Quantum Cryptographic Key Distribution Using An Optical Coupler

Yi Mu and Yuliang Zheng

Center for Computer Security Research, Department of Computer Science,
University of Wollongong, Wollongong, NSW 2522, AUSTRALIA
Email: {yi, yuliang}@cs.uow.edu.au

May 26, 1994

Abstract

We develop a quantum cryptographic key distribution protocol based on two non-commuting quantum states by utilizing an optical coupler in the receiver. Each bit of cryptographic signal is encoded using quadrature phase amplitudes, which cannot be simultaneously measured, according to the uncertainty principle in quantum physics. Quieter light output can be achieved in comparison to a conventional theoretical model based on two nonorthogonal quantum states, when a squeezed laser is used as incident light of the coupler waveguide.

Interest in quantum cryptography has recently been inspired due to its use in secure communications. Quantum cryptography employs quantum mechanical phenomenon such as Heisenberg's uncertainty principle [1, 2] so called BB protocol, and quantum correlation - Einstein-Podolsky-Rosen-Bohm *gedankenexperiment*(EPR)[3, 4] to protect distributions of cryptographic key. BB protocol suggests that information can be enclosed in one of two non-commuting observables so that any eavesdropper's attempt to extract the information by measurement will destroy some information. This causes a change in the signal between the legitimate users, which therefore reveals the the presence of the eavesdropper. EPR technique is initially developed to study Bell's inequality [5]. Interestingly, it has been shown to be useful for quantum cryptography. Under this scheme, the secure quantum key distribution can also be achieved by exploitation of the properties of quantum-correlated particles. Any eavesdropping unavoidably adds some local condition which causes the data measured by legitimate users to display no violation of Bell's inequality and then reveals the attempt at interception. The technique without using Bell's inequality has been developed by Bennett *et al*

A recent experiment [2] has demonstrated BB protocol can in principle prevent any eavesdropping attacks including intercept/resend and beamsplitting. However in order to overcome a beamsplitting attack, very dim light pulses had to be used. This therefore limits the transmission distance to about 32 cm. It is noted that an experimental work has demonstrated a single-photon transmission being up to 10 km by using single photon interference technique, a time-division Mach-Zehnder interferometer [6], which could be a good approach for quantum cryptographic systems. We have recently developed a higher power quantum cryptographic system, using state-mixing technique, which has been proved secure against any attacks including beamsplitting [7].

Different from BB protocol [2] which uses four nonorthogonal quantum states, quantum cryptography using any two nonorthogonal states has been studied by Bennett [8], by means of the photon interferometric mechanism. In this paper, we develop a cryptosystem which allows the cryptographic signal to be encoded in two non-commuting quadrature phase amplitudes of optical signal. The receiver employs an optical coupler which allows the cryptographic signal to couple with a squeezed light. The combination of the light pulses can gain the signal to noise ratio and hence quality cryptographic communication can be achieved.

Fig. 1 illustrates our cryptosystem using a single mode fibre and an optical coupler. The basic intention is to establish between two parties, say Alice and Bob, who share no

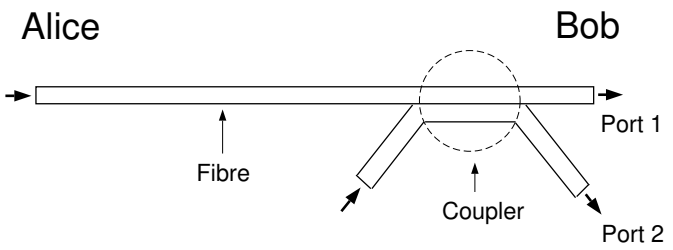

Figure 1: The schematic diagram of the quantum cryptosystem using two non-commuting quantum states and an optical coupler.

secret information in the cryptographic communication. Bob can choose his own input source for the coupler. Output signal is detected using two homodyne detectors, one for each port.

The signal mode in the fibre can be expressed by creation and annihilation operator $a^\dagger$ and a, which are now the signal mode sent by Alice. The incident light mode in the tap fibre is represented by creation and annihilation operator $b^\dagger$ and b that are controled by Bob. As shown in Fig. 1, for two isolated-mode optical waveguides with coupler constant κ, the waveguide fields after the coupled-mode interaction obey [9]

$$a' = (1-\kappa)^{1/2} a + \kappa^{1/2} b, \tag{1}$$

$$b' = -\kappa^{1/2} a + (1-\kappa)^{1/2} b. \tag{2}$$

$\kappa = 0$ corresponds to no signal exchange between the waveguides, while $\kappa = 1$ corresponds to a complete signal exchange between the waveguides. Corresponding field quadrature operators are

