a single-photon counting module (SPCM) based on a Si APD. Because the PPLN waveguides used in the two up-conversion detectors are phase-matching at slightly different wavelengths, temperature tuning is used to adjust their peak conversion efficiency at the signal wavelength. The quantum efficiency and dark count rate experimental data for the up-conversion single-photon detectors with the SPCM devices that were used for the QKD experiments are shown in Figs. 5.2 and 5.3, respectively. As we discussed in Sec. 4.2, due to the low after-pulse probability of the Si APDs the up-conversion detectors are operated in nongated mode, so the sifted key generation rate is limited only by the dead time of the detector, as shown in Eq. (4.2). The dead time of the SPCMs is 50 ns.

The events detected by the two SPCMs are recorded using a time interval analyzer

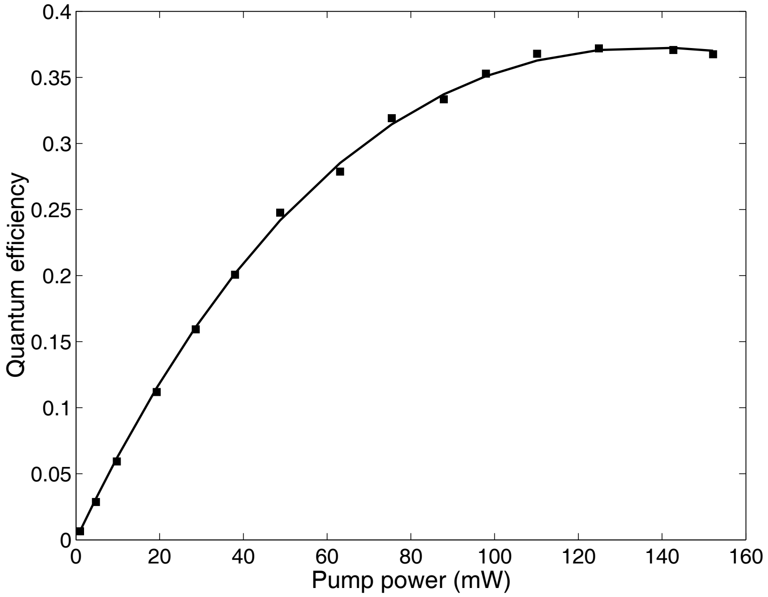

Figure 5.2: Quantum efficiency of the up-conversion single-photon detector as a function of pump power.

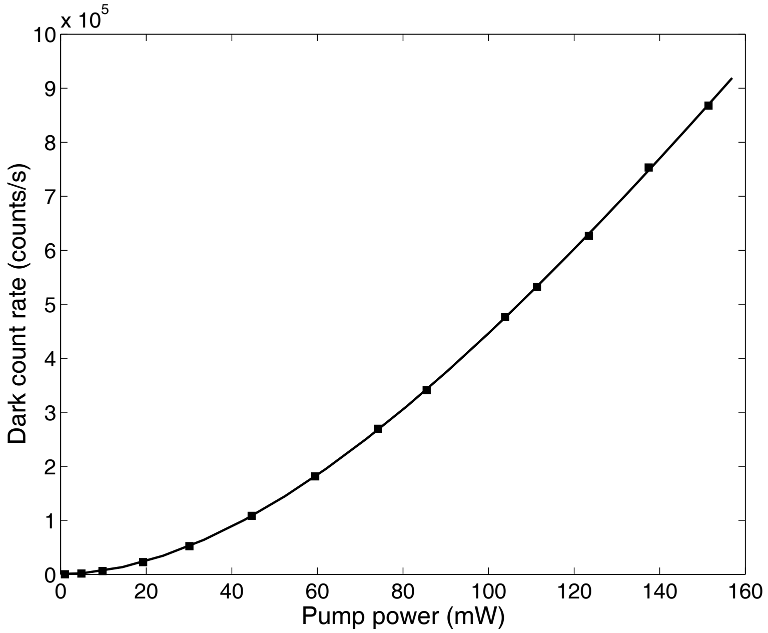

Figure 5.3: Dark count rate of the up-conversion single-photon detector as a function of pump power.

(TIA). Figs. 5.4(a) and (b) shows histograms of detected photons counted by DET1 and DET2 in Fig. 5.1, respectively, for a fixed phase modulation pattern after a 20 km fiber transmission. These data are taken with only the corresponding detector connected to the TIA. For each of these measurements, the average photon number per pulse μ is set to 0.1 and the quantum efficiency of the detector η is set to 8.8%. The tailing distribution that is clearly observed in this figure is mostly due to detector timing jitter, which is related to the uncertainty in the detection time of the incoming photons, and is typically about 500 ps for the SPCM device. This broadening of the received signal induces errors in the transmission, and so to reduce the system bit error rate we apply a time window to the recorded data, as shown in Fig. 5.1. Applying this measurement time window also reduces the dark counts per time window, a crucial parameter for the performance of the QKD system, at the expense of reduced key generation rate. Another way to avoid large bit error rates due to the large dark counts of the up-conversion single-photon detector is to keep the pump power at a relatively low level, at the expense of reduced quantum efficiency and thus again reduced key generation rate. In general, as we will see, by tuning the pump power to levels appropriate for desired dark count and quantum efficiency values, the focus of the QKD system can be adjusted to achieve high secure key generation rate or long communication distance, depending on the application.

Using the 20 dB splitter and the power meter shown in Fig. 5.1 we carefully calibrate the loss of the second variable attenuator in the setup so that the number of photons entering the optical fiber, or else the average photon number per pulse μ of the signal sent from Alice to Bob, is exactly known. This parameter is set at its optimum value for each fiber length. In particular, based on the experimental parameters of the system, we maximize the secure key generation rate with respect to μ for each fiber length, using Eqs. (3.10) and (3.5) when the security analysis against restricted attacks is considered, and Eqs. (3.10) and (3.24) when the security analysis against general individual attacks is taken into account. This means that the optimum μ depends on the security requirements of the QKD system. Once the appropriate μ is set, we perform QKD experiments, that is we measure the generation rate of the sifted keys that Alice and Bob exchange, and by directly comparing the yielded keys we also

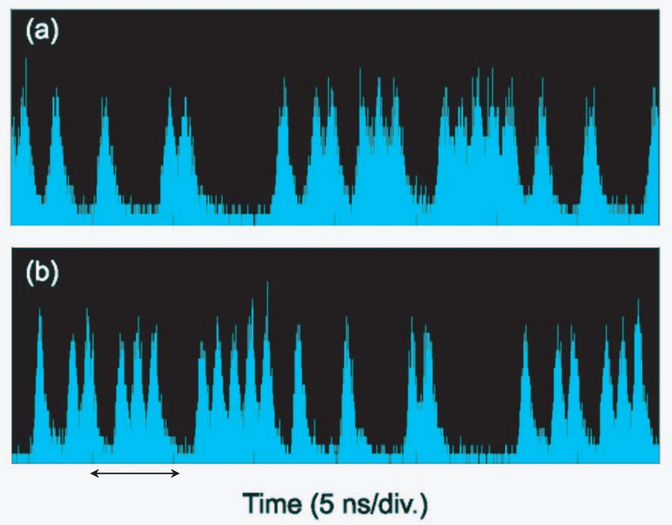

Figure 5.4: Histograms of the received signal at (a) DET1 and (b) DET2 for a fixed phase modulation pattern.

measure the bit error rate of the transmission. For each fiber length, we measure the sifted key generation rate and error rate 5 times and take the average value. Error correction and privacy amplification are not implemented; instead we calculate the secure key generation rate from the appropriate theoretical equation that depends on the security requirements of the experiment using the experimental results for the sifted key generation rates and bit error rates. Fiber transmission experiments are performed using fiber spools, with Alice and Bob located in the same room, while some additional data are taken with an optical attenuator simulating fiber loss. In the following, we present the QKD results that we obtained with the described setup and procedure.

5.3 Experimental results

5.3.1 Results for restricted attacks security analysis

When the security analysis of the DPS-QKD protocol against a set of restricted attacks is considered, the optimal average photon number per pulse μ is determined by the equation that was derived in Sec. 3.3 and is repeated here in compact form:

$$R_{\text{restricted}} = R_{\text{sifted}} \{[1 - 2\mu(1-T) - 2e] + f(e)[e \log_2 e + (1-e)\log_2(1-e)]\} \quad (5.1)$$

where we have included the appropriate privacy amplification factor τ from Eq. (3.5) and R_{sifted} is given by Eq. (4.2) since the sifting parameter is 1 for this protocol. Based on the above equation and our experimental parameters, we find the optimum μ for each fiber length. This optimum value is around 0.16 - 0.18, depending on η, d, and the fiber length. The experimental parameters as well as the experimental results that we obtained are summarized in Table 5.1, while Fig. 5.5 shows the theoretical curves and experimental results for the sifted and secure key generation rate as a function of fiber length for several cases.

First, we set the overall quantum efficiency of the up-conversion single-photon detectors to $\eta = 8.8\%$, which corresponds to a pump power of about 15 mW, as we see from Fig. 5.2. For this pump power level, the dark count rate is $D = 13$ kHz. The measurement time window used to reduce the effective dark counts and bit errors due to the SPCM timing jitter is 600 ps, so the number of dark counts per time window in these experiments is $d = 7.8 \times 10^{-6}$. The use of the 600 ps time window also decreases the effective quantum efficiency by 33%. Under these operating conditions, we perform QKD experiments for 20, 30, and 75 km of optical fiber. We used dispersion-shifted fiber (DSF) for the fiber spools in order to avoid chromatic dispersion induced pulse broadening. As a result, the pulse broadening caused by chromatic dispersion is negligible compared to that caused by the timing jitter of the detectors. The curves (a) of Fig. 5.5 correspond to the theoretical prediction for the sifted and secure key generation rate under these experimental conditions, when μ is optimized to maximize the secure key generation rate at each fiber length. A baseline system error rate of 3% is assumed in these calculations. The clear squares represent the fiber transmission experimental results for the secure key generation rate, while the sifted key generation rate at the corresponding fiber lengths is represented by the clear diamonds. Finally, the clear circles and stars show the experimental results when we simulate additional fiber loss with an optical attenuator. As we observe in

Table 5.1: Summary of fiber transmission experimental conditions and results for the restricted attacks security analysis case.

Fiber length (km)	20	30	75	75	105
Fiber loss (dB)	4.5	6.9	15.2	15.2	22.1
Dark count rate (kHz) (each detector)	13	13	13	1.35	1.35
Quantum efficiency (%)	8.8	8.8	8.8	2	2
Time window width (ps)	600	600	600	200	200
Average photon number per pulse	0.1	0.18	0.17	0.17	0.16
Sifted key generation rate (kbits/s)	1020	1050	157	22.6	4.93
Bit error rate (%)	3.94	5.19	6.96	4.06	7.95
Secure key generation rate (kbits/s)	455	210	13.8	6.65	0.209

Fig. 5.5, the theoretical curves fit very well with the experimental results. At fiber lengths of 30 km or less, the achieved sifted key generation rate is more than 1 Mbit/s. The sifted key rate cannot greatly exceed 1 Mbit/s because of the timing jitter of the SPCM devices. In particular, as noted on Table 5.1, for a fiber length of 20 km, the value $\mu = 0.1$ was used instead of the optimum value of $\mu = 0.18$. This is because the timing jitter of the SPCM surges when the count rate increases, and thus at this low loss point we cannot enlarge μ because the error rate becomes prohibitively large. The maximum attainable sifted key generation rate is limited by this effect. Even with this limitation, however, the achieved sifted rate is two orders of magnitude larger than the previous record of 45 kbits/s over 10.5 km of fiber [55]. The secure key generation rate is 0.455 Mbits/s over 20 km of optical fiber. Thus, even with the moderate 8.8% quantum efficiencies, the key rate is significantly increased, and this is due to the nongated mode operation of the up-conversion single-photon detectors.

In order to achieve long-distance quantum key distribution, we now set the pump power level, quantum efficiency, dark count rate, and time window width at approximately 3 mW, 2%, 1.35 kHz and 200 ps, respectively. This further reduces the errors caused by the dark counts, which are now $d = 2.7 \times 10^{-7}$ counts/time window. Here, the use of the 200 ps time window reduces the effective quantum efficiency of the detector by 60%. Under these operating conditions, we perform QKD experiments for 75 and 105 km of fiber. The curves (b) of Fig. 5.5 correspond to the theoretical

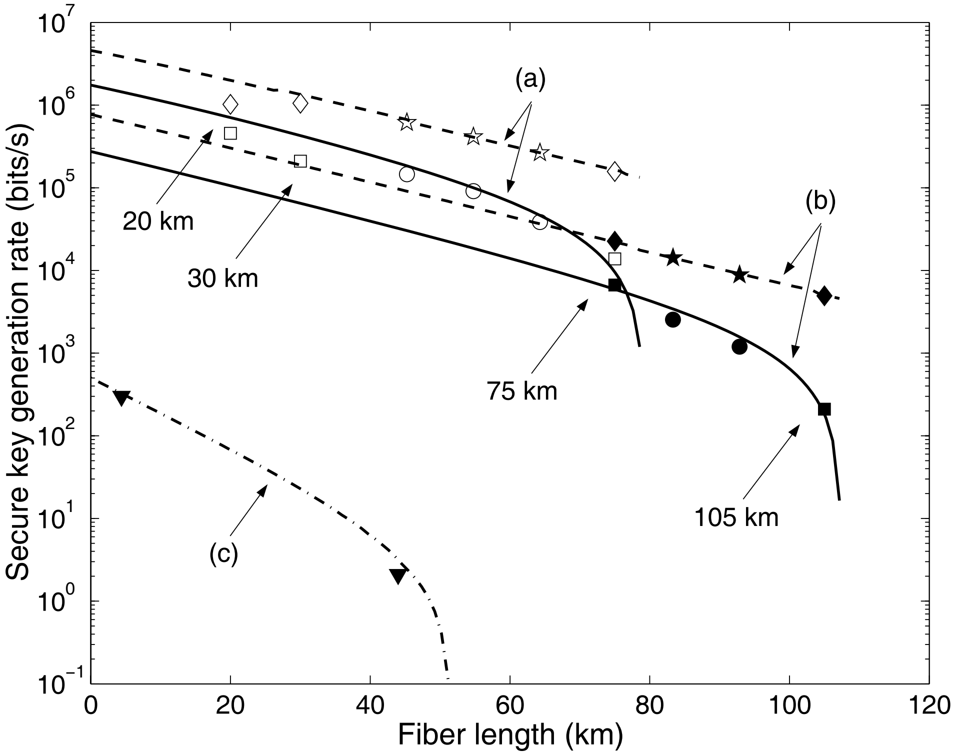

Figure 5.5: Secure and sifted key generation rate as a function of fiber length for 3 cases. (a) The dashed and solid curves are theoretical predictions for the sifted and secure rate, respectively, when $\eta = 8.8\%$ and $d = 7.8 \times 10^{-6}$, and security against restricted attacks is taken into account. The clear diamonds and squares are the experimental fiber transmission data for the sifted and secure key generation rate under these conditions. The clear stars and circles are the data taken with attenuation used to simulate additional fiber loss. (b) The dashed and solid curves are the theoretically predicted sifted and secure rate, when $\eta = 2\%$ and $d = 2.7 \times 10^{-7}$. The filled diamonds and squares are the experimental fiber transmission data under these conditions. The filled stars and circles are the simulated attenuation data. A baseline system error rate of 3% is assumed in all theoretical calculations. The effective quantum efficiency factor is 0.67 for (a) and 0.4 for (b). (c) The dash-dot curve is the theoretical prediction and the filled triangles the experimental results for the best experiment employing the BB84 protocol with Poisson light and InGaAs/InP APDs.

