Int J Theor Phys (2016) 55:3579–3587
DOI 10.1007/s10773-016-2986-y

# Deterministic Secure Quantum Communication and Authentication Protocol based on Extended GHZ-W State and Quantum One-time Pad

**Na Li**[1,2] · **Jian Li**[1,3] · **Lei-Lei Li**[1] · **Zheng Wang**[1] · **Tao Wang**[1]

Received: 29 October 2015 / Accepted: 15 March 2016 / Published online: 1 April 2016

**Abstract** A deterministic secure quantum communication and authentication protocol based on extended GHZ-W state and quantum one-time pad is proposed. In the protocol, state $\left|\varphi^-\right\rangle$ is used as the carrier. One photon of $\left|\varphi^-\right\rangle$ state is sent to Alice, and Alice obtains a random key by measuring photons with bases determined by ID. The information of bases is secret to others except Alice and Bob. Extended GHZ-W states are used as decoy photons, the positions of which in information sequence are encoded with identity string ID of the legal user, and the eavesdropping detection rate reaches 81%. The eavesdropping detection based on extended GHZ-W state combines with authentication and the secret ID ensures the security of the protocol.

**Keywords** Deterministic secure quantum communication · Extended GHZ-W state · One-time pad · Authentication

## 1 Introduction

Quantum communication technology is mainly divided into two parts, the Quantum Key Distribution (QKD) [1–5] and quantum direct communication, which is the main research content of the quantum information with the best application prospect.

✉ Na Li
lina68001@126.com

Jian Li
buptlijian@126.com

[1] School of Computer Science, Beijing University of Posts and Telecommunications, Beijing 100876, China

[2] JiLin Medical University, Jilin, 132013, China

[3] Hefei National Laboratory for Physical Sciences at the Microscale, University of Science and Technology of China, Hefei 230026, China

With the rapid development and maturity of quantum technology, QKD plays an important role in the development of quantum cryptography. It is an important research part of quantum cryptography. QKD makes the communication between the two sides share a series of security random key through the quantum method. In theory, QKD and one-time pad (OTP) [6] are combined to achieve the unconditional security of cryptosystem.

Making use of quantum physical properties to keep the information secret, is the first proposed by S. Wiesner of the University of Columbia in 1969, but this idea was not accepted by people at that time. Ten years later, Bennett of IBM company and Brassard [7] of Montreal University reconsidered this issue, proposed the concept of quantum cryptography and given the first quantum key distribution protocol-BB84 protocol on the basis of S. Wiesner'thoughts. After this, there are more protocols: E91, B92, GV95, continuous variable, Decoy state, etc. Quantum direct communication includes Determination Secure Quantum Communication (DSQC) [8–11] and Quantum Secure Direct Communication (QSDC) [12–15].QSDC is a new way of communication which is different from QKD. In QSDC, the secret messages are transmitted in the quantum channel directly without being leaked. In DSQC, the communication between the two sides needs the classic information as an auxiliary in the communication process.

Identity authentication to prevent the middle attack is a difficult task in quantum communication. The use of a message authentication code can ensure that the source of the classic information is reliable and not to be tampered with. Combined with One-Time Pad (OTP), it is a secure message authentication scheme. Block transmission of quantum data are used to improve the security of information transmission [16].

In this paper, deterministic secure quantum communication and authentication protocol based on extended GHZ-W state and quantum one-time pad is proposed. Extended GHZ-W states are used as decoy photons [17–20], and the eavesdropping detection rate reaches 81%. Both parties, that is, Alice and Bob share ID in advance. Then the positions of decoy photons in the information sequence are encoded with the identity string of Alice and Bob which are known by themselves only. Bob sends the information sequence mixed with decoy photons to Alice, Alice extracts decoy photons and makes measurements. In this process, Alice not only determines whether eavesdroppers exist, but also verifies the legality of Bob. State $\left|\varphi^-\right\rangle$ is used as the carrier. One photon of $\left|\varphi^-\right\rangle$ state is sent to Alice, and Alice obtains a random key by measuring photons with bases determined by ID. The information of bases is secret to others except Alice and Bob. The eavesdropping detection based on extended GHZ-W state and the secret positions and bases determined by the secret ID ensures the security of the protocol.

## 2 Description of Protocol

Now let's start an explicit description of the extended GHZ-W state protocol which is called GWPP. Suppose that the sender Alice wants to transmit his secret message to the legitimate receiver Bob. There is a series of N-bit sting ID shared by Alice and Bob representing their identities beforehand. Of course, Alice's secret message is composed of a series of classical 0 or 1 numbers which is called M.

