SILICON INTEGRATED TRANSMITTER FOR QUANTUM KEY DISTRIBUTION

by

Chaoxuan Ma

A thesis submitted in conformity with the requirements for the degree of Master of Applied Science
Graduate Department of Electrical and Computer Engineering
University of Toronto

© Copyright 2016 by Chaoxuan Ma
Abstract

Silicon Integrated Transmitter for Quantum Key Distribution

Chaoxuan Ma
Master of Applied Science
Graduate Department of Electrical and Computer Engineering
University of Toronto
2016

Silicon (Si) photonics is reaching maturity and has the potential of offering low-cost, reliable, chip-scale systems for quantum key distribution (QKD). On the other hand, QKD is also maturing with the bridging of theory and practice. This work presents a Si integrated photonic transmitter for polarization-encoded QKD. The chip was fabricated in a standard Si photonic foundry process and integrates a pulse generator, intensity modulator, variable optical attenuator, and polarization modulator in a 1.3 mm × 3 mm die area. The devices in the photonic circuit meet the requirements for QKD. The transmitter was used in a proof-of-concept demonstration of the BB84 QKD protocol over a 5 km long fiber link. A quantum bit error rate of 5.4% and an asymptotic secure key rate of 0.95 kbps is obtained. This work shows the feasibility of foundry based Si photonics for quantum information applications.
Acknowledgements

I am particularly grateful to my supervisor, Prof. Poon, who has been providing generous guidance and support to my research career. Every time I was in trouble with the experiment, she was there to help and offered constructive advice and inspirational ideas. Joyce’s excellent leadership and communication skills have set a good example for me. Plus, Joyce’s cheerful spirit and optimistic altitude towards work and life have always been a source of energy for me.

I also than Dr. Wesley Sacher for his excellent design of the chip and his generous help at the start of my experimental work. His rich experience in the field of Si photonics has provided me invaluable guidance both on the experimental work and my future research career.

I would like especially thank Zhiyuan for being so generous with his time to help me with the experimental demonstration of QKD. I am in debt with him for staying overnight to complete the experiment and tried hard to the last minute. Without him, I would not have gained so much insight into the practical implementation of QKD. I want to express my gratitude as well to Prof. Lo and Feihu for their constant input of expertise.

I am also thankful to Yisu for his assistance with the characterization of ring modulators and to Prof. Qian for her generous sharing of single photon detectors, and to Torrey for his assistance with the characterization of Si PIN diodes.

I would also like to say thank you to my dear family and Songyan for their unconditional support and love for me. They have always been the strong backing for my pursuit.

Lastly, I would like to thank all of my team members, Dave, Zheng, Ilan, Torrey, Jason, Antoine, Wesley, Jared and Yisu, and Joyce again for what they’ve taught me and shared with me, and for all the unforgettable days we’ve spent together. It’s the smartest and cheerful team I’ve ever seen. And I can not be more proud to be part of it.
# Contents

1 Introduction  
  1.1 Overview .................................................. 1  
  1.2 Thesis Outline ........................................... 3

2 Silicon Integrated Photonics  
  2.1 Why Silicon ................................................ 4  
  2.2 Basic Components ........................................... 5  
    2.2.1 Waveguides ............................................. 5  
    2.2.2 Fiber-to-Chip Couplers ................................ 6  
    2.2.3 Modulators ............................................... 6  
    2.2.4 Photodetectors .......................................... 9  
  2.3 Foundry Services .......................................... 10

3 Quantum Key Distribution  
  3.1 The Principle ............................................... 13  
    3.1.1 Uncertainty Principle .................................. 13  
    3.1.2 Non-cloning Theorem .................................... 13  
  3.2 Protocols .................................................. 14  
  3.3 QKD Components ............................................ 16  
    3.3.1 Single Photon Sources ................................. 16  
    3.3.2 Single Photon Detectors ............................... 18  
    3.3.3 Random Number Generators ............................ 20  
  3.4 Integrated Photonics for Quantum Key Distribution: A Literature Review .......... 20

4 Configuration, Fabrication and Characterization  
  4.1 Circuit Configuration ....................................... 24
4.2 Device Fabrication ................................................................. 24
4.3 Device Characterization ...................................................... 25
  4.3.1 Waveguides ................................................................. 25
  4.3.2 Ring Modulators ........................................................... 25
  4.3.3 Variable Optical Attenuator ........................................... 27
  4.3.4 Polarization Modulator .................................................. 29

5 Proof-of-Principle Demonstration of Quantum Key Distribution 36
  5.1 Experimental Method ....................................................... 37
    5.1.1 Experimental Setup ................................................... 37
    5.1.2 System Synchronization ............................................... 37
  5.2 Numerical Analysis .......................................................... 38
    5.2.1 BB84 Decoy States without Decoy States ......................... 39
    5.2.2 BB84 Decoy States with One Decoy State ......................... 41
    5.2.3 Simulation Results .................................................... 41
  5.3 Experimental Results ..................................................... 43

6 Summary and Outlook .......................................................... 44
  6.1 Summary ................................................................. 44
  6.2 Outlook ................................................................. 45

Bibliography ................................................................. 47
List of Figures

2.1 Waveguides on the standard SOI platform (the BOX and upper cladding for the waveguides are not shown). .............................................. 6

2.2 The basic structure of a microring. .................................................. 7

2.3 A typical design of a MZI modulator. .............................................. 8

2.4 Schematic cross section of IME A*STAR 30GHz Si photonic platform. The figure is from [111]. .......................................................... 10

3.1 Photon pair generation. (a) Spontaneous parametric down conversion process. (b) Spontaneous four wave mixing process. ................................................. 17

4.1 Schematic of the Si PIC transmitter for polarization-encoded QKD. The transmitter consists of a microring pulse generator, a microring intensity modulator, a VOA, and a polarization controller. .................................................. 23

4.2 Optical micrograph of the Si PIC transmitter for polarization-encoded QKD. ............ 24

4.3 (a) Optical micrograph of the microring modulator. (b) Schematic of the microring modulator. .......................................................... 25

4.4 (a) The normalized transmission spectrum with both microrings biased at critical coupling. (b) DC tuning of the transmission spectrum. (c) Histogram of a single pulse. (d) Histogram of 8000 overlapping pulses generated by the first microring modulator. (e) The time-dependent accumulated photon counts due to two alternating intensities from the modulation of the two microrings. The time bin is 1 ns. (f) The photon number distribution of the pulses in (e). The photon counts were calculated using a time bin of 5 ns. .......................................................... 26

4.5 (a) Optical micrograph of the VOA. (b) Schematic of the VOA. The VOA is a cascade of four identical MZIs (labeled M1 to M4). .................................................. 27
4.6 (a) Typical I-V curve of a 250 nm-long heater. (b) Normalized transmission of each MZI. The maximum attenuation provided by each MZI is 40.3, 44.0, 53.3 and 46.4 dB. The transmission is normalized to the starting point (zero bias).

4.7 (a) Optical micrograph of the polarization modulator. (b) Schematic of the polarization modulator. The two PIN diodes, heaters T1 and T2 have electrical interconnects on them for modulation and bias.

4.8 Coordinates of the Si waveguides $\hat{x}, \hat{y}$ and PBS $\{\hat{x}', \hat{y}'\}$

4.9 Simulations results of the normalized transmission of the two orthogonal polarizations vs. the differential phase shift $\Delta \theta$ applied to the PIN diodes (the left column) and the total transmitted power (normalized) and power ratio between the two orthogonal components vs. $\Delta \theta$ (the right column). (a) and (b) are under ideal conditions. (c) and (d) are the case when the system has a constant PDL of 1 dB. (e) and (f) are the consequences of absorption modulation by the plasma dispersion effect.

4.10 (a) Normalized transmission of the four polarizations vs. $\pm \Delta V$ applied to the PIN diodes in the MZI at a bias of 1.2 V. (b) The total transmitted power (normalized) and power ratio within each basis vs. $\Delta V$.

4.11 Projections of the polarization states onto $|D\rangle$ showing multi-level modulation using the second microring, VOA, and polarization modulator.


5.2 Output of the central AFG clock. (a) The internal trigger of the AFG with a period of 103 $\mu$s. (b) Output of the AFG’s first channel. Pulse generator driving the LiNbO$_3$ modulator is triggered by this channel. (c) Output of the AFG’s second channel. The TIA and AFGs driving the on-chip ring modulator (for intensity modulation, if needed) and polarization modulator are trigger by this channel.

5.3 Simulation results of secure key rate. (a) Secure key rate without using decoy states. The detector is SPAD. (b) Secure key rate without using decoy states. The detector is SNSPD. (a) Secure key rate using only one decoy state. The detector is SPAD. (b) Secure key rate using only one decoy state. The detector is SNSPD.
Abbreviations

AFG arbitrary function generator
APD avalanche photodiode
BOX buried oxide
BPF bandpass filter
CMOS complementary metal-oxide-semiconductor
COW coherent one way
CW continuous wave
DFS differential phase shift
DCR dark count rate
ER extinction ratio
FWHM full width half maximum
FWM four wave mixing
Ge germanium
IC integrated circuit
MMI multimode interference
MPW multi-project wafer
MZI Mach-Zehnder interferometer
PBS polarization beam splitter
PC polarization controller
PDK process design kit
PDL polarization dependent loss
PER polarization extinction ratio
PIC photonic integrated circuit
PNS photon number splitting
PRC polarization rotator combiner
QBER quantum bit error rate
QC quantum cryptography
QKD quantum key distribution
QRNG quantum random number generator
R&D research and development
RIE reactive ion etching
RNG random number generator
RTA rapid thermal anneal
SFWM spontaneous four wave mixing
Si silicon
SNSPD superconducting nanowire single photon detector
SOI silicon-on-insulator
SPAD single photon avalanche diode
SPD single photon detector
SPDC spontaneous parametric down conversion
SPM self-phase modulation
TBS tunable beam splitter
TCSPC time-correlated single photon counting
TE0 fundamental transverse electric mode
TM0 fundamental transverse magnetic mode
THG third harmonic generation
TIA time interval analyzer
UHVCVD ultrahigh vacuum chemical vapor deposition
VCSEL vertical-cavity surface-emitting laser
VOA variable optical attenuator
WCP weak coherent pulse
WDM wavelength division multiplexer
Chapter 1

Introduction

1.1 Overview

Leveraging the infrastructure for complementary metal-oxide-semiconductor (CMOS) electronics manufacturing, silicon (Si) photonics is emerging as a key technology for next-generation computing and communication systems with low power consumption and potentially low-cost optoelectronic integration. In recent years, Si photonic foundry fabrication services are maturing to form a fabless ecosystem [1].

Many Si photonic devices for classical optical communication have been successfully demonstrated, including waveguides, high-speed optical modulators, photodetectors, wavelength converters and polarization management components [2–4]. The availability of these building blocks, coupled with photon sources in Si and hybrid integration methods for single-photon detectors [5], paves the way for Si photonics to be applied to quantum information.

Quantum photonics has traditionally relied on bulk optical devices or exquisitely fabricated, singular microphotonic devices that have limited scalability and integration compatibility with other classical computing or communication components. Maturing Si photonic foundry fabrication services can enable Si photonic integrated circuits (PICs) for quantum information [3, 6], reducing the cost of incorporating quantum photonic functionality into classical systems.