$$a_1 = (a + a^\dagger)/2, \quad a_2 = (a - a^\dagger)/2i, \tag{3}$$

$$b_2 = (b + b^\dagger)/2, \quad b_2 = (b - b^\dagger)/2i. \tag{4}$$

The explicit expression of quadrature components for coupled states can be obtained in terms of Eqs. (1)-(4). The uncertainty principle based those quadrature components is given by

$$\langle \Delta a_1^2 \rangle \langle \Delta a_2^2 \rangle \geq 1/16, \tag{5}$$

where $\langle \Delta a_1^2 \rangle$ ($\langle \Delta a_2^2 \rangle$) denotes the variance of a_1 (a_2). The formula is similar for mode b, while a being replaced by b in Eq. (5). The uncertainty inequality suggests that only one quadrature component can be accurately measured at one time.

Our quantum cryptographic protocol is arranged as follows:

Alice	Bob	Photon State After Coupling	$\theta = x_2/x_1$	Status
a_1	b_1	$a_1' = \frac{1}{\sqrt{2}}(a_1 + b_1)$	0	Enhanced
		$b_1' = \frac{1}{\sqrt{2}}(-a_1 + b_1)$		Canceled
	$-b_2$	$a_1' = \frac{1}{\sqrt{2}}a_1, \quad a_2' = -\frac{1}{\sqrt{2}}b_2$	-45^0	Uncertain
		$b_1' = -\frac{1}{\sqrt{2}}a_1, \quad b_2' = -\frac{1}{\sqrt{2}}b_2$	225^0	Uncertain
a_2	b_1	$a_1' = \frac{1}{\sqrt{2}}b_1, \quad a_2' = \frac{1}{\sqrt{2}}a_2$	45^0	Uncertain
		$b_1' = \frac{1}{\sqrt{2}}b_1, \quad b_2' = -\frac{1}{\sqrt{2}}a_2$	-45^0	Uncertain
	$-b_2$	$a_2' = \frac{1}{\sqrt{2}}(a_2 - b_2)$		Canceled
		$b_2' = -\frac{1}{\sqrt{2}}(a_2 + b_2)$	-90^0	Enhanced

Table 1: The result of the photon coupling. The illustration is based on a quadrature plane. x_1 denotes a_1' or b_1'; x_2 denotes a_2' or b_2'. We have assumed equal intensity for mode a and b.

1: Alice chooses a vector $A = (\alpha_1, \alpha_2, ..., \alpha_n)$ of n random bits, $\alpha_i \in \{a_1, a_2\}$.

2: Bob chooses a vector $B = (\beta_1, \beta_2 ...., \beta_n)$ of n random bits, $\beta_i \in \{b_1, -b_2\}$.

3: The communication is carried out by using very weak photon pulses. Alice sends α_i (encoded using quadrature component a_1 or a_2), while Bob uses β_i (enclosed using quadrature component b_1 or $-b_2$) that is coupled with α_i in Bob's optical coupler. The result of coupling action is shown in Table 1.

$$\text{Bob sets } \beta_i' = \begin{cases} 0 & \text{(a bright flash at Port 1 and nothing at Port 2),} \\ 1 & \text{(a bright flash at Port 2 and nothing at Port 1)} \end{cases}$$

Then repeat the process until whole string is sent.

4: Bob keeps B and $B' = (\beta_1', \beta_2', ..., \beta_n')$ secret. Alice keeps A secret.

5: Bob opens his commit to public: *Accept* if Bob saw a bright flash at Port 1 (2) (an double intensity) and nothing at Port 2 (1); *reject* if Bob saw flash at both ports (the intensity is about half of the previously mentioned cases). Note that Bob only needs to say: either "Yes" – accept or "No" – reject for each pulse.

6: Alice and Bob keep the instances which have been accepted as the key distribution.

Table 1 shows all possible coupling results in Bob's coupler, where four different cases are illustrated. If Alice and Bob use quadrature components either a_1 and b_1 or a_2 and $-b_2$, Bob will measure an enhanced signal at Port 1 or Port 2. Accordingly a cancellation of the signal at the other port is resulted. These instances contain real key information. However, if they use different quadrature components, i.e. Alice uses a_1 and Bob uses $-b_2$ or Alice uses a_2 and Bob uses b_1, Bob can view light from both ports, but dimmer than previous cases, since the phase of the coupled pulse has been changed. These instances have to be discarded, because the uncertainty exists in any measurement involving both quadrature components.

