Performance monitoring for quantum key distribution systems

Yu, Timothy Shengrong

2014

Yu, T. S. (2014). Performance monitoring for quantum key distribution systems. Master's thesis, Nanyang Technological University, Singapore.

<https://hdl.handle.net/10356/65360>

<https://doi.org/10.32657/10356/65360>

**PERFORMANCE MONITORING
FOR
QUANTUM KEY DISTRIBUTION SYSTEMS**

YU SHENGRONG TIMOTHY

School of Electrical & Electronic Engineering

A thesis submitted to the Nanyang Technological University
in partial fulfilment of the requirement for the degree of
Master of Engineering

2014

STATEMENT OF ORIGINALITY

I hereby certify that the content of this thesis is the result of original research done by me and has not been submitted for a higher degree to any other university or institute.

Date

Yu Shengrong Timothy

ACKNOWLEDGEMENTS

Firstly, I would like to express my immense gratitude to my supervisors, Assistant Professor Luan Feng and Dr. Lim Han Chuen for their patience and guidance. I am also truly grateful to Mr. Yap Jiunyan for his invaluable help and comments on my work. I would like to extend my thanks to the staff and students in the Fibre Technology Lab for their kind assistance.

I would also like to thank Nanyang Technological University, School of Electrical and Electronic Engineering for providing me with the opportunity to carry out my research work.

Lastly, I would like to thank my family for their patience and support over the years. Without their encouragement, this thesis would not have been possible.

ABSTRACT

In 1946, C. E. Shannon proved that One-Time Pad is truly unbreakable [1]. However, stringent conditions pose difficulties such as the key distribution problem which limited its practicability. Fortunately, public key cryptosystem widely used today was developed to solve the key distribution problem. Its security is based on the assumption that an adversary has limited computational power to factor a number with large prime factors. With the increase in computational power and technological advancement, this security may one day be compromised.

In contrast, quantum key distribution (QKD) offers a platform for secure key distribution and everlasting secrecy. Unlike conventional cryptography, quantum key distribution's security is governed by the laws of quantum mechanics. The basic principle of quantum key distribution is to encode classical binary bit information onto the properties of quantum states such as the polarisation of a photon. Because of the quantum no-cloning theorem, an eavesdropper is unable to simply duplicate these photons. Moreover, by intercepting these photons, the eavesdropper will leave detectable trace which will reveal its presence.

In 1989, the first experimental demonstration of QKD using the polarisations of single photons based on the BB84 protocol occurred through 32cm of air [2]. Since then, QKD over hundreds of kilometres of optical fibre

and free space have been reported [3-5]. Key generation rate of a few megahertz have also been demonstrated [6-8]. However, photons travelling through optical fibres are subjected to random polarisation drifts. Moreover, clock drifts often causes inaccuracy during the detection of these photons. If these performance issues were not addressed, the reliability and availability of QKD systems and their cryptographic keys will be affected.

Therefore, polarisation recovery schemes have been implemented to mitigated polarisation drifts [9-14]. However, these schemes often limit the transmission distance, slow down or even disrupt the key generation process for polarisation recovery. These limitations lead to the proposed development of a polarisation-encoded QKD system based on an adaptive polarisation state monitoring and recovery scheme that adapts the system to the existing polarisation drift condition in the transmission link to enhance its reliability and availability.

On the other hand, current high-speed single-photon detection schemes are often designed to work with idealised parameters such as fixed gating rate and operating temperature. Therefore, such schemes are unable to accommodate changes in gating frequency induced by clock drifts which results in the reduction of detection efficiency. Hence, a proposed robust high-speed single-photon avalanche diode with tunable sinusoidal gate frequency was developed to mitigate the effect caused by clock drift in order to maintain the detection efficiency over varying operating conditions.

TABLE OF CONTENTS

STATEMENT OF ORIGINALITY	i
ACKNOWLEDGEMENTS	ii
ABSTRACT.....	iii
TABLE OF CONTENTS	v
LIST OF FIGURES	viii
ACRONYMS.....	xv
CHAPTER 1 INTRODUCTION	1
1.1 BACKGROUND	1
1.2 MOTIVATIONS	3
1.3 OBJECTIVES AND SCOPE.....	6
1.4 ORGANISATION OF THESIS	6
1.5 MAJOR CONTRIBUTIONS OF THESIS.....	7
CHAPTER 2 REVIEW OF QUANTUM KEY DISTRIBUTION AND SINGLE PHOTON DETECTION	8
2.1 QUANTUM KEY DISTRIBUTION.....	8
2.1.1 BB84 Protocol	8
2.1.2 Polarisation Recovery In Quantum Key Distribution Systems	13
2.1.3 “Interruption” Polarisation Recovery Scheme	15
2.1.4 “Real-time” Polarisation Recovery Scheme.....	18
2.2 SINGLE PHOTON DETECTION	24
2.2.1 Equivalent Circuit Model	25
2.2.2 Measures of Performance	26
2.2.2.1 Detection Efficiency.....	27
2.2.2.2 Afterpulsing.....	27
2.2.2.3 Dark Counts.....	28
2.2.3 Geiger Mode Operation.....	28

	2.2.3.1	Passive Quenching	29
	2.2.3.2	Gated-mode Operation	30
	2.2.4	Single Photon Detection Schemes.....	33
	2.2.4.1	Self-Differencing.....	33
	2.2.4.2	Sinusoidal Gating With Band-Stop Filter	34
	2.2.4.3	Sinusoidal Gating with Phase-shifter	37
CHAPTER 3		ADAPTIVE POLARISATION STATE MONITORING AND RECOVERY SCHEME FOR POLARISATION-ENCODED QUANTUM KEY DISTRIBUTION SYSTEMS.....	39
3.1		PRINCIPLE OF OPERATION	40
3.1.1		Generation of Quantum and Reference Signals	43
3.1.2		Synchronisation	47
3.1.3		Detecting the Quantum and Reference Signals	49
3.1.4		Polarisation Control Theory	51
3.1.5		Adaptive polarisation state monitoring and recovery..	55
3.1.6		Leakage of Reference Signals into SPAD.....	58
3.1.7		Sifted Key Rate	60
3.2		EXPERIMENTAL RESULTS AND DISCUSSION	62
3.2.1		Key Distribution with Simulated Parameters	62
3.2.2		Key Distribution in Laboratory	68
3.2.3		Key Distribution over Installed Optical Fibre.....	70
3.3		SUMMARY	73
CHAPTER 4		HIGH-SPEED SINGLE-PHOTON AVALANCHE DIODE WITH TUNABLE SINUSOIDAL GATE FREQUENCY.....	75
4.1		PRINCIPLE OF OPERATION	76
4.1.1		SPAD Gate and Cancellation Signals	76
4.1.2		SPAD Temperature DC Reverse-Bias	78
4.1.3		Synchronisation	78
4.1.4		Transferred Response Cancellation.....	79

4.1.5	Measurement Methods	80
4.2	EXPERIMENTAL RESULTS AND DISCUSSION	82
4.3	SUMMARY	86
CHAPTER 5	CONCLUSION AND FUTURE WORK.....	87
5.1	CONCLUSION	87
5.2	FUTURE WORK	89
REFERENCES		91

LIST OF FIGURES

Figure 2.1.1	BB84 protocol	9
Figure 2.1.2	Cryptographic key generation procedure for QKD from photon transmission to secure communication	9
Figure 2.1.3	Alice and Bob use the same basis.	10
Figure 2.1.4	Alice and Bob uses incompatible basis.	11
Figure 2.1.5	Typical receiver setup for “interruption” polarisation recovery scheme	15
Figure 2.1.6	Polarisation recovery of the horizontal SOP reference pulse	17
Figure 2.1.7	Typical receiver setup for “real-time TDM” polarisation recovery scheme	19
Figure 2.1.8	Timing diagram for the SPADs at the receiver in the “real-time TDM” scheme to extract the appropriate optical signals.....	20
Figure 2.1.9	Typical receiver setup for “real-time WDM” polarisation recovery scheme	22
Figure 2.1.10	Timing diagram for creating dark slot during photon transmission in the “real-time WDM” to minimise Raman noise (Vertical axis is the optical power).....	23

Figure 2.2.1	Typical I-V characteristic of a SPAD with rectangular-wave gating signal superimposed. V_A : DC reverse bias voltage; V_B : Reverse breakdown voltage; V_C : Peak voltage for gating signal.....	25
Figure 2.2.2	Equivalent circuit model of a SPAD. SW : Switch; R_d : Space-charge resistance; V_B : Reverse bias voltage; C_d : Junction capacitance ($\sim 1\text{pF}$).26	26
Figure 2.2.3	Schematic of a passive quenching circuit. R_L : Load resistor; R_S : Output resistor; C_B : Decoupling capacitor.	29
Figure 2.2.4	Schematic of a gated passive quenching circuit. R_m : Impedance matching resistor; C_g : Gate capacitor; R_L : Load resistor; R_S : Output resistor; C_B : Decoupling capacitor.	30
Figure 2.2.5	(a) Rectangular gate signal for the SPAD. (b) Capacitive response at SPAD anode (c) Capacitive response delayed by one clock cycle. Vertical scale in (d) is scaled up by a factor of 10 as compared to (b) and (c) for clarity. (e) Experimental setup for self-differencing scheme. (f) Output after differencer scale up by a factor of 40.....	34
Figure 2.2.6	Setup employed for sinusoidal gating scheme. R_m : Impedance matching resistor; C_b : DC block capacitor; R_L : Load resistor; R_O : Output resistor; C_n : Decoupling capacitor; BRF: Band-rejection filter (Band-stop filter).	35
Figure 2.2.7	Frequency spectrum of the output of the GPQC before the band-stop filter. Black line is when the excess bias voltage was 1.9V with	

transferred response and without avalanche. Grey line is when the excess bias voltage was 4.2V with transferred response and avalanche. 36

Figure 2.2.8 The experimental setup employed by Y. Liang. (a) The transferred response signal with avalanche superimposed after low pass filter (LPF1). (b) The avalanche signal after power combiner. 37

Figure 3.1.1 Transmitter unit for polarisation-encoded QKD system with adaptive polarisation state monitoring and recovery. FPGA: Field programmable gate array; ADC₁₋₆: Analog-to-digital converter; APC LD: Automatic power control laser driver; BS: Beam splitter; C₁₋₃: Optical couplers; DAC₁₋₄: Digital-to-analog converter; EOM_{1,2}: Electro-optic modulator; MCU: Microcontroller unit; PBS: Polarisation beam splitter; PD₁₋₆: Classical photodetector; PR: Polarisation rotator; Pulsed LD: Pulsed laser driver; QWP: Quarter-wave plate; RNG: Random number generator; VOA: Variable optical attenuator; SFP Tx: Small form-factor pluggable transmitter; WDM: Wavelength division multiplexer..... 41

Figure 3.1.2 Receiver unit for polarisation-encoded QKD system with adaptive polarisation state monitoring and recovery. FPGA: Field programmable gate array; ADC₇₋₁₀: Analog-to-digital converter; C₄: Optical coupler; DAC₅₋₈: Digital-to-analog converter; EPC_{R,D}: Electronic polarisation controller; FBG filter: Fibre Bragg grating filter; MCU: Microcontroller unit; OSW₁₋₄: Optical switch; PBS_{R,D}: Polarisation beam splitter; PD₇₋₁₀: Classical photodetector; RNG: Random number generator; SFP Rx: Small form-factor

pluggable receiver; SPAD ₁₋₄ : Single photon avalanche diode; WDM: Wavelength division de-multiplexer.....	42
Figure 3.1.3 Time-interleaved reference and quantum (before attenuation) pulses at 1 MHz observed on an oscilloscope.	44
Figure 3.1.4 Predetermined polarisation sequence for reference pulses. Random polarisation for quantum pulses depending on the RNG. t_{ref} is the temporal spacing between two sets of reference pulses; t_{ph} is the temporal spacing between two quantum pulse and Δt_r is the temporal spacing between the reference and quantum pulse to prevent afterpulsing.	45
Figure 3.1.5 Optical power across PD_2 where the intensity of the reference pulse for vertical polarisation is at its maximum hence indicating that vertical polarisation encoding is accurate.	46
Figure 3.1.6 40 MHz synchronisation clock with an embedded trigger to indicate the position of the reference signals.	48
Figure 3.1.7 Timing diagram for clock and trigger recovery.	49
Figure 3.1.8 Optical spectrum of the reference and quantum signals with anti-stokes Raman scattering induced by the 1550nm synchronisation clock..	50
Figure 3.1.9 Flowchart of the polarisation recovery algorithm for EPC_R in the rectilinear basis.	54

Figure 3.1.10	Flowchart for the APSMR algorithm for the transmitter and receiver.	56
Figure 3.1.11	Time-correlation between the quantum and reference signals as a function of transmission distance for various f_{ref}	57
Figure 3.1.12	Experimental setup to determine the required temporal (t_r) spacing between the reference and quantum signals.	58
Figure 3.1.13	Count rate observed on id201 SPAD by tuning the SPAD gate temporally for $P_{ref} = -35\text{dBm}$, -40dBm and -45dBm	59
Figure 3.2.1	Experimental setup with simulated polarisation drift (polarisation scrambler) and transmission loss (optical attenuator).	62
Figure 3.2.2	Typical randomised output SOP trace on the Poincare sphere.	63
Figure 3.2.3	QBER as a function of scrambling frequency for f_{ref} at (a) 1 kHz, (b) 5 kHz, (c) 10 kHz and (d) 20 kHz. The region boxed in green is the threshold relative intensity error (RIE) for the APSMR algorithm to increase f_{ref}	64
Figure 3.2.4	QBER and scrambling frequency as a function of the operation time with simulated transmission loss and polarisation drift.	66
Figure 3.2.5	Sifted key rate and scrambling frequency as a function of the operation time with simulated transmission loss and polarisation drift.	67

Figure 3.2.6	Experimental setup with optical fibre (laboratory or field).	68
Figure 3.2.7	QBER and sifted key rate as a function of time with key distribution performed over 10 km optical fibre spool in the laboratory. $\sigma_{\text{QBER}} = 0.367\%$ and $\sigma_{\text{sifted}} = 0.075$ k bits/s.	69
Figure 3.2.8	QBER and sifted key rate as a function of time with key distribution performed over ~ 2 km of installed fibre and APSMR enabled. $\sigma_{\text{QBER}} = 0.591\%$ and $\sigma_{\text{sifted}} = 0.112$ k bits/s.	71
Figure 3.2.9	QBER and sifted key rate as a function of time with key distribution performed over ~ 2 km of installed fibre and APSMR disabled. $\sigma_{\text{QBER}} = 2.198\%$ and $\sigma_{\text{sifted}} = 0.088$ k bits/s.	72
Figure 4.1.1	Schematic for the single-photon avalanche detector with tuneable sinusoidal gate frequency. <i>LNA</i> : Low noise amplifier; <i>C_d</i> : DC blocking capacitor; <i>R_m</i> : Impedance matching resistor; <i>R_L</i> : Load resistor; <i>R_S</i> : Output resistor; <i>C_S</i> : Decoupling capacitor; <i>LPF</i> : Low pass filter; <i>PA</i> : Power amplifier; <i>ADC</i> : Analog-to-digital converter; <i>MCU</i> : Microcontroller unit; <i>DAC</i> : Digital-to-analog converter.	77
Figure 4.1.2	Typical I-V characteristic of a SPAD with sinusoidal-wave gating signal superimposed. <i>V_A</i> : DC reverse bias voltage; <i>V_B</i> : Reverse breakdown voltage; <i>V_C</i> : Peak voltage for gating signal.	78
Figure 4.1.3	Timing diagrams for measuring the counts occurring in the illuminated gates.	81

