ISSN 1674-1056
http://cpb.iphy.ac.cn
http://iopscience.iop.org/cpb
中国物理 B
Chinese Physics
中国物理 Chinese Physics B

Dynamic quantum secret sharing protocol based on two-particle transform of Bell states

Yu-Tao Du(杜宇韬), Wan-Su Bao(鲍皖苏)

Citation: Chin. Phys. B . 2018, 27(8): 080304. **doi:** 10.1088/1674-1056/27/8/080304

Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Improving continuous-variable quantum key distribution under local oscillator intensity attack using entanglement in the middle

Fang-Li Yang(杨芳丽), Ying Guo(郭迎), Jin-Jing Shi(石金晶), Huan-Li Wang(王焕礼), Jin-Jin Pan(潘矜矜)

Chin. Phys. B . 2017, 26(10): 100303. **doi:** 10.1088/1674-1056/26/10/100303

Round-robin differential quadrature phase-shift quantum key distribution

Chun Zhou(周淳), Ying-Ying Zhang(张莹莹), Wan-Su Bao(鲍皖苏), Hong-Wei Li(李宏伟), Yang Wang(汪洋), Mu-Sheng Jiang(江木生)

Chin. Phys. B . 2017, 26(2): 020303. **doi:** 10.1088/1674-1056/26/2/020303

Cryptanalysis and improvement of quantum broadcast communication and authentication protocol with a quantum one-time pad

Zhi-Hao Liu(刘志昊), Han-Wu Chen(陈汉武)

Chin. Phys. B . 2016, 25(8): 080308. **doi:** 10.1088/1674-1056/25/8/080308

Countermeasure against probabilistic blinding attack in practical quantum key distribution systems

Qian Yong-Jun, Li Hong-Wei, He De-Yong, Yin Zhen-Qiang, Zhang Chun-Mei, Chen Wei, Wang Shuang, Han Zheng-Fu

Chin. Phys. B . 2015, 24(9): 090305. **doi:** 10.1088/1674-1056/24/9/090305

Cryptanalysis and improvement of a quantum secret sharing scheme based on χ-type entangled states

Zhu Zhen-Chao, Zhang Yu-Qing, Fu An-Min

Chin. Phys. B . 2012, 21(1): 010307. **doi:** 10.1088/1674-1056/21/1/010307

Dynamic quantum secret sharing protocol based on two-particle transform of Bell states*

Yu-Tao Du(杜宇韬)[1,2] and Wan-Su Bao(鲍皖苏)[1,2,†]

[1] Henan Key Laboratory of Quantum Information and Cryptography, Zhengzhou Information Science and Technology Institute, Zhengzhou 450001, China
[2] Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei 230026, China

(Received 7 December 2017; revised manuscript received 13 April 2018; published online 10 July 2018)

To solve the problems of updating sub-secrets or secrets as well as adding or deleting agents in the quantum secret sharing protocol, we propose a two-particle transform of Bell states, and consequently present a novel dynamic quantum secret sharing protocol. The new protocol can not only resist some typical attacks, but also be more efficient than the existing protocols. Furthermore, we take advantage of the protocol to establish the dynamic secret sharing of a quantum state protocol for two-particle maximum entangled states.

Keywords: quantum secret sharing, two-particle transform of Bell states, attack, dynamic

PACS: 03.67.Dd, 03.67.Ac, 03.67.Hk **DOI:** 10.1088/1674-1056/27/8/080304

1. Introduction

Quantum secret sharing (QSS)[1] is one of the most attractive research branches in quantum cryptography,[1–5] which allows a secret of the dealer to be shared among many agents, and only the authorized groups of agents can reconstruct the secret information. In 1999, Hillery *et al.*[1] proposed the first QSS protocol based on the GHZ states. From then on, QSS has received widespread attention and a range of QSS protocols[6–24] have been presented in succession, which can be classified purposefully as two categories:[1] one is to share classical information and the other is to share quantum information (secret sharing of quantum state).

Although varieties of QSS protocols have been presented in recent decades, how we add or delete agents as well as update secret or sub-secrets (the messages held by agents) in the QSS protocol is still a novel field. Here we call it the problem of dynamic parameter update, and refer to this kind of protocol as a dynamic quantum secret sharing (DQSS) protocol. In 2011, Yang *et al.*[21] presented a DQSS protocol for the member expansion based on the ideas of the classical Shamir scheme.[25] However, in this protocol, the cost of quantum resource and the number of the transmission for member expansion are considerable. In 2012, Jia *et al.*[22] presented two DQSS protocols based on starlike duster states, which allows the agent group to change during the procedure of sharing classical and quantum secrets. But these protocols also consume too many quantum resources, and they cannot update secret or sub-secrets dynamically like Yang's protocol can. In 2013, another DQSS protocol was presented by Hsu *et al.*[23] based on the entanglement swapping of EPR pairs, which can allow an agent to be added or deleted. However, it has been proved that the protocol cannot resist a collective attack.[26] In 2016, a multi-group DQSS protocol was presented by Liu *et al.*[24] based on single photons, which is more flexible and practical, but it is fitter for sharing secrets between a boss and some groups.

