scientific reports

OPEN

Standard (3, 5)-threshold quantum secret sharing by maximally entangled 6-qubit states

Yinxiang Long[1]✉, Cai Zhang[2] & Zhiwei Sun[3]✉

In this paper, a standard (3, 5)-threshold quantum secret sharing scheme is presented, in which any three of five participants can resume cooperatively the classical secret from the dealer, but one or two shares contain absolutely no information about the secret. Our scheme can be fulfilled by using the singular properties of maximally entangled 6-qubit states found by Borras. We analyze the scheme's security by several ways, for example, intercept-and-resend attack, entangle-and-measure attack, and so on. Compared with the other standard threshold quantum secret sharing schemes, our scheme needs neither to use *d*-level multipartite entangled states, nor to produce shares by classical secret splitting techniques, so it is feasible to be realized.

Classical secret sharing (CSS), proposed by Shamir[1] and Blakley[2] independently in 1979, is an important issue in modern cryptography. Its basic idea is to divide the classical secret into some shares such that the dealer can transmit the shares to the participants respectively through classical channel, and only all the participants work together can recover the secret, at the same time, some parts of them can not get any information of the secret. Hillery et al.[3] proposed the concept of quantum secret sharing with reference to the classical secret sharing schemes, and designed two quantum secret sharing (QSS) schemes by using the quantum correlation of the GreenHorne–Zeilinger (GHZ) states in 1998. In Hillery's QSS scheme of classical information, Alice shares her classical key with Bob and Charlie based on the correlations of the results of measurements with Pauli operators X or Y. However, in their QSS scheme of quantum information, teleportation is used for Alice to share quantum state with Bob and Charlie. In the same year, Karlsson et al.[4] proposed another secret sharing protocol using the quantum correlation of two-particle entangled states, which encodes one bit information into unbiased orthogonal entangled state set $\{|\psi^+\rangle, |\phi^-\rangle\}$ or $\{|\Psi^+\rangle, |\Phi^-\rangle\}$ randomly in order to prevent the attack from a dishonest receiver or an eavesdropper, who wants to obtain the secret alone without the help of other agents by capturing both particles and performing a measurement with Bell basis. Here,

$$\begin{aligned} |\psi^+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), |\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \\ |\Psi^+\rangle &= \frac{1}{\sqrt{2}}(|\psi^+\rangle + |\phi^-\rangle), |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|\psi^+\rangle - |\phi^-\rangle). \end{aligned} \tag{1}$$

Guo[5] proposed the first QSS scheme of classical key using product state as quantum channel. It is based on BB84 by encoding 1 bit with $\{|00\rangle, |11\rangle\}$ or $\{|++\rangle, |--\rangle\}$ randomly. Afterwards, several novel QSS protocols using single photon and local unitary operations were presented by Zhang[6], Han[7], and Yan[8], respectively. Recently, Tavakoli[9] pointed that a wide class of quantum protocols using d-level GHZ entanglement states (d is odd prime) can be mapped into simple ones involving one qudit, and proposed a QSS protocol which requires only sequential communication of a single d-level quantum system. Furthermore, Hao[10] proposed a novel quantum secret sharing scheme by a single-particle p^2-dimensional quantum system (p is a prime) and unitary transformation between these mutually unbiased bases.

However, entangled states play a more important role in all sorts of quantum information processing tasks including QSS. Up to now, in addition to Hillery's and Karlsson's schemes mentioned earlier, a large number of QSS schemes have been proposed based on various entangled states, such as GHZ states[11–14], GHZ like states[15,16], Bell states[17–21], genuine multiparty entangled states (including maximally genuine multiparty entangled states,

[1]Department of Automation Engineering, Guangdong Technical College of Water Resources and Electric Engineering, Guangzhou 510925, China. [2]College of Mathematics and Informatics, South China Agricultural University, Guangzhou 510642, China. [3]School of Artificial Intelligence, Shenzhen PolyTechnic, Shenzhen 518055, China. ✉email: longyxlongyx@163.com; smeker@szpt.edu.cn

cluster states and graph states, etc.)[22–26], and d-level entangled states (for example, d-level GHZ states and d-level Bell states)[27–32].

A $(t, n)(t \leq n)$ threshold secret sharing (abbreviated to TSS) scheme divides a secret into n pieces such that any t or more than t out of n pieces can recover the secret, while less than t pieces can not. Shamir and Blakley proposed independently the first threshold classical secret sharing (abbreviated to TCSS) schemes, which are called Lagrange interpolating polynomial scheme and vector scheme, respectively. Naturally, if a TSS scheme is implemented by quantum technique, it is called (t, n) threshold quantum secret sharing (abbreviated to TQSS) scheme.

By using the technique of quantum error correction coding, the first TQSS scheme sharing quantum states was proposed by Cleve[33] in 1999. In 2013, Gheorghiu[34] introduced a scheme by embedding a classical linear code into a quantum error-correcting code and then mapping the latter to a quantum secret sharing protocol. In this protocol, some of the players are only required to perform local measurements and share their measurement results via classical channels.

It is worth pointing out that TQSS schemes based on quantum error correction coding can also be used to share classical messages because schemes sharing quantum state can also share classical information. However, these methods are not easy to be implemented because they usually require complicated operations and d-level multiparty entangled states.

Another importatnt idea of TQSS sharing classical information is to employ Shamir's secret splitting technique[1] to produce shares (classical information) and transmit shares by quantum mechanics. At present, a large number of TQSS schemes sharing classical information have been developed. Some examples are listed as follows:

(1) In 2005, Tokunaga[35] presented the notion of threshold collaborative unitary transformation or threshold quantum cryptography. It employs Shamir's secret splitting technique and avoids the constraint of the quantum no-cloning theorem.

(2) In 2008, Yang[36] proposed a (t, m)-(s, n) TQSS scheme, in which any t of m members in group 1 can recover the secret in cooperation with any s of n members in group 2 using a sequence of single photons. The president firstly generates a classical key K and randomly divides it into $K1$ and $K2$ whose values meet $K = K_1 \bigoplus K_2$. He makes $m(n)$ shares of the $K1(K2)$ using Shamir's secret splitting technique.

