博士論文

Study on Improved implementation of a transmitter in BB84 quantum key distribution system

（ＢＢ８４量子鍵配送システムの送信機実装の改善に関する研究）

Hokkaido University
Graduate School of Information Science and Technology
Division of Electronics for Information
Research Group of Advanced Electronics
Laboratory of Optical Processing and Networking

Weiyang Zhang

Contents

Chapter 1

Introduction

Conventional cryptosystems such as ElGamal, Rabin, or RSA, are based on the computation complexity. According to the development of the novel computer science and technology, for example the quantum computer, the current encryption cannot undertake the attack from future eavesdroppers. However the quantum cryptography, a combination of information theoretical cryptography and quantum mechanics, provides a new concept for encryption. Quantum key distribution (QKD) is founded on principles of fundamental physics rather than computational assumptions. The significant feature of QKD system is that it can detect the attack in real time and drop the eavesdropped information to keep the secure key safe. Therefore, QKD system with the one-time pad (OTP) allows two parties (Alice and Bob) to share information with the information theoretically secure key, even if the eavesdropper (Eve) exists.

The first QKD protocol proposed in 1984 is called BB84 [1] after its inventors (Bennett and Brassard). It has been extensively developed in theory and implementation [2]. QKD allows two distant parties, Alice and Bob, to share secure cryptographic keys, even in the presence of an eavesdropper, Eve. The performance of QKD systems has improved in recent years. For example, ultrafast QKD systems operating with above-gigahertz clock speeds provide secure key distribution at several hundred kilobits per second over 50 km transmissions [3–6]. Moreover, systems installed on fiber networks can continuously operate for months [7-12]. Despite such remarkable achievements, QKD systems have not been widely deployed in mainstream networks.

One of the main obstacles for QKD adoption is the lack of security certifications for practical devices. Although the unconditional security of the BB84 protocol for QKD has been proved theoretically [13], the proof requires several conditions to be satisfied. Among them, the transmitter should encode the information on the photon states without introducing errors, but this premise may not be fully satisfied in practice due to device imperfections.

Most high-speed QKD systems implementing the phase-encoding BB84 protocol use modulators based on lithium niobate for phase and intensity modulation controlled by electric signals during state preparation. Although the lithium niobate modulators are

suitable for conventional optical communication systems, high-speed QKD systems can be adversely affected by imperfect modulation [14]. In fact, the state preparation flaw [15], that is, the difference between the modulated and ideal states, arises from degraded electrical signals applied to the modulators. Although signal degradation due to practical bandwidth-limited devices is common in high-speed systems, it substantially increases the error rate in QKD systems compared to conventional light-wave communication systems, given the analog nature of quantum states [16]. Moreover, discrepancy between prepared quantum states and theoretical quantum states caused by imperfection of device, especially the phase modulator which will be discussed in this article, severely decreases the key generation rate given the increased channel loss [17]. Therefore, modulation devices should be more tolerant to degraded electric signals for realizing security certified ultrafast QKD systems. Although a loss-robust protocol is recently available [18], it requires to constrain the state errors into a small range to provide high key generation rate. In this article, we propose using a dual parallel modulator (DPM) to mitigate the state preparation flaw. We show that the DPM allows to generate QKD states that are robust to inaccurate voltage signals. We quantitatively define the state preparation flaw with fidelity between conjugated-basis states to relate the corresponding density matrices. Then, we examine the mechanism of state preparation flaw in conventional modulators and introduce the proposed DPM approach. We describe the method and results of state characterization using state tomography. Then, we estimate the state preparation flaw caused by varying the supply voltage based on the results of state tomography. We also calculate the secure key generation rate and show that this rate is not affected by degraded modulation signals in the proposed approach.

Another obstacle is that QKD systems require amount of random numbers during its operation [1]. The random number generation should be reliable, economical and practical. As new generation cryptographic scheme, quantum key distribution is based on quantum mechanics. Therefore, random number generators (RNG) likewise based on nature of quantum process comes to front [19]. Unlike pseudo-RNG based on competitional algorithms, quantum random number generator (QRNG) has true randomness obtained via quantum process involving inherent randomness. QRNG is divided into three types, trusted device QRNG, self-testing QRNG, semi-self-testing QRNG. Among three types, the trusted device QRNG, also called practical QRNG has been developed rapidly because of its convenience and low cost. With a well-designed post-process, the trusted device QRNG is information-theoretically secure and meets the security requirements of most applications.

In the trusted device QRNG, many quantum processes are used to build practical

QRNG [20-25], including photon number, vacuum fluctuation of quantum state, phase fluctuation of amplified spontaneous emission, intensity fluctuation of amplified spontaneous emission and so on. Among the above, phase noise, or phase fluctuation of amplified spontaneous emission, which is quantum mechanical by nature, is one of the major schemes adopted as random source [26,27]. Because it has high generation rate and requires relatively simple implementation setup.

Traditionally, QRNG based on phase noise requires a light source and a self-delayed interferometer. These two devices are commonly implemented in BB84 QKD systems. If we can build QRNG with equipment in QKD system, it will cut more cost and reduce the risk of information leak during random number transmission from external QRNGs. Therefore, in this study, we propose a QRNG based on a transmitter of a time-bin BB84 QKD system. It uses the laser diode (LD) in QKD system as the phase noise source and Asymmetrical Mach-Zehnder interferometers (AMZI) in QKD system as the time-delay device. In addition, a Faraday mirror, a photo detector, an analog to digital converter (ADC) and a computer are used as the measurement part. With extraction and feedback process, we can generate random number at several GHz rate in theory, and supply to the QKD system in real time. However, it is difficult to use the AMZI in a high-speed QKD system, because a long-time delay (~10ns) [25] is required in a common QRNG based on phase noise to reduce the effects of potential phase correlation between light emission from the laser. Such long-time delay could not be supplied by the interferometer in a real QKD system, because a short time delay (400-1600 ps) interferometer is necessary in high transmission speed QKD system [4,5]. We found that the phase noise randomness from the gain switched LD depends on the operating condition. We optimized the laser operating condition to maximize the phase randomness and obtained a high generation rate. We could build a QRNG system with simple implementation and obtained the high random number generation rate that matched the requirement for QKD system. We tested random numbers from our QRNG and obtained successful results [28,29]. We implemented a feedback system to improve the randomness, and optimized it by using test results to improve the tradeoff between QRNG generation rate and randomness.

In this thesis based on the our works in preparation. The outline of this thesis is as follows:

Chapter 2

In chapter 2, we review quantum communication and protocol of quantum key distribution based on different quantum characteristics. They are polarization encoding

quantum key distribution and phase encoding QKD. This introduction is aid to understand the significance and secure of quantum key distribution.

Chapter 3

In chapter 3, we analyze the influence of imperfect device on the security of QKD system and make a proposal to reduce the imperfection. We investigated the system performance of the QKD system with our proposed DPM against the modulation voltage fluctuation, which is a common effect in high speed systems due to the limited bandwidth of the practical devices.

Chapter 4

In Chapter 4, we show the modulation voltage fluctuation is overcome by using DPM and we use a control experiment and Quantum state tomography to prove that. To verify the effectiveness of the dual parallel modulator, we characterize the generated states using state tomography and estimate the key generation rate based on the Gottesman–Lo–Lütkenhaus–Preskill theory with fidelity derived from the estimated density matrices. Simulation results show that the key generation rate remains unaffected by modulation voltage shifts up to 20%.

Chapter 5

In this chapter, we introduce the significance of random numbers and 2 different random number generators including pseudo-random number generator based on competitional algorithms, quantum random number generator (QRNG) having true randomness obtained via quantum process involving inherent randomness. After that, we introduce the trusted-device QRNG which is previse research of our proposal in detail.

Chapter 6

In Chapter 6, we introduce our proposal, a QRNG sharing a light source and interferometer with a transmitter of a time-bin BB84 QKD system. When I introduce the principle of Proposed QRNG, we discuss the phase noise in a gain-switched laser in with simulation and give a definition to the gain-switching laser diode operation.

Chapter 7

In this part, we discuss our experiment on proposed QRNG, we change the gain-switching laser diode operation to maximize the randomness of the output of QRNG. Min-entropy is used to quantify randomness of raw data. We use an analog to digital converter to digitize the raw data to bit strings. The optimal Min-entropy of 7.9bits per pulse was obtained with 625MHz clock frequency, which is smaller than the ADC resolution, because signal pulse does not obey the ideal arcsine distribution under the influence of an electrical noise and the limited dynamic range of PD and ADC. Nevertheless, the theoretical generation rate is exceeded the required rate, 5 bits per pulse for a two-decoy BB84 transmitter. We implemented the extraction method (Toeplitz-hashing matrix) in PC and generated random numbers passing random number test successfully.

Chapter 8

Chapter 8 is devoted to summary, conclusions and outlook.

Chapter 2

Quantum key distribution

It is no exaggeration to say that the history of the cryptography is as long as the human history. In the accent time, the Greeks use Polybius checkerboard [30] to transform information secretly. As the development of the science, especially the invention of the telegraph, the mechanical cryptography was used in the diplomatic and military communication. Until 1949, Shannon published his epoch-marking paper, *A Mathematical Theory of Communication*, founding the information theory. Since then, the electronic cryptography came into the world. Data Encryption Standard (DES) and the RSA [31] algorithm, published in 1970s, highly influenced the advance of modern cryptography. Until now, these successful modern encryption algorithms serve us in our daily life, for example the network security and the electronic commerce security. However, the information theory shows that the modern key cryptosystem cannot be perfectly secure. Because in the modern key cryptosystem the length of the secure key is shorter than cleartext, it is broken by the eavesdropper using quantum computer in principle. The perfect secrecy can be achieved only when the key is at least as long as the plain text and is used only once. This encryption algorithm is called One-Time Pad (OTP) [32]. However, there are serious drawbacks for OTP in practical deployment. First, generation of truly random numbers (as opposed to pseudorandom numbers generated by an algorithm) is non-trivial. Second, information theoretically secure key exchange is impossible by classical communication without limitations on the ability of the eavesdroppers. In general, it is hard to ensure whether the limitations are applicable in practice. This is the biggest problem for OTP to use in practice to transfer a large-scale data at high speed. Finally, it is difficult to make sure that it continues to remain secret, and is disposed of correctly preventing any reuse in whole or part—hence "one time". Therefore, the development of the key distribution, for example the quantum key distribution, is able to popularize the OTP. Quantum key distribution (QKD) resolves the key-sharing problem and supports the OTP [33]. The combination of OTP and QKD creates a new cryptosystem called quantum cryptography, which guarantees information theoretic security that cannot be broken even by the eavesdroppers using the quantum computer.

2.1 Quantum key distribution (QKD)

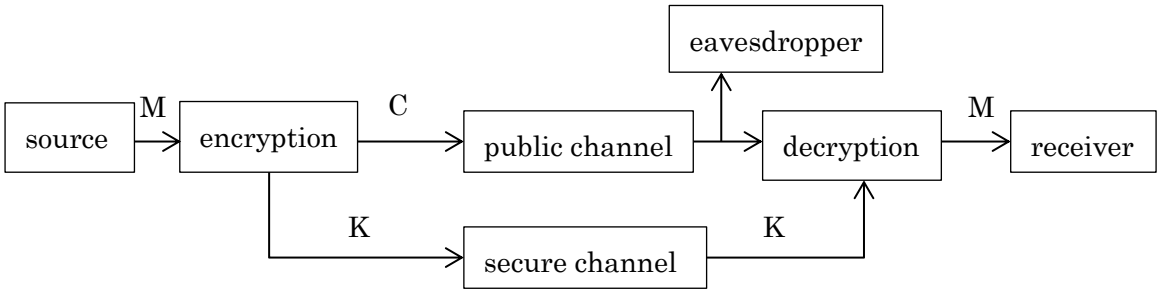


Fig. 2.1 Construction of the classic secure communication

In the 19th century, the Kerckhoffs's principle[34] was stated: A cryptosystem should be secure even if everything about the system, except the key, is public knowledge. This principle was reformulated by Claude Shannon as so called Shannon's maxim [32]. These principles imply that the security of the cryptosystem depends on the security of the key management system [33].

The key management system includes the generation, storage, distribution, usage and disposal of key. It affects not only the security but also the reliability, validity and cost of the cryptosystem. The key generation refers to generating random numbers that should be completely random and unpredictable. To this end, physical noise is often used as a seed. In modern cryptography, key is distributed from the seed with algorithm, such as Duffie-Helman (DH) [35], and RSA. However, since these algorithms are computationally secure, the improvement of computers and algorithms may break the key distributed with the current technology. Therefore, information theoretically secure key distribution is desirable to ensure the security against future decryption technology.

According to the quantum mechanics, which governs the microscopic world, Heisenberg's uncertainty principle [36] and no-cloning theorem [37] prohibit us from measuring unknown quantum states certainly and creating an perfect copy of an arbitrary unknown quantum state. This means that eavesdroppers cannot obtain useful information by hacking the quantum channel. Furthermore, they will introduce detectable errors by measurement. These two properties provide a base of the security of the quantum communication. However, it is impractical to use the quantum channel for direct message transmission, due to the loss and disturbance in the channel. Instead, we can use the quantum channel to share random numbers by combining with a classical communication channel, which is necessary to extract bit information. The shared random numbers can be used as key for data encryption. The key sharing with a quantum channel is called

quantum key distribution (QKD,) which provides information theoretically secure key. Perfectly secure communication is achieved with the key provided by QKD by encrypting information with one-time-pad protocol. In the next part, I will introduce some typical QKD systems briefly.

2.2 Security of BB84 protocol

If there is no Eve, both sift key match without errors, as shown in table 2.2. However, if Eve tries to obtain information on the key, her eavesdropping causes bit errors. Suppose she makes so called absorption-resend attack. She measures the quantum states in her randomly selected basis and resend Bob the quantum states encoding the measured bit value in her basis, as depicted in table 2.3. Eve can eavesdrop on the bits when she chooses the same basis as Alice and Bob without being detected. However, when she chooses the different basis from Alice and Bob, eavesdropping results in errors. If Alice, Bob, and Eve selects their bases with the probability of 50%-50%, the possibility that the eavesdropping is not detected is 0.75. Therefore, the possibility that Eve obtains n-bit information without being detected is 0.75^n, which can be made arbitrary small value by increasing the size of the test bits. For example, when n is set to 100 the probability is reduced to $0.75^{100} \approx 3 \times 10^{-13}$. If Eve eavesdrops on a fraction of bits sent, the resultant error rate is smaller than 0.25. Then, Alice and Bob can estimate the amount of Eve's information from the error rate. The attack is called individual, if Eve eavesdrops on one qubit at a time as described above. It is easy to prove the security of the BB84 protocol against the individual attacks.

Eve may, however, attack on whole the qubits with a quantum compute, which refers to coherent attack. For general (i.e., any eavesdropping method that quantum mechanics allows) attacks, the analysis becomes formidable to prove the security by directly calculating Eve's information. I will introduce the proof of security of BB84 QKD protocol against the general attack briefly.

In the quantum communication, errors occur not only on the bit error $0 \mapsto 1$ but also the phase $|0\rangle \mapsto -|0\rangle,\ |1\rangle \mapsto -|1\rangle$. Since errors are caused by eavesdropping, the QKD protocol is secure, if we can correct both errors and obtain the error-free qubits. However, a quantum computer is necessary to correct errors in this way. Shor-Preskill's proof [13] uses CSS codes (named after its inventors Calderbank, Shor and Steane) which have a nice property that their generators are given in the form of either X-type or Z-type. i.e., the bit-flip and phase error correction procedures are decoupled. Since we require only the bit values, which is not affected by phase error, as the output of the QKD protocols, Alice and Bob do not actually need to perform phase error correction in the protocol.

Consequently, no quantum computers are needed. What is important is that the phase error correction is not actually performed, but that it should be successful, if it were performed. We can connect the error correction and privacy amplification in BB84 protocol to the bit error correction and phase error correction with CSS code. The generation rate R of the secure final key is given by

$$R = 1 - H(\delta_b) - H(\delta_p), \tag{2-1}$$

where $H(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is Shannon entropy, δ_b and δ_p represent bit error rate and phase error rate, respectively. The term $-H(\delta_p)$ reflects the virtual phase error correction.

2.3 BB84 protocol

BB84 was proposed in 1984 and named after its inventors, Charles Bennett and Gilles Brassard. The BB84 protocol uses four quantum states to encode the key information. These states consist of two orthogonal states in one basis and two orthogonal states in the conjugate basis. This QKD protocol is based on the fact that non-orthogonal states cannot be measured without disturbing the original states. The BB84 protocol is described as follows. We here assume that the bit value {0,1} of the key is encoded in either computation basis denoted as $"+" = \{|0\rangle, |1\rangle\}$ or the conjugated basis $"\times" = \{|+\rangle, |-\rangle\}$, which are defined as $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. The quantum state is determined by the bit value and the selected basis as depicted in Table 2.1.[1]

Table 2.1 Basis

Basis/Bit	0	1
+	↑	→
×	↗	↘

Table 2.2 Process of the BB84 protocol if no Eve exists

Alice's random bits	0	0	0	1	0	1	1	1
Alice's selection of basis	+	+	×	×	+	×	+	+
State Alice sends	↑	↑	↗	↘	↑	↘	→	→
Bob's selection of measuring basis	+	+	+	×	×	+	+	×
measurement result of Bob.	0	0	1	1	1	1	1	0
Public discussion of basis	Match	Match	Un match	Match	Un match	Un match	Match	Un match
Shared secret key	0	0		1			1	

The process of BB84 protocol is as follow:

1. Quantum transmission

(1) Alice generates a random bit sequence.

(2) Alice chooses a basis randomly for each bit and prepares the quantum state.

(3) Alice sends the quantum state to Bob. Alice keeps the record on the bit value and selected basis.

(4) Bob chooses a basis randomly for each bit. Bob measures the received quantum state and obtains the bit value. Bob keeps the record of the measurement bases and obtained bit values.

2. Classical communication

I. Extract sift key

(1) Bob shows his choice of measurement basis for each bit.

(2) Alice informs Bob her choice of the basis.

Alice and Bob keeps the bits where both basis choices coincide as sift key, and discard others.

II. Error estimation

(1) Alice and Bob choose a part (*n* bits) of their sift keys as test bits randomly and estimate the error rate by comparing them through a public channel.

(2) If the error rate is smaller than a predetermined value, Alice and Bob continue the session, but otherwise they discard the session.

(3) Alice and Bob correct the errors in remaining part of the sift key and obtain error-corrected key. (4) Alice and Bob estimate the upper-bound of Eve's information. They discard an amount of the error-corrected key determined from the estimated upper-bound. This process, called privacy amplification [13], reduces Eve's information on the key to less than the required value.

If there is no Eve, both sift key match without errors, as shown in table 2.2. However, if Eve tries to obtain information on the key, her eavesdropping causes bit errors. Suppose she makes so called absorption-resend attack. She measures the quantum states in her randomly selected basis and resend Bob the quantum states encoding the measured bit value in her basis, as depicted in table 2.3.

Table 2.3 Process of protocol if Eve exists

Number	1	2	3	4	5	6	7	8	9	10
Alice's random bits	0	1	0	1	1	0	1	0	0	0
Alice's random sending basis	×	+	+	×	+	×	×	+	×	×
State Alice sends	↗	→	↑	↘	→	↗	↘	↑	↗	↗
Eve's measurement basis	+	×	+	+	×	+	×	×	+	×
Eve's bits	1	1	0	1	0	1	1	1	0	0
Bob's measurement basis	×	×	+	×	×	+	×	+	+	×
Bob's bits	0	1	0	1	0	1	1	1	0	0
Public discussion of basis	M	U	M	M	U	U	M	M	U	M
Sift key	0		0	1			1	0		0

Eve can eavesdrop on the bits when she chooses the same basis as Alice and Bob without being detected. However, when she chooses the different basis from Alice and Bob, eavesdropping results in errors. If Alice, Bob, and Eve select their bases with the probability of 50%-50%, the possibility that the eavesdropping is not detected is 0.75. Therefore, the possibility that Eve obtains *n*-bit information without being detected is 0.75^n, which can be made arbitrary small value by increasing the size of the test bits. For example, when *n* is set to 100 the probability is reduced to $0.75^{100} \approx 3 \times 10^{-13}$. If Eve eavesdrops on a fraction of bits sent, the resultant error rate is smaller than 0.25. Then, Alice and Bob can estimate the amount of Eve's information from the error rate. For general (i.e., any eavesdropping method that quantum mechanics allows,) it is possible to bind the Eve's information, any BB84 protocol is proven to be secure against general attack.

2.3.1 Polarization encoding BB84 protocol

As a concrete example of implementing the BB84 protocol, we describe polarization encoding. In the polarization encoding, we use the polarization of a photon as a quantum state: the linear polarization at +45°$|\mathrm{D}\rangle$, the linear polarization at -45°$|\overline{\mathrm{D}}\rangle$, the horizontal polarization $|\mathrm{H}\rangle$ and the vertical polarization $|\mathrm{V}\rangle$. The linear polarization state at +45° and the linear polarization state at -45° define an orthonormal basis, and the horizontal polarization state and the vertical polarization state define another orthonormal basis [1].

$$\langle \mathrm{H}|\mathrm{V}\rangle = 0 \tag{2-2}$$

$$\langle \mathrm{D}|\overline{\mathrm{D}}\rangle = 0 \tag{2-3}$$

The relationship between $|\mathrm{D}\rangle, |\overline{\mathrm{D}}\rangle, |\mathrm{H}\rangle$ and $|\mathrm{V}\rangle$ is shown as

$$|\mathrm{D}\rangle = \frac{1}{\sqrt{2}}(|\mathrm{H}\rangle + |\mathrm{V}\rangle) \tag{2-4}$$

$$|\overline{\mathrm{D}}\rangle = \frac{1}{\sqrt{2}}(|\mathrm{H}\rangle - |\mathrm{V}\rangle) \tag{2-5}$$

We encode the bit value "0" to either $|H\rangle$ or $|D\rangle$, and "1" to either $|V\rangle$ or $|\overline{D}\rangle$, respectively, as shown in table 2.4, which corresponds to table 2.1.

Table 2.4 Basis

Basis/Bit	0	1
+	H	V
×	D	$\overline{\mathrm{D}}$

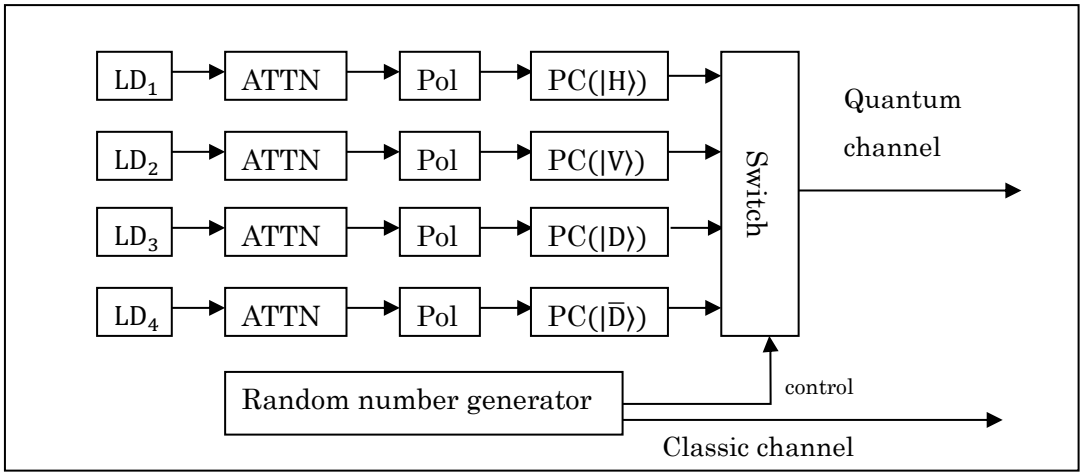


Fig. 2.3 Schematic structure of a transmitter for the polarization encoding BB84 protocol. LD represents a laser diode, ATTN: an attenuator, Pol: a polarizer, and PC: a polarization controller [14]

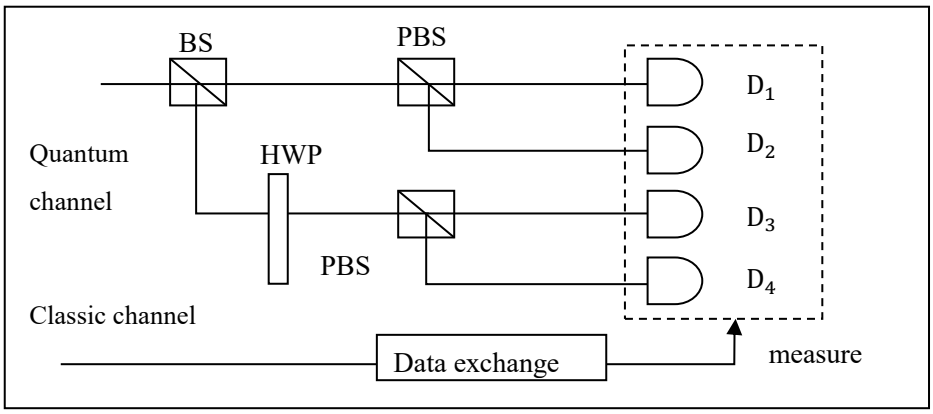


Fig. 2.4 Schematic construction for polarization encoding BB84 protocol. BS represents a beam splitter, PBS a polarization beam splitter, HWP a half-wave plate, and D a detector [14],

A transmitter for polarization encoding BB84 protocol is constructed as shown in Fig.2.3. In the transmitter, the states, $|D\rangle, |\bar{D}\rangle, |H\rangle$ and $|V\rangle$, are prepared with a photon from the laser diode (LD,) the attenuator, the polarizer and the polarization controller. A two-bit random number determines the bit value and the basis of a photon pulse with an optical switch by choosing one of four quantum states. The selected quantum state is sent to Bob through a quantum channel. Selection of the basis is sent after the quantum communication has completed through a public channel.

In the receiving end in polarization encoding BB84 protocol, quantum states are

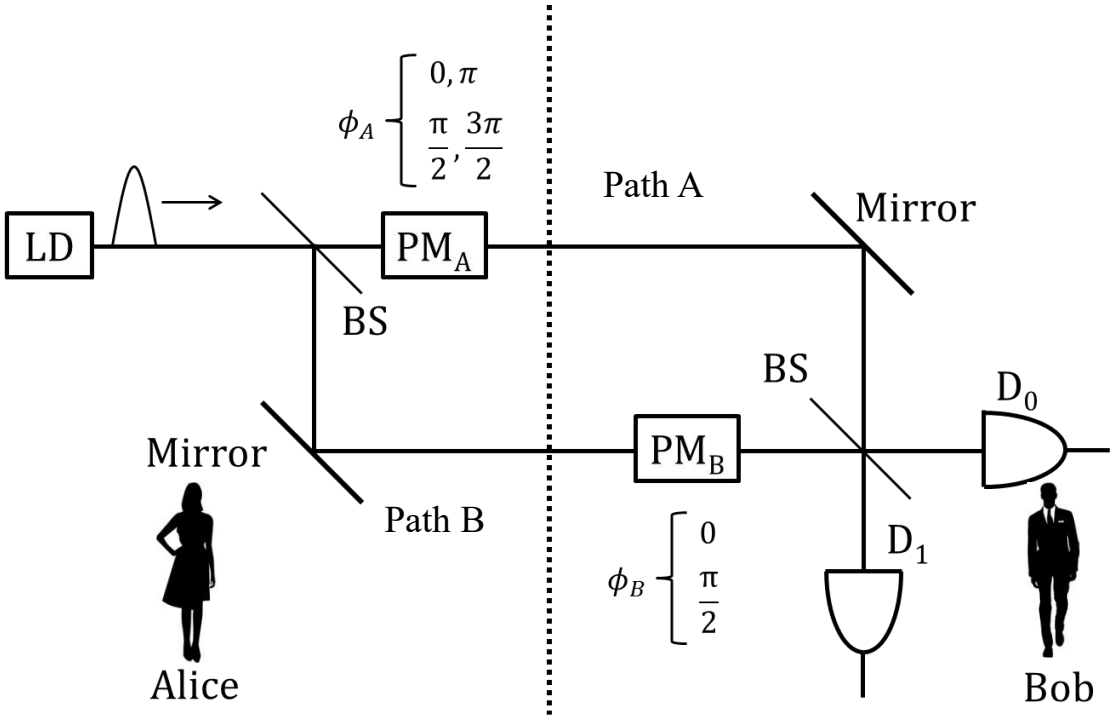


Fig. 2.5 Schematic implementation of phase encoding BB84 protocol. LD is the laser diode, D represents the detector, BS is the beam splitter, PM is the phase modulator

measured randomly through a set of the polarization beam splitters and the beam splitter. They compare the measurement results through the classic channel to generate a secret key.