Notice that since α_i is chosen at random, it reveals no information to Eve. Of course, Eve can intercept it in the hope of learning something from her measurement. Say that Eve knows there are two detectors. One can correctly measure a_1 and the other can correctly measure a_2. However since she does not know which photon has been sent by Alice, she has no better way than to choose a detector randomly. If she chooses a correct detector, a correct measurement can be obtained; if she uses a wrong detector, a wrong result will be obtained in terms of the uncertainty principle. For instance, using a wrong detector to measure a_1 will create a wrong message a_2 for Eve. So if she wants to resend the signal she has measured to Bob, about half of the signal string will not be the original one sent by Alice, which will therefore cause substantial mistakes in Bob's measurement. The eavesdropping is then revealed.

If the field modes associated with a and b are in the states $|n_a\rangle$ and $|n_b\rangle$, we find that the signal to noise ratio, under a homodyne detection, for the detector one

$$SNR_1 = \langle a_1' \rangle^2 / \langle \Delta a_1'^2 \rangle = \frac{[(1-\kappa)^{1/2}\langle a_1 \rangle + \kappa^{1/2}\langle b_1 \rangle]^2}{(1-\kappa)\langle \Delta a_1^2 \rangle + \kappa \langle \Delta b_1^2 \rangle} \tag{6}$$

and for the detector two

$$SNR_2 = \langle b_2' \rangle / \langle \Delta b_2'^2 \rangle = \frac{[-\kappa^{1/2}\langle a_2 \rangle - (1-\kappa)^{1/2}\langle b_2 \rangle]^2}{\kappa \langle \Delta a_2^2 \rangle + (1-\kappa)\langle \Delta b_2^2 \rangle}, \tag{7}$$

where we consider the bright flashes only. We are particularly interested in the case of $\kappa = 1/2$. For an coherent state - a kind of minimum uncertainty state (the equality holds in Eq. (5)), the variance for both quadrature components is $1/4$, which reaches the classical limit or shot noise.

The substantial difference between Bennett's interferometer and our photon coupler lies in which one of coupled beams in our system is controlled by Bob, but not coming from Alice's transmitter. Therefore, in our system Bob can use a specific photon source

in his optical coupler. In particular, Bob can use a squeezed light [10], which has been extensively studied both theoretically and experimentally in last ten years. An ideal squeezed state is another kind of minimum uncertainty state. One quadrature component (say a_1) of the field has smaller fluctuations than the other quadrature component (say a_2), in terms of the uncertainty principle. Explicitly, $\langle \Delta a_1^2 \rangle < 1/4$ and $\langle \Delta a_2^2 \rangle > 1/4$. Using the quadrature component with less noise can greatly improve signal to noise ratio of the system.

Let us examine the signal to noise ratio using squeezed light for the mode b. The noise in the denominator observed in homodyne detection comes from both the signal mode sent by Alice (a) and the auxiliary coupler mode (b). If the intensity for both modes is equal, we find the ratio

$$\frac{SNR_{sq}}{SNR_{coh}} = 1 + \frac{\kappa}{1-\kappa} \frac{\langle \Delta b_1^2 \rangle}{\langle \Delta a_1^2 \rangle}, \tag{8}$$

where SNR_{sq} denotes the signal to noise ratio at port one when using profect squeezed light; SNR_{coh} is the signal to noise ratio for coherent input. If $\kappa = 1/2$ and Alice uses coherent light, then a twice increasing of the signal to noise ratio can been obtained. The calculate for part two is similar. Under current technique, squeezed light is not suitable for a long haul communication, since low noise property rapidly disappears during propagation. However, it presents premise for a local optical device, such as an optical coupler.

In summary, we have developed a novel cryptographic key distribution protocol that uses two non-commuting quantum states. We have shown how, in principle, the optical coupler using squeezed light can provide low-noise cryptographic signal which has the signal to noise ratio twice as much as that using coherent light. It is noted that our system is substantially different from the system developed by Bennett [8] using optical interferometric technique, in terms of the theory based and devices employed. Furthermore, our system has less noise.

This work is supported in part by the Australian Research Council under the reference number A49232172.

References

[1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, pp. 175–179, Bangalore, India, 1984.

[2] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, Journal of Cryptology **5**, 3 (1992).

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

[4] A. K. Ekert, J. G. Rarity, P. R. Tapster, and G. M. Palma, Phys. Rev. Lett. **69**, 1293 (1992).

[5] J. S. Bell, Physics (N.Y.) **1**, 195 (1965).

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

[7] Y. Mu, Y. Zheng, J. Seberry, and Y.-X. Lin, A quantum cryptosystem secure against beamsplitting attacks, (unpublished).

[8] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[9] J. H. Shapiro, Optics Letters **5**, 351 (1980).

[10] D. F. Walls, Nature **306**, 141 (1983), (and references therein).