prediction for the sifted and secure key generation rate when the above experimental conditions are assumed. The filled squares and diamonds represent the fiber transmission experimental results, while the filled circles and stars correspond to data taken using the attenuator to simulate additional fiber loss. Again, the theoretical curves fit very well with the experimental data. By using these operating conditions, secure keys are distributed at a rate of 209 bits/s over 105 km of fiber. The bit error rate for the 105 km experiment is 7.95%. It is induced by several sources, that are summarized as follows:

$$e_{\mathrm{total}} = e_{\mathrm{interferometer}} + e_{\mathrm{dark}} + e_{\mathrm{electrical}} + e_{\mathrm{jitter}} \tag{5.2}$$

The first term represents errors due to imperfect interference, and can be inferred from the extinction ratio of the interferometer. The PLC Mach-Zehnder interferometer that we used had a 20 dB extinction ratio, which results in a 1% error rate. The second term is due to the dark counts of the detector. This term increases with the fiber transmission distance, since the dark count rate remains constant while the number of received signal photons reduces, which leads to a worse signal to noise ratio. For the 105 km experiment, the sifted key rate is 4930 counts/s, while the dark count rate is 1350 counts/s, which means that 270 counts/time window are included in the 200 ps time window for each detector. Thus, if we take into account both detectors and the fact that half of the dark counts lead in errors, we find that the contribution of the dark counts to the error rate is 5.5%. The third term in Eq. (5.2) represents errors caused by electrical noise, which we estimate to be negligible in this case. Finally, the last term corresponds to the timing jitter of the detectors and the remaining 1.45% error rate for the 105 km experiment is due to this effect. Fig. 5.6 shows the theoretical prediction based on Eq. (3.9) for the bit error rate under the experimental conditions discussed above, as well as the error rate values obtained in the experiments. For the theoretical curve, a baseline system error rate of 3% is assumed, as in the corresponding calculations for Fig. 5.5.

To compare the results obtained using the DPS-QKD system with up-conversion detectors with the best results obtained so far, we plot curve (c) in Fig. 5.5, which

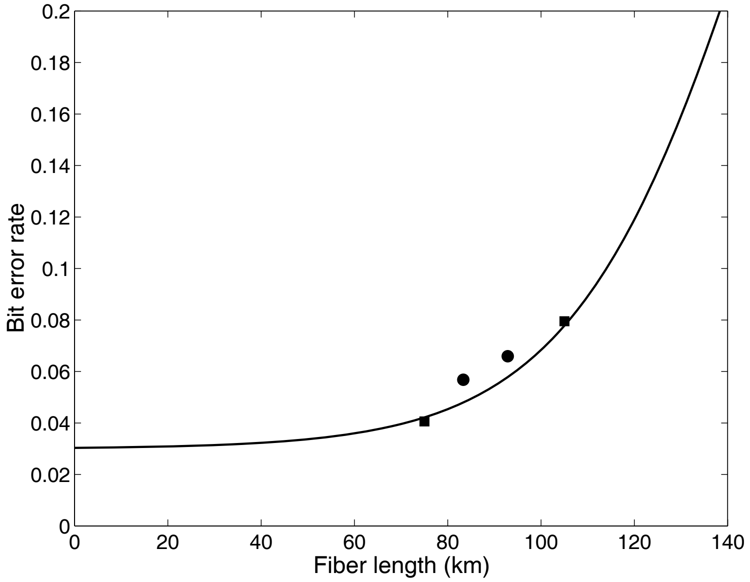

Figure 5.6: Theoretical prediction and experimental results for the bit error rate as a function of fiber length, when $\eta = 2\%$ and $d = 2.7 \times 10^{-7}$. The squares and circles correspond to fiber transmission and simulated attenuation experiments, respectively.

shows the theoretical prediction for the secure key generation rate, as well as the experimental results for the best QKD system implementing the standard BB84 protocol with an attenuated Poisson source and InGaAs/InP APDs to date [71]. The comparison between the curves shows that the DPS-QKD system significantly outperforms a QKD system based on the BB84 protocol, in terms of both secure key generation rate and communication distance. This improvement is due to the robustness of the DPS-QKD protocol to photon number splitting attacks, which extends the communication distance, and the high speed nongated mode of the up-conversion single-photon detectors, which extends the key generation rate.

5.3.2 Results for individual attacks security analysis

Although a practical QKD system capable of transmitting keys that are secure against a set of realistic eavesdropping attacks such as the beamsplitter and intercept and resend attacks discussed in Sec. 3.3 is very important, it is also crucial to take into

Table 5.2: Summary of fiber transmission experimental conditions and results for the general individual attacks security analysis case.

Fiber length (km)	20	75
Fiber loss (dB)	4.5	15.2
Dark count rate (kHz) (each detector)	13	1.35
Quantum efficiency (%)	8.8	2
Time window width (ps)	600	200
Average photon number per pulse	0.1	0.17
Sifted key generation rate (kbits/s)	1020	22.6
Bit error rate (%)	3.94	4.06
Secure key generation rate (kbits/s)	125	0.871

account more elaborate attacks that will be available in the near future, and guarantee the security of the system against these types of attacks. Thus, below we reinterpret the results obtained in the experiments described in the previous section when the security analysis against general individual attacks that was developed in Sec. 3.4 is considered.

In this case, because the average number of photons per pulse μ was not optimized based on the individual attacks analysis, only two fiber transmission experiments were found to have been secure against the more powerful eavesdropping attacks: the 20 km experiment with conditions (a) of Fig. 5.5, and the 75 km experiment with conditions (b) of the same figure. The parameters and results that correspond to these experiments are summarized in Table 5.2, while Fig. 5.7 shows the theoretical curves and experimental results for the sifted and secure key generation rate as a function of fiber length for the two different detector operating conditions, when the security analysis against general individual attacks is taken into account. To obtain the secure key generation rates shown in Table 5.2 and Fig. 5.7, we insert the experimental values for the sifted key generation rate and error rate, as well as the experimental parameters, in the equation that was derived in Sec. 3.4 and is repeated here in compact form:

$$\begin{aligned} R_{\text{individual}} &= R_{\text{sifted}}\{-[1-2\mu(1-T)]\log_2[1-e^2-\frac{(1-6e)^2}{2}] \\ &\quad +f(e)[e\log_2 e+(1-e)\log_2(1-e)]\} \end{aligned} \tag{5.3}$$

where we have included the appropriate privacy amplification factor τ from Eq. (3.24) and R_{sifted} is again given by Eq. (4.2). As we see in Fig. 5.7, even with the strict security requirements imposed by the general individual attacks analysis, the DPS-QKD system with the up-conversion detectors offers a very enhanced performance compared to the system that implements the BB84 protocol with InGaAs/InP APDs.

In the experiments that we described, the secure key distribution distance is limited by two factors related to the up-conversion single-photon detectors. The first factor is the large dark count rate, which as we explained in Sec. 4.3.4 is caused by noise photons generated via a spontaneous Raman scattering process in the waveguide. These noise photons can potentially be suppressed by choosing a pump wavelength longer than the signal wavelength. The second factor that limits the performance of the system is the large timing jitter of the SPCM devices, which is on the order of 500 ps. As we discussed in the previous sections, for small fiber losses and large count rates the timing jitter surges and limits the key generation rate. But even for high fiber losses, the broadening of the received signal pulses that the timing jitter induces leads to a larger bit error rate, which results in a reduction of the secure key distribution distance. It is therefore clear that by improving the performance of the Si APDs with respect to their timing jitter the capabilities of the QKD system can be substantially extended. Fortunately, the timing jitter of these devices is not determined by an intrinsic process, rather it is limited by the electronic circuit used for the quenching of the avalanche process. Progress in research related to these detectors has recently led to commercial devices that feature low timing jitter, on the order of 50 ps. The development of these low-jitter photon counting detection modules (PDMs) opens the way to the implementation of quantum cryptography systems with enhanced capabilities, as was suggested in [99] and we experimentally show in the following section.

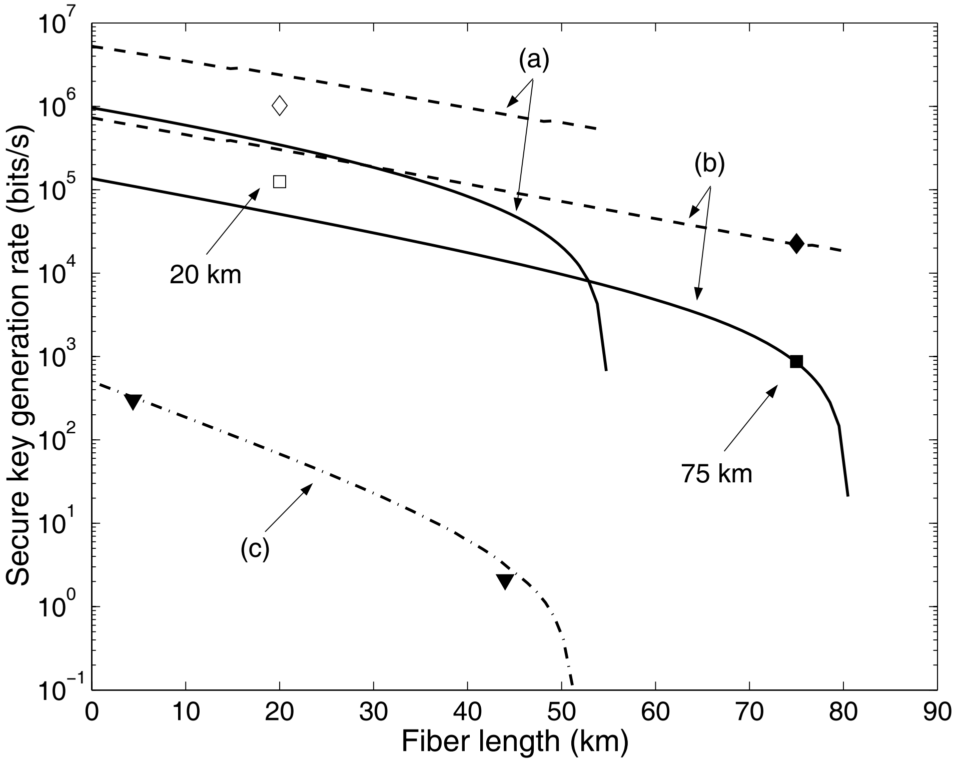

Figure 5.7: Secure and sifted key generation rate as a function of fiber length for 3 cases. (a) The dashed and solid curves are theoretical predictions for the sifted and secure rate, respectively, when $\eta = 8.8\%$ and $d = 7.8 \times 10^{-6}$, and security against general individual attacks is taken into account. The clear diamond and square are the experimental fiber transmission data for the sifted and secure key generation rate under these conditions. (b) The dashed and solid curves are the theoretically predicted sifted and secure rate, when $\eta = 2\%$ and $d = 2.7 \times 10^{-7}$. The filled diamond and square are the experimental fiber transmission data under these conditions. For the theoretical calculations we have made the same assumptions as in the case of restricted attacks. (c) The dash-dot curve is the theoretical prediction and the filled triangles the experimental results for the best experiment employing the BB84 protocol with Poisson light and InGaAs/InP APDs.

5.4 Experimental results with low-jitter detectors

The experimental setup used for the QKD experiments that we describe in this section is the same as the setup shown in Fig. 5.1, except for two modifications. First, the pulse pattern generator is operated at 15 GHz so that the resulting pulse width obtained with the intensity modulator driven by the generator is 66 ps instead of 100 ps that was used in the previous experiments. Second, the high-jitter SPCM devices are replaced by the low-jitter PDM devices, resulting in low-jitter up-conversion single-photon detectors. Both of these modifications have the goal of reducing the bit error rate caused by timing jitter, and thus achieve better performance of the DPS-QKD system with respect to both key generation rate and communication distance.

In order to evaluate the performance of the low-jitter up-conversion detectors, we first perform timing jitter measurements. For these measurements, the phase modulator and PLC interferometer in Fig. 5.1 are not used, and only one detector is connected to the time interval analyzer at a time. Furthermore, the pulse pattern generator is adjusted so that the 66 ps pulses are generated every 10 ns instead of every 1 ns as in the QKD experiments. Under these conditions, a typical detection signal from the up-conversion single-photon detector with the low-jitter Si APD is shown in Fig. 5.8 for a count rate of 10^5 counts/s. As we observe in this figure, the full width at half maximum (FWHM) of the signal is rather small, about 75 ps. However, the signal is clearly not Gaussian and there is a long tail that can potentially cause errors in the next 1 ns time slot in a QKD experiment with a repetition rate of 1 GHz. Thus, a more appropriate figure of merit is the full width at tenth maximum (FWTM) of the signal, which is 240 ps for the signal pulse in Fig. 5.8. As we discussed in Sec. 5.3, the timing jitter of the SPCM devices surged at high count rates, preventing the sifted key generation rate from exceeding 1 Mbit/s for small fiber losses. To determine the corresponding behavior of the low-jitter detectors, we record the FWHM and FWTM of the detected signal pulses for several count rate values. Fig. 5.9 shows the experimental results obtained with these timing jitter measurements. Although the FWHM remains below 100 ps even for 10^6 counts/s, the FWTM becomes larger for high count rates. Nevertheless, Figs. 5.8 and 5.9 show

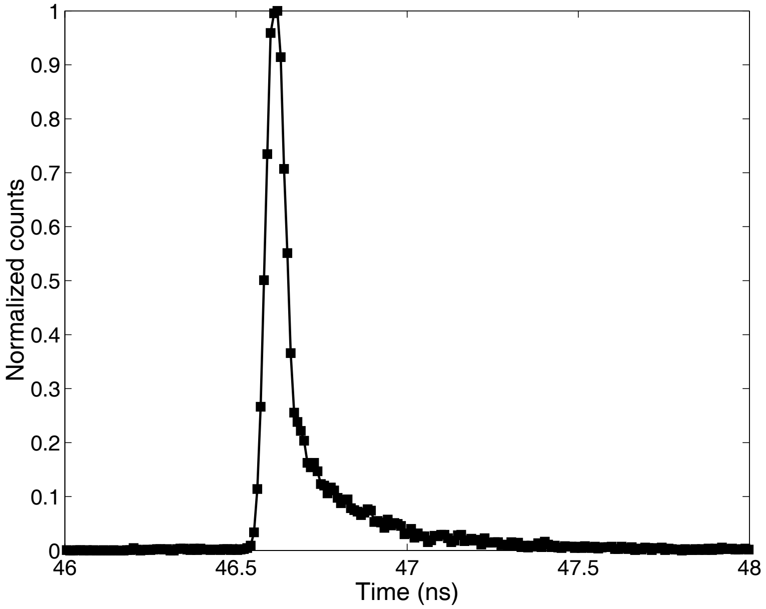

Figure 5.8: Typical detection signal from the up-conversion single-photon detector with a low-jitter Si APD when 66 ps pulses are used. This curve corresponds to DET2 and a count rate of 10^5 counts/s.

that the improvement in timing jitter achieved with these Si APDs is significant, and so the error rate should be considerably lower both in high bit rate and long-distance QKD experiments employing these detectors.

