Optical and Quantum Electronics (2024) 56:759
https://doi.org/10.1007/s11082-024-06434-3

An efficient controlled semi-quantum secret sharing protocol with entangled state

Monireh Houshmand[1] · Shima Hassanpour[2] · Majid Haghparast[3]

Received: 17 February 2023 / Accepted: 22 January 2024 / Published online: 25 March 2024

Abstract
In this paper, we present an entangled state controlled semi-quantum secret sharing CSQSS protocol for the first time. In this scheme, with the permission of a trusted classical user, Bob_1, Alice, as a quantum user, can share a one-bit specific message with n classical users, and the secret can only be recovered by the cooperation of all classical users. Then, the protocol is extended where m-bit specific messages, $K\,(k_1, k_2, ..., k_m)$, can be shared with n classical users. The security of the proposed protocol against common attacks is analysed in detail, which shows that the proposed protocol is theoretically secure. Compared with previous SQSS protocols, the proposed protocol can achieve a lower cost because it does not use returning qubits for producing the secret message, uses fewer returning qubits for eavesdropping check, and does not perform entangled state measurement. Moreover, the proposed protocol has the highest qubit efficiency among the previous SQSS schemes.

Keywords Semi-quantum secret sharing · Semi-quantum secret sharing · Entangled state · Efficiency

1 Introduction

The Quantum Internet (QI) consists of a quantum network that enables quantum communication between distant quantum devices. Quantum communication provides robust security (Ekert 1991; Sasaki et al. 2014; Yin et al. 2016) within the QI. Unlike classical cryptography, which is based on computational complexity problems, the security of quantum cryptography is based on fundamental laws of quantum mechanics. In 1984, Bennett and Brassard (1984a) proposed the first quantum cryptography protocol. Many interesting and valuable applications have been presented, such as quantum key distribution (QKD) (Li et al. 2008; Zhang et al. 2014; Xu et al. 2020), quantum secure direct communication (QSDC) (Bin et al. 2011; Hassanpour and Houshmand 2015; Zhou et al. 2020), quantum

✉ Monireh Houshmand
m.hooshmand@imamreza.ac.ir

[1] Department of Electrical Engineering, Imam Reza International University, Mashhad, Iran

[2] Chair of Privacy and Network Security, TU Dresden, Dresden, Germany

[3] Faculty of Information Technology, University of Jyväskylä, Jyväskylä, Finland

teleportation (QT) (Saha and Panigrahi 2012; Hassanpour and Houshmand 2016; Yuan and Pan 2020), quantum secret sharing (QSS) (Hillery et al. 1999; Zhang et al. 2005; Markham and Sanders 2008; Yang and Tsai 2020; Liao et al. 2021; Li et al. 2022; Khorrampanah and Houshmand 2022; Khorrampanah et al. 2022), and so on.

Secret sharing is a technique in the field of computation which is proposed by Shamir (1979) and Blakley (1979) in 1979. In the classical secret sharing scheme, some encrypted messages are shared among n parties in such a way that certain subsets of the parties can reconstruct the original secret message from their shares, but parties that are not in the subset cannot reveal any partial information about the secret. Classical secret sharing cannot address the problem of a malicious party, but features of quantum mechanics, such as the no-cloning theorem (Wootters and Zurek 1982) and multiparticle entanglement, prevent the action of a dishonest party. QSS allows a secret to be shared among multiple participants, and the secret can be recovered when all participants collaborate together. A pioneering QSS protocol based on a multi-particle Greenberger–Horne–Zeilinger (GHZ) state was first proposed by Hillery et al. in 1999 Hillery et al. (1999). Following the proposal of this scheme, several QSS protocols have been proposed from different perspectives (Zhang et al. 2005; Markham and Sanders 2008; Yang and Tsai 2020; Liao et al. 2021; Li et al. 2022; Khorrampanah and Houshmand 2022; Khorrampanah et al. 2022). However, while the quantum cryptography protocols have security advantages, their cost is too high due to the need to implement them with quantum resources. Therefore, the concept of semi-quantum cryptography (Boyer et al. 2007) has been promptly introduced to use few quantum resources. In the semi-quantum cryptography protocols, only one participant needs to have full quantum capabilities, and the other participants are classical participants with limited quantum capabilities. Among the semi-quantum cryptographic protocols, semi-quantum secret sharing (SQSS) (Li et al. 2010; Wang et al. 2012; Li et al. 2013; Yang and Hwang 2013; Xie et al. 2015; Yin and Fu 2016; Gao et al. 2017; Yin and Chen 2021) is an important application. SQSS is a fundamental quantum cryptography protocol for the future quantum internet, which promises secure communication.

