An Alternative Model of Quantum Key Agreement via Photon Coupling

Yi Mu[1] and Yuliang Zheng[2]

[1] Department of Computing, University of Western Sydney,
Nepean, Kingswood, NSW 2747, Australia
[2] School of Computing & Information Technology, Monash University,
McMahons Road, Frankston, VIC 3199, Australia

Abstract. It has recently been shown that shared cryptographic quantum bits are achievable through the use of an optical coupler, instead of polarised photons. We show that such shared cryptographic bits can also be produced by using a different optical apparatus - a beam-splitter. An important advantage of such a system is that it could be experimentally more feasible than an optical coupler.

1 Introduction

The central idea behind quantum cryptography is that an eavesdropper cannot monitor transmission based on quantum mechanics without being noticed by participants. This feature is based upon quantum mechanical phenomena such as Heisenberg's uncertainty principle and quantum correlation. The later is represented by the EPR or Einstein-Podolsky-Rosen-Bohm *gedankenexperiment* [9, 1]. A well-known protocol was suggested by Bennett, Brassard and co-workers in Refs. [6, 5]. This protocol is now called BB protocol. The BB protocol shows that information can be enclosed in one of four nonorthogonal quantum states (based on photon polarisation) on two bases in such a way that any attempt to extract the information by an eavesdropper will randomise and hence destroy the information. In other words, the eavesdropper's acts will definitely cause a change in the signal between the legitimate users, which therefore reveals the presence of the eavesdropper. On the other hand it has been demonstrated that EPR and Bell's theorem or inequality [3] are also useful in quantum cryptography. Protocols based EPR and Bell's theorem exploit the properties of quantum-correlated particles [10]. A further simplified protocol which does not use Bell's inequality has been proposed by Bennett *et al*[8]. Although there are some other interesting protocols, for instance, by photon interferometry[4], teleporting [7], rejected-data[2], and so on, the BB protocol and Ekert's protocol are the most typical models in quantum cryptography.

Recently, it has been shown that without using polarised photons one can also achieve a secure quantum cryptographic protocol [11]. This system is based on an optical apparatus - optical coupler. In practice, however, there may exist certain difficulties to achieve efficient photon coupling, largely due to the fact a signal beam in the system is calculatedly chosen to be very weak in order to avoid potential beamsplitting attacks.

In this paper, using a beam-splitter, we develop a new quantum cryptosystem which also allows a cryptographic key bit to be encoded using four *nonorthogonal* quantum states described by non-commuting *quadrature phase amplitudes* (not photon polarisations !). We suggest that the proposed new system present a more promising solution from the experimental point of view.

Similarly to the system in Ref. [11], in the present system the nonorthogonal states are designed to have a large multi-overlap, hence it is impossible to obtain a certain result if a measurement is performed on only one of these states. This property forms the basis of security against any potential eavesdropping.

2 Background on quantum states and uncertainty

In this section, we briefly introduce some basic knowledge of quantum states, including coherent states and squeezed states, which will later be used to describe our system.

For a quantum field mode c, we can write it in the form of $c = c_1 + ic_2$, where c_1 and c_2 are quadrature phase amplitudes. The inequality of uncertainty for the quadrature phase amplitudes is given by

$$\langle \Delta c_1^2 \rangle \langle \Delta c_2^2 \rangle \geq 1/16. \tag{1}$$

where $\langle \Delta c_1^2 \rangle$ ($\langle \Delta c_2^2 \rangle$) denotes the variance of c_1 (c_2). Inequality (1) suggests that only one of two quadrature phase amplitudes is certain.

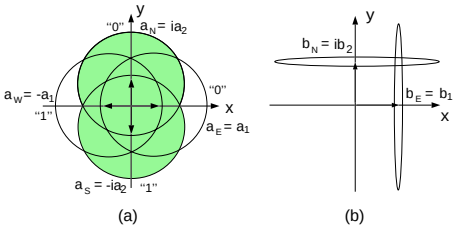

Fig. 1. On planes of quadrature-phase amplitudes, (a) shows Alice's encoding strategy based on four nonorthogonal coherent states; (b) shows Bob's probe modes using squeezed light. Uncertainty of a state is represented by error ellipses for squeezed states and by error circles for coherent states.