Figure 4.2.1	Suppression ratio and the residual voltage of the cancellation circuit as a function of the SPAD gate frequency.....	83
Figure 4.2.2	Dark count probability as a function of the excess bias voltage at various SPAD gating rate.....	84
Figure 4.2.3	Quantum efficiency as a function of the excess bias voltage at various SPAD gating rate.....	84

ACRONYMS

A

ADC	Analog-to-Digital Converter
APSMR	Adaptive Polarisation State Monitoring and Recovery
APD	Avalanche Photodiode

B

BB84	QKD protocol invented by C. Bennett and G. Brassard [15]
BS	Beam Splitter
BSF	Band-stop Filter

C

CW	Continuous-Wave
COTS	Commercial-off-the-shelf

D

DAC	Digital-to-Analog Converter
-----	-----------------------------

E

EOM	Electro-optic Modulator
EPC	Electronic Polarisation Controller

F

FBG	Fibre Bragg Grating
FPGA	Field Programmable Gate Array
FWHM	Full-width at half-maximum

G

GPQC	Gated Passive Quenching Circuit
------	---------------------------------

L

LD	Laser Driver/Diode
LNA	Low Noise Amplifier
LPF	Low Pass Filter

M

MCU	Microcontroller Unit
-----	----------------------

O

OC	Optical Coupler
OSW	Optical Switch

P

PBS	Polarisation Beam Splitter
PC	Personal Computer
PD	Photodetector
PLL	Phase Lock Loop
PMD	Polarisation Mode Dispersion
PQC	Passive Quenching Circuit
PR	Polarisation Rotator

Q

QBER	Quantum Bit Error Rate
QKD	Quantum Key Distribution

R

RIE	Relative Intensity Error
RF	Radio Frequency
RNG	Random Number Generator

S

SOP	State Of Polarisation
-----	-----------------------

SPAD Single Photon Avalanche Diode

T

TDM Time-division Multiplex

U

USB Universal Serial Bus

V

VOA Variable Optical Attenuator

W

WDM Wavelength-division Multiplex

CHAPTER 1 INTRODUCTION

1.1 BACKGROUND

The aim in cryptography is to provide legitimate users, typically called Alice and Bob, a means of secure communication even in the presence of an eavesdropper, Eve. The One-Time Pad, invented in 1918 was proven to be a truly unbreakable cryptosystem by C. E. Shannon on four conditions – the key is kept secret, same length as the message, truly random and never reused [1]. However, these conditions limit the practicality of One-Time Pad. Firstly, the key will have to be physically transported from Alice to Bob or vice versa. A courier assigned to do the job could be compromised resulting in the keys being copied without leaving any trace. This is known widely as the key distribution problem. Secondly, as the amount of transmitted information grows, the required key length must also increase. Because these keys must be unique, therefore an excessive amount is required to ensure secure communication.

Fortunately, public key cryptosystem was developed to solve the key distribution problem. In such a system, two mathematically correlated keys are generated. One is known as the public key which is broadcasted while the other called the private key is kept. The transmitter uses the broadcasted public key to encrypt a message. The encrypted message can only be decrypted by the matching private key kept with the intended recipient. In doing so, secure communication is attained. Although this system exploited the present

computational limitation in factoring large prime numbers to attain security, public-key cryptography is still susceptible to technological advancement and progression in computation power.

In 1984, C. H. Bennett and G. Brassard devised the BB84 protocol which uses quantum states to distribute random cryptographic keys [15]. The security of this protocol is based on the laws of quantum mechanics [16] and hence unlike public key encryption, it is immune to technological advancement. Making use of binary bit information encoded in quantum states (qubits), Alice and Bob will be able to generate cryptographic keys remotely and estimate the amount of information the eavesdropper might have on these keys. If they are satisfied with the security, they proceed with secret communication with this set of keys. Therefore, the key distribution problem was solved. In 1989, the first experimental demonstration of quantum key distribution (QKD) using polarisations of single photons based on the BB84 protocol occurred through 32cm of air [2]. Over the years, reports on quantum key distribution over hundreds of kilometres of optical fibre and free space links have been reported [3-5]. Key generation rate of a few mega-hertz have also been demonstrated [6-8].

Implementation of fibre-based polarisation encoding QKD systems were challenging due to unpredictable fluctuations in the state of polarisation of the qubits when travelling through optical fibre. Therefore, polarisation recovery schemes based on different operating principles were introduced to counter such state of polarisation (SOP) drifts [9-14].

Qubits reaching the receiver were detected by single photon avalanche diodes (SPAD) to obtain the bit information. SPADs are well known to be plagued by noise [17]. Therefore, specially designed circuits and schemes were used to detect these qubits efficiently [18-23]. In a practical system, these schemes often rely on synchronisation clock signals to activate the SPADs for accurate photon detection.

In general, the performance of the polarisation and clock recovery schemes are amongst the most important determinant factor on the reliability and availability of a polarisation-encoded QKD system. Therefore, this thesis addresses the following two performance issues – the drift in polarisation and synchronisation clock.

1.2 MOTIVATIONS

In polarisation encoded QKD systems, Alice encodes classical binary bit information onto the polarisation of a photon before sending them through a quantum channel. At the other end, Bob directs these photons to their respective detectors based on their polarisation in order to extract the classical bit information and after several key distillation steps; both parties are able to establish a set of cryptographic keys. If they are satisfied with its integrity, they proceed onto secure communication. However, Alice and Bob are often separated by long spans of optical fibre which introduces random dynamic drift in the polarisation of the photons. Moreover, clock drift where the frequency deviates from the fundamental rate due to factors such as environmental

perturbation, power supply instability and even aging of components [24] will cause inaccuracy during the detection of photons. If these problems were not addressed, the reliability and availability of QKD systems and their cryptographic keys will be affected. Therefore, “interruption” [9, 12, 25] and “real-time” [10, 13, 14] polarisation recovery schemes were developed to counter SOP drifts introduced by these optical fibres.

The “interruption” polarisation recovery scheme disrupts the key generation process every 15 minutes to make appropriate adjustments to the polarisation controllers [25]. However, it is widely accepted that polarisation drifts can vary in the order of seconds to days [26-28]. Therefore, polarisation adjustments at 15 minutes interval in some cases may be insufficient while too frequent on other occasions. In fact, it was reported that systems using the “interruption” scheme were sometimes unable to track the SOP drift and hence required recalibration [25]. Such outages are not beneficial to the availability of a QKD system.

In contrast, the “real-time” scheme makes use of time [9, 10] or wavelength [13, 14] multiplexed periodical reference signals (not involved in key generation) containing predetermined polarisation information to recover any SOP drift. Therefore, to accommodate fast polarisation drifts, reference signals are sent frequently at the expense of the key generation rate. However, such systems are unable to adapt to slow SOP drift where reference signals could be replaced with quantum pulses to increase the cryptographic key

generation rate. Therefore, a QKD system with adaptive polarisation state monitoring and recovery scheme that automatically adapts the system to the existing polarisation drift condition in the transmission link can potentially enhance its reliability and key generation rate.

On the other hand, clock drift is a problem for ever increasing data rates in electronic communication systems. Researchers in this area have devised solutions such as timing synchronisation mechanism to mitigate its effect [24, 29-31]. In QKD systems, SPADs at the receiver are often gated by signals recovered from instable synchronisation clocks that have travelled large distances from the transmitter. These inaccuracies of the synchronisation clock are often problematic in the current technology for high-speed single-photon detection as existing schemes are often designed to work with idealised parameters such as accurate gating rate and constant ambient temperature. However, we know this is not true for practical deployment of a system. For example, the sinusoidal gating scheme which utilises band-stop filters to remove transferred response generated by the detectors requires the gating signal to fall within the narrow stop band of the filter [19, 32-34]. Moreover, the stop band of these filters tends to change with its operating conditions. Additionally, commercially available SPADs such as the id210 from idQuantique can only be gated up to 100 MHz [35]. Therefore, any deviation will make photon detection difficult. Hence, there is a need to develop a robust high-speed single-photon detection system that is able to operate even with inaccurate clock signals in practical QKD systems.

1.3 OBJECTIVES AND SCOPE

There are two main objectives in this thesis:

1) Develop an adaptive polarisation state monitoring and recovery scheme for QKD systems based on polarisation-encoding. This system will be able to automatically adapt to existing polarisation drift condition of the transmission link to optimise the cryptographic key generation rate while maintaining its reliability.

2) Develop a high-speed single-photon avalanche diode with tunable sinusoidal gate frequency. This system will be able to detect photons at high-speed and with a tunable gate frequency, it will be able to work with inaccurate clock rate.

1.4 ORGANISATION OF THESIS

The thesis began with the first chapter providing a background, motivation and objective of the topic. This will be followed by Chapters 2 and 3 which provides an in-depth review on quantum key distribution and single photon detection respectively. Next, Chapter 4 and 5 discusses the demonstration of the proposed work on adaptive polarisation state monitoring and recovery scheme for polarisation-encoded quantum key distribution systems and high-speed single-photon avalanche diode with tunable sinusoidal gate frequency. Finally, Chapter 6 concludes the thesis and ends with a summary about future work.

1.5 MAJOR CONTRIBUTIONS OF THESIS

The major contributions are discussed below.

- 1) Adaptive polarisation state monitoring and recovery scheme for polarisation-encoded quantum key distribution.

We have experimentally demonstrated for the first time a scheme that automatically adapts a polarisation-encoded QKD system to the varying polarisation drift speed of an optical fibre to maintain an acceptable QBER for continuous unconditionally secure cryptographic key generation. The experiments that we conducted on installed optical fibre link that was subjected to environmental perturbation showed that the QBER for our system was kept below the 11% threshold [36]. Therefore, our scheme was able to automatically adapt to the existing polarisation drift conditions to optimise the cryptographic key generation rate while still ensuring its security and availability.

- 2) High-speed single-photon avalanche diode with tunable sinusoidal gate frequency

We have experimentally demonstrated for the first time a sinusoidal gated high-speed single-photon detection system that utilises a feedback algorithm to cancel the transferred response. When gated at 1 GHz, our system was able to detect photons at a rate that is 330 times faster than commercially available unit [35]. Furthermore, we also showed the possibility of operating our system at a gate frequency range from 0.75 GHz to 1.25 GHz.

CHAPTER 2 REVIEW OF QUANTUM KEY DISTRIBUTION AND SINGLE PHOTON DETECTION

2.1 QUANTUM KEY DISTRIBUTION

The idea of utilising quantum states to distribute cryptographic keys first appeared in a theoretical paper published in 1984 [15]. In this paper, C. H. Bennett et al. described the distribution of cryptographic keys by encoding classical binary bit information onto the polarisation of a photon by following a given set of rules which came to be known as the BB84 protocol – the first for QKD. Subsequently, C. H. Bennett et al. successfully demonstrated experimental quantum key distribution over 32cm of air [2]. Since then, encoding binary bit information onto different properties of quantum states such as its phase and polarisation have been realised [6, 9, 10, 12-14, 25, 37, 38]. In this chapter, the basic principle and key distribution procedure will first be examined using the BB84 protocol. This will be followed by a review of the current polarisation recovery techniques.

2.1.1 BB84 Protocol

In the BB84 protocol, its inventors Bennett and Brassard described the encoding of classical binary bits onto four equally likely non-orthogonal polarisation of a photon as shown in Figure 2.1.1 [15].

Basis	Classical Bit '0'	Classical Bit '1'
Rectilinear	Horizontal Polarisation	Vertical Polarisation
Diagonal	+ 45° Polarisation	- 45° Polarisation

Figure 2.1.1 BB84 protocol

Figure 2.1.2 shows the cryptographic key generation procedure for QKD. The photon transmission is carried out through a quantum channel while key distillation and secure communication are done using a classical channel.

Figure 2.1.2 Cryptographic key generation procedure for QKD from photon transmission to secure communication

The key generation process begins with Alice creating a random bit and encoding it onto the polarisation of a photon by randomly switching between bases. Alice records in her memory, the bit information and its corresponding encoding basis. For example, Alice's random number generator creates a bit '0' and she randomly selects the rectilinear encoding basis. Therefore, a photon that is horizontal polarised will be created. The photon which is now encoded with polarisation bit information is often referred to as a qubit. This qubit is then transmitted to Bob through a quantum channel which may be an optical fibre link or even air. Since Bob has no knowledge of the basis used for encoding, he will randomly select between two equally likely bases to decode the arriving qubit. This action by Bob will lead to two equally likely outcomes:

Outcome 1: Alice and Bob use the same basis (Figure 2.1.3)

Figure 2.1.3 Alice and Bob use the same basis.

Outcome 2: Alice and Bob uses different basis (Figure 2.1.4).

Figure 2.1.4 Alice and Bob uses incompatible basis.

In the first outcome, Bob will successfully detect a horizontal polarised photon and based on the BB84 protocol; he will extract the bit information '0'. However, if an incompatible basis was used, Bob will have an equally likely probability in detecting the $+45^\circ$ or -45° polarisation and extract bit information '0' or '1' respectively. This phenomenon is known as the collapse of superposition for quantum states. Nevertheless, Bob will record the decoding basis he utilised and the corresponding bit information observed for subsequent post processes.

A quantum state can be represented as a superposition of other states. For example, a horizontal polarisation can be represented as the superposition of $+45^\circ$ and -45° polarisations. However, the act of observing the superposition states (using a diagonal basis in this example) will cause the collapse of this superposition to either -45° or $+45^\circ$ with equal probability.

The transmission sequence described above is repeated until a large number of qubits has been accumulated. Alice and Bob will now hold a string of random bits known as the “raw key”. They will then proceed to reveal publicly over a classical communication channel the encoding and decoding basis they used for each qubit respectively. Next, they will agree to discard the measurement results for the incompatible basis and those that Bob failed to detect a photon. This step is known as “basis reconciliation” which will leave Alice and Bob with a shortened string of random bits known as the “sifted key”. They will then reveal the measurement results of a number of randomly selected bits to estimate the quantum bit error rate. In a practical system, additional error correction and privacy amplification steps are usually executed to further enhance the integrity of the keys. Finally, the “secure key”, available only to Alice and Bob is used to encrypt and decrypt a message for secret communication.

However, what we have described above is in the absence of an eavesdropper, Eve. In the case where Eve is present, she is unable to duplicate the photons freely because she is bounded by the quantum no-cloning theorem that forbids her from directly duplicating an unknown quantum state. Instead, she will employ the intercept and resend attack where she samples and decodes the photons just like Bob. Eve will then create new photons based on her measurement results and transmits them to Bob. Without knowledge of the basis used for encoding, Eve will also randomly select a basis for decoding. By doing so, she will use the wrong basis for half of the time and change the

polarisation state of the photon because of the collapse of superposition. This will lead to error in Bob's measurement even when Alice and Bob uses identical basis (Figure 2.1.3). Therefore, by checking the quantum bit error rate (QBER), Alice and Bob can reveal the presence of an eavesdropper and decide if the key is suitable to be used for secret communication. P. W. Shor et al. showed that in order for unconditional security, the QBER must be less than or equal to 11% [36].

