# Quantum Overloading Cryptography Using Single-Photon Nonlocality *

TAN Yong-Gang(谭勇刚)[1,2], CAI Qing-Yu(蔡庆宇)[1**], SHI Ting-Yun(史庭云)[1]

[1]*State Key Laboratory of Magnetic Resonances and Atomic and Molecular Physics, Wuhan Institute of Physics and Mathematics, Chinese Academy of Sciences, Wuhan 430071*

[2]*Graduate School of the Chinese Academy of Sciences, Beijing 100049*

(Received 12 March 2007)

*Using the single-photon nonlocality, we propose a quantum novel overloading cryptography scheme, in which a single photon carries two bits information in one-way quantum channel. Two commutative modes of the single photon, the polarization mode and the spatial mode, are used to encode secret information. Strict time windows are set to detect the impersonation attack. The spatial mode which denotes the existence of photons is noncommutative with the phase of the photon, so that our scheme is secure against photon-number-splitting attack. Our protocol may be secure against individual attack.*

*PACS: 03. 67. Dd, 03. 65. Ud*

Nonlocality is one of the basic characters of quantum physics. For many years, people only cared about the nonlocality of multi-photon states, which has been acknowledged by most physicists.[1,2] However, since the beginning of the 1990s, the nonlocality of single-photon state has been a very debated issue.[3] Experimental evidence for the nonlocal property of single-photon was first presented in Young's interference experiment performed by Grangier, Poger and Aspect, where only a single photon is incident on the two slits.[4] It is interesting that this nonlocal property can make single-photon a novel resource for quantum cryptography.[5,6] In fact, quantum cryptography, or more precisely called quantum key distribution, is a physically secure method, by which private key can be created between two partners, Alice and Bob, who share a quantum channel and a public authenticated channel. Security of the quantum key distribution (QKD) is based on the premise that one cannot distinguish two non-orthogonal states. Another equivalent description is that one cannot clone an unknown state. The pioneering work in QKD is presented by Bennett and Brassward in 1984 (BB84),[7] which is considered as the first scheme that can be utilized commercially in a quantum information field. Similar such one-way protocols include the two-state protocol[8] and six-state protocol.[9] Entanglement can be used as a very important resource in QKD, such as in the Einstein–Podolsky–Rosen (EPR) protocol[10] and dense coding protocol.[11,12] A single-photon two-step cryptography scheme was presented as a QKD scheme with orthogonal states in which every photon is sent to Bob in two steps.[5,6]

In this Letter, we present a novel single-photon overloading QKD scheme, in which two-bit information is encoded in a single-photon. Two commutative modes are used to encode the secret key. In this Letter, first we introduce our single-photon overloading QKD protocol. Second, we show that our scheme is secure against impersonation attack and photon-number-splitting (PNS) attack. Then we show that our scheme may be secure against individual attack. Finally, we discuss the experimental feasibility of our scheme and conclude.

The single-photon two-qubit state, one of whose degrees is entangled with its another different degree, is widely used in some ingenious quantum cryptography protocols. In the GV scheme[5] and KI scheme,[6] photon mode and vacuum mode are entangled, that is, the existence and inexistence of the photon in the channels are entangled,

$$|\Phi_0\rangle = \sqrt{T}|0\rangle_a|1\rangle_b - i\sqrt{R}|1\rangle_a|0\rangle_b,$$
$$|\Phi_1\rangle = \sqrt{R}|1\rangle_a|0\rangle_b - i\sqrt{T}|0\rangle_a|1\rangle_b, \quad (1)$$

where $|0\rangle$ denotes that there is no photon in the channel and $|1\rangle$ denotes there is a photon in the channel. In our scheme, we use the single-photon two-qubit state pointed out by Kim,[13] in which entanglement was produced between the polarization mode and spatial mode of a photon,

$$|\Psi^{(\pm)}\rangle = \frac{1}{\sqrt{2}}(|a,H\rangle \pm |b,V\rangle),$$
$$|\Phi^{(\pm)}\rangle = \frac{1}{\sqrt{2}}(|a,V\rangle \pm |b,H\rangle), \quad (2)$$

where $a$ and $b$ denote the channels, $H$ and $V$ denote the horizontal and vertical polarizations of the wave packets, respectively.

* Supported by the National Natural Science Foundation of China under Grant No 10504039, and the Foundation of One Hundred Talent Project of Chinese Academy of Sciences.

