Vol 18 No 8, August 2009
1674-1056/2009/18(08)/3238-05

Chinese Physics B

© 2009 Chin. Phys. Soc.
and IOP Publishing Ltd

Quantum secret sharing protocol using modulated doubly entangled photons*

Wang Chuan(王 川)† and Zhang Yong(张 勇)

School of Science and Key Laboratory of Optical Communication and Lightwave Technologies, Beijing University of Posts and Telecommunications, Beijing 100876, *China*

(Received 7 November 2008; revised manuscript received 2 December 2008)

In this paper, we propose a quantum secret sharing protocol utilizing polarization modulated doubly entangled photon pairs. The measurement devices are constructed. By modulating the polarizations of entangled photons, the boss could encode secret information on the initial state and share the photons with different members to realize the secret sharing process. This protocol shows the security against intercept-resend attack and dishonest member cheating. The generalized quantum secret sharing protocol is also discussed.

Keywords: quantum secret sharing, doubly entangled photons
PACC: 0367

The purpose of classical secret sharing is to distribute secret keys between the boss and his two or more agents. The boss expects to generate secret keys with the two agents separately and the two agents cannot reveal the boss's information until they combine their results. Quantum cryptography is an important branch of quantum information which combines quantum mechanics and classical communications, and quantum secret sharing (QSS) is a special utilization of quantum mechanics in classical secret sharing. The basic model of QSS permits the boss and two (or more) remote parties to share the secret keys and any eavesdropping behavior will be discovered by the communication parties. QSS was first proposed by M. Hillery, V. Bužek and A. Berthiaume[1] (here we called HBB quantum secret sharing protocol). In HBB protocol, a three-particle maximally entangled state (the Green–Horne–Zeilinger state) is used to realize the secret sharing process. Koashi and Imoto considered the correlation of the two-qubit Bell state in their quantum secret sharing scheme.[2] The idea of QSS have attracted a vast amount of research effort ever since the work of M. Hillery *et al* . There have been many theoretical developments in this subject,[3−15] and the experiment research of QSS has also progressed rapidly.[16−18]

Traditionally, the polarization entangled photon pairs are generated by a spontaneous parametric down conversion (SPDC)[19] process in which a nonlinear crystal was pumped by high intensity lasers and two photons marked with idler (i) and signal (s) are created under the phase match conditions: $\omega_p = \omega_s + \omega_i$, $k_p = k_s + k_i$. Here in Ref.[20] the authors proposed the scheme of doubly entangled photon state (DEPS) generation and experimentally realized it by using a AlGaAs multi-layer waveguide under the pumping of laser pulses. The scheme shows a higher conversion efficiency than the usual methods. The frequency and polarization maximally entangled DEPS can be written as:

$$|\Psi_{ab}^{+}\rangle = \frac{1}{\sqrt{2}}(|H,\omega_s\rangle|V,\omega_i\rangle + |V,\omega_{s'}\rangle|H,\omega_{i'}\rangle). \quad (1)$$

Here H and V represent the horizontally and vertically polarized states of photons, respectively, ω_s, $\omega_{s'}$, ω_i, $\omega_{i'}$ are the frequencies of the signal photons and idler photons, respectively. The entanglement purification protocol of DEPS has been studied recently.[21]

Here in this paper, we propose a high capacity QSS protocol exploiting polarization and frequency doubly entangled photon states. Suppose the boss Charlie wants his two agents Alice and Bob to finish the secret sharing tasks. And Charlie owns the doubly entangled photon source which generates the photons in the state $|\Psi_{ab}^{+}\rangle$.

The quantum secret sharing process is described as follows: Charlie prepares a series of DEPSs in the state $|\Psi_{ab}^{+}\rangle$ and performs jointly unitary operations $L_A \otimes L_B$ on each of the entangled pairs. The opera-

*Project supported by the National Natural Science Foundation of China (Grant No 10704010).
†Corresponding author. E-mail: chuan-wang03@mails.tsinghua.edu.cn

tion L is chosen randomly from the set $[I, \sigma_z, \mathrm{i}\sigma_y, \sigma_x]$. This operation transforms the initial state $|\Psi_{ab}^{+}\rangle$ to other eight bases shown below:

$$|\Phi_{ab}^{\pm}\rangle = \frac{1}{\sqrt{2}}(|H,\omega_s\rangle_a|H,\omega_i\rangle_b \pm |V,\omega_{s'}\rangle_a|V,\omega_{i'}\rangle_b); \quad (2)$$

$$|\Psi_{ab}^{\pm}\rangle = \frac{1}{\sqrt{2}}(|H,\omega_s\rangle_a|V,\omega_i\rangle_b \pm |V,\omega_{s'}\rangle_a|H,\omega_{i'}\rangle_b); \quad (3)$$