2.1.2 Polarisation Recovery In Quantum Key Distribution Systems

Light travelling in optical fibres suffer from random polarisation fluctuations due to varying birefringence attributed to various reasons such as mechanical and environmental effects [39, 40]. Generally, a polarisation state at an optical fibre's input differs from that at its output and this changes over time due to varying birefringence [41]. S. C. Rashleigh attributed the birefringence to imperfections introduced during the manufacturing process and from external perturbations to the fibre [39]. Noncircular core and asymmetrical lateral stress resulted from the fabrication process introduces linear birefringence [39]. External perturbations such as bending and twisting will also introduce birefringence [39]. Moreover, an electric field will lead to an increase of linear birefringence via the electro-optic Kerr effect [39]. Large changes in the state of polarisation were also observed during sunrise and sunset for terrestrial links with fibre connectors placed above ground due to the considerable ambient temperature fluctuation [40].

In conventional optical systems, polarisation division multiplexing is typically used in conjunction with modulation schemes to allow transmission speeds of 100 Gb/s or higher. Therefore, robust and efficient control on the polarisation is often required to counter random polarisation fluctuations in optical fibres so that the data signals can be mapped efficiently to their respective detectors. Researchers in this area have managed to track polarisation drift of 0.1 rad/s in 1988 [28] to 50 Grad/s in 2010 [42]. In such conventional systems, researchers such as B. Koch et al. simply split part of the incoming data signal for polarisation recovery.

However, in optical fibre based polarisation encoded QKD systems, the need to track polarisation drift results from the requirement that the polarisation state at the receiver must be the same as that at transmitter for successfully key generation. Due to the quantum nature and unknown polarisation state of the photons, polarisation recovery techniques utilising these quantum signals are impossible. Therefore, researchers in this area have developed schemes that employs reference signals to provide polarisation drift information to recover the polarisation state of the quantum signals. The two main approaches that will be discussed subsequently in this section are the “interruption” and “real-time” method.

2.1.3 “Interruption” Polarisation Recovery Scheme

As its name implies, the “interruption” polarisation recovery schemes implemented for polarisation encoded QKD systems will suspend the key generation process at fixed periodic intervals to recover the polarisation of the quantum signals [9, 12, 25]. For such schemes, the polarisation recovery and key distribution processes can be viewed as two separate procedures. A typical receiver setup for such a scheme is shown in Figure 2.1.5.

Figure 2.1.5 Typical receiver setup for “interruption” polarisation recovery scheme

During normal key distribution process, the transmitter will encode binary bit information onto the polarisation a photon as described in Section 2.1.1. To reach the receiver, this photon travels through a long span of optical fibre which introduces unpredictable polarisation changes that varies over time. The resulting SOP of this arriving photon will be different from that prepared by the transmitter. Basis selection will randomly direct the photon into either

the rectilinear or diagonal path where polarisation controllers, EPC_R or EPC_D will cancel the polarisation drift induced by the optical fibre and recover the initial transmitted polarisation. Subsequently, the polarisation beam splitter (PBS) will route the quantum signal to its respective SPAD and the classical bit information is extracted. For effective cancellation of the polarisation drift induced by the optical fibre, the “interruption” polarisation recovery scheme is utilised to determine a suitable driving voltages (V_R and V_D) for the polarisation controllers.

Before commencing the key generation process, reference signals with predetermined polarisation sequence will be transmitted to calibrate the initial driving voltages (V_R and V_D) for the polarisation controllers. These reference signals travel through the same optical fibre that serves as a quantum channel for the photons during key generation. Therefore, polarisation drift information for the quantum channel can be extracted from these reference signals to determine the appropriate driving voltages, V_R and V_D .

For example, to calibrate V_R , the transmitter prepares horizontally polarised reference signals and sends them through the optical fibre which will introduce polarisation drift. At the receiver, these reference signals are divided equally between the rectilinear and diagonal paths. Since the aim is to calibrate V_R , the reference signals in the diagonal path are ignored. Depending on the state of polarisation of these reference signals, counts will be registered on detectors $SPAD_1$ or $SPAD_2$ and relayed to an algorithm implemented in the

controller. The objective of the algorithm is to adjust V_R such that the count visibility between the detectors is maximised. The situation where the polarisation has been successfully recovered is depicted in Figure 2.1.6. V_R drives the electro-optic modulator (EPC) based on the electro-optic effect such that the incoming reference signals which suffered from polarisation drift are successfully recovered as horizontally polarised and reflected into $SPAD_I$ by the PBS . This will maximise the count visibility between the two detectors and inform the algorithm that the appropriate V_R has been obtained. A similar procedure as the abovementioned is executed on the diagonal path to calibrate V_D before key generation commences. Subsequently, the key generation process is interrupted periodically the above described calibration procedure for V_R and V_D .

Figure 2.1.6 Polarisation recovery of the horizontal SOP reference pulse

In such a scheme, each reference pulse usually contains a few photons to prevent saturating the extremely sensitivity SPADs. Furthermore, due to low quantum efficiency and dark count effects inherent in SPADs, large amounts of counts are accumulated to enhance the polarisation recovery accuracy. L. Ma et

al. reported that each calibration procedure takes approximately 3 minutes during which key generation is not possible [25]. Moreover, this scheme relies on the assumption that the polarisation variations remains slow to allow key distribution without polarisation recovery between the periodic suspensions. However, this may not be true as reported by L. Ma et al. where they report that their 15 minutes interruption interval is at times too long which results in unusable keys due to high QBER [25]. Therefore, such scheme is not beneficial for the reliability and availability of the QKD system.

2.1.4 “Real-time” Polarisation Recovery Scheme

In the “real-time” polarisation recovery scheme, two different approaches to deliver the reference signals were presented. In these demonstrations, the reference signals were either time division multiplexed or wavelength division multiplexed with the quantum signals [10, 13, 14]. In both cases, these quantum and reference signals experience polarisation changes induced by the optical fibre during propagation. By analysing the polarisation changes encountered by the reference signals, appropriate compensation can be applied to recover the initial state of polarisation for the quantum signals. In the remainder of this chapter, we shall first review the time division multiplexed approach followed by the wavelength division multiplexed approach.

Figure 2.1.7 Typical receiver setup for “real-time TDM” polarisation recovery scheme

The time division multiplexed (TDM) approach was demonstrated by J. Chen et al. in 2008 [10]. They utilised a Mach-Zehnder interferometer to induce a temporal delay between the quantum and reference signals as shown in Figure 2.1.8. The reference signals for the rectilinear and diagonal bases were delayed by 50 ns and 90 ns from the quantum signal respectively. To vary the power of the quantum and reference signal, optical attenuators were placed in each arm of the Mach-Zehnder interferometer. By adjusting the attenuation level, 0.2 photons per pulse and 4 photons per pulse were obtained for the quantum and reference signals respectively. Six SPAD shown in Figure 2.1.7 were utilised – four to detect the quantum signals for QKD and two to detect reference signals. The detectors were gated appropriately as shown in Figure 2.1.8 to accept only the desired signals. This is important to ensure that afterpulses that increase the QBER are not created.

Figure 2.1.8 Timing diagram for the SPADs at the receiver in the “real-time TDM” scheme to extract the appropriate optical signals.

In this scheme, because of the low power for the reference pulses and limited efficiency of the SPAD, large amount of counts is necessary to make correct adjustments. Therefore, if such systems were exposed to fast depolarisation, reference pulses will need to be sent more frequently for polarisation recovery. However, there is a temporal limit on the separation between the quantum and reference signals where the crosstalk will eventually lead to an increase in the QBER due to afterpulsing. N. J. Muga et al. showed that this limit is 3.5 ns for a detector gate width of 6 ns [43].

M. Karlsson et al. [26] showed that the correlation between two absolute SOP vectors measured at two distinct time, t_1 and t_2 can be represented by the following autocorrelation function:

$$\langle \hat{s}(t_1) \cdot \hat{s}(t_2) \rangle = \exp\left(-\frac{|\delta t|}{t_d}\right) \quad (1)$$

where, $t_d = \frac{2t_0}{(3\omega^2 D_p^2 z)}$, δt , is the time separation between the reference signal of the same polarisation. t_d , is the typical drift time for the SOP vector. t_0 , is a measure of the drift time of the index difference in the birefringence element used to model the fibre. ω , is the optical frequency. D_p , is the polarisation mode dispersion (PMD) coefficient and z , is the transmission distance.

N. J. Muga reported that for a fixed δt , the correlation between the reference and quantum signals drops at longer transmission distances. Therefore, to achieve higher correlation at longer distance, the temporal separation needs to be decreased. Eventually, the temporal limit on the separation between the reference and quantum signal will be reached. This minimum temporal separation was reported to be dependent on several factors – the SPAD's shape and gate width, power of the reference pulses and its isolation from the SPAD [43].

The wavelength division multiplexed approach for counter-propagating and co-propagating quantum and reference signals were demonstrated by G. B. Xavier et.al [13, 14]. A typical receiver in the co-propagating scheme is illustrated in Figure 2.1.9. Since the reference and quantum signals are at different wavelengths, a wavelength division de-multiplexed can be used to separate them. The separated quantum signals can then be used for cryptographic key generation.

Figure 2.1.9 Typical receiver setup for “real-time WDM” polarisation recovery scheme

On the other hand, the reference pulses were sent through polarisers Pol_R and Pol_D before being detected by classical photodetectors, PD_R and PD_D respectively. For successful polarisation recovery, an algorithm keeps the power across PD_R and PD_D at maximum by applying appropriate adjustments to the driving voltage for the EPC, V_E . In this scheme, G. B. Xavier et.al showed that in order to remove Raman noise produced by the reference signals, they created a dark slot when quantum signals were being sent (Figure 2.1.10).

Figure 2.1.10 Timing diagram for creating dark slot during photon transmission in the “real-time WDM” to minimise Raman noise (Vertical axis is the optical power).

The correlation between two SOP vectors at two optical frequency, ω_1 and ω_2 can be represented by the following autocorrelation function [26]:

$$\langle \hat{s}(\omega_1) \cdot \hat{s}(\omega_2) \rangle = \hat{s}(\omega_1) \cdot \hat{s}(\omega_2) \exp\left(-\frac{D_p^2 z (\omega_1 - \omega_2)^2}{3}\right) \quad (2)$$

where $\hat{s}(\omega_1)$ and $\hat{s}(\omega_2)$ are the input SOP vector of optical frequency of ω_1 and ω_3 respectively. D_p , is the PMD coefficient and z , is the transmission distance. For a fixed PMD coefficient, the correlation degrades as the transmission distance increases. Therefore, to achieve higher correlation at longer distance, the difference in optical frequency between the reference and quantum signal needs to be reduced. However, N. J. Muga et al. showed that for transmission distances beyond 20 km, a wavelength separation smaller than 0.8 nm is required for successful polarisation control [43]. With the current wavelength-division multiplex (WDM) technology, polarisation recovery beyond 20 km may not be possible.

2.2 SINGLE PHOTON DETECTION

Single-photon detection is the ability to detect extremely low light level down to a single photon. However, dark counts, afterpulsing and low gating speed have long been obstacles towards the effective detection of photons. Over the years, detection of single-photon has evolved from the use of photomultiplier tubes to SPAD due to its low power consumption, compactness and cryogen-free operation. SPADs have been employed in applications such as quantum key distribution [33, 44, 45], laser ranging [46] and fibre optic sensing [47, 48]. They are essentially specially designed avalanche photodiodes designed for Geiger mode operation. Si SPADs are usually used to detect photons of 600nm to 900nm wavelength while InGaAs/InP SPADs are used to sense photons of 1300nm to 1650nm wavelength.

In Geiger mode operation, the SPAD is reversed biased above its breakdown voltage. In this region of operation, a single charged carrier (thermally or photon induced) in the depletion region is able to create a self-sustaining avalanche through the effect of impact ionisation. The flow of these charged carriers give rise to a macroscopic current. Specially designed passive quenching circuits are used to stop the continuous flow of this current [17]. However, detectors operating in Geiger mode are plagued by thermally generated dark count problem and afterpulsing effect (Section 2.2.2). Therefore, SPADs operating in gated-mode were devised (Section 2.2.3.2) to mitigate the afterpulsing effect by applying a long dead-time (micro-second range) in the

expense of detection rate. However, recent emphasis has been placed on sinusoidal gated single-photon detector that is able to detect photons at high speed because of its low afterpulsing probability.

2.2.1 Equivalent Circuit Model

Figure 2.2.1 Typical I-V characteristic of a SPAD with rectangular-wave gating signal superimposed. V_A : DC reverse bias voltage; V_B : Reverse breakdown voltage; V_C : Peak voltage for gating signal.

Figure 2.2.1 shows a typical I-V characteristic of a SPAD. In the linear mode, the SPAD does not possess single-photon sensitivity because carrier created by an absorbed photon does not trigger impact ionisation. However, SPADs operating above the breakdown voltage, V_B , in the Geiger mode is able to induce a large current flow through impact ionisation and therefore it is used for single-photon detection.

Figure 2.2.2 Equivalent circuit model of a SPAD. SW : Switch; R_d : Space-charge resistance; V_B : Reverse bias voltage; C_d : Junction capacitance ($\sim 1\text{pF}$).

A SPAD can be represented by common electrical components as shown in Figure 2.2.2. The SPAD's junction capacitor (C_d) is in parallel with a switch (SW), the SPAD's breakdown voltage (V_B) and space-charge resistance (R_d). An open and closed switch is used to represent the quenching and photon detection processes respectively. These processes will be discussed in Section 2.2.3.

2.2.2 Measures of Performance

There are three important parameters to measure a SPAD's performance. These are the dark count probability, afterpulsing probability and quantum efficiency. They are essential during characterisation and also used as a tool for comparison among related works.

2.2.2.1 Detection Efficiency

The detection efficiency, η is defined as the total probability of detecting a photon, P against the number of incident photons, n . As discussed in [49], the probability of detecting a photon can be represented by equation 3 where P_{dc} is the probability of detecting a dark count. Equation 3 can then be manipulated to obtain the detection efficiency, η (equation 4).

$$P = 1 - (1 - P_{dc})e^{-n\eta} \quad (3)$$

$$\eta = \frac{1}{n} \ln \left(\frac{1-P_{dc}}{1-P} \right) \quad (4)$$

2.2.2.2 Afterpulsing

The afterpulsing phenomenon occurs when carriers trapped in the deep levels of the depletion region during a previous avalanche are subsequently released and retrigger another avalanche. The delayed release of these carriers fluctuates statistically. A higher and wider avalanche pulse will ensure a larger number of trapped carriers which consequently increase the afterpulsing probability. Hence, the afterpulsing probability is proportional to the applied excess bias voltage, V_{excess} and the delay to the onset of avalanche quenching. To counter such problems, long dead-time where detections are ignored ensures that high-speed photon detection is not possible.

2.2.2.3 Dark Counts

Dark counts in SPAD can be classified into two categories – primary and secondary [50]. Primary dark counts are contributed by thermally generated carriers in the depletion region. On the other hand, secondary dark counts are caused by the afterpulsing effect. When a thermally induced avalanche occurs, large amount of charged carriers will flow in the SPAD. These charged carriers can be trapped in the defects present in the depletion region. After some time, if the trapped carriers are released while the SPAD is operating above the breakdown voltage, secondary avalanches due to the afterpulsing effect occur. These thermally-induced avalanches and afterpulses are indistinguishable from their photon-induced counterparts. Therefore, to reduce their undesirable effects, SPADs are often cooled to a temperature of -30°C to -50°C . At such low temperature, the occurrence of these thermally generated carriers will be greatly reduced.