(3) In 2009, Li[37] proposed a TQSS scheme to share classical secret based on Bell states and Pauli operators by using Shamir's secret splitting technique.

(4) In 2013, Massoud[38] proposed a (t, m)-(s, n) TQSS scheme to share classical secret based on GHZ states and Pauli operators by using Shamir's secret splitting technique.

(5) In 2015, Qin[39] proposed a TQSS scheme to share a quantum state based on the phase shift operation on single qubit by using Shamir's secret splitting technique, in which the participants perform the phase shift operations on the quantum state according to their private keys, and any t out of the n participants can reconstruct the original quantum state. In 2018, Lu[40] proposed another TQSS scheme to share classical information in addition to quantum states by using the similar idea to Qin's.

(6) In 2016, Qin[41] proposed a TQSS scheme based on single particle by using Shamir's secret splitting technique, in which the Hash function is used to guarantee the security of particle transmission.

(7) In 2017, Song[42] proposed a TQSS scheme sharing a d-dimensional classical secret based on quantum Fourier transformation (QFT) and a d-level GHZ state by using Shamir's secret splitting technique. However, Kao[43] points out a calculation problem in Song's paper, which indicates that the agents are unable to obtain the boss's secret information. But, they have not suggested any improvement of the scheme in Ref.[42] to mitigate this loophole. To mitigate the loophole, Roy[44] has recently proposed a TQSS scheme sharing a d-level classical message based on a d-dimensional multi-particle entangled state by using QFT and classical secret splitting technique.

(8) In 2019, Bai[45] proposed a quantum secret sharing scheme using a set of orthogonal generalized Bell states in $C^4 \bigotimes C^4$ and local distinguishability. In their proposed protocol the participants use one-way loop classical communication and local projective measurements to distinguish between the orthogonal states. And combined with the classical Shamir (t, n)-threshold scheme, a (t, n)-threshold quantum scheme was presented.

It is worth pointing out that TQSS schemes based on classical secret splitting technique are easy to understand, but they are not purely quantum and they are complex in calculating the shares.

In 2015, Rahaman[14] presented a novel restricted $(2, n)$-threshold LOCC-QSS scheme, in which any two cooperating players, one from each of two disjoint groups of players, can always reconstruct the secret based on the local distinguishability of n-qubit GHZ states. So far, based on the local distinguishability of multiparty entangled states, a great deal of threshold LOCC-QSS schemes have been found successively and summarized below:

(1) In 2015, Yang[46] presented a standard $(2, n)$-threshold LOCC-QSS scheme, in which any two players can collaboratively recover the secret, using some pairs of locally distinguishable orthogonal d-level multipartite entangled states to represent the encoded secret.

(2) In 2017, Bai[28] proposed a standard $(2, n)$-threshold LOCC-QSS scheme and a restricted $(2, n)$-threshold LOCC-QSS scheme based on the local distinguishability of an orthogonal pair of n-qudit GHZ states.

(3) In 2017, using the discriminability of two orthogonal d-level GHZ states under LOCC, Bai[47] proposed multiple QSS schemes to realize three types of access structures, i.e., the (n, n)-threshold, the restricted $(3, n)$-threshold and restricted $(4, n)$-threshold.

(4) In 2017, Wang[48] proposed the concept of judgment space to investigate the quantum secret sharing scheme based on local distinguishability, and developed a standard (3, 4)-threshold LOCC-QSS scheme and a standard (5, 6)-threshold LOCC-QSS scheme with three orthogonal 4-qudit (4-level) entangled states and three orthogonal 6-qudit (6-level) entangled states, respectively. Furthermore, Liu[49] proposed a standard (6, 7)-threshold LOCC-QSS scheme with five orthogonal 7-qudit (7-level).

(5) In 2020, Dou[50] followed the work of Wang[48] and investigate the judgement space deeply. The digital representation and graphical representation of judgement space were given, and an algorithm was designed to search optional states for any given k and n.

(6) In 2018, Bai[51] constructed a group of orthogonal multipartite entangled states in d-dimensional system and investigated the distinguishability of these entangled states under restricted local operations and classical communications, and proposed a restricted (5, n)-threshold quantum secret sharing scheme and a restricted (5, 8)-threshold quantum secret sharing scheme as an example based on these properties.

It is worth pointing out that, in the TQSS schemes based on the local distinguishability of multiple orthogonal entangled quantum states, we need to use high-dimensional quantum systems, namely qudit states instead of qubits.

From above, it is known that complicated entangled qudit states or classical secret splitting technique is required in the existing standard TQSS schemes. However, TQSS schemes that are based on qubit system and do not require classical secret splitting technique are easier to implement. So, we study this question and propose a novel standard TQSS scheme sharing classical secret, in which the maximally entanged 6-qubit state (for convenience, called it BPB state) discovered by Borras[52] is used as channel and no classical secret splitting technique is required.

The remainder of this paper is organized as follows. Firstly, some singular properties of the BPB state will be described, and a standard (3, 5)-TQSS protocol sharing classical messages by the BPB states is presented. Then, the security of the protocol is analyzed. Finally, we conclude with a summary.

Standard (3, 5)-threshold quantum secret sharing

In this section, a standard (3, 5)-threshold quantum secret sharing scheme based on the BPB states is presented. In our protocol, we adopt the data block transmission technique[53] and the decoy photon technique[24,54–56] to assure the security of the transmission. First some key properties of the BPB state are developed, then a standard (3, 5)-threshold quantum secret sharing scheme is constructed by using the singular properties of the BPB state and Bell states, and finally the security analysis of the proposed protocol is presented.