2.3.2 Phase encoding BB84 protocol [38]

In the polarization coding, the implementation is straight forward and easy to understand, as shown in sec. 2.3.1. However, it has a severe drawback when applied to practical optical fiber transmission. It is hard to maintain the polarization in a long-haul transmission using optical fiber, because stress and deformation in the fiber changes the polarization state during the transmission.

To circumvent the needs of precise polarization control, phase coding is often used for optical fiber transmission. The phase encoding BB84 protocol uses four values of phase difference in qubits. As shown in Fig.2.4, a path qubit is defined in a Mach-Zehnder interferometer, where the pulse from LD is divided into two branches by a BS. The photon amplitudes in the branches A and B define the computational basis states $|0\rangle$ and $|1\rangle$,

respectively. A phase modulator (PM_A) in the branch A, which changes the phase of the $|0\rangle$ state by ϕ_A at Alice side, provides qubit state $e^{i\phi_A}|0\rangle + |1\rangle$. By setting $\phi_A = 0, \pi$, the photon state is$(|0\rangle \pm |1\rangle)/\sqrt{2}$, which is the orthonormal states in X-basis. Similarly, setting $\phi_A = \pi/2\,, 3\pi/2$ yields $(|0\rangle \pm i|1\rangle)/\sqrt{2}$, the orthonormal basis states in Y-basis. The measurement basis is defined by the phase shift by a phase modulator PM_B by ϕ_B in branch B at Bob's side.

The phase difference between branches A and B is [39]

$$\Delta\varphi = \psi_0 + \phi_A + Kl - (\psi_0 + \phi_B + Kl) = \phi_A - \phi_B \qquad (2\text{-}6)$$

where ψ_0 is the original pulse phase, ϕ_A is the phase shift in branch A, ϕ_B is the phase shift in branch B, *K* is the propagation coefficient, and *l* is the length of each branch. The lengths of branches A and B should be exactly the same to ensure the interference between the branches. The detection probability at detector D_0 is unity at $\Delta\varphi = \phi_A - \phi_B = 0$, whereas the detection probability at detector D_1 is 0. On the contrary, the detection probability at detector D_1 is unity at $\Delta\varphi = \phi_A - \phi_B = \pi$, and the detection probability at D_0 becomes 0. When $\Delta\varphi = \phi_A - \phi_B = \frac{\pi}{2}$ or $\frac{3\pi}{2}$, both the detection probabilities at D_0 and D_1 become 1/2. Those observations show that, as in polarization coding, the bit value is obtained deterministically when the basis selections of Alice and Bob coincide, and no information is obtained when the basis selection is different. Table 2.5 shows the relationship between bit values and basis selection. Here, Alice sends the bit value "0 "by setting $\phi_A = 0\ or\ \frac{\pi}{2}$, and Alice sends "1" by setting $\phi_A = \pi\ or\ \frac{3\pi}{2}$, respectively. Bob chooses the measurement basis by setting $\phi_B = 0$ or $\frac{\pi}{2}$ randomly. In table 2.5, ? means the detection events where the basis choices by Alice and Bob are unmatched.

Table 2.5 the relationship between bit values and basis selection in Phase encoding BB84 protocol

Sending bit	ϕ_A	ϕ_B	$\Delta\varphi$	D_0	D_1	Receiving bit
0	0	0	0	1	0	0
0	0	$\frac{\pi}{2}$	$\frac{\pi}{2}$	?	?	
0	$\frac{\pi}{2}$	0	$\frac{\pi}{2}$	?	?	
0	$\frac{\pi}{2}$	$\frac{\pi}{2}$	0	1	0	0
1	π	0	π	0	1	1
1	π	$\frac{\pi}{2}$	$\frac{\pi}{2}$	?	?	
1	$\frac{3\pi}{2}$	0	$\frac{3\pi}{2}$	?	?	
1	$\frac{3\pi}{2}$	$\frac{\pi}{2}$	π	0	1	1

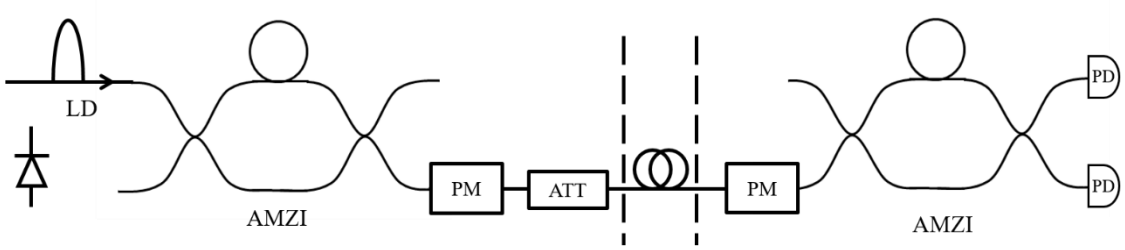


Fig. 2.6 Schematic implementation of phase encoding BB84 protocol using AMZI. LD is the laser diode, BS is the beam splitter, PM is the phase modulator, LD is the laser diode, ATT is attenuator, PD represents the photon detector

In the practice experiment, we use an asymmetric Mach-Zehnder interferometer in the phase encoding BB84 protocol [40]. A single-pulse is emitted from LD and passes through a asymmetric Mach-Zehnder interferometer with the adjustable length difference τ between two paths to generate a time-bin qubit. If the photon takes the short path, it is said to be in the state $|0\rangle$; if it takes the long path, it is said to be in the state $|1\rangle$. If the

photon has a non-zero probability to take either path, then it is in a coherent superposition of the two states:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad (2\text{-}7)$$
$$|\alpha|^2 + |\beta|^2 = 1$$

The time-bin qubit is phase modulated in Alice's station to

$$|\psi\rangle = \frac{|0\rangle + e^{i\theta_A}|1\rangle}{\sqrt{2}} \qquad (2\text{-}8)$$

where θ_A is phase modulation in Alice's station. We encode the bit value "0" to either $\theta_A = 0$ or $\theta_A = \frac{\pi}{2}$, and "1" to either $\theta_A = \pi$ or $\theta_A = \frac{3\pi}{2}$, respectively, as shown in table 2.6, which corresponds to table 2.1. Bob has an asymmetric Mach-Zehnder interferometer with the same length difference τ between two paths and chooses the measurement basis by setting $\phi_B = 0$ or $\frac{\pi}{2}$ randomly as measurement bases. The measurement results responding to bits 0 and 1 respectively are the consequence of destructive interference and constructive interference detected by two photon detectors connecting to the output of AMZI. Because of its convenience in practice, in the following thesis I will use the phase encoding BB84 protocol to introduce my work.

Table 2.6 Basis and bits in Alice's station

	$\|\psi\rangle$	θ_A
$X0$	$\frac{\|0\rangle + \|1\rangle}{\sqrt{2}}$	$\theta_A = 0$
$X1$	$\frac{\|0\rangle - \|1\rangle}{\sqrt{2}}$	$\theta_A = \pi$
$Y0$	$\frac{\|0\rangle + i\|1\rangle}{\sqrt{2}}$	$\theta_A = \frac{\pi}{2}$
$Y1$	$\frac{\|0\rangle - i\|1\rangle}{\sqrt{2}}$	$\theta_A = \frac{3\pi}{2}$

Table 2.7 Basis and bits in Bob's station

θ_A \ θ_B	0(X)	$\frac{\pi}{2}$(Y)
0(X0)	0	-
π(X1)	1	-
$\frac{\pi}{2}$(Y0)	-	0
$\frac{3\pi}{2}$(Y1)	-	1

Chapter 3

The state generation in Phase-encoding BB84 QKD system and State preparation flaw

Imperfect device such as imperfect single-photon sources, lossy channels, imperfect single-photon detection efficiency and detectors' dark counts will cause lots of flaws to practical BB84 QKD protocol [41]. As shown in the chapter 2, in the BB84 phase encoding protocol, the bases of the generating states is determined by the phase difference between two time-bin pulses. Therefore, the phase modulator is used to modulate the phase of the pulse. It is necessary to analysis potential flaw during phase modulation. In this chapter, I will introduce the state preparation flaw in detail, firstly, I will define the state preparation flaw. Secondly, I will show the relationship between the state preparation flaw and the quantum key generation rate. Then, I will introduce the principle of the phase modulator. I will introduce the conventional dual-drive modulator (DDM) and how it generates the states. We propose the dual-parallel modulator in place of the DDM as the phase modulator. Finally, I will show one of the state preparation flaws is caused by the fluctuation of the signal voltage to the modulator in the BB84 phase encoding. We compare results of two phase modulators against the fluctuation of the signal voltage, and show you the robust of our proposal theoretically.

3.1 Definition of the state preparation flaw

Most security analysis on QKD assume that the photon state emitted from Alice is perfect. For BB84 protocol, the states are defined as $(|0\rangle \pm |1\rangle)/\sqrt{2}$ in X-basis and $(|0\rangle \pm i|1\rangle)/\sqrt{2}$ in Y-basis. Since bit values are selected randomly with the probability of 1/2, the states are described as $\rho_X = \rho_Y = \boldsymbol{I}/2$, where ρ_X and $\rho_{Y,}$ denote the density operator in X-basis and Y-basis, respectively. The assumption that X-basis states and Y-basis states are equal to the half of the identity operator $\boldsymbol{I}$ in two-dimensional Hilbert space implies that no information can be extracted without basis information. It is essential for the security. If these are distinguishable, Eve may improve her measurement to obtain the key information without causing errors. State preparation flaw refers to the imperfection of the photon states prepared by Alice, which increases the distinguishability between the X-basis states and the Y-basis states. Suppose the absorption-and-resend attack. If Alice and Bob select their bases with the probability of 50%-50%, and we assume the probability that Eve select the same basis becomes 80%. The possibility that the eavesdropping is not detected is 0.9, which is much greater than the 0.75 when state generation is perfect.

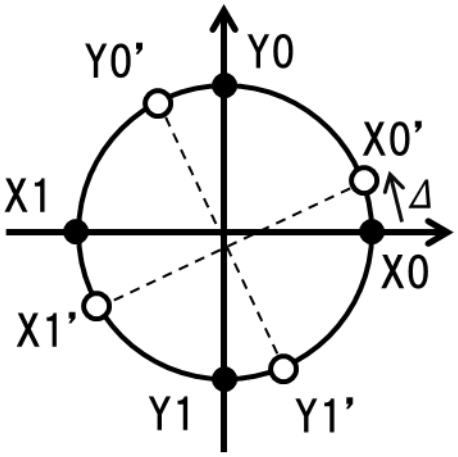


Fig 3.1 cross-section view of X-Y bases

As shown in Fig 3.1, the state preparation flaw Δ is an error from the intended states in BB84 protocol leading to the imperfect non-orthogonal states. The state preparation flaw Δ can be quantitatively defined with the fidelity $F(\rho_X, \rho_Y)$ [42] between the X-basis state ρ_X and Y-basis state ρ_Y as

$$\Delta = \frac{1 - F(\rho_X, \rho_Y)}{2} \tag{3-1}$$

where the fidelity in quantum information theory is a measure of the "closeness" of two quantum states. The fidelity is calculated with

$$F(\rho_X, \rho_Y) = \mathrm{tr}\left(\sqrt{\left(\sqrt{\rho_X}\sqrt{\rho_Y}\right)^{\dagger}\sqrt{\rho_X}\sqrt{\rho_Y}}\right) \tag{3-2}$$

using the density operators

$$\rho_X = \frac{1}{2}(|\mathrm{X0'}\rangle\langle\mathrm{X0'}| + |\mathrm{X1'}\rangle\langle\mathrm{X1'}|) \tag{3-3}$$

$$\rho_Y = \frac{1}{2}(|\mathrm{Y0'}\rangle\langle\mathrm{Y0'}| + |\mathrm{Y1'}\rangle\langle\mathrm{Y1'}|) \tag{3-4}$$

3.2 Relationship between State preparation flaw and Quantum key generation rate

As discussed in section 2.2, the bit-flip error rate δ and phase error rate δ_P determine the final key generation rate R as

$$R = 1 - H(\delta) - H(\delta_P). \tag{3-5}$$

If we assume that the final key is generated from the sift key obtained from the photons encoded in X-basis, we set the bit-flip error rate $\delta = \delta_X$ and the phase error rate $\delta_P = \delta_Y$, where δ_X and δ_Y denotes the bit error rate on X-basis and Y-basis, respectively. The final key rate is given by

$$R = 1 - H(\delta_X) - H(\delta_Y). \tag{3-6}$$

When an imperfection happens in the state generation, it is easier for Eve to distinguish between two bases. Therefore, the amount of Eve's information is larger than that estimated by Alice and Bob from the observed error rate δ_Y. The effects of the state preparation flaw can be treated by increasing the phase error rate [43] as

$$\delta'_{\mathrm{Y}} = \delta_{\mathrm{Y}} + 4\Delta + 4\sqrt{\Delta\delta_{\mathrm{Y}}} \tag{3-7}$$

where Δ' is defined with transmittance η as,

$$\Delta' = \frac{\Delta}{\eta}, \qquad \eta = e^{-\alpha l} \tag{3-8}$$

The transmittance is determined by the absorption coefficient α in the channel and the

path length l. Here the formula means the loss in the path increases the influence of the state preparation flaw Δ on the phase error rate, because Eve can select the pulses that are the most advantageous to her. The final key generation rate given with the decoy state method [44–46] influenced by the state preparation flaw Δ is:

$$R \geq q\left[Q_1\left(1-H(\delta'_{\mathrm{Y}})\right)-Q_{\mathrm{s}} fH(\delta_{\mathrm{X}})\right] \tag{3-9}$$

where δ_{X} is the bit-flip error rate, whereas Q_1 and Q_{s} represent the gains of the single-photon states sent by Alice in the received pulses and the signal states, respectively. We here assume key distillation from X-basis pulses and phase error estimation using Y-basis pulses. A constant q is given by the selection ratio of the X basis [2]. The key generation rate relates to the bit and phase error rates through Shannon binary entropies $H(\delta_{\mathrm{X}})$ and $H(\delta'_{\mathrm{Y}})$ in the signal pulses. Parameter f represents the efficiency of error correction. Obviously, the key generation rate is reduced due to the state preparation flaw. Therefore, our investigation aims to decrease the state preparation flaw and enhance the quantum key generation rate should examine the imperfection in practical BB84 QKD protocol, as presented in the following chapters.

3.3 Principle of the phase modulator

The principle of the phase modulation is based on the electro-optic effect, where the refractive index of the material is changed by the electric field supplied when the light passes the material. The change in the refractive index of the electro-optic crystal is due to the electric polarization caused by the supplied electric field. Here we assume that the velocities of light in vacuum and in the crystal are c and v, the magnetic permeability and dielectric constant of the crystal are μ and ϵ, the magnetic permeability and dielectric constant in vacuum are μ_0 and ϵ_0, respectively. Then, refractive index n is given by

$$n = \frac{c}{v} = \sqrt{\frac{\epsilon\mu}{\epsilon_0\mu_0}} \tag{3-10}$$

The electro-optic effect changes the refractive index by the change of the dielectric constant with the electric field. When the modification of the refractive by an electric field is in proportion to the field strength, it is called the linear electro-optic effect (also called the Pockels effect). When the modification of the refractive index is proportional to the square of the field strength, it is called the Kerr effect (also called the quadratic electro-optic effect), which is much smaller than the Pockels effect. The Pockels effect [47] occurs only in crystals that lack inversion symmetry, such as lithium niobate ($LiNbO_3$ or

LN) [48] or gallium arsenide (GaAs), meanwhile all materials show a Kerr effect. It is general to use LN for the phase modulator in light-wave communication, because it is a ferroelectric material of low loss and high electro-optic constant. Moreover, a LN crystal is easily grown with a simple process.

Because LN is uniaxial crystal, birefringence occurs depending on the light direction. Here we assume that the optical axis of the LN crystal is *z*-axis, and light is incident on the *y*-direction. When an electric field E_Z is applied to the crystal in parallel to the *z*-axis, the refractive indices n_x and n_z for the light fields in *x*- and *z*-directions are change as

$$n_x = n_0 - \Delta n_x = n_0 - \frac{1}{2} r_{13} n_0^3 E_z \tag{3-11}$$

$$n_z = n_e - \Delta n_z = n_e - \frac{1}{2} r_{33} n_e^3 E_z, \tag{3-12}$$

where, n_0 and n_e are refractive indices for the *x*- and the *z*-directions without the electric field. r_{13} and r_{33} are electro-optics constants for the light fields in *x*- and *z*-directions with the electric field applied in the *z*-direction. When the polarization of the input light is in *z*- direction, phase ϕ of the output light is modulated by

$$\phi(V) = -\frac{2\pi}{\lambda} n_z(V) l = -\frac{2\pi l}{\lambda}\left(n_e - \frac{1}{2} r_{33} n_e^3 \frac{V}{d}\right) \tag{3-13}$$

where l is the length of the LN crystal in the *y*-direction, and d is the crystal thickness in the *z*-direction. Equation (3-13) shows that the phase shift is proportional to the applied voltage *V*. Because the electro-optics constant r_{33} is largest in LN crystal, the phase modulation can be performed most efficiently to the *z*-polarized light by applying the electric field in the *z*-direction. The polarization of the input beam often needs to be aligned with one of the optical axes of the crystal to keep the polarization state.

3.3.1 Conventional state generation method: Dual-drive modulator (DDM)

The state preparation for BB84 protocol requires phase modulation with four values. A simple phase modulation described in the previous section needs four values of applied voltage.[16] This requirement makes the drive circuit complicated. Moreover, it is hard to control the voltage precisely in high speed modulation. A dual-drive modulator (DDM) solves this problem. The DDM is based on a Mach-Zehnder (MZ) interferometer, where two electrodes attached to the branched waveguides supply two different modulation signals. as shown in Fig. 3.2. The applied voltages $V_{\phi 1}$ and $V_{\phi 2}$ to the upper electrode and the lower electrode lead the phase changes ϕ_1 and ϕ_2 to the pulses through the upper and lower waveguides, respectively. The result of phase modulation for the pulse through the DDM is

$$e^{i\theta} = \frac{e^{i\phi_1} + e^{i\phi_2}}{\sqrt{2}} \tag{3-14}$$

Therefore, we can use DDM to generate the phase difference between pulses $|0\rangle$ and $|1\rangle$, and modulate the input state $(|0\rangle + |1\rangle)/\sqrt{2}$ to the output state $\left(|0\rangle + e^{i\theta}|1\rangle\right)/\sqrt{2}$ used as the four states in the phase encoding BB84 protocol. For example, if we want to get the state X0, no phase difference is required between $|0\rangle$ and $|1\rangle$ components. Then, we set the voltages $V_{\phi_1}^{(0)}$ and $V_{\phi_2}^{(0)}$ so as to supply the phase changes $\phi_1^{(0)} = 0$ and $\phi_2^{(0)} = 0$ to the pulse $|0\rangle$, and set the voltages $V_{\phi_1}^{(1)}$ and $V_{\phi_2}^{(1)}$ so as to supply the phase change $\phi_1^{(1)} = 0$ and $\phi_2^{(1)} = 0$ to the pulse $|1\rangle$. We obtain the state

$$\frac{1}{\sqrt{2}}\left(\frac{e^{i\phi_1^{(0)}} + e^{i\phi_2^{(0)}}}{\sqrt{2}}|0\rangle + \frac{e^{i\phi_1^{(1)}} + e^{i\phi_2^{(1)}}}{\sqrt{2}}|1\rangle\right) = \frac{1+i}{\sqrt{2}}\frac{|0\rangle + |1\rangle}{\sqrt{2}}. \tag{3-15}$$

Here $(1+i)/\sqrt{2} = e^{i\pi/4}$ is a global phase and can be ignored. The state $\mathrm{X0} = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ is thus generated. Similarly, we can generate all the four states used in BB84 phase encoding protocol by changing the voltage supplied to two electrodes as Table 3.1. In summary, the electric field of input light E_i is transformed into that of output light E_o as follows:

$$E_o = \frac{1}{2}(e^{i\phi_1} + e^{i\phi_2}) = \cos\frac{\phi_1 - \phi_2}{2} e^{i\frac{\phi_1+\phi_2}{2}} E_i \tag{3-16}$$

Then the photon state is given by:

$$|\Psi\rangle = \frac{1}{\sqrt{2}} \sum_{j=0,1} \exp(i\frac{\phi_1^j + \phi_2^j}{2}) \cos\frac{\phi_1^j - \phi_2^j}{2} |j\rangle \tag{3-17}$$

The reason that we choose DDM as the phase modulator is that, firstly, only two values for each electrode are necessary to generate the four states, and secondly, the difference of the applied voltage is V□ for both electrodes, as shown in the table 3.1. These features simplify the design of the drive circuit significantly.

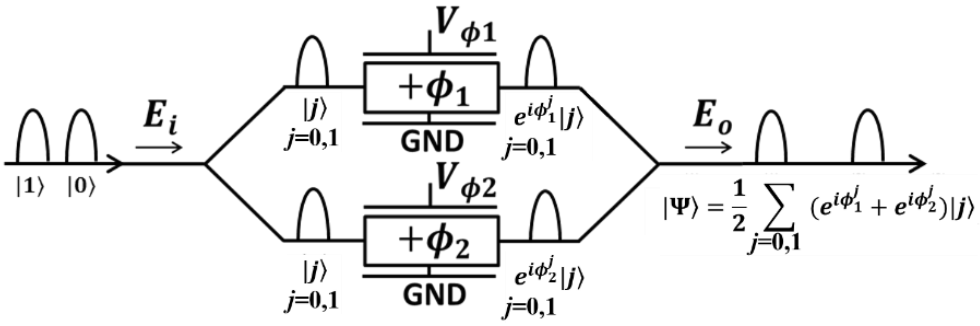


Fig. 3.2 Schematic of DDM (E_i, electric field of input light; V_ϕ, applied voltage to electrodes; ϕ, phase shift; E_o, electric field of output light). DDM is based on MZI and modulates light intensity and phase by applying phase shifts independently on upper and lower paths.

Table 3.1 Phase shifts in DDM to generate photon states X0, X1, Y0, and Y1. Variable $\boldsymbol{\phi_i^{(j)}}$ (i = 1, 2, j = 0, 1) denotes phase applied to i-th electrode for state $|\boldsymbol{j}\rangle$.

	$\phi_1^{(0)}$	$\phi_1^{(1)}$	$\phi_2^{(0)}$	$\phi_2^{(1)}$	θ	State
X0	0	0	$\frac{\pi}{2}$	$\frac{\pi}{2}$	0	$\frac{\|0\rangle + \|1\rangle}{\sqrt{2}}$
X1	0	π	$\frac{3\pi}{2}$	$\frac{\pi}{2}$	π	$\frac{\|0\rangle - \|1\rangle}{\sqrt{2}}$
Y0	0	π	$\frac{\pi}{2}$	$\frac{\pi}{2}$	$\frac{\pi}{2}$	$\frac{\|0\rangle + i\|1\rangle}{\sqrt{2}}$
Y1	π	π	$\frac{\pi}{2}$	$\frac{3\pi}{2}$	$\frac{3\pi}{2}$	$\frac{\|0\rangle - i\|1\rangle}{\sqrt{2}}$

3.3.2 Proposed state generation method: Dual-parallel modulator (DPM)

We propose the use of a dual-parallel modulator (DPM) [49] for state preparation in QKD systems. The DPM is often used as an I-Q modulator in coherent optical communication. As depicted in Fig. 3.3, DPM is constructed with two push-pull driven MZ modulators connected in parallel. In each MZ modulator, an electrode provides phase shifts to the two branches, where the phase shifts are the same amount and opposite sign. For example, in the upper interferometer, phase modulation in waveguides A and B, denoted by ϕ_{1A} and ϕ_{1B}, are described as

$$e^{i\phi_{1A}} = e^{-i\phi_1} \tag{3-18}$$

$$e^{i\phi_{1B}} = e^{i\phi_1}. \tag{3-19}$$

Therefore, the phase modulation ϕ_{1AB} of the combined pulse becomes

$$e^{i\phi_{1AB}} = e^{-i\phi_1} + e^{i\phi_1} = \cos\phi_1 \tag{3-20}$$

Similarly, the phase modulation on the lower interferometer is $\cos\phi_2$. An electrode at the output shown as block *i* in Fig. 3.3 provides a fixed phase shift of $\pi/2$. Then, the final phase modulation $e^{i\theta}$ becomes

$$e^{i\theta} = \frac{\cos\phi_1 + i\cos\phi_2}{\sqrt{2}} \tag{3-21}$$

We can use the DPM to generate the phase difference between pulses $|0\rangle$ and $|1\rangle$ to prepare the four states in the phase encoding BB84 protocol. For example, if we want to get the state X0, no phase difference is required between $|0\rangle$ and $|1\rangle$ components. Then, we set the voltages $V_{\phi_1}^{(0)}$ and $V_{\phi_2}^{(0)}$ so as to supply the phase changes $\phi_1^{(0)} = 0$ and $\phi_2^{(0)} = 0$ to the pulse $|0\rangle$, and set the voltages $V_{\phi_1}^{(1)}$ and $V_{\phi_2}^{(1)}$ so as to supply the phase change $\phi_1^{(1)} = 0$ and $\phi_2^{(1)} = 0$ to the pulse $|1\rangle$. We obtain the state X0 as

$$\frac{1}{\sqrt{2}}\left(\frac{e^{i\phi_1^{(0)}} + e^{i\phi_2^{(0)}}}{\sqrt{2}}|0\rangle + \frac{e^{i\phi_1^{(1)}} + e^{i\phi_2^{(1)}}}{\sqrt{2}}|1\rangle\right) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle). \tag{3-22}$$

Similarly, we can generate all the four states in BB84 phase encoding protocol by changing the voltages supplied to the electrodes. In summary, the electric field of the output light, E_o, is related to that of the input light, E_i, as follows:

$$E_o = \frac{\cos\phi_1 + i\cos\phi_2}{\sqrt{2}} E_i \tag{3-23}$$

Then the photon state is given by:

$$|\Psi\rangle = \frac{\sum_{j=0,1}\left(\cos {\phi_1}^{(j)} + i\cos {\phi_2}^{(j)}\right)}{\sqrt{\sum_{j=0.1}(\cos^2 {\phi_1}^{(j)} + \cos^2 {\phi_2}^{(j)})}}|j\rangle \tag{3-23}$$

Then, the four states, X0, X1, Y0, and Y1, $|\psi\rangle = [|0\rangle + \exp(i\theta)\,|1\rangle]/\sqrt{2}$ $\theta \in \{0, \pi/2, \pi, 3\pi/2\}$, can be obtained by adjusting voltages V_{ϕ_1} and V_{ϕ_2} to provide the appropriate phase shifts, ϕ_1 and ϕ_2, respectively, as shown in Table 3.2. Here global phase is ignored. The DPM is operated with two phase shifts of 0 and π on each interferometer to generate the four states, and thus only two output values of 0 and V_π are required, simplifying the driver.