2.2.3 Geiger Mode Operation

In Geiger mode operation, the voltage applied to the SPAD exceeds its breakdown voltage. The SPAD remains in a quiescent state until a primary carrier is generated in the depletion region. Because of the high reverse bias voltage, this primary carrier triggers the process of impact ionisation involving thousands of carriers leading to a flow of macroscopic avalanche current. The generation of the primary carrier is indicated by the leading edge the avalanche current. External circuitry is required to quench the self-sustaining avalanche

current by lowering the applied voltage below its breakdown voltage to halt the impact ionisation process. There are three main quenching modes – (a) passive quenching, (b) active quenching and (c) gated-mode operation. In this chapter, only quenching modes (a) and (c) will be discussed.

2.2.3.1 Passive Quenching

Figure 2.2.3 Schematic of a passive quenching circuit. R_L : Load resistor; R_S : Output resistor; C_B : Decoupling capacitor.

Passive quenching is the easiest and straight-forward method to stop the flow of the avalanche current. Figure 2.2.3 shows a typical passive quenching circuit (PQC) where the SPAD is reversed biased through a large value load resistor, R_L . In the SPAD's equivalent circuit model, the SPAD is in the quiescent state with switch, SW in the open position. At this time, the junction capacitor, C_d is charged by the applied bias voltage, V_A . The SPAD remains in this quiescent state until the creation of a primary carrier through photon absorption. This process is denoted by the closing of the switch and C_d is

discharged as the avalanche current flows through the circuit. The avalanche current develops a large voltage drop across R_L and the voltage across the SPAD returns to V_A after a quenching time constant T_q . The SPAD is now ready for detection. T_q can be calculated using equation 5. R_S is placed in series with the SPAD to convert the avalanche current into voltage for further processing. It is typically impedance matched with subsequent circuits.

$$T_q = (C_d + C_s) \frac{R_d R_L}{R_d + R_L} \approx (C_d + C_s) R_d \quad (5)$$

2.2.3.2 Gated-mode Operation

Figure 2.2.4 Schematic of a gated passive quenching circuit. R_m : Impedance matching resistor; C_g : Gate capacitor; R_L : Load resistor; R_S : Output resistor; C_B : Decoupling capacitor.

In the gated-mode operation, the SPAD is placed in the gated passive quenching circuit (GPQC) shown in Figure 2.2.4. A gate signal is added through the cathode pin to pulse-bias the SPAD above the breakdown voltage

for a short period of time (typically nanoseconds) when a photon is expected to arrive. It can be observed that C_g , C_d and C_B form a capacitive voltage divider. Therefore, the attenuated amplitude of the gate signal, V'_g applied to the SPAD can be calculated from equation 6 [17]. Hence, to minimise the attenuation of the gate voltage, $C_g \leq 100(C_d + C_s)$ [17].

$$V'_g = V_g \frac{C_g}{(C_g + C_d + C_s)} \quad (6)$$

where, V_g is the original amplitude of the gate signal

Moreover, R_L , C_d and C_s forms a low pass filter with cut-off frequency, f_L while R_L , C_g , C_d and C_s forms a differentiator with cut-off frequency, f_H . It is evident that the frequency of the gate signal, f_{gate} must be kept between f_L and f_H . This analysis allows the formation equation 7 and 8. Since $C_g \leq 100(C_d + C_s)^{-1}$, the approximation in equation 10 is valid.

$$f_L = \frac{1}{2\pi R_L(C_d + C_s)} \gg f_g \quad (7)$$

$$f_H = \frac{1}{2\pi R_L(C_g + C_d + C_s)} \cong \frac{1}{2\pi R_L C_g} \ll f_g \quad (8)$$

With the bias voltage at V_C (Figure 2.2.1), the SPAD is for a ready to detect a photon. This interval is known as the “gate on” period and is adjusted to coincide with a photon arrival. With the SPAD in the “gate on” period, a primary carrier created through the absorption of a photon will trigger the impact ionisation process that leads to a self-sustained avalanche current flow

which is simply quenched when the gate signal falls below the breakdown voltage to V_B (Figure 2.2.1), The SPAD biased at V_A (Figure 2.2.1), operates in the “gate off” period where a charged carrier in the depletion region is unable to create an avalanche. Due to the finite capacitance of the SPAD, a rectangular gate through the SPAD will produce a positive peak, followed by a negative peak. This is known as the capacitive response.

In the presence of the capacitive response, a large excess bias (hence a large avalanche) is required to distinguish between the avalanche and capacitive response. This will in turn create more charged carrier which may be trapped within the defects in the material. Therefore, a long dead-time (usually in the microsecond range) is required to permit the release of these trapped carriers without allowing it to trigger an avalanche (dark count). However, this lengthy dead-time limits the SPAD’s detection rate to the range of mega-hertz. The detection efficiency is reduced by a dead-time factor shown in equation 9 where, n is the number of photons, η is the detection efficiency without dead-time and N_B is the number of light pulse block by the dead-time [18].

$$(1 + n\eta N_B)^{-1} \tag{9}$$

To attain a higher detection rate, it is evident that the afterpulsing effect which dictates the length of the dead-time needs to be reduced. Therefore, the main approach is to reduce the amplitude of the avalanche which consequentially limits the amount of trapped carriers. Different circuits and

techniques have since been developed [18, 20, 22]. A new gating scheme using sinusoidal signal has been shown to increase the detection rate while keeping the afterpulsing probability low [19]. These will be discussed subsequently in this chapter.

2.2.4 Single Photon Detection Schemes

This section will analyse the various techniques developed to eliminate the SPAD response resulting from gated-mode operation of an SPAD.

2.2.4.1 Self-Differencing

The self-differencing scheme depicted in Figure 2.2.5 was demonstrated by Z. L. Yuan [51]. The SPAD was gated using a rectangular wave as illustrated in Figure 2.2.5a. Hence, a capacitive response as shown in Figure 3.5b is produced at the SPAD anode. As the name of the scheme implies, the capacitive response was split into two parts. One portion passes directly, while the other (Figure 2.2.5c) was delayed by a clock cycle before entering a differencer. In the event of an avalanche, a positive and negative peak (Figure 2.2.5d) separated by one clock cycle can be observed at the output of the differencer. However, when an avalanche is absent, no significant peak is produced. Since these peaks are produced only when an avalanche occurs, either one of them can be used for discrimination.

The dark count probability was reported to be 2.3×10^{-6} per gate and an afterpulsing probability was 6.16% at a quantum detection efficiency and gate frequency of 10.8% and 1.25GHz respectively.

Figure 2.2.5 (a) Rectangular gate signal for the SPAD. (b) Capacitive response at SPAD anode (c) Capacitive response delayed by one clock cycle. Vertical scale in (d) is scaled up by a factor of 10 as compared to (b) and (c) for clarity. (e) Experimental setup for self-differencing scheme. (f) Output after differencer scale up by a factor of 40.

Figure reproduced from: Z. L. Yuan, A. W. Sharpe, J. F. Dynes, A. R. Dixon, and A. J. Shields, "Multi-gigahertz operation of photon counting InGaAs avalanche photodiodes," *Applied Physics Letters*, vol. 96, pp. 071101-3, 2010.

2.2.4.2 Sinusoidal Gating With Band-Stop Filter

The first sinusoidal gated SPAD was first demonstrated by N. Namekata et al. using the setup shown in Figure 2.2.6 [19]. The transferred response generated by the SPAD was removed using band-stop filters. A transferred response in sinusoidal gating is analogous to the capacitive response in rectangular wave gating. Their difference will be highlighted subsequently in this section.

Figure 2.2.6 Setup employed for sinusoidal gating scheme. R_m : Impedance matching resistor; C_b : DC block capacitor; R_L : Load resistor; R_O : Output resistor; C_n : Decoupling capacitor; BRF: Band-rejection filter (Band-stop filter).

Figure reproduced from: N. Namekata, S. Sasamori, and S. Inoue, "800 MHz single-photon detection at 1550-nm using an InGaAs/InP avalanche photodiode operated with a sine wave gating," *Opt. Express*, vol. 14, pp. 10043-10049, 2006.

The SPAD is reverse biased through a load resistor R_L . Sinusoidal gate signal with frequency, ω_g is supplied through a DC block capacitor C_b . In the absence of an avalanche, only the transferred response is observed across R_O . When viewed in the frequency spectrum, this transferred response consists of the transferred gate signal at ω_g and subsequent higher order harmonics ($2\omega_g$, $3\omega_g$, $4\omega_g$...). The transferred response above $3\omega_g$ can be ignored because they are extremely weak. Band-stop filters centred at ω_g , $2\omega_g$ and $3\omega_g$ can be utilised to eliminate these transferred response. In the event of an avalanche, because of its impulse-like nature (grey region in Figure 2.2.7), most of its energy is retained at the output of the band-stop filter. Hence, the avalanche can be discriminate easily. This is unlike rectangular wave gating where the action of filtering the capacitive response will simultaneously eliminate the avalanche signal.

Figure 2.2.7 Frequency spectrum of the output of the GPQC before the band-stop filter. Black line is when the excess bias voltage was 1.9V with transferred response and without avalanche. Grey line is when the excess bias voltage was 4.2V with transferred response and avalanche.

Figure reproduced from: N. Namekata, S. Sasamori, and S. Inoue, "800 MHz single-photon detection at 1550-nm using an InGaAs/InP avalanche photodiode operated with a sine wave gating," *Opt. Express*, vol. 14, pp. 10043-10049, 2006.

The sinusoidal gating scheme provides a technique to reduce the noise level to an extremely low level of 0.1mV in which the discrimination level can be set at 0.5mV. Therefore, only avalanches with small amplitude are required. This can be associated with the discussion in Section 2.2.2.2, where small avalanches reduce the amount of trapped carriers which in turns lower the afterpulsing probability.

The group obtained a dark count probability of 9.2×10^{-6} per gate and an afterpulsing probability of 6% at a quantum efficiency and gate frequency of 8.5% and 800MHz respectively. It must also be noted that the dead-time following each detection was 50ns to suppress afterpulsing.

Subsequently in 2009, N. Namekata et al. reported a dark count probability of 6.3×10^{-7} per gate and an afterpulsing probability of 2.8% at a quantum efficiency and gate frequency of 10.8% and 1.5GHz respectively [32].

This was followed by a report by J. Zhang et al. who showed a dark count probability of 4.8×10^{-7} per gate and an afterpulsing probability of 8.3% at a quantum efficiency and gate frequency of 10% and 2.23GHz respectively [33].

2.2.4.3 Sinusoidal Gating with Phase-shifter

In 2011, Y. Liang et al. demonstrated a sinusoidal gated SPAD using a phase-shifter to eliminate the transferred response [21]. The setup employed by Y. Liang et al. is depicted in Figure 2.2.8.

Figure 2.2.8 The experimental setup employed by Y. Liang. (a) The transferred response signal with avalanche superimposed after LPF1. (b) The avalanche signal after power combiner.

Figure reproduced from: L. Yan, E. Wu, C. Xiuliang, M. Ren, Y. Jian, W. Guang, *et al.*, "Low-Timing-Jitter Single-Photon Detection Using 1-GHz Sinusoidally Gated InGaAs/InP Avalanche Photodiode," *Photonics Technology Letters, IEEE*, vol. 23, pp. 887-889, 2011.

A power divider split the sinusoidal with frequency ω_g , into two equal parts. One part was amplified and filtered to remove the amplified sideband noise before being used to gate the SPAD. The other portion travelled through an attenuator and phase-shifter to serve as the cancellation signal. The transferred response signal (ω_g , $2\omega_g$ and $3\omega_g$), sometimes with the avalanche superimposed is passed through a low pass filter (LPF_1). This step will remove the higher order harmonics and suppress the transferred gate signal by 40dB as depicted in Figure 2.2.8a. Next, the phase shift between the cancellation signal and transferred gate signal was adjusted to 180° . These two signals were then combined using a power combiner such that the transferred gate signal was suppressed, hence, leaving only the avalanche (Figure 2.2.8b). The avalanche signal was amplified and discriminated.

The group obtained a dark count probability of 6.1×10^{-6} per gate and an afterpulsing probability of 3% at a quantum efficiency and gate frequency of 10.4% and 1GHz respectively [21].

CHAPTER 3 ADAPTIVE POLARISATION STATE MONITORING AND RECOVERY SCHEME FOR POLARISATION-ENCODED QUANTUM KEY DISTRIBUTION SYSTEMS

As discussed in Chapter 2, current polarisation recovery schemes either limit the transmission distance of polarisation-encoded QKD systems due to requirements for narrow wavelength separation or disrupt the availability of the key generation process for polarisation recovery. It was also discussed that reference pulses sent periodically at a high repetition rate to counter fast depolarisation for the “real-time” polarisation recovery schemes are unable to adapt to slow polarisation changes where reference pulses can be substituted by photon signals to increase the key generation rate.

This chapter describes the proposed experimental demonstration of an adaptive polarisation state monitoring and recovery scheme for QKD systems based on polarisation-encoding. Such a system is able to adapt to the rate of polarisation drift to optimise the sifted key rate (hence secure key rate) while maintaining the QBER below the required threshold for generating unconditionally secure keys [36]. In the remaining of this chapter, the principle of operation for the proposed scheme will be described first, followed by a discussion on the experimental demonstration carried out in the laboratory and field trials.

3.1 PRINCIPLE OF OPERATION

The setup of our proposed adaptive polarisation state monitoring and recovery scheme for QKD systems based on polarisation-encoding is illustrated in Figure 3.1.1 and Figure 3.1.2. The system consists of a transmitter and receiver unit linked by a span of optical fibre which serves as the quantum channel. A separate Ethernet connection to two personal computers (PCs) at both ends serve as the classical channel for post processing. Quantum pulses were delivered through the optical fibre for cryptographic key generation with reference signals time-interleaved to enable polarisation state monitoring and recovery. An algorithm designed to adaptively alter the frequency of these reference pulses based on the rate of polarisation drift in the optical fibre ensures that optimum key generation rate can be achieved while maintaining the QBER below 11% to generate unconditionally secure keys. Files containing the basis and bit information (for encoding and decoding) were generated at both the transmitter and receiver ends. They were transferred through a universal serial bus (USB) connection and stored in the memory of the PCs. After completing the transmission of quantum pulses, these files containing the basis and bit information will be used for key distillation through the classical communication channel. Based on the estimated QBER, the transmitter and receiver will decide to discard or utilise the cryptographic keys for secure communication.

Figure 3.1.1 Transmitter unit for polarisation-encoded QKD system with adaptive polarisation state monitoring and recovery. FPGA: Field programmable gate array; ADC_{1,6}: Analog-to-digital converter; APC LD: Automatic power control laser driver; BS: Beam splitter; C_{1,3}: Optical couplers; DAC_{1,4}: Digital-to-analog converter; EOM_{1,2}: Electro-optic modulator; MCU: Microcontroller unit; PBS: Polarisation beam splitter; PD_{1,6}: Classical photodetector; PR: Polarisation rotator; Pulsed LD: Pulsed laser driver; QWP: Quarter-wave plate; RNG: Random number generator; VOA: Variable optical attenuator; SFP Tx: Small form-factor pluggable transmitter; WDM: Wavelength division multiplexer.