(S1) Bob prepares N ordered Bell states $\left|\varphi^-\right\rangle$ and N/4 extended GHZ-W state $\left|\psi\right\rangle_{1234}$.

$$\left|\varphi^-\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{12} = \frac{1}{\sqrt{2}}(|+-\rangle + \langle -+|)_{12}$$

$$|\psi\rangle_{1234} = \frac{1}{\sqrt{3}}(|0000\rangle + |1100\rangle + |1111\rangle)_{1234}$$

The ordered N $\left|\varphi^{-}\right\rangle$ states are marked as {[$P_1$(1), $P_1$(2)], [$P_2$(1), $P_2$(2)], ..., [$P_N$(1), $P_N$(2)]}, where the subscript represents the order of each state in the sequence and the number 1, 2 in brackets indicate the two particles of each state. Bob extracts the first particle from each Bell state, and these articles form an ordered sequence {$P_1$(1), $P_2$(1), ..., $P_N$(1)}, called $S_A$ sequence (the travel qubits). Then the remaining particles compose $S_B$ sequence {$P_1$(2), $P_2$(2), ..., $P_N$(2)}(the home qubits). The N/4 ordered extended GHZ-W state $|\rangle_{1234}$ are denoted as {$GW_1$(1), $GW_1$(2), $GW_1$(3), $GW_1$(4), $GW_2$(1), $GW_2$(2), $GW_2$(3), $GW_2$(4), ..., $GW_N$(1), $GW_N$(2), $GW_N$(3), $GW_N$(4)}, marked as $S_T$ sequence, which will be used as decoy sequence.

(S2) Bob inserts the decoy sequence $S_T$ into the sequence $S_A$ according to ID, forming a new sequence $S_{A'}$. For example, Bob inserts the $i$th photon of $S_T$ behind the $i$th photon of $S_A$ if the $i$th bit of ID is 0; Bob inserts the $i$th photon of $S_T$ before the $i$th photon of $S_A$ if the $i$th bit of ID is 1. Only Alice and Bob know the positions of these decoy photons. Then Bob sends $S_{A'}$ to Alice.

(S3) Alice filters out the invisible photons with a different wave-length by using special filter. Then Alice uses the photon number splitter (PNS) or beam splitters to check the received photons. This has been described in [21].

(S4) Alice extracts the decoy photons from $S_{A'}$ which sending from Bob according to ID and performs extended GHZ-W state measurement on the extracted sequence $S_T$. Ideally, every measurement result should be in the extended GHZ-W state. Of course, there are some errors in the actual situation. Alice believes Bob is legal and there is no eavesdropping if the error rate is low enough. At this time, the communication continues. Otherwise, the communication is interrupted. On the assumption that N is the number of photons in $S_A$, K is the number of $|\rangle_{1234}$states in $S_T$. Obviously, K is no less than N/4 if all photons are dispersed in $S_A$.

(S5) Alice measures the remaining photons of $S_{A'}$, that is, $S_A$ with basis $B_z = \{|0\rangle, |1\rangle\}$or $B_x = \{|+\rangle, |-\rangle\}$in order according to ID. Alice measures the corresponding photon of $S_A$ with $B_z$ basis if the bit of ID is 0; Otherwise, Alice uses $B_x$ basis. Alice obtains a series of classical number $C_A$ in order after measuring photons in $S_A$ with $B_z$ basis or $B_x$ basis. For example, Alice marks the bit of $C_A$ as 0 if the measurement result is $|0\rangle$ or $|+\rangle$; Otherwise Alice marks the bit of $C_A$ as 1. Then Alice publishes which photons she does not receive.

(S6) Bob discards the corresponding photons in $S_B$ after he knows which photons of $S_A$ are not received by Alice. For example, Bob discards the corresponding photon $P_x$(2) in $S_B$ if photon $P_x$(1) in $S_A$ is not received by Alice. Therefore, photons in $S_B$ will be always one-to-one matching with photons in $S_{A.}$

(S7) Suppose that the length of $C_A$ is L. Alice uses L as the unit length to divide the secret message M into several parts. Each part is marked as $M_i$ ($i$ = 1,2, ...), which includes L bits classical secret information. Alice encrypts the secret message $M_1$ with $C_A$ bit by bit using XOR operation and gets $C_1$ .That is, $C_1 = M_1$ XOR $C_A$. Alice publishes $C_1$.

(S8) Bob also measures the remaining photons in $S_B$ in the same way as Alice. Bob can also form a series of classical number $C_B$ in order. However, the rule is different from that of $C_A$. Bob marks the bit of $C_B$ as 0 if the measurement result is $|0\rangle$ or $|-\rangle$; Otherwise Bob marks the bit of $C_B$ as 1. Bob decrypts $C_1$ with $C_B$ bit by bit using XOR operation and gets $M_1$. That is, $M_1 = C_1$ XOR $C_B$.

(S9) Bob stores the secret message $M_{1.}$

(S10) Alice and Bob continue the next transmission until all the secret messages are finished.

## 3 An Example of the Protocol

Suppose that the secret message M = 1011010100110101 and ID = 01001010.