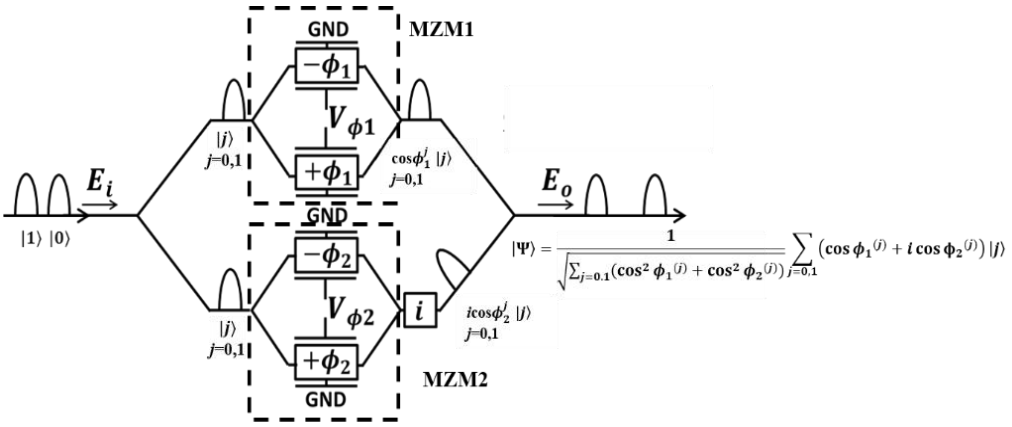


Fig. 3.3 Schematic of DPM (E_i, electric field of input light; V_ϕ, applied voltage to electrodes; ϕ, phase shift; E_o, electric field of output light; MZM, Mach–Zehnder modulator; i, $\pi/2$ phase shift). DPM is constructed with two push–pull Mach–Zehnder modulators connected in parallel.

Table 3.2 Phase shifts in DPM to generate photon states X0, X1, Y0, and Y1. Variable $\phi_i^{(j)}$ (i = 1, 2, j = 0, 1) denotes phase applied to i-th electrode for state $|j\rangle$.

	$\phi_1^{(0)}$	$\phi_1^{(1)}$	$\phi_2^{(0)}$	$\phi_2^{(1)}$	θ	State
X0	0	0	0	0	0	$\frac{\|0\rangle + \|1\rangle}{\sqrt{2}}$
X1	0	π	0	π	π	$\frac{\|0\rangle - \|1\rangle}{\sqrt{2}}$
Y0	0	π	0	0	$\frac{\pi}{2}$	$\frac{\|0\rangle + i\|1\rangle}{\sqrt{2}}$
Y1	0	0	0	π	$\frac{3\pi}{2}$	$\frac{\|0\rangle - i\|1\rangle}{\sqrt{2}}$

3.4 Voltage fluctuation applied for the phase modulators

In recent high-speed QKD systems, the clock rate of the system reaches 1 GHz, so that, the phase modulators need to be operated at this rate. However, the limited-bandwidth of the electric circuit results in the degradation of the modulation signal at such high frequency, as shown in Fig. 3.4. We observe that electric signal to the modulator varies 20% in 200 ps from time A to B as illustrated in Fig. 3.4 which is longer than the pulse duration of light (100 ps). Therefore, the phase modulation to the light pulse differs up to 20%, if the timing of light pulse fluctuates from time A to B. This inaccuracy in voltages applied for phase modulators will produce error in the phase difference resulting in the state generation flaw in BB84 protocol. Although limited-bandwidth devices have been investigated on light intensities regarding the decoy effect [16], it also affects the accuracy of state preparation. In this thesis, we consider the effects of fluctuation in the voltages applied to the phase modulator for both DDM and DPM.

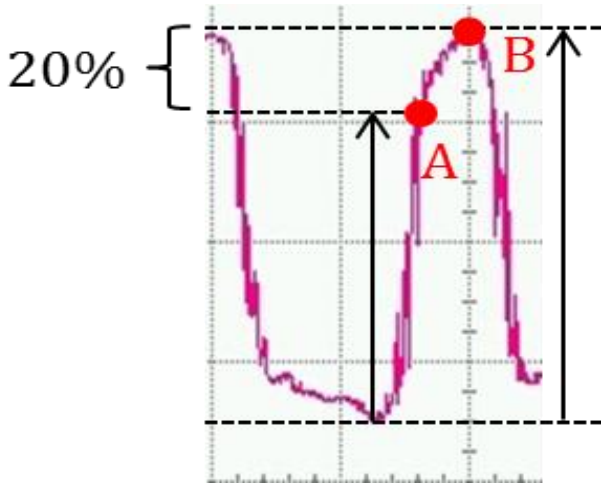


Fig. 3.4 Inaccurate square wave signals in high frequency

Firstly, we consider a voltage fluctuation V_ε occurs on V_{ϕ_2} (the electrode on the upper branch) in DDM. As the electro-optical effect is linear with the applied electric field, phase shift error ε to ϕ_2 also varies linearly according to voltage shift V_ε. Then, the coefficients in Eq. (3-16) change to

$$\exp\left(\mathrm{i}\frac{\phi_1^{(j)}+\left(\phi_2^{(j)}+\varepsilon\right)}{2}\right)\cos\frac{\phi_1^{(j)}-\left(\phi_2^{(j)}+\varepsilon\right)}{2}$$
$$=\exp\left(i\frac{\phi_1^{(j)}+\phi_2^{(j)}}{2}\right)\left[(1+i\varepsilon)\cos\frac{\phi_1^{(j)}-\phi_2^{(j)}}{2}+\varepsilon\sin\frac{\phi_1^{(j)}-\phi_2^{(j)}}{2}\right]. \tag{3-25}$$

up to the first order of ε. The phase shift error results in the change of the amplitude ratio and the relative phase. In a widely used direct phase modulator, the phase shift error causes the relative phase shift linear to ε, as the phase varies linearly on the applied voltage.

Secondly, we consider the phase modulation error in the DPM, where a voltage fluctuation V_ε occurring in V_{ϕ_2} (two opposite electrodes on the lower branch) produces an error ε. As the cosine varies proportionally to the square of the error for $\phi_2 = 0$ or □:

$$\cos(\phi_2+\varepsilon)=\cos\phi_2\left(1-\frac{1}{2!}\varepsilon^2+\frac{1}{4!}\varepsilon^4-\cdots\right). \tag{3-26}$$

Therefore, the lowest-order error during phase modulation is proportional to the square of phase shift error ε. When error ε is small enough (i.e., much lower than 1), the relative phase error by the DPM is negligible. Hence, the state preparation flaw is suppressed in the DPM much more effectively than in the DDM. In the next chapter, I will compare the state generation flaw in DDM and DPM experimentally.

Chapter 4

PM Experiment and Analysis

To experimentally prove the superiority of DPM over DDM, we need to take a comparison experiment. In this experiment, it is important that we use the DDM and DPM to modulate the phase of double pulses and keep other part of the experiment is the same. For example, both of the DDM and DPM are controlled under the same change of DC bias and the voltages of the pulse height from PPG to simulate the fluctuation in voltage supply. We will use the measurement results to analyze the output light states from the phase modulator with the quantum state tomography to obtain the density operators. Fidelity between X-basis states and Y-basis states are calculated to quantify the state generation flaw caused by the voltage fluctuation. Finally, we calculate the final key generation rate, and show the superiority of the DPM over the DDM on the resistance to the fluctuation.

4.1 Set up of the experiment

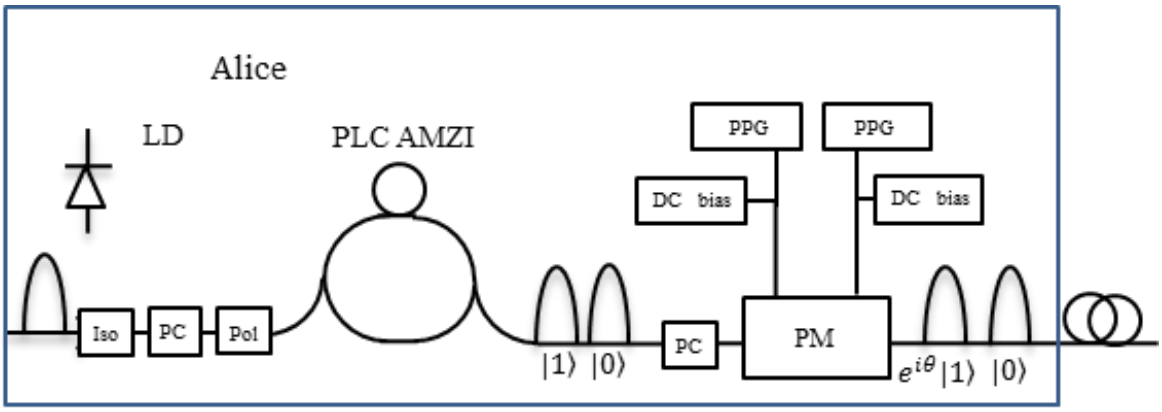


Fig. 4.1 Experimental setup for phase encoding BB84 quantum system in Alice's station

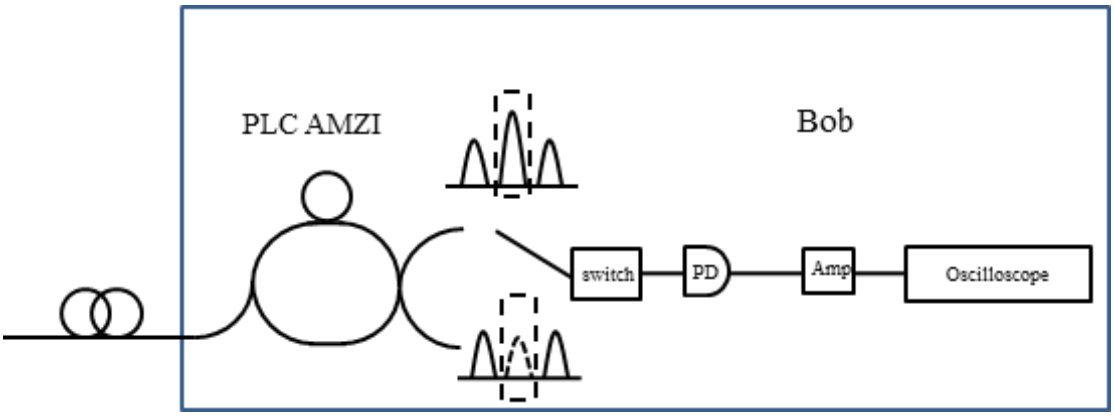


Fig. 4.2 Experimental setup for phase encoding BB84 quantum system in Bob's station

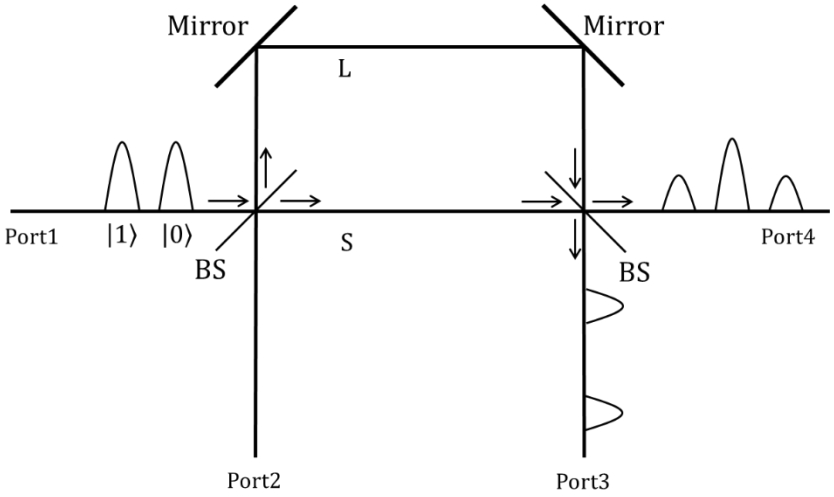


Fig. 4.3 Schematic structure of Asymmetric Mach Zehnder Interferometer (AMZI) used in our experiment

Experimental setup to investigate the effects of voltage shifts on the photon states in the phase encoding BB84 QKD system is shown in Figs. 4.1-4.3. The setup consists of the state generation part (we here call it Alice's station after the description in QKD) and the state measurement part (here Bob's station.) At Alice's station depicted in Fig. 4.1, a laser diode (LD) emits light pulses of 1550-nm wavelength, 625MHz and 100 ps duration, through the isolator, which prevents the reflected light by the connectors and the optical devices from being fed back to the laser. A polarization controller (PC) and a polarizer define the polarization of the light. The pulse is converted to a coherent double-pulse with 800 ps time delay using the planar lightwave circuit (PLC) [50] asymmetric Mach Zehnder interferometer (AMZI), the schematic structure of which is shown in Fig. 4.3. We use silica-based PLC, which refers to a planar integrated optical circuit of silica waveguides formed on a substrate of with the technique of the semiconductor process. As for the AMZI, a path difference varies with the temperature-dependent propagation constant in the silica waveguide. In other words, the path difference can be controlled precisely by the temperature control. In this experiment, the temperatures of the AMZI's are controlled with computer-controlled temperature controllers with the accuracy of 0.01 degree to set the identical path difference τ to AMZI's in Alice's station and Bob's.

The double-pulse enters into a phase modulator (PM) after another PC. We select DDM or DPM for comparison. The PM is driven by two pulse pattern generators (PPG) and DC biases. The polarization control is necessary to obtain reliable results because of polarization dependence of the PM's.

To measure the states of light, a PLC-AMZI is used at Bob's station. We select the measurement basis X or Y by changing the relative phase between the arms in AMZI with the temperature. We use a switch to choose detection port from the two output ports of the AMZI and measure the light intensity with a high-speed photodetector instead of using two photodetectors connecting to two ports. We use a single photodetector to avoid the error that may be caused from the difference between two photodetectors. The output of the AMZI contains three components, only the center of which bring the information of relative phase between $|0\rangle$ and $|1\rangle$. We select this part from the detection signal of a high-speed photo detector, and store it. We recorded the intensities of the interference signals with an oscilloscope of 6 GHz bandwidth and 20 GSa/s sampling rate. The intensity was defined as the pulse area. We also need to measure the states in Z-basis to perform the quantum state tomography. The measurement in Z-basis refers to the intensity measurement on each component of the double pulses after the PM in Alice's station. The measurements were done with unattenuated light. Therefore, the measured intensities were proportional to the expectation values, considering the attenuation as independent from the photon states. This assumption is natural, because the characteristics of passive attenuators are expected to remain unchanged during the period of double-pulse components and keep the relative phase.

4.2 Experimental method

To examine the effects of voltage fluctuation, we intentionally change the voltages applied to the phase modulator. In the present experiment, we fix the shift of the voltage. Here, we investigate two types to change the voltage: one is DC bias and the other is the pulse height from PPG to simulate the sift of the operating point of the modulator and the fluctuation of the control signals, as shown in Fig. 4.4. The difference between two types is that both pulse $|0\rangle$ and $|1\rangle$ are influenced by the change of DC bias, while there is only an impact on the pulse $|1\rangle$ for the change of the pulse height from PPG.

In our experiment, we change the voltages including the PPG and DC bias from -0.25V_π to 0.25V_π on purpose to simulate the fluctuation of the voltage. Here V_π represents the voltage that causes π phase shift at the phase modulator. Then we record the intensities of inference signals to calculate the visibility and the fidelity. We also record the intensities of double-pulses after generated in Alice's station as Z basis measurement.

Actual experiment is proceeded as follows. We set the pulse amplitude from PPG and DC bias to modulate the time-bin double-pulse to generate a nearly perfect state, and we set the measurement basis to X. We assume that the measurment bases to be perfect. The setup is controlled so as to yield the highest visibility. Then, we change the DC bias from

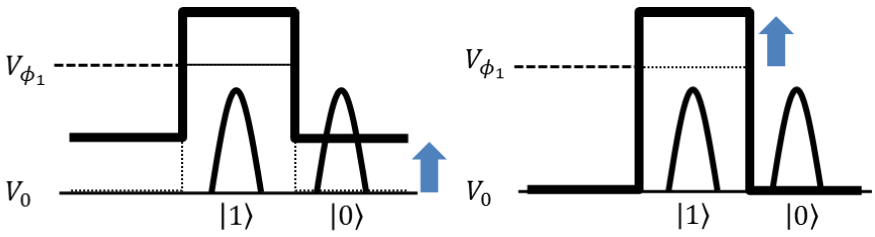


Fig. 4.4 Two type of the voltage sift to the modulator to simulate the fluctuation

-0.25V_π to 0.25V_π to simulate the shift in DC bias and record the interference signal. After completion, we change the basis to Y, and perform the same measurement. We also record the intensities of the double-pulse components as measurement in Z-basis. We continue the measurement by changing the pulse amplitude (AC) with the same procedure.

4.3 Quantum state tomography

As the definitions of the state preparation flaw and fidelity introduced in chapter 3, we need to calculate the density matrix of the states. Here, we introduce the Quantum state tomography to estimate the density matrix of states [51][52].

Since we need to determine a single qubit state, we present the density matrix as a linear expansion with Pauli matrices $\hat{\sigma}_i$'s as

$$\hat{\rho} = \frac{1}{2}\sum_{i=0}^{3}\frac{S_i}{S_0}\hat{\sigma}_i \tag{4-1}$$

where the expansion coefficients are related to the Stokes parameters, which are originally introduced to define the polarization states in Poincare sphere. They are determined from a set of four intensity measurements (1) with a filter that transmits 50% of the incident radiation, regardless of its polarization; (2) with a polarizer that transmits only horizontally polarized light; (3) with a polarizer that transmits only light polarized at 45° to the horizontal; and (4) with a polarizer that transmits only right-circularly polarized light. The intensities obtained in these four experiments are as follows:

$$n_0 = \frac{N}{2}(\langle H|\rho|H\rangle + \langle V|\rho|V\rangle)$$

$$= \frac{N}{2}(\langle R|\rho|R\rangle + \langle L|\rho|L\rangle)$$

$$n_1 = N(\langle H|\rho|H\rangle)$$
$$n_2 = N\langle \bar{D}|\rho|\bar{D}\rangle \tag{4-2}$$
$$n_3 = N\langle R|\rho|R\rangle,$$

where $|H\rangle$, $|V\rangle$, $|\bar{D}\rangle = \frac{|H\rangle - |V\rangle}{\sqrt{2}}$, and $|R\rangle = \frac{|H\rangle - i|V\rangle}{\sqrt{2}}$ represent the state polarized in the linear horizontal, linear vertical, linear diagonal (45°), and right-circular senses respectively. A two-by-two density matrix ρ describes polarization state of the light, and N is a constant depending on the detector efficiency and light intensity. The Stokes parameters, which fully characterize the polarization state of the light, are then defined by

$$\begin{aligned} S_0 &= 2n_0 = N(\langle R|\rho|R\rangle + \langle L|\rho|L\rangle) \\ S_1 &= 2(n_1 - n_0) = N(\langle R|\rho|L\rangle + \langle L|\rho|R\rangle) \\ S_2 &= 2(n_2 - n_0) = Ni(\langle R|\rho|L\rangle + \langle L|\rho|R\rangle) \\ S_3 &= 2(n_3 - n_0) = N(\langle R|\rho|R\rangle - \langle L|\rho|L\rangle) \end{aligned} \tag{4-3}$$

We here use the equivalence between polarization and time-bin qubits, and regard $|0\rangle$ as $|H\rangle$ and $|1\rangle$ as $|V\rangle$. We can connect our $|X1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ to $|\bar{D}\rangle$ and $|Y1\rangle = \frac{|0\rangle - i|1\rangle}{\sqrt{2}}$ to $|R\rangle$. Then, the measurement results in our experiment determine the state generated in X-basis ρ_X as follows:

$$\begin{aligned} n_0 &= \frac{N}{2}(\langle 0|\rho_X|0\rangle + \langle 1|\rho_X|1\rangle) \\ &= P(Z0|X0) + P(Z0|X1) + P(Z1|X0) + P(Z1|X1) \\ n_1 &= N\langle 0|\rho_X|0\rangle = P(Z0|X0) + P(Z0|X1) \\ n_2 &= N\langle X_1|\rho_X|X_1\rangle = P(X1|X0) + P(X1|X1) \\ n_3 &= N\langle Y_1|\rho_X|Y_1\rangle = P(Y1|X0) + P(Y1|X1) \end{aligned} \tag{4-4}$$

where $P(Z0|X0')$ refers to the probability that the measurement result is 0 in Z-basis when the state $|X0'\rangle$ is generated. In the experiment, we calculate the probability from the intensity measurement as

$$P(Z0|X0') = \frac{I(Z0|X0)}{I(Z0|X0) + I(Z1|X0)} \tag{4-5}$$

where $I(Z0|X0)$ represents the intensity of $|0\rangle$ and $I(Z0|X0)$ the intensity of pulse $|1\rangle$, when the state $|X0\rangle$ is intended to generate in Alice's station.

$$P(X1|X0) = \frac{I(X1|X0)}{I(X1|X0) + I(X0|X0)} \tag{4-6}$$

where $I(X1|X0)$ represents the intensity of destructive interference signal in X-basis, when the state $|X0\rangle$ is intended to generate in Alice's station. We can calculate other

probabilities similarly. The Stokes parameters for the states are related to n_i's as

$$\begin{aligned} S_0 &= 2n_0 = N(\langle Y1|\rho_X|Y1\rangle + \langle Y0|\rho_X|Y0) \\ S_1 &= 2(n_1 - n_0) = N(\langle Y1|\rho_X|Y0\rangle + \langle Y0|\rho_X|Y1\rangle) \\ S_2 &= 2(n_2 - n_0) = Ni(\langle Y1|\rho_X|Y0\rangle + \langle Y0|\rho_X|Y1\rangle) \\ S_3 &= 2(n_3 - n_0) = N(\langle Y1|\rho_X|Y1\rangle - \langle Y0|\rho_X|Y0\rangle) \end{aligned} \tag{4-7}$$

We substitute the estimated Stokes parameters into Equation. 4-1 to obtain the density matrices.

4.4 Results and discussion

Figure 4.5 shows the reconstructed density matrices ρ_X for X states. They are reconstructed by the intensities of the interference signals and substituted into Eq. (4-1) - (4-7). Experimental details are shown in the section 4.3. Figures 4.5(a) and 4.5(d) show that, without voltage shift, the density matrices from the DDM and DPM are both close to half of the identity matrix, which implies that the states are almost ideal [51]. However, the states generated by the DDM in Figs. 4.5 (b) and 4.5 (c), deviate from the ideal one by changing 25% of V_π in the applied AC or DC voltage, whereas those generated by the DPM remain close to ideal as shown in Figs. 4.5 (e) and 4.5 (f).

The effects of the modulation voltage on fidelity $F(\rho_X, \rho_Y)$ are summarized in Figs. 4.6 (a) and 4.6 (b) for the DC bias and AC amplitude changes, respectively. We substitute the reconstructed density matrices into Eq. (3-2) to obtain the fidelity. The error bars mainly originate from the noise of the oscilloscope during the measurement of output states. The observed signal-to-noise ratio was approximately 16 dB. The effect of this estimation error was negligible on the final key generation rate, as verified in the simulation reported below. The fidelity of sent states using the DPM remained almost at unity for the voltage deviation range in the present experiment, whereas the states generated by the DDM were affected by the voltage deviation. These results agree well with the theoretical prediction. A small decrease observed under a large voltage deviation may result from the nonlinear response of the phase modulators.

We then evaluated the QKD system performance by simulating the final key generation rate considering the state preparation flaw for decoy state BB84 protocol in the asymptotic case. We use experimentally obtained fidelity and visibility to express the state preparation flaw as described in section 2. For the simulation, we used experimental results described in Chapter. 3, Eq. (3-9) and the parameters listed in Table 4.1, and the error rates were calculated for signal (s) and decoy (d) pulses in the X and Y bases, as follows [44–46]:

$$e_{i,j} = \frac{1}{S_{\mu_j}}\left[\left(1-\exp\left(-\eta\mu_j 10^{-\frac{\alpha l}{10}}\right)\right)E_i + \frac{1}{2}\exp\left(-\eta\mu_j 10^{-\frac{\alpha l}{10}}\right)y_0\right], i = \mathrm{X,Y}, j = \mathrm{d,s} \tag{4-8}$$

where η is the detector efficiency, α (in dB/km) is the loss coefficient in fiber, l is the transmission distance, y_0 is the background rate, μ_{s} and μ_{d} are the mean photon numbers of the signal and nontrivial decoy state, respectively, E_i is the source error rate for the corresponding basis, $S_{\mu_{\mathrm{d}}}$ is the count rate of the decoy pulse, and $S_{\mu_{\mathrm{s}}}$ is the count rate of signal pulse:

$$S_{\mu_{\mathrm{d}}} = 1+(-1+y_0)\exp\left(-\eta\mu_{\mathrm{d}}10^{-\frac{\alpha l}{10}}\right), \tag{4-9}$$

$$S_{\mu_{\mathrm{s}}} = 1+(-1+y_0)\exp\left(-\eta\mu_{\mathrm{s}}10^{-\frac{\alpha l}{10}}\right). \tag{4-10}$$

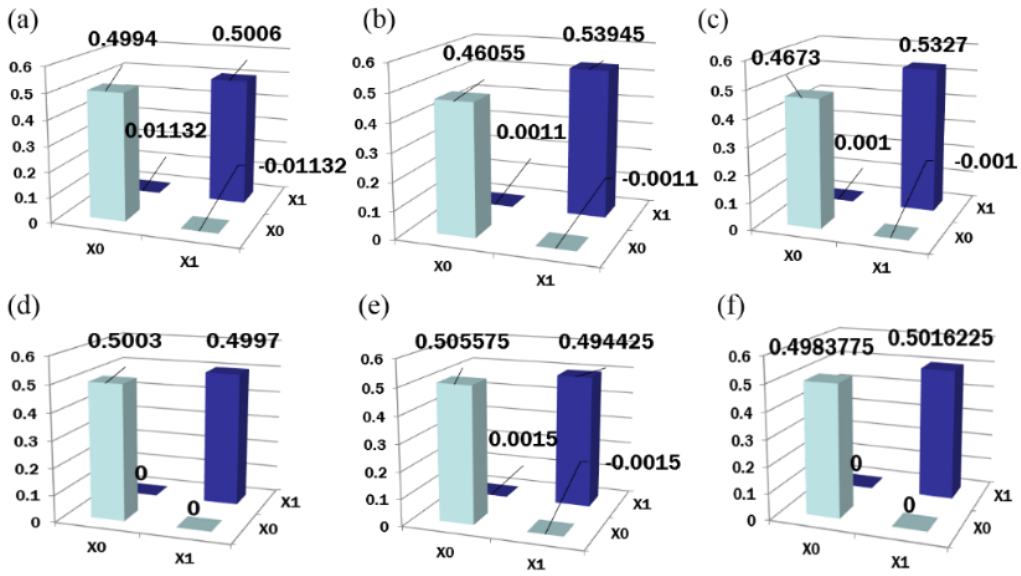


Fig. 4.5 Reconstructed state ρ_X with DDM (a) without voltage variation and with (b) 25% DC bias and (c) 25% AC amplitude change. Reconstructed state ρ_X with DPM (d) without voltage variation and with (e) 25% DC bias and (f) 25% AC amplitude change.