A quantum technology prime for widespread use is quantum key distribution (QKD) [7–11], which exploits statistics of single photons to generate secure encryption keys. Owing to the quantum non-cloning theorem [12, 13], inevitable disturbances introduced by eavesdropping lead to a higher than expected quantum bit error rate (QBER) that can be detected by the two communication parties.
Moreover, unconditional security with weak coherent pulses (WCPs) can be achieved using decoy states [14–17].

Most of today’s commercial QKD systems use discrete components [18–20]. For chip-scale devices, many integrated material platforms, silica-on-silicon [21–25], laser written waveguides [26, 27], photonic crystal [28, 29], diamond [30], GaAs [31], InP [32], SiON [32, 33] and Si [34–37], have previously been used to implement circuits for multiple quantum applications [38] including QKD. In the long run, however, Si photonic platform would be a preferred choice: the high optical confinement in Si waveguides and resonance structures with small radii would result in high scalability and integration density; III-V/Si hybrid lasers [39], photon pair sources [40–42] and single photon detectors [43, 44] compatible with the Si platform have all been under development, so that a blueprint of monolithic integration of source, circuit, and detector is within reach; besides, multilayer silicon nitride-on-silicon platform [45, 46] reduces fiber-to-chip coupling losses and waveguide losses, and makes possible 3D circuit design with more design flexibility and complexity.

In this work, we demonstrated the first transmitter PIC for polarization-encoded QKD realized in a standard Si foundry platform. The transmitter PIC supports decoy states polarization-encoded QKD protocols and contains ring modulators, a variable optical attenuator (VOA) and polarization modulator. Each component on the chip has been characterized and a proof-of-concept QKD demonstration was conducted to evaluate the performance of the whole transmitter PIC. The PIC was designed and implemented by Wesley Sacher and Jared Mikkelsen. The characterization of the rings was assisted by Yisu Yang and the QKD demonstration was assisted by Zhiyuan Tang. An asymptotic secret key rate of 0.952 kbps was achieved with a QBER of 5.4% for the proof-of-concept QKD demonstration using the BB84 protocol. A paper summarizing the results was posted to arXiv [47]. Phase and time-bin encoding protocols should also be possible using Si photonics, such as BB84, COW and DFS, but such implementations require asymmetric interferometers with long on-chip delay lines, which introduce extra losses and a large footprint. Even though polarization states are not maintained in standard single mode telecommunication fibers, the relations between the polarization states are preserved at the receiver, and the polarization states can be recovered [48–53]. Polarization encoded QKD is also preferred for free-space links, such as satellite-to-ground communications [54–57]. Besides, QKD can also benefit short-distance applications such as card-less payments, network access or the internet of things, which also require a high level of security.


\section*{1.2 Thesis Outline}

The thesis is organized as follows. Motivations of Si integrated photonics, together with its fundamentals, is presented in Chapter 2. The recent progress in Si fabrication foundries will also be discussed. An overview of the basic knowledge about QKD, and the BB84 protocol are given in Chapter 3. Also included is a literature review of the demonstrated integrated photonic QKD systems. In Chapter 4, a detailed explanation of the circuit design is presented. The rationale, simulation and characterization results of each device on the transmitter PIC are presented and analyzed. Chapter 5 shows the proof-of-principle BB84 QKD demonstration, including its setup, numerical analysis and experimental results. Finally, the thesis is concluded with a summary in Chapter 6. Future device optimizations are also pointed out. And an outlook of the prospects for Si quantum photonics is given.
Chapter 2

Silicon Integrated Photonics

2.1 Why Silicon

Si is an essential element widely distributed on the earth in the various forms of silica and silicates. It is easy to process and mechanically strong, can be doped, has a high thermal conductivity and possesses a native oxide (SiO$_2$) which can be used as a high-quality insulator. The abundance of Si, together with its good physical properties, makes it a prime material for electronic integrated circuits (ICs). In the past half century, the microelectronic technologies have served as the main momentum to drive the information revolution of our society. From the emergence of transistors in the 1950s, their integration density on ICs has doubled every single year, which is known as the Moore’s law. This is achieved by relentlessly scaling down the size of transistors, which now has almost reached some physical limit. Further scaling may not only be technically unfeasible, but will also degrade the performance of ICs due to thermal issues. On the other hand, with the booming of the Internet sector, there is an urgent need for increased communication bandwidth and computation speed. People are therefore searching beyond the classical transistors for a substitute technology. Using light for information transmission becomes a natural solution because of the fast speed, high bandwidth, low power consumption and minimal thermal effects.

Si photonics is the leading candidate for this transform. Fabricating photonic devices in Si would mean that the current expertise and facilities for microelectronics, which have been invested and developed for 50 years, could be reused. And the integration of electronic and photonic devices on a single chip would be simplified. Si integrated photonics, which is compatible with the CMOS technology, is thus potentially the cheapest solution. CMOS technology is the standard design and fabrication tech-
nology for electronic ICs. If Si photonics would finally be mature enough for commercialization, the high precision, high yield and low cost of volume manufacturing in the existing fabs, would be soon translated to a technological and economical success.

Si also possesses good optical properties. A standard silicon-on-insulator (SOI) platform consists a thin Si layer (usually 220 nm) on top of a 2 μm-thick buried oxide (BOX) layer in SiO$_2$, as shown in Fig.2.1. The bottom is a thick Si substrate. All the devices are situated on the top layer. With the high index contrast between Si (3.48) and SiO$_2$ (1.44) or air (1), strong confinement of light at the telecommunication wavelength of 1550 nm is provided within Si waveguides. This allows for miniaturization of devices, enabling a high integration density. The current Si PIC platforms offer integration of both passive and active components, which are able to realize complex functionalities, such as optical transceivers [58–60], optical interconnects [61–63], computer processors [64–66], bio-sensors [67–69] and LiDAR [70–72]. Plus, the multiple nonlinear effects [73] (e.g., self-phase modulation (SPM), four wave mixing (FWM), the Raman effect, and third harmonic generation (THG) ) in Si extend its applications to supercontinuum generation [74–76], green light emission [77], light amplification [78, 79] and lasing [80–82], and all optical wavelength conversion [83–85]. The main disadvantage of Si, however, is that it can not efficiently emit light due to the indirect bandgap ($E_g = 1.12 eV$), which hinders the monolithic integration of a laser source on the PICs. Multiple approaches have been used to realize integrated Si lasers, among which Ge-on-Si lasers [86–88] and III-V/Si hybrid lasers [89–92] appear to be most practical. Current Si platforms consequently use an off-chip laser as the light source. The other challenges include on-chip isolators [93–96], passive fiber-to-chip coupling [97, 98], circuit-level design and simulation tools [99, 100] and optoelectronic integration [101, 102].

2.2 Basic Components

2.2.1 Waveguides

Integrated photonics uses waveguides for light routing. The waveguide is usually a structure with a high-index core and low-index cladding, which is similar to a fiber. On the SOI platform, the high index contrast between Si (3.48) and its cladding SiO$_2$ (1.44) or air (1) provides high confinement of the light, which also avoids the interaction between light and rough sidewalls and reduces the propagation loss. Typical designs of Si waveguides are shown in Fig. 2.1. The Channel waveguide is usually 400~500 nm wide, which ensures the single mode transmission of the fundamental transverse electric mode (TE0). The rib waveguide is usually used in the modulator to form a PN or PIN diode. For PN diodes, P doped
region and N doped region intersect in the rib. For PIN diode, the rib usually remains intact as the intrinsic region and dopants are only implanted to the slab.

### 2.2.2 Fiber-to-Chip Couplers

Fiber-to-chip coupling is one of the main challenges in Si photonics due to the large mode mismatch between their mode profile. On the standard Si platforms, there are two methods for the coupling: grating couplers and inverse tapers. Grating couplers couples light out of the plane. It thus has the flexibility to be placed anywhere on the chip, which does not require facet polishing and allows for testing on the whole wafer scale. Grating couplers are more tolerant of misalignment. Today, foundry available grating couplers can have a coupling efficiency of $<-3$ dB with a bandwidth of $\sim 25$ nm [104, 105]. The inverse taper, however, has to be placed on the edge of the chip with a cleaved facet, which requires additional fabrication process (deep trench). The advantages of using an edge coupler is a higher efficiency of $<-2$ dB and a larger bandwidth in [106] compared to grating couplers.

### 2.2.3 Modulators

An optical modulator is used to modulate the intensity, phase or polarization of an optical wave. An established way for traditional semiconductor materials is electro-optic or Pockels effect. The complex refractive index can be written as $n + ik$, where $n$ is the refractive index in the conventional context and $k$ is the optical extinction coefficient, which is related to the absorption coefficient $\alpha$ by $k = \alpha \lambda / 4\pi$. In the electro-optic effect, applying an external electric field will change both the refractive index and absorption coefficient.

Unfortunately, the electro-optic effect is either absent or very weak effectively in Si due to the centrosymmetry of Si crystal [107]. The thermo-optic effect is present in Si, but it is too slow (usually
at kHz) for the high speed telecommunication applications. Instead, Si relies on the plasma dispersion effect [107] to change the refractive index. In the plasma dispersion effect, change of carrier density in the material affects both the refractive index $n$ and the absorption coefficient $\alpha$. Thus one can achieve modulation either by carrier injection or depletion. The relation at 1550 nm is found to be [107]

$$\Delta n = -[8.8 \times 10^{-22} \times \Delta N_e + 8.5 \times 10^{-18} \times (\Delta N_h)^{0.8}], \quad (2.1a)$$

$$\Delta \alpha = 8.5 \times 10^{-18} \times \Delta N_e + 6.0 \times 10^{-18} \times \Delta N_h, \quad (2.1b)$$

where $\Delta N_e$ and $\Delta N_h$ are changes in the free electron density and free hole density measured in cm$^{-3}$; $\Delta n$ and $\Delta \alpha$ are the consequent changes in the refractive index ($n$) and absorption coefficient ($\alpha$).

The most common modulator structures today are ring modulators [108–110] and Mach-Zehnder interferometer (MZI)-based modulators [111–114], both translate phase modulation into intensity modulation. A typical ring modulator is shown in Fig. 2.2. It consists of a ring and access waveguide, which is coupled to the ring. Light with specific wavelengths coupled into the ring cavity will go through multiple round trips and build-up intensity because of constructive interference. The modulation efficiency is thus improved without extending the length of phase shifters. The transmission of the ring resonator is very sensitive to the wavelength. A small change in the refractive index inside the ring, which can be modulated by the intra-cavity PIN diode via the plasma dispersion effect, would induce a sharp change in the transmission at a specific wavelength. The steady-state or static transmission of a ring modulator
Chapter 2. Silicon Integrated Photonics

Figure 2.3: A typical design of a MZI modulator.

is given by [115]

\[
T_{\text{ring}} = \frac{\sigma - a e^{i\phi}}{1 - a\sigma e^{i\phi}}, \quad (2.2a)
\]

\[
|T_{\text{ring}}|^2 = \frac{\sigma^2 + a^2 - 2a \sigma \cos(\phi)}{1 + a^2 \sigma^2 - 2a \sigma \cos(\phi)}, \quad (2.2b)
\]

where \(\sigma\) is the resonator-waveguide transmission coefficient, \(a\) is the intra-cavity loss and \(\phi\) is the intra-cavity phase shift experienced by the light.