The properties of the BPB state. The BPB state discovered by Borras is in the following form:

$$\begin{aligned}\frac{1}{\sqrt{32}}\Bigg[\bigg(&|000000\rangle+|111111\rangle+|000011\rangle+|111100\rangle\\&+|000101\rangle+|111010\rangle+|000110\rangle+|111001\rangle\\&+|001001\rangle+|110110\rangle+|001111\rangle+|110000\rangle\\&+|010001\rangle+|101110\rangle+|010010\rangle+|101101\rangle\\&+|011000\rangle+|100111\rangle+|011101\rangle+|100010\rangle\bigg)\\&-\bigg(|010100\rangle+|101011\rangle+|010111\rangle+|101000\rangle\\&+|011011\rangle+|100100\rangle+|001010\rangle+|110101\rangle\\&+|001100\rangle+|110011\rangle+|011110\rangle+|100001\rangle\bigg)\Bigg]_{123456}.\end{aligned} \tag{2}$$

Hereafter, subscripts $\{1, 2, 3, 4, 5, 6\}$ represent the serial number of particles.

Now, let us rewrite the 6-qubit entangled state in the following form of generalized Schmidt decomposition of three-partite split (12|36|45):

$$\begin{aligned}1/2\bigg(&|\phi^+\rangle_{12}|\phi^+\rangle_{36}|\phi^+\rangle_{45}+|\phi^-\rangle_{12}|\psi^-\rangle_{36}|\psi^+\rangle_{45}\\&+|\psi^-\rangle_{12}|\psi^+\rangle_{36}|\phi^-\rangle_{45}+|\psi^+\rangle_{12}|\phi^-\rangle_{36}|\psi^-\rangle_{45}\bigg).\end{aligned} \tag{3}$$

By formula (3), we have:

$$\rho_1 = \rho_2 = \rho_3 = \rho_4 = \rho_5 = \rho_6 = \frac{1}{2}I_2, \tag{4}$$

$$\rho_{12} = \rho_{36} = \rho_{45} = \frac{1}{4}I_4, \tag{5}$$

$$
\begin{aligned}
\rho_{123} = &\rho_{124} = \rho_{125} = \rho_{126} = \frac{1}{8} I_8, \\
\rho_{361} = &\rho_{362} = \rho_{364} = \rho_{365} = \frac{1}{8} I_8, \\
\rho_{451} = &\rho_{452} = \rho_{453} = \rho_{456} = \frac{1}{8} I_8.
\end{aligned}
\tag{6}
$$

Hereafter, ρ_i, ρ_{ij} and ρ_{ijk} represent reduced density operators of particles $\{i\}$, $\{i,j\}$ and $\{i,j,k\}$, respectively, and I_2, I_4 and I_8 represent the identity density operators on two-dimensional Hilbert space H_2, four-dimensional Hilbert space $H_2^{\otimes 2}$ and eight-dimensional Hilbert space $H_2^{\otimes 3}$, respectively.

Similarly, we can reformulate $|\Psi\rangle_{6qb}$ in the forms of generalized Schmidt decomposition of three-partite split (13|24|56),(14|26|35),(15|23|46) and (16|25|34), respectively as follows:

$$
\begin{aligned}
1/2\bigg(&-|\phi^-\rangle_{13}|\phi^-\rangle_{24}|\phi^+\rangle_{56} + |\phi^+\rangle_{13}|\psi^+\rangle_{24}|\psi^+\rangle_{56} \\
&- |\psi^+\rangle_{13}|\psi^-\rangle_{24}|\phi^-\rangle_{56} - |\psi^-\rangle_{13}|\phi^+\rangle_{24}|\psi^-\rangle_{56}\bigg),
\end{aligned}
\tag{7}
$$

$$
\begin{aligned}
1/2\bigg(&|\phi^-\rangle_{14}|\phi^+\rangle_{26}|\phi^-\rangle_{35} + |\phi^+\rangle_{14}|\psi^+\rangle_{26}|\psi^+\rangle_{35} \\
&+ |\psi^-\rangle_{14}|\psi^-\rangle_{26}|\phi^+\rangle_{35} + |\psi^+\rangle_{14}|\phi^-\rangle_{26}|\psi^-\rangle_{35}\bigg),
\end{aligned}
\tag{8}
$$

$$
\begin{aligned}
1/2\bigg(&|\phi^+\rangle_{15}|\phi^+\rangle_{23}|\phi^+\rangle_{46} + |\phi^-\rangle_{15}|\psi^+\rangle_{23}|\psi^-\rangle_{46} \\
&+ |\psi^+\rangle_{15}|\psi^-\rangle_{23}|\phi^-\rangle_{46} + |\psi^-\rangle_{15}|\phi^-\rangle_{23}|\psi^+\rangle_{46}\bigg),
\end{aligned}
\tag{9}
$$

$$
\begin{aligned}
1/2\bigg(&|\phi^-\rangle_{16}|\phi^+\rangle_{25}|\phi^-\rangle_{34} + |\phi^+\rangle_{16}|\psi^-\rangle_{25}|\psi^-\rangle_{34} \\
&+ |\psi^+\rangle_{16}|\psi^+\rangle_{25}|\phi^+\rangle_{34} + |\psi^-\rangle_{16}|\phi^-\rangle_{25}|\psi^+\rangle_{34}\bigg).
\end{aligned}
\tag{10}
$$

In the same way, by formulas (7)–(10), we have:

$$
\begin{aligned}
\rho_{13} &= \rho_{24} = \rho_{56} = \frac{1}{4} I_4, \\
\rho_{14} &= \rho_{26} = \rho_{35} = \frac{1}{4} I_4, \\
\rho_{15} &= \rho_{23} = \rho_{46} = \frac{1}{4} I_4, \\
\rho_{16} &= \rho_{25} = \rho_{34} = \frac{1}{4} I_4,
\end{aligned}
\tag{11}
$$

$$
\begin{aligned}
\rho_{134} &= \rho_{135} = \rho_{146} = \rho_{156} = \frac{1}{8} I_8, \\
\rho_{234} &= \rho_{235} = \rho_{246} = \rho_{256} = \frac{1}{8} I_8.
\end{aligned}
\tag{12}
$$

According to formula (4), it is known that there is 1 ebit of entanglement between any one particle and the other particles. Similarly, we have, there exists 2 ebits of entanglement between any splits of $(2 - particles|4 - particles)$ by formulas (5) and (11), and 3 ebits of entanglement between any splits of $(3 - particles|3 - particles)$ by formulas (6) and (12).