For a coherent state, since the photon distribution is Poissonian, the uncertainties for both quadrature-phase amplitudes are equal and the equality in (1) also holds. Hence both variances of the quadrature phase amplitudes are 1/4. Accordingly, in figure 1 (a) we can see a noise circle for each coherent state, where we have assumed that mode a represents a coherent state with four encoding arrangements $a_E = a_1$, $a_W = -a_1$, $a_N = ia_2$, and $a_S = -ia_2$ (east, west, north, and south states). Under our encoding strategy, overlaps among

these states should be as large as possible, thus it is accordingly assumed that the overlap between the east and west states is approximately 65%, so does the overlap between the north and south states. This requires that the mean number of photons for each state should be around 0.1. The absolute magnitude of overlap of two coherent states can be calculated by

$$|\langle\alpha|\beta\rangle|^2 = e^{-|\alpha-\beta|^2}. \tag{2}$$

With the mean number of photons per state being 0.1, it is easy to find that the overlap between the east and west state or the north and south states is 65%, and between the east and north states is around 82% (the same for each other pairs of neighbour states).

When a state is in an overlap between two states, it will not be able to be determined with certainly because it could belong to either of these states. On the other hand, when a state is not in the overlap region, it will be possibly determined without mixing with other states. Since under our arrangement *total* area of overlaps in a state is more than 90% and a large part of area has four overlap layers, it is almost impossible to obtain a certain result when performing a measurement on these states.

Homodyne detection is the most sound scheme for performing a measurement on a quadrature phase amplitude. The value of measurement is actually equal to the projection on the axis of the corresponding detector. We may lock a homodyne detector to an orientation, $x, -x, y$, or $-y$, which suits the measurements for different encodings, and consistently, we define four detection vectors V_x, V_{-x}, V_y, or V_{-y}, which in fact are four noncommuting projection operators.

We first look at homodyne detection performed on a *single* coherent state, the east state or the north state, and ignore the superposition for a while. In order to measure the east state, the homodyne detector must be locked at x direction (i.e., using V_x). This is because it has the largest probability of obtaining the correct result – a value of the mean $\langle a_1\rangle$, despite the uncertainty $\langle \Delta a_1^2\rangle$ =1/4. When utilising the same projection operator V_x to detect the north state, we will then be unable to obtain a correct value, but have a high probability of obtaining zero (the uncertainty also equals 1/4). On the other hand, if a state does not have any projection on the detection vector, the state will not be able to be determined. For example, using V_x, we cannot determine the west state, since it does not have any useful projection on V_x (except the projection due to noise). It is concluded that for obtaining a correct detection the detection vector must be set accordingly to the direction of the signal state.

Since we are using four nonorthogonal states and each state has a large area of overlap with other states, it is hardly possible to correctly determine one out of these states by using a homodyne detector. This feature presents a promise for us to apply these states to cryptography.

For a squeezed state which is a minimum uncertainty state, the equality of (1) will hold, while the variance of one of the quadrature components is squeezed (to zero for a perfect squeezed state) and the variance of the other quadrature component is enlarged (to infinity for a perfect squeezed state). Assuming that

b is a squeezing mode. The variances of quadrature phase amplitudes can be described by

$$\langle \Delta b_1^2 \rangle = \frac{1}{2} e^{-2r}, \quad \langle \Delta b_2^2 \rangle = \frac{1}{2} e^{2r}. \tag{3}$$

As showed in figure 1 (b), two orthogonal squeezed states are used by Bob as his input to the optical coupler. The mode $b_E = b_1$ corresponds to $r >> 0$, while the mode $b_N = ib_2$ corresponds to $r << 0$. One advantage of using squeezed light is that one of quadrature components can be measured with little influence of quantum noise.

The area of an ellipse for a mode represents uncertainty (or noise). For instance, we can see that, for the squeezed mode $b_E = b_1$ the x component (the projection on x axis) is knowable (small noise, ideally zero), but the y component (the projection on y axis) is uncertain (large noise, ideally infinity). We can explain the other mode similarly.

3 The new system

Our system is constructed using an optical beam-splitter as showed in figure 2, where a cryptographic communication is implemented between Alice and Bob. Alice is the sender who has a signal generator which can produce four nonorthogonal states and Bob is the receiver who measures the signal states by means of a beam-splitter. One feature of the system is that it allows cryptographic signals to be coupled with Bob's squeezed light. The coupling of light pulses provides us with a significant gain in the signal to noise ratio in comparison with that using a conventional coherent light source. This in turn provides us with a more efficient cryptographic key distribution protocol.