In this paper, we firstly propose the two-particle transform of Bell states to solve the problems of dynamic parameter update in QSS, which can perform different local unitary operations separately on two particles of Bell states. According to this transform, we present a DQSS protocol realizing the functions of adding or deleting agents and updating sub-secrets or secrets. The new protocol can resist attacks such as a dense-coding attack, compound entanglement swapping attack, and a cheating attack from a dishonest agent. Based on the high coding-efficiency of a two-particle transform of Bell states and the exchangeability of the phase shift operation set, the number of coding operations is only half of the secret bits, and the computation complexity of the secret reconstruction is $O(n-1)$. Furthermore, we take advantage of the new protocol to establish the dynamic secret sharing of the quantum state (DSSQS) protocol for the two-particle maximum entangled states.

2. Two-particle transform of Bell states

We propose a method by the name of two-particle transform of Bell states, which can perform the different local unitary operations chosen by the dealer and agents separately from the Pauli operations and the 3-element phase shift

*Project supported by the National Basic Research Program of China (Grant No. 2013CB338002).
†Corresponding author. E-mail: bws2010thzz@163.com
© 2018 Chinese Physical Society and IOP Publishing Ltd

operations[27] on two particles of Bell states. Firstly, we prove the following conclusions.

Theorem 1 Suppose U_1 and U_2 are two arbitrary two-dimensional unitary operations, and $|\varphi\rangle_{th}$ is an arbitrary Bell state, thus

$$(U_1^{-1}\otimes I)(I\otimes U_2)(U_1\otimes I)|\varphi\rangle_{th}=(I\otimes U_2)|\varphi\rangle_{th}.$$

Proof Suppose $U_1=\begin{pmatrix}a_1 & a_2\\ a_3 & a_4\end{pmatrix}$ and$U_2=\begin{pmatrix}b_1 & b_2\\ b_3 & b_4\end{pmatrix}$. We can deduce it as follows:

$$\begin{aligned}&(I\otimes U_2)\cdot(U_1\otimes I)\\ &=\begin{pmatrix}U_2 & 0\\ 0 & U_2\end{pmatrix}\cdot\begin{pmatrix}a_1I & a_2I\\ a_3I & a_4I\end{pmatrix}\\ &=\begin{pmatrix}b_1 & b_2 & 0 & 0\\ b_3 & b_4 & 0 & 0\\ 0 & 0 & b_1 & b_2\\ 0 & 0 & b_3 & b_4\end{pmatrix}\cdot\begin{pmatrix}a_1 & 0 & a_2 & 0\\ 0 & a_1 & 0 & a_2\\ a_3 & 0 & a_4 & 0\\ 0 & a_3 & 0 & a_4\end{pmatrix}\\ &=\begin{pmatrix}b_1a_1 & b_2a_1 & b_1a_2 & b_2a_2\\ b_3a_1 & b_4a_1 & b_3a_2 & b_4a_2\\ b_1a_3 & b_2a_3 & b_1a_4 & b_2a_4\\ b_3a_3 & b_4a_3 & b_3a_4 & b_4a_4\end{pmatrix}\\ &=\begin{pmatrix}a_1U_2 & a_2U_2\\ a_3U_2 & a_4U_2\end{pmatrix}=(U_1\otimes U_2).\end{aligned}$$

Using the same process as above, we have

$$\begin{aligned}&(U_1\otimes I)\cdot(I\otimes U_2)\\ &=\begin{pmatrix}b_1a_1 & b_2a_1 & b_1a_2 & b_2a_2\\ b_3a_1 & b_4a_1 & b_3a_2 & b_4a_2\\ b_1a_3 & b_2a_3 & b_1a_4 & b_2a_4\\ b_3a_3 & b_4a_3 & b_3a_4 & b_4a_4\end{pmatrix}=(U_1\otimes U_2).\end{aligned}$$

Thus

$$\begin{aligned}&(U_1^{-1}\otimes I)(I\otimes U_2)(U_1\otimes I)|\varphi\rangle_{th}\\ &=(U_1^{-1}\otimes I)(U_1\otimes I)(I\otimes U_2)|\varphi\rangle_{th}=(I\otimes U_2)|\varphi\rangle_{th}.\end{aligned}$$

According to theorem 1, when designing the QSS protocol, we can regard U_1 as the compound operation on photon t performed by agents, and U_2 as the encoding operation of the secret on photon h performed by the dealer, and U_1^{-1} as the reverse compound operation on photon t performed by agents.