** To whom correspondence should be addressed. Email: qycai@wipm.ac.cn

©2007 Chinese Physical Society and IOP Publishing Ltd

The single-photon two-qubit state embodies its nonlocality from two aspects. First, from the traditional nonlocality view, the nonlocality denotes that a local operation in one channel can affect the result of the other. Secondly, the adjustment of the phase and polarization elements in the channels can reach the deterministic results fully of the four Bell-type states.[13] Peres and Terno thought that this type of entanglement may not be used in quantum cryptography because the two modes cannot be separated far away.[14] However we will show that they can indeed be used as a type of cryptographic resource in the following.

We call our scheme quantum overloading cryptography because it has distinct characters compared with other protocols. It is a deterministic one-way communication scheme with two-bit information encoded in single photon. First, it is deterministic because there is no need of bases reconciliation between Alice and Bob, which is different from the BB84 protocol and EPR protocol. Secondly, two-bit information is encoded in one photon and it is also a typical one-way communication which differentiates it from dense coding protocol. However, it is also different to quantum secure direct communication (QSDC) schemes.[15] Our overloading cryptography scheme can be described as follows (see Fig. 1):

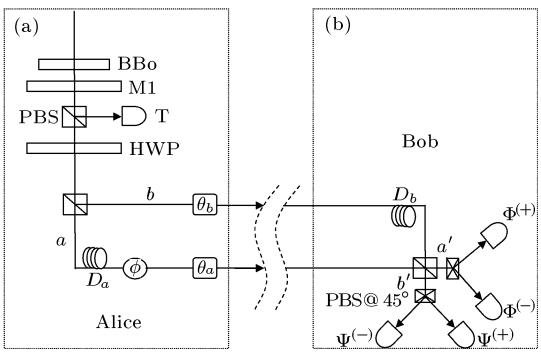



**Fig. 1.** Outline of the experiment. (a) Type-Ⅱ BBO crystal is used to generate the single state of Bell states. The PBS is used to let the horizontal polarization photon fly to Bob and the vertical polarization photon stay at home. The detector $T$ is used to check the existence of the home photon and take the sending time $t_s$. HWP rotates the horizontal polarization of the single photon to 45° polarization and the second PBS prepares a single-photon Bell state. Additional phase and polarization elements $\phi_a$, $\theta_a$ and $\theta_b$ are used to prepare the other three Bell states. The time delay loop $D_a$ is used to protect wave packets in channels $a$ and $b$ against Eve controlling two wave packets at the same time. (b) The time delay loop $D_b$ is used to compensate for the distance difference introduced by the time delay loops $D_a$. The PBS is used to mix the spatial modes $a$ and $b$, which is followed by a 45° oriented PBS located at each output port. The detector clicks at the outputs of 45° oriented PBS that uniquely identifies the four single-photon Bell states.

(A) The message sender, Alice, uses type-Ⅱ BBO crystal to generate photons with single-state Bell state $|\Pi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|H\rangle_A|V\rangle_B - |V\rangle_A|H\rangle_B)$, where $|H\rangle$ denotes horizontal polarization state and $|V\rangle$ denotes vertical polarization state, and $A$ and $B$ denote the two different photons. Then she lets the photons pass through a PBS so that the photon with vertical polarization will be left at home and the photon with horizontal polarization will be sent to Bob. Alice uses a detector to convince the existence of the home photon and takes the time as sending time $t_s$.

(B) Alice lets the photon which will be sent to Bob pass through a half-wave plate (HWP) in order to rotate the horizontal polarization of the photon to 45° polarization. Then she lets this photon pass through another PBS. Such PBS divides the photon into two wave packets. Because the 45° polarization state can be written as $\frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$, the wave packet with vertical polarization chooses channel $b$ and the wave packet with horizontal polarization chooses channel $a$. Then two internal degrees of the photon are entangled and the photon is in the state $|\Psi^+\rangle$.

(C) If Alice wants to send state $|\Psi^+\rangle$ to Bob, she performs nothing on the photon and sends it to Bob directly follow the previous step. Sometimes, if Alice wants to send Bob the state $|\Psi^-\rangle$, she adds a spatial phase delay $\phi$ of $\pi$ in channel $a$. If she wants to send Bob the state $|\Phi^+\rangle$, she inserts polarization HWPs $\theta_a$ and $\theta_b$ in both the channels $a$ and $b$. Both the polarization rotating $\theta_a$ and $\theta_b$ and a spatial phase delay $\phi$ of $\pi$ in channel a denote that Alice wants to send the state $|\Phi^-\rangle$ to Bob.