From formulas (3) and (7)–(10), it is known that the other four particles will collapsed to tensor product of two pairs of EPR when we measure the BPB state on any two qubits $\{i,j\}$ with the Bell states basis $\{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$. For example, suppose that the result of measurement on particles 1 and 2 is $|\phi^+\rangle$, then the other four particles will collapse to $|\phi^+\rangle_{36}|\phi^+\rangle_{45}$ (see Table 1).

It is necessary to point out the form and properties of the Bell states. There are four orthogonal Bell states as follows:

i, j	Measure results on particles i, j	Corresponding states of the other four particles	i, j	Measure results on particles i, j	Corresponding states of the other four particles
1,2	$\|\phi^+\rangle$	$\|\phi^+\rangle_{36}\|\phi^+\rangle_{45}$	1,2	$\|\psi^+\rangle$	$\|\phi^-\rangle_{36}\|\psi^-\rangle_{45}$
1,2	$\|\phi^-\rangle$	$\|\psi^-\rangle_{36}\|\psi^+\rangle_{45}$	1,2	$\|\psi^-\rangle$	$\|\psi^+\rangle_{36}\|\phi^-\rangle_{45}$
1,3	$\|\phi^+\rangle$	$\|\psi^+\rangle_{24}\|\psi^+\rangle_{56}$	1,3	$\|\psi^+\rangle$	$\|\psi^-\rangle_{24}\|\phi^-\rangle_{56}$
1,3	$\|\phi^-\rangle$	$\|\phi^-\rangle_{24}\|\phi^+\rangle_{56}$	1,3	$\|\psi^-\rangle$	$\|\phi^+\rangle_{24}\|\psi^-\rangle_{56}$
1,4	$\|\phi^+\rangle$	$\|\psi^+\rangle_{26}\|\psi^+\rangle_{35}$	1,4	$\|\psi^+\rangle$	$\|\phi^-\rangle_{26}\|\psi^-\rangle_{35}$
1,4	$\|\phi^-\rangle$	$\|\phi^+\rangle_{26}\|\phi^-\rangle_{35}$	1,4	$\|\psi^-\rangle$	$\|\psi^-\rangle_{26}\|\phi^+\rangle_{35}$
1,5	$\|\phi^+\rangle$	$\|\phi^+\rangle_{23}\|\phi^+\rangle_{46}$	1,5	$\|\psi^+\rangle$	$\|\psi^-\rangle_{23}\|\phi^-\rangle_{46}$
1,5	$\|\phi^-\rangle$	$\|\psi^+\rangle_{23}\|\psi^-\rangle_{46}$	1,5	$\|\psi^-\rangle$	$\|\phi^-\rangle_{23}\|\psi^+\rangle_{46}$
1,6	$\|\phi^+\rangle$	$\|\psi^-\rangle_{25}\|\psi^-\rangle_{34}$	1,6	$\|\psi^+\rangle$	$\|\psi^+\rangle_{25}\|\phi^+\rangle_{34}$
1,6	$\|\phi^-\rangle$	$\|\phi^+\rangle_{25}\|\phi^-\rangle_{34}$	1,6	$\|\psi^-\rangle$	$\|\phi^-\rangle_{25}\|\psi^+\rangle_{34}$

Table 1. The other four qubits will collapse to tensor product of two pairs of EPR when we measure the BPB state on any two qubits i, j (for example, i=1) with the Bell basis.

	Bell state $\|\phi^+\rangle$	Bell state $\|\phi^-\rangle$	Bell state $\|\psi^+\rangle$	Bell state $\|\psi^-\rangle$
$I \otimes I$	$\|\phi^+\rangle$	$\|\phi^-\rangle$	$\|\psi^+\rangle$	$\|\psi^-\rangle$
$I \otimes \sigma_x$ or $\sigma_x \otimes I$	$\|\psi^+\rangle$	$\|\psi^-\rangle$	$\|\phi^+\rangle$	$\|\phi^-\rangle$
$I \otimes \sigma_y$ or $\sigma_y \otimes I$	$\|\psi^-\rangle$	$\|\psi^+\rangle$	$\|\phi^-\rangle$	$\|\phi^+\rangle$
$I \otimes \sigma_z$ or $\sigma_z \otimes I$	$\|\phi^-\rangle$	$\|\phi^+\rangle$	$\|\psi^-\rangle$	$\|\psi^+\rangle$

Table 2. An arbitrary Bell state will transform to another Bell state if a Pauli operator is applied on any one of its particles.

$$\begin{aligned}
|\phi^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle) \\
|\phi^-\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = \frac{1}{\sqrt{2}}(|+-\rangle + |-+\rangle) \\
|\psi^+\rangle &= \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) = \frac{1}{\sqrt{2}}(|++\rangle - |--\rangle) \\
|\psi^-\rangle &= \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle) = \frac{1}{\sqrt{2}}(|+-\rangle - |-+\rangle)
\end{aligned} \tag{13}$$

Here, $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. It is known to all that, for any Bell state, if we apply a local unitary operator from $\{\sigma_x, \sigma_y, \sigma_z\}$ on any particle of the Bell state, then it will be transformed into another orthogonal Bell state (see Table 2). That is to say, $|\phi^+\rangle$ ($|\psi^-\rangle$) will be transformed into $|\psi^-\rangle$ ($|\phi^+\rangle$) if we apply a unitary operation $I \otimes \sigma_y$ or $\sigma_y \otimes I$ to it. From formula (13), we have that the two Bell states $\{|\phi^+\rangle, |\psi^-\rangle\}$ can be distinguished by local measure with basis $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$, so can the two Bell states $\{|\phi^-\rangle, |\psi^+\rangle\}$. For example, for given two Bell states $|\phi^+\rangle$ and $|\psi^-\rangle$, if the result of measurement is $|0\rangle|0\rangle$ ($|+\rangle|+\rangle$) or $|1\rangle|1\rangle$ ($|-\rangle|-\rangle$), then we can conclude that the Bell state is $|\phi^+\rangle$.