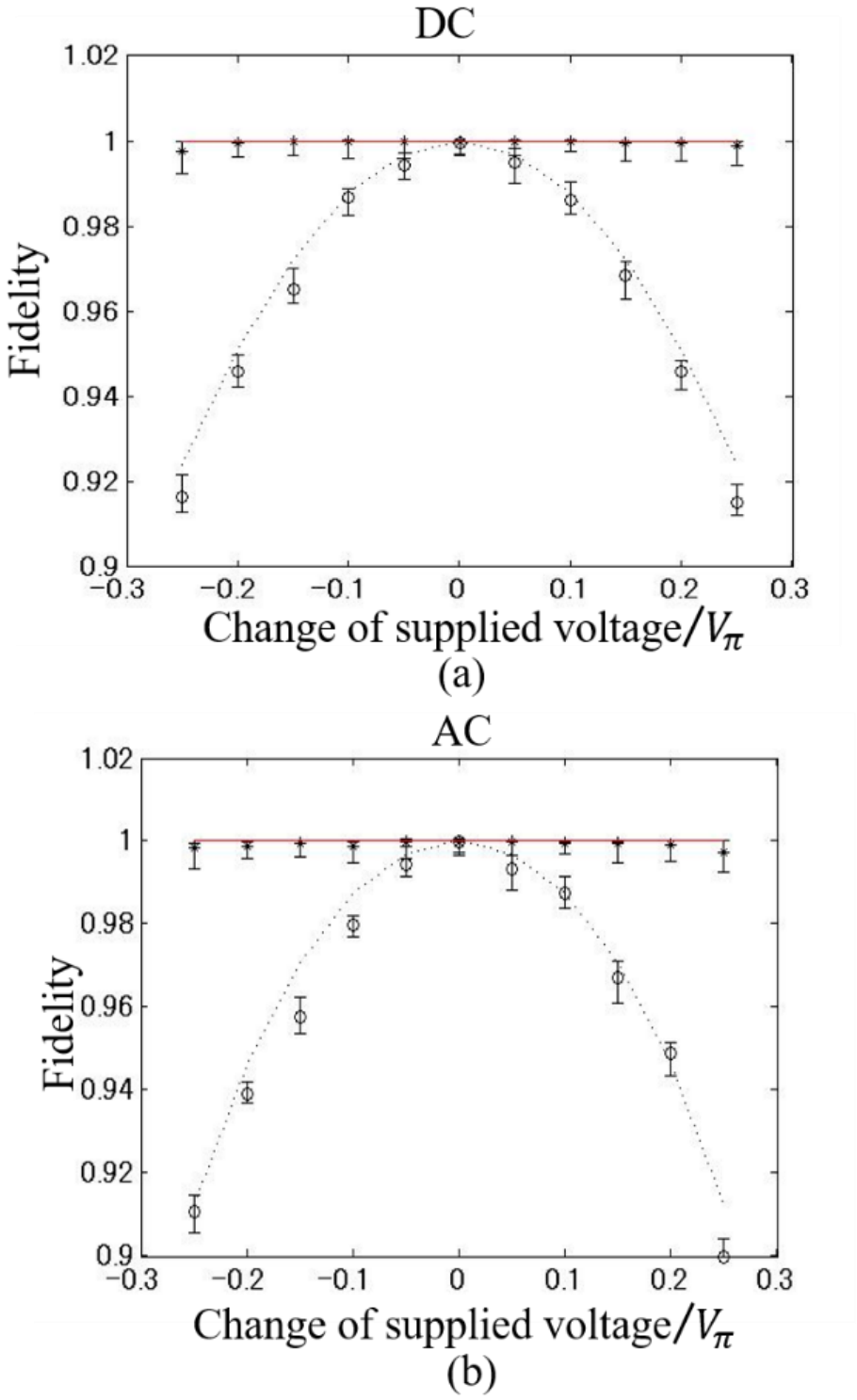


Fig. 4.6 (a) Fidelity according to DC bias. (b) Fidelity according to pulse amplitude (AC). Squares and stars represent the measured values for DDM and DPM, respectively. The solid and dotted lines represent the theoretical values for DDM and DPM, respectively.

Source error rate E_i (i = X, Y) represents the rate at which Alice generates states with incorrect bit values in the corresponding basis and is related to visibility v_i of the interference by

$$E_i = \frac{1 - v_i}{2}. \tag{4-11}$$

The visibilities can be calculated from the measured intensities as

$$v_X = \frac{I(\mathrm{X0}\,|\,\mathrm{X0}') - I(\mathrm{X1}\,|\,\mathrm{X0}')}{I(\mathrm{X0}\,|\,\mathrm{X0}') + I(\mathrm{X1}\,|\,\mathrm{X0}')}, \tag{4-12}$$

$$v_Y = \frac{I(\mathrm{Y0}\,|\,\mathrm{Y0}') - I(\mathrm{Y1}\,|\,\mathrm{Y0}')}{I(\mathrm{Y0}\,|\,\mathrm{Y0}') + I(\mathrm{Y1}\,|\,\mathrm{Y0}')}. \tag{4-13}$$

where I(X0|X0') and I(X1|X0') represent the intensities of pulses measured in photodetectors X0 and X1, respectively, when Alice generates state |X0'⟩ while intending to send state |X0⟩.

The result of the visibility is:

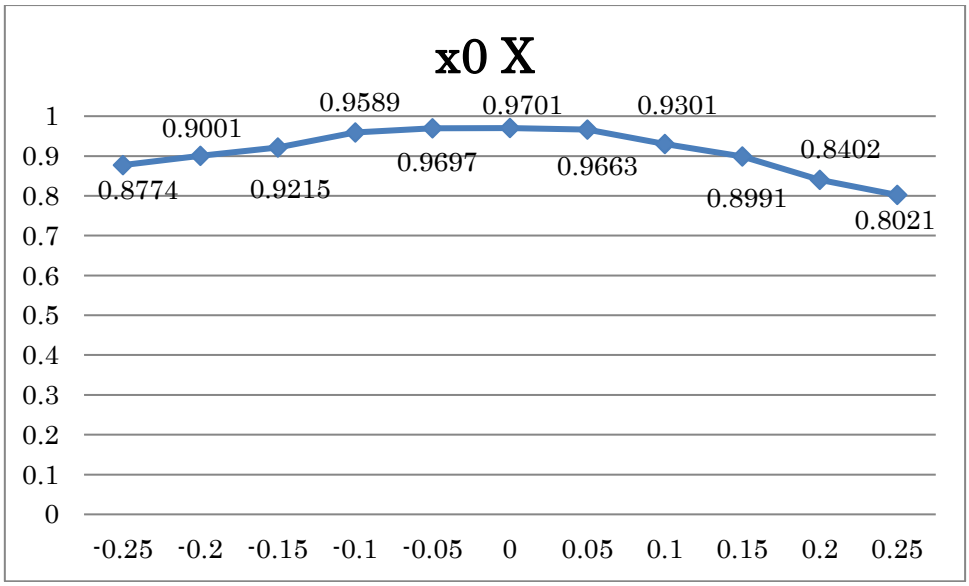


Fig. 4.7 Visibility of DDM by changing AC from -0.25V_π to 0.25V_π

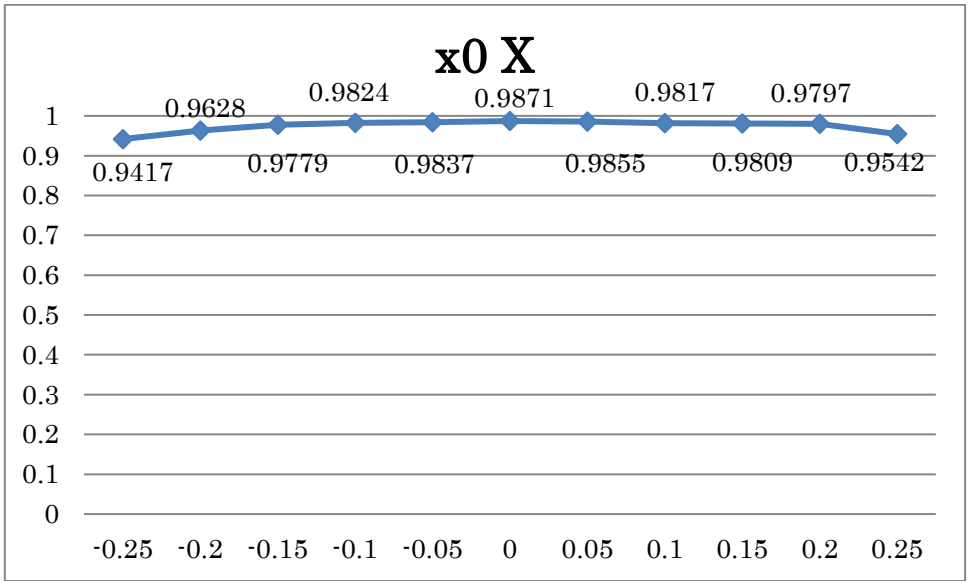


Fig. 4.8 Visibility of DPM by changing AC from -0.25V_π to 0.25V_π

In our decoy state method to calculate the secure key generated from signal pulses, we used quantum bit error rate (QBER) $\delta_{\mathrm{X}} = e_{\mathrm{X},s}$ calculated with Eq. (4-8). Using vacuum+weak decoy states [45], we consider the single-photon state error rate,

$$e_1 \le \frac{e_{\mathrm{Yd}} e^{\mu_{\mathrm{d}}} - e_0 y_0}{y_1^{L,\mu_{\mathrm{d}},0} \mu_{\mathrm{d}}}, \qquad (4\text{-}14)$$

as phase error rate δ_{Y}. To account for the influence of the state preparation flaw Δ, the fidelity from the experimentally obtained density matrices with Eq. (3-2) is used in Eq. (2-1),.We calculate δ'_{Y} as Eq. (3-8) and substitute it into Eq. (3-9) to obtain the final key. Here, e_0 is the error rate of zero-photon state, and we used the same value of $e_0 y_0$ as in [45]. The yield of the single-photon state is given by

$$y_1^{L,\mu_{\mathrm{d}},0} = \frac{\mu_{\mathrm{s}}}{\mu_{\mathrm{d}}\mu_{\mathrm{s}} - \mu_{\mathrm{d}}^{\,2}} \left(Q_{\mathrm{d}} e^{\mu_{\mathrm{s}}} - Q_{\mathrm{s}} e^{\mu_{\mathrm{d}}} \frac{\mu_{\mathrm{d}}^{\,2}}{\mu_{\mathrm{s}}^{\,2}} - \frac{\mu_{\mathrm{s}}^{\,2} - \mu_{\mathrm{d}}^{\,2}}{\mu_{\mathrm{s}}^{\,2}} y_0 \right), \qquad (4\text{-}15)$$

where the superscript in $y_1^{L,\mu_{\mathrm{d}},0}$ represents distance, mean photon number of the weak decoy state, and mean photon number of the vacuum decoy state. The gains can be calculated as above with the given parameters as

$$Q_1 \ge Q_1^{L,\mu_{\mathrm{d}},0} = \frac{\mu_{\mathrm{s}}^2}{\mu_{\mathrm{d}}\mu_{\mathrm{s}} - \mu_{\mathrm{d}}^{\,2}} \left(S_{\mu_{\mathrm{d}}} e^{\mu_{\mathrm{s}}} - S_{\mu_{\mathrm{s}}} e^{\mu_{\mathrm{d}}} \frac{\mu_{\mathrm{d}}^{\,2}}{\mu_{\mathrm{s}}^{\,2}} - \frac{\mu_{\mathrm{s}}^{\,2} - \mu_{\mathrm{d}}^{\,2}}{\mu_{\mathrm{s}}^{\,2}} y_0 \right), \qquad (4\text{-}16)$$

Table 4.1 Parameters for key generation rate

Parameter	Value
Fraction of X basis q	1
Error correction efficiency f	1.1
Efficiency of photon detector η	0.1
Absorption coefficient α (dB/km)	0.2
Mean photon number in signal pulse μ_s	0.5
Mean photon number in decoy pulse μ_d	0.1
Background rate y_0	1.0×10^{-6}

The simulation results are shown in Fig. 4.9 and clearly describe the effects of the state preparation flaw. In both the DC bias and AC amplitude changes, the DPM yields higher key generation rate than the DDM. The final key generation rate is almost unchanged up to $0.2V_\pi$ deviation for AC, and a finite key generation rate is obtained at 180 km under DC bias variation. As the DC bias changes the phases of both states $|0\rangle$ and $|1\rangle$, its effect is more notable, though the errors in DC bias would be much smaller than AC deviation in a practical device. As our experimental fidelity and simulation result, state preparation flaw generated by the imperfection in implementation will lead to a decrease in key generation rate as theoretical analysis [2], [18-41]. The improvement on intensity modulator and phase modulator is also studied to decrease the imperfection in implementation [53]. Our proposal take advantage of the PLC-AMZI to keep the stable interference to avoid inaccuracy during the state preparation. Moreover, our proposal, DPM, is an off-the-shelf device used in optical communication. It requires only two values, 0 and $V_{\square}$ to define the BB84 states will simplify the design of the driving circuit. Other researches based on the feedback of the quantum key distribution system were also supplied to decrease the imperfection in implementation [54]. Our proposal can suppress the state preparation flaw without complicated feedback circuits. Of course, the combination of these researches and ours will decrease state preparation flaw further and provide a much more efficient transmitter.

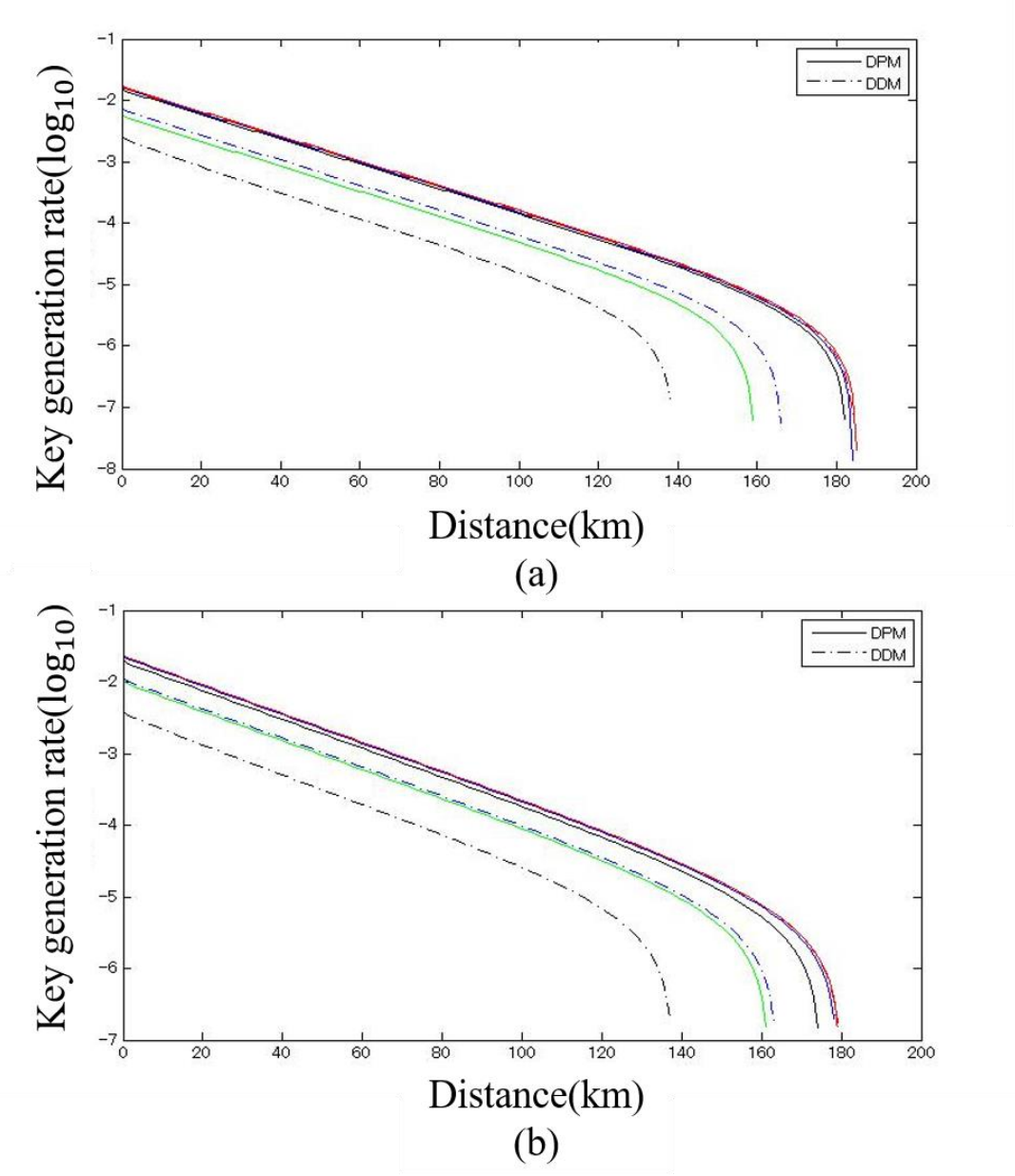


Fig. 4.9 Final key generation rate by (a) DC and (b) AC variations in the modulator. Dashed lines represent voltage deviation of 0 (red), $0.05V_\pi$ (blue) and $0.1V_\pi$ (black) in DDM. Solid lines represent voltage deviation of 0 (red), $0.05V_\pi$ (blue), and $0.1V_\pi$ (black) and $0.2V_\pi$ (green)in DPM.

Chapter 5

Quantum Random number generator

As described in introduction, another obstacle is that QKD systems require amount of random numbers during its operation. In this section, we will discuss reason and method we generate random numbers. And firstly, I will introduce 2 types of random numbers, pseudorandom numbers and true random numbers. As the requirement of different application, different random numbers are generated and utilized. True random numbers generated from quantum random number generator (QRNG) based on quantum mechanics are usually called as quantum random numbers [19, 55]. For many superiors that we will discuss in this section, QRNG is on the front in the last 20 years. Then, I will show you the common block description of QRNG.

5.1 Random numbers

Random numbers play significant roles in many fields, secure communication, fundamental science test, gambling industry, numerical simulation and many aspects in our daily life. Some applications need a particle of random numbers and utilize the manual and mechanical methods to generate randomness, for example, tossing a coin, throwing a die, spinning a roulette wheel or a drawing some balls from a lottery machine. Here, we will focus on the random number generators with high generation rate applying to computers.

5.1.1 Pseudorandom number generator

As the development of computer science, a large number of random numbers are required. Meanwhile, generating random numbers directly from computers looks like a matter of course. PRNG is full named as pseudorandom number generators that produce random numbers from a deterministic algorithm. The greatest benefit of this generator is its high generation rate, because it is only limited by the calculation speed of a computer.

The pseudorandom number of a computer is calculated by random seeds according to a certain calculation method. For example, we can use real time in computer as the seed and build random numbers. As long as the calculation method is certain and the random seeds are certain, the random number generated is fixed. It means that generated random numbers could be reproducible, if seed and generation algorithm is known. This character might be an advantage for some applications, for example, we can repeat the same simulation when we do some researches.

Back in the 1940s, when computers were first invented, Von Neumann came up with a so-called "Middle-square method" method to generate random numbers. Take a four-digit number, such as 1234, as the seed, calculate that its square is 1522756, fill the left side with a 0, change to 01522756, and then he output the middle four numbers as random numbers, that is 5227. And then we square 5227 and we take the middle four digits and we repeat. This algorithm is doubtful after you realize it, the last number is very simple to know what the next output is, no matter what seed number you used. So, how can it be called random number? But Von Neumann felt that the random numbers met his needs, they were fast, required fewer resources, and were repeatable and easy to troubleshoot. If you use other hardware to generate random numbers, such as a punched paper tape machine for input, it's too slow and consumes too much resources. At the time, Von Neumann also pointed out that using overly complex mathematics to generate so-called "random numbers" might hide more errors than it solves.

But it was clear that Von Neumann's algorithm could not satisfy the need for random numbers in many cases. Since the 1960s, a method called linear congruency or LCG algorithm [56] has been widely used to generate random numbers. The linear congruence algorithm is very simple, it's just a function $ax + b \bmod c$, and it takes the remainder as a random number, and then the next random number takes the last remainder as x, and iterates over the next remainder. You could even take *b* to be equal to 0, which is ax over *c*. In practice, each remainder can be converted into a binary number and output in turn. Recursive formula of LCG algorithm:

$$X_{n+1} = aX_n + c \bmod m \tag{5-1}$$

The advantages of the above algorithm are obvious, that is, simple and efficient. And if I make the *c* that's being divided big enough, I can make the period very long, and I can pass almost all the statistical tests. So this algorithm was widely used as soon as it appeared, for example, the Random function in the Standard library of The Java language is still the LCG algorithm, where the dividend *c* is 2^48, because if the calculation by the power of 2 is the fastest in the computer, just shift it. And a is a strange number 25214903917, *b*=11. Instead of writing out the remainder each time, you write the numbers in reverse, from the 47th to the 16th digits, because the higher digits have a shorter cycle, so the lower digits pass the statistical test better.

The above algorithm has been used since the 1960s, which shows its superiority. But it certainly has some drawbacks. One is that you must choose your parameters a, b, and c carefully, and if you don't choose them well, you have a problem. Another problem is that you should not use the LCG algorithm in cases where encryption is required, because if someone wants to, they can count your seeds backwards from your history output. So this is kind of a math problem: you know the remainder of a, b, c and ax plus b divided by c, and you figure out x. You could write a polynomial time algorithm to solve this problem.

Then there is the so-called "cryptography secure" random number generation algorithm. First of all, we need to define "cryptographic security". We see that the previous algorithm is "unsafe", which is unsafe because we can predict the number of seeds you use by looking at the historical data, and finally achieve the effect of the random number generated after the prediction. That, in turn, is a cryptographically-secure random number algorithm, where I can give you fairly long historical data, and you have very strong computers, and I can still make sure that you can't make any "nonnegligible" changes in a sufficiently long period of time, for example, a year, to guess what random numbers I'm going to produce in the future. "Fairly long," "very strong," "sufficiently long," and "not negligible," are variables that we do not need to have a precise numerical definition of,

as long as we know that these variables can be used to measure the quality of the final algorithm. In different cases, we can define some values for these variables, and if the algorithm can achieve the values we define, then the algorithm can be used in our case.

5.1.2 True random number generator

However, in other application, unpredictability, that we cant reproduce generated random numbers, is significant. Especially in cryptography, with the development of modern computer science, normal random number algorithms will be hard to meet the requirement of cryptography secure. Random numbers cant be predicted is called true random numbers or hardware random number generator and its generator is called true random number generator (TRNG).

Physical process, which is hard to predict or even is unpredictable, is utilized by true random number generators to create the random number strings. So that, it is also called physical random number generator. The unpredictability of PRNG is ensured by values from the software in the computer or create the bit strings in a professional device that inputs it into the operating system. There are physical TRNGs based on different principles, such as chaotic systems [57], thermal noise in electronic circuits [58], free running oscillators [59], or biometric parameters as a few examples.

Many IT vendors product processors containing physical random number generators using physical values in this device. An example is that Intel integrate a digital RNG based on a metastable thermal noise working at 3 GHz rate into his production which is normally used in our computers. This integrated RNG can be directly accessed from a processor instruction, RdRand [60]. In addition, the VIA Technologies Nehemiah processor core from Taiwan contains an on-chip random number generator which is based on a series of oscillators where thermal noise alters the jitter so that the combination of the oscillators' output is random. These integrated RNG combines with conditioning circuits that process the output to remove biases.

However, there are inconveniences that have impeded wider adoption of physical TRNGs. Some of the problems in physical TRNGs are: first, limited generation rate. Physical RNG usually produce random numbers at a much smaller rate than algorithm methods. There would be a fundamental limitation in the rate of change of the sampled physical parameter during several physical phenomenon. If the sampling rate is too high in this system, the system will have not enough time to change and the random numbers which make them not independent. Secondly, a convincing argument for the randomness of the data is hard to supplied. So that, the randomness of the chosen physical phenomenon could be doubtful. From this point, many physical random number

generators are generated by our ignorance to describe a physical process rather than its intrinsic randomness. However, if no one can describe this randomness with our own knowledge, it is a kind of pseud-random number generator which may be solved someday in future. The third one is that it is inconvenient to add an external device in the physical phenomenon. Finally, it is difficult to detect failures in this system. If a hardware random number generator fails during operation, it can be difficult to notice. Official recommendations suggest introducing a startup test, a total failure test and an online test to check errors during operation [87].

An important distinction between pseudorandom number generators and physical random number generators is the focus on product or process randomness. For pseudorandom number generators we can only evaluate the output strings. We focus on the product of the ultimately deterministic algorithm and we try to determine whether the string has all the properties of a random sequence. In order to determine if we have product randomness our options are limited to checking the output strings and submitting them to certain statistical test. In physical TRNG we concentrate on process randomness. We look for a process that produces a random output and seek to obtain true random numbers from fundamentally random physical phenomena. Here, randomness is usually taken as unpredictability. While, properly, classical phenomena can not be considered truly random, in common use, the terms physical and true random number generator are used interchangeably. Usually, it is fine to use an unpredictable physical system as a randomness source. However, there remains a doubt whether the backing physical process is truly random or, at least, presents serious difficulties to be predicted, like a chaotic system, or we simply have a poor model and a better one could destroy the illusion of randomness. Quantum random number generators (QRNG) excel in that aspect: they use very well defined inherently random processes as the source of their bits.

5.2 Block description

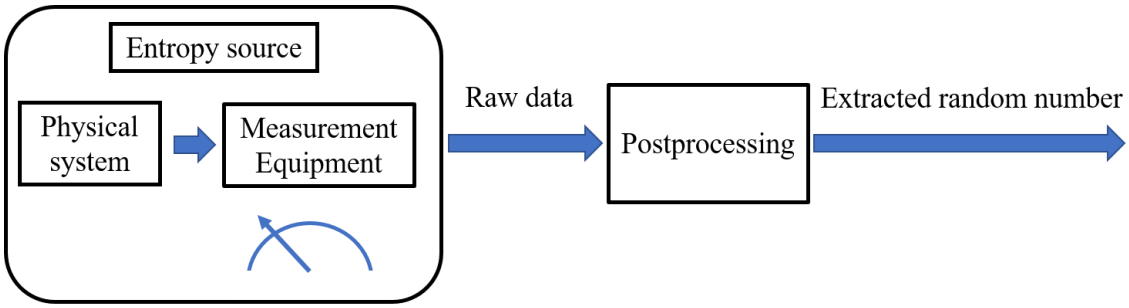


Fig. 5.1 Block figure of a typical physical random number generator.