(S1) Bob prepares n (n≥8) $\left|\varphi^-\right\rangle$ states and n/4 extended GHZ-W state $\left|\psi\right\rangle_{1234}$. The ordered n $\left|\varphi^-\right\rangle$ states are marked as {[$P_1$(1), $P_1$(2)], [$P_2$(1), $P_2$(2)], …, [$P_n$(1), $P_n$(2)]}. Bob divides the $\left|\varphi^-\right\rangle$ state sequence into two groups: $S_A$ {$P_1$(1), $P_2$(1), …, $P_n$(1) }and $S_B$ {$P_1$(2), $P_2$(2), …, $P_n$(2)}. The extended GHZ-W state sequence is marked as $S_{T.}$

(S2) Bob inserts $S_T$ into $S_A$ according to ID, which forms $S_{A'.}$ Bob sends $S_{A'}$ to Alice.

(S3) Alice filters out the invisible photons and checks the received photons by using (PNS) or beam splitters.

(S4) Alice extracts $S_T$ from $S_{A'}$ according to ID and performs extended GHZ-W state measurement on $S_T$. Alice considers Bob as legitimate user and there is no eavesdropping if the error rate is low enough.

(S5) Alice measures the remaining photons of $S_{A'}$, that is, $S_A$ with basis $B_z = \{|0\rangle, |1\rangle\}$or $B_x = \{|+\rangle, |-\rangle\}$in order according to ID. The rule is that Alice measures the corresponding photon of $S_A$ with $B_z$ basis if the bit of ID is 0; Otherwise, Alice uses $B_x$ basis. By using this rule the bases Alice chooses should be $B_z$ $B_x$ $B_z$ $B_z$ $B_x$ $B_z$ $B_x$ $B_{z.}$ Suppose that the measurement result is $|1\rangle$ $|-\rangle$ $|0\rangle$ $|1\rangle$ $|+\rangle$ $|1\rangle$ $|+\rangle$ $|0\rangle$, the corresponding photons in $S_B$ will collapse to $|1\rangle$ $|+\rangle$ $|0\rangle$ $|1\rangle$ $|-\rangle$ $|1\rangle$ $|-\rangle$ $|0\rangle$. Alice marks the bit of $C_A$ as 0 if the measurement result is $|0\rangle$ or $|+\rangle$; Otherwise Alice marks the bit of $C_A$ as 1 according to the rule. So $C_A$ should be 11010100. Alice publishes which photons she does not receive.

(S6) Bob discards the corresponding photons in $S_B$ for the photons in $S_A$ not received by Alice. So, photons in $S_B$ will be always one-to-one matching with photons in $S_{A.}$

(S7) Suppose that the length of $C_A$ is eight. Alice divides the secret message M into two parts ($M_1$ = 10110101 and $M_2$ = 00110101). Alice encrypts $M_1$ with $C_A$ bit by bit using XOR operation and gets $C_1$ ($C_1$ = $M_1$ XOR $C_A$ = 01100001). Alice publishes $C_1$.

(S8) Bob also measures the remaining photons in $S_B$ in the same way as Alice. The measurement result should be $|1\rangle$ $|+\rangle$ $|0\rangle$ $|1\rangle$ $|-\rangle$ $|1\rangle$ $|-\rangle$ $|0\rangle$.Bob marks the bit of $C_B$ as 0 if the measurement result is $|0\rangle$ or $|-\rangle$; Otherwise Bob marks the bit of $C_B$ as 1, so $C_B$ should be 11010100. Bob decrypts $C_1$ with $C_B$ bit by bit using XOR operation and gets $M_1$ ($M_1$ = $C_1$ XOR $C_B$ = 10110101).

(S9) Bob stores the secret message $M_{1.}$

(S10) Alice and Bob continue the next transmission until all the secret messages are finished.

## 4 Security Analysis

The security of the protocol is guaranteed by the identity string ID and the eavesdropping detection strategy based on extended GHZ-W state. The protocol will not be threatened by man-in-the-middle attack, because identity authentication is implemented based on the identity string. Now, let us analyze the eavesdropping detection rate of the protocol.

In the original “ping-pong” protocol [22–25], the author calculated the maximal amount of the information $I(d_{lO})$ that Eve can eavesdrop and the probability $d_{lO}$ that Eve is detected. And the function $I(d_{lO}))$ is provided. When $p_0 = p_1 = 0.5$, $I(d_{lO}) = -d_{lO} log_2 d_{lO} - (1 - d_{lO}) log_2 (1 - d_{lO})$. The above method can be used to compare the eavesdropping detection rate between the two protocols.

In the protocol, the extended GHZ-W state is used as decoy photons to detect eavesdropping. Eve cannot distinguish decoy photons from information photons, because the positions of decoy photons are secret. So what he can do is only performing the same attack operation on all photons.