The procedure followed for the experiments implementing the DPS-QKD protocol with low-jitter up-conversion detectors is the same as the one described in Sec. 5.2. The quantum efficiency and dark count rate experimental data for the up-conversion single-photon detectors with the PDM devices that were used for the QKD experiments are shown in Figs. 5.10 and 5.11, respectively. The maximum quantum efficiency of the PDM device at the SFG wavelength of 715 nm is $\sim$ 25% instead of 70% for the SPCM device, which explains the lower overall quantum efficiencies of the low-jitter up-conversion detector that we observe in Fig. 5.10 compared to Fig. 5.2. Since the dark counts of the up-conversion detector are mainly caused by spurious optical processes in the waveguide, the smaller quantum efficiency of the PDM device also results in less efficient conversion of the dark counts, and the relatively smaller

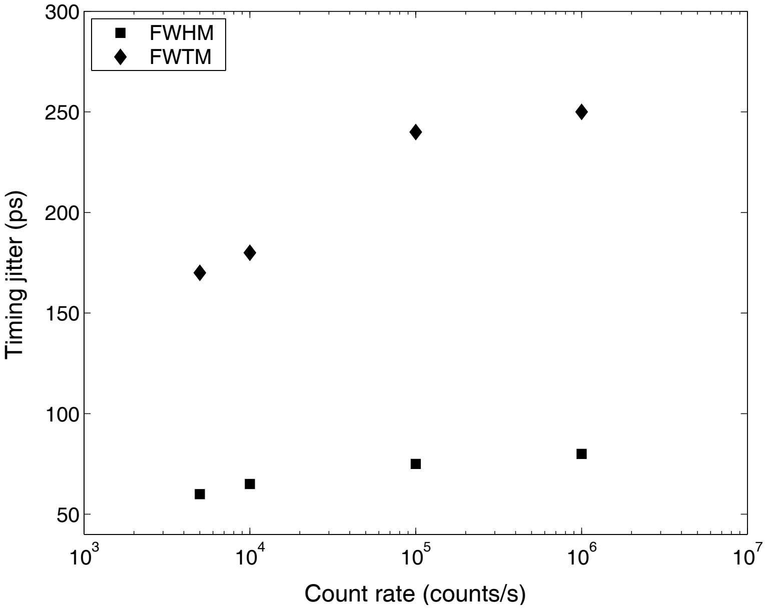

Figure 5.9: Timing jitter as a function of count rate for the low-jitter up-conversion detectors when 66 ps pulses are used.

dark count rates we observe in Fig. 5.11. Finally, the low-jitter up-conversion detector is operated in nongated mode, so the sifted key generation rate is again limited by the dead time of the detector, which is 85 ps for the PDMs.

For the QKD experiments, we first set the average photon number per pulse μ at its optimal value based on the experimental parameters and the security analysis for general individual attacks, that is we use Eq. (5.3) for our calculations. The optimal value is around 0.2 in this case, the exact value depending on η, d, and the fiber length. The experimental parameters as well as the experimental results that we obtained are summarized in Table 5.3, while Fig. 5.12 shows the theoretical curves and experimental results for the sifted and secure key generation rate as a function of fiber length for two different experimental conditions.

As with the experiments of Sec. 5.3, we first set the detector operating condition to levels appropriate for achieving high bit rate quantum key distribution. More specifically, the quantum efficiency and dark count rate of the low-jitter up-conversion single-photon detectors are set to 6% and 98 kHz, respectively. These values do not

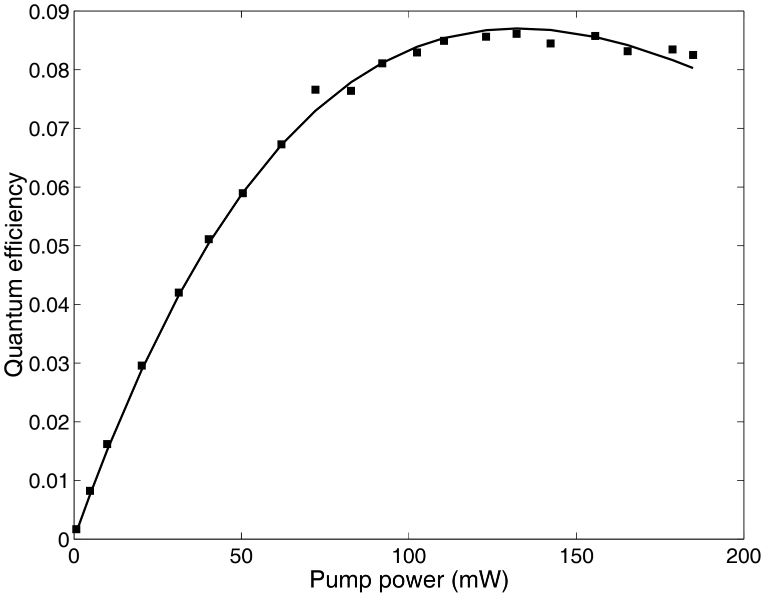

Figure 5.10: Quantum efficiency of the low-jitter up-conversion single-photon detector as a function of pump power.

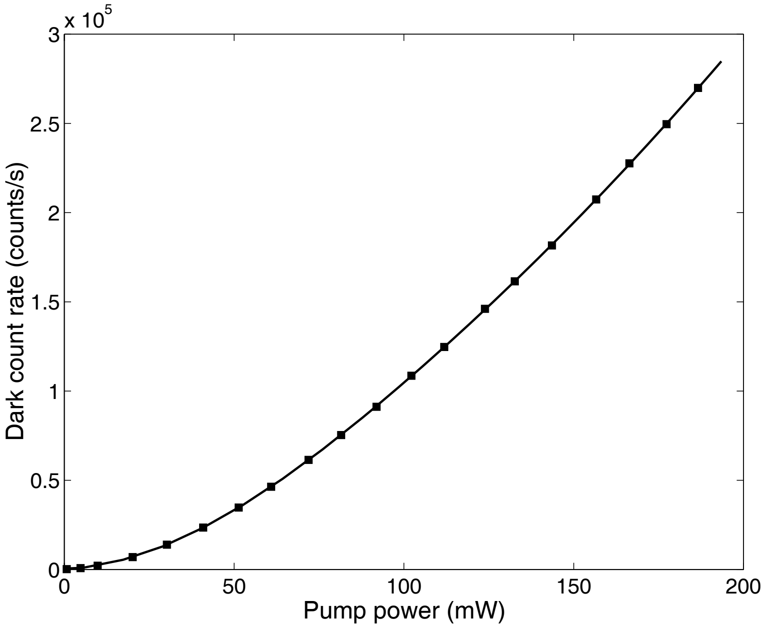

Figure 5.11: Dark count rate of the low-jitter up-conversion single-photon detector as a function of pump power.

Table 5.3: Summary of fiber transmission experimental conditions and results for the general individual attacks security analysis case and low-jitter up-conversion detectors.

Fiber length (km)	10	25	75	100
Fiber loss (dB)	2.4	5.7	15.2	20.9
Dark count rate (kHz) (each detector)	98	0.35	0.35	0.35
Quantum efficiency (%)	6	0.4	0.4	0.4
Time window width (ps)	200	100	100	100
Average photon number per pulse	0.2	0.2	0.2	0.2
Sifted key generation rate (kbits/s)	2020	37.7	6.7	2.1
Bit error rate (%)	2.2	1.3	2.4	3.4
Secure key generation rate (kbits/s)	468	13.8	1.39	0.166

correspond to the same pump power level in Figs. 5.10 and 5.11 because the performance of the detectors was slightly degraded when the QKD experiments were performed compared to when the quantum efficiency and dark count rate data were taken. Due to the low timing jitter of the PDMs we can now use a smaller measurement time window to significantly reduce the effective dark counts without greatly affecting the signal to noise ratio. This window is set to 200 ps, so the dark counts per time window in these experiments are $d = 1.95 \times 10^{-5}$. The use of the 200 ps time window also decreases the effective quantum efficiency by 40%. Under these operating conditions, we perform QKD experiments for 10 km of dispersion-shifted optical fiber. The curves (a) of Fig. 5.12 correspond to the theoretical prediction for the sifted and secure key generation rate under these experimental conditions, when μ is optimized to maximize the secure key generation rate at each fiber length using the general individual attacks security analysis. A baseline system error rate of 1.2% is assumed in these calculations. The clear square represents the fiber transmission experimental result for the secure key generation rate, while the sifted key generation rate at the corresponding fiber length is represented by the clear diamond. The clear circles and stars show the experimental results when we simulate additional fiber loss with an optical attenuator. As we observe in Fig. 5.12, the theoretical curves fit very well with the experimental results. At the fiber length of 10 km the achieved sifted key generation rate is 2 Mbits/s, while the secure key generation rate at this fiber length is 0.468 Mbits/s. The comparison with the results of Table 5.2 shows that the use of the low-jitter detectors has doubled the sifted rate at small fiber loss, and quadrupled the secure key generation rate because of the significantly improved error rate.

Subsequently, we set the quantum efficiency, dark count rate, and time window width at approximately 0.4%, 350 Hz and 100 ps, respectively, to achieve long-distance quantum cryptography. The use of the 100 ps time window sets the dark counts per time window to $d = 3.5 \times 10^{-8}$, and also reduces the effective quantum efficiency of the detector by 54%. Under these operating conditions, we perform QKD experiments for 25, 75 and 100 km of optical fiber. The 75 km fiber spool was dispersion-shifted fiber, while the 25 km spool was standard single-mode fiber. The curves (b) of Fig. 5.12 correspond to the theoretical prediction for the sifted and secure key generation rate when the above experimental conditions are assumed. The filled squares and diamonds represent the fiber transmission experimental results, while the filled circles and stars correspond to data taken using the attenuator to simulate additional fiber loss. Again, we observe that the theoretical curves fit very well with the experimental data. By using these operating conditions, keys that are secure against general individual eavesdropping attacks are distributed at a practical rate of 166 bits/s over 100 km of fiber. As we observe in Table 5.3, the error rate achieved in these experiments is significantly lower that the one achieved in the experiments with the SPCMs, ranging from only 1.3% for the 25 km experiment to 3.4% for the 100 km experiment. This error rate is induced by the sources indicated in Eq. (5.2). For the 100 km experiment, 1% error rate is attributed to imperfect interferometry, 1.7% to the dark counts of the detector, and the remaining 0.7% to the timing jitter. Fig. 5.13 shows the theoretical prediction based on Eq. (3.9) for the bit error rate under the experimental conditions discussed above, as well as the error rate values obtained in the experiments. For the theoretical curve, a baseline system error rate of 1.2% is assumed, as in the corresponding calculations for Fig. 5.12. These results show that the use of the low-jitter detectors has considerably extended the secure key distribution

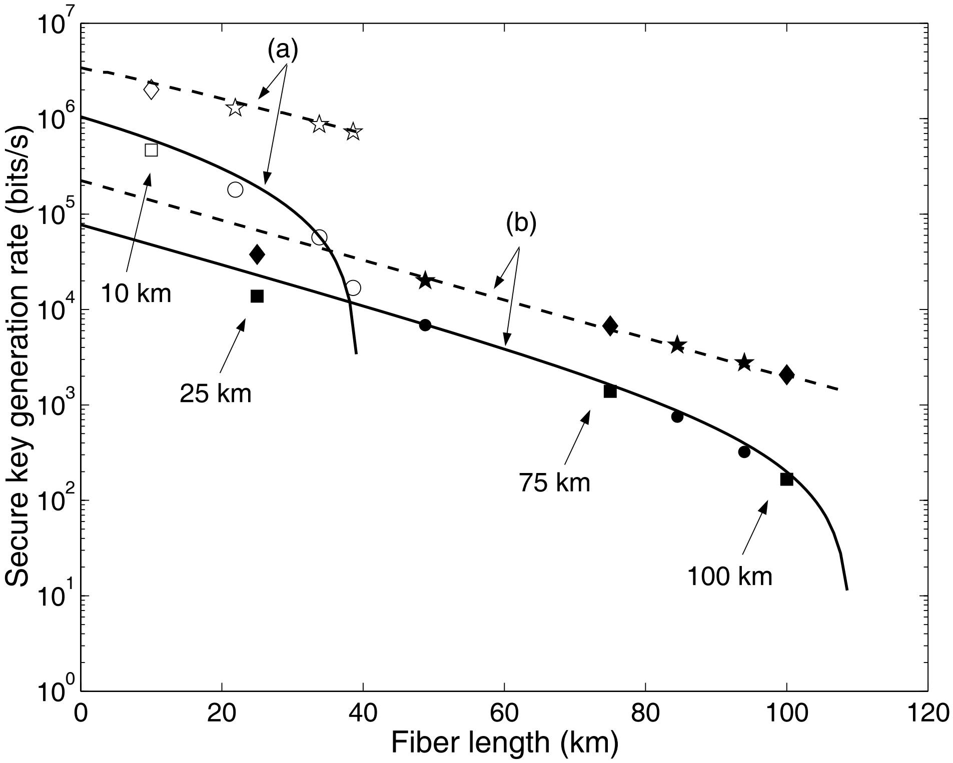

Figure 5.12: Secure and sifted key generation rate as a function of fiber length for 2 cases. (a) The dashed and solid curves are theoretical predictions for the sifted and secure rate, respectively, when $\eta = 6\%$ and $d = 1.95 \times 10^{-5}$, and security against general individual attacks is taken into account. The clear diamond and square are the experimental fiber transmission data for the sifted and secure key generation rate under these conditions. The clear stars and circles are the data taken with attenuation used to simulate additional fiber loss. (b) The dashed and solid curves are the theoretically predicted sifted and secure rate, when $\eta = 0.4\%$ and $d = 3.5 \times 10^{-8}$. The filled diamonds and squares are the experimental fiber transmission data under these conditions. The filled stars and circles are the simulated attenuation data. A baseline system error rate of 1.2% is assumed in all theoretical calculations. The effective quantum efficiency factor is 0.6 for (a) and 0.46 for (b).