Standard (3, 5)-threshold quantum secret sharing scheme of classical message.

Now, let us construct the standard (3, 5)-threshold quantum secret sharing scheme based on the BPB state by the correlations of the measurement results on it and local distinguishability of Bell states. Our scheme is divided into four phases: preparing phase, checking phase, coding phase and decoding phase.

(1) Phase for preparing BPB states and inserting decoy photons. In this step, the dealer Alice prepares N BPB states indexed from 1 to N. All particles numbered $i(1 \leq i \leq 6)$ in the BPB states constitute a particle sequence S_i with length N. Then, Alice prepares randomly a different sequence, $r_i = \Pi_i(1, 2, \ldots, N)$, for each user Bob_i. Here, $\Pi_i(1, 2, \ldots, N)$ represents an arbitrary permutation of the sequence $(1, 2, \ldots, N)$. Now, for each particle sequence $S_i(i = 1, 2, \ldots, 6)$, Alice exchanges the order of particles in it to make a new sequence $S_i^{'}$ according to the permutation sequence r_i. In order to detect eavesdropping, for each particle sequence S_i, Alice prepares some decoy particles, which are randomly in the states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, and randomly inserts these decoy particles into the sequence $S_i^{'}(1 \leq i \leq 6)$ to make a new sequence $S_i^{''}(1 \leq i \leq 6)$ with length $N^{'}$. Finally, She keeps a record of the position and the initial state of each decoy particle, and sends the $i - th(i(1 \leq i \leq 6))$ sequence $S_i^{''}$ to the $i - th$ agent Bob_i who saves these particles in quantum register to be used in the future. After receiving all the $N^{'}$ particles, $\text{Bob}_i(1 \leq i \leq 6)$ announces the fact.

Measurement results with Bell basis by *Bob*$_2$ and *Bob*$_4$	**Measurement results with $Z(X)$ basis by *Bob*$_3$**	**Measurement results with $Z(X)$ basis by *Bob*$_1$**	**Operators for encoding**	**Secrets to be recovered**
$\lvert\phi^+\rangle$	$\lvert 0\rangle(\lvert +\rangle)$	$\lvert 1\rangle(\lvert -\rangle)$	I	0
$\lvert\phi^+\rangle$	$\lvert 1\rangle(\lvert -\rangle)$	$\lvert 0\rangle(\lvert +\rangle)$	I	0
$\lvert\phi^+\rangle$	$\lvert 0\rangle(\lvert +\rangle)$	$\lvert 0\rangle(\lvert +\rangle)$	σ_y	1
$\lvert\phi^+\rangle$	$\lvert 1\rangle(\lvert -\rangle)$	$\lvert 1\rangle(\lvert -\rangle)$	σ_y	1
$\lvert\phi^-\rangle$	$\lvert 0\rangle(\lvert +\rangle)$	$\lvert 0\rangle(\lvert -\rangle)$	I	0
$\lvert\phi^-\rangle$	$\lvert 1\rangle(\lvert -\rangle)$	$\lvert 1\rangle(\lvert +\rangle)$	I	0
$\lvert\phi^-\rangle$	$\lvert 0\rangle(\lvert +\rangle)$	$\lvert 1\rangle(\lvert +\rangle)$	σ_y	1
$\lvert\phi^-\rangle$	$\lvert 1\rangle(\lvert -\rangle)$	$\lvert 0\rangle(\lvert -\rangle)$	σ_y	1
$\lvert\psi^+\rangle$	$\lvert 0\rangle(\lvert +\rangle)$	$\lvert 0\rangle(\lvert +\rangle)$	I	0
$\lvert\psi^+\rangle$	$\lvert 1\rangle(\lvert -\rangle)$	$\lvert 1\rangle(\lvert -\rangle)$	I	0
$\lvert\psi^+\rangle$	$\lvert 0\rangle(\lvert +\rangle)$	$\lvert 1\rangle(\lvert -\rangle)$	σ_y	1
$\lvert\psi^+\rangle$	$\lvert 1\rangle(\lvert -\rangle)$	$\lvert 0\rangle(\lvert +\rangle)$	σ_y	1
$\lvert\psi^-\rangle$	$\lvert 0\rangle(\lvert +\rangle)$	$\lvert 1\rangle(\lvert +\rangle)$	I	0
$\lvert\psi^-\rangle$	$\lvert 1\rangle(\lvert -\rangle)$	$\lvert 0\rangle(\lvert -\rangle)$	I	0
$\lvert\psi^-\rangle$	$\lvert 0\rangle(\lvert +\rangle)$	$\lvert 0\rangle(\lvert -\rangle)$	σ_y	1
$\lvert\psi^-\rangle$	$\lvert 1\rangle(\lvert -\rangle)$	$\lvert 1\rangle(\lvert +\rangle)$	σ_y	1

Table 3. *Bob*$_2$,*Bob*$_3$ and *Bob*$_4$ can unite to recover the secret shared by *Bob*$_1$ through combining the $Z(X)$ basis measurement by *Bob*$_1$, the $Z(X)$ basis measurement by *Bob*$_3$ and the joint measurements by *Bob*$_2$ and *Bob*$_4$.

(2) Phase for checking eavesdropping by decoy photons. After confirming that Bob$_i$ $(1 \leq i \leq 6)$ has received the sequence S_i'', Alice publicly announces the position of the decoy particles via classical channel and asks Bob$_i$$(1 \leq i \leq 6)$ to measure these particles with the basis $\{\lvert 0\rangle, \lvert 1\rangle\}$ or $\{\lvert +\rangle, \lvert -\rangle\}$ chosen randomly. Bob$_i$$(1 \leq i \leq 6)$ publishes his measurement base and results. For the decoy particles measured with correct base, Alice can compute the error rate by comparing the measurement results to the initial states. If the error rate exceeds the predefined threshold value, Alice aborts the process and starts a new one because quantum communication between Alice and the agents may be attacked. Otherwise, they continue the protocol.