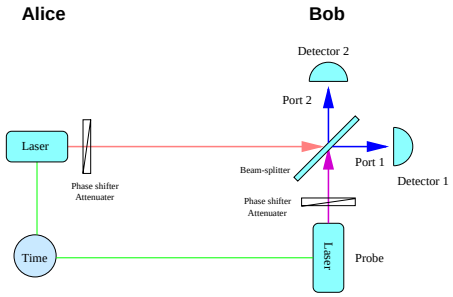

Fig. 2. The schematic diagram of the quantum cryptosystem using an optical beam splitter.

A quantised light field can be represented by a creation operator and an annihilation operator. We assume that Alice's signal mode is expressed by a creation operator $a^\dagger$ or an annihilation operator a and Bob's mode (the probe light) is represented by a creation operator $b^\dagger$ or an annihilation operator b. For a

50-50 beam-splitter with a mirror amplitude refectivity $1/\sqrt{2}$, the output beams obey

$$a' = \frac{1}{\sqrt{2}}[a\exp(i\theta_a) + ib\exp(i\theta_b)] = \frac{i}{\sqrt{2}}(a+b), \tag{4}$$

$$b' = \frac{1}{\sqrt{2}}[ia\exp(i\theta_a) + b\exp(i\theta_b)] = \frac{1}{\sqrt{2}}(-a+b) \tag{5}$$

where θ_a and θ_b are the reference phases of mode a and mode b, respectively. It is reasonable to assume $\theta_a = \pi/2$ and $\theta_b = 0$, which results in the second equalities. The above equations can be transferred into equations of quadrature phase amplitudes, with $a = a_1 + ia_2$ and $b = b_1 + ib_2$.

To simplify our discussions, we have employed a symmetric (50-50) beam-splitter. In practice, however, it might be necessary to use an asymmetric one that allows a large portion of Alice's signal to pass through (ideally, all photons). This change would be important, since Alice's signal is very weak.

4 The protocol

The basic intention is to establish a common key between two parties, Alice and Bob, who share no secret information at the beginning of the cryptographic communication. The beam-splitter is controlled by Bob who can independently choose the probe light (squeezed light). Both signal generators are controlled by a time base that guarantees a perfect photon coupling action. The output signal is detected using two homodyne detectors, one for each port. Also, importantly, in order to realise a perfect coupling action in the beam-splitter, Alice and Bob need to choose a phase reference before their communication starts. This can be done by Alice sending a sequence of bright reference pulses to Bob and publicly announcing their phases.

Alice's generator produces a faint coherent light, on the average, 0.1 photon per pulse, i.e., $\langle a^\dagger a\rangle = 0.1$. As we have mentioned, under this assumption the total overlap on a state is over 90%. The probability a signal pulse contains one or more photons is approximately 10%. This figure suggests that 90% of the total pulses are vacuum. Note that it is possible to employ a weaker signal light such that the superposition of the four nonorthogonal states is even larger. However we do not intend to do that, since our assumption is sufficient for our cryptographic protocol. Bob's squeezed light is much brighter and has on average one photon per pulse.

Because of the noise of light, it is very difficult for Bob to identity the correct detection result. In order to resolve this problem, we give the following definition:

Definition screening criterion *An output bit from the beam-splitter is recorded, if and only if Bob finds that two photons are projected on the detector at one port and nothing is projected on the detector at the other port.*

Bob's measurements are based on a homodyne detection scheme, where both detectors are arranged in terms of the probe mode used by Bob himself. Bob

Table 1. The results of the photon coupling. The illustration is based on a quadrature plane. We have assumed equal intensity for both mode a and mode b, the symbol "$\times$" represents "discarded", C represents "Cancelled", E represents "Enhanced", and a sign, character or binary figure in front of "/" has a higher probability of appearance. In other words, those in front of "/" are correct; those behind "/" are associated with the overlap on the corresponding opposite state. The later ones can be corrected eventually.