Critical coupling is obtained if \(\sigma = a\), in which case light in the access waveguide and light coupled out from the resonator interfere destructively and results in zero transmission. Highest extinction ratio is achieved when the wavelength is tuned on and off critical coupling. Plus, the SOI platform has a high index contrast and thus a high optical confinement, which makes the single-mode Si waveguides submicron, so a ring with small radii could be made. The high optical confinement coupled with resonance structure provides extremely compact devices. The resonance structure, however, also causes high sensitivity to the ambient environment.

A typical MZI is shown in Fig. 2.3. For the optical part, a general MZI is composed of two \(2 \times 2\) couplers separated by phase shifters. For simplicity, assuming a push-and-pull modulation with a signal \(\Delta V\) at a zero bias. The corresponding phase shifts on the two arms are \(\pm \Delta \theta/2\). The static transfer function of the MZI is thus given by

\[
\begin{pmatrix}
P3 \\
P4
\end{pmatrix} = i
\begin{pmatrix}
\sin \frac{\Delta \theta}{2} & \cos \frac{\Delta \theta}{2} \\
\cos \frac{\Delta \theta}{2} & -\sin \frac{\Delta \theta}{2}
\end{pmatrix}
\begin{pmatrix}
P1 \\
P2
\end{pmatrix}. \quad (2.3)
\]
Assuming an input to P1 and no input to P2, the output intensity of the MZI would be

\[
\begin{pmatrix}
P_3 \\
P_4
\end{pmatrix} = \begin{pmatrix}
\sin^2 \frac{\Delta \phi}{2} \\
\cos^2 \frac{\Delta \phi}{2}
\end{pmatrix}.
\] (2.4)

Thus, the intensity of an optical wave is modulated. Compared to ring modulators, MZI modulators are less thermally sensitive and have higher bandwidth. But due to the weak dependence of the refractive index of Si on the carrier density, MZI modulators usually require long phase shifters to completely switch from zero to unity transmission [111–114], which results in a much larger footprint (millimeters) and thus a higher insertion loss, cost and power consumption. Besides, since electro-optic modulators usually use lumped electrode structures, the bandwidth of the device will be limited by the RC constant, which is equal to the product of the circuit and junction resistance and capacitance.

2.2.4 Photodetectors

The on-chip germanium (Ge) photodetectors are reverse biased PIN diodes. Upon incidence of light into the intrinsic region, photons with enough energy will be absorbed and free electron-hole pairs are generated. The free carriers will be swept out by the reverse bias field and forms a current.

The biggest problem is that the integration of Ge on Si suffers from the 4.2% lattice mismatch between the two crystals, which brings about two problems: 1) a highly rough surface that makes the integration process difficult because CMOS devices require planar processing [116]; 2) a high threading and misfit dislocation density that degrade the performance of the detector, e.g., increased dark current [117]. Over time, advances in integration methods finally make Ge photodetectors a routine component on the standard Si integrated photonics. Multiple approaches have been used, such as inserting SiGe buffer layers [118, 119] as transitional layers between Si and Ge. Another approach is using two-step growth [120, 121], with the first thin layer of Ge served as a buffer layer. After these strategies, today’s foundries will also employ the post-growth annealing [105, 122] at a high temperature to further reduce the threading dislocation density.

With the integration onto the SOI platform, high performance Ge photodetectors with high quantum efficiency, high bandwidth and low dark currents have been demonstrated [116]. The latest high-speed Si platform has offered a 50 GHz Ge photodetectors [106] with a low dark current of 50 nA and a high responsivity with $\sim 0.88$ A/W in the C band.
2.3 Foundry Services

The greatest advantage of Si photonics is the ability to leverage the current CMOS technology. However, for a long time, there has been a limited access to affordable and advanced fabrication processes, tools and device libraries [123]. Researchers and small companies have to devote a lot of resources and effort to the fabrication process in their own cleanrooms, which hinders the innovation of Si photonics. Running and maintaining a cleanroom could also be a financially prohibitive task. The solution is multi-project wafer (MPW) shuttle runs provided by public manufacturing foundries, which allows multiple users to share the prohibitive cost of a photomask and fabrication run. Nowadays, several MPW runs from research and development (R&D) foundries [105, 122, 124, 125] have been available to the public, whose standard platforms have enabled more complex integration and higher performance reliability. Researchers are thus able to outsource the chip fabrication with a reasonable cost and at the same time, get guaranteed device performance. With the adoption of MPW runs, the innovation and development processes are accelerated and the entry barrier to prototyping is greatly reduced for academic groups and fabless companies[1, 123]. Si photonics is finally building up a fabless ecosystem.

The main providers of foundry services in the Si photonics community are IME [122] and ePIXfab[126] under the collaboration agreement of IMEC [105] and CEA-Leti [125]. Users are allowed to share a small area of the wafer, which are then fabricated through a standard process before being diced and sent to users. Our transmitter PIC is fabricated by IME A*STAR baseline Si photonics process. The platform includes low-loss waveguides, grating couplers, high speed Si modulators and Ge photodetectors. A detailed explanation about its fabrication process will be given in Chapter 4.

Process design kit (PDK) would be available after users sign the license agreement. Currently, PDK includes process documentation, library performance, layout guidelines for custom, design and
verification rules. It should ultimately include the device and circuit simulation tool, which is currently under development with software companies, to replicate the success of microelectronics [1].
Chapter 3

Quantum Key Distribution

In the era of the Internet, the security of information and communication has become a critical need for almost everyone. Cryptography, which protects the security of information by combining it with a key and thus allows two parties to share information against unauthorized access from the third party, offers higher levels of protection for the data. Unfortunately, the security of classical cryptography relies only on the computational complexity of mathematical problems (e.g. factoring large integers), which may possibly be compromised by future mathematical advances or quantum computing. The one-time pad protocol [127], where plaintext is combined with a random key with the same length and each key is for one-time use only, provides the only theoretically unbreakable encryption according to the information theory [128]. However, it requires that the two parties in communication have to share the key with an absolutely trusted channel or courier, which is hardly available in the real life.

The idea of quantum cryptography (QC) was first proposed by Stephen Wiesner [129] in 1983 and Charles H. Bennett and Gilles Brassard [7] in 1984. The most common and famous application of QC today is QKD, which is the process of distributing secret keys using quantum particles such as polarized photons. Unlike its classical counterpart, the unconditional security of key distribution in QKD relies on the quantum physics of single photons, instead of a fully trusted transmission channel.

The practice of QKD, however, suffers from imperfect devices (e.g., single photon sources and detectors, random number generators ), and lossy or noisy channels. Despite a number of limitations, QKD has undergone explosive progresses in the recent decade. QKD is more and more close to the reality with researchers’ efforts in bridging the theory and practice of QKD [130], such as decoy state method [15, 16], measurement-device-independent method [53, 131, 132], and loss-tolerant protocols [133]. Long-distance QKD both in fibers [53, 134, 135] and free space [54–57] have been achieved. Field tests have been
carried out in Japan [136], China [137, 138] and Europe [139]. With the maturity of QKD technologies, China is going to launch the first quantum satellite in July this year [140]. The ultimate aim is to realize global quantum communications. Finally, QKD steps out of the lab.

3.1 The Principle

3.1.1 Uncertainty Principle

In quantum mechanics, Heisenberg’s Uncertainty Principle sets the limit to the accuracy that any pair of physical properties can be measured, for example, position $x$ and momentum $p$. These properties are complementary in the sense that any measurement of one property would disturb the precision of measurements on the other. For example, the standard deviation of $x$ and $p$ has the relation below:

$$\sigma_x \sigma_p \geq \frac{\hbar}{2}.$$  

(3.1)

The two bases used in the BB84 protocol [7], for example, constitute such a pair. It is therefore impossible for one, no matter the eavesdropper (Eve) or the receiver (Bob), to measure the states with two conjugate bases simultaneously. According to quantum mechanics, only the eigenstates of the measurement would not be changed. So, Eve should have 50% chance of choosing the wrong basis, and thus inevitably causes disturbances on the system that can be detected by the two communication parties (Alice and Bob), which are usually in the form of QBER.

3.1.2 Non-cloning Theorem

The non-cloning theorem [12, 13] asserts that the linearity of quantum mechanics makes it impossible to obtain a perfect copy of an arbitrary quantum state. Let’s assume a device that is able to copy an arbitrary incoming quantum states $|s\rangle$. According to quantum mechanics, the transformation could be represented by a linear operator, which is given by

$$|\Phi_0\rangle|s\rangle = |\Phi_s\rangle|ss\rangle,$$  

(3.2)

where $|\Phi_0\rangle$ is the initial state of the device and $|\Phi_s\rangle$ is its final state.

Then for an incoming horizontal state $|H\rangle$ and vertical state $|V\rangle$, the device is able to get of a copy of both, which can be expressed by:

$$|\Phi_0\rangle|H\rangle = |\Phi_H\rangle|HH\rangle.$$  

(3.3a)
\[ |\Phi_0\rangle|V\rangle = |\Phi_V\rangle|VV\rangle. \quad (3.3b) \]

Now, if an arbitrary state \( \alpha |H\rangle + \beta |V\rangle \), which is a superposition of \( |H\rangle \) and \( |V\rangle \) with \( \alpha^2 + \beta^2 = 1 \), is incident, the result of the transformation would be given by the linearity of the system:

\[ |\Phi_0\rangle(\alpha |H\rangle + \beta |V\rangle) = \alpha |\Phi_H\rangle|HH\rangle + \beta |\Phi_V\rangle|VV\rangle. \quad (3.4) \]

The output of the device would be different from the initial state \( \alpha |H\rangle + \beta |V\rangle \) except that it is a purely horizontal state \( |H\rangle \) or vertical state \( |V\rangle \). It shows that there may be a device that can copy two special states, such as the horizontal state \( |H\rangle \) or vertical state \( |V\rangle \), but there can never be one that can copy an arbitrary quantum state. For QKD, it rules out the possibility that Eve could simply intercept the single photon, make a copy, and then send the original one to Bob, which would not cause any perturbation on the communication system and be noticed by Alice and Bob. In that case, Eve can measure the photon after Alice and Bob publicly announces the bases they used for each photon event and obtains all the information.

### 3.2 Protocols

The first working scheme for quantum key distribution, BB84 [7], was proposed by Charles H. Bennett of the IBM’s Thomas J. Watson Research Center, and Gilles Brassard of the University of Montreal, in 1984. The protocol uses four quantum states, \{\( |H\rangle, |V\rangle, |+\rangle, |−\rangle \}\), that constitute two conjugate bases, where \(|+\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)\) and \(|−\rangle = \frac{1}{\sqrt{2}}(|H\rangle − |V\rangle)\). They are conjugate in the sense that any pair of states, one from each basis, have the same overlap, e.g. \(|\langle H|+\rangle| = 1/2 [9]\). In the polarization-encoded scheme, the states can be identified as the polarization angles \{0°, 90°, 45°, −45°\}. Usually, \(|H\rangle \) and \(|+\rangle\) are denoted as bit '1', and \(|V\rangle \) and \(|−\rangle\) are denoted as bit '0'. The sender, Alice, prepares a sequence of single photons, which are randomly encoded in these four quantum states. The photons are then transmitted to the receiver, Bob, who measures the photons one at a time in a random choice of the two conjugate bases. These keys are called the raw key. Obviously, there is a 50% chance that Alice and Bob use different bases. Alice and Bob will then compare the bases they use for each photon in a public channel, and the keys for which they use incompatible bases would be discarded. The remaining keys after the basis reconciliation are called the sifted key. The sifted key usually has an error rate of a few percent, which is defined as QBER. It could be due to the technical imperfections of the devices and transmission channels, or the intervention of Eve. The definition of QBER was invented to avoid confusion with the bit error rate (BER) in the classical communication, where only a BER lower than
10^{-9} would be acceptable.