(3) Phase for sharing secret. After Alice has distributed N BPB states to Bob$_i$ $(1 \leq i \leq 6)$ in security, she informs each Bob$_i$$(1 \leq i \leq 6)$ of the order of the particles sent to him, respectively, i.e., the permutation $\Pi_i(1, 2, \ldots, N)$. Then Bob$_i$ reorders his particles by the permutation. Now, any one user from { Bob$_1$,Bob$_2$,Bob$_3$,Bob$_4$,Bob$_5$,Bob$_6$} can share N bits of message among the other five users using the N BPB states. That is to say, each BPB state can be used to share one bit. Suppose Bob$_k$ $(1 \leq k \leq 6)$ wants to share N bits $\{b_0 b_1 \cdots b_N\}$ among the other five users. Now, Bob$_k$ performs an appropriate unitary operation U_j on the $j - th$ particle to encode the secret b_j. Here, U_j satisfy:

$$U_j = \begin{cases} I, & b_j = 0 \\ \sigma_y, & b_j = 1 \end{cases}$$

Then, *Bob*$_k$ measures each of his own particles with basis $\{\lvert 0\rangle, \lvert 1\rangle\}$ or $\{\lvert +\rangle, \lvert -\rangle\}$ randomly, respectively. Finally, *Bob*$_k$ publishes the measurements through classical channel.

(4) Phase for recovering the secret messages. After *Bob*$_k$ has shared secret messages, any three of the other five users can work together to recover the secrets to be shared. Let's give an example to illustrate it. Suppose *Bob*$_1$ has shared his secrets by the procedure above. Now, any three users from $\{Bob_j \mid 2 \leq j \leq 6\}$ can unite to disclose the secrets by the following method:

Two users can make joint measurements on their particles in the same BPB state with Bell basis, and the third user makes local measurement with the same basis as *Bob*$_1$. Now, By combining their own measurements with *Bob*$_1$'s measurements, they can obtain the secrets. For an instance (see Table 3), suppose that *Bob*$_2$, *Bob*$_3$ and *Bob*$_4$ want to recover the secret shared by *Bob*$_1$, then *Bob*$_2$ and *Bob*$_4$ can unite to make Bell measurement, and *Bob*$_3$ can make local measurement using the same basis as *Bob*$_1$. Further, suppose that the joint measurement result from *Bob*$_2$ and *Bob*$_4$ is $\lvert\phi^+\rangle$, and the results from *Bob*$_3$ and *Bob*$_1$ are $\lvert +\rangle$ and $\lvert +\rangle$, respectively, then we can infer that the secret is 1. It is worth pointing out, to fulfil the task, only specific two users(e.g., *Bob*$_2$ and *Bob*$_4$ in the example above), instead of any two users, can be chosen to unite to make measurement with Bell basis. By formulas (3) and (7)–(10), we can know which two of the three users need to make joint measurement with Bell basis, and which one needs to make local measurement in order to recover the secrets (see Table 4).

Participating players	Players to make unite measurement	Player to make local measurement
Bob_2, Bob_3, Bob_4	Bob_2, Bob_4	Bob_3
Bob_2, Bob_3, Bob_5	Bob_2, Bob_3	Bob_5
Bob_2, Bob_3, Bob_6	Bob_3, Bob_6	Bob_2
Bob_2, Bob_4, Bob_5	Bob_4, Bob_5	Bob_2
Bob_2, Bob_4, Bob_6	Bob_2, Bob_6	Bob_4
Bob_2, Bob_5, Bob_6	Bob_2, Bob_5	Bob_6
Bob_3, Bob_4, Bob_5	Bob_3, Bob_5	Bob_4
Bob_3, Bob_4, Bob_6	Bob_3, Bob_4	Bob_6
Bob_3, Bob_5, Bob_6	Bob_5, Bob_6	Bob_3
Bob_4, Bob_5, Bob_6	Bob_4, Bob_6	Bob_5

Table 4. Any three users from $\{Bob_2, Bob_3, Bob_4, Bob_5, Bob_6\}$ can unite to recover the secret shared by Bob1 through choosing two users to make Bell measurement and the third to make local measurement.

	The first class	The second class	The third class	Our scheme
Represntative	Cleve[33]	Tokunaga[35]	Yang[46]	Our scheme
Existing protocols	[33,34]	[35,38–42,44,45]	[46,48–50]	Our scheme
Main princple	Based on quantum error correction coding	Based on classical secret splitting techique and QKD	Based on local distinguishability of specific d-level entangled states	Based on singular propertites of the maximally qubit entangled states
Quantum channels	d-Level entangled state	Single particle qubit or qudit entangled state	Specfic d-level entangled state	The maximally entangled 6-qubit state
Quantum computation	Unitary operations on multi-particles	Unitary operation on single particle, e.g. σ_x, QFT, etc	Local projective measurements	Measurements with $X(Z)$ basis or Bell basis
Classical computation	No need	Need	No need	No need

Table 5. A brief comparison of the various existing standard TQSS schemes sharing classical information (for convenience, we divide them into three classes) with our scheme.

Security analysis of the presented TQSS protocols

In this section, we'll discuss how this protocol can prevent a dishonest Bob or a third eavesdropper Eve from acquiring the secret without being detected. In general, there are usual two types of attack method from attackers, i.e., intercept and resend attack, and entanglement attack.

In our protocol, the decoy photons widely adopted in quantum secret sharing are used to check eavesdropping[39–41]. Consequently, when eavesdropper Eve intends to excute intercept-and-resend attack and tries to obtain the transmitted message, he can only intercept the quantum sequence but can not acquire the sequence states, and thus fails to resend a perfect copy of the sequence due to Heisenberg uncertainty principle and quantum no-cloning principle. Because Eve does not know the positions and states of the decoy photons, the attack will cause an increase in error rate to about 1/2 and thus be detected. On the other hand, If Eve possesses several agents' particles, he might attack successfully by making union measurement on his particles with Bell basis. However, since Eve can not distinguish which particles contribute to the same BPB state in the preparing phase, his measure must bring error rate of 1/2 in checking phase.