It is obvious that there are three properties on this transform:

(i) Independence of operations

Based on Theorem 1, the operation on one particle of Bell states has no influence on the operation on the other particle. Thus we can make use of this property to design the DQSS protocol.

(ii) Nonlocal correlation of measuring results

Based on the nonlocal space properties of quantum entangled states, the local operation performed on one particle of Bell states can be deduced just by measuring collectively on the Bell states. Thus when we design the QSS protocol, the property can ensure the security of the protocol: if the unauthorized groups cannot obtain enough messages of agents' operations (as the sub-secrets), they cannot deduce the encoding operation (as the secret) by measuring.

(iii) High coding-efficiency

Based on the quantum high-coding scheme,[28] the Pauli operations on 1 qubit can code 2 bit classical messages; that is to say, the Pauli operation $I(\sigma_x,\sigma_z,\mathrm{i}\sigma_y)$ corresponds to the two classical bits "00" ("10","01","11"). In the QSS protocol, if the number of classical secrets is n bits, the number of coding operations is $\lceil n/2\rceil$, as many as half of the secret bits.

3. DQSS protocol based on two-particle transform of Bell states

The new DQSS protocol consists of two parts as follows.

3.1. Process of secret sharing

Suppose that Alice is the dealer with her secret, the set of agents is B = {Bob, Charlie, ..., Zach}, and the number of B is n. The purpose of the protocol is that Alice shares a secret M among these agents in B, and all the agents can only reconstruct the secret information by cooperating with each other.

i) Alice prepares k pairs of Bell states (i.e., $|\varphi_1\rangle_{th},\ldots,|\varphi_k\rangle_{th}$) randomly from $\{|\phi^+\rangle,|\phi^-\rangle,|\psi^+\rangle,|\psi^-\rangle\}$, here $|\phi^\pm\rangle=(|00\rangle\pm|11\rangle)/\sqrt{2}$, $|\psi^\pm\rangle=(|01\rangle\pm|10\rangle)/)/\sqrt{2}$. Then she stores all the photons h of these Bell states (as H-sequence) in her laboratory, and sends all the photons t (as T-sequence) to Bob.

ii) After receiving the T-sequence, Bob firstly ascertains whether it is the single-photon sequence by using the photon number splitter (PNS: 50 = 50) or photon beam splitter(PBS: 50 = 50), etc. If not, he aborts the communication; otherwise, he performs the local unitary operations $U(\alpha_i)$ $(i=1,2,\ldots,k)$ respectively on the photon t_i of the T-sequence, which is chosen randomly from the phase shift operation set $S=\{U(0),U(2\pi/3),U(4\pi/3)\}$.[27] Here

$$U(\alpha_i)=\begin{pmatrix}\cos\alpha_i & -\sin\alpha_i\\ \sin\alpha_i & \cos\alpha_i\end{pmatrix},\quad \alpha_i\in\left\{0,\frac{2\pi}{3},\frac{4\pi}{3}\right\}.$$

Then Bob stores all of the operation messages as his sub-secret, and sends the $\mathrm{T}^{(1)}$-sequence (transformed from T-sequence) to Charlie.

iii) Charlie and the other agents perform procedures similar to Bob till the last agent Zach finishes his operations. At that time, Zach stores all the photons of the $\mathrm{T}^{(n)}$-sequence in his laboratory, and tells Alice by the classical channel that all the operations of agents have been finished.

iv) After receiving the message from Zach, Alice encodes the secret M by performing the Pauli operations on the

photons of the H-sequence according to the following definitions: $I(\sigma_x, \sigma_z, \mathrm{i}\sigma_y)$ corresponds to the two classical bits "00" ("10","01","11"). Here

$$I = |0\rangle\langle 0| + |1\rangle\langle 1|, \quad \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|,$$
$$\sigma_x = |1\rangle\langle 0| + |0\rangle\langle 1|, \quad \mathrm{i}\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|.$$

Then Alice sends the $\mathrm{H}^{(1)}$-sequence (encoded from H-sequence) to Zach.

v) After receiving the $\mathrm{H}^{(1)}$-sequence, Zach together with other agents firstly performs the eavesdropping detection with Alice. First Alice chooses randomly k_1 positions of $\mathrm{T}^{(n)}$-sequence to tell all the agents. Then the agents choose randomly a delegate (like Green) to collect the others' messages of operations on the chosen photons and to perform the reverse compound operations deduced by these messages. Then Green measures these photons associated with the corresponding photons of the $\mathrm{H}^{(1)}$-sequence in the Bell-basis, and sends the measuring results to Alice. According to the results and the initial states of corresponding Bell states, Alice deduces the corresponding operations and judges whether the photons are attacked by comparing them with the corresponding messages of the secret. If so, the communication is aborted. Otherwise, Alice announces all of the initial Bell states.