To detect the presence of tampering, Alice and Bob would repeatedly compute the QBER of a random subset of the sifted key, to see if it is below a reasonable threshold value. A higher than usual QBER would abort the communication. Otherwise, Alice and Bob would use some classical post-processing protocols, such as error correction algorithms and privacy amplification [141], to get rid of errors in the sifted key and reduce Eve’s information to an arbitrary low value [9]. With error correction, Alice and Bob can finally get a sequence of key with error rate down to the classical standard. In case Eve still has partial information, privacy amplification is employed. Privacy amplification is a process that allows two parties to distill a secret key from a larger body of shared information, which is partially secret. Alice and Bob generally know nothing about Eve’s information except that it satisfies a certain constraint. But Alice and Bob can publicly choose a compression algorithm, e.g. replacing randomly selected two bits with their XOR value, such that Eve’s information is even less if she does not know the exact value of the two bits, while the shortened keys are still error free. These keys are called the secure key, which will be used in combination with the one-time pad for information encryption.

There are other variations of the BB84 protocol, such as the BB92 protocol which uses two non-orthogonal states and the Ekert protocol which exploits quantum entanglement within a photon pair. More protocols emerged to simplify the process and setup. The differential phase shift (DFS) protocol encodes key values in the differential phase shift between two sequential single-photon pulses. The coherent one way (COW) protocol simply uses the arrival time of pulses to generate keys. The phase-encoded or time-encoded BB84, DFS and COW protocols are most common protocols demonstrated on integrated photonic platforms, due to their simple implementation and stability in fiber-optic systems [32, 142–146].

Most of today’s practical QKD systems uses WCPs as a substitute for an ideal single photon source, which would compromise the security of QKD without the decoy state protocol. The idea of the decoy state method was first proposed by Hwang et al. [14] and developed by Lo et al. [15] and Wang et al. [17]. The decoy state QKD uses more than one intensities of pulses. While only one of the intensities are used to produce keys, which is called the signal state, the other intensities are used as decoy states to detect Eve’s attacks only. By measuring the yields and QBER of the decoy states, a tight bound of the secure key rate can be estimated and therefore, substantially higher key generation rate is obtained.
3.3 QKD Components

The performance of the QKD components directly affects the efficiency and security of QKD. Practical QKD suffers from the imperfections of most QKD components.

3.3.1 Single Photon Sources

QKD is based on single photon Fock states. For most of the QKD protocols, even a small probability of multi-photon emission would compromise the unconditional security of QKD. Though the decoy state protocol [15] and privacy amplification have relieved the need for a perfect single photon source, they ensure the security at the expense of operation complexity and communication efficiency, compared to those using a perfect single photon source. In recent years, the explosive advances of QKD, together with other quantum information technologies, have motivated the development of related hardwares, such as single photon sources, single photon detectors (SPDs) and random number generators (RNGs).

Photon Source

An ideal single photon source [147] has the following characteristics:

1) The probability of firing one single photon is 100% and that of firing a multi-photon emission is 0%. That is, the mean photon number is 1, but the variance is 0.

2) The source has to fire on demand and at an arbitrarily fast speed except for the limitation posed by the temporal pulse duration [148].

3) Subsequent emitted photons are indistinguishable.

A variety of mechanisms are exploited for deterministic single photon emitters, which emit a single photon at every trigger, hence the name "photon gun". Most of them are quantum systems with two internal levels, such as semiconductor quantum dots [149, 150], single molecules [151, 152], single atoms[153, 154], single ions [155, 156], and color centers[157, 158]. Due to the lack of an ideal single photon source in real life, experimental QKD demonstrations often uses WCPs and photon pair sources. which we will discuss next.
Weak Coherent Pulse

For a coherent laser source, the number of photons in each pulse follows Poisson distribution. For a mean photon number of $\mu$, the probability for a pulse having $k$ photons is given by

$$P(k) = \frac{\mu^k e^{-\mu}}{k!},$$  \hspace{1cm} (3.5)$$

Thus, the probability of having a multi-photon emission is given by

$$P_{\text{multi}} = 1 - P(0) - P(1)$$
$$= 1 - (1 + \mu) e^{-\mu}$$
$$\approx \mu^2,$$  \hspace{1cm} (3.6)$$

where $\mu \ll 1$. In QKD, laser pulses are usually attenuated to, say, 0.1, to ensure a small possibility of multi-photon emission. However, since $\mu$ can never be zero, there are always a possibility of a multi-photon emission. Even such a small probability would subject the security of QKD to photon number splitting (PNS) \[159, 160\] attacks by a potential eavesdropper. In the PNS attacks, Eve (i) intercepts all pulses and counts the number of photons; (ii) For multi-photon pulses, she keeps one in a quantum memory and forwards the other to Bob; (iii) measures the photon after Alice and Bob publicly announces the bases they used for each photon and obtains all the information.

Furthermore, in order to maintain a low possibility of multi-photon emission, $\mu$ has to be extremely small, which, on the other hand, increases the possibility of a vacuum emission. The consequences are reduced key rate and higher QBER due to the dark counts of the SPDs. Fortunately, the decoy state method provides a theoretically unconditional security for QKD using WCPs, which has now become an essential supplement to most of the practical QKD demonstrations.

Photon Pair

![Photon pair generation. (a) Spontaneous parametric down conversion process. (b) Spontaneous four wave mixing process.](image)
Another substitute for an ideal single photon source is correlated photon pair sources. Photon pairs are usually generated from spontaneous parametric down conversion (SPDC) process [161] and spontaneous four wave mixing (SFWM) process [162], which are depicted in Fig. 3.1. SPDC is a $\chi^{(2)}$ nonlinear process, where a photon splits into two daughter photons (the so called idler and signal) with the energy and momentum conserved. SPDC is present in the BBO, KDP, LiNO$_3$, LiIO$_3$ crystals, etc. Si, on the contrary, lacks the mechanism due to the centrosymmetry of its lattice structure. SFWM is a $\chi^{(3)}$ nonlinear process, where two photons of the same wavelength are converted to two daughter photons with different wavelengths. Si has a high $\chi^{(3)}$ coefficient and can thus be used for photon pair generation via SFWM process. Both of the processes have to meet the requirement of phase matching.

The statistics of photon pairs again follows probabilistic distribution. Therefore, the average photon pair number also needs to be controlled to a low value to avoid multi-pair emission at a time. Photon pairs are useful in the time-energy entanglement QKD [163, 164] and polarization entanglement QKD [165, 166]. In the first protocol, the photon pair is used as a pseudo single photon source. One out of the photon pair is used as the heralding photon and the other is used as the signal photon. Only a signal photon being heralded by its sister would be detected. The latter exploits the quantum correlation in the photon pair’s polarization states. Alice and Bob each receives one photon out of the entangled pair and then randomly choose one of the three measurement bases independently. Measurements along parallel axes would produce a key, while measurements along oblique axes are used to test Bell’s inequality [167]. Eve’s attacks would disturb the inequality and reveal herself.

One of the disadvantage of such sources is the probability of multi-pair emission, like weak coherent pulses. The other disadvantage is the low efficiency of the nonlinear mechanisms, which can be in the order of $10^{-7} \sim 10^{-11}$.

### 3.3.2 Single Photon Detectors

SPDs are used to detect the arrival of single photons, which is the ultimate limit for optical detection. Normally, the detector would output an electrical pulse when a photon is registered. Combined with a time interval analyzer (TIA), one can precisely record the arrival times of registered photons. An ideal SPD should have the following characteristics:

1) The SPD outputs an electrical signal every time a photon is incident.

2) There is no noise generated by the SPD.

3) The SPD can operate at an arbitrary fast speed (except for the limit posed by the temporal width of electrical pulses).
The timing of the electrical outputs is accurately correlated with the arrival times of photons. However, in practice, not all the photons hitting the detector would produce such an electrical output. The probability of producing an electrical output on the incidence of a photon is the detection efficiency ($\eta_D$). A more deleterious effect for QKD is the dark count, which originates from the electronic noise and stray light inside the SPD circuits. Therefore, even in the absence of optical signals, there are still outputs from the SPD, faking a photon detection event. This feature is characterized by dark count rate (DCR). Besides, there is always a speed limit to the SPD, due to the time it takes to recover from a photon detection event, which is characterized by the dead time ($\tau$). The dead time sets the upper bound of the detector’s operation speed. Last, the timing uncertainty between the generation of electrical output and arrival of photons sets the timing resolution of detection.

The most commonly used single photon detectors for QKD are Si single photon avalanche diode (SPAD) and InGaAs SPAD. Avalanche photodiodes (APD) are PN or PIN diodes reversed biased above the breakdown voltage (known as Geiger mode). An absorption of photon would generate carriers that instantly undergo avalanche gain and break down the diode junction [168]. This mechanism has to be coordinated with quenching electronics to quench the current and restore the photodiode for the next detection event. Si SPAD has a high efficiency (can be as high as 80% at 800 nm [18]) from visible to near-infrared wavelengths (350-1000 nm), which is suitable for both fiber and free space detection, with low DCR (typically a few tens to hundreds Hz [18, 169]) and high timing resolution (typically a few hundreds ps). However, Si APDs have a low detection efficiency around telecommunication wavelengths, 1310 nm and 1550 nm, which is due to the bandgap of Si. One has to resort to InGaAs APD (950-1700 nm) for better performance. The InGaAs can reach a 20% detection efficiency at 1550 nm [18] but with a very high DCR of a few KHz, which reduces the signal-to-noise ratio (SNR).

The superconducting nanowire SPD (SNSPD) [170, 171] is a booming technology in recent years due to its superb performance. In superconducting nanowire (commonly in NbN or NbTiN), the absorption of even a single photon would form a local hotspot, a nonequilibrium state disrupting the superconductivity state of the nanowire. The equilibrium is reached by a sequence of relaxation process and finally form a resistive barrier across the width of the nanowire, which generates a measurable abrupt increase in the resistance [171]. SNSPDs usually have a DCR <100 Hz and can be further suppressed to a few Hz [18]. The dead time is usually <100 ns. The timing jitter can be <100 ps. The SNSPD has an extended operating wavelength range compared to Si APD and much higher performance than InGaAs APD, which becomes a preference for long-distance QKD demonstrations and field tests. The disadvantage of SNSPD is that it has to operate under a ultra-low temperature (~2.3K).
3.3.3 Random Number Generators

RNGs are used to select the encoding quantum states, measurement basis, and sometimes, method to produce key bits [172]. Random number generators are thus an essential component that greatly affect the security of QKD. However, most of today’s RNGs are pseudo-random number generator, which generates random numbers using deterministic computer algorithms, which may be cracked or manipulated by improved computational ability in the future.