By the same analysis as Jiang[24] and Wang[56], entangle-and-measure attack will cause error and be detected in checking step due to the decoy photons. In other words, if Eve wanted to get some useful information by entangling the attached particles, he will inevitably introduce interference, which will be found by the participants in the eavesdropping detection.

Conclusion

We have presented a standard (3, 5)-threshold quantum secret sharing protocol by genuinely maximally entangled 6-qubit states, i.e., BPB states. In our protocol, six users $\{Bob_1, Bob_2, Bob_3, Bob_4, Bob_5, Bob_6\}$ a priori share a series of BPB states, of which Bob_i owns the $i-th$ particle of each BPB state. A BPB state can be reformulated as generalized Schimdt decomposition of any split $(ij|kl|mn)(1 \leq i \neq j \neq k \neq l \neq m \neq n \leq 6)$, and the results of measurement on partial particles of the BPB state are correlative. Based on these singular properties, any three users except Bob_i can recover the secret shared by Bob_i. In fact, after preparing step, any one of the six users can share secret, and any three from the other five users can unite to recover the secret. The presented protocol is secure against eavesdropping by inserting the decoy photons into the distributed particle sequences.

A brief comparison of the various existing TQSS schemes sharing classical secrets with our scheme is summarized in Table 5. In summary, our protocol has the advantage that, it uses qubit entangled state instead of d-level entangled state as channel, in addtion it doesn't need to utilize Shamir's classical threshold scheme to produce secret shares. Therefore, our method is more simple and feasible.

Received: 8 August 2021; Accepted: 2 November 2021
Published online: 22 November 2021

References

1. Shamir, A. How to share a secret. *Commun. ACM* **22**(11), 612–613 (1979).
2. Blakley, G. R. Safeguarding cryptographic keys. In *AFIPS* 313. (IEEE Computer Society, 1979).
3. Hillery, M., Bužek, V. & Berthiaume, A. Quantum secret sharing. *Phys. Rev. A* **59**, 1829 (1999).
4. Karlsson, A., Koashi, M. & Imoto, N. Quantum entanglement for secret sharing and secret splitting. *Phys. Rev. A* **59**, 162 (1999).
5. Guo, G. P. & Guo, G. C. Quantum secret sharing without entanglement. *Phys. Lett. A* **310**, 247–251 (2003).
6. Zhang, Z. J., Li, Y. & Man, Z. X. Multiparty quantum secret sharing. *Phys. Rev. A* **71**(4), 044301 (2005).
7. Han, L. F., Liu, Y. M., Liu, J. & Zhang, Z. J. Multiparty quantum secret sharing of secure direct communication using single photons. *Opt. Commun.* **281**, 2690–2694 (2008).
8. Yan, F. L., Gao, T. & Li, Y. C. Quantum secret sharing protocol between multiparty and multiparty with single photons and unitary transformations. *Chin. Phys. Lett.* **025**(004), 1187–1190 (2008).
9. Tavakoli, A. *et al.* Secret sharing with a single d-level quantum system. *Phys. Rev. A* **92**, 030302(R) (2015).
10. Hao, N. *et al.* A new quantum secret sharing scheme based on mutually unbiased bases. *Int. J. Theor. Phys.* **58**(3), 1249–1261 (2019).
11. Xiao, L. *et al.* Efficient multiparty quantum secret sharing schemes. *Phys. Rev. A* **69**, 052307 (2004).
12. Deng, F. G. *et al.* Efficient multiparty quantum secret sharing with Greenberger–Horne–Zeilinger states. *Chin. Phys. Lett.* **23**(5), 1084–1087 (2006).
13. Zhang, Z. J. & Man, Z. X. Multiparty quantum secret sharing of classical messages based on entanglement swapping. *Phys. Rev. A* **72**, 022303 (2005).
14. Rahaman, R. & Parker, M. G. Quantum scheme for secret sharing based on local distinguishabality. *Phys. Rev. A* **91**, 022330 (2015).
15. Hsieh, C. R., Tasi, C. W. & Hwang, T. Quantum secret sharing using GHZ like state. *Commun. Theor. Phys.* **54**, 1019–1022 (2010).
16. Massoud, H. D. & Elham, F. A novel and efficient multiparty quantum secret sharing scheme using entangled states. *Sci. China-Phys. Mech. Astron.* **55**(10), 1828–1831 (2012).
17. Zhang, Z. J. Multiparty quantum secret sharing of secure direct communication. *Phys. Lett. A* **342**, 60–66 (2005).
18. Abulkasim, H. *et al.* Authenticated quantum secret sharing with quantum dialogue based on Bell states. *Phys. Scr.* **91**(8), 085101 (2016).
19. Shi, R. H. *et al.* Multiparty quantum secret sharing with Bell states and Bell measurements. *Opt. Commun.* **283**(11), 2476–2480 (2010).
20. Shi, R. H. *et al.* Quantum secret sharing between multiparty and multiparty with Bell states and Bell measurements. *Sci. China-Phys. Mech. Astron.* **53**, 2238–2244 (2010).
21. Tan, X. & Jiang, L. Improved three-party quantum secret sharing based on Bell states. *Int. J. Theor. Phys.* **52**(10), 3577–3585 (2013).
22. Liu, Z. *et al.* Quantum simultaneous secret distribution with dense coding by using cluster states. *Quant. Inf. Process.* **12**(12), 3745–3759 (2013).
23. Long, Y. X., Qiu, D. W. & Long, D. Y. Quantum secret sharing of multi-bits by an entangled six-qubit state. *J. Phys. A* **45**(19), 195303 (2012).
24. Jiang, S. *et al.* Efficient verifiable quantum secret sharing schemes via eight-quantum-entangled states. *Int. J. Theor. Phys.* **60**(5), 1757–1766 (2021).
25. Markham, D. & Sanders, B. C. Graph states for quantum secret sharing. *Phys. Rev. A* **78**(4), 042309 (2008).
26. Chen, X. B. *et al.* A kind of universal quantum secret sharing protocol. *Sci. Rep.* **7**, 39845 (2017).
27. Yu, I. C., Lin, F. L. & Huang, C. Y. Quantum secret sharing with multilevel mutually (un)biased bases. *Phys. Rev. A* **78**(1), 012344 (2008).
28. Bai, C. M., Li, Z. H., Xu, T. T. & Li, Y. M. Quantum secret sharing using the d-dimensional GHZ state. *Quant. Inf. Process.* **16**, 59 (2017).
29. Zhang, K. J. *et al.* A new n-party quantum secret sharing model based on multiparty entangled states. *Quant. Inf. Process.* **18**(3), 81 (2019).
30. Yang, W. *et al.* Secret sharing based on quantum Fourier transform. *Quant. Inf. Process.* **12**(7), 2465–2474 (2013).
31. Mansour, M. & Dahbi, Z. Quantum secret sharing protocol using maximally entangled multi-qudit states. *Int. J. Theor. Phys.* **59**(12), 3876–3887 (2020).
32. Hu, W. W. *et al.* A novel dynamic quantum secret sharing in high-dimensional quantum system. *Quant. Inf. Process.* **20**, 159 (2021).
33. Cleve, R., Gottesman, D. & Lo, H. K. How to share a quantum secret. *Phys. Rev. Lett.* **83**, 648 (1999).
34. Gheorghiu, V. & Sanders, B. C. Accessing quantum secrets via local operations and classical communication. *Phys. Rev. A* **88**(2), 022340 (2013).
35. Tokunaga, Y., Okamoto, T. & Imoto, N. Threshold quantum cryptography. *Phys. Rev. A* **71**(1), 012314 (2005).
36. Yang, Y. G. & Wen, Q. Y. Threshold quantum secret sharing between multi-party and multi-party. *Sci. China Ser. G Phys. Mech. Astron.* **51**(9), 1308–1315 (2008).
37. Li, B. K., Yang, Y. G. & Wen, Q. Y. Threshold quantum secret sharing of secure direct communication. *Chin. Phys. Lett.* **26**(1), 010302 (2009).
38. Massoud, H. D. & Elham, F. Threshold quantum secret sharing between multiparty and multiparty using Greenberger–CHorne–CZeilinger state. *Quant. Inf. Process.* **12**(2), 1299–1306 (2013).
39. Qin, H., Zhu, X. & Dai, Y. (t, n) Threshold quantum secret sharing using the phase shift operation. *Quant. Inf. Process.* **14**(8), 2997 (2015).
40. Lu, C. *et al.* Threshold quantum secret sharing based on single qubit. *Quant. Inf. Process.* **17**(3), 64 (2018).
41. Qin, H. & Dai, Y. An efficient (t, n) threshold quantum secret sharing without entanglement. *Mod. Phys. Lett. B* **30**(12), 1650138 (2016).
42. Song, X. L. *et al.*(t, n) Threshold d-level quantum secret sharing. *Sci. Rep.* **7**, 6366 (2017).
43. Kao, S. H. & Hwang, T. Comment on "(t, n) Threshold d-level Quantum Secret Sharing". quant-ph/1803.00216 (2018).
44. Roy, S. & Mukhopadhyay, S. (t, n) Threshold d-level quantum secret sharing based on quantum Fourier transformation. *Quant. Inf. Comput.* **20**(11 & 12), 957–968 (2020).
45. Bai, C. M., Zhang, S. J. & Liu, L. (t, n)-Threshold quantum secret sharing based on one-way local distinguishability. *IEEE Access.* **7**, 147256–147265 (2019).
46. Yang, Y. H. *et al.* Quantum secret sharing via local operations and classical communication. *Sci. Rep.* **5**, 16967 (2015).
47. Bai, C. M., Li, Z. H., Liu, C. J. & Li, Y. M. Quantum secret sharing using orthogonal multiqudit entangled states. *Quant. Inf. Process.* **16**, 304 (2017).
48. Wang, J. T. *et al.* Quantum-secret-sharing based on local distinguishability of orthogonal multiqudit entangled states. *Phys. Rev. A* **95**, 022330 (2017).
49. Liu, C. J. *et al.* Quantum secret sharing scheme based on local distinguishability of orthogonal seven-qudit entangled states. *Int. J. Theor. Phys.* **57**(3), 428–442 (2017).

