Improve the Sender Unit of Polarised-Based DVQKD BB84

YEUNG Tung Yan
Quantum Device Engineering, MSc Optoelectronic and Quantum Technologies, Uinversity of Bristol

(Dated: 26 April 2024)

Abstract— **The growing concern of modern public key cryptography systems becoming increasingly breakable has been addressed. How is Quantum Key Distribution (QKD) a potential solution to tackle the security issue will be discussed. The paper investigates the implementation of a polarised-based Discrete-Variable QKD (DVQKD) device based on the BB84 protocol via an optical fibre by weak lasers as source. The primary objective this study is to enhance the device's performance and security against Photon Number Splitting (PNS) attacks of the proposed QKD setup from the eavesdroppers, which is due to the presence of optical pulses may have multiple photons. Two improvement methods will be analysed, by adding intensity modulator after the weak lasers for decoy source or replacing weak lasers with true single photon source (SPS) emitters.**

I. MOTIVATION

Modern cryptography can be classified into two cryptosystems: symmetric and asymmetric (public). Symmetric encryption refers to the system where Alice and Bob have the same key for both processes of encrypting and decrypting. This is known as the one-time pad (OTP) encryption[1]. OTP is proven to be secure if the key is random as ideal and is discarded after using. Due to distribution of the key is through an insecure transmission channel, the security of the system is not guaranteed[2]. This becomes a main concern.

On the contrary, asymmetric encryption circumvents the problem of key distribution. Alice uses a one-way function to generate a public key from a private key[3]. This encryption system is based on the computational complexity of mathematical algorithms, for example, RSA[4], which is based on the prime factorisation. At first, two random prime numbers p and q are being chosen that $n = pq$. Bob uses this to generate a public key (e, n) and private key (d, n), where satisfies $(n) = (p-1)(q-1)$ and $gcd(e, \Phi(n)) = 1$. The value of p and q are maintained secure. The public key can be transmitted through a conventional insecure channel. Then, Bob can obtain private as $d \equiv (mod\Phi(n))/e$. Alice encrypts the message M as ciphertext $C = M^e(mod\ n)$. Bob decrypts the message as $M = C^d(mod\ n)$. Suppose Eve has the information of the public key e, n and ciphertext c, in order to crack the message M , she has to know about the value of d. Based on the values Eve already have, she only needs to know p and q for n and she can calculate the value for d using the above formulas[4]. A worrying prospect is that algorithms such as Shor's algorithm have shown that the RSA can be exploited by the cryptanalysts using a Quantum Computer[5]. When a perfect quantum computer is introduced, RSA cryptography system will no longer be secure.

QKD is a promising method to solve the insecurity issue in public key cryptography[6]. This technique, is fundamentally based on the no cloning theorem[7], that a quantum state cannot be cloned without permanently changing its state and losing its information. Thus, eavesdropping attempts from other parties will inevitably result in errors that can be detected. The initial approach of QKD is DV protocol. Bennett and Brassard conceived of a protocol in 1984, known as BB84, is the most recognisable DVQKD prodocol[8]. This paper analyses the design of device capable of

Quantum Transmission & Detection	Photons Alice sends	$\nearrow$	$\nwarrow$	$\nwarrow$	$\uparrow$	$\rightarrow$	$\nearrow$	$\nwarrow$	$\uparrow$
	Random bits by Alice	1	0	0	1	0	1	0	1
	Bob detects	$\uparrow$	$\nearrow$	$\nwarrow$	$\uparrow$	$\nearrow$	$\nearrow$	$\nwarrow$	$\nwarrow$
	Bits Bob detects	1	1	0	1	1	1	0	0
Public Discussion	Basis Bob picks and lets Alice know	+	×	×	+	×	×	×	×
	Bit to keep that Alice lets Bob know	-	-	✓	✓	-	✓	✓	-
	Their sifted key	-	-	0	1	-	1	0	-

TABLE I: Protocol scheme of BB84.