Figure 3.1.2 Receiver unit for polarisation-encoded QKD system with adaptive polarisation state monitoring and recovery. FPGA: Field programmable gate array; ADC₇₋₁₀: Analog-to-digital converter; C₄: Optical coupler; DAC₅₋₈: Digital-to-analog converter; EPC_{R,D}: Electronic polarisation controller; FBG filter: Fibre Bragg grating filter; MCU: Microcontroller unit; OSW₁₋₄: Optical switch; PBS_{R,D}: Polarisation beam splitter; PD₇₋₁₀: Classical photodetector; RNG: Random number generator; SFP Rx: Small form-factor pluggable receiver; SPAD₁₋₄: Single photon avalanche diode; WDM: Wavelength division de-multiplexer.

3.1.1 Generation of Quantum and Reference Signals

Firstly, a train of quantum pulses $1\mu\text{s}$ apart with full-width at half-maximum (FWHM) of 1 ns were created by modulating the 1310 nm continuous wave (CW) laser output with two electro-optic modulators (EOM_1 and EOM_2) followed by attenuation (VOA) with Poisson photon number statistics. To guarantee an accurate photon number for the quantum pulses, the output of the CW laser was stabilised to an accuracy of approximately $\pm 0.05\text{ mW}$ by using an automatic optical power control algorithm. A field programmable gate array (FPGA) generates 1 ns electrical pulses, RF_1 and RF_2 , to modulate EOM_1 and EOM_2 respectively to create an equivalent optical output based on the electro-optic effect. Quantum pulses with FWHM of 1 ns allows the use of the finest gate width in the commercial-off-the-shelf (COTS) id201 quantum detectors ($SPAD_{1-4}$) to reduce trapped carriers hence the afterpulsing effect which degrades the QBER. A portion of the modulated optical output at each EOM was extracted via optical couplers (OC_1 and OC_2) and converted into its electrical equivalent by photodetectors (PD_5 and PD_6) for a feedback algorithm that ensure maximum signal-to-noise ratio by adjusting DC_1 and DC_2 . The microcontroller unit (MCU) regulates the amount of optical attenuation provided by the variable optical attenuator (VOA) via the digital-to-analog converter, $DAC3$ to attenuate the optical pulses. The amount of required attenuation, A , to achieve the desired mean photon number can be calculated from the following equation

$$A\text{ (dB)} = 10 \log \left[\left(\frac{hc}{\lambda} \times f_{ph} \times \mu \right) - E_{op} \right] \quad (10)$$

where, h is the Planck's constant, c is the speed of light, λ is the optical wavelength, f_{ph} is the frequency of the quantum pulses, μ is the desired number of photons per quantum pulse and E_{op} is the optical energy before attenuation.

Next, a sequence of four reference pulses $1\mu\text{s}$ apart with FWHM of 400 ns each were produced by directly modulating a 1310 nm pulsed laser driver. This pulsed laser driver was specially designed to induce a reverse bias to the laser diode such that no light was emitted during the transmission of quantum pulses. This is again to prevent afterpulsing due to trapped carriers in the quantum detectors which will degrade the QBER. The relatively large pulse-width was selected for easy timing alignment in the classical photodetectors. Finally, the quantum and reference pulses were fed into OC_3 to produce the time-interleaved signals at a frequency of 1 MHz shown in Figure 3.1.3 which was observed on an oscilloscope with an avalanche photodiode (APD).

Figure 3.1.3 Time-interleaved reference and quantum (before attenuation) pulses at 1 MHz observed on an oscilloscope.

The time-interleaved signals were then sent through a polarisation controller (PR) where the random number generator (RNG) determines the polarisation to be encoded onto each quantum pulse based on the BB84 protocol. On the other hand, a predetermined sequence of horizontal, vertical, -45° and $+45^\circ$ polarisations was applied onto each of the reference pulse as shown in Figure 3.1.4. The encoding basis for the quantum pulses and its corresponding bit information generated by the RNG was transferred through a USB connection and stored as a file in the computer's memory.

Figure 3.1.4 Predetermined polarisation sequence for reference pulses. Random polarisation for quantum pulses depending on the RNG. t_{ref} is the temporal spacing between two sets of reference pulses; t_{ph} is the temporal spacing between two quantum pulse and Δt_r is the temporal spacing between the reference and quantum pulse to prevent afterpulsing.

Encoding was achieved by applying an appropriate voltage to the polarisation rotator (PR) through DAC_4 . To ensure the accuracy of the encoding scheme, the free-space module was constructed to extract polarisation information to adjust DAC_4 . A beam splitter divides the pulses into two equal parts. Signals exiting the transmitted port were used for key generation while the reflected signals were further divided into two parts. Subsequently, two PBS

were used to extract the polarisation information from the reference pulses in the rectilinear and diagonal basis. A polarisation encoding algorithm then samples the optical intensities across the corresponding photodetectors (PD_{1-4}) to determine an appropriate change for DAC_4 to achieve accurate polarisation encoding. For example, to ensure the accuracy of the vertical polarisation, the PE algorithm samples the optical intensity from PD_2 . Since the polarisation sequence of the reference pulses were predetermined, the polarisation encoding algorithm will alter DAC_4 such that the vertical reference pulse intensity is at its maximum as shown in Figure 3.1.5. Reference signals for other polarisations are ignored as they provide no useful information.

Figure 3.1.5 Optical power across PD_2 where the intensity of the reference pulse for vertical polarisation is at its maximum hence indicating that vertical polarisation encoding is accurate.

Back at the transmitted output of the first beam splitter in the free-space module, the quantum and reference pulses will be wavelength division multiplexed with a synchronisation clock signal before being transmitted through the optical fibre to the receiver unit. Before discussing the procedures performed at the receiver, synchronisation between the transmitter and receiver will be evaluated first in the next section.

3.1.2 Synchronisation

Synchronisation between the transmitter and receiver is vital so that the basis and bit information can be evaluated sequentially and correctly during key distillation to successfully generate secure cryptographic keys. To synchronise the transmitter and receiver units, a typical transceiver often used in conventional optical communication was employed to generate a 40 MHz synchronisation clock. The optical wavelength was chosen to be at 1550 nm so that it can be easily separated from the 1310 nm quantum and reference pulses using a wavelength division de-multiplexer. Moreover, to allow the adaptive polarisation state monitoring and recovery (APSMR) scheme to alter the frequency of the reference pulses, a trigger was embedded in the synchronisation clock as shown in Figure 3.1.6. The receiver will recover this trigger to switch the optical switch (OSW) in order to route the respective signals to their corresponding detectors so as to prevent afterpulsing due to the leakage of reference signals into the quantum detectors ($SPAD_{1-4}$).

Figure 3.1.6 40 MHz synchronisation clock with an embedded trigger to indicate the position of the reference signals.

The clock recovery procedure at the receiver will be explained with the aid of the timing diagram in Figure 3.1.7. After the reference, quantum and synchronisation clock signals were separated according to their wavelength, the transceiver converts the 1550nm clock signal into its electrical equivalent. This was fed into the FPGA, where a phase lock loop (PLL) was used to produce a stable 40 MHz periodic clock signal to drive the receiver unit. To recover the embedded trigger, the PLL output was delayed and used to sample the transceiver's output. During normal operating circumstances where a trigger is not present, the sampled signal will always remain at logic high. However, when a reference signal is being transmitted, the embedded trigger will ensure that the sampled signal falls to logic low for two clock cycles. Therefore, a '1001' sequence in the sampled signal indicates the arrival of the reference

signals and a recovered trigger was generated to switch the optical pulses into their respective paths (*OSW output 1* and *OSW output 2*). This is the key technique the APSMR employed to synchronise the transmitter and receiver unit when adjusting the frequency of the reference pulses according to the rate of polarisation drift in the transmission fibre.

Figure 3.1.7 Timing diagram for clock and trigger recovery.

3.1.3 Detecting the Quantum and Reference Signals

As mentioned in Section 3.1.2, the 1310nm and 1550nm signals arriving at the receiver were wavelength separated. However, observations in Figure 3.1.8 shows that the 1550 nm signal creates undesirable anti-stokes Raman

scattering in the 1310 nm region where the quantum and reference signals were located. Therefore, an optical fibre Bragg grating (FBG) filter was used to reject these unwanted noises by approximately 25 dB to a negligible level.

Figure 3.1.8 Optical spectrum of the reference and quantum signals with anti-stokes Raman scattering induced by the 1550nm synchronisation clock.

Next, C_4 performs passive basis selection for the quantum signals and divides the reference signal into the rectilinear and diagonal paths. EPCs were placed in these paths to cancel the polarisation drift introduced by the optical fibre and recover the original transmitted polarisation. The EPCs were driven by appropriate voltages V_{R1} , V_{R2} , V_{D1} and V_{D2} which were determined by the APSMR algorithm. Polarisation recovery will be discussed subsequently in Sections 3.1.4 and 3.1.5. With the recovered trigger discussed in Section 3.1.2, OSW_{1-4} routes the quantum and reference signals into $SPAD_{1-4}$ and PD_{1-4} respectively. The reference signals were used by the APSMR algorithm for polarisation state monitoring and recovery while the quantum signals were

detected by the SPADs. The detection results of the SPADs were recorded along with the decoding basis in a file stored in the computer's memory. After completing the transmission cycle of the quantum signals, the files containing the basis and bit information at the transmitter and receiver were used to perform basis reconciliation to obtain the sifted key. Finally, the QBER was analysed to detect the presence of an eavesdropper and verify the integrity of the sifted key. Since, our aim is to show that the proposed APSMR scheme is able to adapt to the rate of polarisation drift to maintain a reasonably well QBER with an optimal sifted key rate, we did not perform the subsequent steps of error correction and privacy amplification.

3.1.4 Polarisation Control Theory

The relationship between the SOP of the quantum pulses arriving at the receiver and sent from the transmitter can be written as:

$$|\Psi\rangle_R = T_F |\Psi\rangle_T \quad (11)$$

where T_F is the unitary rotation transformation caused by random birefringence changes in the fibre. To recover the transmitted polarisation, our receiver performs T_R , where $T_R = T_F^{-1}$, such that the SOP of the quantum pulses at the output of the EPC can be written as:

$$|\Psi\rangle_R = T_R T_F |\Psi\rangle_T = |\Psi\rangle_T \quad (12)$$

$$|R_H\rangle = C_R |R_H\rangle \quad (13)$$

$$|R_{+45}\rangle = C_D |R_{+45}\rangle \quad (14)$$

At the receiver, two EPCs were used to perform compensation rotations, C_R and C_D , around the Poincare sphere for the rectilinear and diagonal basis respectively to recover the polarisation of the reference signals. Therefore, it can be seen that $C_R = C_D = T_R$. Since, the EPCs are driven by V_{R1} , V_{R2} , V_{D1} and V_{D2} , by applying these voltages to the quantum signals, T_F will be removed and hence $|\Psi\rangle_R = |\Psi\rangle_T$ where the transmitted SOP is recovered at the receiver. To obtain the appropriate driving voltage for the EPCs, a polarisation recovery algorithm was developed. For simplicity in the discussion, only the flowchart of the polarisation recovery algorithm for EPC_R in the rectilinear basis is shown in Figure 3.1.9. The polarisation recovery procedure for EPC_D is similar as described subsequently in this section.

Since EPC_R is driven by two voltages V_{R1} and V_{R2} , they were altered in four different combinations ($+V_{R1}$, $+V_{R2}$; $+V_{R1}$, $-V_{R2}$; $-V_{R1}$, $-V_{R2}$; $-V_{R1}$, $+V_{R2}$) during the polarisation recovery attempt. The optical power of the reference signal sampled by ADC_I was then recorded correspondingly ($P_{ref(0)}$, $P_{ref(1)}$, $P_{ref(2)}$, $P_{ref(3)}$). An EPC cycle counter keeps track of the recovery sequence. After examining all four combinations (i.e. *EPC cycle counter* = 4), the recorded power of the reference signal were compared. Finally, only the voltage

combination that produces the highest reference power will be applied to the quantum pulses. However, if the new reference power is not higher than that obtained from the previous recovery cycle, V_{R1} and V_{R2} from the previous cycle will be applied to the quantum pulses. In this way, the horizontal SOP of the reference pulse was recovered and the driving voltage for the EPC, V_{R1} and V_{R2} , dither about the ideal point. The key method of the polarisation recovery algorithm is to alter the driving voltage for the EPC such that the power of the reference pulse for that particular decoding basis (i.e. horizontal SOP for rectilinear basis) is at maximum. The rest of the reference pulses (vertical, $+45^\circ$, -45° SOP in rectilinear path) were disregarded as they produce no useful information. By applying this driving voltage when the quantum pulses passes through the EPC, the transmitted polarisation were recovered.

Figure 3.1.9 Flowchart of the polarisation recovery algorithm for EPC_R in the rectilinear basis.

3.1.5 Adaptive polarisation state monitoring and recovery

The flowchart for the APSMR algorithm for the transmitter and receiver are depicted in Figure 3.1.10. An initialisation step was carried out to reset the $P_{ref(max)}$ and P_{th} to its default values and set f_{ref} to 20 kHz. Next, the algorithm sampled the power of horizontal SOP reference signal from ADC_I and stored the value in $P_{ref(C)}$. A comparison was carried out to determine if the current detected power was higher than a predetermined threshold which corresponds to a relative intensity error (RIE). This provides the APSMR algorithm with information on the efficiency of the compensation algorithm. A higher $P_{ref(C)}$ denotes efficient polarisation recovery while a lower $P_{ref(C)}$ indicates the vice-versa. Depending on the comparison results, counters A and B will be adjusted accordingly. These counters were used to minimise the momentary power fluctuation due to the dithering effect in our polarisation recovery procedure as described in Section 3.1.4. Whenever a counter reaches the maximum, f_{ref} will be modified accordingly and an indication is delivered to Alice. If Alice detects a change in the indicator, the position of the embedded trigger in the synchronisation clock will be altered together with the frequency of the reference signals. Quantum or reference pulses will be inserted or remove accordingly to keep the QBER below 11% for optimal key generation rate. In this way, the QKD system was able to automatically adapt to existing polarisation drift conditions of the transmission link to optimise the cryptographic key generation rate while maintaining its reliability.

Figure 3.1.10 Flowchart for the APSMR algorithm for the transmitter and receiver.

For accurate polarisation recovery, the reference and quantum pulses must be highly correlated. However, this degrades with the increase of distance and the temporal spacing between these pulses. This will result in an increase of the QBER. Therefore, equation 1 was utilised to analyse the f_{ref} for the APSMR scheme. The PMD coefficient was set to $0.05 \text{ ps/km}^{1/2}$. Since the simulated transmission distance was short, t_d was set to 120 s. The time autocorrelation

was calculated and plotted as a function of transmission distance in Figure 3.1.11.

Figure 3.1.11 Time-correlation between the quantum and reference signals as a function of transmission distance for various f_{ref} .

From the results above, the maximum transmission distance such that the correlation is high (i.e. $\leq 90\%$) between the quantum and reference signals for various f_{ref} were tabulated in Table 4.1.

