A Quantum Cryptosystem Secure Against Beamsplitting Attacks

Yi Mu, Yuliang Zheng, and Jennifer Seberry

Center for Computer Security Research, Department of Computer Science,
University of Wollongong, Wollongong, NSW 2522, Australia

and

Yan-Xia Lin

Department of Applied Statistics,
University of Wollongong, Wollongong, NSW 2522, Australia

Abstract

An important area in computer and communications security research is to make various pioneering ideas practical. In this paper we develop a new cryptographic key distribution system based on the uncertainty principle in quantum physics. The new system employs a novel technique that *mixes two quantum states* in the transmission of photonic signals. On one hand, this technique forces an eavesdropper to extract more signal energy in an eavesdropping process, which renders an eavesdropping attempt easily detectable. And on the other hand,it allows legitimate communicants to transmit higher power photonic signals, whereby secure communications are made possible over a significantly longer haul than any other system based on the same principle could support. Another contribution of this paper is to present a new powerful attack based on a pair of beamsplitters. We show that while a well-known quantum key distribution system proposed previously is prone to the new attack, our system is immune to it.

1 INTRODUCTION

In conventional cryptography, it is assumed that an eavesdropper learns entire communication contents, without the sender or receiver of a message being aware that any eavesdropping has taken place. This assumption is no longer true with quantum cryptography which utilizes quantum-mechanical principles such as Heisenberg's uncertainty principle [1] and Bell's inequality[2]. Recent years have seen an increasing interest in the area, and it has attracted a considerable amount of research from both a theoretical and an experimental point of view [1-5].

An experiment conducted recently [1] has demonstrated that a quantum key distribution system can in principle prevent any eavesdropping attacks including intercept/resend and, in particular, beamsplitting. This is achieved by using very dim light pulses. Although such low intensity signals make beamsplitting attacks impossible, they place a severe limit on the signals' transmission distance. In the experiment reported in [1], the distance was only 32 cm, far less than that required by any practical application. Therefore it is an extremely challenging task to search for a quantum cryptosystem that is more secure, more practical and supports longer haul communications.

In [6] it has been argued that, by using the single photon interference technique, as well as a time-division Mach-Zehnder interferometer, a single-photon transmission of up to 10 km could be potentially possible. This technology could provide a promising approach for quantum cryptography. However, due to its sophistication and complexity, it could take quite some time for the interesting technology to become a reality. On the other hand, a real telecommunication system often uses high power light signals to overcome losses in optical fiber, whereby a long haul information transmission is possible. Therefore, alternatively, we hope to develop a high power quantum cryptographic system, which might be suitable for practical optical communication systems. In this paper, we develop a multi-photon quantum key distribution system based on the uncertainty principle and quantum detection. With this quantum key distribution system a binary bit is represented by a photon pulse which is a mixture of two quantum states, one for "0" and the other for "1". The population percentage of each individual state in a single pulse is involved in the determination of the binary bit carried by the pulse. To be more precise, the binary bit is defined to be that represented by the majority of the photons in the pulse. An important advantage of this system is that it is infeasible for an eavesdropper to estimate the population information unless he/she extracts a large portion of photons from a signal pulse by such means as beamsplitting. The legitimate communicants can readily detect the existence of an eavesdropping attempt by observing the loss of signals' intensity. Another advantage of the system is that it is also secure against the less powerful intercept/resend attack. Due to the various advantages, we believe that the novel quantum-state-mixing key distribution technique could provide us with an appealing avenue towards a realistic quantum cryptosystem.