The attack operation on the composed system that Eve performs is marked as$\hat{\mathrm{E}}$. After performing the attack operation$\hat{\mathrm{E}}$, the state $|0\rangle$ become $\left|\varphi_0^{'}\right\rangle = \hat{\mathrm{E}} \otimes |0x\rangle = a\,|0x_0\rangle + \beta\,|1x_1\rangle$ and the state $|1\rangle$ become $\left|\varphi_1^{'}\right\rangle = \hat{\mathrm{E}} \otimes |1x\rangle = m\,|0y_0\rangle + n\,|1y_1\rangle$ , Where $|x_i\rangle$ and $|yi\rangle$ are the pure ancillary states determined by $\hat{\mathrm{E}}$ uniquely, and $|\alpha|^2 + |\beta|^2 = 1, |m|^2 + |n|^2 = 1.$

Attacked by Eve, the state of composed system changes to

$$|\psi\rangle_{Eve} = E \otimes E \otimes E \otimes E[\frac{1}{\sqrt{3}}(|0x0x0x0x\rangle + |1x1x0x0x\rangle + |1x1x1x1x\rangle)]$$

$$\begin{aligned}
&= \tfrac{1}{\sqrt{3}}[(\alpha\,|0x_0\rangle + \beta\,|1x_1\rangle) \otimes (\alpha\,|0x_0\rangle + \beta\,|1x_1\rangle) \otimes \alpha(|0x_0\rangle + \beta\,|1x_1\rangle) \otimes (\alpha\,|0x_0\rangle + \beta\,|1x_1\rangle)\\
&+(m\,|0y_0\rangle + n\,|1y_1\rangle) \otimes (m\,|0y_0\rangle + n\,|1y_1\rangle) \otimes (\alpha\,|0x_0\rangle + \beta\,|1x_1\rangle) \otimes (\alpha\,|0x_0\rangle + \beta\,|1x_1\rangle)\\
&+(m\,|0y_0\rangle + n\,|1y_1\rangle) \otimes (m\,|0y_0\rangle + n\,|1y_1\rangle) \otimes (m\,|0y_0\rangle + n\,|1y_1\rangle) \otimes (m\,|0y_0\rangle + n\,|1y_1\rangle)]\\
&= \tfrac{1}{\sqrt{3}}(\alpha^4\,|0x_0 0x_0 0x_0 0x_0\rangle + \alpha^3\beta\,|0x_0 0x_0 0x_0 1x_1\rangle + \alpha^3\beta\,|0x_0 0x_0 1x_1 0x_0\rangle + \alpha^2\beta^2\,|0x_0 0x_0 1x_1 1x_1\rangle\\
&+\alpha^3\beta\,|0x_0 1x_1 0x_0 0x_0\rangle + \alpha^2\beta^2\,|0x_0 1x_1 0x_0 1x_1\rangle + \alpha^2\beta^2\,|0x_0 1x_1 1x_1 0x_0\rangle + \alpha\beta^3\,|0x_0 1x_1 1x_1 1x_1\rangle\\
&+\alpha^3\beta\,|1x_1 0x_0 0x_0 0x_0\rangle + \alpha^2\beta^2\,|1x_1 0x_0 0x_0 1x_1\rangle + \alpha^2\beta^2\,|1x_1 0x_0 1x_1 0x_0\rangle + \alpha\beta^3\,|1x_1 0x_0 1x_1 1x_1\rangle\\
&+\alpha^2\beta^2\,|1x_1 1x_{01} 0x_0 0x_0\rangle + \alpha\beta^3\,|1x_1 1x_1 0x_0 1x_1\rangle + \alpha\beta^3\,|1x_1 1x_1 1x_1 0x_0\rangle + \beta^4\,|1x_1 1x_1 1x_1 1x_1\rangle\\
&+m^2\alpha^2\,|0y_0 0y_0 0x_0 0x_0\rangle + m^2\alpha\beta\,|0y_0 0y_0 0x_0 1x_1\rangle + m^2\alpha\beta\,|0y_0 0y_0 1x_1 0x_0\rangle + m^2\beta^2\,|0y_0 0y_0 1x_1 1x_1\rangle\\
&+mn\alpha^2\,|0y_0 1y_1 0x_0 0x_0\rangle + mn\alpha\beta\,|0y_0 1y_1 0x_0 1x_1\rangle + mn\alpha\beta\,|0y_0 1y_1 1x_1 0x_0\rangle + mn\beta^2\,|0y_0 1y_1 1x_1 1x_1\rangle\\
&+mn\alpha^2\,|1y_1 0y_0 0x_0 0x_0\rangle + mn\alpha\beta\,|1y_1 0y_0 0x_0 1x_1\rangle + mn\alpha\beta\,|1y_1 0y_0 1x_1 0x_0\rangle + mn\beta^2\,|1y_1 0y_0 1x_1 1x_1\rangle\\
&+n^2\alpha^2\,|1y_1 1y_1 0x_0 0x_0\rangle + n^2\alpha\beta\,|1y_1 1y_1 0x_0 1x_1\rangle + n^2\alpha\beta\,|1y_1 1y_1 1x_1 0x_0\rangle + n^2\beta^2\,|1y_1 1y_1 1x_1 1x_1\rangle\\
&+m^4\,|0y_0 0y_0 0y_0 0y_0\rangle + m^3 n\,|0y_0 0y_0 0y_0 1y_1\rangle + m^3 n\,|0y_0 0y_0 1y_1 0y_0\rangle + m^2 n^2\,|0y_0 0y_0 1y_1 1y_1\rangle\\
&+m^3 n\,|0y_0 1y_1 0y_0 0y_0\rangle + m^2 n^2\,|0y_0 1y_1 0y_0 1y_1\rangle + m^2 n^2\,|0y_0 1y_1 1y_1 0y_0\rangle + mn^3\,|0y_0 1y_1 1y_1 1y_1\rangle\\
&+m^3 n\,|1y_1 0y_0 0y_0 0y_0\rangle + m^2 n^2\,|1y_1 0y_0 0y_0 1y_1\rangle + m^2 n^2\,|1y_1 0y_0 1y_1 0y_0\rangle + mn^3\,|1y_1 0y_0 1y_1 1y_1\rangle\\
&+m^2 n^2\,|1y_1 1y_1 0y_0 0y_0\rangle + mn^3\,|1y_1 1y_1 0y_0 1y_1\rangle + mn^3\,|1y_1 1y_1 1y_1 0y_0\rangle + n^4\,|1y_1 1y_1 1y_1 1y_1\rangle)
\end{aligned}$$