$$|\Gamma_{ab}^{\pm}\rangle = \frac{1}{\sqrt{2}}(|V,\omega_s\rangle_a|H,\omega_i\rangle_b \pm |H,\omega_{s'}\rangle_a|V,\omega_{i'}\rangle_b); \quad (4)$$

$$|\Upsilon_{ab}^{\pm}\rangle = \frac{1}{\sqrt{2}}(|V,\omega_s\rangle_a|V,\omega_i\rangle_b \pm |H,\omega_{s'}\rangle_a|H,\omega_{i'}\rangle_b). \quad (5)$$

Charlie separates the two photons and distributes his photon sequence $[a_1b_1, a_2b_2, a_3b_3, \ldots, a_nb_n]$ to Alice and Bob, respectively, which means the photon sequence marked with a is sent to Alice and the sequence marked with b is sent to Bob. For the purpose of secure communication, Charlie randomly adds some checking photons (called "decoy photons") into the sequence.[22] The polarization of the photons are randomly in one of the four states: $|H\rangle$, $|V\rangle$, $|H+V\rangle$, $|H-V\rangle$. And the frequencies of the photons are ω_s or $\omega_{s'}$ in the a sequence and are ω_i or $\omega_{i'}$ in the b sequence.

When the two photons arrive at Alice's and Bob's sides, they perform the security checking procedures with Charlie on the "decoy photons" respectively. Then they send the remaining photons into their measurement devices. They record the time instances at which the detectors clicked and the results of the detectors. Then both Alice and Bob announce the time instances when they detected the photons. For the time instance when Alice and Bob both received the signals, they record it as the shared key. For the time instance when only one of them receives the signals, they recorded it as the loss signal since one photon might be lost during the channel transmission or there might be dark counts on the detectors. Dropping the loss instance, they share a sequence of keys with Charlie. Alice and Bob cannot recover the secret keys unless they combine their results.

The apparatus of DEPS QSS is shown in Fig.1. Charlie's source locates between Alice and Bob. When the photon pairs arrive at Alice and Bob's detection device, they both pass through the WDM device and inject into different ports of PBS. Between WDM and PBS, there is C for the wavelength conversion process which is described in Refs.[23] and [24]. It consists of a WDM coupler, a periodically poled lithium niobate (PPLN) waveguide and a filter. The photons pass through the WDM as signal light and are pumped by a high intensity laser with a certain wavelength on a PPLN waveguide. The filter followed is used to filter out the pump laser light. Then the sum-frequency process generates a photon with frequency ω. The frequencies of a and b photons are changed to the same frequency by the wavelength conversion process, which means that the DEPSs transform to usual Bell states.

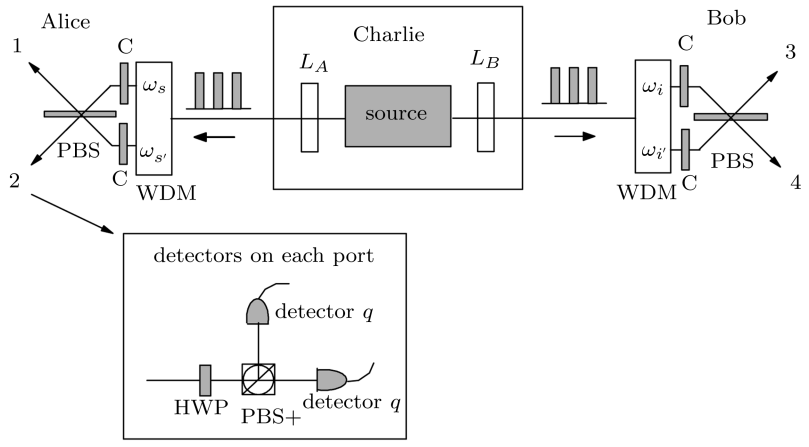


Fig.1. Quantum secret sharing apparatus. Here WDM is the wavelength-division multiplexing device. HWP and PBS are the half wave plate and the polarizing beam splitter, respectively. C is used to induce the wavelength conversion process.

Then the photons with the same frequency are measured by σ_x measurement which trigger the detectors at different ports. We can see in Table 1 the correspondence between the detector clicks and the states. Here we mark the detector on the transmitted line with p and the detector on the reflected line with q. For example, assume that Charlie's secret message is encoded in the state $|\Phi_{ab}^{+}\rangle$. When the photons arrive at the detectors, Alice's p detector on port 2 is clicked and Bob's p detector on port 4 is clicked, or Alice's q detector on port 2 and Bob's q detector on port 4 are clicked. When one round of secret sharing is finished, Alice and Bob record two clicks of the detectors. By repeating the process many times, the recorded information can be shared as the secret keys between the three parties.