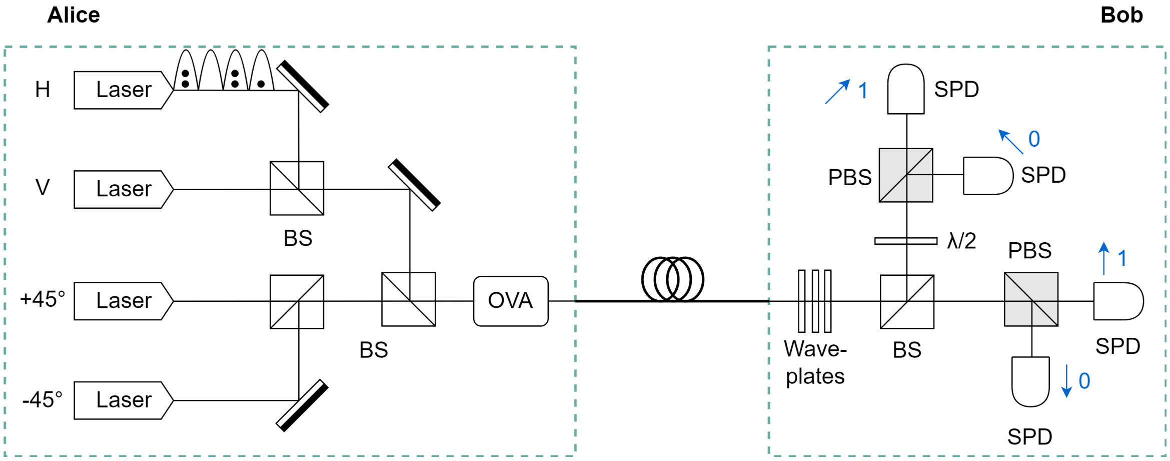

Fig. 1: Configuration of the DVQKD design[9, 10]. Laser: weak lasers, BS: beam splitter, OVA: optical variable attenuator, PBS: polarisation beam splitter, SPD: single photon detector.

performing BB84.

II. Device Operation

Working Principles: Table I presents an illustration of the BB84 principle. Alice encodes her random string of bits in bases selected at the random: the rectilinear basis (+) and the diagonal basis (×). Every bit is encoded in a polarisation state that is possibly to be: horizontal or vertical or $\pm 45°$, i.e. $\frac{1}{\sqrt{2}}(|H> \pm |V>)$. Alice transmits the polarised photons to Bob via the quantum channel. Bob selects a basis at random from Alice in order to measure each photon with a 50% chance of receiving an error if Bob selects a different basis than Alice does. Alice and Bob communicate with each other over an insecure classical channel or public announces what basis they used to measure each qubit but not the measurement outcomes. This public announcement allows them to compare which measurements were performed in matching bases and helps identify potential eavesdropping attempts, as Eve's interception and measurement would introduce errors in the correlation according to the no cloning theorem. Alice and Bob will then sift errors out corresponding to the qubits measured in different bases. The identical string of random bits now Alice and Bob have is called a sifted key[6].

Experimental Design: The configuration of the experimental design is shown in Figure 1. A proposal published in 1992[9] encodes qubits into the phases of individual photons served as the foundation for the architecture. The experiment uses weak laser since this is the current available SPS, which average optical strength is at the sub-single photon level, as the true SPS technology is still in the early stages of development. Using optical couplers, Alice's optical paths are joined onto a single fiber. Each photon pulse laser is triggered in accordance with this to produce different polarisation states. The beams are merged by BSs, attenuated by OVA to an approximate single photon level to fulfill the indistinguishability, and then delivered via optical fiber to Bob. At Bob's side, the polarisation will be changed and the change will not be expected to be stable because the transmission is performed by an optical fiber rather than in free-space. The rotation of the polarisation in the optical fiber can be compensated for by adding waveplates before Bob's measurement. After that, the photon pulses are divided into two paths for diagonal and rectangular base detections. A BS is used as a passive device to select a basis at random. In both outputs, there is a PBS and two SPDs. An additional $\pi/2$ plate in front of the PBS in one output allows an incoming linear polarisation to be rotated by $\pm 45°$. The diagonal basis of photons, "1" or "0," can be identified in here. A photon measured with an incorrect basis produces a random projection on one of the PBS's two output states, leading to a random outcome. InGaAs/InP Avalanche Photodiode (APD), which can detect photons with wavelengths ranging from roughly 950 to 1650 nm, is the SPD that is most frequently used in DVQKD systems[11]. Bob detects the single photons Alice sends using SPDs[9, 10].