If there is no eavesdropping, all the agents can recover the secret by collaborating together. Similarly, they choose randomly a delegate (like Green) to collect all the agents' messages of operations. Then Green performs the reverse compound operations deduced by these messages on photons of the $\mathrm{T}^{(n)}$-sequence and measures these photons associated with the corresponding photons of the $\mathrm{H}^{(1)}$-sequence in the Bell-basis. Finally, he can deduce the secret M, according to both the initial Bell states from Alice and the corresponding measuring results. The structure of the new protocol is depicted in Fig. 1.

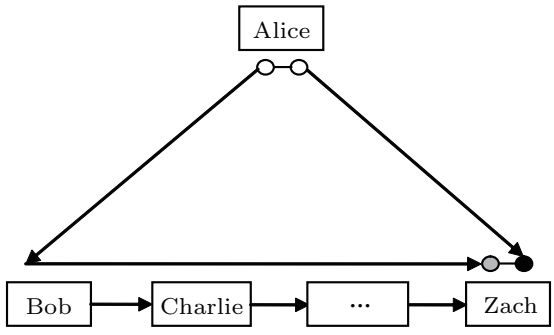


Fig. 1. Structure of the dynamic QSS protocol.

Symbol "○–○" denotes Bell states $|\varphi_i\rangle_{th}$ $(i = 1, 2, \ldots, k)$ prepared by Alice; symbol "○–●" represents the new entangled states, the left particle of which the phase shift operations have been performed on by all of the agents, and the right particle of which the Pauli operations have been performed on by Alice.

3.2. Process of dynamic parameters update

Without loss of generality, we suppose that $|\phi^+\rangle_{th}$ are the Bell states prepared by Alice, $U = \prod_{i=1}^{n} U_i$ is the compound operation on photon t by all the agents and N is the encoding operation on photon h by Alice. At that time, the new entangled state is $|\varphi\rangle_{th} = (U \otimes N)|\phi^+\rangle_{th}$. Before Alice sends photon h to agents, two actions are taken as follows.

3.2.1. Update the sub-secret or secret message

(I) Some agent (like Green) wants to update his sub-secret U_j $(j = 1, 2, \ldots, n)$. He can ask Zach to send photon t to himself, and then perform operation $U_j' \cdot U_j^{-1}$ on it. At that time, the new entangled states have transformed like this

$$(U_j' \cdot U_j^{-1} \otimes I)|\varphi\rangle_{th} = (U' \otimes N)|\phi^+\rangle_{th}, \quad U' = U_j' \cdot \prod_{i=1, i\neq j}^{n} U_i.$$

(II) Alice wants to update the secret. She can perform operation $N' \cdot N$ on photon h. At that time, the new entangled states have transformed like this

$$(I \otimes N' \cdot N)|\varphi\rangle_{th} = (U \otimes N')|\phi^+\rangle_{th}.$$

3.2.2. Add or delete an agent

I) Some agent (like Green) wants to leave the protocol. He can ask Zach to send photon t to himself, and then perform operation U_j^{-1} on it. At that time, the new entangled states have transformed like this

$$(U_j^{-1} \otimes I)|\varphi\rangle_{th} = (U' \otimes N)|\phi^+\rangle_{th}, \quad U' = \prod_{i=1, i\neq j}^{n} U_i.$$

II) The new agent (like James) wants to take part in the protocol. Similarly, he can ask Zach to send photon t to himself to perform his own operation U_{n+1}. At that time, the new entangled states have transformed like this

$$(U_{n+1} \otimes I)|\varphi\rangle_{th} = (U_{n+1} \cdot U \otimes N')|\phi^+\rangle_{th}.$$

If Alice has sent photon h to agents, the secret cannot be updated obviously. Before measuring the entangled states, however, it is allowed to update the sub-secrets of agents, and add or delete an agent.

4. Security analysis

According to Ref. [29], the QSS protocol is secure if and only if both the sub-secret and secret are secure. Except a series of attacks in the practical views by using the photon number splitter, etc., we will analyze the security of both the sub-secret and secret separately from the theoretical views.

4.1. Security of the sub-secret message

The theoretic foundation of attack to sub-secret is as follows: the attacker measures the different quantum states which are gained by performing the different unitary operations (like I, σ_x, σ_z, $\mathrm{i}\sigma_y$) on the same quantum states, and then can deduce these operations by distinguishing among the quantum states. The typical example is the dense-coding attack.[30]

In the dense-coding attack strategy,[30] the attacker (like Eve) intercepts the $\mathrm{T}^{(j)}$-sequence ($j = 1,\ldots,n$) sent from one agent (like Green) to the other agent (like Hulk), and replaces them by a fake T'-sequence, which is composed of the first particles of the ordered Bell states (like $|\psi^-\rangle_{t'h'}$) prepared by herself. Eve sends the T'-sequence to Hulk and intercepts them again when Hulk has operated on these photons and sends them to the next agent. Then Eve performs collective measurements on each pair of Bell states to deduce the operations of Hulk, and performs the same local operations on every photons of the $\mathrm{T}^{(j)}$-sequence to send them to the next agent. At that time, Eve can obtain the sub-secret of Hulk while she has not been detected by anyone.