Fortunately, people can rely on optical quantum noises for true random number generation, which is faster and harder to attack compared to electronic noises [173, 174]. There are multiple demonstrations for quantum random number generators (QRNG) already. The most simple example is a beam splitter dividing single-photon pulses [165, 175, 176]. The single photons has 50% of probability of entering each branch due to quantum mechanics. The generation speed depends on the detector’s speed. This removes the need for active components at Bob’s side. However, this method may suffer from slight asymmetry in the beam splitting ratio and detector’s detection efficiency, causing biased choice of ‘random numbers’. Other schemes for QRNGs include quantum phase noise of a highly attenuate laser [177], temporal discrimination of photon arrival times [178, 179], Optical homodyne detection of vacuum fluctuations [180] and physical chaos [181].

Another critical issue of random number generation is the characterization of true randomness which is elusive unfortunately. There are randomness tests [182], which can be used to determine where the set of data has a recognizable pattern and thus whether the number generation process is significantly random. However, these tests are by no means complete and pseudo-random numbers still have a chance to pass them. Therefore, a real-time self-testing of the output entropy of the random numbers is essential [183]. Possible solutions include device-independent QRNG [184, 185], random certification by the uncertainty principle [186] and from a pair of incompatible quantum measurements [183]. However, these methods are either difficult to implement or device dependent.

3.4 Integrated Photonics for Quantum Key Distribution: A Literature Review

QKD has been traditionally relied on individual bulk devices that are bolted to a large optical table for practical demonstrations. Such implementations are unscalable and would suffer from the instability of the individual devices. Though, quantum communication has emerged as a promising technology in the recent decade, classical communication would still be dominant in the foreseeable future. Thus, quantum
communication systems have to be compatible with the current classical communication networks by implementing in integrated photonics. Moreover, integrated photonics provides the stability and compactness that would not be possible with individual bulk components. After all, integrated photonics is a cheap and fast solution for customization and innovation. Several integrated photonic platforms have been used to implement QKD.

Silica planar lightwave circuits [142–146] have been a popular choice for waveguides and on-chip interferometers, which require high visibility quantum interference and sub-wavelength stability. The small thermal expansion coefficient (0.35 × 10⁻⁶K⁻¹ compared to Si’s 2.5 × 10⁻⁶K⁻¹ [187]) and elastic constants result in a minimal stress-induced waveguide birefringence, which makes the waveguides less polarization sensitive. The small thermal coefficient offers more stability as well. However, since the core of the waveguide is defined by doped SiO₂, there is only an index contrast of <1%, which provides low propagation loss but low mode confinement. The large mode profile in silica waveguides makes chip-to-fiber coupling efficiency higher than that in Si, but also results in larger device footprint, and lower integration density. On the other hand, it may be true that devices will be more tolerant of fabrication imperfections, but with the fabrication technology progress in precise lithography enabling small feature size (e.g. 193 nm UV lithography enabling a small feature size of 160 nm for Si waveguides [105]), this advantage is compromised. Nambu et al. and Kristensen et al. have both demonstrated long-distance time-bin encoded BB84 protocol on silica-on-silicon platform. However, the circuits were entirely passive due to a lack of fast modulation mechanisms on the glass platform and only limited functionalities can be integrated.

Similarly, laser-written platforms [188] also lack electro-optic modulation mechanisms. On these platforms, an ultrafast laser beam is focused into an optical material to modify its refractive index, which results in the formation of waveguide structures. The QKD sender unit for the BB84 protocol demonstrated by Mélen et al. [146] only used laser written waveguides as a beam combiner to combine different polarized beams from four off-chip vertical-cavity surface-emitting lasers (VCSELs). External polarizers and micro-lenses had to be used to obtain different polarization states and couple light between the source and chip. The system is quite cumbersome and unscalable compared to a monolithic integrated chip. Although laser-written technique enables rapid prototyping, simple fabrication process and 3D circuit design, the lack of active components on these platforms largely limits their applications in complex quantum photonic systems. And such techniques are only suitable for low-volume production.

Recently, Sibson et al. reported an encouraging work of a monolithic InP integrated photonic transmitter together with a SiN receiver (without the single photon detectors), fabricated in monolithic indium phosphide (InP) and silicon nitride (SiN) integrated photonic platforms available through foundries
The system is compatible with time-bin encoding BB84, DFS, and COW protocols. The InP platforms enables fast transmission rate and on-chip source integration and SiN offers a low loss and stable platform, which is especially important to the long delay line in the asymmetric MZI at Bob’s end. But compared with InP and SiN, the large wafer sizes available in Si photonic foundry processes (8” or 12” diameters [3, 189, 190] vs. 3” for InP [191] and or 4” for SiN [192]) and dense integration are conducive to scaling to high volume manufacturing. The lack of polarization management components on the InP platform also hinders its application in polarization-encoded protocols. Plus, the low-loss SiN is also compatible with the SOI platform [45, 46]. Therefore, an implementation on the Si platform will take the advantage of both the high-performance active components in Si and low-loss passive components in SiN, so that a complicated transmitter and a low-loss receiver can be realized on the same platform.

In conclusion, Si has the best overall performance, with the strengths in low loss, low cost, high integration density and mass production. The main weakness lies in the lack of an on-chip single photon source, but can be circumvented using photon pair sources [193, 194], which has been well explored using the SFWM process. It may also be addressed by the Ge-on-Si lasers [86–88] and III-V/Si hybrid lasers [89–92] under development.
In this thesis work, we demonstrated the first QKD transmitter PIC for polarization-encoded QKD realized in a Si foundry platform. The chip was designed by W. D. Sacher. Each component on the chip has been characterized and a proof-of-concept QKD demonstration was conducted to evaluate the performance of the whole transmitter PIC. The characterization of the rings was assisted by Yisu Yang.

Figure 4.1: Schematic of the Si PIC transmitter for polarization-encoded QKD. The transmitter consists of a microring pulse generator, a microring intensity modulator, a VOA, and a polarization controller.
Chapter 4. Configuration, Fabrication and Characterization

4.1 Circuit Configuration

The transmitter PIC is designed for polarization-encoded BB84 QKD. Fig. 4.1 shows the schematic of the transmitter PIC. It consists of two ring modulators, a VOA and a polarization modulator. The first ring modulator generates periodic nanosecond (ns) pulse trains from a continuous-wave (CW) laser, while the second ring modulates pulse intensities to create decoy and signal states, if needed. The VOA attenuates the pulses into single photon level, and the polarization modulator prepares the polarization state of photons. Light is coupled into/out of the chip using on-chip adiabatic inverse waveguide tapers and lensed fibers with a 2.5 \( \mu \text{m} \) spot diameter. The tip of the edge couplers has a cross section of 200 nm \( \times \) 220 nm, to minimize the polarization dependent loss (PDL). Extra input and output ports are available in the PIC to enable the characterization of the individual devices.

4.2 Device Fabrication

The optical micrograph of the PIC is shown in Fig. 4.2. The transmitter, with a small size of 1.3 mm \( \times \) 3 mm, was fabricated at A*STAR IME using its baseline Si photonics process, which has a similar fabrication process as described in [122]. The Si photonics platform has several heights available at the top Si layer, which enable the integration of various passive and active devices such as channel and rib waveguides, low-loss grating couplers, MZIs, high-speed modulators and Ge photodetectors.
Chapter 4. Configuration, Fabrication and Characterization

4.3 Device Characterization

4.3.1 Waveguides

The main types of waveguides in the transmitter PIC are single-mode channel waveguides and rib waveguides, which preferentially support TE0 mode. The standard routing waveguide is a 500 nm-wide channel waveguide. The rib waveguide with a 500 nm width and 90 nm slab thickness, is used in the Si modulators’ PIN junctions and resistive heaters for modulation and static bias respectively. The waveguides have an average propagation loss of \(\sim 2\) dB and \(\sim 0.8\) dB at the central wavelength of 1538 nm across dies, and attain a similar performance in the measurements for 1550 nm [1]. Bending loss for a 5 \(\mu\)m Si channel waveguide bend (width of 500 nm) was measured to be 0.016 dB per 90\(^\circ\) bend.

For calibration purposes, there are straight waveguides and bend structures on the chip. The straight waveguide and bend structure span across a total length of 2.6 mm, both with an 200 \(\mu\)m long inverse tapers on each side for chip-to-fiber coupling. The latter has 224 90\(^\circ\) bends with a radius of 10 nm in series. The transmission of the straight waveguide is -8.38 dB, which is largely due to the chip-to-fiber coupling loss and the loss of the straight waveguide should be minimal. The bend structure has a total transmission of -9.77 dB, which means a negligible loss of 0.006 dB per 90\(^\circ\) bend with 10 \(\mu\)m radii.

4.3.2 Ring Modulators

The two microring modulators are used for pulse generation and multi-level intensity modulation for decoy and signal states. Thanks to the strong mode confinement and resonant structure, microring modulators have a small footprint, which reduces the insertion loss, fabrication cost and power consumption, and increases the integration density of PICs. For QKD, modulators have to be fast enough (GHz) to generate ns pulses and have a high extinction ratio (ER) to reduce error rate. Fig. 4.3 shows the optical micrograph and schematic of the microring modulator. Each microring contains a 400 \(\mu\)m long
Figure 4.4: (a) The normalized transmission spectrum with both microrings biased at critical coupling. (b) DC tuning of the transmission spectrum. (c) Histogram of a single pulse. (d) Histogram of 8000 overlapping pulses generated by the first microring modulator. (e) The time-dependent accumulated photon counts due to two alternating intensities from the modulation of the two microrings. The time bin is 1 ns. (f) The photon number distribution of the pulses in (e). The photon counts were calculated using a time bin of 5 ns.

PIN diode phase-shifter inside the ring for modulation. A 2 × 2 MZI coupler and an intracavity 100 µm long doped Si resistive heater provide independent tuning of the coupling coefficient and resonance wavelength, respectively, to achieve modulation with a high ER. Thin film heaters were not available in this foundry process.

Fig. 4.4(a) shows the static transmission of the transmitter when both microrings were set to the critical coupling condition and slightly detuned from each other. The microrings had a free spectral range of 0.65 nm, and the minimum transmission was about -27 dB. The intrinsic $Q$ factor of the microrings was about $1.9 \times 10^6$. Fig. 4.4(b) shows the tuning of the transmission at a fixed wavelength of 1549.9 nm as a DC voltage was applied to the intracavity PIN diode of the first microring. A static ER of 25.6 dB was achieved by an applied voltage of only 50 mV. The starting point experienced extra attenuation in the first ring, which resulted in the asymmetry of the transmission in the low and high tuning voltages. And the asymmetry of the shape was a consequence of the nonlinear I-V curve of the PIN diode. Fig. 4.4(d) shows the pulse shape generated by the first microring modulator, which is a histogram of 8000 overlapping pulses. The microring modulator was driven by a programmable pattern generator with bursts of 8000 1 ns-wide long pulses at a repetition rate of 10 MHz to generate a train of nominally
Figure 4.5: (a) Optical micrograph of the VOA. (b) Schematic of the VOA. The VOA is a cascade of four identical MZIs (labeled M1 to M4).

identical pulses. The tests last for >5 min. The optical pulses had a full width half maximum (FWHM) of 2.4 ns and the jitter was 1.2 ns. The dynamic ER was 20 dB, which, to our knowledge, is the highest of any Si microring and MZI modulator. A high ER reduces the QBER penalty [9]. The long tail of the pulse was produced by the long minority carrier recombination time of the injected carriers.