III. Limitations

The drawback of using weak laser will be discussed in this section. The average power of each pulse is known to have less than one photon, even with this case, there is still a possibility that a tiny percentage of the emitting pulses include more than one photon. Eve might potentially launch a PNS attack as a result of this issue[12]. From these multi-photon pulses, Eve can separate and retain one photon, sending the remaining ones to Bob. Thus, she could learn the basis information from the public channel and read part of the or the whole key without introducing additional quantum bit error rates (QBER)[12].

Each weak laser pulse that emits has a photon count that is determined by a Poisson distribution, therefore weak laser is also called Poissonian source. The Poisson distribution of the weak laser is represented by the equation[11]:

$$p(k, \mu) = e^{-\mu} \frac{\mu^k}{k!} \tag{1}$$

where k is the actual number of photons in a pulse and μ is the mean number of photons per pulse. By substituting the values of k and μ to equation 1 and the calculated probability is plotted in Figure 2, this has demonstrated that the lower the μ is, the lower the probability of having more than one photon in a pulse.

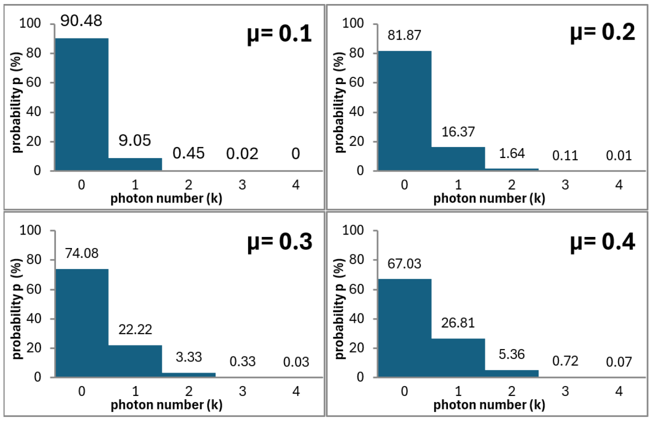

Fig. 2: Calculated Poisson distribution for weak lasers.

Consequently, some researchers proposed to reduce the intensity of the weak lasers, having lower chance of multi photons in a pulse in a QKD link to offset the problem of PNS attacks. However, this way does not truly solve the issue and on the other hand, it introduces another issue, that is a lower value of μ does, indicating a decreased probability of single photon pulses. Because of the inherent loss of the quantum channel, this will reduce both the maximum transmission distance and the yield of raw keys[13]. As a result, the limitations of the traditional BB84 using weak lasers as source can be concluded that, it either encounters high chance of PNS attack with high mu or encounters a lower chance of PNS attack with low mu but secure key can only be shared within a limited distance.

IV. Improvements

In this section, two different ways to modify the design will be presented to explain how to defend against PNS attack. To solve the issue from the root, the new designs make changes to the components on the sender unit (Alice side).

The first way is to add new components after the weak laser source. An intensity modulator can be added after each laser to the BB84 to create decoy source as illustrated in Figure 3.

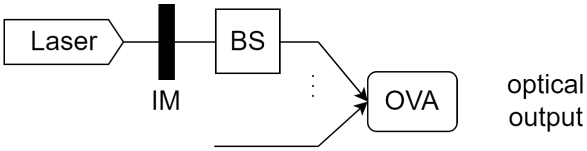

Fig. 3: Four intensity modulators (IM) added to produce decoy states based on the BB84 design proposed in Section II.