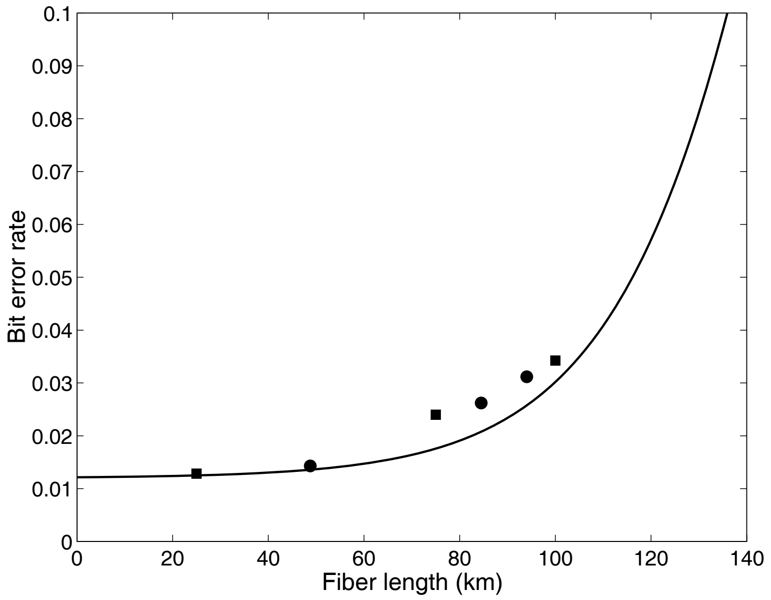

Figure 5.13: Theoretical prediction and experimental results for the bit error rate as a function of fiber length, when $\eta = 0.4\%$ and $d = 3.5 \times 10^{-8}$. The squares and circles correspond to fiber transmission and simulated attenuation experiments, respectively.

distance of the DPS-QKD system. This is partly due to the smaller pulse broadening, which results in smaller error rate, but most importantly due to the reduced effective dark counts of the detector, which are one order of magnitude smaller than the case of the previous long-distance experiments with high-jitter detectors. The latter is only possible because the low timing jitter allows the use of a smaller time window without the degradation of the signal to noise ratio that would occur in the previous experiments.

5.5 Summary

In this chapter, we presented the experimental realization of a simple and practical quantum key distribution system that implements the DPS-QKD protocol with the up-conversion single-photon detectors. We described the experimental results that were initially obtained taking into account the security analysis against restricted eavesdropping attacks, and we reinterpreted these results when stricter security requirements are imposed from the general individual attacks analysis. With this system we achieved 1 Mbit/s sifted key generation rate over 20 km, and transmission of secure keys over 75 km of optical fiber. Although these results significantly outperformed previous QKD experiments, they also highlighted the limitations imposed on the system from the high timing jitter of the single-photon detectors. By using newly developed low-jitter detectors we demonstrated a DPS-QKD system that achieved 2 Mbits/s sifted key generation rate over 10 km, and transmission of secure keys over 100 km of optical fiber.

If we can eliminate the noise photons and all losses in the system except for the fiber loss, and achieve a negligible timing jitter compared to the pulse width, we find that the secure key distribution distance of the DPS-QKD system with low-jitter up-conversion detectors can reach 270 km. This means that in this ideal case, an entanglement-based quantum repeater system will be required only if the length of the system exceeds 270 km. This argument shows that the capabilities of fiber-optic QKD systems can be extended even further by improving the timing jitter of the Si APDs and by reducing the dark counts of the up-converter. Of course, in practical quantum cryptography systems spanning hundreds of kilometers problems resulting from the chromatic dispersion and birefringence in optical fibers may appear. In this chapter, we have seen some effective solutions to these problems, such as the use of dispersion-shifted fibers and a phase-encoding protocol with small polarization-dependence interferometers.

Before technology advances sufficiently to reach the above predictions, a natural question that arises from the considerably enhanced performance of the QKD system achieved with the use of the low-jitter detectors is whether we can achieve even better performance with currently available technology. In the next chapter, we will present the implementation of a DPS-QKD system with low-jitter up-conversion detectors operating at 10 GHz repetition rate, and we will show that unfortunately even these detectors cannot guarantee the security of this system that reaches the limits of today's capabilities.

Chapter 6

Implementation of a 10 GHz differential phase shift QKD system

6.1 Introduction

The progress in classical optical communications in the last decade has been impressive, with 40 GHz systems currently operating in research laboratories and the industry and 100 GHz components under development for use in the near future. Quantum communications can greatly benefit from this progress, although the requirements in these systems are very different from those of their classical counterparts, as we will see in this chapter.

In the following sections, we will present the experimental realization of a quantum cryptography system implementing the DPS-QKD protocol, in which components developed for the advanced telecommunication industry are used to achieve a 10 GHz repetition rate. We will show that although this rate is standard for classical communications it reaches the limits of quantum communication systems. This is due to limitations imposed by the components developed for quantum optics applications, namely the single-photon detectors. Even the good characteristics of the low-jitter Si APDs that we described in the previous chapter are not sufficient to achieve secure key generation in the 10 GHz DPS-QKD system. We will present the experimental results we obtained with this system, we will explain what are the limiting factors, and discuss possible solutions.

6.2 Experimental setup

The experimental setup for the quantum key distribution experiments that were performed at a repetition rate of 10 GHz and implemented the DPS-QKD protocol with 1.55 μm low-jitter up-conversion detectors, is shown in Fig. 6.1. At Alice's site, a 10 GHz mode-locked fiber laser is used to generate an optical pulse train at 1.55 μm. The waveform of the pulses emitted by the laser is monitored with a sampling oscilloscope, and is shown in Fig. 6.2. The pulses are Gaussian with a FWHM specification of 10 ps, which corresponds to a bandwidth of 0.36 nm or 45 GHz at 1.55 μm. This matches well the waveguide bandwidth, which is about 50 GHz, so we can achieve the overall quantum efficiency of the detectors shown in Fig. 5.10. The large spectral width of these pulses, however, makes the system more sensitive to the effect of chromatic dispersion induced pulse broadening. For example, in this case we cannot use the 25 km single-mode fiber (SMF) that was used in the 1 GHz DPS-QKD experiment with low-jitter up-conversion detectors. The dispersion of such fibers at 1550 nm is 17 ps/km/nm, so if a pulse with a linewidth of 0.36 nm propagates in 25 km of SMF, the dispersion will be equal to 153 ps. This pulse width is prohibitive for the tight requirements of the 10 GHz DPS-QKD system, where pulses are only separated by 100 ps. On the contrary, for the 66 ps pulses used in the 1 GHz DPS-QKD setup with low-jitter detectors, the corresponding dispersion was 23 ps, which did not have any substantial effect on the performance of the system. The use of dispersion-shifted fibers is absolutely required, however, in the 10 GHz system.

Following the DPS-QKD protocol, the pulse train generated by the mode-locked laser is phase modulated by 0 or π using a high-speed LiNbO$_3$ phase modulator. The phase modulation signal is a 10 Gbit/s pseudo-random bit sequence with a length of 100 bits, which is provided by a pulse pattern generator. Subsequently, the pulses are appropriately attenuated and sent to Bob through an optical fiber. At Bob's site,

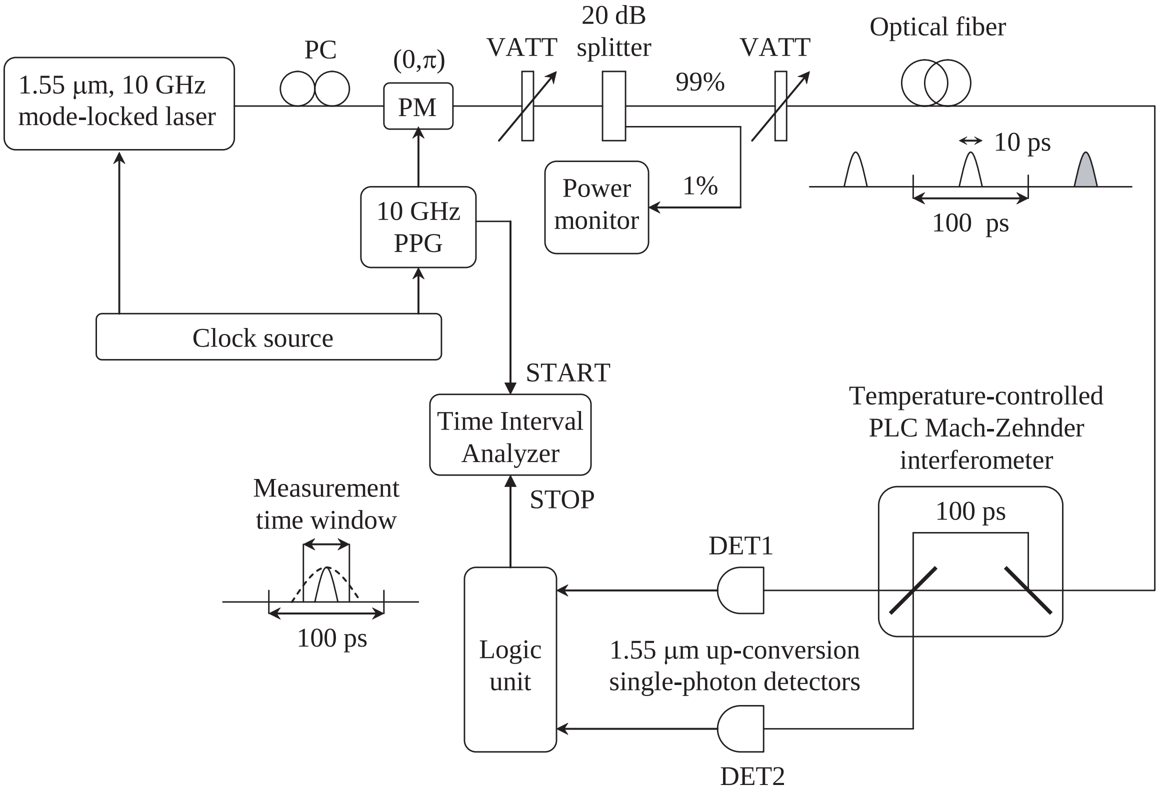

Figure 6.1: Experimental setup for the 10 GHz DPS-QKD system. PC, polarization controller; PM, phase modulator; VATT, variable attenuator; PPG, pulse pattern generator.

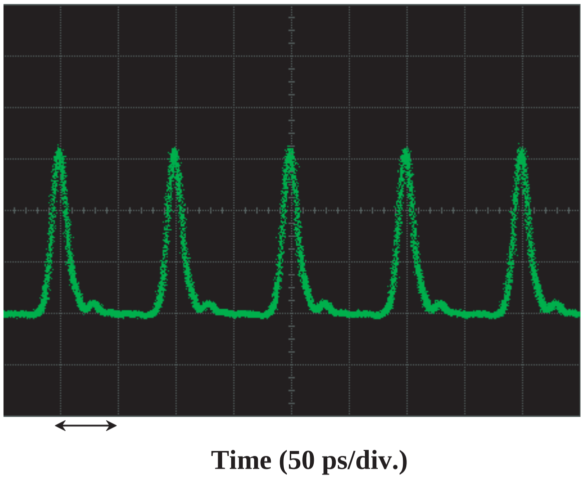

Figure 6.2: Optical pulse train generated from the 10 GHz mode-locked laser.

the pulses enter a PLC Mach-Zender interferometer, which has a 2 cm path length difference, and so it introduces the required 1-bit delay of 100 ps to the incoming pulses. The insertion loss of the interferometer is 2.5 dB, and the coherence of the mode-locked laser is sufficient to achieve an extinction ratio of 19-20 dB. Two 1.55 μm up-conversion single-photon detectors with low-jitter PDMs operating in nongated mode are placed at the output ports of the interferometer.

The events detected by the two Si APDs are recorded using a time interval analyzer (TIA). Fig. 6.3 shows a histogram of detected photons counted by DET2 for a fixed modulation pattern after a 10 km fiber transmission. For this measurement, only DET2 is connected to the TIA, while the average photon number per pulse is set to 0.1 and the quantum efficiency of the detector to 0.2%. The comparison of this figure with the histograms of Fig. 5.4 that correspond to the high-jitter SPCM devices shows the great advantage the low-jitter Si APDs provide in terms of reduced pulse broadening. However, it is also apparent in Fig. 6.3 that the long tail of the detection signal that we observed in Fig. 5.8 causes a significant intersymbol interference, which will result in considerable errors in the transmission. Thus, to reduce the bit error rate, we apply a time window to the recorded data, which also reduces the effective dark counts of the system.

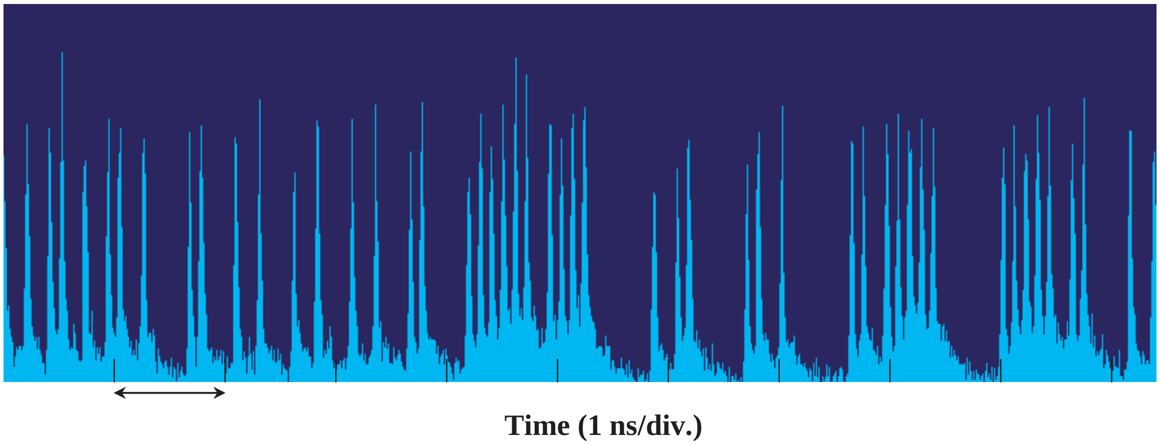

Figure 6.3: Histogram of the received signal at DET2 for a fixed phase modulation pattern.