Alice's mode	Bob's mode	Output from Beamsplitter	Measurement			Final Result
			Vector	Status	Result	
a_E	b_E	$a' = \frac{i}{\sqrt{2}}[(+/-)a_1 + b_1]$	V_y	E/C	0/1	0
		$b' = \frac{1}{\sqrt{2}}[(-/+)a_1 + b_1]$	V_x	C/E		
	b_N	$a' = \frac{i}{\sqrt{2}}[(+/-)a_1 + ib_2]$	V_{-x}	Uncertain	$\times$	
		$b' = \frac{1}{\sqrt{2}}[(-/+)a_1 + ib_2]$	V_y	Uncertain		
a_W	b_E	$a' = \frac{i}{\sqrt{2}}[(-/+)a_1 + b_1]$	V_y	C/E	1/0	1
		$b' = \frac{1}{\sqrt{2}}[(+/-)a_1 + b_1]$	V_x	E/C		
	b_N	$a' = \frac{i}{\sqrt{2}}[(-/+)a_1 + ib_2]$	V_{-x}	Uncertain	$\times$	
		$b' = \frac{1}{\sqrt{2}}[(+/-)a_1 + ib_2]$	V_y	Uncertain		
a_N	b_E	$a' = \frac{i}{\sqrt{2}}[b_1 + (+/-)ia_2]$	V_y	Uncertain	$\times$	
		$b' = \frac{1}{\sqrt{2}}[b_1 - (+/-)ia_2]$	V_x	Uncertain		
	b_N	$a' = \frac{i}{\sqrt{2}}[(+/-)ia_2 + ib_2]$	V_{-x}	E/C	0/1	0
		$b' = \frac{1}{\sqrt{2}}[(-/+)ia_2 + ib_2]$	V_y	C/E		
a_S	b_E	$a' = \frac{i}{\sqrt{2}}[b_1 - (+/-)ia_2]$	V_y	Uncertain	$\times$	
		$b' = \frac{1}{\sqrt{2}}[b_1 + (+/-)ia_2]$	V_x	Uncertain		
	b_N	$a' = \frac{i}{\sqrt{2}}[(-/+)ia_2 + ib_2]$	V_{-x}	C/E	1/0	1
		$b' = \frac{1}{\sqrt{2}}[(+/-)ia_2 + ib_2]$	V_y	E/C		

should have a rule which allows him to determine which detection vector needs to be used.

Definition detection rule *If the probe mode is associated with b_E, the detector at Port 1 is set toward the y direction (using V_y) and the detector at Port 2 to the x direction (using V_x); if the probe mode is associated with b_N, the detector at Port 1 is set to $-x$ direction (using V_{-x}) and the detector at Port 2 to y direction (using V_y).*

Under the detection rule, Bob needs only two sets of detection vectors: $\{V_y, V_x\}$ and $\{V_{-x}, V_y\}$. Each time Bob chooses only one of them.

Our quantum cryptographic key distribution protocol is described as follows:

During the preparation stage, both Alice and Bob need to prepare their data. Assuming that α_i is randomly selected from four quantum states $a = \{a_E, a_W, a_N, a_S\}$, Alice constructs a vector $A = (\alpha_1, \alpha_2, ..., \alpha_n)$ of n random choices, $\alpha_i \in a = \{a_E, a_W, a_N, a_S\}$. a is public information, while A is private

data only known to Alice. Bob independently chooses a vector $B = (\beta_1, \beta_2 ...., \beta_n)$ of n random choices, $\beta_i \in b = \{b_E, b_N\}$. b is public information, but B is private data only known to Bob.

Phase one: Signal transmission and measurement:

1: Alice sends Bob a $\alpha_i \in A$, while Bob injects a β_i which interacts with α_i in Bob's beam-splitter. All possible outcomes are shown in Table 1. In terms of the subsequent detection and the screening criterion,

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

Otherwise, Bob deletes the bit. Alice and Bob repeat the process until the whole signal string is sent. "bright flash" means that two photons have been projected on Bob's detection vector.
Bob keeps B and $B' = (\beta_1', \beta_2', ..., \beta_n')$ secret.

2: Bob speaks to Alice publicly for each β_i': *Accept* if Bob "saw" a bright flash at Port 1 (2) and nothing at Port 2 (1) (obeying the screening criterion); *reject* if Bob "saw" flashes at both ports or other instances which do not satisfy the screening criterion.

3: Bob announces to Alice which detection vector has been used for each accepted bit (but nothing about the outcome of the measurement).

4: Alice asks Bob to delete those bits obtained using an incorrect detection vector. For example, Alice may ask him to delete a north-state-related "0" bit which is obtained by using V_x. This step ensures that all flawed bits subject to the overlaps with two closer neighbour states (but not the opposite state) are removed. (We will give more explanation later.)