2 THE STRATEGIES OF BEAMSPLITTING ATTACKS

We consider the situation where two users Alice and Bob who share no secret information initially want to agree upon a common strings of random bits, or a common key, in such a way that the key is kept secret from a third party Eve who eavesdrops on communications between Alice and Bob. In cryptography this problem is called the key distribution problem. The system presented in [1] represnts a pioneering piece of work on utilizing quantum michenical principles in key distribution. The system is based on two bases (see Fig. 1 in Ref.[1]). The basic idea is that Alice sends a random sequence key distribution containing all four canonical kinds of photons to Bob; Bob chooses bases randomly and independently to measure them (note that a wrong basis will randomize the measurement due to the uncertainty principle); Bob tells Alice which basis he used and Alice tells Bob which basis is correct (Obviously, some wrong measurements due to wrongly choosing bases, basically due to the uncertainty principle, have been screened); then Bob and Alice might have a common key distribution. However, the bit string possessed by Bob may still not be consistent with the bit string by Alice. To overcome this problem, privacy amplification and error-correcting techniques are used to distill the inconsistent strings. At the end of those procedures, Alice and Bob will share, with an extremely probability, a common secret key. If Eve wants to measure Alice's initial key distribution, say via intercept and resend, she will randomize some of keys because of wrongly choosing the bases of measurement, which causes a substantial error rate in Alice-Bob's communication, and then her attack can be aware.

Alice and Bob's approach is good when they use very dim light pulses to transmit information. Nevertheless, if they want to have a longer distance cryptosystem, they have to increase the signal power for overcoming losses in optical fiber. This provides a chance for Eve to use a beamsplitter to eavesdrop the information [1]. Since Eve might eavesdrop a small number of photons from each signal pulse, her attack is undetectable. In an optimal situation discussed by Bennett *et al*, Eve can store her share of each pulse until the Alice announces the correct bases. Under that situation, Alice has to wait arbitrarily long time for Eve's stored beam to decay. Consequently, Alice and Bob are successful in their communication.

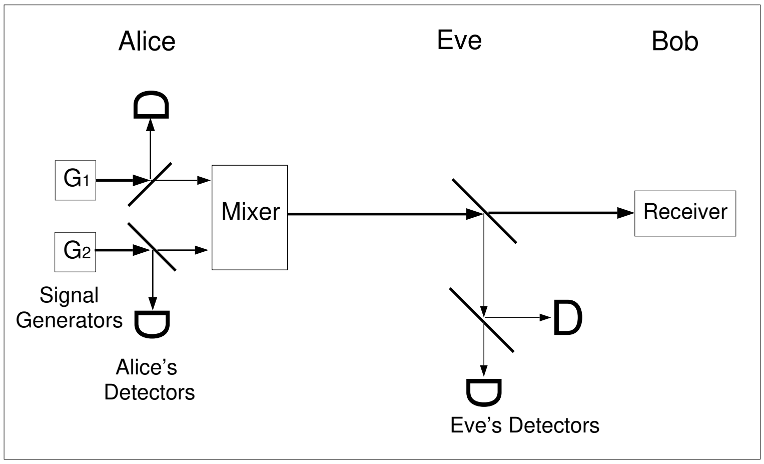

Figure 1: The schematic diagram of the quantum cryptosystem. The communication between Alice and Bob is eavesdropped by Eve who uses beamsplitters.

We now consider a better method for Eve: using multi-beamsplitters (see Fig. 1). Eve thus does not need to store her share, because actually the technology of photon storing is beyond her knowledge (or say unrealistic in practice). As shown in Fig. 1, the main beamsplitter extracts a small number of photons, letting remainder pass undisturbedly to Bob. Each share from the beamsplitter is split (via a 50/50 beamsplitter) into two beams measured using *different* bases. Eve records each measurement and determines which basis is correct only after the correct bases are announced publicly. Consequently, Eve obtains prefect information she needs without being known by Alice and Bob. This problem cannot be solved by Alice and Bob using the key distribution of Bennett *et al*.[1]

3 STATE-MIXING QUANTUM KEY DISTRIBUTION

3.1 State-mixing quantum key distribution and measurement

We now develop a secure communication environment for Alice and Bob against Eve's beam-splitting attack. We first introduce two bases $B_1 = \{\Phi_O, \Phi_I\}$ and $B_2 = \{\Psi_O, \Psi_I\}$, which are closed and nonorthogonal. Φ_O and Φ_I are eigenvalues of operator $\hat{O}_1$; Ψ_O and Ψ_I are eigenvalues of operator $\hat{O}_2$. An important fact is that $\hat{O}_1$ and $\hat{O}_2$ do not commute, namely, $[\hat{O}_1, \hat{O}_2] \neq 0$. For simplicity, we denote the two conjugate bases by $B_1 = \{O_1, I_1\}$ and $B_2 = \{O_2, I_2\}$ respectively.