Before conducting the QKD experiments, we first want to evaluate the performance of the low-jitter detectors with this system; we thus perform timing jitter measurements in the same way as we described in Sec. 5.4. More specifically, for these measurements we omit the phase modulator and PLC interferometer and we only connect one detector at a time to the TIA. We also insert an intensity modulator driven by a 10 GHz pulse pattern generator in the system so that only 1 every 10 pulses of the pulse train generated by the mode-locked laser is selected, and the spacing between the pulses becomes 1 ns instead of 100 ps as in the QKD experiments. This is necessary to infer the quality of the detection signal from the time interval analyzer data. Under these conditions, a typical detection signal from the low-jitter up-conversion detector is shown in Fig. 6.4 for a count rate of 3×10^5 counts/s. The FWHM of the signal is only 30 ps, while the FWTM, which is a more appropriate figure of merit as we explained in Sec. 5.4, is 116 ps. These values are smaller than the corresponding values for the signal in Fig. 6.4 since much shorter pulses are used for this measurement. Fig. 6.5 shows experimental results for the FWHM and FWTM of the detection signal obtained for different count rates. Similarly to the corresponding behavior in Fig. 5.9, the FWHM remains below 40 ps even for high count rates, while the FWTM becomes significantly larger when the count rate exceeds 10^5 counts/s.

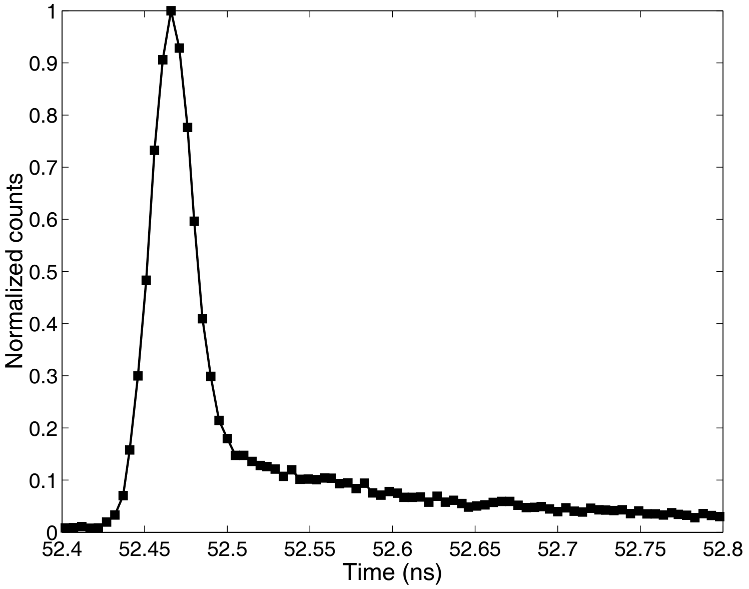

Figure 6.4: Typical detection signal from the up-conversion single-photon detector with a low-jitter Si APD when 10 ps pulses are used. This curve corresponds to DET2 and a count rate of 3×10^5 counts/s.

Although the measured timing jitter values are extremely beneficial for the 1 GHz DPS-QKD system that we described in Sec. 5.4, the effect of the long tail observed in Fig. 6.4 and quantified with the FWTM values in Fig. 6.5 is detrimental for the 10 GHz DPS-QKD system. With only 100 ps time separation between adjacent pulses this tail induces large errors in the next time slots, since counts from a bit in a certain time slot that are attributed to subsequent slots yield uncorrelated results and thus lead in errors. From Fig. 6.4 we can estimate the error rate due to this effect to be on the order of 9-10% for the adjacent slot, 5-6% for the second next slot, and 2-3% for the third next slot. Therefore, the timing jitter measurements reveal a source of large errors for the 10 GHz DPS-QKD system. In the next section, we show that this is indeed the predominant source of errors in the system, and prevents the generation of secret keys between Alice and Bob.

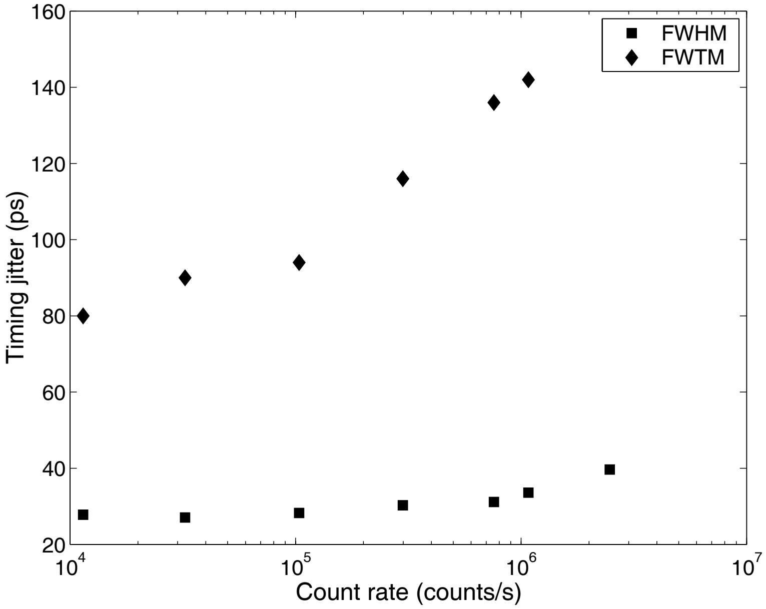

Figure 6.5: Timing jitter as a function of count rate for the low-jitter up-conversion detectors when 10 ps pulses are used.

6.3 Experimental results

For the experiments implementing the DPS-QKD protocol with low-jitter up-conversion detectors at a repetition rate of 10 GHz, we set the quantum efficiency and dark count rate of the low-jitter up-conversion detectors to 0.27% and 320 Hz, respectively. Due to the very narrow pulse width and the small FWHM of the detection signal in this system, we can decrease the measurement time window significantly while achieving at the same time a reasonable signal to noise ratio. For a 10 ps time window the effective dark counts are reduced to the very small value of $d = 3.2 \times 10^{-9}$ counts/time window, while the effective quantum efficiency factor takes values between 0.16 and 0.19, depending on the fiber length. Finally, based on Eq. (5.3) for the security analysis against general individual attacks and the experimental parameters we described, we set the average number of photons per pulse to 0.2. Under these conditions, we perform QKD experiments for 10, 30, 75, and 105 km of dispersion-shifted optical fiber. The experimental parameters and the results that we obtained are summarized

Table 6.1: Summary of fiber transmission experimental conditions and results for the 10 GHz DPS-QKD system with low-jitter up-conversion detectors.

Fiber length (km)	10	30	75	105
Fiber loss (dB)	2.4	6.5	16.1	22.1
Dark count rate (kHz) (each detector)	0.32	032	0.32	0.32
Quantum efficiency (%)	0.27	0.27	0.27	0.27
Time window width (ps)	10	10	10	10
Average photon number per pulse	0.2	0.2	0.2	0.2
Estimated bit error rate due to dark counts (%)	0.012	0.035	0.19	0.88
Bit error rate (%)	10.9	10.1	9.2	9.7
Portion of detected events in time window (%)	15.9	16.2	18.2	18.5
Sifted key generation rate (kbits/s)	267	93.8	15.5	3.69

in Table 6.1.

An interesting observation that we can make from this table is that the contribution of the dark counts to the error rate is extremely small, which is possible because of the use of a very narrow measurement time window. This fact is also verified by a second observation that the total bit error rate is nearly independent of the fiber length. The contribution of imperfect interference to the error rate is estimated to be about 1.1%, while the term in Eq. (5.2) related to the electrical noise is not negligible in the 10 GHz system due to an imperfect amplification system used to generate the 10 GHz modulation signal. It is estimated to contribute about 0.5-1% to the total error rate. All the remaining errors are attributed to the timing jitter effect. At small fiber losses the larger FWTM of the detection signal that we observed for larger count rates leads to a slightly increased error rate. The error rate is high for high fiber losses as well, however, partly because of the increased dark count contribution but mainly because of the dominating timing jitter induced errors. Unfortunately, the threshold error rate for secure key generation calculated from Eq. (5.3) with the experimental parameters that we used is 4.5%, so the error rate of about 10% that we measured does not allow the extraction of secure keys from the generated sifted keys for any fiber length. This threshold error rate is determined by the tight security requirements of the individual attacks analysis and imposes great limitations on the acceptable error levels in the system.

In Figs. 6.6 and 6.7 we plot the estimated error rate due to dark counts and the sifted key generation rate, respectively, as a function of the measurement time window width for the case of the 105 km experiment. As expected, the sifted key generation increases when the time window becomes wider because the effective quantum efficiency factor increases, but this happens at the expense of an increased error rate due to the larger contribution of the timing jitter induced errors. For time windows smaller than 10 ps, we observe a saturation of the error rate due to dark counts, which is expected because the number of errors due to dark counts included in the time window does not change significantly for these narrow widths.

6.4 Summary

In this chapter, we presented the experimental realization of a quantum key distribution system that implements the DPS-QKD protocol with low-jitter up-conversion detectors and operates at a repetition rate of 10 GHz. With this system, we generated sifted keys over 105 km of optical fiber with a bit error rate of 9.7%. This error rate was not sufficient to generate secure keys, and we showed that it is limited only by the timing jitter characteristics of the Si APD devices, since the dark count contribution was very small due to the narrow pulse width and the narrow FWHM of the detection signal. Therefore, by improving the timing jitter behavior of the single-photon detectors, it will be possible to achieve distribution of secure keys with the 10 GHz DPS-QKD system. Continuing research in the development of these detectors will undoubtedly yield the desired characteristics, and will thus enable the successful implementation of quantum key distribution at 10 GHz.

If we can eliminate the noise photons in the system and all losses except for the fiber loss, and achieve a negligible timing jitter compared to the pulse width, a 10 dB improvement in both the secure key generation rate and the maximum channel loss can be achieved with the 10 GHz system compared to the 1 GHz system. This will lead in megahertz secure key generation rates and key distribution distance exceeding

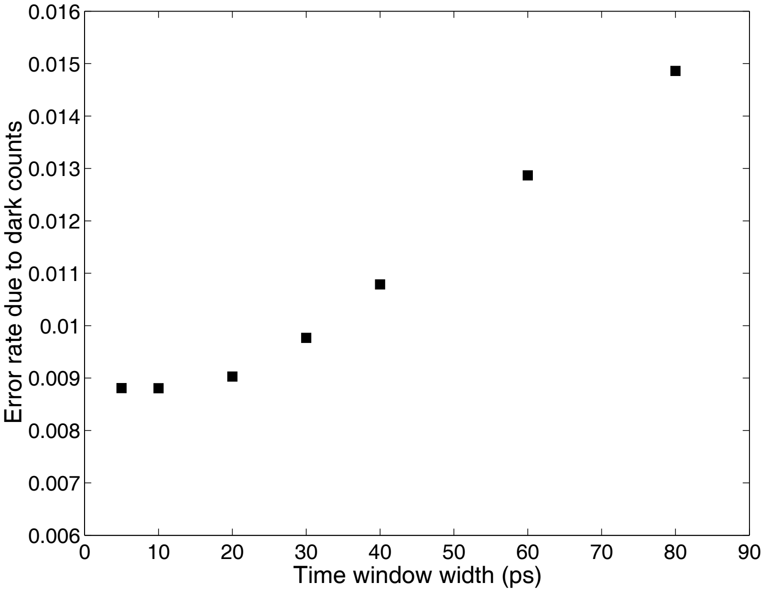

Figure 6.6: Experimental results for the bit error rate as a function of measurement time window width for the 105 km experiment.

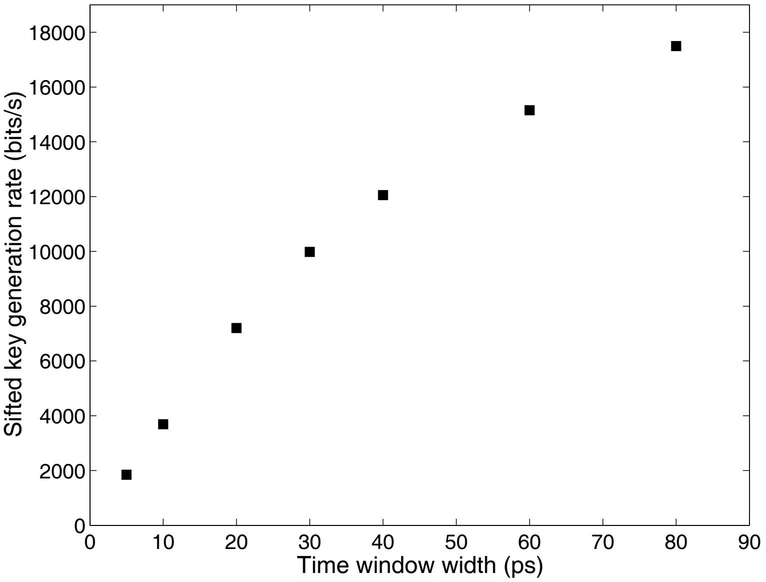

Figure 6.7: Experimental results for the sifted key generation rate as a function of measurement time window width for the 105 km experiment.

300 km. A practical quantum cryptography system with the above capabilities is a very appealing prospect, and opens the way to the integration of such systems in current telecommunication networks.

In the previous chapters, we have focused on quantum cryptography systems and we have shown that the 1.55 μm up-conversion single-photon detector is a useful tool for achieving enhanced performance of such systems. However, this simple and efficient single-photon detector that operates in high speed nongated mode, is also a very useful technology for classical applications requiring low light sensitivity in the infrared wavelength range, such as optical time domain reflectometry (OTDR) [100], laser detection and ranging (LADAR), and astronomy and deep-space communications. In the next chapter, we will present the experimental realization of a photon-counting OTDR system employing an up-conversion detector, and will discuss how this system benefits from the characteristics of this detector.