Physical random number generators can be divided into separate blocks with well-defined subtasks. The two most important blocks are the entropy source and the postprocessing stage. The entropy source consists of a physical system with some random physical quantity and the measurement equipment that reads these random variables. In digital random number generators, we usually need to convert analog measurements into bit strings with the help of analog-to-digital converters. Measurement and quantization are noisy processes and there will be some contamination in what is called the raw bit string even if the measured quantity is truly random and free from correlations. The postprocessing block takes the raw bits and distills a shorter sequence without correlations.

The most important phase in postprocessing is randomness extraction. Randomness extractors are functions that transform the bits from the raw sequence into a uniform random sequence at the output with most or all of the randomness available in the input.

Fig. 5.1 shows the block diagram of a typical physical random number generator. The exact parts vary from device to device. For instance, some physical random number generators are designed to produce raw sequences with negligible bias and forgo the postprocessing phase. There is a delicate balance in choosing an adequate postprocessing system. More involved randomness extraction methods usually allow to minimize the amount of random bits that are thrown away, but are slower. The overall bit rate depends on whether the increased production of bits compensates or not for the slower processing circuit or if it is justified to use a faster but more complex hardware to remove biases from the raw bit sequence.

5.3 Quantum random number generator

In quantum mechanics, the state of a physical system can be prepared as a superposition state. In Stern–Gerlach electron spin experiment [61] in Fig. 5.1, we assume optional vertical upward and downward along a vertical direction. If the electron is started with 2 superimposed directions, the electron spin detection for failure out of an electronic start in which the coherence state of superposition, and therefore have a true random measurement. According to the Born rule, the nature of the measurement results of quantum states shown above is random and unpredictable, which means that we cannot have a better prediction method than blind guessing. Therefore, the inherent randomness in quantum measurement can be used to generate true random numbers. In quantum mechanics, quantum coherence can be regarded as a kind of resource. The measurement process can destroy the coherence of the measured sub-state on a certain measurement basis vector, thereby generating randomness equivalent to the quantum coherence

consumed. In turn, the quantum coherence can be quantified from the inherent randomness.

A simple example of a quantum random number generator shown in Fig 5.1. Based on different mechanisms and equipment of the method, the actual QRNGs are diverse. In general, a good quantum random number generator program should have a low cost and a high random number generation rate. In fact, in each quantum random number generator scheme, quantum effects are often mixed with classical noise. By establishing a suitable physical model, even if the quantum signal and classical noise cannot be separated technically, the signal-to-noise ratio can be calculated, and the true randomness can be accurately estimated.

This can usually be achieved by a high number of theoretical modeling of the random number generator generates a random rate. However, the random number generator only when the device is authentic, the output of the random number sequence that has the " information-theoretic security" of randomness. If the device is manipulated by an adversary, the output may not be truly random. For instance, if a quantum random number generator is provided by a malicious manufacturer, a very long random string is copied to a large hard drive and removed in order from the hard drive outputs numbers, and the manufacturer can always predict the output of the device.

On the other hand, we can design the quantum random number generator by means of an approach, called " random is not dependent on physical apparatus". By means of a self-testing method for preparing apparatus, even if the physical means are not enough trusted, we can still produce truly random numbers. Its basic principle is entanglement witness or locality witness, the observation of Bell inequality violation. Even if output this random number generator, mixed with classic noise, according to the detection result of Bell's inequality, we can still estimate a lower bound of true randomness. Since Bell's inequality itself requires random input, random seeds are necessary in this kind of random number generator. So that, this process is more appropriate to be considered as a process of random expansion, using less randomness to generate more randomness. The disadvantage of this random number generator is that the generation rate is very slow.

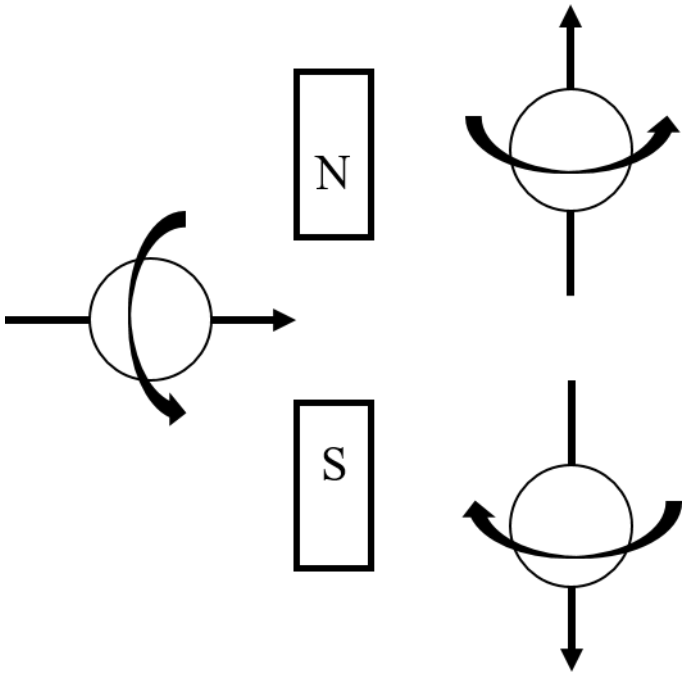


Fig. 5.1 Electron spin detection in the Stern–Gerlach experiment. Assume that the spin takes two directions along the vertical axis, denoted by $|\uparrow\rangle$ and $|\downarrow\rangle$. If the electron is initially in a superposition of the two spin directions, $|\rightarrow\rangle = (|\uparrow\rangle + |\downarrow\rangle)/\sqrt{2}$, detecting the location of the electron would break the coherence, and the outcome ($\uparrow$ or $\downarrow$) is intrinsically random.

We wish to make a compromise between generation rate and safety. In general, in the actual apparatus, a random number generator can be divided into source and the measurement device 2 modules as shown in last section. We can partially trust the equipment of the random number generator, that is, a trusted source or a trusted measurement device. Such a random number generator scheme is between the above two schemes. It has a certain degree of security but does not lose too much of the generation rate. It is called a semi-self-testing random number generator. In this paper, we will focus on the trusted device QRNG or we can call it practical QRNG.

5.4 Trusted device QRNG

From the above, the true randomness can be obtained by any method that destroys the properties of quantum coherent superposition. Due to the high quality of optical devices and the potential to be integrated on the chip, most actual quantum random number

generators currently use optics system. I will introduce the principles of various optical quantum random number generators below.

Generate quantum random numbers by measuring the state of qubits. We can directly compare the superposition state $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ under the measurement basis vector (Z basis vector, $|0\rangle$ and $|1\rangle$ are the eigen basis vector of Z) to generate quantum random numbers. The biggest advantage of this quantum random number method is that it directly depends on a clear and simple principles of quantum mechanics, and thus theoretically straightforward. This method is widely adopted early quantum random number generator. In this lower frame, each photon we can get a measurement 1b random numbers. Rate of random number generator is limited primarily by the detector parameters such as dead time of the detector, the detection efficiency and so on. For instance, a silicon single-photon detector (SPD) based on a typical avalanche diode hold tens of nanoseconds dead time [62], then the generation rate of the quantum random number generated in such a frame rate is restricted to order of several tens of Mbps. It cannot meet the requirement of some applications, such as high-speed quantum key distribution (key distribution already do GHz rate as described in chapter 2). There are already a large number of random numbers generated based on a single photon measurement method to improve this plan.

Generate quantum random numbers based on the measurement of time patterns. One way to increase the rate of random number generation is to obtain random numbers by measuring in a higher-dimensional space, such as measuring the time or space pattern of photons. In this method, a continuous-wave mode laser emits photons and shoots into a single-photon detector with time resolution. The intensity of laser can be accurately controlled to ensure that the number of photons detected within a selected time period T is expected to be 1. The time t of a single photon detected is uniformly distributed within the time period T and discretized by the time detection precision δ_t. The probe time t is recorded as raw data for random numbers. So for each probe, we can generate the original random number 1b (T/δ_t). In essence, the resolution of a time probe is limited by the detector's time jitter (typically on the order of 100ps), which is much shorter than the detector's dead time (typically on the order of 100ns). The important advantage of time detection to generate random numbers is that through each measurement, we can extract quantum random numbers exceeding 1b, which can increase the rate of random number generation. We usually choose the time period T that is at the same order of magnitude as the detector dead time. Compared with the qubit-based measurement method, the scheme of generating random numbers based on time measurement alleviates the impact of the detector dead time. For example, if the time resolution and dead time of a SPD are 100ps

and 100ns respectively, so the random number generation rate is about 1b:1000×10Mbps, which is higher than the previous measurement method based on qubits. The method of generating random numbers based on time detection has been extensively studied recently.

The generation of quantum random numbers based on the measurement of spatial patterns is similar to the generation of random numbers based on time detection. By detecting the spatial pattern of a photon through a detection system with spatial resolution, we can generate multi-bit random numbers. A simple spatial detection It can be achieved by letting photons pass through a 1×N beam splitter to detect the path of the outgoing photons. In this method, distributed random number depends on the intensity and spatial distribution SPD detection efficiency of the array have a property. The spatial-pattern-based approach has similar properties as the time-based approach, but it requires multiple detectors. At the same time, there may be a correlation between the generated random numbers, because the signals received on the closely spaced detectors may overlap.

Based on the measurement of multiple photon number states, quantum random number randomness can be generated not only from the measurement of a single photon, but also from the state containing multiple photons. For example, quantum coherent states

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} |n\rangle \tag{5-2}$$

is superposition from different photon number states $|n\rangle$ (Fock state), where n is the number of photons and $|\alpha|^2$ is the average number of coherent states. Then, by measuring the number of photons in the coherent state pulse generated by the laser with a photon number resolution detector, we can obtain random numbers satisfying the Poisson distribution. The method of obtaining random numbers by measuring the number of photons has been successfully implemented by experiments [63]. This method is used in the first smart phone with a QRNG inside from Samsung (Galaxy A Quantum). The photon number distribution achieved through LED light sources and commercial cameras in Galaxy A Quantum, and quantum random numbers are generated.

Generate quantum random numbers based on vacuum fluctuations. In quantum optics, the quadrature of the amplitude and phase of the vacuum state in the phase space is represented by a pair of noncommutative operators *X*, *P*, which satisfy [*X* , *P*]=*i*/2, this pair of physical quantities cannot be accurately detected at the same time,

$$\langle(\triangle X)^2\rangle \times \langle(\triangle P)^2\rangle \geq 1/16 \tag{5-3}$$

where the mean value of the operator is $\langle O\rangle$, and the deviation is defined as $\Delta O = O - \langle O\rangle$. We can easily visualize this uncertainty relationship in the phase space. In the phase space, the vacuum state is represented as a two-dimensional Gaussian distribution, the

center of which is located at the origin, and the uncertainty in each direction is 1/4. In principle, the Gaussian distribution of random numbers can be obtained by measuring the orthogonal components of any phase space. One possible solution is to detect the orthogonal components of the phase space using a strong laser pulse through a symmetrical beam splitter and a balanced detector to detect the difference beat signals. The local oscillator in Homodyne detector is a single-mode coherent state created by the laser intensity. The quadrature component of the uncertainty will be shot noise embodied in the form of a random number generated by the program will follow the Gaussian distribution. This approach has several outstanding advantages: first, The light source based on this scheme is in a vacuum state, which is easy to be prepared in experiments with high fidelity; second, such a random number generator is not sensitive to the detection loss of the detector, and we can easily compensate for it by increasing the light intensity ; third, since the quadrature component of the phase space is a continuous variable, through one measurement, we can extract a random number of multiple bits. However, it is still technically difficult to construct a wide-band, scattered-particle noise limited zero-difference detector in the range of several hundred MHz. These will limit the final random number generation rate.

In order to overcome the problem of bandwidth limitation in homodyne detection under the limitation of shot noise, researchers have developed a novel scheme for generating quantum random numbers based on measuring the phase or amplitude fluctuations of amplified spontaneous emission (ASE). The first option is to measure the amplified spontaneous radioactive phase noise. In this option, random numbers can be generated by measuring the "phase-randomised weak coherent states" (signal States) in the phase space with their orthogonal components. Random number generators based on phase noise will have better immunity to detector noise. In fact, this scheme can be implemented using commercial photon detectors at the GHz scale.

Another solution is to use an interferometer to measure the light intensity fluctuations caused by the phase fluctuation of the spontaneous emission of the laser as shown in Fig. 5.2. This solution consists of a CW laser source and a about 10ns delayed self-heterodyning detection system. Random numbers can be achieved by detecting the phase difference between time t and time t+ΔT. Intuitively, if the time delay ΔT relative to the coherence of the laser If the time is long enough, then the interference of the two laser beams in the second beam splitter in the figure can be regarded as the laser interference produced by two independent laser light sources. In this case, the phase difference is one in [-π, π) uniformly distributed random numbers and have nothing to do with the classical noise generated by the unbalanced interferometer. This shows that a robust quantum

random number generator can be constructed by an interferometer without phase stabilization device. On the other hand, if we have performed a phase-stabilized operation in the interferometer, and the time delay ΔT can be shortened to much less than the coherence time of the laser, thus providing a higher sampling rate method. This stable-phase interferometer generates random numbers program has been experimentally adopted ≥6Gb ps [64] and 68Gbps [25].

In addition, a pulsed laser source can supply an automatically randomized phase difference between adjacent pulses. So that, the QRNG based on phase noise has also been implemented using a pulsed laser source [76, 77]. A speed of 43 Gbps (raw rate 82 Gbps as shown in Table 5.1) has been demonstrated [85]. Our proposal holds the same principle as this method, so I will discuss it in detail in next chapter.

In the last, I will show you some QRNG examples using methods described in this section in Table 5.1.

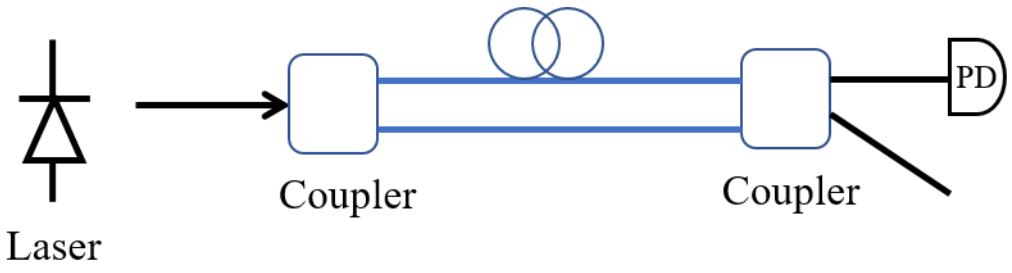


Fig. 5.2 Configure of QRNG based on ASE-phase noise

Table 5.1 Parameters for key generation rate

Year	Entropy source	Detection	Raw	Refined	Aquisition
2000[20]	Spatial mode	SPD	1 Mbps	—	Dedicated
2000[65]	Spatial mode	SPD	100 Kbps	—	Dedicated
2014[66]	Spatial mode	MCP-PCID	8 Mbps	—	Dedicated
2008[21]	Temporal mode	SPD	4.01 Mbps	—	Dedicated
2009[67]	Temporal mode	SPD	55 Mbps	40 Mbps	Dedicated
2011[68]	Temporal mode	SPD	180 Mbps	152 Mbps	Dedicated
2014[25]	Temporal mode	SPD	109 Mbps	96 Mbps	Dedicated
2010[22]	Photon number	PNRD	50 Mbps	—	Dedicated
2011[69]	Photon number	PNRD	2.4 Mbps	—	Dedicated
2015[70]	Photon number	PNRD	—	143Mbps	Oscilloscope
2010[71]	Vacuum noise	Homodyne	10 Mbps	6.5 Mbps	Dedicated
2010[72]	Vacuum noise	Homodyne	—	12 Mbps	Dedicated
2011[73]	Vacuum noise	Homodyne	3 Gbps	2Gbps	Dedicated
2010[24]	ASE-intensity noise	PD	12.5 Gbps	—	Dedicated
2011[74]	ASE-intensity noise	PD	20 Gbps	—	Dedicated
2010[75]	ASE-phase noise	Self-heterodyne	1 Gbps	500Mbps	Oscilloscope
2011[76]	ASE-phase noise	Self-heterodyne	1.2 Gbps	1.11 Gbps	Oscilloscope
2012[64]	ASE-phase noise	Self-heterodyne	8 Gbps	6 Gbps	Oscilloscope
2014[77]	ASE-phase noise	Self-heterodyne	80 Gbps	—	Oscilloscope
2014[85]	ASE-phase noise	Self-heterodyne	82 Gbps	43 Gbps	Oscilloscope
2015[25]	ASE-phase noise	Self-heterodyne	80 Gbps	68 Gbps	Oscilloscope

5.4 Postprocessing

In theory, a QRNG can produce random numbers with provable randomness. In practice, quantum signals (the source of true randomness) are inevitably mixed with classical noises. An adversary can, in principle, control the classical noise and gain partial information about the raw random numbers. In QRNG research, we assume a trusted device scenario, but the classical noise might be deterministic if we calibrate the system more carefully. For instance, imagine that an input to our device is an external power supply. Imagine further that through carefully monitoring the input value of the power to our device, we have determined that the power may still fluctuate by, say, up to 1%. In principle, the source of such fluctuations of an external power supply might be the action of an adversary—Eve—who, therefore, always has complete knowledge about the actual value of the power supply.

Therefore, it is necessary to apply a postprocessing procedure to distill out the true randomness that Eve has almost no information about. This distilling procedure is called randomness extraction, realized by employing randomness extractors. The goal of randomness extractors is to extract (almost) perfect randomness from the raw data generated from a practical QRNG with the help of a short random seed, which requires an extra source of randomness. The key input parameter of a randomness extractor is the min-entropy of raw data.

5.4.1 Entropy estimation

Entropy represents the degree of disorder in a random distribution and offers a convenient way to measure randomness in its many forms. In information theory, Rényi entropy is the general one, its definition is shown as [78]

$$\mathrm{H}_{\alpha}(X) = \frac{1}{1-\alpha}\log\left(\sum_{i=1}^{n} P_i^{\alpha}\right) \tag{5-4}$$

Where α is the order, X is a discrete random variable with possible outcomes {1,2,3,4…n}, and corresponding probabilities $P_i = \Pr(X = i)$ for i=1,2,3…n. The logarithm is conventionally taken to be base 2, especially in the context of information theory where bits are used. It is easy to find that the common entropy (called Shannon entropy) in information theory is the limiting value of H_{α} as $\alpha \to 1$,

$$\mathrm{H}_1(X) \equiv \lim_{\alpha \to 1} \mathrm{H}_{\alpha}(X) = -\sum_{i=1}^{n} P_i \log_2(P_i) \tag{5-5}$$

In a uniform random process, all the outcomes are equally “surprising”, and we need to use all the bits. Less surprising distributions where some results are more likely than others would need, on average, less bits to be described. Table 5.2 shows an example of bit representations for the results of throwing a balanced and an unbalanced die. For each possible outcome of a throw (first column) there is an associated probability shown in the second column. The third column shows a possible way to assign a bit sequence to each outcome. For a balanced die we have three bits of entropy $H(X) = -6(1/6)\log_2(1/6) = 2.585$. For a loaded die, we have an entropy $H(X) = -(1/2)\log_2(1/2) - (1/4)\log_2(1/4) - (1/8)\log_2(1/8) - (1/16)\log_2(1/16) - 2(1/32)\log_2(1/32) = 1.9375$. For the given encoding, we can check we need an average of 1*(1/2) +2*(1/4) +3*(1/8)+4*(1/16)+2* 5*(1/32) = 1.9375 bits to describe the result.

Table 5.2 Entropy calculation example for a fair and a loaded die

Fair die		
x	P(x)	Sequence
1	1/6	001
2	1/6	010
3	1/6	011
4	1/6	100
5	1/6	101
6	1/6	110

Loaded die		
x	P(x)	Sequence
1	1/2	0
2	1/4	10
3	1/8	110
4	1/16	1110
5	1/32	11110
6	1/32	11111

In the limit as $\alpha \to \infty$, the Rényi entropy H_α converges to the Min-entropy H_∞ [77]

$$H_\infty(X) \equiv \lim_{\alpha\to\infty} H_\alpha(X) = -\log_2(\max_{x\in A} P_X(x)) \tag{5-5}$$

The min-entropy gives a lower, worst-case bound to all the Rényi entropies. In this sense, it is the strongest way to measure the information content of a discrete random variable. So that, Min-entropy is widely used for quantifying the randomness of a probability distribution from entropy source. In a distribution with min-entropy k, every possible outcome x has a bounded probability $P_X(x) \leq 2^{-k}$. Any probability distribution of min-entropy k can be written as a convex combination of distributions that are uniform for k bits. This gives an important interpretation of min-entropy as the number of uniform bits that can be extracted from a given distribution. Generally speaking, we can extract k bits from every random output at most.

5.4.2 Randomness extractor

The randomness extractor is an algorithm that converts unevenly distributed raw data into uniformly distributed random numbers. Some simple methods have been widely used for QRNGs. For example, an xor operation has been employed in the literature [80]: dividing the raw data into two-bit strings and performing a bitwise xor operation between them. This operation can certainly refine the raw data to pass some randomness statistical tests. However, with this method, the generated randomness is not information-theoretically provable.

First, I will give you definition of a randomness extraction, a $(k, \varepsilon, n, d, m)$ extractor

$$\text{Ext}: \{0,1\}^n \times \{0,1\}^d = \{0,1\}^m \tag{5-6}$$

Here, for every probability distribution X on $\{0,1\}^n$ with min-entropy is bigger than k, the probability distribution Ext(X,U_d) is ε close to the uniform distribution on $\{0,1\}^m$. From this definition, we can know that the extractor is a function that takes a small seed of d bits and a partially random source of n bits to output an almost perfect random bit string of m bits. Here I will introduce a strong extractor using Toeplitz-Hashing which is information-theoretically secure [81]. In principle, because of the similarity between the definitions of extractors and privacy amplification [82], some privacy amplification can be used as a random number extractor. Toeplitz-Hashing extractor is one of methods for privacy amplification and is made of a Toeplitz matrices for universal hashing function construction. A Toeplitz matrix of dimension n × m requires only the specification of the first row and the first column. Other elements of the matrix are determined by descending diagonally down from left to right. Thus, the total number of random bits required to construct a Toeplitz matrix is n + m− 1.

The detail of this extraction is shown as:

1. Given raw data of size n with a min-entropy of k and a security parameter ε, b is ADC resolution determine the output length to be

$$m = \frac{nk}{b} + 2log\varepsilon \tag{5-7}$$

2. Construct a Toeplitz matrix with an n+m-1 random-bit seed. Here, seeds from pseudorandom number generator or other physical random number generator is used.

3. The extracted random bit string is obtained by multiplying the raw data with the Toeplitz matrix. In stance, the n=$2^{12} = 4096$ data is chosen, and min-entropy of raw data from quantum source is 7.9, $\frac{nk}{b}$ is calculated as 4096*(7.9/12) = 2697. If we set m=2569, ε will be resulted in 2^{-64}.

Chapter 6

Proposed QRNG

As shown in last part of 5.4.1, QRNG based on phase noise from ASE in optical source requires a light source and a self-delayed interferometer. By coincidence, as shown in Chapter 2, this two equipment is commonly implemented in BB84 QKD system, which require amount of random numbers during its operation. If we could build QRNG with equipment in QKD system, it will cut more cost and reduce the risk of information leak during random number transmission from external QRNGs. So that, we propose a QRNG based on a transmitter of a time-bin BB84 QKD system. It uses the laser diode (LD) in QKD system as the phase noise source and Asymmetrical Mach-Zehnder interferometers (AMZI) in QKD system as time-delay structure. In addition, a Faraday mirror, a photo detector, analog to digital converter (ADC) and computer are used as the measurement part. However, a long-time delay (~10ns [25]) is required in an existing high generation rate QRNG based on phase noise, because of the potential phase correlation ship between two close emissions from laser. And such long-time delay could not be supply by interferometer in real QKD system, because a short time delay interferometer is necessary in high transmission speed QKD system. Fortunately, the phase noise randomness from the gain switched LD depends on the operating condition [83, 89]. We will introduce it in this chapter.

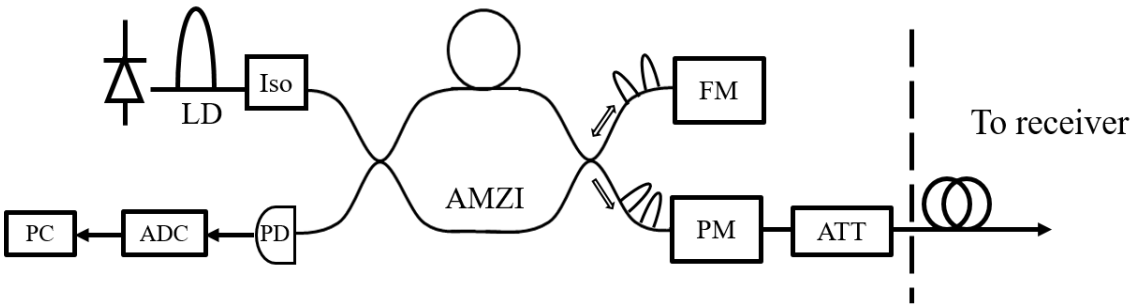


Fig 6.1. Configuration of QRNG integrated in transmitter in BB84 QKD system (LD, laser diode; Iso, isolator; AMZI, asymmetric Mach–Zehnder interferometer; FM, faraday mirror; PM, phase modulator; ATT, attenuator; PD, photon detector; ADC, analog to digital converter; PC, computer)

6.1 Configuration of Proposed QRNG

As shown in Fig.1, our QRNG shares the LD and the AMZI with the transmitter of BB84 time-bin QKD system. The LD emitted light pulses of 1550 nm wavelength, 625MHz and 150 ps duration with random phase fluctuation. The AMZI has two input ports and two output ports. Usually, one input port and one output port are used, and unused ports are closed. We connect a Faraday mirror (FM) to the output port and a high-speed photodetector (PD) to the input port. Only these two devices provide the optical part of the QRNG. Since the time difference generated in the AMZI (800ps) is set to the half of pulse interval from the LD (1.6ns), the reflected pulse can interfere with the adjacent pulse at the input beam splitter of the AMZI. The interference signal intensity is random, because the gain-switched LD provides phase-randomized optical pulses. To avoid the back reflection into the oscillator cavity, an isolator (Iso) is supplied here. An analog to digital converter (ADC) with 12 bits resolution and 5.4 GS/s sampling rate (TI ADC12DJ2700) [84] and computer (PC) were used to extract random number bits from random interference pulse intensities.

6.2 Principle of Proposed QRNG

Pulses A, B from laser source hold 1.6 nano seconds interval. They passed AMZI with 0.8 nano seconds time delay first time. Then, they turned to 4 pulses with 0.8 nano seconds interval at the output. They are reflected by faraday mirror and pass AMZI with 0.8 nano seconds time delay second time. Finally, they interfered at another input of AMZI. The interference signal intensity is random, because the gain-switching Laser Diode provides

phase-randomized optical pulses.