Alice extracts $\mathrm{S_T}$ and performs extended GHZ-W state measurement on $\mathrm{S_T}$ after she receives $\mathrm{S_{A'}}$ (mixture of $\mathrm{S_A}$ and $\mathrm{S_T}$). If the probability $p(|\psi\rangle)$ that Alice gets correct measurement results is considered as the probability without eavesdroppers, $p(|\psi\rangle)$ can be calculated as

$$p(|\psi\rangle) = \frac{1}{3}(|\alpha^4|^2 + |\alpha^2\beta^2|^2 + |\beta^4|^2 + |m^2\alpha^2|^2 + |n^2\alpha^2|^2 + |n^2\beta^2|^2 + |m^4|^2 + |m^2n^2|^2 + |n^4|^2)$$

Suppose$|\alpha|^2 = a, |\beta|^2 = b, |m|^2 = s, |n|^2 = t$, where $a$, $b$, $s$ and $t$ are positive real numbers, and $a + \quad b = \quad s + \quad t = 1$. Then

$$p(|\psi\rangle) = \frac{1}{3}(3a^4 - 6a^3 + 8a^2 - 4a + 3a^2t^2 - 2a^2t - 2at^2 + 3t^4 - 6t^3 + 8t^2 - 4t + 2)$$

So the lower bound of the detection rate is

$$d_{low} = 1 - p(|\psi\rangle) = 1 - \frac{1}{3}(3a^4 - 6a^3 + 8a^2 - 4a + 3a^2t^2 - 2a^2t - 2at^2 + 3t^4 - 6t^3 + 8t^2 - 4t + 2)$$

Now, let us analyze how much information Eve can gain maximally. First, Alice takes measurement on the photon in her hand and supposing that the quantum state of the photon is$|\rangle$. Then the state of the system composed of Bob' photon is

$\left|\psi'\right\rangle = \hat{\mathrm{E}}\,|O, E\rangle = \hat{\mathrm{E}}\,|O\rangle\,|E\rangle = \alpha\,|O\rangle\,|\varepsilon_{00}\rangle + \beta\,|1\rangle\,|\varepsilon_{01}\rangle = \alpha\,|0, \varepsilon_{00}\rangle + \beta\,|1, \varepsilon_{01}\rangle$ . The probability that Eve can be detected is $\rho' = |\alpha|^2\,|0, \varepsilon_{00}\rangle\,\langle 0, \varepsilon_{00}| + |\beta|^2\,|1, \varepsilon_{00}\rangle\,\langle 1, \varepsilon_{00}| + |\beta|^2\,|1, \varepsilon_{01}\rangle\,\rangle 1, \varepsilon_{01}| + \alpha\beta^*\,|0, \varepsilon_{00}\rangle\,\langle 1, \varepsilon_{01}| + \alpha^*\beta\,|1, \varepsilon_{01}\rangle\,\langle 0, \varepsilon_{00}|$.