(D) When the photon reaches Bob, it first passes through a PBS, then $|\Psi^+\rangle$, $|\Psi^-\rangle$, $|\Phi^+\rangle$ and $|\Phi^-\rangle$ are turned into

$$\begin{aligned}
&|\Psi^+\rangle \Rightarrow |a'\rangle(|H\rangle + |V\rangle) \Longrightarrow |a'\rangle| + 45^\circ\rangle,\\
&|\Psi^-\rangle \Rightarrow |a'\rangle(|H\rangle - |V\rangle) \Longrightarrow |a'\rangle| - 45^\circ\rangle,\\
&|\Phi^+\rangle \Rightarrow |b'\rangle(|H\rangle + |V\rangle) \Longrightarrow |b'\rangle| + 45^\circ\rangle,\\
&|\Phi^-\rangle \Rightarrow |b'\rangle(|H\rangle - |V\rangle) \Longrightarrow |b'\rangle| - 45^\circ\rangle. \qquad (3)
\end{aligned}$$

At the end of channel $a'$ and channel $b'$, two 45° oriented polarizing beam splitters ($PBS@45^\circ$) are set to distinguish the incoming states.

(E) When the photon is detected by one of Bob's detectors, Bob will know clearly what Alice has sent and at the same time he takes the time as the receiving time $t_r$. Then Bob announces $t_r$ to verify the validity of this communication.

In order to ensure the security of the communication, some measures are taken. (a) First, two equal time delay loops are added in both channels $a$ and $b$. One is put in Alice's laboratory which is called $D_a$, and the other one called $D_b$ is put in Bob's laboratory. The role of delay $D_a$ is used to prevent Eve

from accessing the packet in channel $a$ after she having accessed the other one that in channel $b$. $D_b$ is used to compensate for the time delay caused by $D_a$. (b) After the key was distributed, Bob will announce partial of his measurement results to obtain the quantum bit error rate (QBER). If the QBER is abnormal higher than the tolerable threshold, they abandon this communication. Otherwise, they can perform error-correcting and privacy amplification to gain the secure final key.

In order to gain Alice's information, two types of impersonation schemes at least Eve can use to eavesdrop on the communication, as discussed in Refs. [5,6]. In the first attack scheme, she can obtain a copy of Bob's devices to read out Alice's information. Using this attack scheme, Eve can indeed obtain full of Alice's information. However, she must send the packet into Bob's delay loop $D_b$ before the packet running along channel a emerges from Alice's delay loop $D_a$, namely, before she learns the bit value sent by Alice. That is, she must inject a fake photon to Bob before she know what Alice has sent. In this case, Eve can gain full of Alice's information. However, mutual information between Alice and Bob is zero, that is, $I(A,B)=0$ with QBER$=0.75$. Consequently, Eve's such eavesdropping can be detected easily.

The second attack scheme is the one-channel impersonation attack, Eve only intercepts channel $b$ to read Alice's information, and channel $a$ is blocked. In this attack scheme, the density matrix of the photon she obtained can be depicted as

$$\rho=\frac{1}{2}(|V\rangle\langle V|+|H\rangle\langle H|). \tag{4}$$

After learning the polarization of the photon, she injects a photon with the same polarization as the detected one and randomly encodes the photon between the two possible states. In this case, Eve can gain Alice's partial information. However, this would cause a very high QBER ($\geq 50\%$).

Our scheme is also robustly secure against PNS attack. In the famous BB84 protocol, information is encoded in the polarization of the photon. Since the photon number and the polarization of the photon are commutative, one can use photon-number-splitting (PNS) attack to eavesdrop some of Alice's information without being detected.[16] However, in our scheme, the spatial mode which denotes the photon number is noncommutative with the phase. Any attempt to obtain the photon number must disturb the phase of the photon. Therefore, our scheme is robustly secure against PNS attack.

In order to show that our protocol is secure against individual attack, we first assume that the quantum channels outside Alice's and Bob's laboratories is completely controlled by Eve. Generally, Eve may use some probes to intervene in the channels. Assuming the interactions between the probes and the wave packets are unitary, one can obtain the combined states of the wave packets and the probes. Assuming Alice sends $|\Psi^+\rangle=|aH\rangle+|bV\rangle$ to Bob, the polarization modes of the wave packets and the probes in the channels $a$ and $b$ are

$$\begin{aligned} U|a,H\rangle|0\rangle&=|a,H\rangle|f_1\rangle+|a,V\rangle|e_1\rangle,\\ U|b,V\rangle|0\rangle&=|b,V\rangle|f_2\rangle+|b,H\rangle|e_2\rangle, \end{aligned} \tag{5}$$

where $|0\rangle$ is the initial state of Eve's probes before they interact with the wave packets sent from Alice, $U$ is the unitary interaction between the probes and the wave packets and $|f_i\rangle$ and $|e_i\rangle$ $(i=1,2)$ are the final states after the unitary interaction. Taking the inner product of each of the above equations, one can obtain

$$\begin{aligned} \langle f_1|f_1\rangle+\langle e_1|e_1\rangle&=1,\\ \langle f_2|f_2\rangle+\langle e_2|e_2\rangle&=1. \end{aligned} \tag{6}$$