Table 4.1 Maximum transmission distance for $ACF \leq 90\%$ at various f_{ref} based on the results in Figure 3.1.11.

f_{ref} (kHz)	Maximum transmission distance for $ACF \leq 90\%$ (km)
1	1.630
5	8.150
10	16.300
20	32.590
40	65.180

3.1.6 Leakage of Reference Signals into SPAD

Another important effect that will be analysed for the APSMR scheme is the leakage of reference signals into the SPAD. From the discussion in Chapter 2, it was noted that an incident photon on the SPAD operating in the linear mode will also create a carrier that may be trapped and released subsequently. When multiple photons like those leaked from the strong reference signals are incident on the SPAD, numerous trapped carriers could be created. If the SPAD is subsequently gated, these trapped carriers may be released and cause an avalanche. Hence, the SPAD may register a count even in the absence of a photon. This undesirable effect will degrade the QBER and reduce the reliability of the QKD system. Therefore, such unwanted leakage should be prevented by introducing a temporal spacing, Δt_r (Figure 3.1.4), between the reference and quantum pulses during which, the SPAD is to be disabled. The experiment shown in Figure 3.1.12 was performed to find the minimum required temporal spacing Δt_r .

Figure 3.1.12 Experimental setup to determine the required temporal (t_r) spacing between the reference and quantum signals.

In this experiment, a digital delay generator created a 20 kHz reference signal and gated the SPAD 20,000 times per second. The OSW was always switched to lead the reference signal into the PD such that any counts detected on the SPAD is a result of either the inherent dark count or the leakage of the reference signal. By tuning the SPAD gate temporally away from the reference pulse, the count rate on the SPAD was recorded. The experiment was performed for P_{ref} at -35 dBm, -40 dBm and -45 dBm with the result plotted in Figure 3.1.13.

Figure 3.1.13 Count rate observed on id201 SPAD by tuning the SPAD gate temporally for $P_{ref} = -35$ dBm, -40 dBm and -45 dBm.

It was observed that for Δt_r between 0 ns to ~ 200 ns, the SPAD saturates at 20,000 counts per second. This implies that the influence of the leaked reference pulse is so strong that it triggers an afterpulse in every SPAD gate. This situation is evident for all P_{ref} values mentioned above. However, when the detector's gate was shifted (i.e. increase Δt_r), the count rate began to drop

exponentially and finally to the SPAD's inherent dark count level as depicted in Figure 3.1.13. As discussed earlier, these counts were attributed to the afterpulsing effect found in SPADs. Therefore, Table 4.2 shows the minimum required Δt_r in order to avoid such undesirable effects.

Table 4.2 Minimum temporal spacing (Δt_r) for different reference power

Average reference power (dBm)	Minimum temporal spacing, Δt_r (μ s)
-35	31.950
-40	26.950
-45	16.950

P_{ref} for our QKD system was measured to be approximately -42 dBm to -46 dBm depending on the transmission fibre utilised. Therefore, based on the results of the experiment described above, Δt_r was set to be 25μ s. We verified that there was no influence by the reference pulse on the SPAD by disconnecting the 1310 nm pulsed laser driver with no observable changes to the SPAD's count rate. This implies that all counts observed on the SPAD were due to its inherent dark counts.

3.1.7 Sifted Key Rate

$$R_{sift} = \frac{1}{2}R_{raw} = \frac{1}{2} \times f_{ph} \times \mu \times \eta \times 10^{-\frac{L}{10}} \quad (15)$$

After basis reconciliation, the length of the sifted key will be half that of the raw key due to the 50% probability that the transmitter and receiver utilised

incompatible basis. The sifted key rate, R_{sift} , can be estimated from equation 15, where R_{raw} is the raw key rate, f_{ph} is the frequency of the transmitted photons, μ is the mean photon number, η is the SPAD's detection efficiency and L is the loss of the system. Table 4.3 shows the calculated expected sifted key rate based on the measured loss of our system for various f_{ref} in the APSMR scheme.

Table 4.3 Expected sifted key rate for various experimental setup

Setup	L (dB)	f_{ref} (kHz)	f_{ph} (kHz)	Photon to reference ratio (f_{ph}/f_{ref})	R_{sift} (kHz)
~2km installed fibre	11.97	1	975	975	6.201
		5	875	175	5.566
		10	75	75	4.770
		20	50	25	3.180
10km fibre in lab	12.69	1	975	975	5.254
		5	875	175	4.715
		10	75	75	4.042
		20	50	25	2.694
Simulated loss	13.22	1	975	975	4.651
		5	875	175	4.174
		10	75	75	3.577
		20	50	25	2.385

3.2 EXPERIMENTAL RESULTS AND DISCUSSION

3.2.1 Key Distribution with Simulated Parameters

Firstly, key distribution was performed by simulating the transmission loss and polarisation drift of an optical fibre with a 4.22 dB optical attenuator and polarisation scrambler as illustrated in Figure 3.2.1. The encoding basis and its corresponding bit information was transferred to *PC1* through a USB connection and stored as a file in the computer's memory. Similarly, the decoding basis and the decoded bit information was transferred and stored as a file in the memory of *PC2*. After completing the transmission of quantum pulses, these files containing the basis and bit information were used to analyse the QBER through an Ethernet channel.

Figure 3.2.1 Experimental setup with simulated polarisation drift (polarisation scrambler) and transmission loss (optical attenuator).

In this experiment, APSMR was first disabled and the QKD system was operated at fixed reference frequencies of 1 kHz, 5 kHz, 10 kHz and 20 kHz independently. To simulate polarisation drift, the polarisation scrambler was

operated to change the input SOP around the Poincare sphere (Figure 3.2.2) in a random but continuous manner before entering the receiver. Polarisation recovery relied on fixed reference rate to remove the simulated polarisation drift. The QBER was recorded as a function of the scrambling frequency and the results were plotted in Figure 3.2.3 where each QBER point represents the analysis results of 100 million transmitted quantum pulses. Moreover, the relative intensity error of the reference signal was obtained using equation 16 and plotted against the scrambling frequency in Figure 3.2.3.

$$RIE_{f_{scr}}^{f_{ref}} = \left(1 - \frac{I_{f_{scr}}^{f_{ref}}}{I_{0(max)}} \right) \times 100 \quad (16)$$

where f_{ref} is the reference frequency and f_{scr} is the scrambling frequency. Therefore, the relative intensity error defined at a particular reference and scrambling frequency is the ratio between the intensity of the reference signal with scrambling ($I_{f_{scr}}^{f_{ref}}$) and maximum intensity without scrambling ($I_{0(max)}^{f_{ref}}$).

Figure 3.2.2 Typical randomised output SOP trace on the Poincare sphere.

Figure reproduced from: G. Photonis. *MCP201 datasheet*. Available: www.generalphotonics.com/pdf/MPC-201.pdf

Figure 3.2.3 QBER as a function of scrambling frequency for f_{ref} at (a) 1 kHz, (b) 5 kHz, (c) 10 kHz and (d) 20 kHz. The region boxed in green is the threshold relative intensity error (RIE) for the APSMR algorithm to increase f_{ref} .

The maximum scrambling frequency where each reference rate is capable of effectively recovering the input SOP before exceeding the QBER threshold limit of 11% such that unconditionally secure key generation is no longer possible was tabulated in Table 4.4. Therefore, from the results in the above experiment, the QKD system with the APSMR scheme can accommodate polarisation drift up to $\sim 0.3 \pi$ rad/s with a QBER and sifted key rate of $\sim 10.39\%$ and 2.33 k bits/s. For polarisation drifts lower than $\sim 0.04 \pi$ rad/s the f_{ref} can be decreased to 1 kHz for high sifted key rate of 4.54 k bits/s with a QBER of 7.38%.

Table 4.4 Maximum scrambling frequency for f_{ref} with QBER below 11%

f_{ref} (kHz)	Scrambling frequency (π rad/s)	QBER (%)	Sifted key rate (k bits/s)
1	0.04	7.377	4.543
5	0.12	7.994	4.072
10	0.20	9.556	3.475
20	0.30	10.388	2.327

From the results in Figure 3.2.3, the APSMR algorithm was set to increase f_{ref} at a predetermined threshold RIE of $\sim 2.8\%$, $\sim 7.4\%$ and $\sim 8.9\%$ for f_{ref} at 1 kHz, 5 kHz and 10 kHz respectively to maintain the QBER below 6%. For example, if the QKD system is currently operating at f_{ref} of 1 kHz and the threshold RIE of 2.8% was detected by the APSMR algorithm, the system will automatically increase f_{ref} to 5 kHz so as to maintain a relatively constant QBER as shown in the following experiment.

The APSMR was enabled and the key generation process was started. The scrambling frequency was adjusted from 0 π rad/s to 0.2 π rad/s in steps of 0.02 π rad/s every fifteen minutes and subsequently reduced to 0.12 π rad/s, 0.04 π rad/s and finally 0 π rad/s. The QBER was analysed and plotted against the operation time in Figure 3.2.4 for every 10 million transmitted quantum pulses. In addition, the f_{ref} was recorded throughout the entire key generation process and represented by the coloured regions in Figure 3.2.4. It was observed that the APSMR algorithm automatically adjusts f_{ref} in response to an increasing scrambling frequency that results in the rise of the RIE. The average QBER obtained during this key generation process was 5.01% with a minimum

and maximum of 2.95% and 6.85%. It is clear that the APSMR scheme maintains the QBER below the 11% threshold for unconditionally secure key generation. It must be noted that the high QBER of 6.85% occurring at ~175 minutes was a result of wavelength mismatch between the laser diodes generating the reference and quantum signals. This effect was caused by temperature change in the pulsed laser driver when f_{ref} changed from 20 kHz to 10 kHz. Once we altered the tempeture to match the lasers' wavelength, the QBER reduces to 5.12%. In fact, we had to alter the pulsed laser's temperature in order to match their wavelegths when f_{ref} changes from 5 kHz to 10 kHz and 10 kHz to 20 kHz. This was not observed in Figure 3.2.4 because the changes occurred during basis reconciliation where no quantum pulses were sent. Hence, the QBER was not affected.

Figure 3.2.4 QBER and scrambling frequency as a function of the operation time with simulated transmission loss and polarisation drift.

The results of this experiment demonstrates the main purpose of our APSMR scheme in adapting to the rate of polarisation drift (scrambling frequency) while maintaining an optimal sifted key rate as shown in Figure 3.2.5.

Figure 3.2.5 Sifted key rate and scrambling frequency as a function of the operation time with simulated transmission loss and polarisation drift.

At f_{ref} of 20 kHz, the sifted key rate can be observed to be approximately half that when f_{ref} is 1 kHz. However, rate of polarisation drift up to 0.3π rad/s can be accommodate when f_{ref} is 20 kHz. Minimum f_{ref} limit at 1kHz was chosen based on autocorrelation analysis in Section 3.1.5 where the maximum transmission distance was estimated to be ~ 1.6 km to maintain high correlation between the quantum and reference singals. Moreover, a futher reduction of f_{ref} to 500 Hz will yield an insignificant $\sim 1\%$ increase in the sifted key rate. From the analysis on the leakage of reference signal into SPAD in Section 3.1.6, the

minimum temporal spacing between the reference and quantum signals, Δt_r was $\sim 25\mu\text{s}$ which results in a photon to reference ratio of 1:25 when f_{ref} is 20 kHz. By increasing f_{ref} to 40 kHz, no photon can be transmitted due to the strong influence of the reference signal on the SPAD. Therefore, the upper f_{ref} limit for the APSMR scheme was chosen to be 20 kHz.

3.2.2 Key Distribution in Laboratory

Figure 3.2.6 Experimental setup with optical fibre (laboratory or field).

The experimental setup was modified as depicted in Figure 3.2.6 to perform key distribution through physical optical fibres. A typical 10 km fibre spool placed in the laboratory with an end to end loss of 3.69 dB was used for key distribution. This particular fibre spool was enclosed in a box and therefore relatively well shielded from environmental perturbations. Moreover, the laboratory's ambient temperature was kept constant at $\sim 20^\circ\text{C}$. The system was operated for ~ 5.6 hours and yielded an average QBER of 3.24% with an average sifted key rate of 5.25 k bits/s. The standard deviation of the QBER and sifted key rate were 0.37% and 0.08 k bits/s. The results were plotted as a

function of time in Figure 3.2.7 where each point was the analysis results of 10 million transmitted quantum pulses. Table 4.5 shows the time and duration of three isolated occurrence where the APSMR algorithm altered f_{ref} to 5 kHz in response to an increase in the RIE (hence, rate of polarisation drift). The operation of f_{ref} at 5 kHz lasted only 44 seconds before the algorithm returns f_{ref} to 1 kHz suggested that the increase in the rate of polarisation drift occurred only momentarily which P. M. Krummrich et al. observed as a fast polarisation change with considerable amplitude change in the Stokes parameters [52]. Therefore, it can be concluded that the rate of polarisation drift for the 10 km optical fibre spool in the laboratory was relatively stable over time.

Table 4.5 Instances during key distribution over ~10 km fibre in lab where APSMR altered f_{ref} to counter fast polarisation drift

Start (HH:MM:SS)	Stop (HH:MM:SS)	Duration (s)	QBER (%)
12:16:07	12:16:51	44	3.748
12:57:32	12:58:16	44	4.172
13:31:17	13:32:01	44	3.764

Figure 3.2.7 QBER and sifted key rate as a function of time with key distribution performed over 10 km optical fibre spool in the laboratory. $\sigma_{QBER} = 0.367\%$ and $\sigma_{sifted} = 0.075$ k bits/s.

3.2.3 Key Distribution over Installed Optical Fibre

Finally, we performed key distribution over approximately 2 km of installed optical fibre between two buildings in DSO national laboratories. The optical fibre originated from our laboratory and travelled through open areas which subjected the optical fibre to environmental perturbations before reaching the other building. It was then looped back to terminate in our laboratory. This experiment allowed us to perform key distribution in an environment where the optical fibre is subjected to both intrinsic and extrinsic perturbations to observe the performance of the APSMR scheme when deployed in practical experiments.

We performed key distribution for ~ 5.9 hours and yielded an average QBER of 3.25% with an average sifted key rate of 5.96 k bits/s. The standard deviation of the QBER and sifted key rate were 0.59% and 0.11 k bits/s. The results were plotted in Figure 3.2.8 and the eight instances where the APSMR algorithm alters f_{ref} to 5 kHz in response to an increase in the RIE were recorded in Table 4.6. In most cases, the algorithm returns f_{ref} to 1 kHz within 33 seconds to 55 seconds which suggests the increase in the rate of polarisation drift occurred only momentarily which was observed by P. M. Krummrich et al. [52]. However, there was an instance from 11:27:11 to 11:32:41 where the QKD system operated at f_{ref} of 5 kHz for 5.5 minutes. This implies that there was a sustained increase in the rate of polarisation drifts to between $\sim 0.02 \pi$ rad/s and $\sim 0.1 \pi$ rad/s. According to our results in Section 3.2.1, with APSMR

disabled, the QBER could possibly rise to $\sim 24.95\%$ where secure key generation is not possible. It was also noted that among the eight instances, five of them occurred between 11:00:00 to 13:00:00 where the ambient temperature and human activities should be at its peak. As a comparison, key distribution was performed with APSMR disabled and f_{ref} fixed at 1 kHz.

Figure 3.2.8 QBER and sifted key rate as a function of time with key distribution performed over ~ 2 km of installed fibre and APSMR enabled. $\sigma_{\text{QBER}} = 0.591\%$ and $\sigma_{\text{sifted}} = 0.112$ k bits/s.