50. Dou, Z. *et al.* Searching for optimal quantum secret sharing scheme based on local distinguishability. *Quant. Inf. Process.* **19**(10), 1–19 (2020).
51. Bai, C. M. *et al.* Restricted (k, n)-threshold quantum secret sharing scheme based on local distinguishability of orthogonal multi-qudit entangled states. *Quant. Inf. Process.* **17**(11), 312 (2018).
52. Borras, A. *et al.* Multi-qubit systems: Highly entangled states and entanglement distribution. *J. Phys. A* **40**, 13407 (2007).
53. Long, G. L. & Liu, X. S. Theoretically efficient high-capacity quantum-key-distribution scheme. *Phys. Rev. A* **65**, 032302 (2002).
54. Li, C. Y. *et al.* Secure quantum key distribution network with Bell states and local unitary operations. *Chin. Phys. Lett.* **22**, 1049 (2005).
55. Li, C. Y. *et al.* Efficient quantum cryptography network without entanglement and quantum memory. *Chin. Phys. Lett.* **23**, 2896 (2006).
56. Wang, T. Y. & Cai, X. Q. An efficient quantum secret sharing scheme with decoy states. *Int. J. Mod. Phys. B* **26**(20), 313–317 (2012).

Acknowledgements

This work is funded by the National Natural Science Foundation of China (Nos 61902132, 11647140), the Natural Science Foundation of Guangdong Province of China (Nos 2018A030310147, 2016a030313736), the Guangdong Basic and Applied Basic Research Foundation (No. 2021A1515011985), the Key Projects of Basic Research and Application Basic Research in Ordinary Universities in Guangdong Province (No. 2018GKZDXM009), and the Shenzhen Science and Technology Program (No. JCYJ20190809152003992, JCYJ20210324100813034).

Author contributions

Y.L. wrote the main manuscript text, C.Z. and Z.S. were involved in the analysis and discussion, and all authors reviewed the manuscript.

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to Y.L. or Z.S.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.