The key distribution system we propose employs both bases and its schematic diagram is presented in Fig. 1. As shown in Fig. 1 (also see Tab. 1), the basic quantum key distribution protocol begins with Alice generating two random sequences of Poissonian photons by using two separate signal generators G_1 and G_2. The two generators are synchronized. At each time interval they use the same basis, which is selected uniformly at random from B_1 and B_2, to produce a pair of photon pulses of opposite states. Thus, at any particular point of time, the binary bits carried by a pair of photon pulses are always complementary. Clearly there are only four possible combinations of photon pulses: (O_1, I_1), (I_1, O_1), (O_2, I_2) and (I_2, O_2), where the first pulse is from G_1 while the second from G_2. For simplicity, we say such a pair of pulses to be complementary. Note that with each complementary pair of pulses generated by G_1 and G_2, the order to decide which pulse carries which state (O or I) is again determined uniformly at random by Alice.

As mentioned earlier, photon pulses generated by G_1 and G_2 obey two independent Poissonian distributions. Before a pair of pulses are merged together, each is split into two smaller pulses of equal intensity by a 50/50 beamsplitter. Now Alice has two identical pairs of complementary photon pulses, one is for the purpose of measuring and the other is to be merged. By measuring the first pair Alice can obtain complete information about the second pair, such as the precise number of photons contained by each pulse. The second pair of pulses enters a pulse mixer which can produce a superposition of O state and I state. The mixed state is then injected into optical fiber toward Bob.

An important property of the generators are that they produce photon pulses with different mean intensity, so in each mixed pulse, the population of O state is *different* from that of I state. Actually, the ratio R of population of O state to population of I state is totally random for Poissonian process. If we denote O state in a mixed pulse to be Ψ_O and I state to be Ψ_I, the mixed state

$$\Psi = c_1 \Psi_O + c_2 \Psi_I. \tag{1}$$

In each measurement of the mixed state, we obtain either O or I. $|c_1|^2$ and $|c_2|^2$ are probabilities obtaining O state and I state for the measurement. The binary information delivered by a mixed pulse is determined by the population ratio of O and I states, R. In the other word, we stipulate that the property of the pulse is represented by the *majority* photon.

In Tab. 1 we explain the process of sending/receiving quantum key distribution. The process starts with Alice sending a random sequence of the mixed O and I photon pulses to Bob. As explained above, Alice knows exactly all information about the pulses, including ratio of population R in each pulse and the binary information. Bob then chooses his bases randomly and independently to carry out the measurement, since he does not know the choice of Alice (in fact, the signal pulses sent by Alice are random). Bob then announces publicly what kinds of bases he used. Alice tells him publicly whether or not he has used correct bases. In this step, Alice also chooses the pulses with higher intensity (say, 50 to 100 photons) and certain ratio of population only (say, $7/3 > R > 6/4$ *and* $3/7 < R < 4/6$), and discards the rest. This assures to minimize measurement error. In order to determine the binary information from each mixed pulse, Bob can use following approaches:

Table 1: Mixed-state key distribution protocol for the process of sending/receiving between Alice and Bob. (1) Alice sends a random sequence of Poissonian photons under the mixed states. the underline denotes majority. The photons are prepared under two bases: B_1: O_1 and I_1; B_2: O_2 and I_2. (2) Bob measures the light pulses in a random sequence of bases. (3) Bob's measurement results. (4) Bob tells Alice which basis she has used for each pulse she received. (5) Alice tells which basis Bob used is correct. (6) Resulting binary information of the key distribution, where O represents "0" and I represents "1".