The two microring modulators, when tuned to have matching resonances, could generate pulses and varying amplitude levels. Fig. 4.4(e) shows the cumulative photon count of $3.75 \times 10^5$ repetitions of a modulation pattern with alternating intensity levels. The first microring was driven with 1 ns long pulses at a repetition rate of 10 MHz, and the second microring modulator was driven by a 5 MHz square-wave from an arbitrary function generator (AFG). The two voltage levels of the AFG produced the two intensities, which could be used for signal and decoy states, as shown in Fig. 4.4(e). Fig. 4.4(f) shows the distribution of cumulative photon counts. The mean photon number per pulse for the two states were $0.129 \pm 0.003$ and $0.009 \pm 0.001$, respectively.

4.3.3 Variable Optical Attenuator

A relatively large attenuation is required from the on-chip variable optical attenuator for the following purposes:

1) The attenuator is capable of attenuating the input pulses into single photon levels.

2) The intensity of the input pulses should be relatively high for monitoring purposes.

The optical micrograph and schematic of the VOA is shown in Fig. 4.5. The VOA in the transmitter PIC consists of four cascaded nominally balanced $2 \times 2$ MZIs. Each MZI has two 3 dB multimode interference (MMI) couplers separated by 300 $\mu$m long phase-shifters, each containing a 250 $\mu$m long resistive heater. A typical I-V curve for the heater is shown in Fig. 4.6(a). For each MZI, heating
Chapter 4. Configuration, Fabrication and Characterization

Figure 4.6: (a) Typical I-V curve of a 250 nm-long heater. (b) Normalized transmission of each MZI. The maximum attenuation provided by each MZI is 40.3, 44.0, 53.3 and 46.4 dB. The transmission is normalized to the starting point (zero bias).

Figure 4.7: (a) Optical micrograph of the polarization modulator. (b) Schematic of the polarization modulator. The two PIN diodes, heaters T1 and T2 have electrical interconnects on them for modulation and bias.

A phase-shifter causes a differential phase shift $\Delta \phi$ between the two arms. The attenuation can be expressed by

$$\text{Att}(dB) = 20 \log_{10} |\cos \frac{\Delta \phi}{2}|.$$ \hspace{1cm} (4.1)

The total attenuation provided by the VOA is a summation of attenuation (in dB) from all the four MZIs. The measured tuning range of each MZI (labeled M1 to M4) is shown in Fig. 4.6(b). Each MZI could provide $> 40$ dB of attenuation, so the VOA could generate an attenuation in excess of 160 dB. As a comparison, a 0 dBm pulsed input at 10MHz needs an attenuation of $\sim 100$ dB to have a mean photon number of 0.1.
4.3.4 Polarization Modulator

The output of the VOA connects to the polarization modulator, which is the most critical component for polarization encoding. The polarization modulator is used to prepare the four states, {\(|H\rangle, |V\rangle, |D\rangle, |A\rangle\)}, which constitute two conjugate bases. In the polarization-encoded scheme, the states are identified as the polarization angles \(\{0^\circ, 90^\circ, 45^\circ, -45^\circ\}\). For the BB84 QKD protocol, the polarization modulator should meet the following criteria:

1) Sufficient modulation speed compatible with the QKD system.

2) A high polarization extinction ratio (PER).

3) A small power distinguishability for different polarization states, that is, a low PDL.

An optical micrograph and schematic of the polarization modulator is shown in Fig. 4.7, and the design is based on our work in [195]. The polarization modulator consists of a nominally balanced MZI followed by a polarization rotator combiner (PRC). The MZI has a 1000 \(\mu\)m long PIN diode and a 250 \(\mu\)m long resistive heater embedded in each phase-shifter. An additional set of heaters are in the inputs to the PRC. While only one in each set of heaters is used for tuning, the other is included to balance the loss of the two paths. The PIN diodes are driven in push-pull and modulate the effective index of the Si waveguides by the plasma dispersion effect [107]. The Si PIC preferentially supports the TE0 mode, while other modes, including the fundamental transverse magnetic mode (TM0), will be quite lossy. TE0 and TM0 are two quasi-orthogonal modes in the Si waveguides. The PRC is able to rotate one of its input from TE0 to TM0 and combine it with the other input which is preserved as the TE0 mode. The rotation is achieved by converting the TM0 mode to TE1 mode through mode hybridization in a bi-level and vertically asymmetric taper. The output Si waveguide is tapered into a tip with cross-section dimensions of 200 nm \(\times\) 220 nm, which makes the coupling efficiency almost polarization independent. The output is coupled to a lensed fiber with a 2.5 \(\mu\)m spot diameter.

Operation Principle

An arbitrary polarization state can be described by a 2 \(\times\) 1 Jones vector as below:

\[
\begin{pmatrix}
A_x \\
A_y
\end{pmatrix} = \begin{pmatrix}
a \\
be^{i\delta}
\end{pmatrix},
\]

where the two components represent two orthogonal polarization states, \(|a|^2 + |b|^2 = 1\) and \(\delta\) is the phase difference between the two components. Note that any common phase in \(a\) and \(b\) can be absorbed by a
constant outside the vector. Thus, a polarization state can be defined by the amplitude ratio of the two orthogonal components and the phase difference in between, which the polarization modulator should be able to manipulate so as to produce arbitrary polarization states.

The combined transfer function of the MZI and the heaters preceding the PRC can be expressed as:

$$
\begin{pmatrix}
P_3 \\
P_4
\end{pmatrix} = -ie^{i(\theta+\Delta\phi_1/2)} \begin{pmatrix} -\sin \beta & \cos \beta \\
e^{i\Delta\phi_2} \cos \beta & e^{i\Delta\phi_2} \sin \beta \end{pmatrix} \begin{pmatrix} P_1 \\
P_2
\end{pmatrix}, \quad (4.3)
$$

where $\beta = (\Delta\theta + \Delta\phi_1)/2$. $\theta$ and $\Delta\theta$ are the constant phase shift on the PIN diodes and the differential phase shift between the two, which are modulated by a small push-and-pull signal superimposed onto a constant bias. $\Delta\phi_1$ and $\Delta\phi_2$ are the phase shifts caused by the constant biases on heaters T1 and T2, respectively. They are shown in Fig. 4.7(b).

Since only the lower input port P2 is enabled during operation, the output wave of the polarization modulator will be:

$$
E(t) = E_0 e^{i(\omega t - k z)}(\hat{x} \cos \beta + \hat{y} e^{i\Delta\phi_2} \sin \beta), \quad (4.4)
$$

where $\omega$ is the angular frequency and $k$ is the propagation constant of light wave. $z$ is the total optical path length. Vectors $\hat{x}$ and $\hat{y}$ are the two orthogonal polarization components. Note that the PRC rotates the lower input to TM0 mode ($\hat{y}$) and combines it with the upper input in TE0 mode ($\hat{x}$). Then we have the corresponding Jones vector:

$$
P = \begin{pmatrix} 
\cos \beta \\
e^{i\Delta\phi_2} \sin \beta
\end{pmatrix}. \quad (4.5)
$$

The function of each tuning component should now be clear. In the polarization modulator, the MZI controls the amplitude ratio between the two orthogonal components and the heater T2 controls the phase difference. The power of the output is theoretically uniform across arbitrary polarization states, since $|\cos \beta|^2 + |e^{i\Delta\phi_2} \sin \beta|^2 \equiv 1$. The four polarization states $\{0^\circ, 90^\circ, 45^\circ, -45^\circ\}$ in our QKD scheme should all be linear states with the relative phase between TE and TM mode being zero. Therefore, T2 should only be biased to compensate the phase mismatch induced by fabrication errors, so that the rotation of the polarization states is confined on the equator of the Poincaré sphere, while the PIN diodes are dynamically driven by a push-and-pull signal to rotate the polarization. T1 can be used to define the output state when $\Delta\theta = 0$. 
PER and PDL

In the ideal situation, the polarization modulator provides unlimited PER and zero PDL. Unfortunately, there are practical undesirable effects that degrade the ER or make the power levels of polarization states distinguishable. These effects include:

1. **Static PDL caused by various mechanisms.** These mechanisms include heating T2, fabrication errors in the PRS and chip-to-fiber coupling.

2. **Absorption coefficient modulation on PIN diodes.** Ideally, only the real part of the complex refractive index is modified, but the plasma dispersion effect also slightly alters the absorption coefficient, which causes a slight PDL and degrades the PER.

To simulate the consequences of these effects, one has to look into Eq. 4.5 more closely and take these effects into consideration. In fact, $\Delta \theta$, $\Delta \phi_1$ and $\Delta \phi_2$ are all complex numbers due to the plasma dispersion effect on the absorption coefficient of Si waveguides.

The phase shift $\Delta \theta$ is now related to the absorption coefficient change:

$$\Delta \theta = k_0(\Delta n + i\frac{\Delta \alpha \lambda}{4\pi})L_{PIN},$$

(4.6)

where $L_{PIN}$ is the length of the PIN diodes. And $k_0$ is the propagation constant of light in the vacuum.

To demonstrate the PER and PDL of the polarization modulator, one can imagine that it is measured by a polarization beam splitter (PBS), which has two output branches connected to optical power meters. PER and PDL can be observed by monitoring the power projections of polarized light onto the PBS’s two outputs. Assuming there is an angle $\varphi$ between the polarization coordinates of Si waveguides $\{\hat{x}, \hat{y}\}$ and the coordinates of the PBS $\{\hat{x}', \hat{y}'\}$, as shown in Fig. 4.8. Then the power at the two outputs
Figure 4.9: Simulations results of the normalized transmission of the two orthogonal polarizations vs. the differential phase shift $\Delta \theta$ applied to the PIN diodes (the left column) and the total transmitted power (normalized) and power ratio between the two orthogonal components vs. $\Delta \theta$ (the right column). (a) and (b) are under ideal conditions. (c) and (d) are the case when the system has a constant PDL of 1 dB. (e) and (f) are the consequences of absorption modulation by the plasma dispersion effect.

would be given by

\[ P_x' = |\cos \beta \cos \varphi - e^{i\Delta \phi_2} \sin \beta \sin \varphi|^2, \tag{4.7a} \]

\[ P_y' = |\cos \beta \sin \varphi + e^{i\Delta \phi_2} \sin \beta \cos \varphi|^2. \tag{4.7b} \]

Fig. 4.9 are the calculation results at 1550 nm. Using Eq. 2.1 and 4.7. The left column shows the
power evolution of the PBS’s two outputs vs. the differential phase shift on the PIN diodes, that is, the real part of $\Delta \theta$. The right column shows the total power variation (dash black) and the power ratio between the two outputs. Local extrema of the blue solid line are the local PER at the point, where the polarization overlaps with one of the PBS’s eigenvectors ($\hat{x}'$ or $\hat{y}'$) to the largest extent and leaves minimum power projected to the other eigenvector. The additional dash blue line in Fig. 4.9(f) is the theoretical PER. For a given polarization state as Eq. 4.2, the PER can be determined by

$$PER = \frac{\tan^2 \gamma + r^2 + 2r \tan \gamma \cos \delta}{1 + r^2 \tan^2 \gamma - 2r \tan \gamma \cos \delta},$$

(4.8)

where $\gamma = \frac{1}{2} \arctan \frac{2r \cos \delta}{r^2 - 1}$ and $r = b/a$. $\varphi$ (see Fig. 4.8 for its definition) is set to be $45^\circ$. The phase difference between TE and TM modes due to fabrication errors and fiber birefringence is neglected. Fig. 4.9(a) and (b) show the ideal situation. As the polarization modulator rotates the polarization, the ratio varies. But the PER remains infinite and there is no power variation. Fig. 4.9(c) and (d) show the consequence of a constant PDL of 1 dB between TE and TM modes. The PER still remains infinite, but the total power varies by 1 dB, which means the polarization states can be distinguished by their power levels. Fig. 4.9(e) and (f) illustrate the plasma dispersion effects. There is obviously a slight PDL and degraded PER. What’s worse, the PER sharply drops with the increase of differential phase shift between the two PIN diodes. Note that the total power transmission is normalized to the point where $\Delta \theta = 0$. That’s why the transmission could exceed 0 dB. The model is justified by the experimental data, which will be presented later.