Theoretical model of the setup is established as follows. Suppose the field at port 1 of the AMZI is

$$E_1(t) = \mathrm{A}\exp[i\omega t + i\varphi(t)]. \tag{6-1}$$

where A is the amplitude of electric field, $\omega=\frac{2\pi}{\mathrm{T}}$ (T is the operation period of laser diode) is the optical center angular frequency, and $\varphi(t)$ is the phase of the laser, respectively. Since the amplitude of laser is tunable and could be very stable during the experiment, the amplitude part of field could be regarded as a constant in our scheme, which means A is a constant. The field reflected by faraday mirror in port 2 is

$$E_2(t) = \frac{\mathrm{A}}{\sqrt{2}}\exp[i\omega(t+\Delta T) + i\varphi(t)]. \tag{6-2}$$

The time change $\frac{\mathrm{T}}{2}$ occurs because the pulse passed AMZI with ΔT=T/2 time delay and BS is set as 50:50 transmission ratio. And the field at port 3 of the AMZI is the interference intensity that caused by the reflected pulses holding interval T/2 and they passed AMZI with T/2 time delay second time. Observed signal for port is shown as

$$\begin{aligned}
P_{out} &= |E_2(t)|^2 = E_2(t)E_2^*(t) \\
&= \frac{\mathrm{A}^2}{2}\left(\exp\left[i\omega\left(t+\frac{\mathrm{T}}{2}\right)+i\varphi(t)\right] + \exp\left[i\omega\left(t+\frac{\mathrm{T}}{2}+\frac{\mathrm{T}}{2}\right)+i\varphi(t+\mathrm{T})\right]\right) \\
&* \left(\exp\left[-i\omega\left(t+\frac{\mathrm{T}}{2}\right)-i\varphi(t)\right] + \exp\left[-i\omega\left(t+\frac{\mathrm{T}}{2}+\frac{\mathrm{T}}{2}\right)-i\varphi(t+\mathrm{T})\right]\right) \\
&= \frac{\mathrm{A}^2}{2}\left(2+2\cos\left(\omega\left((t+\mathrm{T})-\left(t+\frac{\mathrm{T}}{2}\right)\right)+\varphi(t+\mathrm{T})-\varphi(t)\right)\right) \\
&= \mathrm{A}^2\left(1+\cos\left(\frac{2\pi}{\mathrm{T}}*\frac{\mathrm{T}}{2}+\varphi(t+\mathrm{T})-\varphi(t)\right)\right) \\
&= \mathrm{A}^2\big(1+\cos\big(\pi+\varphi(t+\mathrm{T})-\varphi(t)\big)\big) \\
&= \mathrm{A}^2\big(1+\cos\big(\varphi(t)-\varphi(t+\mathrm{T})\big)\big)
\end{aligned} \tag{6-3}$$

Phase fluctuation between 2 pulses is $\Delta\theta = \varphi(t) - \varphi(t+\mathrm{T})$. So that, intensity of output

$$I \propto \mathrm{A}^2(1+\cos(\Delta\theta)) + F. \tag{6-4}$$

where F represents the background noise containing, detection and digitization electronics [71]. Other fluctuation, for example, intensity fluctuation from amplified spontaneous emission is negligible on the scale of the phase fluctuations described below [64].

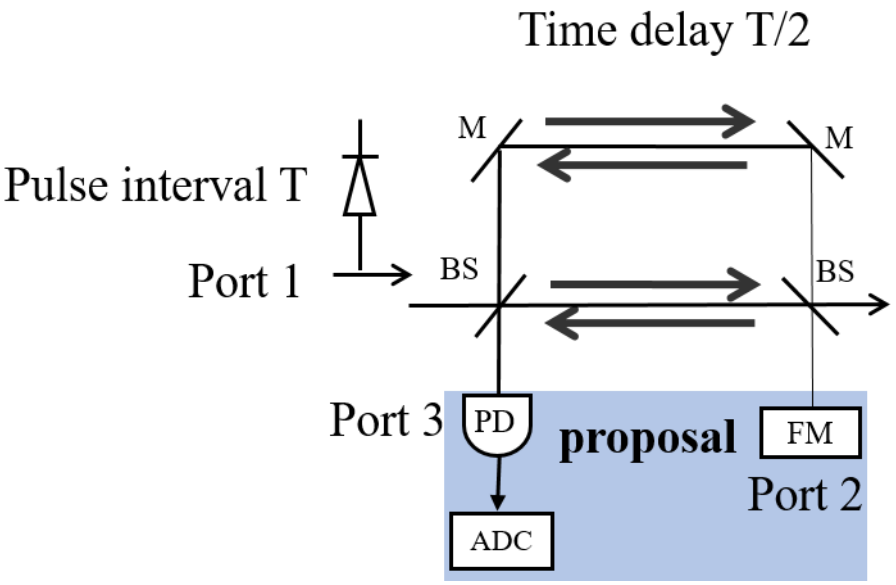


Fig 6.2. Schematic of proposed QRNG containing laser source time-delay system and measurement part (FM, faraday mirror; M, mirror; BS, beam splitter; PD, photon detector; ADC, analog to digital converter)

6.3 Phase noise in a gain-switched laser

In recent decades, semiconductor lasers have become pivotal elements in optoelectronics. They come up with sharp accuracy under sophisticated design that includes complex multi-level structure based on semiconductor gain media. When carrier density is high in the conduction band, due to interband transition stimulated emission occurs and we achieve optical gain. In this experiment a gain-switching distributed feedback laser is working under gain-switching conditions, and the field within the cavity alternately experiences two working regimes: far above threshold and far below threshold. During the former, stimulated emission dominates and coherent optical pulses are emitted. During the latter, the intracavity field is strongly attenuated and significant phase noise occurs.

To be specific, phase noise is a quantum noise that correspond to intrinsic fluctuations in the photon number, carrier number and phase [27]. As research of C. Henry, the quantum noise coming from spontaneous emission can be described with a Langevin rate equation. First, the time variation of the field amplitude is

$$\frac{dE}{dt} = \frac{1}{2}(A - G_{th} + j\Psi)E + U(t). \tag{6-5}$$

where A and Ψ are coefficients of the gain and phase change induced by the stimulated

emission. G_{th} is the threshold gain level. The term $U(t)$ is a complex function describing the rate of change of $E(t)$ due to inclusion of the spontaneous emission in the stimulated emission. The change of the photon number, carrier number and phase in LD can be described as the Langevin rate equation

$$\frac{dS}{dt} = AS - G_{th}S + \frac{a\xi N}{V} + F_S(t) \tag{6-6}$$

$$\frac{d\theta}{dt} = \frac{\alpha a\xi}{2V}(N - \langle N\rangle) + F_\theta(t) \tag{6-7}$$

$$\frac{dN}{dt} = \frac{I}{e} - AS - \frac{N}{\tau_S} \tag{6-8}$$

$$A = \frac{a\xi}{V}N - \frac{a\xi}{V}N_g \tag{6-9}$$

Where S means photon number, a is the differential gain coefficient, ξ is the field confinement factor, N is carrier number, V is the volume of the active region, θ is phase, α is linewidth enhancement factor [27], $\langle N\rangle$ is the time average value of carrier number, I is the injection current, e is the electron charge, τ_S is the electron lifetime, N_g is the electron number at transparency. $F_S(t)$, $F_\theta(t)$ are Langevin force noise which represents the spontaneous emission. As shown in Fig.6.3, red arrows are Langevin force intensity and phase noise generated from green arrow. These noise sources are given by

$$F_S(t) = \sqrt{\frac{V_{SS}}{\Delta t}}\, g_S \tag{6-10}$$

$$F_\theta(t) = \sqrt{\frac{V_{\theta\theta}}{\Delta t}}\, g_\theta = \sqrt{\frac{V_{SS}}{\Delta t}}\frac{g_\theta}{2(S+1)} \tag{6-11}$$

$$V_{SS} = \left[\frac{a\xi}{V}\left(N + N_g\right) + G_{tho}\right]S + \frac{a\xi N}{V} \tag{6-12}$$

where V_{SS} is the variance of autocorrelation. g_S and g_θ are the Gaussian random numbers in ranges of $-1 < g_S < 1$, $-1 < g_\theta < 1$. They are the random source from spontaneous emission and are considered as Gaussian distribution. And Δt is time-step of the calculation. With these equations and parameters in Table 6.1, we can simulate laser operation with different input currents.

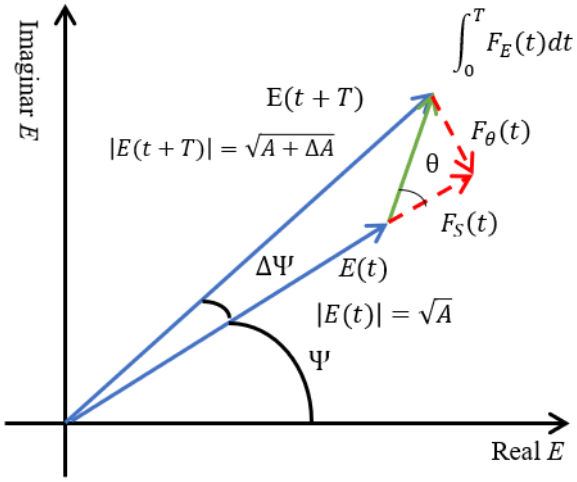


Fig. 6.3 The change of complex field amplitude E(t) during a short time T

Table 6.1 Parameter for simulation of laser [72]

Symbol	Parameter	Value	Unit
a	Slope coefficient of the gain	2.75*10^(-12)	m^3/s
ξ	Optical field confinement factor	0.2	
N_g	Carrier number at transparency	1.89*10^8	
G_{th}	Threshold gain level	5.01*10^11	s^(-1)
τ_S	Electron lifetime	2.79*10^(-9)	s
V	Active region volume	75	μm^(-3)

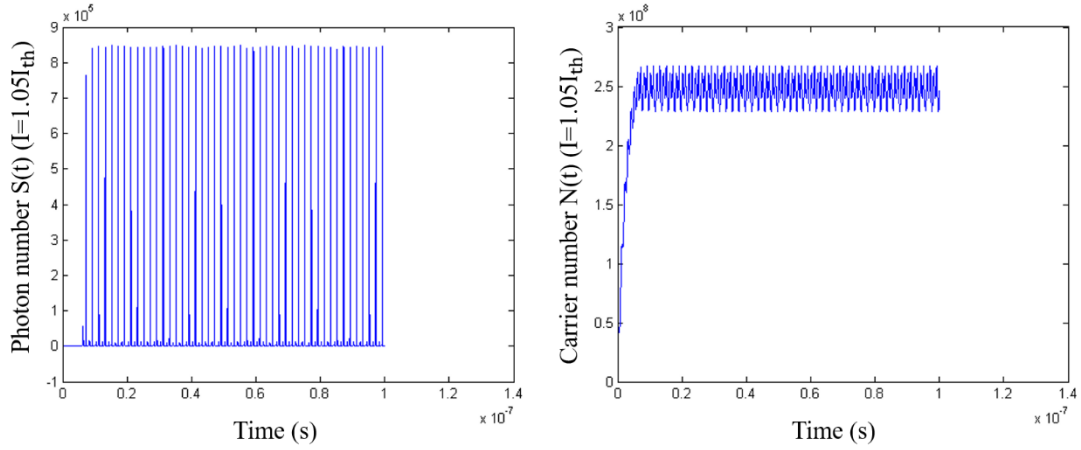


Fig.6.4 Time-variations of the photon number S(t), the carrier number N(t)

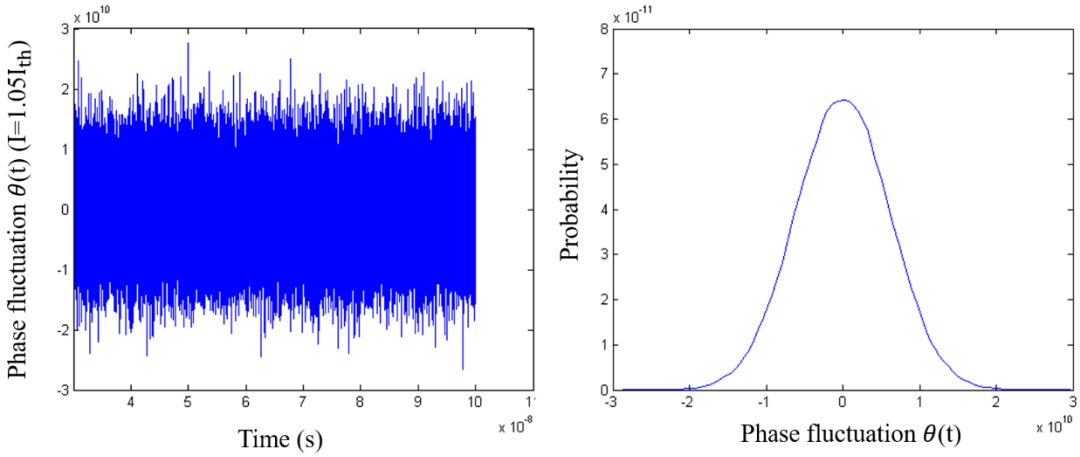


Fig.6.5 Time-variations of the phase fluctuation θ(t), the probability distribution of θ(t)

Fig. 6.4 shows the time-variations of the photon number S(t), the carrier number N(t) with the equation shown above and injection current is set as $I_{th} + 0.8I_{th}\cos(\frac{2\pi t}{10^{-9}})$. A stable state occurs after 5ns shock. The phase fluctuation is shown in Fig. 6.5, and the probability distribution is nearly a Gaussian distribution, because the Langevin force noise is considered as Gaussian distribution. The fluctuation of the lasing frequency is used to describe phase fluctuation in detail.

$$\Delta\nu(t) = \frac{1}{2\pi}\frac{d\theta}{dt} \tag{6-13}$$

In Fig. 6.6, with different injection current $1.05I_{th}$ (a), $1.15I_{th}$ (b), $1.5I_{th}$ (c), $2I_{th}$ (d), frequency fluctuation is about 4GHz, 3GHz, 2GHz, 1.5GHz. This means that the phase

fluctuation decreases when the injection is increasing. When laser is set as reversely biased at the interval, the phase fluctuation will be predominant. Therefore, although, we don't have enough time-delay in interferometer, we can control injection current to optimize phase fluctuation.

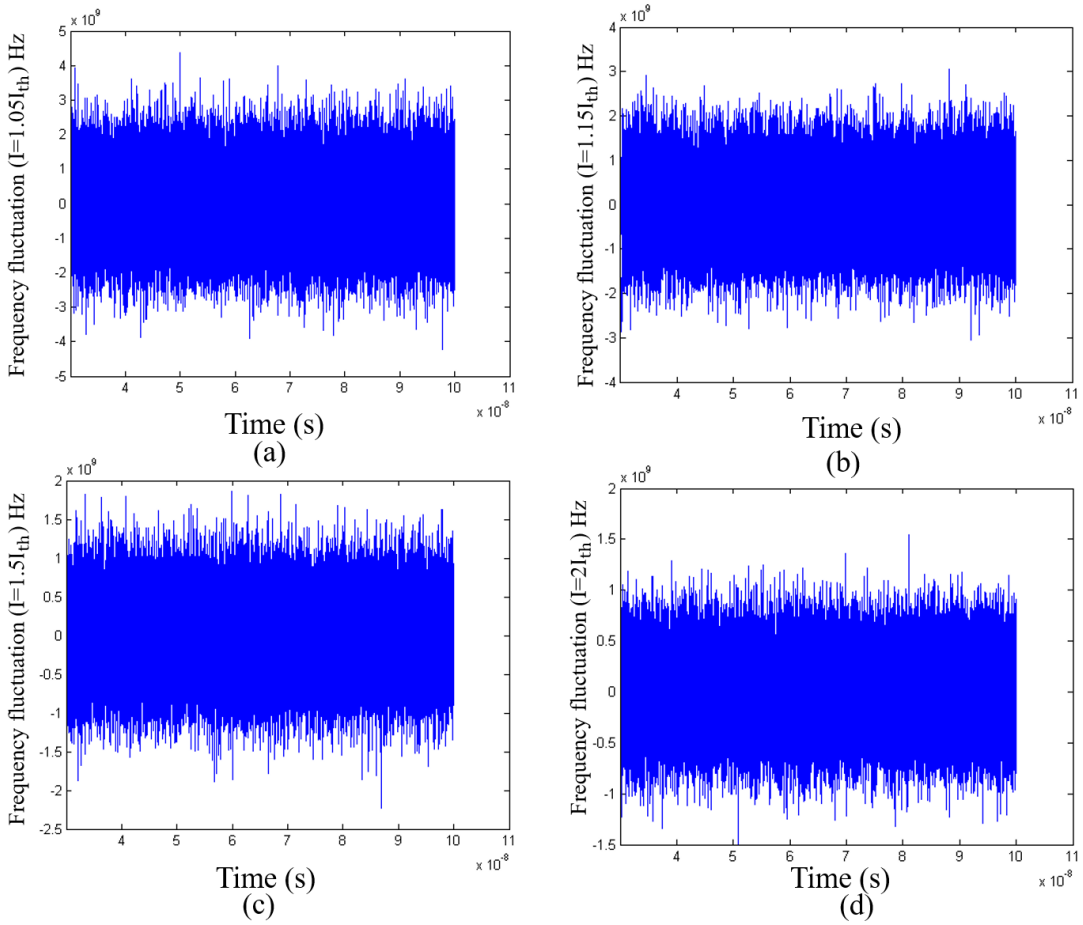


Fig.6.6 Instantaneous fluctuations of the oscillating frequency shift $\Delta\nu(t)$ far from the relaxation regime at different injection

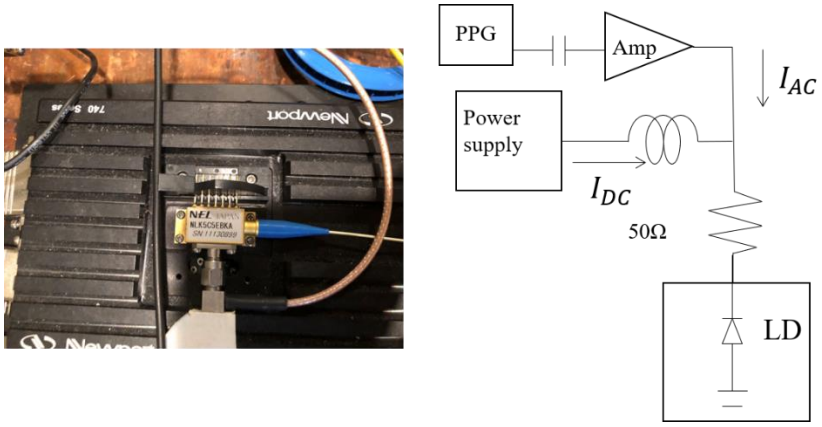


Fig. 6.7 Experimental connection of a Gain-switching laser diode

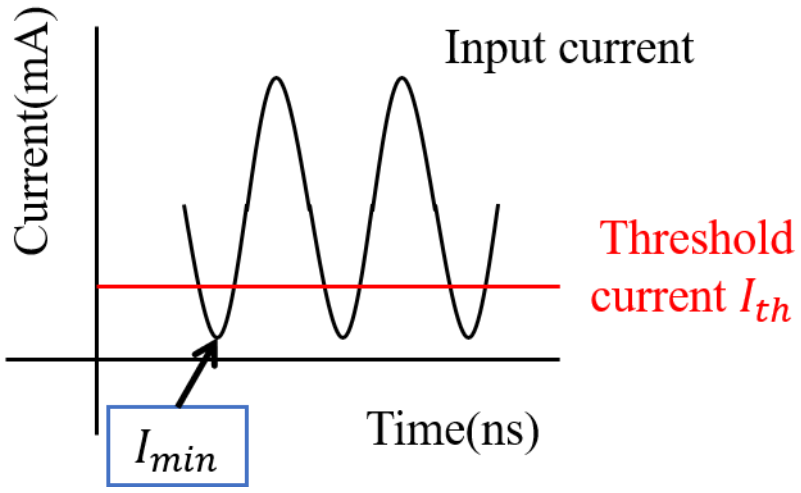


Fig. 6.8 Schematic of Gain-switching laser diode contains Input current and threshold current.

6.4 Gain-switching laser diode operation

As shown in Fig. 6.7, 2 inputs are connecting to a Gain-switching laser diode (NLC5C5EBKA NEL). They are a DC bias current I_{DC} and AC current $I_{AC} = I_{PP}\cos(2\pi ft + \phi_{LD})$, where I_{PP} stands for the peak-to-peak value of the sinusoidal current. The current changes periodically with the frequency f = 625 MHz and an initial phase ϕ_{LD}. The operating condition of the LD was controlled by changing the DC bias current I_{DC}. The sinusoidal signal from a pulse-pattern-generator (PPG) was amplified to

a fixed amplitude V_{PP} = 4.615 V. We estimated the peak-to-peak ac current to the LD as I_{PP} = 92.3 mA, considering the 50Ω load resistance. We define the minimum drive current defined by

$$I_{min} = -\frac{I_{PP}}{2} + I_{DC} \tag{6-14}$$

which refers to the drive current at the bottom of the ac current. In the following, we use normalized excitation to describe the operating condition. The normalized minimum excitation [69] is defined by

$$\Lambda = \frac{I_{min} - I_{th}}{I_{th}} \tag{6-15}$$

Where I_{th} is the threshold current value, which is 9.5mA for this Gain-switching laser diode. The LD was always turned on when $\Lambda > 0$. The LD was turned off during the pulse interval, when $\Lambda < 0$. The turn-off duration increases as the dc bias current decreases, which is obtained as a solution of $I_{AC} + I_{DC} = I_{th}$ with Eq. (6-14). The LD was reversely biased and no current was injected at the minimum, when $\Lambda < -1$. In the next, we control the dc bias current to get an optimized turn-off duration to make sure that laser cavity prior to lasing is empty and the lasing action is triggered entirely by spontaneous emission.

Chapter 7

Random number extraction and Random number test

As described in Chapter 6, phase fluctuation of spontaneous emission from a DFB laser is used as the quantum random source in our proposed QRNG. It is a Gaussian distributed random source as the simulation result. However, in real situation, as equation 6-4, other noise is also contained in our interference intensity result. This part of noise is not quantum noise and could be used by an adversary to predict results of our output. We will optimize the laser operation by control DC current and maximize the randomness of the interferometer intensity. Here, we use postprocessing as described in Chapter 5 to extract the true random number. Firstly, we use the probability distribution of the interferometer intensity to calculate min-entropy which is used to extract uniformly distributed string of numbers. Next, we use the Toeplitz matrix to extract random numbers from raw data. Finally, we use NIST random number test [28], Diehard random number test [29] and autocorrelation ship to test our extracted random numbers.

7.1 Probability distribution of interference intensity

As shown in Chapter 6, ideal probability distribution of phase fluctuation between 2 pulses caused by amplified spontaneous emission obeys Gaussian distribution. When the ideal phase fluctuation is substituted into Eq. (6-4), where the output intensity I is proportional to $(1 + \cos(\Delta\theta))$ (F is neglected firstly), the ideal probability distribution of interference intensity will be the arcsine probability distribution. As shown in Fig. 7.1, probabilty distribution phase fluctuation of $\Lambda = -0.6$ obeys Gaussian distribution with mean (-1.6601*10^8) and variance (4.7137*10^11).

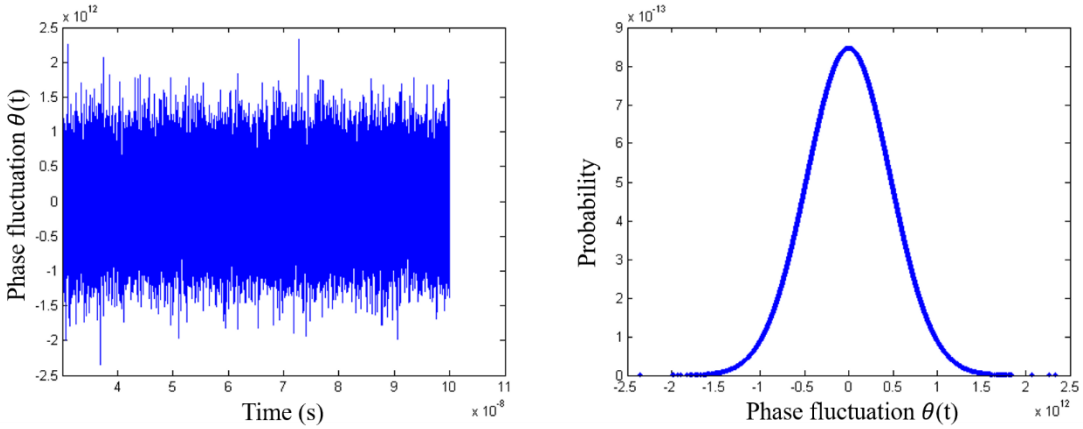


Fig. 7.1 phase fluctuation of $\Lambda = -0.6$, probabilty distribution of phase fluctuation

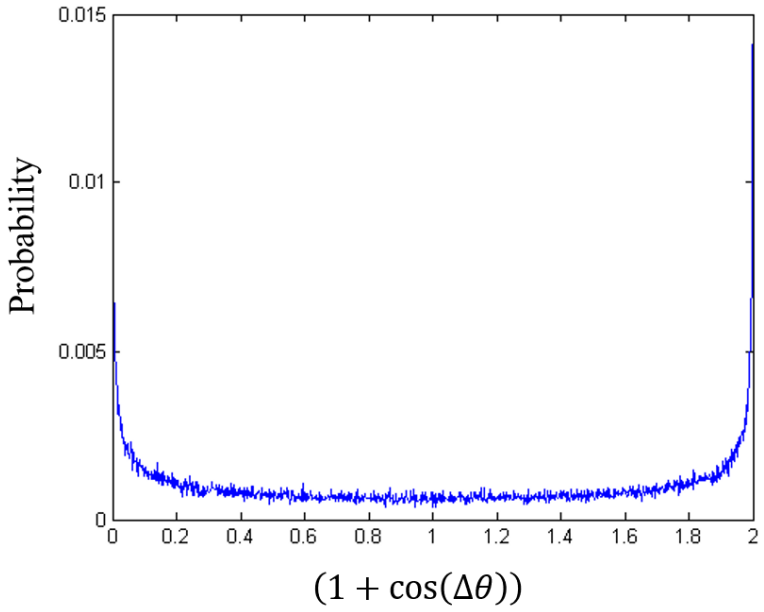


Fig. 7.2 Ideal probability distribution of interference intensity

Probability distribution of $(1+\cos(\Delta\theta))$ is shown in Fig. 7.2 where two peaks occur at two ends of distribution. The mid part of this distribution cold be considered as a uniform distribution. This probability distribution approximates to an arcsine probability distribution function, its mean and its variance are given by:

$$PDF(x) = \frac{1}{\pi\sqrt{(x-a)(b-x)}};$$

$$\mu_x = \frac{a+b}{2}; \tag{7-1}$$

$$var[x] = \frac{1}{8}(b-a)^2$$

Where a and b decide two peaks of this probability distribution.

According to the discussion above, if phase fluctuation is the only fluctuating term, the observed signal would obey an arcsine distribution, the distribution of the cosine of a uniformly distributed phase. However, according to other noise in the output, for example, F part in Eq. (6-4) including photo-detection noise, laser current fluctuations, and digitization errors, and other fluctuation from amplified spontaneous emission, the real probability distribution of interference intensity is not as same as the ideal one. The other noise sources are not guaranteed to be random. Fortunately, the randomness extraction step will remove any non-random effects of these other noise sources, provided that the reduction factor is chosen using the min-entropy of the quantum contribution. So that, we

use ADC to record interference intensity and calculate the probability distribution of interference intensity with different normalized minimum excitation (different laser operation condition). With the probability distribution of interference intensity, we can find out the most probable event to calculate min-entropy.