Phase two: Error correcting:

Up to now, Bob's remaining bits still contain a number of flawed bits subject to overlap with the opposite states. In order to correct (but not remove) the flawed bits, the following steps should be taken:

1: Alice secretly divides all remaining bits related to each state, east, north, west, or south into N groups ($N \geq 100$), where each group contains m bits (in the present case, $m \geq 30$ is appropriate). This requires that the number of original signal bits sent by Alice are sufficient. Each group involves only one signal state, but both binary bits. Amongst these binary bits, one fraction of binary bits ("0" or "1") stem from the correct detections and these bits are the majority; the other fraction of binary bits ("1" or "0") come from the overlap on the opposite state. Note that during the grouping the original positions of the bits were not changed.

2: Alice publicly announces the grouping result, without releasing any encoding information. So nobody knows which group belongs to which state, except Alice herself. Since each Bob's detection vector has been used for two nonorthogonal states, knowing the detection vector of each group releasees no encoding information of the group.

3: Bob calculates the number of "0" or "1" bits in each group. The encoding of the majority bits will represent the encoding of *all bits* in the group. For example, if Bob finds that "0" bits are the majority, he will regard all bits in the group as "0". So far Bob has corrected all mistakes caused by the overlap with the corresponding opposite state and has obtained the encoding information of each group. This step can only be implemented by Bob, because he is the only one who knows the measurement result.

4: Bob tells Alice the positions of all useful bits. Alice knows the full information of these bits.

Upon the completion of communication, Alice and Bob keep the bits which have eventually survived as the secret key.

Our system is summarised in Table 1 and Figure 3. The latter illustrates the protocol.

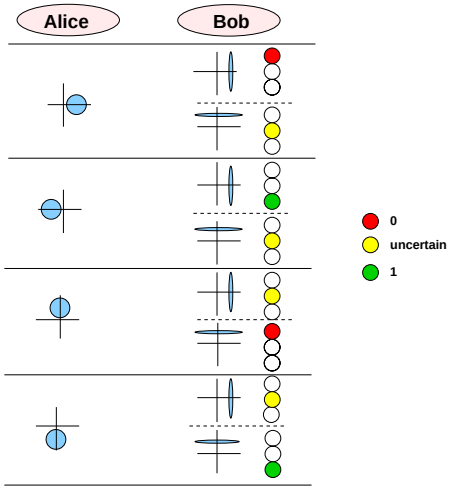

Fig. 3. The summary of the system: light modes and the results are given. The traffic lights are used to illustrate the result of implementing the protocol.

5 Analysis

In comparison with the protocol presented in Ref. [11], the main difference is that in the present protocol, Bob uses different sets of detection vectors. The change is due to the modification of the signal/probe phase.

Table 1 shows all possible detection results obtained by Bob when both light pulses have the same intensity. Instead of explaining all cases in the table, we only focus on the first case, where Alice uses the east state a_E. The explanations

for the remaining cases are similar. In the first case, Bob uses b_E (and V_x consistently). According to the coupling equations, there are two possible outcomes: (1) The output at port 1 is enhanced and the output at port 2 is reduced to a vacuum state due to the cancellation. Bob then further checks whether the outputs satisfy the screening criterion. If the answer is yes, a "0" is accordingly recorded. (2) Because of the superposition between the east state and the opposite west state, a large fraction of bits associated with the east state turn out being mixed with the west state, and Bob could then have a false result and a "1" is hence recorded. The latter is obviously wrong, but Bob is aware of his mistake. In order to overcome this problem, Alice divides all accepted bits related to the east state into N (say 100) groups and each group contains m (say 30) bits (see also our analysis to be presented later). By calculating the number of "0" or "1" bits, Bob is able to find the majority bits which will be used to represent the encoding of all bits in the group. The mechanism of this error correcting method is simple: since the overlap between the states is not 100%, there is a larger probability of obtaining the east state rather than the west state. This is obviously true, because only if the superposition is 100%, the probability of obtaining the east state or the west state is 1/2,