1:	$\underline{O_1}I_1$	$O_2\underline{I_2}$	$\underline{I_1}O_1$	$I_1\underline{O_1}$	$O_2\underline{I_2}$	$\underline{I_2}O_2$	$\underline{O_2}I_2$	$\underline{I_1}O_1$	$\underline{O_2}I_2$	$\underline{O_1}I_1$	$\underline{O_2}I_2$
2:	B_1	B_2	B_2	B_1	B_1	B_2	B_1	B_1	B_2	B_2	B_1
3:	O_1	I_2		O_1	I_1	I_2	O_1		O_2	I_2	O_1
4:	B_1	B_2		B_1	B_1	B_2	B_1		B_2	B_2	B_1
5:	yes	yes		yes		yes			yes		
6:	0	1		0		1			0		

1. Repeating measurement

Bob may extract information from each pulse, by means of repeating measurement. We first consider the case that Eve is absent and losses through optical fiber are negligible, hence Bob can receive the information sent by Alice without disturbed. Bob then measures the same pulse for several times and the binary information is determined in terms of higher probability of measuring either O or I. Unfortunately, this cannot be realized with an ordinary device of measurement, because each single measurement must add noise to the signal pulse so that the measurement becomes not accurate. Bob therefore considers to use the technique of quantum nondemolition detection (QND) which adds no noise to the signal during a measurement[7-10]. Using this method, the error rate can be limited at a very low level, provided the times of measurement m is sufficiently large (see following description). Let x_i be the number of O state being measured in the ith measurement, i.e.

$$x_i = \begin{cases} 1, & \text{when } O \text{ state is obtained} \\ 0, & \text{otherwise} \end{cases} .$$

If the realistic O photon percentage $p > 0.5$ in a pulse, i.e. $R > 1$ (or say O photons are the majority in the pulse). The correct measurement is said to be obtained, provided sample mean $\frac{1}{m}\sum_{i=1}^{m} x_i$ is *greater* than 0.5. The probability of correct measurement ($\frac{1}{m}\sum_{i=1}^{m} x_i > 0.5$) then is

$$P(\frac{1}{m}\sum_{i=1}^{m} x_i > 0.5) = \sum_{k=[0.5m]+1}^{m} \frac{m!}{k!(m-k)!} p^k (1-p)^{m-k}. \tag{2}$$

For example,

$$\begin{array}{llll} & p = 0.6: & p = 0.7: & p = 0.8: \\ m = 10, & P = 0.633, & P = 0.849, & P = 0.967; \\ m = 20, & P = 0.755, & P = 0.962, & P = 0.997; \\ m = 30, & P = 0.822, & P = 0.983, & P = 1; \\ m = 50, & P = 0.902, & P = 0.998. & \end{array}$$

Obviously, the probability Bob is correct is proportional to m and p.

2. One-step measurement

Bob applies a new method, which avoids him using the QND measurement. He divides a pulse into several blocks with equal population. Obviously, the ratio of population of O state and I state in each block is random. After each block has been measured once, the total number of O or I being measured can be used to determine which state is the majority in the pulse. As defined, Alice and Bob choose the majority state to represent the pulse. The accuracy of measurement is proportional to the number of block.

We now calculate what is Bob's success rate in the measurement. Assuming that the total number of photon in a pulse is N, in which the number of O photon is n_0, the majority. Bob divides the pulse into n_b blocks, then measures each block once. For a measurement in the ith block, the indicator of measuring O is

$$y_i = \begin{cases} 1, & \text{when } O \text{ state is obtained} \\ 0, & \text{otherwise} \end{cases} .$$

After measuring all the blocks, we show that the probability Bob is successful in obtaining O (where greater than $[n_b/2]$ measurements are O) is

$$P(\sum_{i=1}^{n_b} y_i > [n_b/2]) = \sum_{k=[n_b/2]+1}^{h} \frac{\begin{pmatrix} k \\ n_0 \end{pmatrix} \begin{pmatrix} n_b - k \\ N - n_0 \end{pmatrix}}{\begin{pmatrix} n_b \\ N \end{pmatrix}}, \tag{3}$$

where

$$h = \begin{cases} n_b & \text{if } n_b \leq n_0 \\ n_0 & \text{if } n_b > n_0 \end{cases} .$$

If the total number of photon N is 100, then

$$\begin{array}{lll} n_0 = 60, & n_b = 20, & P = 0.779; \\ & n_b = 30, & P = 0.867; \\ & n_b = 50, & P = 0.967; \\ & n_b = 70, & P = 0.994; \\ n_0 = 70, & n_b = 20, & P = 0.969; \\ & n_b = 30, & P = 0.995; \\ & n_b = 40, & P = 1. \end{array}$$

It is shown that the success probability of Bob is proportional to the number of blocks and the population of O photon (or, say, the number of I photon, if they are the majority). The number of block required is proportional to the population in the pulse. When the up-limit of the population in pulses sent by Alice is fixed, the number of block can be fixed.