Table 4.6 Instances during key distribution over ~ 2 km installed fibre where APSMR altered f_{ref} to counter fast polarisation drift

Start (HH:MM:SS)	Stop (HH:MM:SS)	Duration (s)	QBER (%)
10:32:07	10:32:40	33	5.351
11:27:11	11:32:41	330	3.738
11:40:22	11:40:55	33	4.538
11:52:16	11:52:49	33	3.631
12:29:00	12:29:44	44	4.849
12:55:55	12:56:39	44	4.709
13:36:20	13:37:04	44	5.038
15:42:35	15:43:30	55	4.035

Key distribution without APSMR was performed for ~ 5.22 hours and the QBER and sifted key rate were plotted as a function of time in Figure 3.2.9. The standard deviation of the QBER and sifted key rate were 2.20% and 0.09 k bits/s. It can be observed that without APSMR, the QBER fluctuates and at times exceeded the 11% threshold where no secure keys can be generated. In order to keep the QBER below the limit for secure key generation, an alternative is to operate the QKD system at fixed f_{ref} of 5 kHz to cater for these rare occurrences of fast polarisation drift. Clearly, this is at the expense of the sifted key rate. Therefore, these experiments showed that with the APSMR scheme, the QBER of the polarisation encoded QKD system can be maintained below the threshold for secure key generation with an optimal sifted key rate based on the existing condition of the transmission link.

Figure 3.2.9 QBER and sifted key rate as a function of time with key distribution performed over ~ 2 km of installed fibre and APSMR disabled. $\sigma_{\text{QBER}} = 2.198\%$ and $\sigma_{\text{sifted}} = 0.088$ k bits/s.

3.3 SUMMARY

In this chapter, we had proposed and demonstrated key distribution in laboratory and field experiments for a QKD system based on polarisation-encoding with adaptive polarisation state monitoring and recovery. We had described the operating principle of our scheme and showed that it was able to accommodate polarisation drift rates up to 0.30π rad/s with a QBER and sifted key rate of 10.39% and 2.33 k bits/s respectively where unconditionally secure keys can be generated.

In the laboratory experiment, we have demonstrated that the APSMR scheme was able to perform successful key distribution over 10 km of optical fibre with an average QBER of 3.235% for ~ 5.6 hours. The maximum recorded QBER of 4.64% ensured that unconditionally secure key generation was always possible from an optimal sifted key rate of 5.245 k bits/s based on the polarisation drift condition of the optical fibre.

In the field experiment, we had successfully performed key distribution over ~ 2 km of installed fibre. The results showed that the APSMR scheme was able to maintain an average QBER of 3.25% for ~ 5.9 hours with a maximum of 5.59% where unconditionally secure key were generated. The APSMR was able to maintain an optimal sifted key rate of 5.956 k bits/s. In contrast, when APSMR was disabled and f_{ref} was fixed at 1 kHz, the QBER may at times exceed the threshold, reaching a maximum of 16.58% where unconditionally

secure key generation was not possible. In order to keep the QBER below 11%, we have discussed the possibility of employing a higher f_{ref} to cater for fast polarisation drift. However, this is at the expense of the key generation rate. Therefore, we have showed that the APSMR scheme optimises the reliability and key generation rate of the polarisation encoded QKD system based on the existing polarisation drift condition of the transmission link.

CHAPTER 4 HIGH-SPEED SINGLE-PHOTON AVALANCHE DIODE WITH TUNABLE SINUSOIDAL GATE FREQUENCY

From the review in Chapter 2, it is clear that current high-speed single-photon detection schemes rely on idealised parameters to detect single photons. For example, the sinusoidal gating scheme requires the SPAD gate signal to fall within the narrow stop band of the band-stop filters so as to remove the transferred response for effective avalanche discrimination [19, 32-34]. However, this may not be possible in the presence of inaccurate gating signals. Moreover, the stop band of these band-stop filter may change based on the operating environment. In the self-differencing and sinusoidal gating with phase-shifter schemes, the path delays between the SPAD's output and differencing signals are assumed to be the same [21, 51]. This may not be true if the system was put to work in a practical environment where ambient temperature may alter the electrical and optical path delays. Therefore, for a robust system, we proposed high-speed single-photon avalanche diode with tunable sinusoidal gate frequency.

In this chapter, the experimental demonstration of the proposed high-speed single-photon avalanche diode with tunable sinusoidal gate frequency will be discussed. The operating principle of the proposed scheme and the measurement methods to obtain characterisation parameters will be evaluated. Finally, the experimental results will be discussed.

4.1 PRINCIPLE OF OPERATION

Figure 4.1.1 depicts the setup for the proposed high-speed single-photon avalanche diode with tuneable sinusoidal gate frequency. We utilised a COTS PGA400 SPAD from Princeton Lightwave and designed a gated passive quenching circuit. To reduce dark counts, a temperature control circuit was designed to cool the SPAD down to approximately -31.85°C . For avalanche discrimination, we also fabricated a transferred response cancellation circuit where the avalanche signal can be extracted. We made use of a COTS SMA100A radio frequency generator from Rohde & Schwarz to produce sinusoidal signal for the experiment.

4.1.1 SPAD Gate and Cancellation Signals

In the experimental setup, the sinusoidal wave with centre frequency, f_{gate} , was produced by a signal generator and divided into two parts. One part was sent through a phase-shifter then attenuator to generate an appropriate 180° out-of-phase cancellation signal to remove the transferred gate response. The other part was amplified by a low noise amplifier and used to gate the SPAD reverse-biased in the GPQC. The output of the GPQC consists of the avalanche signal (broadband) superimposed onto the SPAD's transferred response. The transferred response includes the transferred gate response (f_{gate}) and its higher order harmonics resulting from the SPAD's nonlinear response ($2f_{gate}$, $3f_{gate}$, $4f_{gate}$ and etc).

Figure 4.1.1 Schematic for the single-photon avalanche detector with tuneable sinusoidal gate frequency. LNA : Low noise amplifier; C_d : DC blocking capacitor; R_L : Impedance matching resistor; R_m : Load resistor; R_S : Output resistor; C_S : Decoupling capacitor; LPF : Low pass filter; PA : Power amplifier; ADC : Analog-to-digital converter; MCU : Microcontroller unit; DAC : Digital-to-analog converter.

4.1.2 SPAD Temperature DC Reverse-Bias

In the setup, the SPAD was cooled to approximately -31.85°C by applying an appropriate driving current to its internal thermoelectric cooler and providing suitable heat dissipation. The corresponding reverse breakdown voltage, V_B , at this temperature was -74.4V . The applied DC reverse-bias voltage, V_A , was -73.1V . Figure 4.1.2 shows the IV characteristics representation of the SPAD with the applied DC reverse bias and sinusoidal gate signal superimposed.

Figure 4.1.2 Typical I-V characteristic of a SPAD with sinusoidal-wave gating signal superimposed. V_A : DC reverse bias voltage; V_B : Reverse breakdown voltage; V_C : Peak voltage for gating signal.

4.1.3 Synchronisation

To synchronise the experimental setup, the signal generator produced an additional signal (*Trigger IN*) with frequency $f_{\text{laser}} = f_{\text{gate}}/10000$. This was sent into a digital delay generator which produced two trigger signals (*Trigger OUT*

I and *Trigger OUT 2*) with frequency f_{laser} to drive the COTS id300 laser and SR400 photon counter. Temporal delays for each trigger signal were tuned independently to compensate for electrical and optical path lengths mismatch. The triggered laser produced light pulses at a repetition rate of f_{laser} . These optical pulses were attenuated to a mean photon number of 0.1 by a calibrated optical attenuator. The attenuated optical pulses were tuned temporally to coincide with the SPAD “gate on” period (t_{on}) for maximum detection efficiency. The trigger for the photon counter used during measurements will be discussed in Section 4.1.5.

4.1.4 Transferred Response Cancellation

The GPQC’s output was added to the 180° out-of-phase cancellation signal at the power combiner to remove the transferred gate response. Subsequently, a low pass filter was used to suppress the higher order harmonics – leaving only the avalanche signal which was subsequently amplified and low pass filtered to increase the signal-to-noise ratio before splitting into two parts. One part was sent into a power detector to measure the residual power in order to verify the effectiveness of the cancellation procedure. An algorithm in the MCU tracks this residual power through an analog-to-digital converter. To maintain effective suppression, appropriate changes to the phase and amplitude of the cancellation signal was applied through the DACs. The other part of the divided signal was further filtered and amplified. To remove any DC offset introduced during amplification, a DC block was inserted. A COTS SR400

photon counter from Stanford Research was used to record the number of avalanches.

4.1.5 Measurement Methods

As discussed in Chapter 2, the dark count probability, quantum efficiency and afterpulsing probability are typical parameters used to quantify the performance of the SPAD. As mentioned above, we made use of the commercially available photon counter to record the number of avalanches in order to calculate these characterisation parameters.

Firstly, to obtain the dark count, the laser was turned off hence the SPAD was not illuminated. Any avalanche that creates a rising edge at the photon counter was registered as a dark count. The dark count rate, C_D is the accumulation of the number of dark counts per second and equation 17 was used to obtain the dark count probability per SPAD gate, P_{dc} .

$$P_{dc} = \frac{C_D}{f_{gate}} \quad (17)$$

Next, the SPAD was illuminated and any avalanche that created a rising edge at the photon counter was recorded. The recorded counts over one second is the total count rate, C_{total} , which included the photon-induced avalanche, dark counts and afterpulses.

Figure 4.1.3 Timing diagrams for measuring the counts occurring in the illuminated gates.

With the SPAD still illuminated, the photon counter was set to register a count only when an avalanche falls within the trigger produced by the digital delay generator as shown in Figure 4.1.3. The counts were accumulated for one second and known as the count rate in the illuminated gates (f_{laser}), C_I . Therefore, the count rate in the non-illuminated gate ($f_{gate} - f_{laser}$), C_{NI} , can be calculated from equation 18.

$$C_{NI} = C_{total} - C_I \quad (18)$$

With the count rates obtained above, the quantum efficiency, η , and afterpulsing probability, P_A , can be calculated from equation 19 and 20 respectively.

$$\eta = \frac{1}{\mu} \left[\frac{1 - \frac{C_D}{f_{SPAD}}}{1 - \frac{C_{total}}{f_{laser}}} \right] \quad (19)$$

$$P_A = \frac{C_{NI} - C_D}{C_I - C_{NI}} \times \frac{f_{laser}}{f_{SPAD}} \quad (20)$$

where, μ is the mean photon number and f_{SPAD} and f_{laser} are the SPAD's and laser's gate frequency respectively.

4.2 EXPERIMENTAL RESULTS AND DISCUSSION

Firstly, the suppression efficiency of the transferred gate response and corresponding residual power for our circuit were measured for f_{gate} from 700 MHz to 1300 MHz. The results illustrated in Figure 4.2.1 shows that the residual power begins to increase for f_{gate} below and above 750 MHz and 1250 MHz respectively. The efficiency of the suppression circuit degrades beyond the abovementioned frequencies. This can be attributed to the limited operating bandwidth of the phase-shifter and attenuator that were utilised. The unwanted increase in residual power will make it harder for the discrimination of weak avalanche signals. Therefore, this shows that the proposed system can be operated between f_{gate} of 750 MHz and 1250 MHz.

Figure 4.2.1 Suppression ratio and the residual voltage of the cancellation circuit as a function of the SPAD gate frequency.

In the next set of experiments, the SPAD was operated at three different gating frequencies – 0.9 GHz, 1.0 GHz and 1.1 GHz independently. It was cooled to a temperature of -31.85°C with a corresponding reverse breakdown voltage, V_B , at -74.4V . A DC reverse bias voltage, V_A , of -73.1V was applied to the SPAD. In order to detect a photon, the SPAD relied on the gate signal to bring it over V_B into the Geiger region as illustrated in Figure 4.1.2. The amount of excess bias voltage, V_{excess} , is one determinant factor for the quantum efficiency, dark count and afterpulsing probability. By varying f_{gate} and V_{excess} , the dark count probability and quantum efficiency as a function of the V_{excess} were obtained using the measurement methods described in Section 4.1.5. The results are plotted in Figure 4.2.2 and Figure 4.2.3.

Figure 4.2.2 Dark count probability as a function of the excess bias voltage at various SPAD gating rate.

Figure 4.2.3 Quantum efficiency as a function of the excess bias voltage at various SPAD gating rate.

From the results above, it was observed that a quantum efficiency of $\sim 10\%$ was achieved for all three f_{gate} with a low dark count probability in the order of 10^{-7} per SPAD gate. The afterpulsing probability when f_{gate} was 1 GHz and quantum efficiency at 10.11% was approximately 10.08%. Moreover, if a hold-off time (t_H) [34] was applied to ignore the afterpulses occurring within 30

ns and 50 ns after an avalanche, the afterpulsing probability fell to 4.53% and 2.02% respectively. This improvement of the afterpulsing probability was at the expense of the detection rate which corresponds to 33 MHz and 20 MHz. However, this is still ~ 330 times faster than existing COTS SPADs like the id210 from idQuantique [35].

It was also observed that as f_{gate} increases, the quantum efficiency dropped for a fixed V_{excess} . This phenomenon can be attributed to the decrease in the “gate on” (t_{on}) time. For an SPAD operating at higher f_{gate} , the primary carrier created by the absorbed photon has a shorter time to trigger impact ionisation as the avalanche current was quickly quenched when the gate signal fell and brought the SPAD below V_B . Hence, current through the output resistor, R_S (Figure 4.1.1) decreases and consequently, the voltage of the avalanche signal reduces. Thus, some weaker avalanche signals that falls below the discrimination threshold of the photon counter was not registered as a photon count. Therefore, if we increase f_{gate} , V_{excess} will also need to be increased in order to maintain similar quantum efficiency. Finally, related works were listed in Table 4.1 as a comparison to the proposed scheme to show that comparable results had been achieved. In addition, our proposed scheme has a tunable range of 500 MHz which has not demonstrated by others. It was also experimentally demonstrated that operation at various f_{gate} was possible without any modifications to the experimental setup.

Table 4.1 Comparison to related works on high-speed single photon detection.

Scheme	f_{gate} (GHz)	η (%)	P_D (per gate)	P_A (%)	t_H (ns)
Our scheme	1	10.2	1.43×10^{-6}	2.02	50
BSF ^[32]	1.5	10.8	6.30×10^{-7}	2.80	50
BSF ^[33]	2.23	10.0	4.80×10^{-7}	8.30	10
SD ^[51]	1.25	10.9	2.34×10^{-6}	6.16	10
PS ^[21]	1	10.4	6.10×10^{-6}	3.00	10

4.3 SUMMARY

In this chapter, we have proposed and demonstrated a high-speed single-photon avalanche diode with tuneable sinusoidal gate frequency. We had described the operating principle for our scheme and showed a 500 MHz tuneable range from 0.75 GHz to 1.25 GHz was possible.

We operated the system at 0.9 GHz, 1 GHz and 1.1 GHz and performed characterisation experiments which showed that our detection scheme was comparable with similar works [21, 32, 33, 51]. Moreover, our scheme employed a feedback algorithm to optimise the cancellation of transferred response. This feature is extremely important in practical systems which are subjected to environmental perturbations. Since our scheme was able to operate at various f_{gate} without a change in the experimental setup, it will be able to accommodate any drift in the clock frequency which results in a change in the SPAD gating rate.

CHAPTER 5 CONCLUSION AND FUTURE WORK

5.1 CONCLUSION

In this thesis, we have discussed two performance issues in the field of quantum key distribution systems. These are the polarisation and clock drifts. These performance issues are important as they affect the reliability and availability of a QKD system and its generated cryptographic keys. To solve these issues, we have proposed and demonstrated the following:

- 1) Adaptive polarisation state monitoring and recovery scheme for QKD systems based on polarisation-encoding to the counter polarisation drift.
- 2) High-speed single-photon avalanche diode with tunable sinusoidal gate frequency to counter clock drift.