For statistical testing, more than 1 million samples were recorded 1 time on a fast 14-bit ADC with 3.125GHz sample rates as shown in Fig.7.3. On the board of ADC evaluation module, white circle marked ADC chip (ADC12DJ2700), ADC sampling clock should be adjusted same as clock as input signal. As shown in Fig. 7.4, it is adjusted to meet the 625MHz and 1.25GHz input which is used in our experiment. Two USB 3.0 make sure that our data transmission has high rate. Power is supplied by 2 DC source. TSW14J57EVM is a pattern generator and data capture card which capture up to 1G 16-bit samples at a maximum line rate of 15 Gbps and hold a 16G DDR4 memory.

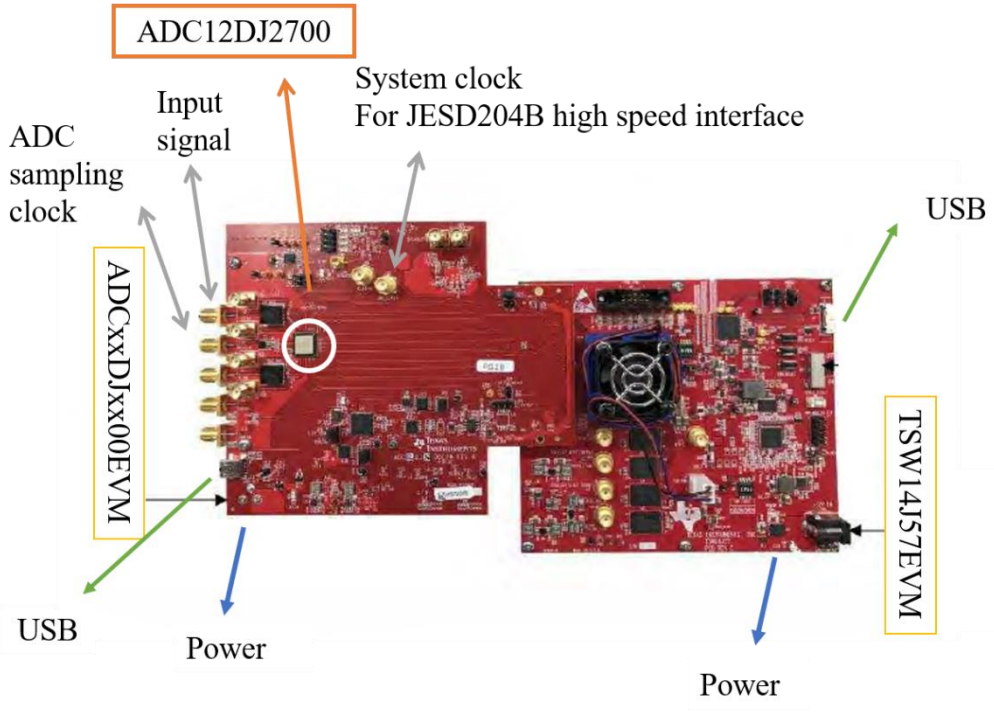


Fig. 7.3 Set up of Analog to Digital Converter (ADC)

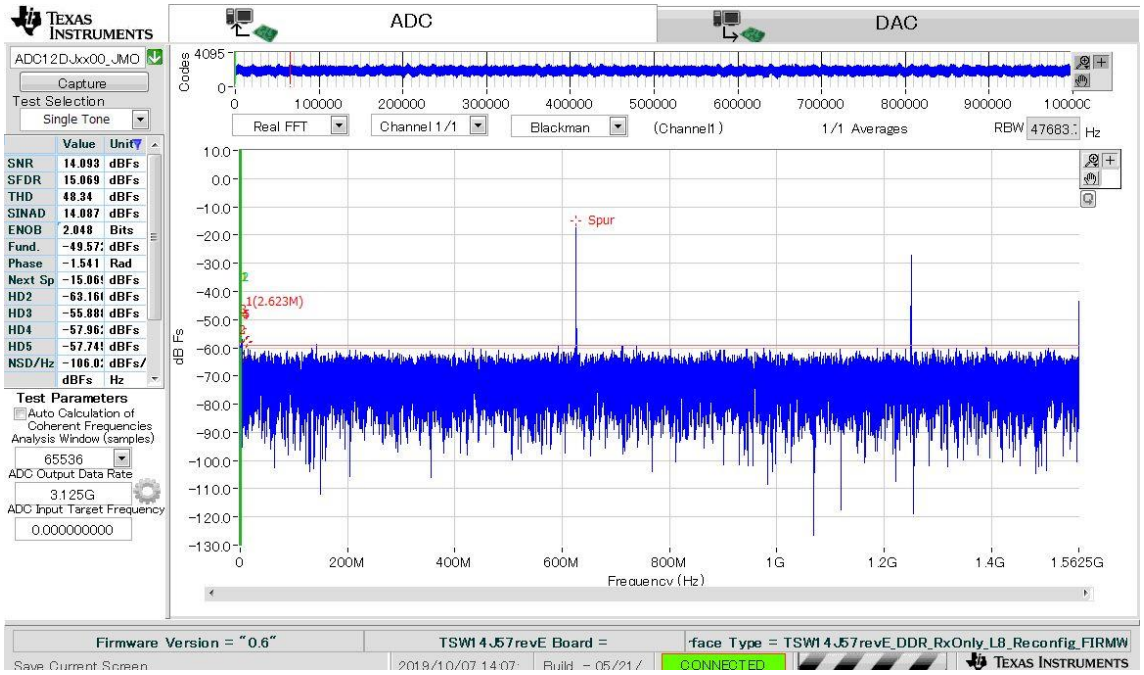


Fig. 7.4 frequency spectrum of Input without noise which is used to adjust sampling rate

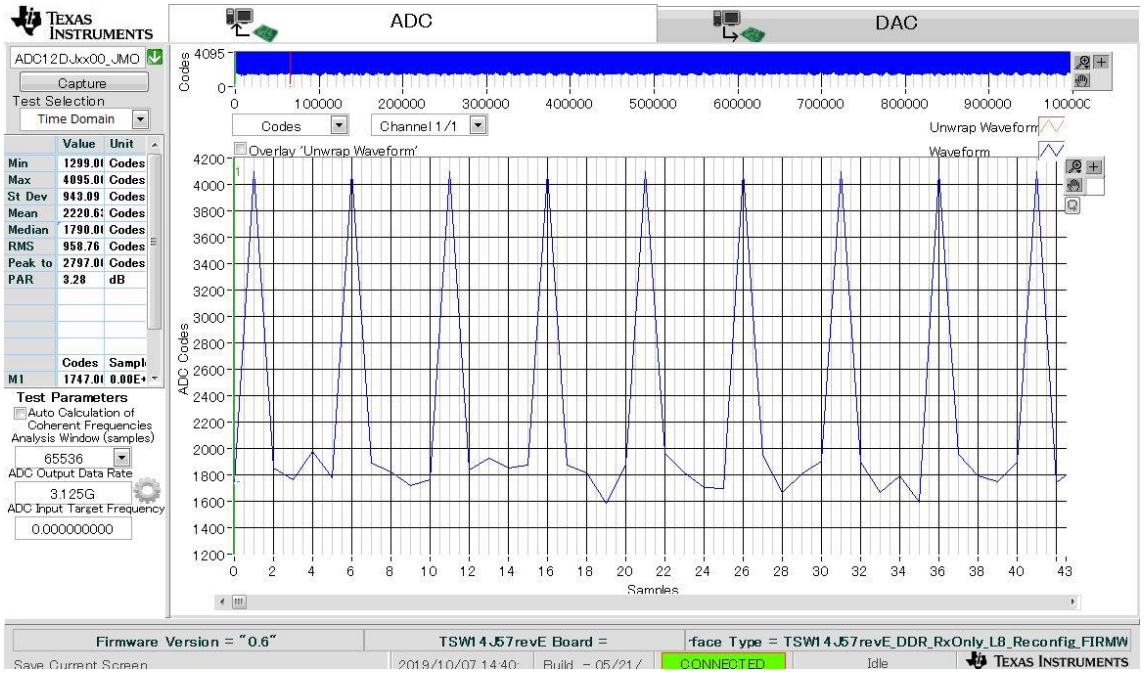


Fig. 7.5 frequency spectrum of Input without noise which is used to adjust sampling rate

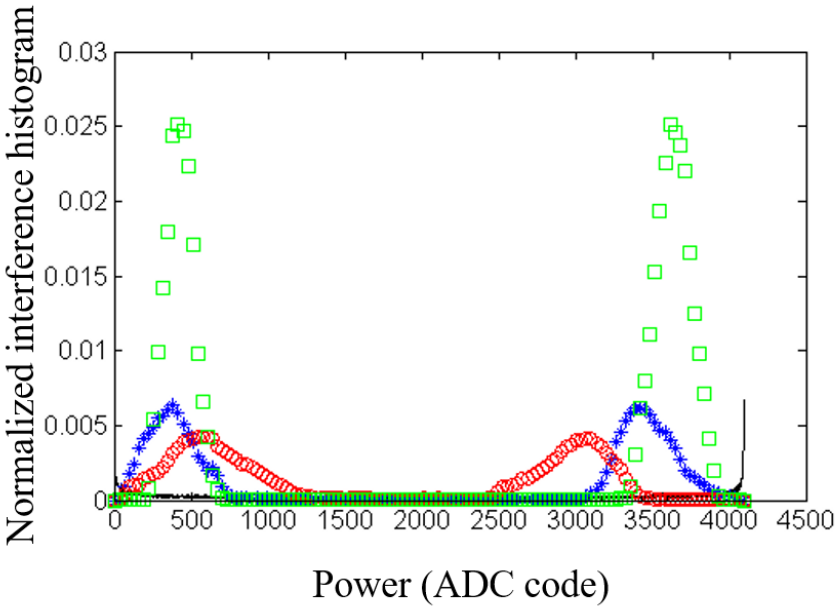


Fig. 7.6 The probability distribution of interference intensity. Green square means experimental interference intensity probability distribution (Λ=−0.5), Blue asterisk means experimental interference intensity probability distribution (Λ=−0.88), Red circle means experimental interference intensity probability distribution (Λ=−0.9), Black line means theoretical interference intensity probability distribution (phase fluctuation as Gaussian white noise)

As shown in Fig. 7.5, some part of input signal is recorded. The setting sample 3.125GHz is 5 times as 625MHz, so that 5 samples record an input pulse. The probability distribution of interference intensity is shown in Fig. 7.6. In this figure, different experimental interference probability distributions with different laser operation are shown, which is Λ=−0.5, −0.88 and −0.9. Theoretical interference intensity probability distribution also is drawn in this figure, we just substitute $\Delta\theta$ with Gaussian distribution into $(1+\cos(\Delta\theta))$. We did more experiments that changing the normalized minimum

excitation from -1.5 to 1, however, the probability of most event become too big to show in one figure clearly. In an addition, 4096 events are recorded, but 128 events are shown in one figure. Our experiment results prove that results of experiment do not obey the ideal arcsine distribution under the influence of flaw from gain switching laser and detection and electrical noise as our discussion above. In the next part, I will use interference intensity probability distribution to calculate min-entropy to distill the random numbers from phase fluctuation in amplified spontaneous emission from laser diode.

7.2 Min-entropy

Randomness extractors transform non-uniformly-distributed sequences into uniformly distributed sequences [79] at the cost of losing a fraction of the bits. In our experiment, this cost might be the photo-detection noise, laser current fluctuations, and digitization errors, and other fluctuation from amplified spontaneous emission, which has no use for our QRNG. The min-entropy

$$\mathrm{H}_{\infty}(X) = -\log_2(\max_{x\in\{0,1\}^n} P_X(x)) \tag{7-2}$$

as Eq. (5-5) shows that it only depends on the weight of the most probable event. A simple illustration of the evaluation process is shown in Fig. 7.7, where the raw-data follows a Gaussian distribution and is digitized by a 3-bit ADC [64]. Hence, the raw-data will be mapped to a binary sequence X with 3 dimensions (n=3 in Eq. (7-2)). The sample point (one of the 8 bins in Fig. 7.7) with maximal probability is '011' (or '100') and its corresponding probability P_{max} can be calculated from its bin area. Note that in Fig. 7.7, three key parameters to determine P_{max} are the standard deviation of Gaussian distribution (σ), the ADC sampling range and the resolution of ADC (3-bit in Fig 5).

Similarly, normalization probability distribution of our experiment can be used to calculate min-entropy. We just need to find out the most probable event in the figure. As Eq. (7-1) and Fig. 7.2, the arcsine distribution is peaked at x = $Power_{min}$ or $Power_{max}$, and because the min-entropy only depends on the weight of the most probable event, the min-entropy of the digitized arcsine distribution only depends on the probability of the first bin (or the last bin). However, in real state, most probable event might be other bins as shown last page, so that we need to calculate every bin area and find the most probable one. Calculation result of min-entropy with different Λ value (-1.5~1) is shown in Fig. 7.8. LD is optimized at Λ=-0.9 and get max min-entropy 7.9 bits. Min-entropy decrease under the influence of an electrical noise and the limited dynamic range of photon detector and ADC.

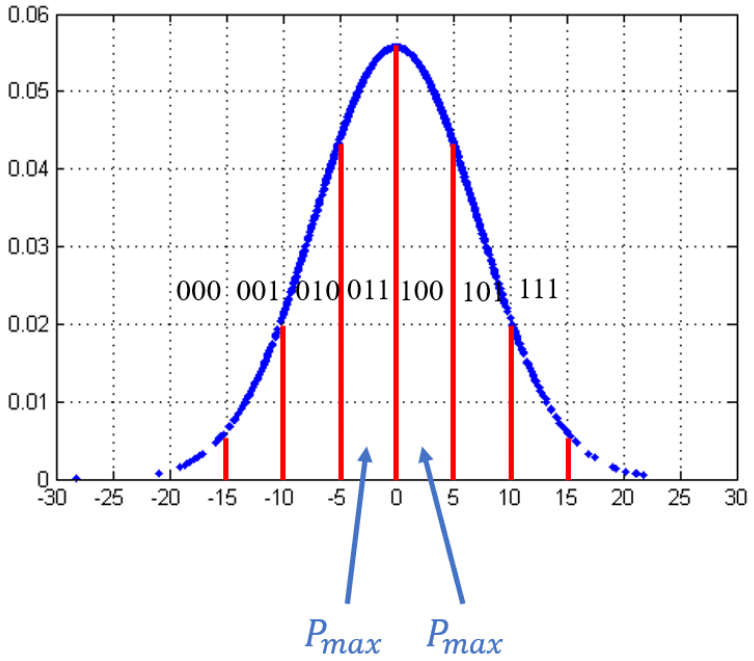


Fig. 7.7. A simple illustration of min-entropy evaluation (toy model). The raw-data follows a Gaussian distribution (μ = 0 and σ = 7) and is digitized by a 3-bit ADC. From Eq. (6), the min-entropy is determined by the sample point x with the maximal probability P_{max}. Here, x equals to the bin of '011' (or '100') and P_{max} can be calculated from its bin area.

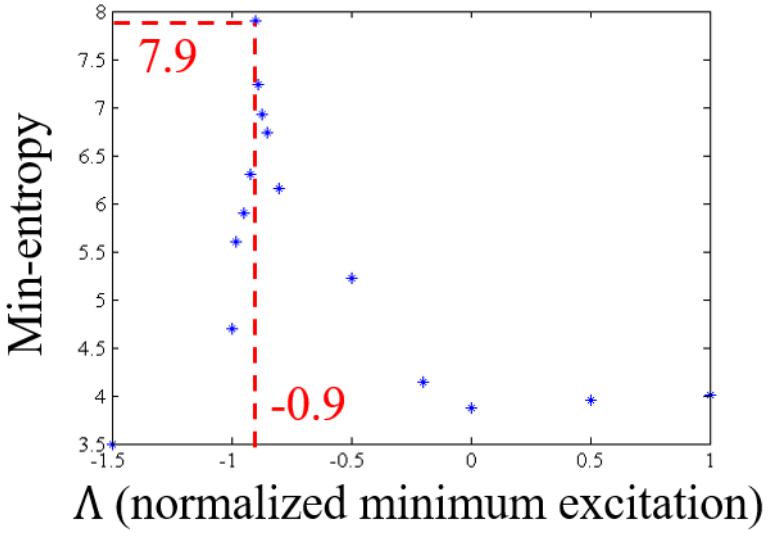


Fig. 7.8. Min-entropy using 12 bits ADC, its x axis represents normalized minimum excitation. We get the biggest Min-entropy at $\Lambda = -0.9$

The optimal Min-entropy of 7.9bits per pulse was obtained with 625MHz clock frequency, random number generation rate will be 4.9375GHz theoretically. 7.9 bits is smaller than the ADC resolution 12 bits, nevertheless, the theoretical generation rate is exceeded the required rate, 5 bits per pulse for a two-decoy BB84 transmitter as shown in Section 4-4.

7.3 Randomness extraction

We use a Toeplitz-hashing extractor here to extract 7.9 min-entropy bits from our raw data. As described in section 5.4.2, flow of this extractor is that 1. Given raw data of size n with a min-entropy of k and a security parameter ε, b is ADC resolution determine the output length to be

$$m = \frac{nk}{b} + 2log\varepsilon \tag{5-7}$$

2. Construct a Toeplitz matrix with an n+m-1 random-bit seed. 3. The extracted random bit string is obtained by multiplying the raw data with the Toeplitz matrix. In our QRNG experiment, the n=$2^{12} = 4096$ data from 12 bits ADC is chosen, and min-entropy of raw data from quantum source is 7.9, $\frac{nk}{b}$ is calculated as 4096*(7.9/12) = 2697. If we set m=2569, ε will be resulted in 2^{-64}. However, the random seed from pseudorandom number sequence will reduce the randomness of our QRNG, and a requirement of an extra physical random number generator disobeys our original intention that building a QRNG integrated into a transmitter of BB84 QKD system. Here, we use a seed improvable Toeplitz-hashing extractor to solve this problem. Flow chart of this extractor is shown in Fig. 7.9 [86].

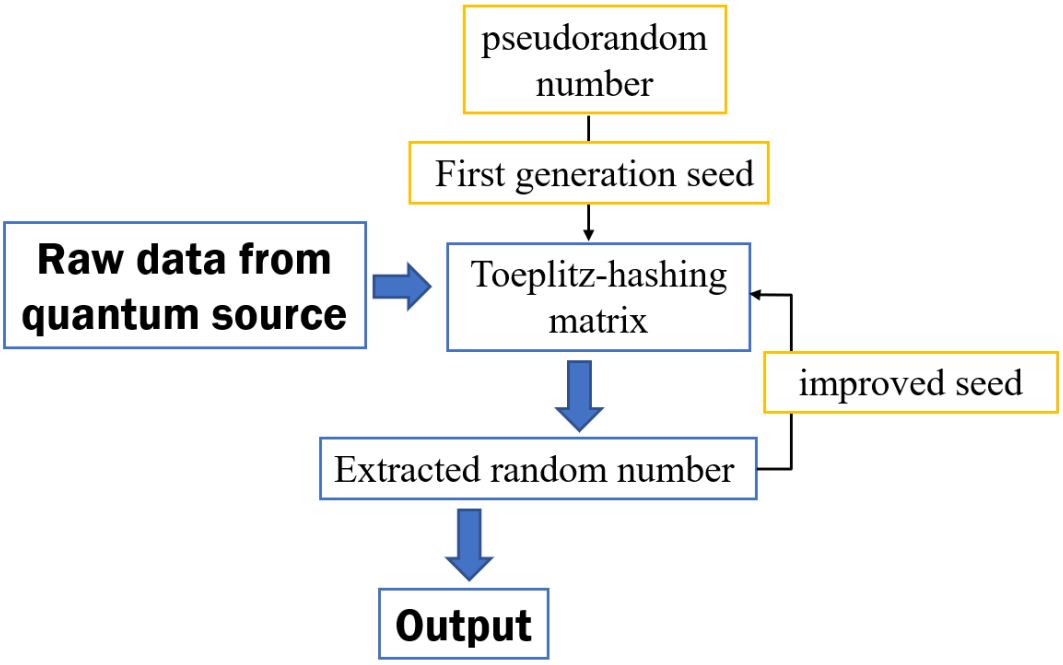


Fig. 7.9 Flow chart of a seed improvable Toeplitz-hashing extractor

Seed from pseudorandom number generated by PC is used to generate Toeplitz matrix firstly. Then, raw data from our quantum source is input into Toeplitz matrix and get an extracted random number string. This string can be a part of a second-generation Toeplitz matrix. In addition, the insertion of the extracted sequence into the second-generation Toeplitz matrix is not limited to the case of inserting at one place and may be inserted at multiple places or continuously. Since the second generation has higher randomness extractor matrix as compared to the first generation, the distillation process performed through such a second-generation extractor matrix is possible to output a random number with improved randomness. As a result, the output random numbers generated in the second generation have further improved unpredictability and Non-Reproducibility. Similarly, when the third, fourth, fifth generation Toeplitz extraction matrix is used, randomness will be much higher.

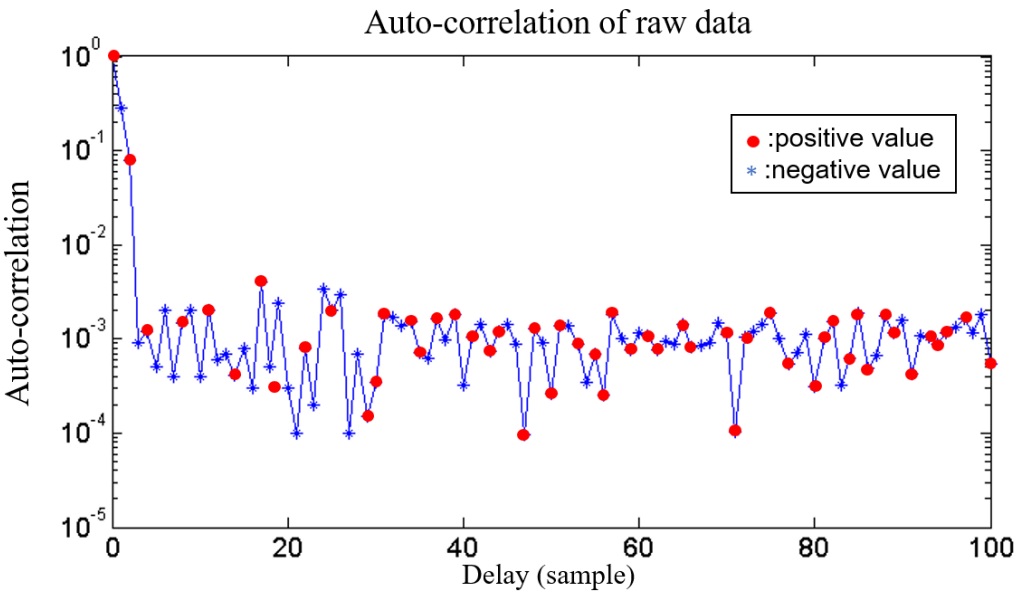
7.4 Random number test

The autocorrelations are often used to evaluate the randomness of a random number string [25, 77, 85]. An ordered sequence of random variables is compared to itself, which is the definition of autocorrelation function in statistics. Every sequence with no phase difference is similar to itself, in which case the autocorrelation function has the greatest value. If the components of the sequence are correlated with each other (no longer

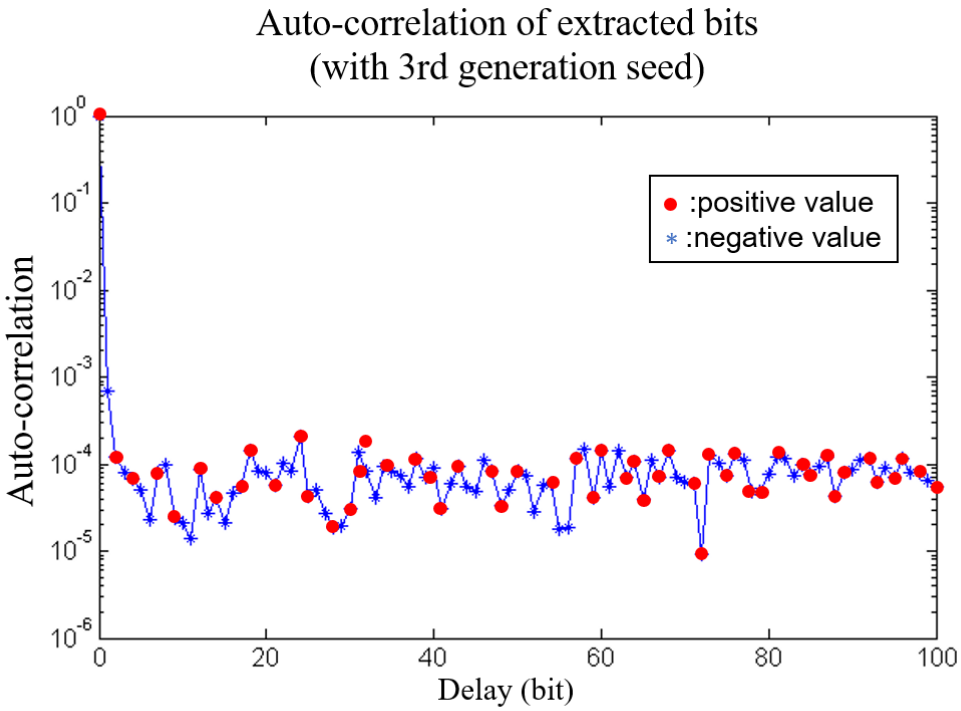
random), then the values calculated by the following correlation value equation are no longer zero, and such components are autocorrelated. The autocorrelation coefficient R of a sequence X is defined as

$$R(j) = \frac{E[(X_i - \mu)(X_{i+j} - \mu)]}{\sigma^2} \tag{7-3}$$

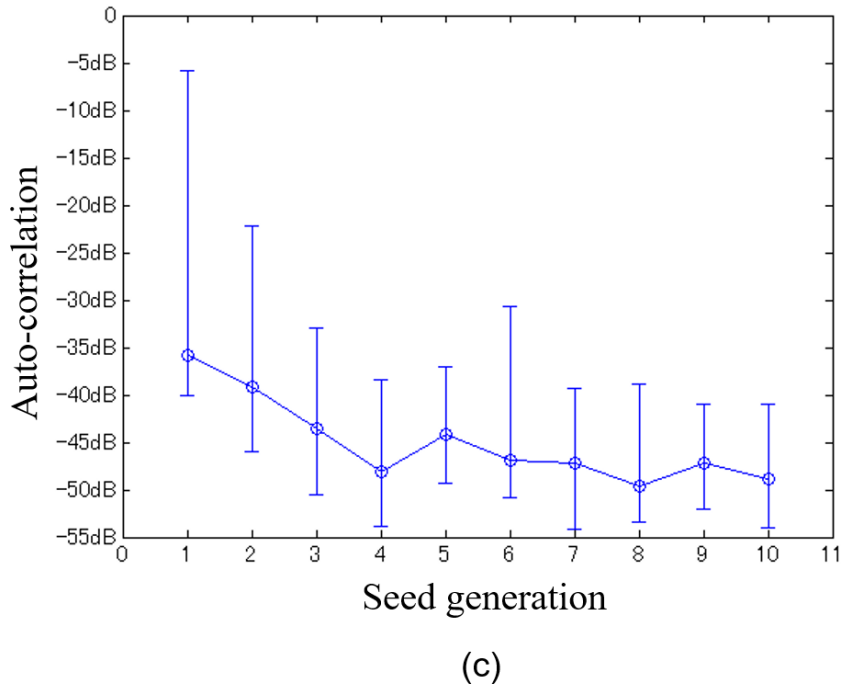
where $E[\bullet]$ is the expected value operator, j is the sample delay (or shift),μ and σ are the mean and the standard deviation of X. The value range of correlation value R is [-1,1], where 1 is the maximum positive correlation value, -1 is the maximum negative correlation value, and 0 is irrelevant. Fig. 7.10 (a) shows the autocorrelation results of our raw-data with 100 samples delay. The low values of the autocorrelation between raw samples (12-bit per sample) verify the assumption of our physical model for min-entropy evaluation. A slightly large coefficient at the 2nd delay sample is attributed to the finite bandwidth of our photodetector. After post-processing, the autocorrelation with 100 bits delay is substantially reduced as shown in Fig. 7.10 (b). Autocorrelation of raw data is around -30dB and auto-correlation of extracted random string with 3rd generation seed is around -40dB. This proves that our randomness extractor improves the quality of random numbers. Because the calculation time is positive to the loop numbers, so we want to make a trade-off between the calculation time and randomness. In Fig. 7.10 (c), Auto-correlation stays around -45dB when seed is improved more than 3 times. Here, the error bar means the autocorrelation of different numbers of delays. So that, in our QRNG, we will use the third-generation seed Toeplitz-hashing extractor.