With further efforts, these problems can be addressed with the following possible solutions:

1) **PDL.** The PDL at the chip output can be compensated by adding tunable attenuators at the inputs of the PRC to allow for fine balancing of the loss between the TE and TM components. One can also control the intensities of pulses for different states at the ring modulators.

2) **PER.** The degradation of PER is due to dynamically modulated phase difference between TE and TM modes, which results from the absorption coefficient modulation on the PIN diodes. The PER can thus be increased by including PIN diode phase-shifters at the inputs of PRC for the dynamic compensation of the phase mismatch between the two polarization components.

**Experimental Results**

To measure the polarization tunability, the output of the polarization modulator was passed through a fused fiber polarization independent 3 dB splitter, and each output branch passed through an in-fiber
Chapter 4. Configuration, Fabrication and Characterization

Figure 4.10: (a) Normalized transmission of the four polarizations vs. $\pm \Delta V$ applied to the PIN diodes in the MZI at a bias of 1.2 V. (b) The total transmitted power (normalized) and power ratio within each basis vs. $\Delta V$.

Figure 4.11: Projections of the polarization states onto $|D\rangle$ showing multi-level modulation using the second microring, VOA, and polarization modulator.

polarization controller (PC) followed by a fiber-based PBS. The PCs were set such that the coordinates of each PBS were aligned to the rectilinear and diagonal bases, respectively, so that Bob was able to measure the incoming photons with the two bases. Fig. 4.10(a) shows the transmission at the outputs of each PBS vs. a small-signal voltage sweep, $\Delta V$, applied in push-pull mode to the PIN diodes in the on-chip polarization modulator at a bias of 1.2 V. That is, voltages of $1.2V \pm \Delta V$ were applied to the phase-shifters. Fig. 4.10(b) shows the total transmitted power and power ratio of the two orthogonal components within each basis. The results matched well with the numerical simulation results in Fig. 4.9. One can see that the experimental results were a superposition of PDL in the system and absorption coefficient modulation by the plasma dispersion effect. The system’s PDL is $\sim 1.6$ dB. A PER of $>30$ dB was obtained, and the power variation across the four polarization states was 0.9 dB.
Dynamic modulation was also tested using InGaAs SPADs and WCPs at a repetition rate of 10 MHz with a repeating pattern of \{\ket{H}, \ket{V}, \ket{D}, \ket{A}\}. A QBER of 4.18% and 8.22% for the vertical and diagonal bases, respectively, was achieved.

Fig. 4.11 shows the photon number histograms of the four polarizations projected onto \ket{D} using the second microring modulator, VOA, and polarization modulator, illustrating the capability to generate variable amplitude levels (e.g., for decoy states [15]), attenuation, and polarization modulation. The input to the chip was a periodic pulse train, to reduce the onus of tuning and stabilizing the two microring modulators. The mean photon numbers for the two intensities were estimated to be 0.094 and 0.029.
Chapter 5

Proof-of-Principle Demonstration of Quantum Key Distribution

Here, we present a proof-of-concept polarization-encoded BB84 QKD demonstration using the on-chip VOA and polarization modulator at the wavelength of 1550 nm. The QKD demonstration was assisted by Zhiyuan Tang.

![Figure 5.1: Setup schematic. PS: power supply, PG: pulse generator, IM: intensity modulator, AFG: arbitrary function generator, BPF: bandpass filter, SMF: single mode fiber, TBS: tunable beam splitter, PC: polarization controller, PBS: polarization beam splitter, SPAD: single photon avalanche photodetector, TIA: time interval analyzer.](image-url)
Chapter 5. Proof-of-Principle Demonstration of Quantum Key Distribution

5.1 Experimental Method

5.1.1 Experimental Setup

The setup is shown in Fig. 5.1. For improved modulation ER and thermal stability, the microring modulators were bypassed and an external LiNbO$_3$ intensity modulator was used to modulate a CW laser at 1550 nm instead. The external modulator provided a dynamic ER of 30 dB compared to 20 dB of the microring, reducing the penalty on the QBER. For a perfect single photon source, to obtain a secret key with Shor-Preskill’s proof [196] requires a QBER less than ∼11%. Secure QKD can be done with weak coherent pulses [197]. At the sender (Alice’s) side, the input to the PIC was bursts of 1000 optical pulses with a FWHM of 1 ns at a repetition rate of 10 MHz. The bursts were at the clock frequency of 9.71 kHz. The PIC attenuated pulses to single photon level and randomly prepared the four polarization states. A wavelength division multiplexer (WDM) and a bandpass filter (BPF) were added at the output of the PIC to filter out the weak broadband electroluminesence peak near a wavelength of 1150 nm from the forward biased Si PIN diodes [198]. The WDM and BPF added a loss of 5 dB and can be replaced by an integrated on-chip filter in future designs.

The signals were transmitted over a 5 km long spool of standard single mode fiber. At the receiver (Bob’s) side, a tunable beam splitter (TBS) balanced the losses of two paths so that each basis has a 50% probability to be chosen for the measurement. The PC preceding each PBS was tuned for the measurement of two conjugated bases in the two paths, and the photons were detected using InGaAs SPADs. The detection efficiency of the SPADs was 20% and the dead time was set to 15 µs. The SPAD would output an electrical pulse to the TIA every time it detected a photon, so that the arrival time of every photon could be recorded by the TIA. The four channels at Bob’s end were measured sequentially, rather than simultaneously, to maintain an identical detection efficiency. The loss of the link, which includes the fiber and Bob’s equipment, was about 6.1 dB. The TIA was synchronized with the clock to perform time-correlated single photon counting (TCSPC).

5.1.2 System Synchronization

A synchronization clock was provided by a two-channel AFG outputting signals in burst mode, as shown in Fig. 5.2. The two channels shared a common internal trigger with a period of 103 µs. One channel output 1000 voltage pulses at a repetition rate of 10 MHz on every trigger, and the voltage pulse train triggered the driver of the LiNbO$_3$ modulator. The other channel of the AFG output one pulse on every trigger, synchronizing the TIA to perform TCSPC. The clock AFG also provided a synchronization
signal, which triggered the AFGs that drove the on-chip microring modulator (if used for decoy states) and polarization modulator. A 1000-bit long random pattern was repeated on every external trigger, corresponding to random decoy states (if used) and polarization states modulation respectively.

The whole system is now well synchronized. Every clock cycle, the transmitter output a burst of 1000 optical pulses at a repetition rate of 10 MHz. The pulses were a 1000-bit long random pattern with polarization states.

### 5.2 Numerical Analysis

The optimal performance expected for the system is analyzed using the method in [15, 16, 177, 199]. System parameters are summarized in Table 5.1.

![Figure 5.2: Output of the central AFG clock. (a) The internal trigger of the AFG with a period of 103 µs. (b) Output of the AFG’s first channel. Pulse generator driving the LiNbO₃ modulator is triggered by this channel. (c) Output of the AFG’s second channel. The TIA and AFGs driving the on-chip ring modulator (for intensity modulation, if needed) and polarization modulator are trigger by this channel.](image-url)

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Definition</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>$t_{AB}$</td>
<td>channel transmittance</td>
<td>6.1 dB</td>
</tr>
<tr>
<td>$\eta_D$</td>
<td>SPAD’s detection efficiency</td>
<td>0.2</td>
</tr>
<tr>
<td>$g$</td>
<td>detection window</td>
<td>5 ns</td>
</tr>
<tr>
<td>$f$</td>
<td>transmission rate</td>
<td>10 MHz</td>
</tr>
<tr>
<td>$D$</td>
<td>dark count rate</td>
<td>2000 Hz</td>
</tr>
<tr>
<td>$\tau$</td>
<td>SPAD’s dead time</td>
<td>15 µs</td>
</tr>
<tr>
<td>$N_\nu$</td>
<td>number of pulses used as decoy states</td>
<td>281 Mbits</td>
</tr>
</tbody>
</table>
5.2.1 BB84 Decoy States without Decoy States

The idealized gain for a perfect single photon source [16] is

\[ \eta = t_{AB}\eta_D, \]  

where \( t_{AB} \) is the channel transmission, which also takes into consideration the internal transmission at Bob’s end. \( \eta_D \) is the SPAD’s detection efficiency. Unfortunately, the dark counts and dead time of the SPAD will degrade the efficiency. The detector model can be described as follows [199]. Assume the SPAD has a dead time of \( \tau \). After the detection of a photon, the bias voltage across the PN junction would take \( \tau \) to climb back above the breakdown voltage, before which the detector is completely paralyzed and the detection efficiency is zero. Also note that photons that strike the detector before its full recovery would not extend its dead time. Now we can calculate the possibility that optical pulses with a mean photon number of \( \mu \) can be detected. To get a signal electrical output from the SPD, three conditions must be satisfied:

1) The pulse survives the link loss and make it to the detector.

2) The detector is active.

3) The incident pulse is registered by the detector.

At average, the mean photon number of the optical pulses at the input of the detector, denote as \( \mu_d \), is given by

\[ \mu_d = t_{AB}\mu, \]  

The conditional probability of detecting a photon given that the detector is active is given by

\[ P_0 = \sum_{n=0}^{\infty} e^{-\mu_d} \frac{\mu_d^n}{n!} (1 - (1 - \eta_D)^n) \]
\[ = 1 - e^{-\mu_d\eta_D} \]
\[ = 1 - e^{-\mu\eta}, \]  

where \( \eta_D \) is the detection efficiency of the detector. Note that the Poisson distribution of photon numbers in each pulse is included. For only one SPD, assuming a detection rate of \( C \), a time of \( C\tau \) is occupied per second, which means that the probability a detector stays active when the optical pulse arrives is

\[ P_a = 1 - C\tau. \]
Therefore, we arrive at the yield of the optical detection event (the ratio between the total number of Bob’s detection events, excluding the dark counts, to the signals sent by Alice, given that they use a compatible basis)

\[ Y_n = P_0 P_a. \]  

(5.5)

Another source of Bob’s detection events is the background noise due to stray light and the detector’s dark counts, whose yield \( Y_0 \) can be seen as that of the vacuum states.

\[ Y_0 = 2D \times (g/f) \times P_a/f \]
\[ = 2D \times g \times P_a, \]

(5.6)

where \( g \) is the detection window and \( f \) is the transmission rate.