Table 1. The correspondence between the detector clicks and the states. The numbers 1, 2, 3, 4 indicate the ports of the measurement devices and p, q indicate the two detectors on different lines.

triggered ports	corresponding states
2p,4p(2q,4q)	$\|\Phi^{+}\rangle$
2p,4q(2q,4p)	$\|\Phi^{-}\rangle$
2p,3p(2q,3q)	$\|\Psi^{+}\rangle$
2p,3q(2q,3p)	$\|\Psi^{-}\rangle$
1p,3p(1q,3q)	$\|\Upsilon^{+}\rangle$
1p,3q(1q,3p)	$\|\Upsilon^{-}\rangle$
1p,4p(1q,4q)	$\|\Gamma^{+}\rangle$
1p,4q(1q,4p)	$\|\Gamma^{-}\rangle$

In the DEPS QSS protocol, security checking is performed both between Alice and Charlie and also between Bob and Charlie. The security checking procedures are equivalent to the security checking in BB84 quantum key distribution.[25] In the DEPS QSS procedure, Charlie produces a series of "decoy photons" in the AC and BC sequence, respectively. The "decoy photons" are in the states $|H,\omega_{s(s')}\rangle, |V,\omega_{s(s')}\rangle, |H \pm V,\omega_{s(s')}\rangle$ corresponding to the AC channel and in the states $|H,\omega_{i(i')}\rangle, |V,\omega_{i(i')}\rangle, |H \pm V,\omega_{i(i')}\rangle$ corresponding to the BC channel. After Charlie distributes all the photons with Alice and Bob, he announces the positions of the "decoy photons" used for security checking. Then Alice (Bob) chooses to measure the sample qubit in either the σ_z or the σ_x basis. Then they announce the basis information to Charlie along a classical channel. For the bases they choose which are the same with Charlie's, they keep the results and compare the results with Charlie, respectively. If the error rate of both channels are lower than the security bound, then the secure communication process is secure.

The DEPS QSS protocol is robust against intercept-resend attack and dishonest member cheating. In the QSS process, there is only one photon in the channel at each time slot. When Eve performs intercept-resend attack, the photon will be lost and will not trigger simultaneously on Alice's and Bob's detectors if she eavesdrops the photon without adding a fake one. Eve has to finish her intercept-resend attack in the transmission process, i.e., Eve performs a Bell state measurement on each time slot on the two photons. Using the DEPS measurement device, Eve reads out the state completely. But the Bell state measurement will introduce errors to the "decoy photons". If Charlie adds a $|H+V,\omega_s\rangle_a \otimes |H+V,\omega_{i'}\rangle_b$ state, the two photons will pass through the WDMs along the ω_s and $\omega_{i'}$ ports when Eve performs a Bell state measurement. Then the photon will be transmitted with 50% probabilities and be reflected with 50% probabilities by the polarizing beam splitter. The state will cause clicks on the four ports with equal probabilities. For example, if Eve's clicks are on the 2p and 4p ports, then she produces the state $|\Phi_{ab}^{+}\rangle$ and sends to Alice and Bob the a and b photons, respectively. Alice's and Bob's measurements will cause errors on the security checking photons and the error rate is 75%. So Eve's intercept-resend attack will be discovered by the communication parties.

Suppose there is one dishonest party, say Bob, in the secret sharing process, Charlie encodes the secret keys by performing the $L_A \otimes L_B$ operations, then he sends photons to Alice's and Bob's channels, respectively. The dishonest agent Bob tries to get full information on the secret keys without being discovered by Alice and Charlie using the intercept and resend attack.

In the DEPS QSS protocol, Bob cannot avoid blocking the "decoy photons". With the photons in the state $|H,\omega_{s(s')}\rangle$, $|V,\omega_{s(s')}\rangle$, $|H \pm V,\omega_{s(s')}\rangle$, Bob cannot distinguish them from the DEPS. For example, if Bob intercepts the security checking photons in the state $|H,\omega_s\rangle \otimes |H,\omega_i\rangle$ and sends them to the measuring apparatus. With the operation of the polarizing beam splitter and the half wave plate, the $|H,\omega_s\rangle \otimes |H,\omega_i\rangle$ state becomes

$$\begin{aligned} & |H,\omega_s\rangle|H,\omega_i\rangle \\ \mapsto\ & |H,\omega_s\rangle|H,\omega_i\rangle + |H,\omega_s\rangle|V,\omega_i\rangle \\ & + |V,\omega_s\rangle|H,\omega_i\rangle + |V,\omega_s\rangle|V,\omega_i\rangle. \end{aligned} \tag{6}$$