This protocol can resist this attack. Now we prove that the operations of the phase shift operations set $S = \{U(0), U(2\pi/3), U(4\pi/3)\}$ cannot be distinguished exactly by measuring the different quantum states, which are gained by someone's performing operations of set S randomly on the same Bell states (from $\{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$).

Proof Without loss of generality, we suppose that the Bell states are $|\phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, and may choose randomly the operation of set S on the first particle of $|\varphi^+\rangle$ as follows:

$$\begin{aligned} & U(\alpha)\otimes I\,|\phi^+\rangle \\ = & \frac{1}{\sqrt{2}}(\cos\alpha\,|00\rangle - \sin\alpha\,|01\rangle + \sin\alpha\,|10\rangle + \cos\alpha\,|11\rangle). \end{aligned}$$

If $\alpha = 0$, $U(0)\otimes I\,|\phi^+\rangle = \dfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\phi^+\rangle$.

If $\alpha = \dfrac{2}{3}\pi$, let

$$\begin{aligned} |\delta\rangle &= U\left(\frac{2}{3}\pi\right)\otimes I\,|\phi^+\rangle \\ &= \frac{1}{\sqrt{2}}\left(\frac{1}{2}|00\rangle + \frac{\sqrt{3}}{2}|01\rangle - \frac{\sqrt{3}}{2}|10\rangle + \frac{1}{2}|11\rangle\right) \\ &= \frac{1}{2}|\phi^+\rangle + \frac{\sqrt{3}}{2}|\psi^-\rangle. \end{aligned}$$

If $\alpha = \dfrac{4}{3}\pi$, let

$$\begin{aligned} |\beta\rangle &= U\left(\frac{4}{3}\pi\right)\otimes I\,|\phi^+\rangle \\ &= \frac{1}{\sqrt{2}}\left(\frac{1}{2}|00\rangle - \frac{\sqrt{3}}{2}|01\rangle + \frac{\sqrt{3}}{2}|10\rangle + \frac{1}{2}|11\rangle\right) \\ &= \frac{1}{2}|\phi^+\rangle - \frac{\sqrt{3}}{2}|\psi^-\rangle. \end{aligned}$$

At this time, the inner products between the two of $\{|\phi^+\rangle, |\delta\rangle, |\beta\rangle\}$ are all nonzero:

$$|\langle\delta|\beta\rangle| = |\langle\delta|\phi^+\rangle| = |\langle\phi^+|\beta\rangle| = \frac{1}{2} \neq 0.$$

Obviously the three entangled states cannot be distinguished exactly in the Bell-basis. The results about $|\phi^-\rangle$, $|\psi^+\rangle$ and $|\psi^-\rangle$ are the same as about $|\phi^+\rangle$. ■

4.2. Security of secret message

There are mainly two kinds of attack strategies on the secret message: one is the compound entanglement swapping attack,[31–33] and the other is the cheating attack.[34]

4.2.1. Security against compound entanglement swapping attack

This kind of attack strategy combines an intercept-and-resend attack and entanglement swapping scheme (such as the collective attack[26]). In these attack strategies,[31–33] the dishonest agent (such as Eve) or their group can intercept and replace the travel photon (such as photon t) with photon t' of Bell state $|\psi^-\rangle_{t'h'}$, and then send it to the dealer. After the dealer sends back photon t' with the secret, Eve can associate with other agents to obtain the secret by measuring both photon t' and h' of $|\psi^-\rangle_{t'h'}$ together. If the eavesdropping detection is coming, Eve can measure both photon t and h' together and deduce the suitable unitary operations according to the discipline of entanglement swapping, to escape from the detection.

The compound entanglement swapping attack requires two basic conditions: firstly, the agents of the QSS scheme need to send photon t to the dealer after their operations, thus Eve has the opportunity to replace it with fake photon t'; secondly, the fake operations declared by Eve must be contained in the unitary operations set of the QSS protocol so that the lies can escape from the eavesdropping detections. Correspondingly, there are two effective means against this kind of attack: firstly, modify the structure of the QSS protocol without sending any photons to the dealer, so that it is useless for Eve to replace the travel photon t; secondly, restrict Eve's announcements, so that she cannot declare the proper unitary operations to hide her behaviors in the process of detections.