After encoding of the unitary operations $U_0$, $U_{1,}$ $U_2$ and $U_3$ with the probabilities $p_0$, $p_1$, $p_2$ and $p_{3,}$ respectively, the state reads

$$\begin{aligned}\rho\text{”} = {} & (p_0 + p_3)\,|\alpha|^2\,|0, \varepsilon_{00}\rangle\,\rangle 0, \varepsilon_{00}| + (p_0 + p_3)\,|\beta|^2\,|1, \varepsilon_0\rangle\,\rangle 1, \varepsilon_{01}| \\ & + (p_0 + p_3)\,\alpha\beta^*\,|0, \varepsilon_{00}\rangle\,\langle 1, \varepsilon_{01}| + (p_0 + p_3)\,\alpha^*\beta\,|1, \varepsilon_{01}\rangle\,\langle 0, \varepsilon_{00}| \\ & + (p_1 + p_2)\,|\alpha|^2\,|1, \varepsilon_{01}\rangle\,\rangle 1, \varepsilon_{01}| + (p_1 + p_2)\,|\beta|^2\,|0, \varepsilon_{00}\rangle\,\rangle 0, \varepsilon_{00}| \\ & + (p_1 + p_2)\,\alpha\beta^*\,|1, \varepsilon_{01}\rangle\,\langle 0, \varepsilon_{00}| + (p_1 + p_2)\,\alpha^*\beta\,|0, \varepsilon_{00}\rangle\,\langle 1, \varepsilon_{01}|\end{aligned}$$

which can be rewritten in the orthogonal basis $\{|0, \varepsilon_{00}\rangle\,, |1, \varepsilon_{01}\rangle\,, |1, \varepsilon_{00}\rangle\,, |0, \varepsilon_{01}\rangle\}$,,

$$\rho\text{”} \quad = \quad \begin{pmatrix} (p_0 + p_3)\;|\alpha|^2 & (p_0 - p_3)\;\alpha\beta^* & 0 & 0 \\ (p_0 - p_3)\;\alpha^*\beta & (p_0 + p_3)\;|\beta|^2 & 0 & 0 \\ 0 & 0 & (p_1 + p_2)\;|\alpha|^2 & (p_1 - p_2)\;\alpha\beta^* \\ 0 & 0 & (p_1 - p_2)\;\alpha^*\beta & (p_1 + p_2)\;|\beta|^2 \end{pmatrix}$$

with$p_0 + p_1 + p_2 + p_3 = 1$.

The information $I_0$ that Eve can get is equal to the Von Neumann entropy$I_0 = \sum_{i=0}^{3} -\lambda i \log 2\lambda i$, where $\lambda i\,(i = 0{,}1{,}2{,}3)$ are the eigenvalues of$\rho$”, which are

$$\lambda 0, 1 = \frac{1}{2}\,(p_0 + p_3) \pm \frac{1}{2}\sqrt{(p_0 + p_3)^2 - 16 p_0 p_3 |\alpha|^2 |\beta|^2} = \frac{1}{2}\,(p_0 + p_3) \pm \frac{1}{2}\sqrt{(p_0 + p_3)^2 - 16 p_0 p_3 (d - d^2)} \tag{1}$$

$$\lambda 2, 3 = \frac{1}{2}\,(p_1 + p_2) \pm \frac{1}{2}\sqrt{(p_1 + p_2)^2 - 16 p_1 p_2 |\alpha|^2 |\beta|^2} = \frac{1}{2}\,(p_1 + p_2) \pm \frac{1}{2}\sqrt{(p_1 + p_2)^2 - 16 p_1 p_2 (d - d^2)} \tag{2}$$

In the case of $p_0 = \quad p_1 = p_2 = \quad p_3 = 0.25$, where Alice encodes exactly 2 bits, expressions (1)-(2) simplify to $\lambda_0 = 0.5d$, $\lambda_1 = 0.5(1 - d)$, $\lambda_2 = 0.5d$, $\lambda_3 = 0.5(1 - d)$. Interestingly, the maximal information that Eve can get is equal to the Shannon entropy of a binary channel

$$I_0 = -\frac{1}{2}d\log_2(\frac{1}{2}d) - (\frac{1}{2} - \frac{1}{2}d)\log_2(\frac{1}{2} - \frac{1}{2}d) - \frac{1}{2}d\log_2(\frac{1}{2}d) - (\frac{1}{2} - \frac{1}{2}d)\log_2(\frac{1}{2} - \frac{1}{2}d).$$

Then assume that Bob sends $|\rangle$ rather than $|\rangle$. The above security analysis can be done in full analogy, resulting in the same crucial relations. The maximum amount of information is equal to the Shannon entropy of a binary channel

$$I_1 = -\frac{1}{2}d\log_2(\frac{1}{2}d) - (\frac{1}{2} - \frac{1}{2}d)\log_2(\frac{1}{2} - \frac{1}{2}d) - \frac{1}{2}d\log_2(\frac{1}{2}d) - (\frac{1}{2} - \frac{1}{2}d)\log_2(\frac{1}{2} - \frac{1}{2}d).$$

So the maximal amount of information that Eve can obtain is

$$I = 0.5(I_0 + I_1) = 1 - d\log_2 d - (1 - d)\log_2(1 - d)$$

After some simple mathematical calculations, when a=t, get

$$d_{low} = \frac{1}{3} - 3a^4 + \frac{16}{3}a^3 - \frac{16}{3}a^2 + \frac{8}{3}a,$$

and the maximum $I$ is

$I(d_{low}) = 1 + H(a)$ where $H(x) = -x\log_2 x - (1 - x)\log_2(1 - x)$.