The state may trigger the detectors on ports 2 and 4 and will be misunderstood by Bob to be the state $|\Phi_{ab}^{+}\rangle$. Then Bob prepares the state $|\Phi_{ab}^{+}\rangle$ and propagates the a photon to Alice. After the transmission of photons, Charlie and Alice perform the security checking. At first, Charlie announces the positions of the checking bit. Alice selects to measure them in either the σ_x or the σ_z basis as in the BB84 quantum key distribution protocol. With half the probabilities she chooses the correct basis (σ_z) but gets the wrong result. With the case Alice chooses the σ_x measurement, they omit the results. Alice and Charlie check the errors of the results publicly, if the error rate is higher than the security bound, they would discover the existence of a potential eavesdropper.

If Bob performs an individual attack[26,27] in which he attaches each of the a photons with an ancillary photon and makes a joint unitary operation, the operation can be described by:

$$\begin{aligned}\hat{J}_B|H\rangle_a \otimes |e_{B1}\rangle &= |H\rangle_a \otimes |\xi'_{B1}\rangle \\ \hat{J}_B|V\rangle_a \otimes |e_{B1}\rangle &= \cos\phi|V\rangle_a \otimes |\xi_{B1}\rangle \\ &\quad + \sin\phi|H\rangle_a|\xi'_{B1}\rangle; \end{aligned} \tag{7}$$

here e_{B1} represents the state of the ancillary photon. Then Bob performs a measurement on his b and e_{B1} photons and reads out the secret results that Charlie encoded. The individual attack may also introduce errors on the "decoy photons" and Bob's individual attack will introduce errors of $\sin^2\theta/2$. So any eavesdropping behavior performed by the dishonest member will be discovered by the security checking process.

The experimentally realized DEPS are in the generalized form

$$\begin{aligned}|\text{ent}\rangle &= \frac{\eta_1}{\sqrt{|\eta_1|^2+|\eta_2|^2}}|\omega_{S,1},H\rangle|\omega_{I,1},V\rangle \\ &\quad + \frac{\eta_2}{\sqrt{|\eta_1|^2+|\eta_2|^2}}|\omega_{S,2},V\rangle|\omega_{I,2},H\rangle. \end{aligned} \tag{8}$$

Here coefficients η_1 and η_2 represent the degrees of entanglement. The DEPS QSS protocol can also be realized using the non-maximally entangled state.[28] When the communication starts, Alice and Bob measure the two photons in the generalized form. The degree of frequencies guarantees the photons to pass the corresponding ports of WDMs and the degree of polarization guarantees them transmitting the corresponding ports of PBS. After the wavelength conversion process, the state transforms to

$$\begin{aligned}|\text{ent}'\rangle &= \frac{\eta_1}{\sqrt{|\eta_1|^2+|\eta_2|^2}}|H\rangle|V\rangle \\ &\quad + \frac{\eta_2}{\sqrt{|\eta_1|^2+|\eta_2|^2}}|V\rangle|H\rangle. \end{aligned} \tag{9}$$

Then we perform the half wave rotation operation, the state transforms to

$$\begin{aligned}|\text{env}\rangle \rightarrow\ & \frac{\eta_1+\eta_2}{2\sqrt{|\eta_1|^2+|\eta_2|^2}}(|+x+x\rangle - |-x-x\rangle) \\ & -\frac{\eta_1-\eta_2}{2\sqrt{|\eta_1|^2+|\eta_2|^2}}(|+x-x\rangle - |-x+x\rangle). \end{aligned} \tag{10}$$

So we can see that with probabilities $\left[\frac{\eta_1-\eta_2}{\sqrt{2|\eta_1|^2+|\eta_2|^2}}\right]^2$, our measurement will introduce errors. With probabilities $\left[\frac{\eta_1+\eta_2}{\sqrt{2|\eta_1|^2+|\eta_2|^2}}\right]^2$, the generalized DEPS QSS protocol works the same as the maximally entangled state. We can see the success probability from Fig.2.

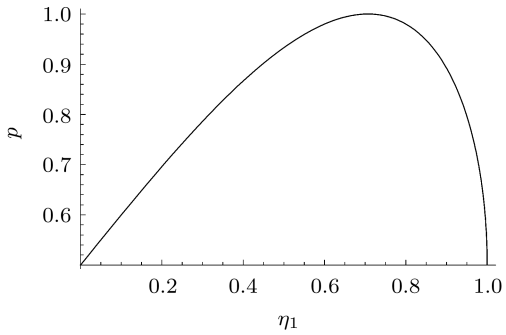


Fig.2. The success probability of QSS using generalized DEPS.