For simplicity of consideration, one can let $f_1=f_2$ and $e_1=e_2$. Then with fidelity of $\langle f|f\rangle=1$ the state $\rho=|\Psi^+\rangle\langle\Psi^+|$ stays on its original state. Detailed calculations show that the more disturbance Eve causes on Alice and Bob's state the less probability Alice and Bob can obtain their original state (this may be published elsewhere for the page limitation). Then by comparing the fidelity of the state, Alice and Bob can detect the existence of Eve.

In the famous dense coding scheme,[11] an EPR pair is used to encode the secret key, and entanglement has been established with the same freedom of two photons. However, our scheme is based on the nonlocality of a single photon. Although the spatial mode and the polarization of the photon are commutative, we have proven that our scheme is secure against impersonation attack, PNS attack, and individual attack. In the first place, the photon is divided into two wave packets and each runs through Eve's realm at different time windows. Although the information is encoded with orthogonal states, it is totally mixed states to an eavesdropper. Therefore, this scheme is secure against the impersonation attack. In the second place, PNS attack will be detected easily since the spatial mode which denotes the existence of the wave packets is not commutative with the phase of them, then PNS attacks may cause the abnormal QBER to Bob's results. Our scheme does not need random sending time $t_r$ as that of GV protocol because Eve can not restore the polarization of the wave packet in the first time window after she has gained the total information in the second time window. Furthermore, our scheme is deterministic so that it can be used not only to distribute the secret key but also to send message directly.

Another important fact is that our scheme is experimentally feasible. In our scheme, we introduce an EPR pair to register the sending time $t_s$. Or else, a perfect single-photon source must be required as in GV and KI. Furthermore, we have verified the secure QBER threshold against the individual attack.

Note: After our work was finished, we found a scheme[17] in which one photon can only transfer one key qubit; the equipment is very complex as compared with the present one.

## References


[1] Bell J S 1964 *Physics* (Long Island City, N.Y.) **1** 195

[2] Wang Q, Huang Y F, Sun F W, Zhang Y Sh, Guo G C 2005 *Chin. Phys. Lett.* **22** 335

[3] Tan S M, Walls D F and Collet M J 1991 *Phys. Rev. Lett.* **66** 252
Hardy L 1994 *Phys. Rev. Lett.* **73** 2279
Peres A 1995 *Phys. Rev. Lett.* **74** 4571
Greenberger D M, Horne M A and Zeilinger A 1995 *Phys. Rev. Lett.* **75** 2064
Hardy L 1995 *Phys. Rev. Lett* **75** 2065
van Enk S J 2005 *Phys. Rev.* A **72** 064306

[4] Grangier P, Roger G and Aspect A 1986 *Europhys. Lett.* **1** 173

[5] Goldenberg L and Vaidman L 1995 *Phys. Rev. Lett.* **75** 1239

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

[7] Bennet C H and Brassard G *Proceeding of IEEE international Conference on Computers, Systems and Signal Processing* (Bangalore, India) (IEEE, New York, 1984) p 175

[8] Bennet C H 1992 *Phys. Rev. Lett.* **68** 3121

[9] Bruss D 1998 *Phys. Rev. Lett.* **81** 3018
Bechmann-Pasquinucci H and Gisin N 1999 *Phys. Rev.* A **59** 4238

[10] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661

[11] Bennet C H and Wiesner S J 1992 *Phys. Rev. Lett.* **69** 2881
Cai Q Y and Li B W 2004 *Phys. Rev.* A **69** 054301

[12] Wang M Y, Yang L G and Yan F L 2005 *Chin. Phys. Lett.* **22** 1053

[13] Kim Y H 2003 *Phys. Rev.* A **67** 040301

[14] Peres A and Terno D R 2004 *Rev. Mod. Phys.* **76** 93

[15] Boström K and Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902
Cai Q Y 2003 *Phys. Rev. Lett.* **91** 109801-1
Cai Q Y and Li B W 2004 *Chin. Phys. Lett.* **21** 601
Deng F G 2006 *Phys. Rev.* A **74** 054302
Deng F G, Long G L and Zhou H Y 2005 *Phys. Lett.* A **340** 43
Man Z X and Xia Y J 2007 *Chin. Phys. Lett.* **24** 15

[16] Lükenhaus N 2000 *Phys. Rev.* A **61** 052304

[17] Beige A, Englert B G, Kurtsiefer C and Weinfurter H 2002 *J. Phys.* A **35** L407