The "decoy state" method was first proposed by Hwang[14]. The main idea is to have a few more states in addition to the standard BB84 states. These additional decoy states vary from the standard states in their intensities. While the standard states are still used to generate the keys, the decoy states are used to detect eavesdropping attacks. Alice intentionally sends the same copy of her laser pulses and compares the final photon numbers Bob received. Eve can be detected by comparison of photon numbers since she doesn't know which pulses are signal or decoy and tries to steal all of them [14, 15].

Another approach is to replace the weak lasers as true SPS emitters, in this way, the attenuator can be removed. The new design is illustrated in 4. Although a true SPS is not available, the performance can still be estimated by the equations. The weak lasers have the property of $\mu < 1$ and $g^2(0) < 1$, while a perfect SPS should have $\mu = 1$ and $g^2(0) = 1$.

The performance of any practical QKD system can be evaluated in terms of quantum bit error rates (QBER) and the secure key rate varying with transmission distance.
The secret key rate is defined as[16]

$$S = R_{sifted} \cdot (1 - 2H(Q)), \tag{2}$$

where H represents the binary Shannon entropy,

$$H(x) = -x \cdot log_2(x) - 1(1 - x) \cdot log_2(1 - x). \tag{3}$$

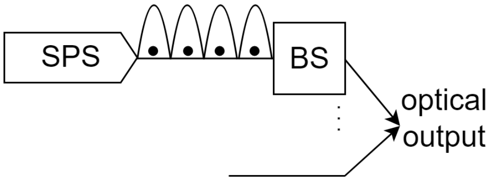

Fig. 4: Four true SPS emitters replace the weak lasers and remove the attenuator based on the BB84 design proposed in Section II.

For R_{sifted}, it is the sifted key rate summated by rates caused by various numbers of photons (n) that are actually emitted is[11]

$$R_{sifted} = \sum_{n} R_n \tag{4}$$

For Q, it is QBER defined as number of incorrect counts relative to the total number of counts[11],

$$Q = \sum_{n} Y_n \varepsilon_n \tag{5}$$

where yield Y_n is the chance of detecting n photons from an emitted signal. $Y_n = \frac{R_n}{R}$ with $\sum_n Y_n = 1$. ε_n is the errors divided into parts related to different photon counts that are emitted. $\varepsilon_n = \frac{R^n_{wrong}}{R}$[11].

Based on the above equations, Tang(2019) conducted the simulations to calculate the secure key rate and maximum key transmission distance to determine the performance of each design of BB84, the simulation result is presented in Figure 5. From the simulation, Since the average photon number μ is normally equal to 0.1 in BB84 protocol, the simulation of the weak laser (green line) and the BB84 with decoy state are both calculated based on $\mu = 0.1$. The figure demonstrates clearly that adding decoy states to the BB84 protocol greatly increases the secure key rate with extending the maximum key transmission distance when compared to the BB84 using weak laser. For the true single photon source design, the secure key rate is further enhanced. It is proven that the two modifications can greatly reduce the chance of PNS attack compared to the design of BB84 using weak lasers proposed in Section II.

V. Potential Negative Effects of the Modification

For the method of adding intensity modulators to add decoy states, there may be potential negative effects to the QKD system.

The first negative effect assumes an attacker is able to control the intensity modulator and eavesdrop the quantum channel simultaneously. For example, an attacker could manipulate the intensity modulator to introduce additional photons or modify the intensity of the transmitted photon to gather information of the photons. However, there is no research has verified this kind of attack may actually pose a threat to the QKD system. Therefore, this is a just an assumption for potential eavesdropping attempt.

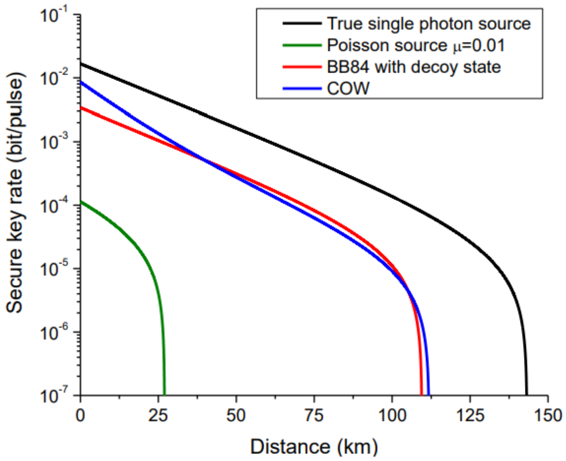

Fig. 5: Simulated secure key rate against key transmission distance[13].