In the adaptive polarisation state monitoring and recovery scheme for QKD systems based on polarisation-encoding, we had successfully demonstrated key distribution in laboratory and field experiments. We showed that our scheme was able to accommodate polarisation drift rates up to 0.30π rad/s while maintaining the QBER below the required limit for unconditionally secure key generation. In the field experiments over ~ 2 km of installed fibre, we found that the polarisation drift rates were often less than 0.02π rad/s with infrequent occurrence of higher drift rates not exceeding 0.1π rad/s. Therefore, our system was able to maximise the key generation rate to produce more sifted

keys at most times of the day. As soon as an increase in the rate of polarisation was detected by our system, quantum signals were automatically replaced by reference pulses to counter these polarisation instabilities. Although this resulted in a decrease of the key generation rate, the system was able to maintain the QBER below 11% where unconditionally secure key generation was still possible. Unlike the case when we operated the QKD system with the APSMR scheme disabled, when polarisation instabilities occurred, the QBER increase beyond 11% and hence no unconditionally secure cryptographic keys were produced. Therefore, we have showed that with the proposed APSMR scheme implemented, the reliability and availability of our QKD system was greatly enhanced.

In the high-speed single-photon avalanche diode with tunable sinusoidal gate frequency scheme, we had successfully showed high speed photon detection up to ~ 33 MHz. This is approximately 330 times faster than commercially available SPADs [35]. We have showed that our system has a 500 MHz tunable range from 0.75 GHz to 1.25 GHz. When we gated the system at 1 GHz, we recorded a quantum efficiency of 10.11% with a dark count and afterpulsing probabilities of 1.43×10^{-6} per gate and 2.02% respectively. We also operated our system at 0.9 GHz and 1.1 GHz with no changes to the experimental setup. The characterisation parameters we obtained were comparable to other similar works but with the added advantage of being able to operate at different gating rates and hence able to accommodate synchronisation clock drift which result in a changing f_{gate} . This is also

important in practical systems where operating conditions such as ambient temperature can change the frequency of the gating signals. However, due to technical difficulties, we were not able to show the detection system's ability to maintain constant quantum efficiency while changing the SPAD's gate frequency.

5.2 FUTURE WORK

Our current APSMR scheme depends only on the RIE to determine an appropriate frequency for the reference signals. However, when an eavesdropping attempt is being carried out, the QBER will be affected and hence no amount of reference pulses will lower it below the 11% limit. With the current scheme, the system does not take the abovementioned situation into account. Therefore, future improvement can be made to analyse other performance parameters such as the QBER in combination with the RIE to determine the source of the system's drop in performance. Moreover, our current system is located in a laboratory therefore we used short RF connections to convey the appropriate f_{ref} change. However, practical systems are located kilometres apart where such RF connections are not possible. Therefore, future improvement can make communication through the classical Ethernet channels possible.

In our experiments, we noted that the wavelength between the two lasers tend to drift apart at different frequency for the reference signals. We had to

manually tune the wavelengths to allow successful polarisation recovery. This problem can be solved if the wavelengths are stabilised and matched. One such way is to employ the Pound–Drever–Hall laser wavelength stabilisation technique [53].

Finally, we would like to integrate our high-speed single-photon detection and QKD systems. This will greatly enhance the key generation rate. Moreover, together with the APSMR implemented, the availability and reliability of our system can be guaranteed.

REFERENCES

- [1] C. E. Shannon, "Communication theory of secrecy systems," *Bell system technical journal*, vol. 28, pp. 656-715, 1949.
- [2] C. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *Journal of Cryptology*, vol. 5, pp. 3-28, 1992/01/01 1992.
- [3] C. Gobby, Z. L. Yuan, and A. J. Shields, "Quantum key distribution over 122 km of standard telecom fiber," *Applied Physics Letters*, vol. 84, pp. 3762-3764, 2004.
- [4] P. A. Hiskett, D. Rosenberg, C. G. Peterson, R. J. Hughes, S. Nam, A. E. Lita, *et al.*, "Long-distance quantum key distribution in optical fibre," *New Journal of Physics*, vol. 8, p. 193, 2006.
- [5] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "Current status of the DARPA quantum network (Invited Paper)," pp. 138-149, 2005.
- [6] A. Tanaka, M. Fujiwara, K. Yoshino, S. Takahashi, Y. Nambu, A. Tomita, *et al.*, "High-Speed Quantum Key Distribution System for 1-Mbps Real-Time Key Generation," *Quantum Electronics, IEEE Journal of*, vol. 48, pp. 542-550, 2012.
- [7] X. Tang, L. Ma, A. Mink, A. Nakassis, H. Xu, B. Hershman, *et al.*, "Quantum key distribution system operating at sifted-key rate over 4 Mbit/s," pp. 62440P-62440P, 2006.
- [8] Q. Zhang, H. Takesue, T. Honjo, K. Wen, T. Hirohata, M. Suyama, *et al.*, "Megabits secure key rate quantum key distribution," *New Journal of Physics*, vol. 11, p. 045010, 2009.
- [9] J. Chen, G. Wu, Y. Li, E. Wu, and H. Zeng, "Active polarization stabilization in optical fibers suitable for quantum keydistribution," *Opt. Express*, vol. 15, pp. 17928-17936, 2007.
- [10] J. Chen, G. Wu, L. Xu, X. Gu, E. Wu, and H. Zeng, "Stable quantum key distribution with active polarization control based on time-division multiplexing," *New Journal of Physics*, vol. 11, p. 065004, 2009.
- [11] Y. Liu, T.-Y. Chen, J. Wang, W.-Q. Cai, X. Wan, L.-K. Chen, *et al.*, "Decoy-state quantum key distribution with polarized photons over 200 km," *Opt. Express*, vol. 18, pp. 8587-8594, 2010.
- [12] C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, *et al.*, "Experimental Long-Distance Decoy-State Quantum Key Distribution Based on Polarization Encoding," *Physical Review Letters*, vol. 98, p. 010505, 2007.
- [13] G. B. Xavier, G. Vilela de Faria, G. P. Temporão, and J. P. von der Weid, "Full polarization control for fiber optical quantum

- communication systems using polarization encoding," *Opt. Express*, vol. 16, pp. 1867-1873, 2008.
- [14] G. B. Xavier, N. Walenta, G. V. d. Faria, G. P. Temporão, N. Gisin, H. Zbinden, *et al.*, "Experimental polarization encoded quantum key distribution over optical fibres with real-time continuous birefringence compensation," *New Journal of Physics*, vol. 11, p. 045015, 2009.
 - [15] C. H. Bennett and G. Brassard, "Quantum cryptography : Public key distribution and coin tossing," *Theoretical Computer Science*, 1984.
 - [16] N. Gisin, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, pp. 145-195, 2002 2002.
 - [17] S. Cova, M. Ghioni, A. Lacaita, C. Samori, and F. Zappa, "Avalanche photodiodes and quenching circuits for single-photon detection," *Appl. Opt.*, vol. 35, pp. 1956-1976, 1996.
 - [18] D. S. Bethune, W. P. Risk, and G. W. Pabst, "A high-performance integrated single-photon detector for telecom wavelengths," *Journal of Modern Optics*, vol. 51, pp. 1359 - 1368, 2004.
 - [19] N. Namekata, S. Sasamori, and S. Inoue, "800 MHz single-photon detection at 1550-nm using an InGaAs/InP avalanche photodiode operated with a sine wave gating," *Opt. Express*, vol. 14, pp. 10043-10049, 2006.
 - [20] A. Tomita and K. Nakamura, "Balanced, gated-mode photon detector for quantum-bit discrimination at 1550 nm," *Opt. Lett.*, vol. 27, pp. 1827-1829, 2002.
 - [21] L. Yan, E. Wu, C. Xiuliang, M. Ren, Y. Jian, W. Guang, *et al.*, "Low-Timing-Jitter Single-Photon Detection Using 1-GHz Sinusoidally Gated InGaAs/InP Avalanche Photodiode," *Photonics Technology Letters, IEEE*, vol. 23, pp. 887-889, 2011.
 - [22] A. Yoshizawa, R. Kaji, and H. Tsuchida, "Gated-mode single-photon detection at 1550 nm by discharge pulse counting," *Applied Physics Letters*, vol. 84, pp. 3606-3608, 2004.
 - [23] Z. L. Yuan, B. E. Kardynal, A. W. Sharpe, and A. J. Shields, "High speed single photon detection in the near infrared," *Applied Physics Letters*, vol. 91, pp. 041114-041114-3, 2007.
 - [24] R. Tjoa, K. L. Chee, P. K. Sivaprasad, S. V. Rao, and J. G. Lim, "Clock drift reduction for relative time slot TDMA-based sensor networks," in *Personal, Indoor and Mobile Radio Communications, 2004. PIMRC 2004. 15th IEEE International Symposium on*, 2004, pp. 1042-1047 Vol.2.
 - [25] L. Ma, H. Xu, and X. Tang, "Polarization recovery and auto-compensation in quantum key distribution network," pp. 630513-630513, 2006.
 - [26] M. Karlsson, J. Brentel, and P. A. Andrekson, "Long-term measurement of PMD and polarization drift in installed fibers," *Lightwave Technology, Journal of*, vol. 18, pp. 941-951, 2000.
 - [27] Y. Namiyama, Y. Horiuchi, S. Ryu, K. Mochizuki, and H. Wakabayashi, "Dynamic polarization fluctuation characteristics of optical fiber submarine cables under various environmental conditions," *Lightwave Technology, Journal of*, vol. 6, pp. 728-738, 1988.

- [28] R. Noe, H. Heidrich, and D. Hoffmann, "Endless polarization control systems for coherent optics," *Lightwave Technology, Journal of*, vol. 6, pp. 1199-1208, 1988.
- [29] T. Inukai, "Onboard clock correction by means of drift prediction," ed: Google Patents, 1986.
- [30] J. M. Belcea, "System and method for correcting the clock drift and maintaining the synchronization of low quality clocks in wireless networks," ed: Google Patents, 2006.
- [31] F. Sivrikaya and B. Yener, "Time synchronization in sensor networks: a survey," *Network, IEEE*, vol. 18, pp. 45-50, 2004.
- [32] N. Namekata, S. Adachi, and S. Inoue, "1.5 GHz single-photon detection at telecommunication wavelengths using sinusoidally gated InGaAs/InP avalanche photodiode," *Opt. Express*, vol. 17, pp. 6275-6282, 2009.
- [33] J. Zhang, P. Eraerds, N. Walenta, C. Barreiro, R. Thew, and H. Zbinden, "2.23 GHz gating InGaAs/InP single-photon avalanche diode for quantum key distribution," 2010, p. 76810Z.
- [34] Q.-L. Wu, N. Namekata, and S. Inoue, "Sinusoidally Gated InGaAs Avalanche Photodiode with Direct Hold-Off Function for Efficient and Low-Noise Single-Photon Detection," *Applied Physics Express*, vol. 6, p. 062202.
- [35] idQuantique. *id210 datasheet*. Available: <http://www.idquantique.com/images/stories/PDF/id210-single-photon-counter/id210-specs.pdf>
- [36] P. Shor and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," *Physical Review Letters*, vol. 85, pp. 441-444, 07/10/ 2000.
- [37] K. A. Patel, J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, *et al.*, "Coexistence of High-Bit-Rate Quantum Key Distribution and Data on Optical Fiber," *Physical Review X*, vol. 2, p. 041010, 2012.
- [38] V. Fernandez, R. J. Collins, K. J. Gordon, P. D. Townsend, and G. S. Buller, "Gigahertz-clocked quantum key distribution in passive optical networks," pp. 678004-678004, 2007.
- [39] S. C. Rashleigh, "Origins and control of polarization effects in single-mode fibers," *Lightwave Technology, Journal of*, vol. 1, pp. 312-331, 1983.
- [40] C. De Angelis, A. Galtarossa, G. Gianello, F. Matera, and M. Schiano, "Time evolution of polarization mode dispersion in long terrestrial links," *Lightwave Technology, Journal of*, vol. 10, pp. 552-555, 1992.
- [41] R. Ulrich, "Polarization stabilization on single - mode fiber," *Applied Physics Letters*, vol. 35, pp. 840-842, 1979.
- [42] B. Koch, V. Mirvoda, G. Grieder, H. Wernz, *et al.*, "Endless Optical Polarization Control at 56 krad/s, Over 50 Gigaradian, and Demultiplex of 112-Gb/s PDM-RZ-DQPSK Signals at 3.5 krad/s," *Selected Topics in Quantum Electronics, IEEE Journal of*, vol. 16, pp. 1158-1163, 2010.
- [43] N. J. Muga, A. J. Almeida, M. F. Ferreira, and A. N. Pinto, "Critical issues in polarization encoded quantum key distribution systems," in

- EUROCON - International Conference on Computer as a Tool (EUROCON), 2011 IEEE*, 2011, pp. 1-4.
- [44] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, A. R. Dixon, and A. J. Shields, "Single photon detection for high bit rate quantum communication," 2011.
 - [45] A. Yoshizawa, R. Kaji, and H. Tsuchida, "After-pulse-discarding in single-photon detection to reduce bit errors in quantum key distribution," *Opt. Express*, vol. 11, pp. 1303-1309, 2003.
 - [46] G. S. Buller, A. McCarthy, R. J. Collins, P. A. Hiskett, V. Fernandez, S. Hernandez-Marin, *et al.*, "Time-of-flight sensing using time-correlated single-photon counting," pp. 69001C-69001C, 2008.
 - [47] A. McCarthy, R. J. Collins, N. J. Krichel, V. Fernández, A. M. Wallace, and G. S. Buller, "Long-range time-of-flight scanning sensor based on high-speed time-correlated single-photon counting," *Appl. Opt.*, vol. 48, pp. 6241-6251, 2009.
 - [48] C. Saunders and P. J. Scully, "Sensing applications for POF and hybrid fibres using a photon counting OTDR," *Measurement Science and Technology*, vol. 18, p. 615, 2007.
 - [49] B. F. Levine, C. G. Bethea, and J. C. Campbell, "Near room temperature 1.3 μm single photon counting with a InGaAs avalanche photodiode," *Electronics Letters*, vol. 20, pp. 596-598, 1984.
 - [50] R. H. Haitz, "Mechanisms Contributing to the Noise Pulse Rate of Avalanche Diodes," *Journal of Applied Physics*, vol. 36, pp. 3123-3131, 1965.
 - [51] Z. L. Yuan, A. W. Sharpe, J. F. Dynes, A. R. Dixon, and A. J. Shields, "Multi-gigahertz operation of photon counting InGaAs avalanche photodiodes," *Applied Physics Letters*, vol. 96, pp. 071101-3, 2010.
 - [52] P. M. Krummrich, E.-D. Schmidt, W. Weiershausen, and A. Mattheus, "Field Trial Results on Statistics of Fast Polarization Changes in Long Haul WDM Transmission Systems," in *Optical Fiber Communication Conference and Exposition and The National Fiber Optic Engineers Conference*, Anaheim, California, 2005, p. OThT6.
 - [53] E. D. Black, "An introduction to Pound–Drever–Hall laser frequency stabilization," *American Journal of Physics*, vol. 69, pp. 79-87, 2001.