Chapter 7

Photon-counting optical time domain reflectometry

7.1 Introduction

Optical time domain reflectometry (OTDR) is a powerful and widely employed method for nondestructive and spatially resolved fault location and optical fiber and system characterization. This technique consists of sending a light pulse into the optical fiber under test and measuring the backscattered light. This backscattered light is due to essentially two physical mechanisms: the Fresnel reflections from fiber discontinuities, and the Rayleigh scattering. Since the velocity of the light in the fiber v is known, the optical backscattered power measured at a time t after the exciting light pulse gives information on the fiber attenuation characteristics at a distance $l = tv/2$, where the factor 2 is required since the light travels for a distance $2l$ from the injection point to the backscattering position and then back to the detector. It follows that if a small portion of the fiber needs to be characterized, the duration of the light pulse as well as the photodetector resolution must be sufficiently short. Except for the spatial resolution of the measurement, which determines how precisely the location of defects can be detected, another important figure of merit of an OTDR system is the sensitivity or dynamic range of the measurement, which determines the minimum detectable backscattered power and thus the maximum fiber length that can be measured. When shorter pulses are used to provide good spatial resolution, the signal to noise ratio is worse because of the smaller backscattered power, so the attainable dynamic range is smaller. This shows that there is a trade-off between spatial resolution and dynamic range in an OTDR measurement. Finally, an important figure of merit for an OTDR system is the total required time of the measurement.

Classical OTDR, which employs a photodiode in the analog regime as the detection apparatus [101], has been very successful in terms of the dynamic range of the measurement, achieving a 40 dB range, which corresponds to a fiber length of 200 km for a fiber with a loss coefficient of 0.2 dB/km. However, the spatial resolution of these systems is only in the kilometer range. Furthermore, classical systems suffer from the so called dead zones. More specifically, when a strong Fresnel reflection is detected by the photodetector, the preamplifier placed at the detector output is very likely to saturate. In this case, the small Rayleigh scattering of the subsequent fiber cannot be detected for a certain distance because the preamplifier has to recover from the nonlinear behavior. This effect defines the dead zone of the measurement, which is a well-known and serious problem in classical OTDR systems.

On the other hand, photon-counting OTDR (pc-OTDR), which employs a single-photon detector as the detection apparatus, does not feature dead zones. This is because while in classical OTDR the information is carried in the analog waveform of the detector pulse, in photon-counting OTDR the detector provides standard pulses and the information is carried in the time of occurrence of these pulses. Moreover, single-photon detectors feature better sensitivity and time resolution, characteristics very useful for the purpose of OTDR measurements. Due to all of the above reasons, photon-counting OTDR has received increasing attention as a potentially ideal technique for characterizing optical fiber networks.

Several pc-OTDR experiments have been performed at the telecommunication wavelengths of 1.3 μm and 1.5 μm with either centimeter spatial resolution or very large dynamic range. Some of the reported results are a 5 cm resolution with 0.04 dB dynamic range, corresponding to only 200 m of fiber [102], 100 m resolution with 25 dB range, corresponding to 125 km of fiber [103], and 1 km resolution with 44 dB range, corresponding to 220 km of fiber, which constitutes an improvement of 4 dB with respect to classical OTDR systems [104]. Possibly the most successful experiment in terms of achieving a good trade-off between spatial resolution and dynamic range is reported in [105], where a carefully designed system achieved a 15 cm spatial resolution with a 20 dB dynamic range, which corresponds to 100 km of optical fiber. In all these implementations, Ge or InGaAs/InP avalanche photodiode detectors (APDs) in Geiger mode were used. As we discussed in Sec. 4.2, these single-photon detectors exhibit high after-pulse probability, caused by charge carriers trapped during the avalanche process. These after-pulse effects can cause significant distortion of the OTDR data [105, 106]. To reduce this effect, the detectors have to be operated in gated mode. In QKD applications, we saw that this operation mode limits the attainable communication rate significantly. In applications like OTDR, where the arrival time of a signal photon is not known a priori, gated mode operation complicates the measurement process significantly. Gated measurement windows have to be used to access only parts of the fiber link at a time. However, even with gating, the effect of after-pulsing is still significant, and therefore post signal processing algorithms and/or control of the detector gate activation time is needed [105]. This results in a long measurement time and a complex control system.

In the following sections, we will present the implementation of a 1.55 μm photon-counting OTDR system that employs an up-conversion single-photon detector as the detection apparatus. We will first discuss the advantage that the use of this detector provides in terms of reduced measurement time. We will then describe the experimental setup and the results that we obtained with this system, and we will show that the nongated mode operation of the Si APD used in the up-conversion detector allows for a high speed pc-OTDR system without any need for a complex control system.

7.2 Measurement time calculation

To illustrate the advantage of the nongated up-conversion detector in terms of reduced measurement time, let us consider a simplified case. We assume that the backscattered light has a constant power for time duration ΔT, instead of a temporally decreasing power as in a real OTDR measurement. When a gated mode InGaAs/InP APD is used in the OTDR system, the signal photons are measured over a gate width Δt_{g} with a period t_{g}, and the gate position is changed to cover the entire time ΔT. If n_{g} is the number of repeated measurements for each gate position, the total number N of photons to be collected is:

$$N = n_{\mathrm{g}} \mu \eta \Delta T \tag{7.1}$$

where η is the quantum efficiency of the detector and μ is the number of photons per second in the signal. Then, the overall measurement time T_{g} is given by the expression:

$$T_{\mathrm{g}} = n_{\mathrm{g}} \Delta T \frac{t_{\mathrm{g}}}{\Delta t_{\mathrm{g}}} = \frac{N t_{\mathrm{g}}}{\mu \eta \Delta t_{\mathrm{g}}} \tag{7.2}$$

where $t_{\mathrm{g}}/\Delta t_{\mathrm{g}}$ is the number of different gate positions required to cover the time ΔT, and we have used Eq. (7.1) to derive the second part of the equation.

On the other hand, when an up-conversion single-photon detector is used in the OTDR system, no gating is needed but the dead time t_{d} of the Si APD effectively alters the measured signal, as we discussed when we derived Eq. (4.2) in Sec. 4.2. In this case, if n_{ng} is the number of repeated measurements, the total number N of collected photons is:

$$N = n_{\mathrm{ng}} \mu \eta \Delta T e^{-\mu \eta t_{\mathrm{d}}} \tag{7.3}$$

Then, the overall measurement time T_{ng} is given by the expression:

$$T_{\mathrm{ng}} = n_{\mathrm{ng}} \Delta T = \frac{N}{\mu \eta e^{-\mu \eta t_{\mathrm{d}}}} \tag{7.4}$$

Assuming the same quantum efficiency η for both detectors, as well as the same values for N and μ, Eqs. (7.2) and (7.4) give:

$$\frac{T_{\mathrm{g}}}{T_{\mathrm{ng}}} = \frac{e^{-\mu \eta t_{\mathrm{d}}} t_{\mathrm{g}}}{\Delta t_{\mathrm{g}}} \tag{7.5}$$

For the typical values $t_{\mathrm{g}} = 1$ μs, $\Delta t_{\mathrm{g}} = 1$ ns, $t_{\mathrm{d}} = 50$ ns, and given that the Si APD count rate per second $\mu\eta$ can reach 10^7 counts/s, we find:

$$\frac{T_{\mathrm{g}}}{T_{\mathrm{ng}}} \geq 0.6 \times 10^3 \tag{7.6}$$

This simple argument shows that by employing the up-conversion detector a photon-counting OTDR system can be almost 3 orders of magnitude faster than when it uses an InGaAs/InP APD.

7.3 Experimental setup

The experimental setup for the implementation of the pc-OTDR system with an up-conversion detector is shown in Fig. 7.1. The 1.55 μm continuous wave signal light enters an optical $\mathrm{LiNbO_3}$ intensity modulator, which is driven by a 200 MHz pulse pattern generator. A train of 5 ns pulses with a repetition rate of 4 kHz is generated. The pulse peak power at the input of the OTDR system is controlled by a variable attenuator and is set at -2.6 dBm (0.55 mW) for the measurement. Subsequently, the pulses enter a 3 dB optical splitter, one of the output ports of which is connected to the fibers under test. We used a combination of an 11 km dispersion-shifted fiber, a 13 km dispersion-shifted fiber, and a 12 m standard single mode fiber. The Rayleigh backscattered light and the strong Fresnel reflections from the connecting points of the fiber link enter the 1.55 μm up-conversion single-photon detector. There, the light is combined in the wavelength-division multiplexer shown in Fig. 4.5 with the 1.32 μm pump light and enters the fiber-pigtailed PPLN waveguide device. The sum frequency generated output is then detected by a single photon counting module (SPCM) based on a Si APD. We take OTDR data using the output electrical pulses of the pulse pattern generator and the SPCM to trigger a time interval analyzer (TIA). Gating of the detector is not required, and data from the entire fiber link are taken continuously. It is important to note that the birefringence of the fiber induces time-dependent fluctuation of the polarization of the backscattered light. On the other hand, the performance of the up-conversion detector is polarization dependent. To overcome this problem, the polarization of the input light is set using the half-wave

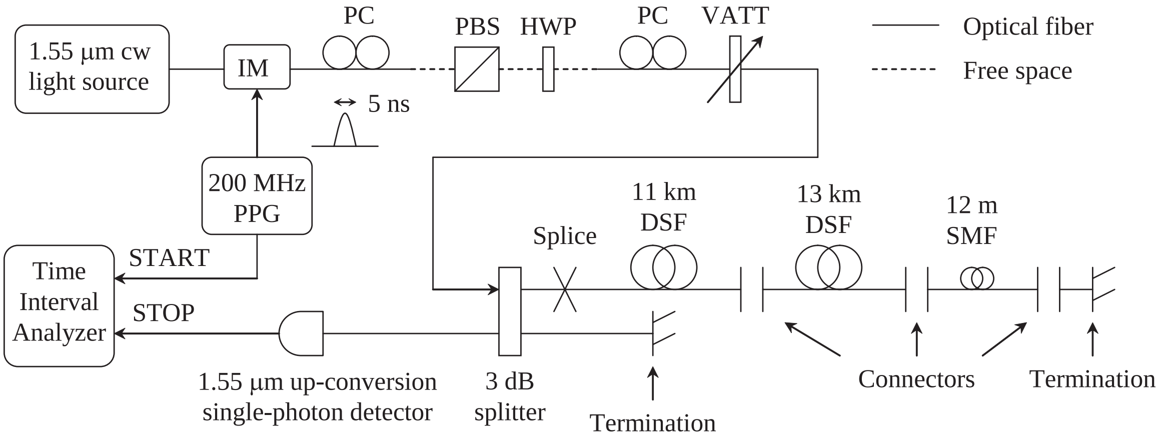

Figure 7.1: Experimental setup for the 1.55 μm pc-OTDR measurement. IM, intensity modulator; PC, polarization controller; PBS, polarizing beam splitter; HWP, half-wave plate; VATT, variable attenuator; DSF, dispersion-shifted fiber; SMF, single-mode fiber; PPG, pulse pattern generator.

plate shown in Fig. 7.1. Experimental data are taken for both horizontal and vertical polarization inputs and are subsequently added.

The choice of the operating point of the single-photon detector is of great importance for a photon counting OTDR system. This is because the minimum detectable power, which defines the sensitivity of the OTDR system, is determined by the noise equivalent power of the detector, defined as NEP $= h\nu\sqrt{2D}/\eta$, where $h\nu$ is the energy of the signal photon, D the dark count rate, and η the quantum efficiency. As we saw in Sec. 4.3, both the dark counts and the quantum efficiency of the up-conversion detector depend on the pump power, and consequently the NEP of the detector is also a function of the pump power. This is demonstrated in Fig. 7.2, where we show NEP values calculated from the quantum efficiency and dark count rate experimental data shown in Figs. 5.2 and 5.3, which correspond to the up-conversion detector that was employed in the pc-OTDR experiment. The NEP takes a minimum value of 2.4×10^{-16} W Hz$^{-1/2}$, which corresponds to a pump power at the entrance of the waveguide equal to 8 mW, $D = 5.7 \times 10^3$ counts/s, and $\eta = 5.8\%$. These conditions are chosen as the operating point of our experiment. In the next section, we present the results that we obtained with the described setup and procedure.

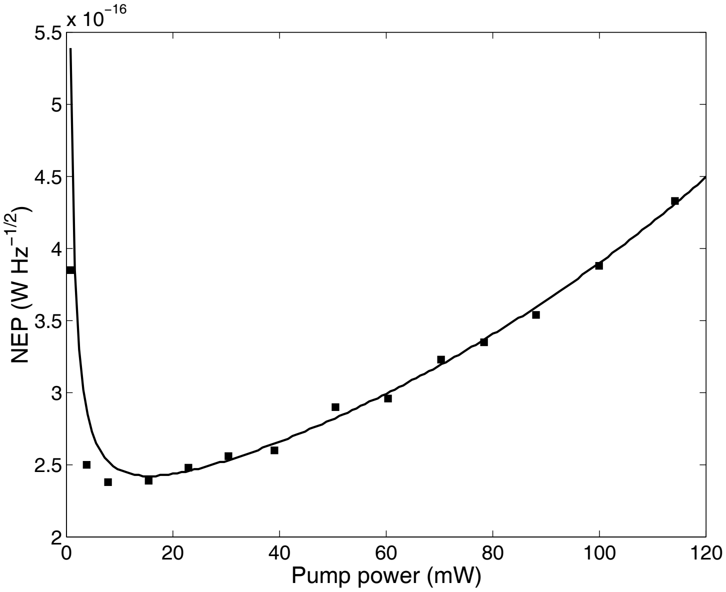

Figure 7.2: NEP of the up-conversion single-photon detector as a function of the pump power. The solid curve is derived from the fitting curves of the quantum efficiency and dark counts experimental data.

7.4 Experimental results

The experimental results for the main characteristics of the 1.55 μm photon-counting OTDR system, namely the dynamic range and the spatial resolution, are shown in Figs. 7.3 and 7.4, respectively.