Another potential negative effect is the intensity modulator itself is an imperfect device. For example, we cannot guarantee all four intensity modulators are completely identical and function ideally due to manufacturing process or some materials may exhibit non-linear responses to the applied electric field. The imperfect intensity modulators may introduce noise. The noise may increase the error ε_n, as a consequence affect the QBER in equation 5.

VI. Conclusions

The devices implement the common method of fiber-based QKD operate only between two-user point-to-point connections with the DV protocol - BB84 by weak lasers are reviewed in this study. A practical security concern for PNS attacks is the weak lasers used for single photon generation. Simulations have been proven by adding intensity modulators to generate decoy state or true single photon source, the concern shall be resolved. Furthermore, assumptions of the potential negative effects to the QKD system after applying intensity modulators have been presented.

References

[1] G. S. Vernam, “Cipher printing telegraph systems for secret wire and radio telegraphic communications,” vol. XLV, pp. 295–301, 1926.

[2] C. E. Shannon, “Communication theory of secrecy systems,” vol. 28, pp. 656–715, 1949.

[3] D. Dolev and A. Yao, “On the security of public key protocols,” *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[4] A. S. R. L. Rivest and L. Adleman, “A method for obtaining digital signatures and publickey cryptosystems,” *Commun. ACM*, vol. 21, pp. 120–126, 1978.

[5] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” *SIAM J. Comput.*, vol. 26, pp. 1484–1509, 1997.

[6] H. Z. D. S. N. B. N. Gisin, G. Ribordy and V. Scarani, “Towards practical and fast quantum cryptography,” *Reviews of Modern Physics*, vol. 74, pp. 145–195, 2002.

[7] W. K. Wootters and W. H. Zurek, “A single quantum cannot be cloned,” *Nature*, vol. 299, p. 802, 1982.

[8] C. H. Bennet and G. Brassard, “Quantum cryptography : Public key distribution and coin tossing,” *Proceedings of the IEEE international conference on Computors, Systems and Signal Processing, Bangalore*, 1984.

[9] G. B. L. S. C. H. Bennett, F. Bessette and J. Smolin, “Experimental quantum cryptography,” *Journal of Cryptology*, vol. 5, pp. 3–28, 1992.

[10] V. G. M. A. M. G. W. A. A. O. J. G. R. C. e. a. A. R. A. Gaya, D. C. Díaz-Aldagalán, “Practical quantum key distribution based on the bb84 protocol,” *Waves*, vol. 1, pp. 4–14, 2011.

[11] N. J. C. M. D. N. L. V. Scarani, H. Bechmann-Pasquinucci and M. Peev, “The security of practical quantum key distribution,” *Reviews of Modern Physics*, vol. 81, pp. 1301–1350, 2009.

[12] T. M. G. Brassard, N. Lütkenhaus and B. C. Sanders, “Limitations on practical quantum cryptography,” *Physical Review Letters*, vol. 85, pp. 1330–1333, 2000.

[13] X. Tang, *Optically Switched Quantum Key Distribution Network*. PhD thesis, 2019.

[14] W.-Y. Hwang, “Quantum key distribution with high loss: Toward global secure communication,” *Physical Review Letters*, vol. 91, p. 057901, 2003.

[15] X. M. H.-K. Lo and K. Chen, “Decoy state quantum key distribution,” *Physical Review Letters*, vol. 94, p. 230504, 2005.

[16] N. L. Daniel Gottesman, Hoi-Kwong Lo and J. Preskill, “Security of quantum key distribution with imperfect devices,” *Quantum Information Computation*, vol. 4, p. 325–360, 2004.