The protocol can resist the kind of attack by using the new structure and the phase shift operation set. Firstly, in our QSS protocol the dealer does not ask agents to send photon t back, but encodes the secret on photon h and then sends it to agents. Secondly, the phase shift operation set $S = \{U(0), U(2\pi/3), U(4\pi/3)\}$ can restrict the fake announcements.[24] Suppose that S' is the fake operation set, and all elements of S and their compositions may establish the

multiplicative group (S). It is easy to know $S=(S)$, then

$$U\left(\frac{2}{3}\pi\right)\cdot U\left(\frac{4}{3}\pi\right)=U\left(\frac{4}{3}\pi\right)\cdot U\left(\frac{2}{3}\pi\right)=U(0) \text{ and}$$
$$\left(U\left(\frac{2}{3}\pi\right)\right)^3=\left(U\left(\frac{4}{3}\pi\right)\right)^3=U(0).$$

It has been demonstrated that $S'\not\subset(S)$ in Ref. [29]. Thus, the fake operations cannot be deduced by all elements of S and their behaviors cannot escape from the detections.

4.2.2. Security against cheating attack

A cheating attack from a dishonest agent[34] is as follows. In the secret reconstruction phase, the dishonest agent may provide a false share so that the secret cannot be recovered correctly by the authorized groups but he can correct the error alone. At present, most schemes cannot resist this attack. Only by using the verifiable QSS scheme,[34] can authorized groups resist an attack by verifying the truth of shares.

Our protocol can also resist this cheating attack by utilizing the phase shift operation set $S=\{U(0),U(2\pi/3),U(4\pi/3)\}$. Suppose that $|\phi^+\rangle$ is the Bell states prepared by Alice, and Eve is a dishonest agent who performed the unitary operation $U(\alpha)\in S$ on photon t in Step 2 or 3. However, she provides the false operation message $U(\beta)\neq U(\alpha)$ in Step 5. If the compound operation of other agents is $U(\theta)$, and the encoding operation of Alice on photon h is N, thus $[(U^{-1}(\beta+\theta)\cdot U(\alpha+\theta))\otimes N]\,|\phi^+\rangle_{th}\neq (I\otimes N)\,|\phi^+\rangle_{th}$, and $N\in\{I,\sigma_x,\sigma_z,\mathrm{i}\sigma_y\}$.

Now, the entanglement states cannot be located in the basis $\{|\phi^+\rangle,|\phi^-\rangle,|\psi^+\rangle,|\psi^-\rangle\}$, but in the basis $\{(|\phi^+\rangle+\sqrt{3}\,|\psi^-\rangle)/2,\ (|\phi^-\rangle+\sqrt{3}\,|\psi^+\rangle)/2,\ (|\psi^-\rangle+\sqrt{3}\,|\phi^+\rangle)/2,\ (|\psi^+\rangle+\sqrt{3}\,|\phi^-\rangle)/2\}$ or $\{(|\phi^+\rangle-\sqrt{3}\,|\psi^-\rangle)/2,\ (|\phi^-\rangle-\sqrt{3}\,|\psi^+\rangle)/2,\ (|\psi^-\rangle-\sqrt{3}\,|\phi^+\rangle)/2,\ (|\psi^+\rangle-\sqrt{3}\,|\phi^-\rangle)/2\}$. Obviously the two bases are non-orthogonal with the Bell basis. If Eve provides the false share for recovery, the authorized group of agents will choose the wrong measurement basis. According to the uncertainty principle, the measurement result about the entanglement states will inevitably be distributed in error states randomly, so that Eve cannot correct and obtain the secret from the error because of the irreversibility of measurement. Therefore, the protocol can resist an in-attacker's cheating attack.

5. Efficiency analysis

The new DQSS protocol is more efficient than previous ones.

Firstly, the two-particle transform of Bell states is based on a quantum dense-coding scheme. Thus we can transmit the 2-bit classical message by performing an operation on 1 qubit in this protocol.

Secondly, the elements of the set $S=\{U(0),U(2\pi/3),U(4\pi/3)\}$ satisfy the commutative principle of multiplication. Suppose $\forall\alpha,\beta\in\{0,2\pi/3,4\pi/3\}$, then

$$\begin{aligned}U(\alpha)\cdot U(\beta)&=\begin{pmatrix}\cos\alpha & -\sin\alpha\\ \sin\alpha & \cos\alpha\end{pmatrix}\cdot\begin{pmatrix}\cos\beta & -\sin\beta\\ \sin\beta & \cos\beta\end{pmatrix}\\&=\begin{pmatrix}\cos(\alpha+\beta) & -\sin(\alpha+\beta)\\ \sin(\alpha+\beta) & \cos(\alpha+\beta)\end{pmatrix}\\&=U(\beta)\cdot U(\alpha)=U(\alpha+\beta).\end{aligned}$$