Auto-correlation of raw data
Auto-correlation
Delay (sample)
:positive value
:negative value
10^0
10^-1
10^-2
10^-3
10^-4
10^-5
0
20
40
60
80
100

(a)


Auto-correlation of extracted bits
(with 3rd generation seed)
Auto-correlation
Delay (bit)
:positive value
:negative value
10^0
10^-1
10^-2
10^-3
10^-4
10^-5
10^-6
0
20
40
60
80
100

(b)



(c)

Fig.7.10 Auto-correlation of raw data, extracted random string (with 3rd generation seed) and extracted random string with different seed generation

In addition, several standard statistic tests, for example, Diehard [28], NIST [29] are used to test our random number bit strings. In detail, 15 items are included in NIST test they are 1. The Frequency (Monobit) Test, 2. Frequency Test within a Block, 3. The Runs Test, 4. Tests for the Longest-Run-of-Ones in a Block, 5. The Binary Matrix Rank Test, 6. The Discrete Fourier Transform (Spectral) Test, 7. The Non-overlapping Template Matching Test, 8. The Overlapping Template Matching Test, 9. Maurer's "Universal Statistical" Test, 10. The Linear Complexity Test, 11. The Serial Test, 12. The Approximate Entropy Test, 13. The Cumulative Sums (Cusums) Test, 14. The Random Excursions Test and 15. The Random Excursions Variant Test. P_{value} is a evaluate parameter in this test. It is a probability (under the null hypothesis of randomness) that the chosen test statistic will assume values that are equal to or worse than the observed test statistic value when considering the null hypothesis. The value range of P_{value} is [-1,1], if P_{value} is close to 0, we will reject hypothesis and sequence is not random. In NIST test, if $P_{value} < 0.01$, sequence is considered as not random. For example, in the Frequency (Monobit) Test, the value 0 and 1 in a string should be the same number, both

50% appearance frequency. If it is a 50:50 string, we think it passed test, and the proportion of passed string to the total string is P_{value}. Diehard is a similar randomness test as NIST random number test. The result of 2 tests is shown in Fig. 7.11.

NIST results of the Toeplitz-hashing output. Data size is 100 Mbits (10 sequences with each sequence around 10 Mbits). To pass the test, P-value should be larger than the lowest significant level $\alpha = 0.01$, and the proportion of sequences satisfying $P > \alpha$ should be greater than 0.9. Where the test has multiple P-values, the worst case is selected. (b) is the Diehard results of the Toeplitz-hashing extractor output. Data size is 10 Mbits. A Kolmogorov-Smirnov (KS) test is used to obtain a final P-value from the case of multiple P-values. Successful P-value is $0.01 \leq P \leq 0.99$.

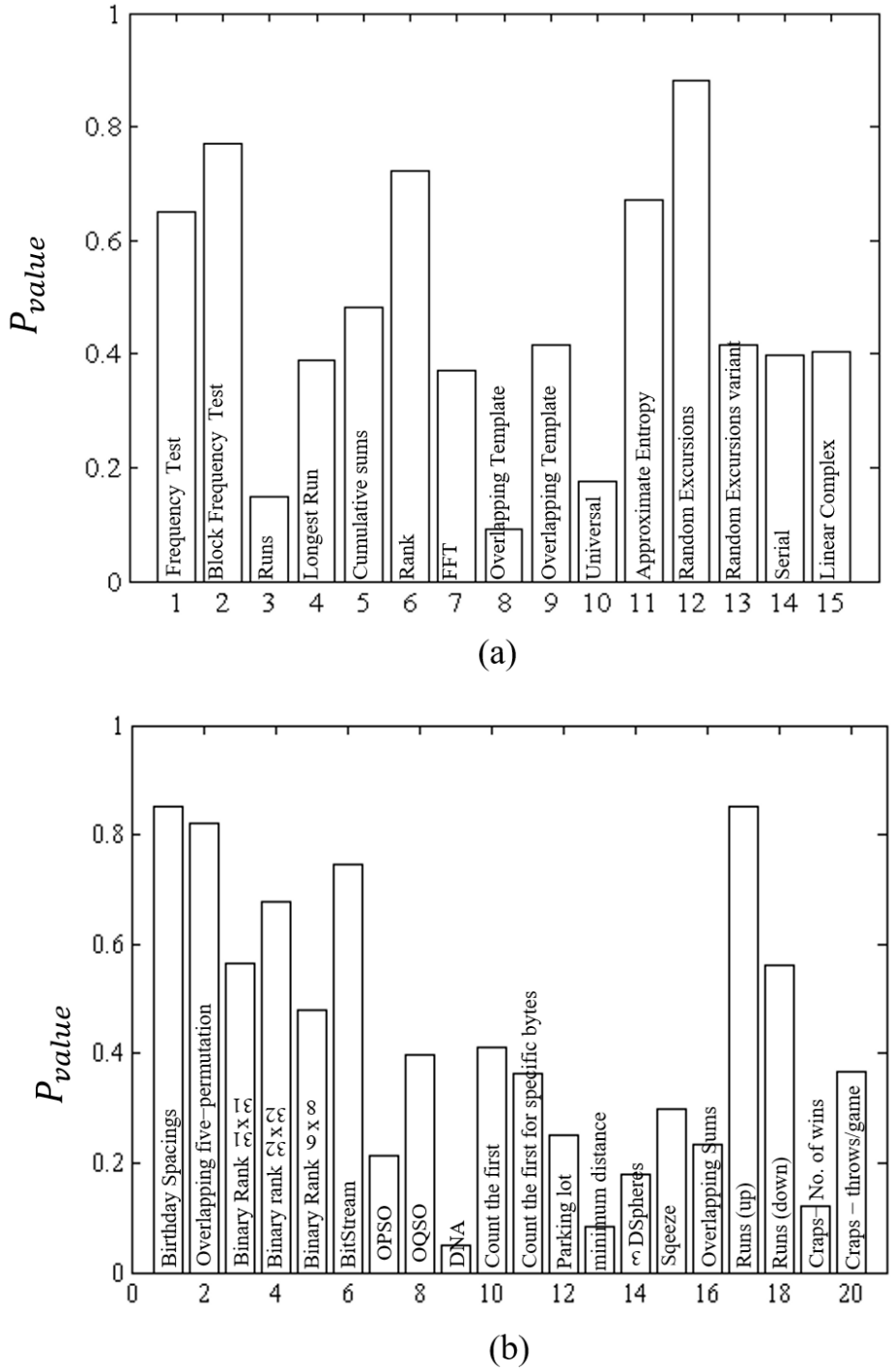


Fig. 7.11 NIST results (s) and Diehard results (b) of extracted random number string

Chapter 8

Conclusion

In this thesis, we have investigated the transmitter of BB84 QKD protocol. We propose the dual-parallel modulator to remove a state preparation flaw in the transmitter and we build up a quantum random number generator integrated into this transmitter.

In the first part of this thesis, we introduce the state preparation flaw caused by the fluctuation in the voltage applied to the phase modulator supplying the phase difference for phase encoding BB84 protocol. In addition, we propose the dual-parallel modulator (DPM) to take place of the conventional dual-drive modulator (DDM), and prove the superiority theoretically and experimentally [90]. We considered two ways to change the voltages supply to simulate the fluctuation. We compare the fidelity and the quantum state tomography to evaluate the state preparation flaw quantitatively. The fidelity of sent states using DPM was kept almost 1 for the voltage deviation range of this experiment, while the states generated by DDM was affected by the voltage deviation. Finally, we calculate the final key generation rate and make a conclusion that DPM is robust to the fluctuation in the modify voltage than DDM.

In the second part of this thesis, we propose a simple construction of a quantum random number generator (QRNG) by adding only a few devices to a time-bin BB84 QKD transmitter to replace the external random number generators supporting the operation of BB84 QKD system [91]. We optimize laser operating condition to maximize min-entropy 7.9 bits and the random number generation rate will be up to 4.9375GHz theoretically. It meets the requirement of a transmitter in a decoy state BB84 QKD system (containing 2 bits for bit value, 2 bits for state basis, 1 bit for intensity of decoy state). We use randomness extraction with seeds from quantum source and post-processing analysis to generate the random number bits passing NSIT test and Diehard test. We also calculate the autocorrelation of raw and extracted bits to find a trade-off between running time and randomness.

However, there are a few questions during my work. For example, in the first part, we consider that the relationship between the fluctuation in power supply and the phase modulation error is linear without strict verification experimentally. This will bring some error to our result. In addition, we consider the fluctuation in power supply in low

frequency used in our experiment is ignorable and use an artificial fluctuation to simulate the the fluctuation in high frequency. This will bring another error to our result.

In the second part, our QRNG work well under 625MHz system clock frequency. However, with higher system clock frequency, in stance, more than 2GHz, pulse interval might be too small and min-entropy per pulse might not meet the requirement of decoy state QKD system (5 bits per pulse). One solution is that we could expand time-delay in the interfermetor, for example, $\frac{3T}{2}$ in our interferometer (T: the period of laser diode output), and interference between pulses with $3T$ interval will happen. Through this way, phase correlationship of raw data will decrease and min-entropy per pulse will be qualified. Another method to solve this problem is that an extra time delay could be added to the output of the interferemetor where there was a faraday mirror. Then we can direct the interference result with a director after this extra time delay. In our furture reaserch, we will try to exclude errors mentioned before or estimate the error to amend our result.

Acknowledgements

I would like to express my gratitude to all those who helped me during the long phase in writing this thesis.

A special acknowledgement should be shown to Professor Akihisa Tomita, from whose guidance I benefited greatly. To my best appreciate, I am grateful to him for the considerable patience during the entire research procedure. He brings me generous assistance when errors and troubles happened in the entire process. If there is no help from my supervisor, it was impossible for me to finish a dissertation of appropriate standard. Furthermore, his understandings for students and the spiritual encouragements are always available in support. It is my honor to have Professor Tomita supervise me on my work.

I am particularly indebted to Yui Kadozawa and Mai Tanaka who taught me how to operate an experiment and made the experiment system together. I would like to thank Atsushi Okamoto for his helpful comments and advices regarding this thesis. I wish to extend my thanks to Tetsuya Asai and Masayuki Ikebe for having insightful discussions in the course of this work. I also want to thank Kazuhisa Ogawa and Kosuke Fukui who supplied me with advice.

In addition, I will thank to all members in the laboratory who gave the care to me during my life of studying aboard. Finally, I would like to express my gratitude to my parents and my girlfriend for constant support.

Reference

[1] C. H. Bennett and G. Brassard, “Quantum cryptography: public key distribution and coin tossing,” Proc. IEEE Int. Conf. Comput. Syst. Signal Process., Bangalore, India, 175–179 (1984).

[2] H.-K. Lo, M. Curty, and K. Tamaki, “Secure quantum key distribution,” Nat. Photonics 8(8), 595–604 (2014).

[3] A.R.Dixon, Z.L.Yuan, J.F.Dynes, A.W.Sharpe and A.J.Shields, “Gigaherts decoy quantum key distribution with 1 Mbit/s secure key rate” Opt. Express, 16(23), 18790-18797 (2008).

[4] S. Wang, W. Chen, J. Guo, Z. Yin, H. Li, Z. Zhou, G. Guo and Z. Han, “2 GHz clock quantum key distribution over 260 km of standard telecom fiber” Opt. Letters, 37(6), 1008-1010 (2012).

[5] S. Wang, W. Chen, Z. Yin, D. He, C. Hui, P. Hao, G. Yuan, C. Wang, L. Zhang, J. Kuang, S. Liu, Z. Zhou, Y. Wang, G. Guo and Z. Han, “Practical gigahertz quantum key distribution robust against channel disturbance” Opt. Letters, 43(9), 2030-2033 (2018).

[6] S. Wang, D. He, Z. Yin, F. Lu, C. Cui, W. Chen, Z. Zhou, G. Guo and Z. Han, “Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system” Phys. Rev. X, 9(2), 021046(2019).

[7] R. J. Hughes, G. L. Morgan, and C. G. Peterson, “Quantum key distribution over a 48 km optical fibre network,” J. Mod. Opt. 47(2–3), 533–547 (2000).

[8] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, “The SECOQC quantum key distribution network in Vienna,” New J. Phys. 11(7), 075001 (2009).

[9] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, “Field test of quantum key distribution in the Tokyo QKD network,” Opt. Express 19(11), 10387–10409 (2011).

[10] D. Stucki, M. Legré, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, L. Monat, J.-B. Page, D. Perroud, G. Ribordy, A. Rochas, S. Robyr, J. Tavares, R. Thew, P. Trinkler, S. Ventura, R. Voirol, N. Walenta, and H. Zbinden, “Long-term performance of the SwissQuantum quantum key

distribution network in a field environment," New J. Phys. 13(12), 123001 (2011).

[11] S. Wang, W. Chen, Z. Yin, H. Li, D. He, Y. Li, Z. Zhou, X. Song, F. Li, D. Wang, H. Chen, Y. Han, J. Huang, J. Guo, P. Hao, M. Li, C. Zhang, D. Liu, W. Liang, C. Miao, P. Wu, G. Guo and Z. Han, "Field and long-term demonstration of a wide area quantum key distribution network" Opt. Express, 22(18), 21739-21756(2014).

[12] Y. Mao, B.-X. Wang, C. Zhao, G. Wang, R. Wang, H. Wang, F. Zhou, J. Nie, Q. Chen, Y. Zhao, Q. Zhang, J. Zhang, T.-Y. Chen, and J.-W. Pan. "Integrating quantum key distribution with classical communications in backbone fiber network," Opt. Express 26(5), 6010–6020 (2018).

[13] P. W. Shor and J. Preskill, "Simple proof of the BB84 quantum key distribution system," Phys. Rev. Lett. 85(2), 441 (2000).

[14] K. Tamaki, M. Curty and M. Lucamarani, "Decoy-state quantum key distribution with a leaky source," New J. Phys. 18, 065008 (2016).

[15] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," Quantum Inf. Comput, 4(5), 325–360 (2004).

[16] K. Yoshino, M. Fujiwara, K. Nakata, T. Sumiya, T. Sasaki, M. Takeoka, M. Sasaki, A. Tajima, M. Koashi, and A. Tomita, "Quantum key distribution with an efficient countermeasure against correlated intensity fluctuations in optical pulses," Npj Quantum Inf. 4(1), 8 (2018).

[17] S. M. Barnett, B. Huttner, and S. J. Phoenix, "Eavesdropping strategies and rejected-data protocols in quantum cryptography", J. Modern Opt. 40(12), 2501–2513 (1993).

[18] K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, "Loss-tolerant quantum cryptography with imperfect sources," Phys. Rev. A 90(5), 052314 (2014).

[19] Xiongfeng Ma, Xiao Yuan, Zhu Cao, Bing Qi and Zhen Zhang, "Quantum random number generation," Npj Quantum Inf. 2. 16021 (2016)

[20] Jennewein, T., Achleitner, U., Weihs, G., Weinfurter, H. & Zeilinger, A. "A fast and compact quantum random number generator." *Rev. Sci. Instrum.* **71**, 1675–1680 (2000).

[21] Dynes, J. F., Yuan, Z. L., Sharpe, A. W. & Shields, A. J. "A high speed, postprocessing free, quantum random number generator." *Appl. Phys. Lett*. **93**, 031109 (2008).

[22] Fürst, H. *et al*. "High speed optical quantum random number generation." *Opt. Express* **18**, 13029–13037 (2010)

[23] Symul, T., Assad, S. & Lam, P. K. "Real time demonstration of high bitrate quantum random number generation with coherent laser light." *Appl. Phys. Lett.* **98**, 231103 (2011).

[24] Williams, C., Salevan, J., Li, X., Roy, R. & Murphy, T. "Fast physical random number generator using amplified spontaneous emission". *Opt. Express* **18**, 23584–23597 (2010).

[25] Nie, Y.-Q. *et al*. "The generation of 68 gbps quantum random number by measuring laser phase fluctuations." *Rev. Sci. Instrum*. **86**, 063105 (2015).

[26] Charles H. Henry, "Phase Noise in Semiconductor Lasers." JOURNAL OF LIGHTWAVE TECHNOLOGY, vol LT-4, NO. 3, (1986).

[27] Henry, C. H. “Theory of the linewidth of semiconductor lasers.” IEEE J. Quant. Electron. 18, 259–264 (1982).

[28] https://webhome.phy.duke.edu/~rgb/General/dieharder.php

[29] https://csrc.nist.gov/projects/random-bit-generation

[30] Bill Thayer, The Histories of Polybius, pp. 217-219, 1927.

[31] Diffie, W.; Hellman, M.E. "New directions in cryptography". IEEE Transactions on Information Theory. 22 (6): 644–654. 1976.

[32] Shannon, Claude. "Communication Theory of Secrecy Systems". Bell System Technical Journal. 28 (4): 656–715.1949.

[33] Hui Chen, et al, "Liangzibaomitongxinyinlun", Beijing institute of technology press, pp.76-78, 2010.

[34] Kahn, David (second edition), “The Codebreakers: the story of secret writing”, Scribners, p.235, 1996.

[35] Merkle, Ralph C "Secure Communications Over Insecure Channels". Communications of the ACM. 21 (4): 294–299. 1978.

[36] Heisenberg, W. "Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik", *Zeitschrift für Physik* (in German), **43** (3–4): 172–198, 1927.

[37] Wootters, William; Zurek, Wojciech. "A Single Quantum Cannot be Cloned". *Nature*. **299**: 802–803.1982.

[38] A. Ruiz-Alba, et all, ISSN 1889-8297 / Waves · 2011

[39] Changxin Pei, *et all*, "quantum communication", Xian electronic technology university press, pp.67-69, 2013.

[40] A. Tomita, "Quantum information for engineers", Morikita press,pp.165, 2017.

[41] D. Gottesman, *et al*., Quantum Information and Computation **4** (5), pp.325-360, 2004.

[42] Y. Koashi, K. Koshiba：量子暗号理論の展開, pp.16-19, 2008

[43] K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, “Loss-tolerant quantum cryptography with imperfect sources,” Phys. Rev. A 90(5), 052314 (2014).

[44] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, “Practical decoy state for quantum key distribution,” Phys. Rev. A 72(1), 012326 (2005).

[45] W.-Y. Hwang, “Quantum key distribution with high loss: toward global secure communication,” Phys. Rev. Lett. 91(5), 057901 (2003).

[46] X.-B. Wang, “Beating the photon-number-splitting attack in practical quantum cryptography,” Phys. Rev. Lett. 94(23), 230503 (2005).

[47] Joseph Valasek, "Properties of Rochelle Salt Related to the Piezo-Electric Effect", Physics Review, Vol XIX, No. 478, (1922).

[48] Weis, R. S.; Gaylord, T. K.. "Lithium Niobate: Summary of Physical Properties and Crystal Structure". *Applied Physics A: Materials Science & Processing*. **37** (4): 191–203.1985.

[49] T. Kawanishi, T. Sakamoto, A. Chiba, M. Izutsu, K. Higuma, J. Ichikawa, T. Lee, and V. Filsinger, "High-speed dual-parallel Mach-Zehnder modulator using thin lithium niobate substrate," Proc. OFC/NFOEC, San Diego, CA, USA, 1–3 (2008).

[50] Y. Nambu, T. Hatanaka and K. Nakamura “B84 quantum key distribution system based on silica-based planar lightwave circuits” Jpn. J. Appl. Phys. Lett. **43**(8B), 1109-1110 (2004).

[51] D. F. V. James, P. Kwiat, W. Munro, and A. White, “Measurement of qubits,” Phys. Rev. A **64**, 052312 (2001).

[52] Matthias Christandl and Renato Renner, Physic review letters, PRL 109, 120403. 2012.

[53] G. L. Roberts, M. Pittaluga, M. Minder, M. Lucamarini, J. F. Dynes, Z. L. Yuan and A. J. Shields “Pattern-effect-free intensity modulator for secure decoy-state quantum key distribution”, Opt. Letters, **43**(20), 5110-5113 (2018).

[54] J. Liu, H. Ding, C. Zhang, S. Xie and Q. Wang, “Practical Phase-Modulation Stabilization in Quantum Key Distribution via Machine learning” Phys. Rev. Applied **12**(1), 014059 (2019).

[55] Miguel Herrero-Collantes, Juan Carlos Garcia-Escartin, “Quantum Random Number Generators” Reviews of Modern Physics 89, 015004 (2017)

[56] "Linear Congruential Generators" by Joe Bolte, Wolfram Demonstrations Project.

[57] Toni Stojanovski, Ljupco Kocarev, “Chaos-based random number generators-part I: analysis [cryptography]” IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, **48**, 3, pp.281-288 (2001)

[58] Salih Ergün Serdar Özoğuz, “A Truly Random Number Generator Based on a Continuous-Time Chaotic Oscillator for Applications in Cryptography”, Computer and Information Sciences - ISCIS 2005, pp 205-214 (2000)

[59] Paul Kohlbrenner, Kris Gaj, “An embedded true random number generator for FPGAs” 12th international symposium on Field programmable gate arrays pp. 71–78 (2004)

[60] Jan Piet van Hamburg, Patrick S Asmawidjaja, Nadine Davelaar, Adriana M C Mus, Ferry Cornelissen, Johannes P T M van Leeuwen, Johanna M W Hazes, Radboud J E M Dolhain, Pieter A G M Bakx, Edgar M Colin, Erik Lubberts “TNF blockade requires 1,25(OH)2D3 to control human Th17-mediated synovial inflammation” 2012 Apr;71(4):606-12

[61] Gerlach, W.; Stern, O. "Der experimentelle Nachweis der Richtungsquantelung im Magnetfeld". Zeitschrift für Physik. 9 (1): 349–352, (1922).

[62] Eisaman, M. D., Fan, J., Migdall, A. & Polyakov, S. V. Invited review article: Single-photon sources and detectors. Rev. Sci. Instrum. 82, 071101 (2011).

[63] Ren, M. et al. Quantum random-number generator based on a photon-numberresolving detector. Phys. Rev. A 83, 023820 (2011)

[64] Xu, F. et al. Ultrafast quantum random number generation based on quantum phase

fluctuations. Opt. Express 20, 12366–12377 (2012)

[65] Stefanov, A., Gisin, N., Guinnard, O., Guinnard, L. & Zbinden, H. “Optical quantum random number generator.” J. Mod. Opt. 47, 595–598 (2000)

[66] Yan, Q., Zhao, B., Liao, Q. & Zhou, N. Multi-bit quantum random number generation by measuring positions of arrival photons. Rev. Sci. Instrum. 85, 103116 (2014).

[67] Wayne, M., Jeffrey, E., Akselrod, G. & Kwiat, P. Photon arrival time quantum random number generation. J. Mod. Opt. 56, 516–522 (2009).

[68] Wahl, M. et al. An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements. Appl. Phys. Lett. 98, 171105 (2011).

[69] Ren, M. et al. Quantum random-number generator based on a photon-numberresolving detector. Phys. Rev. A 83, 023820 (2011).

[70] Applegate, M. et al. Efficient and robust quantum random number generation by photon number detection. Appl. Phys. Lett. 107, 071106 (2015).

[71] Gabriel, C. et al. A generator for unique quantum random numbers based on vacuum states. Nat. Photon. 4, 711–715 (2010)

[72] Shen, Y., Tian, L. & Zou, H. Practical quantum random number generator based on measuring the shot noise of vacuum states. Phys. Rev. A 81, 063814 (2010)

[73] Symul, T., Assad, S. & Lam, P. K. Real time demonstration of high bitrate quantum random number generation with coherent laser light. Appl. Phys. Lett. 98, 231103 (2011).

[74] Li, X., Cohen, A. B., Murphy, T. E. & Roy, R. Scalable parallel physical random number generator based on a superluminescent led. Opt. Lett. 36, 1020–1022 (2011)

[75] Qi, B., Chi, Y.-M., Lo, H.-K. & Qian, L. High-speed quantum random number generation by measuring phase noise of a single-mode laser. Opt. Lett. 35, 312–314 (2010).

[76] Jofre, M. et al. True random numbers from amplified quantum vacuum. Opt. Express 19, 20665–20672 (2011).

[77] Yuan, Z. et al. Robust random number generation using steady-state emission of gain-switched laser diodes. Appl. Phys. Lett. 104, 261112 (2014).

[78] Jizba, P.; Arimitsu, T. (2004). "On observability of Rényi's entropy". Physical Review E. 69 (2): 026128.

[79] N. Nisan and A. Ta-Shma, “Extracting randomness: A survey and new constructions,” J. Comput. Sci. Tech. 58, 148–173 (1999)

[80] B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, Opt. Lett., 35, 312 (2010).

[81] Ma, X. et al. Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction. Phys. Rev. A 87, 062327 (2013).

[82] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Mauer, IEEE Trans. Inf. Theory, 41, 1905 (1995)

[83] Toshiya Kobayashi, Akihisa Tomita, and Atsushi Okamoto “Evaluation of the phase randomness of a light source in quantum-key-distribution systems with an attenuated laser” PHYSICAL REVIEW A 90, 032320 (2014)

[84] https://www.tij.co.jp/product/jp/ADC12DJ2700

[85] Abellán, C. et al. Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode. Optics Express 22: 1645–1654. (2014).

[86] Moustafa Ahmed, Minoru Yamada, and Masayuki Saito “Numerical Modeling of Intensity and Phase Noise in Semiconductor Lasers” IEEE JOURNAL OF QUANTUM ELECTRONICS, VOL. 37, NO. 12, DECEMBER 2001

[87] Fujihara, Takeoka, Sasaki, 5J104 AA18 FA10, JP 2018-147092

[88] Killmann, W. and Schindler, W. A proposal for: Functionality classes for random number generators. AIS 20 / AIS31, 2011

[89] M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. P. Torres, M. W.Mitchell, and V. Pruneri, “True random numbers from amplified quantum vacuum” Opt. Express 19, 20665 (2011).

[90] Weiyang Zhang, Yu Kadosawa, Akihisa Tomita, Kazuhisa Ogawa and Atsushi Okamoto:「State preparation robust to modulation signal degradation by dual parallel modulator for high-speed BB84 quantum key distribution systems」, Opt. Express, Vol.28, No.9, pp.13965-13977 (2020)

[91] Weiyang Zhang, Akihisa Tomita, Kazuhisa Ogawa and Atsushi Okamoto:「A Quantum random number generator integrated into a transmitter of BB84 QKD systems」, 20th Asian Quantum Information Science Conference, Sydney, Australia, December 7-9, No. 18 (2020)