The overall gain \( Q_\mu \) (the ratio between the total number of Bob’s detection events to the signals sent by Alice, given that they use a compatible basis) can now be expressed by

\[ Q_\mu = Y_0 + Y_n. \]  

(5.7)

The overall QBER \( E_\mu \) is given by

\[ E_\mu = \frac{e_0 Y_0 + e_{opt} Y_n}{Q_\mu}, \]

(5.8)

where \( e_0 \) is the error of the background. Since the background is totally random, \( e_0 = 0.5 \). \( e_{opt} \) is the probability that a photon triggered an erroneous detector (caused by e.g. optical misalignment). In this work, the main source of \( e_{opt} \) is a finite PER of the polarization modulator.

Next, we can use the the method in [15] (Eq. 12-13) to simulate the secure key rate of the system for the BB84 protocol without decoy states. The secure key rate is adapted to be

\[ S \geq q Q_\mu \{-f(E_\mu) H_2(E_\mu) + \Omega[1 - H_2(E_\mu/\Omega)]\}, \]  

(5.9)

where \( q \) depends on the protocol (1/2 for BB84 protocol because Alice and Bob have a 50% probability to choose the compatible basis), \( f(e) \) is the error correction efficiency. \( H_2(x) \) is the binary Shannon entropy function, which is given by

\[ H_2(x) = -x \log_2 x - (1 - x) \log_2 (1 - x). \]  

(5.10)
And $\Omega$, a pessimistic estimation of the fraction of detection events by Bob that have originated from single-photon signals emitted by Alice, is given by

$$1 - \Omega = P_{\text{multi}}/Q_{\mu}.$$

(5.11)

where $P_{\text{multi}}$ is the probability of Alice emitting a multi-photon signal.

### 5.2.2 BB84 Decoy States with One Decoy State

The secure key rate of the system for BB84 protocol with only one decoy state can be given by [177]

$$R \geq q\{-Q_{\mu}f(E_{\mu})H_{2}(E_{\mu}) + Q_{1}^{L}[1 - H_{2}(e_{1}^{U})]\},$$

(5.12)

where $Q_{1}^{L}$ is the lower bound of the gain for single photon states $Q_{1}$ and $e_{1}^{U}$ is the higher bound of the error rate for single photon states $e_{1}$.

$$Q_{1} \geq Q_{1}^{L} = \frac{\mu^{2}e^{-\mu}}{\mu\nu - \nu^{2}}(Q_{\nu}^{L}e^{\nu} - Q_{\mu}e^{\mu}\mu - E_{\mu}Q_{\nu}e^{\mu}\frac{\mu^{2} - \nu^{2}}{e\nu^{2}}),$$

(5.13)

$$e_{1} \leq e_{1}^{U} = E_{\mu}Q_{\mu}/Q_{1}^{L},$$

(5.14)

in which $Q_{\nu}^{L}$ is the lower bound of the gain $Q_{\nu}$ for the decoy state.

$$Q_{\nu}^{L} = Q_{\nu}(1 - u_{\alpha}/\sqrt{N_{\nu}Q_{\nu}}),$$

(5.15)

where $N_{\nu}$ is the number of pulses used as decoy states.

### 5.2.3 Simulation Results

The simulation results are shown in Fig. 5.3, where the secure key rate is plotted as a function of mean photon numbers of the signal state (for the case without decoy states) and decoy state (for the case with one decoy state). For the latter, the mean photon number for the signal state is set to be 0.5. The system is analyzed using different types of detectors (SPAD and SNSPD), transmission speed (10 MHz and 1 GHz) and optical error rate $e_{\text{opt}}$ (0.01, 0.001 corresponding to a PER of 20 dB and 30dB), in an effort to find the limiting factors to the secure key rate. The parameters of the SNSPD is based on ID280 Superconducting nanowires from ID Quantique, which has a detection efficiency is 0.5 (minimum), a
dead time of 67 ns (maximum) and a dark count rate of 100 Hz (maximum).

The results show that, for the BB84 protocol without decoy states and using the current SPAD, the optimal secure key rate can reach 3 to 4 kbps using a mean photon number of $\sim 0.035$. Increasing the polarization extinction ratio or transmission rate would not substantially increase the key rate. Instead, the key rate is largely limited by the detector’s performance. That is, using a detector with a high detection efficiency, short dead time and low dark count, the secure key rate can be greatly improved. With such a detector, increasing the transmission rate would make a significant difference. For both detectors, using one decoy state can double the secure key rate or more.

![Graphs showing simulation results of secure key rate.](image)

Figure 5.3: Simulation results of secure key rate. (a) Secure key rate without using decoy states. The detector is SPAD. (b) Secure key rate without using decoy states. The detector is SNSPD. (c) Secure key rate using only one decoy state. The detector is SPAD. (d) Secure key rate using only one decoy state. The detector is SNSPD.
5.3 Experimental Results

In the experimental demonstration, the on-chip VOA provided an attenuation of 27 dB. 562 Mbits (effective) were emitted for each channel test. The measured gains for \{|H\rangle, |V\rangle, |D\rangle, |A\rangle\} polarizations were \{7.92 \times 10^{-4}, 1.02 \times 10^{-3}, 1.76 \times 10^{-3}, 1.68 \times 10^{-3}\}, respectively. The diagonal basis has a higher gain because of a 2.7 dB difference in the connector loss in Bob’s end in the experimental setup. The slight PDL would also contribute to the differences in the QBER and gain. The photon fluxes for the four polarization states had a circa 1 dB variation, after accounting for the differences in the connector loss, in agreement with the classical results. The mean photon number per pulse is estimated to be 0.024 and QBER 5.4%. The raw rate was 13.2 kbps and the asymptotic secure key rate was about 0.95 kbps, which was estimated using Eq. 5.9. Imperfections such as laser power fluctuations and optical misalignment were ignored in our analysis [200]. These results show the feasibility of foundry Si photonics for practical QKD. The QBER can be reduced by the employment of system stability control and a detector with fewer dark counts. The key rate would be improved with faster detectors and higher transmission rate, as the simulation results have suggested.
Chapter 6

Summary and Outlook

6.1 Summary

In summary, we have demonstrated the first Si transmitter PIC for polarization-encoded QKD fabricated in a Si foundry platform. The Si photonic platform is able to provide high performance components for QKD: 1) Low-loss waveguides; 2) Ring modulators with a high dynamic ER of 20 dB and capability of generating ns pulses; 3) VOA with a high attenuation capability of > 160 dB; 4) Polarization modulator with a high PER of > 30 dB and a low PDL of 0.9 dB across the four states used in the BB84 protocol. The proof-of-concept QKD demonstration shows a QBER of 5.4% and an asymptotic secure key rate of 0.95 kbps.

The performance of the chip is largely limited by the detector, as is shown in the simulation results. With a higher modulation speed and faster SPDs, the transmitter PIC has the potential to achieve a few Mbps at a transmission rate of 10 MHz. The chip is also compatible with other polarization-encoded protocols such as BB92. And with a different configuration, other protocols such as DFS and COW can also be implemented in the Si integrated platform. This work shows the potential of using foundry Si photonics for low cost, wafer-scale manufactured components for optical quantum information.

Improvements can be made to elevate the performance of the chip, which include:

1) **Polarization modulator.** For the polarization modulator, the PDL at the chip output can be compensated by adding tunable attenuators at the inputs of the PRC to allow for fine balancing of the loss between the TE and TM components. The PER can be increased by including PIN diode phase-shifters at the inputs of PRC for the dynamic compensation of the phase mismatch between the two polarization components.
2) **Ring modulators.** Since microring structures are extremely sensitive to the ambient perturbations and thermal crosstalk, the two ring modulators could be combined into one to reduce the integration complexity and increase the operation stability. One ring modulator would still be able to generate multiple intensities of pulse trains. And a faster ring modulator is also needed for short pulses, GHz transmission rate and a higher secure key rate.

3) **More integration.** On the transmitter, an on-chip filter should be added to filter out the broadband spontaneous emission of Si PIN diodes and a phase shifter can be used to randomize the phase of laser pulses. A low-loss integrated receiver with a tunable beam splitter and polarization management components would improve the stability of system. The adoption of the multi-layer Si$_3$N$_4$-on-Si platform [45, 46] at Bob’s end would substantially increase the internal transmission of Bob’s system, thus obtain a higher key generation rate. An on-chip SPD will further increase the detection efficiency and remove the instability due to chip-to-fiber coupling.

4) **System stabilization.** The system can be made more stable by temperature control, active polarization compensation and on-chip power monitoring by on-chip Ge photodetectors. For example, a power variation of $< 1\%$ out of the microring requires a precise temperature control within $\sim 1.5 \times 10^{-3}$ K. An integrated hybrid laser on SOI platform would further reduce the laser power variation during the process.

### 6.2 Outlook

In the recent decade, both of quantum information technologies and integrated photonics have achieved rapid improvements, with the most notable examples of QKD and Si photonics. Now, the maturing of both fields has laid a solid foundation for their recent marriage, which takes advantage of both regimes. Quantum information technologies require the detection, generation and manipulation of the quantum states of light, which is apparently more challenging than the classical applications. QKD, its most mature application, is now at the point of bridging theory and practice. The practical implementation of QKD will largely rely on the current classical communication networks, which requires the compatibility of QKD components and standard building blocks. Therefore, an integrated photonic platform would be crucial.

Researchers have been using multiple integrated photonic platforms for quantum photonic applications, such as silica-on-silicon [21–25], laser written waveguides [26, 27], photonic crystal [28, 29], diamond [30], GaAs [31], InP [32], SiON [32, 33]. These platforms would still be competing with Si
Chapter 6. **Summary and Outlook**

Photonics [34–37] for quantum photonic applications in the coming years. In the long run, Si photonics, due to the compatibility with CMOS technology and its strong optical confinement, would have the advantage of low cost, low power consumption, high yield and high scalability for large-scale quantum photonic devices. A lot of challenges, though, have to be addressed before the full deployment of Si photonics as the platform for quantum technologies. There are components missing from standard Si platforms, such as on-chip true single photon sources, isolators and SPDs. Optoelectronic integration and packaging are still difficult and expensive. And circuit-level design tools are yet developed.

Despite these limitations, the Si quantum photonic community has made impressive progresses. A device library for quantum photonics is being built up and various basic quantum functionalities are being demonstrated. So far, single photon pair sources [193, 194] and key passive optical components are available. On-chip single photon detectors using an SNSPD flip-chiped atop a Si waveguide [201] has been demonstrated and Ge-on-Si APDs are being developed [202–204], which has the advantage of room temperature operation. High visibility single photon interference [35, 205] and quantum gates [37, 206] have been implemented using on-chip photon pair sources and simple linear optics. The research community for quantum photonics will also benefit from the availability of Si MPW shuttle run foundry services, which allows affordable costs and fast turnaround time from design to prototyping. As we have seen in this thesis work, the foundry Si photonic platform can offer high-performance components and chip-scale systems for quantum information applications. The complex functionality of polarization state manipulation further shows the feasibility of foundry Si platforms for quantum technologies. In conclusion, Si photonics is the most viable solution for complex quantum photonic systems.
Bibliography


[102] Yi Zhang, Tom Baehr-Jones, Ran Ding, Thierry Pinguet, Zhe Xuan, and Michael Hochberg. Silicon multi-project wafer platforms for optoelectronic system integration. In The 9th International Conference on Group IV Photonics (GFP), 2012.


[106] IMEC. http://www2.imec.be/content/user/File/Brochures/leaflets