Then we can conclude that even using the non maximally entangled state, our DEPS QSS can still be realized with a certain probability related to the value of η_1 and η_2. In the DEPS QSS protocol, each sharing process transmits 3 bits of information for a maximally doubly entangled state. For a generalized QSS state, the efficiency depends on the degrees of entanglement.

In summary, we have proposed a quantum secret sharing protocol using doubly entangled photon states. The counter propagating entangled photons can be generated by using an efficiently pumped AlGaAs waveguide. We constructed the measurement devices. The QSS protocol is secure against intercept-resend attack and member cheating attack. Also the generalized conditions of quantum secret sharing using a non-maximally doubly entangled photon state are discussed.

References

[1] Hillery M, Bužek V and Berthiaume A 1999 *Phys. Rev.* A **59** 1829

[2] Koashi M and Imoto N 1997 *Phys. Rev. Lett.* **79** 2383

[3] Gottesman D 2000 *Phys. Rev.* A **61** 042311

[4] Tyc T and Sanders B C 2002 *Phys. Rev.* A **65** 042310

[5] Lance A M, Symul T, Bowen W P, Tyc T, Sanders B C and Lam P K 2003 *New. J. Phys.* **5** 4

[6] Xiao L, Long G L and Deng F G 2004 *Phys. Rev.* A **69** 052307

[7] Deng F G, Zhou H Y and Long G L 2005 *Phys. Lett.* A **337** 329
Deng F G, Li X H, Li C Y, Zhou P and Zhou H Y 2005 *Phys. Rev.* A **72** 044301
Deng F G, Zhou P, Li X H, Li C Y and Zhou H Y 2006 *Chin. Phys. Lett.* **23** 1084

[8] Li X H, Zhou P, Li C Y, Zhou H Y and Deng F G 2006 *J. Phys.* B **39** 1975

[9] Yan F L and Gao T 2005 *Phys. Rev.* A **72** 012304

[10] Wang J, Zhang Q and Tang C J 2007 *Commun. Theor. Phys.* **47** 454

[11] Man Z X, Xia Y J and An N B 2007 *Euro. Phys. J.* D **42** 333

[12] Zhang Z J, Li Y and Man Z X 2005 *Phys. Rev.* A **71** 044301

[13] Chen P, Deng F G and Long G L 2006 *Chin. Phys.* **15** 2228

[14] Yang Y G and Wen Q Y 2008 *Chin. Phys.* B **17** 419

[15] Sun Y, Du J Z, Qin S J, Wen Q Y and Zhu F C 2008 *Acta Phys. Sin.* **57** 4689 (in Chinese)

[16] Tittel W, Zbinden H and Gisin N 2001 *Phys. Rev.* A **63** 042301

[17] Schmid C, Trojek P, Bourennane P, Kurtsiefer C, Zukowski M and Weinfurter H 2005 *Phys. Rev. Lett.* **95** 230505

[18] Chen Y A, Zhang A N, Zhao Z, Zhou X Q, Lu C Y, Peng C Z, Yang T and Pan J W 2005 *Phys. Rev. Lett.* **95** 200502

[19] Kwiat P G, Mattle K, Weinfurter H, Zeilinger A, Sergienko A V and Shih Y H 1995 *Phys. Rev. Lett.* **75** 4337

[20] Ravaro M, Seurin Y, Ducci S, Leo G, Berger V, Rossi A and Assanto G 2005 *J. Appl. Phys.* **98** 063103

[21] Xiao L, Wang C, Zhang W, Peng J D, Huang Y D and Long G L 2008 *Phys. Rev.* A **77** 042315

[22] Li C Y, Zhou H Y, Wang Y and Deng F G 2005 *Chin. Phys. Lett.* **22** 1049

[23] Takesue H, Diamanti E, Honjo T, Langrock C, Fejer M M, Inoue K and Yamamoto Y 2005 *New. J. Phys.* **7** 232

[24] Thew R T, Tanzilli S, Krainer L, Zeller S C, Rochas A, Rech I, Cova S, Zbinden H and Gisin N 2006 *New. J. Phys.* **8** 32

[25] Bennett C H and Brassard G, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing,* Bangalore, India (IEEE, New York, 1984) 175

[26] Deng F G and Long G L 2004 *Phys. Rev.* A **70** 012311

[27] Niu C S and Griffiths R B 1999 *Phys. Rev.* A **60** 2764

[28] Singh S K and Srikanth R 2005 *Phys. Rev.* A **71** 012328