By means of a Q-representation, we can further explain the error correcting method. A coherent state α in a Q-representation is given by

$$Q(\gamma) = \frac{1}{\pi} e^{-|\gamma-\alpha|^2}, \tag{6}$$

which actually represents a quasi-probability of the coherent state. For the east coherent state with an average projection value of 0.33 (an intensity of 0.1 photon) on the x axis (on the quadrature-phase plane), the probability of a projection being around 1 on a small region $(\Delta x) \cdot y$, where $-\infty < y < \infty$, is given by

$$P(projection = 1|\alpha = 0.33) = \frac{1}{\sqrt{\pi}} e^{-0.67^2} \Delta x \approx 0.36 \Delta x, \tag{7}$$

while the probability of projection being -1 on the small region is given by

$$P(projection = -1|\alpha = 0.33) = \frac{1}{\sqrt{\pi}} e^{-1.33^2} \Delta x \approx 0.0963 \Delta x. \tag{8}$$

It is easy to find that, amongst the total pulses with a value 1 or -1 projection on x axis, the 1-pulses is 79% and the -1-pulses 21%. According to these data, we may roughly calculate the correctness rate of Bob's error correcting: assuming that $m = 30$ and the minimal number of bits m_{min} for Bob to correctly identify the encoding is greater than $m/2 = 15$, we have the correctness rate:

$$P(m_{min} > m/2) = 1 - \sum_{i=1}^{m} \left(\begin{array}{c} m \\ i \end{array} \right) (0.79)^i (0.21)^{m-i} \approx 0.9996. \tag{9}$$

This value suggests that Bob is almost 100% correct. Note however that if an eavesdropper wants to measure the signal, she cannot have such a high ratio of 1-pulses to -1-pulses, since her detection is subject to the superposition from

other two neighbour states, the north and south states. More serious problem for the eavesdropper is that she does not know which detection vector should be used. Bob does not have this problem, because Alice can ask him to delete all bits owing to the superposition with the two neighbour states and due to using incorrect detection vectors. This case will be further studied in next section.

We now focus on the second case, i.e., Alice still uses $a = a_1$ and Bob uses the other mode b_N (and V_y, consistently). Bob is obviously wrong. Most possibly, the outputs at one or both ports are nonzero, Bob can thus "view" a light flash with a various intensity at one or both ports. These bits are useless and can be removed in terms of the screening criterion. However, since the measurement is subject to the noise or overlaps, we must consider that Bob might occasionally obtain a result which meets the screening criterion. When this happens, Bob will not be able to identify the flaw. In order to get rid of these flawed bits, no matter what measurement result has been obtained, Alice will ask Bob to remove the bit.

We have not explained the influence of overlaps associated with the two neighbour states, the north and south states. These instances actually belong to other two cases where Alice sends the north or south state. The corresponding flawed bits will be handled by Alice and Bob using a similar procedure to that given above.

6 Discussion

We have made clear that the quantum states used in our system are not identifiable due to the superposition. More explanations are provided in this section to detail the various potential eavesdroppings from case to case. Some of discussions here have been given in Ref. [11].

- Intercept/resend:
  An adversary (Eve) would intercept the signal and measure it by using a similar apparatus. If she does so, at least half of her measurements will be random, because she has to randomly select her probe states and detection vectors. Moreover, the remaining half of Bob's measurements are also uncertain due to the superposition with respect to Alice's signal. Therefore, it is impossible for Eve to regenerate and resend the signal to Bob, using her own measurement.
- Direct detection:
  Assume that Eve knows that four projection operators, $\{V_{-x}, V_x, V_{-y}, \text{ and } V_y\}$, can be used to detect Alice's signal and these detection vectors respectively suit detecting a_E, a_W, a_N, and a_S. Eve might then wish to use her detector to measure Alice's signal directly, instead of using an optical coupler. However since she does not know which state has been sent by Alice, she has no better way than to choose a detection vector randomly. The probability of choosing the correct detection vector is obviously 1/4. Fortunately, even if she happens to select the correct detector, her measurement is still uncertain

because of the overlap of the encoding states. If Eve has a correct detection vector and knows that a projection of value 1 is important, it is not hard to find there is a probability of 3/5 for her obtaining a wrong projection belonging to the neighbour states. These bits cannot be identified by Eve. The total success rate of measuring a bit is found to be 1/10. In fact it is impossible for Eve to know whether or not she has used the correct detection vector, since, from Bob's public information, she can only know either V_x or V_y has been used by Bob (V_x or V_y corresponds to two Alice's states). This suggests that even if Eve's success rate is 1/10, she cannot know which detection is successful. Consequently, Eve achieves nothing from such eavesdropping.