If Bob had a technique to divide a mixed pulse into two original O and I pulses, then he could measure the exact photon number and binary information of each pulse. This method may be convenient, however it is not realistic in practice.

3.2 The eavesdropping

We then consider Eve's eavesdropping. She knows that intercept/resend is not a good idea, since the light pulses sent by Alice are in a random process being superposition of two Poissonian processes and so it is impossible for her to reproduce the photon pulses which meet the Poissonian processes Alice made. Also, since she has to choose the measurement bases randomly, her measurement has a high error rate due to the uncertainty principle. She then considers to use beamsplitters. But this is still hard for her, because she has to extract enough photons from each pulse to achieve a lower error rate.

Let us consider Eve's strategy. Obviously, under state-mixing scheme, it is useless for Eve to extract a small number of photons from each pulse, because photons extracted from each pulse is totally random and so it is hard for her to have a correct R. If a mixed pulse contains N photons, in which the number of O photon is n_0 (we assume it is the majority), and if Eve takes n_e photons from the pulse by utilizing beamsplitters, the probability Eve takes at least $n_e/2+1$ O photons, i.e. O photons are still majority, is

$$P(O \text{ photons } > [n_e/2]) = \sum_{k=[n_e/2]+1}^{h} \frac{\begin{pmatrix} k \\ n_0 \end{pmatrix} \begin{pmatrix} n_e - k \\ N - n_0 \end{pmatrix}}{\begin{pmatrix} n_e \\ N \end{pmatrix}}, \tag{4}$$

where

$$h = \begin{cases} n_e, & \text{if } n_e \leq n_0 \\ n_0, & \text{if } n_e > n_0 \end{cases} .$$

If Eve's measurement for her share is perfect, Eq. (5) represents the probability of her successful measurement in each single pulse. For example,

$$\begin{array}{llll}
N = 10, & n_0 = 6, & n_e = 2, & P = 0.333; \\
 & n_0 = 7, & n_e = 2, & P = 0.467; \\
N = 20, & n_0 = 12, & n_e = 2, & P = 0.347; \\
 & n_0 = 14, & n_e = 2, & P = 0.479; \\
N = 60, & n_0 = 35, & n_e = 6, & P = 0.544; \\
 & n_0 = 42, & n_e = 6, & P = 0.753; \\
N = 100, & n_0 = 60, & n_e = 10, & P = 0.639; \\
 & n_0 = 70, & n_e = 10, & P = 0.862.
\end{array}$$

Eve's successful measurement is proportional to the light intensity and stolen photons. Alice and Bob, of course, have to assure the light intensity not being too strong and keep Eve having more errors, thus Eve must have larger n_e to have a fair measurement, say extracting 10% of total photons or more. However a loss of 10% can be detectable. A better measurement for Eve is only available when the her share is sufficient, for example, 30% for $N = 100$.

In order to detect the losses due to the eavesdropping Bob has to calculate mean number of photon for a signal-pulse string via measuring the intensity of each pulse in the string, and then compares his result with one which has been announced by Alice publicly. Such measurement is very easy to be realized in practice. Actually, Alice and Bob do not need to measure the intensity of all the pulses, instead, they can measure only some of them, say one in ten pulses. They compare the mean intensity for the measured pulses. It is impossible for Eve to avoid eavesdropping those pulses in a practical beamsplitting process.

There is an approach to further increase the error rate of Eve's measurement. Alice and bob may decide to use two signal pulses as one binary signal, for instance, "1" "1" or "0" "0" to be a new "0", and "1" "0" or "0" "1" to be a new "1", which will greatly decrease Eve's success rate, because new success probability becomes P^2. A further decrease of Eve's success rate is possible if we combine more pulses into one. This method does not affect Bob's detection, provided $p \simeq 1$

There is a measurement method called coherent measurements[11,12], which could potentially be a tool for Eve to attack the pulse-combination method mentioned above. Such measurement treats entire signal string as a single quantum state, hence a single measurement can obtain all information. Fortunately, this approach is extremely infeasible in practice.