Fig. 7.3 shows the measurement result for the backscattered signal power from the entire fiber link of 24 km as a function of fiber length. The measurement time was 12 min. As we observe in the figure, the statistical noise is rather large but can be significantly decreased by increasing the measurement time. A linear fit of the data corresponding to the two long fibers gives the values of 0.21 dB/km and 0.24 dB/km for the loss coefficient of the 11 and 13 km fibers, respectively. The exact length of the fibers can also be determined from this measurement and is 10.650 km and 12.848 km, respectively. We can observe the large Fresnel reflections from the connecting points as well as the loss of 3.2 dB at the connection between the two fibers. From the background noise level shown in Fig. 7.3 we can determine the peak

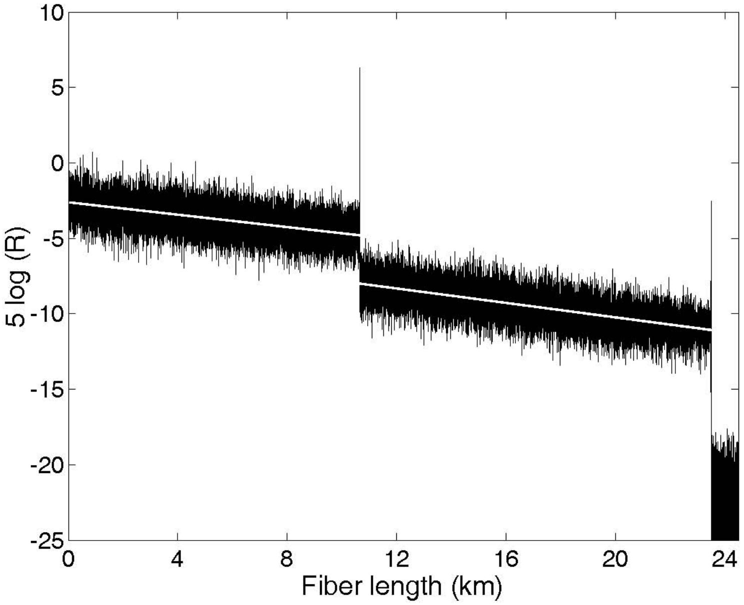

Figure 7.3: pc-OTDR measurement result for the link of 11 km, 13 km and 12 m fibers. R is the backscattered signal power normalized by its value at the splice point.

dynamic range of the pc-OTDR system to be 16 dB, which corresponds to the loss of 80 km of optical fiber. This means that measurement of up to 80 km of fiber is possible with this system, without changing the input power. The fact that we are able to measure this long distance in a short time is due to the nongated mode operation of the up-conversion single-photon detector, as well as the increased sensitivity achieved by careful tuning of the pump power. The dynamic range is limited in this case by the maximum peak input power we are allowed to let into the SPCM to avoid saturation of the detector owing to the large-power backscattered light at the leading edge. We can significantly increase the dynamic range by measuring different segments of the fiber link with a different input power, which can be realized, for example, by inserting a temporal switching function at the detector side. Another approach could be to appropriately gate the 1.32 μm pump in order to avoid up-conversion during the backscattering from the leading edge.

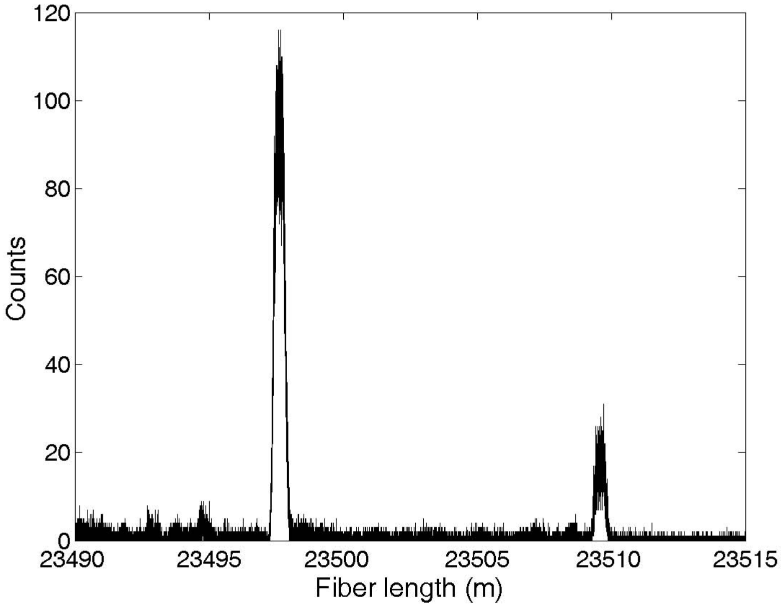

Figure 7.4: Time interval analyzer data for the 12 m fiber, indicating the 1 m spatial resolution of the pc-OTDR system.

The spatial resolution of the pc-OTDR system is explored in Fig. 7.4, which shows the time interval analyzer data for the 12 m single-mode fiber after 6 min of measurement time. We clearly observe the two reflection peaks from the connecting points, indicating that we can detect a 12 m fiber after a distance of 24 km with a spatial resolution of 1 m, determined by the 5 ns pulse width. Using shorter pulses in the same system can readily provide centimeter resolution.

7.5 Summary

In this chapter, we discussed the advantages that the nongated mode operation and the increased sensitivity of the up-conversion single-photon detector offer in the performance of a photon-counting optical time domain reflectometry system. The use of this detector allowed us to perform a continuous and fast pc-OTDR measurement with a simple and practical control system that does not require gate trains or post signal processing algorithms. With the pc-OTDR system that we implemented we achieved a good trade-off between spatial resolution and dynamic range. In particular, the system exhibits a dynamic range of 16 dB, which corresponds to measurement of up to 80 km of fiber without changing the input power, and 1 m spatial resolution. By measuring different segments of the fiber link with a different input power and using shorter pulses we can achieve even better performance of the photon-counting OTDR system.

Chapter 8

Conclusion

This thesis has presented a number of results in the field of quantum cryptography. To conclude, we would like to summarize our main results and discuss some avenues for further research.

We presented a new quantum cryptography algorithm, the differential phase shift quantum key distribution protocol, which uses attenuated coherent states of light as the information carrier, has a very simple system architecture, and requires standard telecommunication components for its implementation. We proved the security of this protocol first against a set of restricted attacks, namely the beamsplitter and intercept and resend attacks. We then extended the security proof to the most general individual attacks allowed by quantum mechanics and photon number splitting attacks. The security proof revealed that the protocol is very robust to powerful attacks that are the main limiting factor in weak laser light implementations of the standard BB84 protocol, and thus enhances considerably the communication speed and distance of a quantum cryptography system.

We then described a new single-photon detector, the up-conversion detector, which uses frequency up-conversion of infrared light in a periodically poled lithium niobate waveguide and subsequent detection of the near-infrared output by a silicon avalanche photodiode to achieve high speed and efficient single-photon detection in the telecommunication wavelength band. We demonstrated an overall quantum efficiency of 46%

at 1.55 μm and we analyzed the source of the high dark counts that the detector exhibited. We also showed that the nongated mode operation of this detector and the tunability offered by the pump power dependence of its characteristics can enhance significantly the performance of a quantum cryptography system.

The differential phase shift quantum key distribution protocol and the up-conversion detectors were subsequently combined to perform quantum key distribution experiments at repetition rates of 1 and 10 GHz. When the security analysis for general individual attacks was taken into account, the 1 GHz system achieved a sifted key generation rate of 1 Mbit/s over 20 km of optical fiber, and secure key distribution over 75 km. These results demonstrated the great potential of this system, while highlighting at the same time the limitations imposed by the timing jitter characteristics of the single-photon detectors. By replacing these detectors with newly developed low-jitter detectors, we demonstrated a quantum cryptography system that achieved a 2 Mbits/s sifted key generation rate over 10 km, and secure key distribution at a rate of 166 bits/s over 100 km of optical fiber. Compared to the best experiments reported to date, these results constitute an improvement of more than two orders of magnitude in communication speed and a factor of two in communication distance. On the other hand, the 10 GHz system did not yield secure keys, due to the tight requirements that this system imposes on the characteristics of the single-photon detectors. With this system, we generated sifted keys over 105 km of fiber with a bit error rate of 9.7%, which is only limited by the timing jitter of the detectors.

The above results demonstrate that practical and secure high speed and long-distance quantum cryptography is possible with currently available technology. The 1 GHz system that we have presented achieves a sufficiently high communication rate and a long enough communication distance to be able to operate in a standard telecommunication network. Of course, improvements in the timing jitter characteristics of silicon avalanche photodiodes as well as the dark count behavior of the up-conversion detectors, to be expected in the coming years, will enhance even more the performance of the quantum cryptography systems that we have implemented. For example, single-photon detectors with Gaussian response and very narrow FWHM may soon become available, and the dark counts of the up-converter can be reduced by two orders of magnitude at 1.55 μm if we use a pump wavelength that is longer than the signal wavelength. Then, megahertz secure key generation rates will be possible, and the distance over which a repeater system is required will be extended to more than 300 km. This will open the way for extremely long distance point to point secure communication.

The differential phase shift quantum key distribution protocol can also be implemented in a quantum cryptography system employing other types of infrared single-photon detectors, that may potentially present desirable characteristics for this purpose. These could include superconducting single-photon detectors (SSPD), which have very low dark counts, small timing jitter, and almost Gaussian response, or hybrid detectors consisting of photomultiplier tubes and avalanche photodiodes that are under development and may also feature the required timing jitter and dark count behavior. Similarly, the up-conversion single-photon detectors can be used in a quantum cryptography system implementing a different protocol, for example the entanglement-based BBM92 protocol, which can withstand larger quantum channel losses and has the potential of enabling very long distance quantum key distribution. Finally, on the theoretical side, the proof of unconditional security for the DPS-QKD protocol will be required to guarantee the security of quantum cryptography systems implementing this protocol against coherent eavesdropping attacks.

Except for quantum cryptography, the ideas and tools that we have developed in this work can be useful for other fields in the area of quantum information processing and communications, such as quantum computation and quantum teleportation. Systems like the ones we implemented, that combine the well established telecommunication technology with new ideas from quantum and nonlinear optics, will be an indispensable part of any future quantum network consisting of quantum computers, quantum memories, and quantum repeaters, all subjects of intense research efforts worldwide. The architecture, security, and topology of such quantum networks is a new research field that attracts the attention of electrical engineers, computer scientists, and physicists due to the interesting challenges that it presents. With the rapid progress in this field, simple tasks in quantum networking will soon be within technological reach.

Finally, we showed that the up-conversion single-photon detector can be useful for classical applications as well by demonstrating a simple and fast photon-counting optical time domain reflectometry measurement system that achieved a good trade-off between spatial resolution and dynamic range. Other applications that can benefit from the high speed nongated mode operation of this detector are laser detection and ranging, and deep-space communications.

References

[1] P. Shor, “Algorithms for quantum computation: Discrete logarithm and factoring,” in *Proceeding of the 35th Annual Symposium on the Foundations of Computer Science, Santa Fe, New Mexico,* pp. 124–134 (IEEE Computer Society Press, Los Alamitos, California, 1994).

[2] L. Grover, “A fast quantum mechanical algorithm for database search,” in *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing (STOC), Philadelphia, Pennsylvania,* pp. 212–219 (May 1996).

[3] J. I. Cirac and P. Zoller, “Quantum Computations with Cold Trapped Ions,” *Physical Review Letters* **74**, 4091–4094 (1995).

[4] J.-M. Raimond, M. Brune, and S. Haroche, “Colloquium: Manipulating quantum entanglement with atoms and photons in a cavity,” *Review of Modern Physics* **73**, 565–582 (2001).

[5] B. E. Kane, “A silicon-based nuclear spin quantum computer,” *Nature* **393**, 133–137 (1998).

[6] E. Knill, R. Laflamme, and G. J. Milburn, “A scheme for efficient quantum computation with linear optics,” *Nature* **409**, 46–52 (2001).

[7] L. M. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang, “Experimental realization of Shor’s quantum factoring algorithm using nuclear magnetic resonance,” *Nature* **414**, 883–887 (2001).

[8] S. Gulde, M. Riebe, G. P. Lancaster, C. Becher, J. Eshner, H. Haffner, F. Schmidt-Kaler, I. L. Chuang, and R. Blatt, “Implementation of the Deutsch-Josza algorithm on an ion-trap quantum computer,” *Nature* **421**, 48–50 (2003).

[9] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in *Proceeding of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India,* pp. 175–179 (IEEE, New York, 1984).

[10] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, “Experimental quantum cryptography,” *Journal of Cryptology* **5**, 3–28 (1992).

[11] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden, “Pulsed energy-time entangled twin-photon source for quantum communication,” *Physical Review Letters* **82**, 2594 (1999).

[12] J. J. Sakurai, *Modern Quantum Mechanics* (Addison Wesley, 1995).

[13] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information* (Cambridge University Press, Cambridge, MA, 2000).

[14] M. O. Scully and M. S. Zubairy, *Quantum optics* (Cambridge University Press, Cambridge, MA, 1997).

[15] N. Lütkenhaus, “Security against individual attacks for realistic quantum key distribution,” *Physical Review A* **61**, 052 304 (2000).

[16] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, “Limitations on Practical Quantum Cryptography,” *Physical Review Letters* **85**, 1330–1333 (2000).

[17] E. Waks, K. Inoue, C. Santori, D. Fattal, J. Vuckovic, G. S. Solomon, and Y. Yamamoto, “Quantum cryptography with a photon turnstile,” *Nature* **420**, 762 (2002).

[18] A. Beveratos, R. Brouri, T. Gacoin, A. Villig, J.-P. Poizat, and P. Grangier, “Single Photon Quantum Cryptography,” *Physical Review Letters* **89**, 187 901 (2002).

[19] C. Santori, D. Fattal, J. Vuckovic, G. S. Solomon, and Y. Yamamoto, "Indistinguishable photons from a single-photon device," *Nature* **419**, 594 (2002).

[20] A. Beveratos, S. Kuhn, R. Brouri, T. Gacoin, J.-P. Poizat, and P. Grangier, "Room temperature stable single-photon source," *European Physical Journal D* **18**, 191 (2002).

[21] S. Fasel, O. Alibart, S. Tanzilli, P. Baldi, A. Beveratos, N. Gisin, and H. Zbinden, "High-quality asynchronous heralded single-photon source at telecom wavelength," *New Journal of Physics* **6**, 163 (2004).

[22] E. Waks, C. Santori, and Y. Yamamoto, "Security aspects of quantum key distribution with sub-Poisson light," *Physical Review A* **66**, 042 315 (2002).

[23] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Review of Modern Physics* **74**, 145–195 (2002).

[24] J. F. Clauser and A. Shimony, "Bell's theorem - experimental tests and implications," *Reports on Progress in Physics* **41**, 1881–1927 (1978).

[25] P. G. Kwiat, K. Mattle, H. Weinfurter, and A. Zeilinger, "New high-intensity source of polarization entangled photon pairs," *Physical Review Letters* **75**, 4337–4341 (1995).

[26] M. A. Rowe, D. Kielpinski, V. Meyer, C. A. Sackett, W. M. Itano, C. Monroe, and D. J. Wineland, "Experimental violation of a Bell's inequality with efficient detection," *Nature* **409**, 791–794 (2001).

[27] D. Fattal, K. Inoue, C. Santori, J. Vuckovic, G. S. Solomon, and Y. Yamamoto, "Entanglement Formation and Violation of Bell's Inequality with a Semiconductor Single Photon Source," *Physical Review Letters* **92**, 037 903 (2004).

[28] O. Benson, C. Santori, M. Pelton, and Y. Yamamoto, "Regulated and entangled photons from a single quantum dot," *Physical Review Letters* **84**, 2513–2516 (2000).

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

[30] M. Koashi and N. Imoto, “Quantum cryptography based on split transmission of one-bit information in two setps,” *Physical Review Letters* **79**, 2383–2386 (1997).

[31] B. Huttner, N. Imoto, N. Gisin, and T. Mor, “Quantum cryptography with coherent states,” *Physical Review A* **51**, 1863–1869 (1995).