So the agents need not consider the order of agents' local unitary operations in step 2 or 3 but just do the addition to deduce the compound operation of all agents. Suppose that Bob_i $(i=1,\ldots,n)$ performs unitary operations $U^{(i)}=U(\theta_i)$ on the photon t, where $\theta_i\in\{0,2\pi/3,4\pi/3\}$. The compound operation of all agents is

$$U=\prod_{i=1}^{n}U^{(i)}=U(\theta)\quad\text{and}\quad\theta=\sum_{i=1}^{n}\theta_i\in\left\{0,\frac{2\pi}{3},\frac{4\pi}{3}\right\}.$$

Thus it reduces the computation complexity of secret reconstruction to $O(n-1)$. It not only provides convenience to the secret reconstruction phase, but also improves the efficiency of the scheme.

Thirdly, the unitary operation set S has the least number of elements on the premise of satisfying the conditions of security, which improves further the efficiency for recovering the secret. According to the conclusions in Refs. [35] and [36], if the elements of set S constitute a multiplicative group (S), the number of elements of (S) must be no less than 3, or else elements of (S) can be distinguished during performing them on a suitable single-particle state or one particle of an entangled state, which cannot satisfy the conditions of security. Obviously, the number of elements of (S) reaches the lower bound: $(S)=S=\{U(0),U(2\pi/3),U(4\pi/3)\}$.

The detailed comparisons between the new protocol and some existing ones are presented in Table 1.

Table 1. Comparisons between new protocol and some existing ones

Issue\protocol	Yang's protocol[21]	Jia's protocol[22]	Hsu's protocol[23]	The new protocol
The total number of photons	2 m$k+k'$	$k(2n+1)+k'$	$2k(n+1)+k'$	$2k$
The times of encoding operations	$2n(n-1)k$	/	/	k
The complexity of secret reconstruction	O(n^t)	/	/	$O(n-1)$

Suppose that the length of the secret message is $2k$ bit, and the total number of sample photons used for detections will be k' bit.

6. New DSSQS protocols

According to Ref. [20], we can also present a kind of DSSQS protocol based on the new protocol above, the DQSS protocol for two-particle maximum entangled states, which is as secure as the former, and similarly has the functions of dynamic parameter update: adding or deleting an agent and updating sub-secrets. Here we just brief it as follows:

Suppose that the unknown two-particle maximum entangled state is $|\varphi\rangle_{12} = \alpha|+x\rangle_1|+y\rangle_2 + \beta|-x\rangle_1|-y\rangle_2\,(\alpha^2+\beta^2 = 1)$. Similarly, Alice prepares two pairs of Bell states (like $|\varphi_1\rangle_{th}$ and $|\varphi_2\rangle_{th}$), one of which is used for the quantum entanglement swapping from Alice to Bob, the other is used to send the classical message of the Bell-state measuring result on both $|\varphi\rangle$ and one particle of $|\varphi_2\rangle_{th}$ to other agents by use of the DQSS protocol we just proposed. In the secret reconstruction phase, Bob and other agents must collaborate together to reconstruct the unknown single quantum state. Moreover, this protocol can expand straightly into the one for unknown GHZ states. The structure of the DSSQS protocol for two-particle maximum entangled states is depicted in Fig. 2.

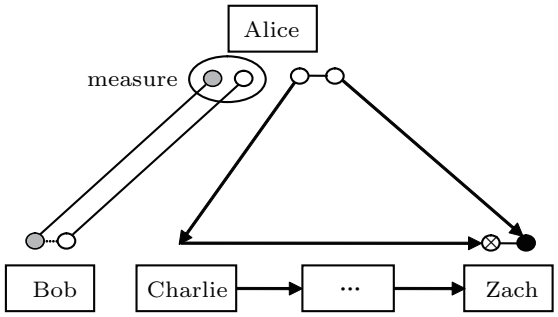


Fig. 2. Structure of the DSSQS protocol for two-particle maximum entangled states.

Symbol "○—○" denotes unknown two-particle entangled state $|\varphi\rangle_{12}$; symbol "○—○" represents Bell states $|\varphi_1\rangle_{th}$ or $|\varphi_2\rangle_{th}$ prepared by Alice; symbol "⊗—●" refers to new entangled states, the left particle of which the phase shift operations have been performed on by agents except Bob, and the right particle of which Pauli operations have been performed on by Alice.

7. Summary

To summarize, firstly, we have proposed the two-particle transform of Bell states, and then presented a novel DQSS protocol for classical messages and DSSQS protocols based on the former one. Compared with the existing QSS protocol, this kind of QSS protocol is not only more secure and efficient, but also has the functions of a dynamic parameter update. Besides, our protocols are merely the (n,n) threshold protocols, which can be described by the fact that at least n agents must combine their sub-secrets together to recover the secret, and we will propose the (t,n) threshold protocol (with $t < n$) in the coming paper. Furthermore, the two-particle transform of Bell states may also have potential impacts on quantum key distribution,[37,38] quantum secure direct communication, quantum signature, and quantum secure multiparty computation, and so on, which is worth further exploration.