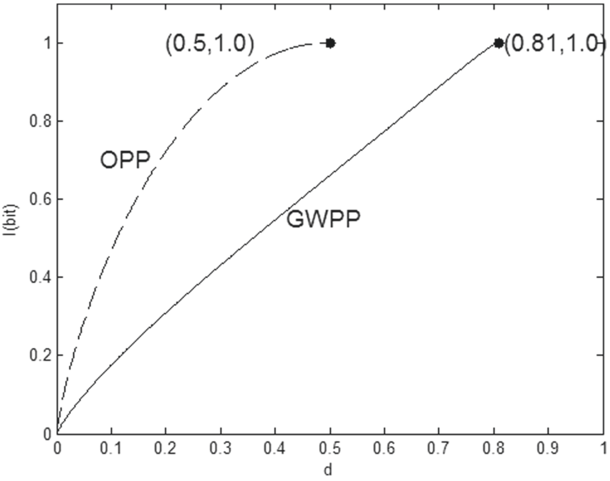

**Fig. 1** The comparison of the two detection results. The dotted line expresses the function $I(d_{lO})$ in OPP and the solid line expresses the function $I(d_{low})$in this protocol

If Eve wants to gain the full information ($I = 2$), the eavesdropping detection rate is $d_{low}(I = 2) = 0.81$. However, in OPP, $d_{lO}$ $(I = 1) = 0.5$. In order to compare the two functions, Fig. 1 is given.

As shown in Fig. 1, if Eve wants to gain the full information, he must face a larger detection rate in GWPP than OPP. This also indicates that GWPP is more secure than OPP.

Considering the probability of the control mode is c, the probability of the message mode is $1 - c$. If Eve wants to eavesdrop on an information transmission without being detected,

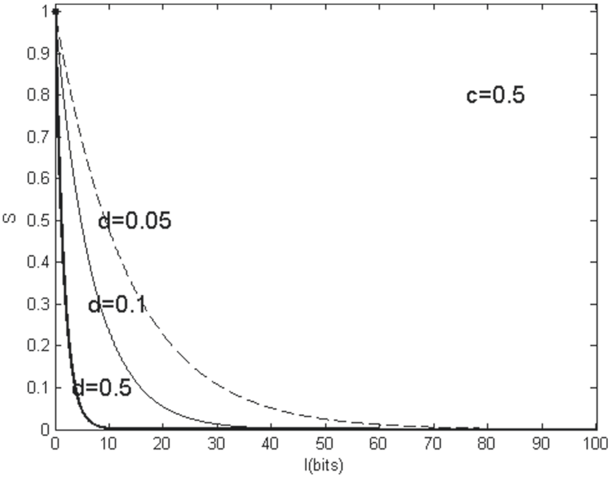

**Fig. 2** The probability of successful eavesdropping as a function of the maximal eavesdropped information, plotted for different detection probabilities $d$ $when$ $a = 0.8292$

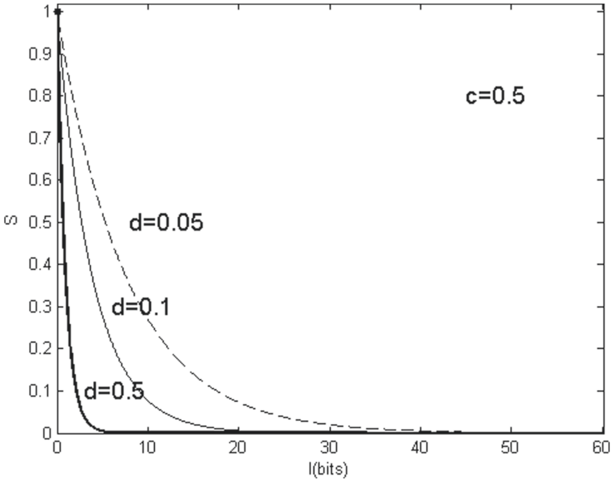

**Fig. 3** The probability of successful eavesdropping as a function of the maximal eavesdropped information, plotted for different detection probabilities *d when* $a = 0.0722$

the probability of the event is

$$s\left(c,d\right) = \left(1-c\right) + c\left(1-d\right)\left(1-c\right) + c^2\left(1-d\right)^2\left(1-c\right) + ... \\ = \tfrac{1-c}{1-c(1-d)}$$

Then the probability of successful eavesdropping $I = nI\left(d\right)$ bits is $s\left(I,c,d\right) = s\left(c,d\right)^{I/I(d)}$. Therefore

$$s\left(I,c,d\right) = \left(\frac{1-c}{1-c(1-d)}\right)^{I/I(d)}$$

When $I$ tends to infinity, $s$ tends to 0. That is to say, the protocol is asymptotically secure. For example, select $c = 0.5$. In Figs. 2 and 3 we have plotted the probability of successful eavesdropping as a function of the information gain $I$, for $c = 0.5$ and for different detection probabilities $d$ which Eve can choose. Variable $a$ has two values

Note that for $d$<0.5, Eve only gets one part of the massage and does not know which part he has got. So, this protocol is proved secure.