[32] A. K. Ekert, “Quantum cryptography based on Bell’s theorem,” *Physical Review Letters* **67**, 661–663 (1991).

[33] C. H. Bennett, G. Brassard, and N. Mermin, “Quantum cryptography without Bell’s theorem,” *Physical Review Letters* **68**, 557–559 (1992).

[34] D. Welsh, *Codes and cryptography* (Clarendon Press, Oxford, UK, 1998).

[35] G. Brassard and L. Salvail, “Secret-key reconciliation by public discussion,” in *Advances in Cryptology-EUROCRYPT’93 (T. Helleseth, ed.), Vol. 765 of Lecture Notes in Computer Science,* pp. 410–423 (Springer-Verlag, Berlin, 1994).

[36] N. Lütkenhaus, “Estimates for practical quantum cryptography,” *Physical Review A* **59**, 3301–3319 (1999).

[37] A. K. Ekert, B. Huttner, G. M. Palma, and A. Peres, “Eavesdropping on quantum-cryptographical systems,” *Physical Review A* **50**, 1047–1056 (1994).

[38] B. Huttner and A. K. Ekert, “Information gain in quantum eavesdropping,” *Journal of Modern Optics* **41**, 2455–2466 (1994).

[39] C. A. Fuchs, N. Gisin, R. B. Griffiths, C. S. Niu, and A. Peres, “Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy,” *Physical Review A* **56**, 1163–1172 (1997).

[40] B. A. Slutsky, R. Rao, P. C. Sun, and Y. Fainman, "Security of quantum cryptography against individual attacks," *Physical Review A* **57**, 2383–2398 (1998).

[41] E. Biham and T. Mor, "Security of quantum cryptography against collective attacks," *Physical Review Letters* **78**, 2256–2259 (1997).

[42] P. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Physical Review Letters* **85**, 441–444 (2000).

[43] H. Inamori, N. Lütkenhaus, and D. Mayers, "Unconditional security of practical quantum key distribution," (2001), quant-ph/0107017.

[44] H.-K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," *Science* **283**, 2050–2056 (1999).

[45] D. Mayers and A. Yao, "Quantum cryptography with imperfect apparatus," in *39th Annual Symposium on Foundations of Computer Science-FOCS'98,* p. 503 (IEEE Computer Society, Palo Alto, CA, 1998).

[46] H. Inamori, L. Rallan, and V. Vedral, "Security of EPR-based quantum cryptography against incoherent symmetric attacks," *Journal of Physics A: Mathematical and General* **34**, 6913–6918 (2001).

[47] H. Ashauer and H. J. Briegel, "Private Entanglement over Arbitrary Distances, Even Using Noisy Apparatus," *Physical Review Letters* **88**, 047 902 (2002).

[48] E. Waks, A. Zeevi, and Y. Yamamoto, "Security of quantum key distribution with entangled photons against individual attacks," *Physical Review A* **65**, 052 310 (2002).

[49] K. Tamaki, M. Koashi, and N. Imoto, "Security of the Bennett 1992 quantum key distribution protocol against individual attack over a realistic channel," *Physical Review A* **67**, 032 310 (2003).

[50] K. Tamaki, M. Koashi, and N. Imoto, "Unconditionally Secure Key Distribution Based on Two Nonorthogonal States," *Physical Review Letters* **90**, 167 904 (2003).

[51] K. Tamaki and N. Lütkenhaus, "Unconditional security of the Bennett 1992 quantum key-distribution protocol over a lossy and noisy channel," *Physical Review A* **69**, 032 316 (2004).

[52] M. Koashi, "Unconditional Security of Coherent-State Quantum Key Distribution with a Strong Phase-Reference Pulse," *Physical Review Letters* **93**, 120 501 (2004).

[53] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Transactions on Information Theory* **41**, 1915–1923 (1995).

[54] N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner, and V. Scarani, "Towards practical and fast quantum cryptography," (2004), quant-ph/0411022.

[55] A. Yoshizawa, R. Kaji, and H. Tsuchida, "10.5 km Fiber-Optic Quantum Key Distribution at 1550 nm with a Key Rate of 45 kHz," *Japanese Journal of Applied Physics* **43**, L735–L737 (2004).

[56] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, "Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations," *Physical Review Letters* **92**, 057 901 (2004).

[57] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Fast and simple one-way quantum key distribution," *Applied Physics Letters* **87**, 194 108 (2005).

[58] H.-K. Lo, X. Ma, and K. Chen, "Decoy State Quantum Key Distribution," *Physical Review Letters* **94**, 230 504 (2005).

[59] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Physical Review A* **72**, 012 326 (2005).

[60] X.-B. Wang, "Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptograpy," *Physical Review Letters* **94**, 230 503 (2005).

[61] K. Inoue, E. Waks, and Y. Yamamoto, "Differential Phase Shift Quanum Key Distribution," *Physical Review Letters* **89**, 037 902 (2002).

[62] K. Inoue, E. Waks, and Y. Yamamoto, "Differential-phase-shift quanum key distribution using coherent light," *Physical Review A* **68**, 022 317 (2003).

[63] H.-K. Lo and J. Preskill, "Phase randomization improves the security of quantum key distribution," (2005), quant-ph/0504209.

[64] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, "'Plug and play' systems for quantum cryptography," *Applied Physics Letters* **70**, 793–795 (1996).

[65] M. Bourennane, F. Gibson, A. Karlsson, A. Hening, P. Jonsson, T. Tsegaye, D. Ljunggren, and E. Sundberg, "Experiments on long wavelength (1550 nm) 'plug and play' quantum cryptography systems," *Optics Express* **4**, 383–387 (1999).

[66] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, "Quantum key distribution over 67 km with a plug&play system," *New Journal of Physics* **4**, 41.1–41.8 (2004).

[67] E. Waks, H. Takesue, and Y. Yamamoto, "Security of differential-phase-shift quantum key distribution against individual attacks," *Physical Review A* **73**, 012 344 (2006).

[68] D. S. Bethune, W. P. Risk, and G. W. Pabst, "A high-performance integrated single-photon detector for telecom wavelengths," *Journal of Modern Optics* **51**, 1359–1368 (2004).

[69] D. Stucki, G. Ribordy, A. Stefanov, H. Zbinden, J. Rarity, and T. Wall, "Photon counting for quantum key distribution with Peltier cooled InGaAs/InP APDs," *Journal of Modern Optics* **48**, 1967–1981 (2001).

[70] M. Bourennane, A. Karlsson, J. Ciscar, and M. Mathés, "Single-photon detectors in the telecom wavelength region of 1550 nm for quantum information processing," *Journal of Modern Optics* **48**, 1983–1995 (2001).

[71] C. Gobby, Z. L. Yuan, and A. J. Shields, "Unconditionally secure quantum key distribution over 50 km of standard telecom fibre," *Electronics Letters* **40**, 1603–1605 (2004).

[72] G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, "Fast and user-friendly quantum key distribution," *Journal of Modern Optics* **47**, 517–531 (2000).

[73] M. M. Fejer, G. A. Magel, D. H. Jundt, and R. L. Byer, "Quasi-Phase-Matched Second Harmonic Generation: Tuning and Tolerances," *IEEE Journal of Quantum Electronics* **28**, 2631–2654 (1992).

[74] R. V. Roussev, C. Langrock, J. R. Kurz, and M. M. Fejer, "Periodically poled lithium niobate waveguide sum-frequency generator for efficient single-photon detection at communication wavelengths," *Optics Letters* **29**, 1518–1520 (2004).

[75] K. R. Parameswaran, R. K. Route, J. R. Kurz, R. V. Roussev, M. M. Fejer, and M. Fujimura, "Highly-efficient second harmonic generation in buried waveguides formed by annealed and reverse proton exchange in periodically poled lithium niobate," *Optics Letters* **27**, 179–181 (2002).

[76] M. Taya, M. C. Bashaw, and M. M. Fejer, "Photorefractive effects in periodically poled ferroelectrics," *Optics Letters* **21**, 857–859 (1996).

[77] M. A. Albota and F. N. C. Wong, "Efficient single-photon counting at 1.55 μm by means of frequency upconversion," *Optics Letters* **29**, 1449–1451 (2004).

[78] A. V. Vandevender and P. G. Kwiat, "High efficiency single photon detection via frequency up-conversion," *Journal of Modern Optics* **51**, 1433–1445 (2004).

[79] A. J. Miller, S. W. Nam, J. M. Martinis, and A. V. Sergienko, "Demonstration of a low-noise near-infrared photon counter with multiphoton discrimination," *Applied Physics Letters* **83**, 791–793 (2003).

[80] P. D. Townsend, J. G. Rarity, and P. R. Tapster, "Single photon interference in 10 km long optical fibre interferometer," *Electronics Letters* **29**, 634 (1993).

[81] R. J. Hughes, G. L. Morgan, and C. G. Peterson, "Quantum key distribution over a 48 km optical fibre network," *Journal of Modern Optics* **47**, 533–547 (2000).

[82] C. Gobby, Z. L. Yuan, and A. J. Shields, "Quantum key distribution over 122 km of standard telecom fiber," *Applied Physics Letters* **84**, 3762–3764 (2004).

[83] Z. L. Yuan and A. J. Shields, "Continuous operation of a one-way quantum key distribution system over installed telecom fibre," *Optics Express* **13**, 660–665 (2005).

[84] D. Rosenberg, S. W. Nam, P. A. Hiskett, C. G. Peterson, R. J. Hughes, J. E. Nordholt, A. E. Lita, and A. J. Miller, "Quantum key distribution at telecom wavelengths with noise-free detectors," *Applied Physics Letters* **88**, 021 108 (2006).

[85] K. J. Gordon, V. Fernandez, P. D. Townsend, and G. S. Buller, "A Short Wavelength GigaHertz Clocked Fiber-Optic Quantum Key Distribution System," *IEEE Journal of Quantum Electronics* **40**, 900–908 (2004).

[86] K. J. Gordon, V. Fernandez, G. S. Buller, I. Rech, S. D. Cova, and P. D. Townsend, "Quantum key distribution system clocked at 2 GHz," *Optics Express* **13**, 3015–3020 (2005).

[87] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, "Experimental Quantum Key Distribution with Decoy States," *Physical Review Letters* **96**, 070 502 (2006).

[88] S. Fasel, N. Gisin, G. Ribordy, and H. Zbinden, "Quantum key distribution over 30 km of standard fiber using time-energy entangled photon pairs: a comparison

of two chromatic dispersion reduction methods," *European Physical Journal D* **30**, 143–148 (2004).

[89] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, "Quantum Cryptography with Entangled Photons," *Physical Review Letters* **84**, 4729–4732 (2000).

[90] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, "Quantum Cryptography Using Entangled Photons in Energy-Time Bell States," *Physical Review Letters* **84**, 4737–4740 (2000).

[91] G. Ribordy, J. Brendel, J.-D. Gautier, N. Gisin, and H. Zbinden, "Long-distance entanglement-based quantum key distribution," *Physical Review A* **63**, 012 309 (2001).

[92] M. Aspelmeyer, H. R. Böhm, T. Gyatso, T. Jennewein, R. Kaltenbaek, M. Lindenthal, G. Molina-Terriza, A. Poppe, K. Resch, M. Taraba, R. Ursin, P. Walther, and A. Zeilinger, "Long-Distance Free-Space Distribution of Quantum Entanglement," *Science* **301**, 621–623 (2003).

[93] H.-J. Briegel, W. Dür, , J. I. Cirac, and P. Zoller, "Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication," *Physical Review Letters* **81**, 5932–5935 (1998).

[94] J. I. Cirac, P. Zoller, H. J. Kimble, and H. Mabuchi, "Quantum State Transfer and Entanglement Distribution among Distant Nodes in a Quantum Network," *Physical Review Letters* **78**, 3221–3224 (1997).

[95] M. D. Lukin, M. Fleischhauer, A. S. Zibrov, H. G. Robinson, V. L. Velichansky, L. Hollberg, and M. O. Scully, "Spectroscopy in Dense Coherent Media: Line Narrowing and Interference Effects," *Physical Review Letters* **79**, 2959–2962 (1997).

[96] L. V. Hau, S. E. Harris, Z. Dutton, and C. H. Behroozi, "Light speed reduction to 17 metres per second in an ultracold atomic gas," *Nature* **397**, 594–598 (1999).

[97] A. Himeno, K. Kato, and T. Miya, "Silica-based planar lightwave circuits," *IEEE Journal of Selected Topics in Quantum Electronics* **4**, 913–924 (1998).

[98] T. Honjo, K. Inoue, and H. Takahashi, "Differential-phase-shift quanum key distribution experiment with a planar light-wave circuit Mach-Zehnder interferometer," *Optics Letters* **29**, 2797–2799 (2004).

[99] R. T. Thew, S. Tanzilli, L. Krainer, S. C. Zeller, A. Rochas, I. Rech, S. Cova, H. Zbinden, and N. Gisin, "Low jitter up-conversion detectors for telecom wavelength GHz QKD," *New Journal of Physics* **8**, 32 (2006).

[100] B. K. Garside and R. E. Park, "Minimum detectable changes in Rayleigh backscatter from distributed fiber sensors," in *Fiber Optic Smart Structures and Skins IV (R. O. Claus and E. Udd, eds.), Proceedings of SPIE - The International Society for Optical Engineering* **1588**, 150–158 (SPIE, Bellingham, WA, 1991).

[101] D. Derickson, *Fiber Optic Test and Measurement* (HP Professional Books, Prentice-Hall, Upper Saddle River, NJ, 1998).

[102] A. Lacaita, P. A. Francesco, S. Cova, and G. Ripamonti, "Single-photon optical-time domain reflectometer at 1.3 μm with 5-cm resolution and high sensitivity," *Optics Letters* **18**, 1110–1112 (1993).

[103] B. F. Levine, C. G. Bethea, and J. C. Campbell, "1.52 μm room-temperature photon-counting optical time domain reflectometer," *Electronics Letters* **21**, 194–196 (1985).

[104] F. Scholder, J.-D. Gautier, M. Wegmüller, and N. Gisin, "Long-distance OTDR using photon counting and large detection rates at telecom wavelength," *Optics Communications* **213**, 57–61 (2002).

[105] M. Wegmüller, F. Scholder, and N. Gisin, "Photon-Counting OTDR for Local Birefrigence and Fault Analysis in the Metro Environment," *Journal of Lightwave Technology* **22**, 390–400 (2004).

[106] G. Ripamonti, F. Zappa, and S. Cova, “Effects of Trap Levels in Single-Photon Optical Time-Domain Reflectometry: Evaluation and Correction,” *Journal of Lightwave Technology* **10**, 1398–1402 (1992).