References

[1] Hillery M, Buzek V and Berthiaume A 1999 *Phys. Rev. A* **59** 1829
[2] Bennett C H and Brassard G 1984 *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (New York: IEEE) p. 175
[3] Zeng G H, Ma W P and Wang X M 2001 *Acta Electron. Sin.* **29** 1098
[4] Long G L, Wang C, Li Y S and Deng F G 2011 *Sci. Sin. Phys. Mech. Astron.* **41** 332
[5] Ma H X, Bao W S, Li H W and Zhou C 2016 *Chin. Phys. B* **25** 080309
[6] Karlsson A, Koashi M and Imoto N 1999 *Phys. Rev. A* **59** 162
[7] Cleve R, Gottesman D and Lo H K 1999 *Phys. Rev. Lett.* **83** 648
[8] Gottesman D 2000 *Phys. Rev. A* **61** 042311
[9] Tittel W, Zbinden H and Gisin N 2001 *Phys. Rev. A* **63** 042301
[10] Karimipour V, Bahraminasab A and Bagherinezhad S 2002 *Phys. Rev. A* **65** 042320
[11] Chau H F 2002 *Phys. Rev. A* **66** 060302
[12] Guo G P and Guo G C 2003 *Phys. Lett. A* **310** 247
[13] Xiao L, Long G L, Deng F G and Pan J W 2004 *Phys. Rev. A* **69** 052307
[14] Zhang Z J, Li Y and Man Z X 2005 *Phys. Rev. A* **71** 044301
[15] Zhang Z J and Man Z X 2005 *Phys. Rev. A* **72** 022303
[16] Zhang Z J 2005 *Phys. Lett. A* **342** 60
[17] Deng F G, Li X H, Zhou H Y and Zhang Z J 2005 *Phys. Rev. A* **72** 044303
[18] Hsu L Y 2003 *Phys. Rev. A* **68** 022306
[19] Han L F, Liu Y M, Liu J and Zhang Z J 2008 *Opt. Commun.* **281** 2690
[20] He L, Zhen Zh, Chen L K, Li Zh D, Liu Ch, Li L, Liu N L, Ma X F, Chen Y Ao, and Pan J W 2016 *Phys. Rev. Lett.* **117** 030501
[21] Yang Y G, Wang Y, Chai H, Teng Y and Zhang H 2011 *Opt. Commun.* **284** 3479
[22] Jia H Y, Wen Q Y, Gao F, Qin S J and Guo F Z 2012 *Phys. Lett. A* **376** 1035
[23] Hsu J L, Chong S K, Hwang T and Tsai C W 2013 *Quantum Inf. Proc.* **12** 331
[24] Liu H W, Ma H Q, Wei K J, Yang X Q, Qu W X, Dou T Q, Chen Y T, Li R X and Zhu W 2016 *Phys. Lett. A* **380** 2349
[25] Shamir A 1979 *Commun. ACM* **22** 612
[26] Wang T Y and Li Y P 2013 *Quantum Inf. Proc.* **12** 1991
[27] Du Y T and Bao W S 2013 *Opt. Commun.* **308** 159
[28] Bennett C H and Wiesner S J 1992 *Phys. Rev. Lett.* **69** 2881
[29] Wang T Y and Wen Q Y 2011 *Quantum Inf. Comput.* **11** 0434
[30] Gao F, Qin S J, Guo F Z and Wen Q Y 2011 *IEEE J. Quantum Electron.* **47** 630
[31] Lin S, Wen Q Y, Gao F and Zhu F C 2008 *Opt. Commun.* **281** 4553
[32] Wang T Y, Wen Q Y, Gao F, Lin S and Zhu F C 2008 *Phys. Lett. A* **373** 65
[33] Gao G 2011 *Opt. Commun.* **284** 902
[34] Yang Y G, Teng Y W, Chai H P and Wen Q Y 2011 *Int. J. Theor. Phys.* **50** 792
[35] Acín A 2001 *Phys. Rev. Lett.* **87** 177901
[36] Duan R Y, Feng Y and Ying M S 2007 *Phys. Rev. Lett.* **98** 100503
[37] Zhou C, Zhang Y Y, Bao W S, Li H W, Wang Y and Jiang M S 2017 *Chin. Phys. B* **26** 020303
[38] Bao H Z, Bao W S, Wang Y, Chen R K, Ma H X, Zhou C and Li H W 2017 *Chin. Phys. B* **26** 050302