## 5 Conclusion

In summary, the protocol based on extended GHZ-W state is secure in theory. Compared with the existing schemes, the protocol has the following differences:

(1) By using extended GHZ-W state as decoy photons, the eavesdropping detection rate reaches 81%, which is higher than OPP.

(2) By using identity authentication, Man-in-the-middle attack can be resisted in the protocol.

(3) For one classical bit, one carrier qubit is transmitted only once. This protocol decreases not only the transmission of carrier qubits but also the number of decoy qubits compared with two-step protocol.

(4) Although the secret message is divides into several parts to transmit, the identity string of Alice and Bob can be reused.

**Acknowledgments** This work is supported by the National Natural Science Foundation of China (Grant No.61472048, No.61402058, No.61572246), Beijing Natural Science Foundation(4152038), China Postdoctoral Science Foundation funded project No.2014M561826.

## References

1. Bennett, C.H.: Phys. Rev. Lett. **68**, 3121–3124 (1992)
2. Bennett, C.H., Brassard, G., Mermin, N.D.: Phys. Rev. Lett. **68**, 557–559 (1992)
3. Chen, S.J., Liu, D.K., You, L.X., et al.: Chin. Sci. Bull. **58**, 1145–1149 (2013)
4. Cui, K., Wang, J., Zhang, H., et al.: Optik - Int. J. Light and Elect. Opt. **126**(23), 4747–4750 (2015)
5. Jasim, O.K., Abbas, S., El-Horbaty, E.M., et al.: Procedia Comput. Sci. **65**, 701–710 (2015)
6. Vernam, G.S.: J. Am. Inst. Elect. Eng. **45**, 109–115 (1926)
7. Bennett, C.H., Brassard, G.: In: proceeding of the IEEE international conference on computers, Systems and Signal Processing, pp. 175–179 (1984)
8. Beige, A., Englert, B.G., Kurtsiefer, C., et al.: J. Phys. S-Math. Gen. **35**, L407–L413 (2002)
9. Tsai, C.W., Hwang, T.: Sci. Chin. Ser. G-Phys. Mech. Astron. **56**, 1903–1908 (2013)
10. Yuan, H., Zhang, Q., Hong, L., et al.: Int. J. Theor. Phys. **53**, 2558–2564 (2014)
11. Xu, S., Chen, X., Wang, L., et al.: Int. J. Theor. Phys. **54**, 2436–2445 (2015)
12. Li, J., Jin, H.F., Jing, B.: Sci China Phys Mech Astron. **54**, 1612-1618 (2011)
13. Yang, Y.: Int. J. Theor. Phys. **53**, 2216–2221 (2014)
14. Li, W., Chen, J., Wang, X., et al.: Int. J. Theor. Phys. **54**, 100–105 (2015)
15. Feng, Z., Ou-Yang, Y., Zhou, V., et al.: Opt. Commun. **340**, 80–85 (2015)
16. Long, G.L., Liu, X.S.: Phys. Rev. A **65**, 032302 (2002)
17. Li, C.Y., Zhou, H.Y., Wang, Y., et al.: Chin. Phys. Lett. **22**, 1049–1502 (2005)
18. Alléaume, R., Branciard, C., Bouda, J., et al.: Theor. Comput. Sci. **560**, 62–81 (2014)
19. Yang, Y., Sun, S., Pan, Q., et al.: Optik - Int. J. Light and Elect. Opt. **126**(23), 3838–3843 (2015)
20. Wen, L., Yong-Bin, W., Wei, C.: Commun. Theor. Phys. **57**(4), 583–588 (2012)
21. Li, X.H., Deng, F.G., Zhou, H.Y.: Phys Rev A **74**, 054302 (2006)
22. Zhang, Z., Man, Z., Li, Y.: Phys. Lett. A **333**(1–2), 46–50 (2004)
23. Boström, K., Felbinger, T.: Phys. Lett. A **372**(22), 3953–3956 (2008)
24. Fei, G., FenZhuo, G., QiaoYan, W., et al.: Sci. China Ser. G Phys. Mech. **51**(12), 1853–1860 (2008)
25. Li, J., Li, L., Jin, H., et al. Phys. Lett. A **377**(39), 2729–2734 (2013)