3.3 signal losses

Now, both Eve's eavesdropping and signal losses in optical fiber are considered. Since the leakage of light in optical fiber is totally random, R may have been changed when Bob receives a signal. In order to overcome this, Alice has to assure the intensity of each pulse being sufficiently large, say 60-100 average photons per pulse (but not too large, otherwise Eve can have higher success rate if she always steals 10% photons in each pulse), and photon loss is small. Assuming κ is the fiber attenuation coefficient and L the fiber length, the light propagation loss is then $1 - e^{-\kappa L}$. Suppose $\kappa = 0.046 km^{-1}$ ($0.2 dB/km$) and fiber length is 2.5 km, about 10 % photons will lose after the propagation. In this case, the initial R should be limited in the region $R > 6/4$ and $R < 4/6$ to avoid the majority photon in some pulses being possibly reduced to minority in some pulses (although the probability is small) and so to assure a low error rate. Therefore, one thing Alice and Bob have to work out is the limit of R after propagation loss has been included. The measurement standard, including the times of measurement and the number of block, must satisfy the condition. For example, if the propagation loss is 10% and the initial R (sent by Alice) is $R > 7/3$ and $R < 3/7$, the limit of R will be $R = 6/4$ and $4/6$ (received by Bob).

The appearance of beamsplitters also causes the change of photon intensity. If the reflection rate of the beamsplitter is γ, the total loss of leakage due to leakage plus eavesdropping should be $\gamma + 1 - e^{-\kappa L}$. When Bob measures the intensity, the propagation loss has to be included before he compares it with that sent by Alice. If the loss rates of both eavesdropping and leakage are equal, say 10%, the total loss will be 20%, which could also result in an increase of error rate for Bob for a certain population ratio R (say, $R = 4/6$ or $R = 6/4$).

In conclusion, we have demonstrated that state-mixing approach can in principle solve the problem of beamsplitting attack in a higher power optical communication. Although in order to avoid Eve having a higher success rate we have to assume the signal power not to be too strong, a light signal with a hundred of mean photon is appropriate. Therefore it is possible for a distance cryptographic communication of a few kilometers. Our system is secure, because intercept/resend is impossible and also Eve's beamsplitting attack can be known in terms of loss of photon intensity. This paper has concentrated on introducing our quantum key distribution protocol and measuring methods for our system. A detailed description of public discussion and error correction will be presented in a subsequent paper.

ACKNOWLEDGES

The first and second authors were supported in part by the Australian Research Council under the reference number A49232172, and the third author by A49130102, A49131885 and A49232172.

REFERENCES

[1] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptol. **5**, 3, (1992).

[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[3] C. H. Bennett, G. Barssard, and D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

[4] Y. Mu, Y. Zheng, and Y.-X. Lin, "Quantum conference key distribution systems" (submitted for publication)

[5] Y. Mu, Y. Zheng, "Quantum cryptographic key distribution using an optical coupler" (submitted for publication)

[6] P. D. Townsend, J. G. Rarity, and P. R. Tapster, Electron. Lett. **29**, 634 (1993).

[7] G. J. Milburn, and D. F. Walls, Phys. Rev. A **28**, 2065 (1983)

[8] M. D. Levenson, R. M. Shelby, M. Reid, and D. F. Walls, "Quantum nondemolition detection of optical quadrature amplitudes", Phys. Rev. Lett. **57**, 2473 (1986).

[9] P. Alsing, G. J. Milburn, D. F. Walls, Phys. Rev. A **37**, 2970 (1988).

[10] M. Dance, M. J. Collett, and D. F. Walls, Phys. Rev. A **48**, 1532 (1993).

[11] C. H. Bennett, G. Brassard, and C. Crepeau, in *Advances in cryptography: Proceedings of Crypto '84*, (Springer-Verlag, New York, 1984), page 351.

[12] G. Brassard, and C. Crepeau, in *Advances in cryptography: Proceedings of Crypto '90*, (Springer-Verlag, New York, 1990), page 49.