- scanning the conversation:

  Eve may not do anything but just listens to Alice and Bob's public conversation. After Alice and Bob implement the protocol, Eve is aware which detection vector has been used, which bits were accepted, and which detection vector has been applied to each group chosen by Alice. Because each Bob's detection vector corresponds to two nonorthogonal states, Eve can only guess whether the bits in each group belong to either "0" or "1". Hence, for each individual group, Eve has a 1/2 chance to succeed. However, since the number of groups for each state $N > 100$, Eve's success rate will be less than $1/2^{400}$ or approximately $1/10^{120}$. In practice, it is highly unlikely for Eve to succeed.

- Statistical analysis:

  The requirement for the number of bits in each group depends on the superposition of encoding states. As discussed in the previous section, if the average number of photons is 0.1, $m = 30$ is appropriate for Bob to obtain a good success rate. However, if Eve has a little knowledge about the encodings, she could also implement a similar statistical analysis. How can Eve obtain a small piece of information on a group? Eve knows that it will not work, if she intercepts all signal pulses. In order to avoid being detected, Eve may randomly intercept/measure only a small fraction of signal pulses using the four detection vectors, for instance 10% in the total number of pulses, and lets the rest go through without being interfered. Can Eve then have good guesses? In the case $m = 30$, Eve intercepts only 3 pulses (among 30). The measurement on the 3 pulses (based on randomly choosing measuring vector) is not adequate for her to implement a statistical analysis. Moreover, intercepting 10% of total pulses could also result in a substantial influence on Bob's measurement which could reveal Eve's attempt.

  However, if the size of m is large, say 1000, with intercepting a small number of bits Eve may then have enough bits used for her statistical analysis. Again, the big problem for her is how to obtain useful encoding information on these bits. The most thinkable way could still be the interception, but according to the discussion in the second paragraph of present section, Eve cannot obtain any useful information even for a single bit. Consequently, even if m is large, Eve is still unable to carry out a statistical analysis. However, there might be some other unseen way such that Eve could obtain a small

fraction of information from Alice's signal. A large m will then in principle be useful for Eve. Therefore we should define an upper limit for m. Because the upper limit depends on the superposition of the signal, we can only define a general criterion: the limit on m should be the minimum value where Bob has a satisfied success rate.

7 Conclusion

In this paper, we have shown that using a beam-splitter and four nonorthogonal states is promising for constructing a secure quantum exchange-key system which is not detectable to eavesdroppers. The main contributions of this work are the proof of availability of beam-splitters and the extension of the proceeding system based on an optical coupler [11] to a experimentally more promising model.

References

1. Aspect, A., Grangier, P., Roger, G.: Experimental realization of Einstein - Podolsky - Rosen - Bohm *gedankenexperiment*: A new violation of Bell's inequalities. Phys. Rev. Lett. **49** (1982) 91–94.
2. Barnett, S. M., Huttner, B., Phoenix, S. J. D.: Eavesdropping strategies and rejected-data protocols in quantum cryptography. Journal of Modern Optics **40** (1993) 2501–2513.
3. Bell, J. S.: On the Einstein Podolsky Rosen Paradox. Physics (N.Y.) **1** (1964) 195.
4. Bennett, C. H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. **68** (1992) 3121–3124.
5. Bennett, C. H., Bessette, F., Brassard, G., Salvail, L., Smolin, J.: Experimental quantum cryptography. Journal of Cryptology **5** (1992) 3–28.
6. Bennett, C. H., Brassard, G., Breidbard, S., Wiesner, S.:. Quantum cryptography, or unforgeable subway token. In Advanced in Cryptography: Prodeedings of Crypto 82 (1983) Plenum Press pp. 267–275.
7. Bennett, C. H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., Wootters, W. K.: Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys. Rev. Lett. **70** (1993) 1895–1899.
8. Bennett, C. H., Brassard, G., Mermin, N. D.: Quantum cryptography without Bell's theorem. Phys. Rev. Lett. **68** (1992) 557–559.
9. Bohm, D. J.:. "Quantum Theory". Prentice-Hall, Englewood Cliffs, N.J. 1951.
10. Ekert, A. K., Rarity, J. G., Tapster, P. R., Palma, G. M.: Practical quantum cryptography based on two-photon interferometry. Phys. Rev. Lett. **69** (1992) 1293–1295.
11. Mu, Y., Seberry, J., Zheng, Y.: Shared cryptographic bits via quantized quandrature phase amplitudes of light. Optics Communications (1996).

This article was processed using the LaTeX macro package with LLNCS style