Li et al. (2010) proposed two novel SQSS protocols with GHZ-like states in 2010. Using Bell states, Wang et al. (2012) presented a SQSS in 2012. Li et al. (2013) proposed a SQSS protocol using two-particle product states in 2013. Then, Yang and Hwang (2013) suggested a novel key construction method to improve the qubit efficiency. Xie et al. (2015) designed a SQSS protocol based on GHZ-like states, where a quantum party can share a specific message with two classical parties instead of a random message. Yin and Fu (2016) proved that Xie et al.'s protocol suffers from a dishonest party attack, and proposed an improvement. Later, Gao et al. (2017) pointed out that Yin and Fu's protocol is not semi-quantum and they presented an improved protocol accordingly.

A semi-quantum secret sharing (SQSS) protocol allowing more than two classical users was presented by Gao et al. (2016) in 2016. Subsequently, Yu et al. (2017) proposed an MSQSS protocol based on n-particle GHZ-like states. Li et al. (2020) proposed an MSQSS scheme using Bell states. Recently, Ye et al. (2021) implemented an MSQSS protocol based on GHZ states and used measured and reflected qubits as the secret keys instead of just the measured qubits.

In this paper, we first proposed a controlled semi-quantum secret sharing (CSQS) protocol in which Alice, as the sender, can share a one-bit specific message with n classical parties $(Bob_i, i = 1, ..., n)$. Bob_1, is also considered a trusted classical user, acts as a controller. CSQS is an extension of the semi-quantum secret sharing protocol. The idea is to allow one party to control the successful completion of the secret sharing process. The property of CSQS can be useful in secure quantum communication networks, where the controller decides when the encrypted secret information should be executed. We then extended the proposed CSQSS protocol, where Alice can share m messages with n classical parties simultaneously. Also, no qubits carrying secret information are transmitted in the quantum channel, and only single state measurement is used to design this protocol.

The rest of the paper is structured as follows. In Sect. 2, the preliminary for this study is presented. Sections 3 and 4 illustrate the proposed CSQSS protocol and the extension, respectively. Then, in Sect. 5, the security of the proposed protocols is analysed. Next, in Sect. 6, the comparison between the proposed CSQSS protocol and other existing SQSS protocols is made. Finally, a conclusion is given in Sect. 7.

2 Preliminary

Before introducing the protocol, it is essential to introduce the basic concepts of quantum computation and information.

2.1 Qubits and unitary operations

A quantum bit (qubit) can be expressed as a linear combination of the two basis states as follows:

$$\begin{aligned} &|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \frac{\alpha+\beta}{\sqrt{2}}|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}|-\rangle, \\ &|\alpha|^2 + |\beta|^2 = 1, \end{aligned} \tag{1}$$

where $|0\rangle, |1\rangle$ and $|+\rangle, |-\rangle$ are eigenvectors of Pauli operators σ_z and σ_x respectively which are defined as Eq. (2).

$$\begin{aligned} I &= |0\rangle\langle 0| + |1\rangle\langle 1|, \\ \sigma_x &= |0\rangle\langle 1| + |1\rangle\langle 0|, \\ i\sigma_y &= |0\rangle\langle 1| - |1\rangle\langle 0|, \\ \sigma_z &= |0\rangle\langle 0| - |1\rangle\langle 1|. \end{aligned} \tag{2}$$

2.2 No-cloning theorem

One of the main differences between classical and quantum communication is no-cloning theorem (Nielsen and Chuang 2002). The no-cloning theorem states that it is not possible to perfectly clone an unknown qubit as a consequence of the laws of quantum mechanics. This theorem is the basis of many quantum cryptography protocols, such as quantum money (Wiesner 1983) and quantum key distribution (Bennett and Brassard 1984a).

2.3 The semi-quantum model

The definition of a semi-quantum implies that one or more parties have only classical abilities. More specifically, on the one hand, a classical party has the following abilities: generating quantum states with the Z basis measurement, measuring quantum states with the Z basis measurement, applying a limited number of unitary operation (only X operation or I operation), reflecting and reordering quantum states. A quantum party, on the other hand, has access to a quantum memory to store a quantum state, generates any arbitrary quantum states and measures in any basis. One of the remarkable aspects of the semi-quantum protocol is the reduction in quantum resource consumption. In the proposed protocols, the $n-1$ classical parties do not need to have the ability to generate, reflect, reorder the quantum states, and apply unitary operations, while they are only able to measure in the Z basis measurement. Thus, from a practical point of view, the classical parties require fewer capabilities compared to the existing counterparts.

3 The proposed CMSQSS protocol

In this section, a CSQSS protocol is presented. Alice, who is a quantum user, wants to share a one-bit specific message with n classical users, $Bob_1, Bob_2, ..., Bob_n$. Alice as a quantum user, has full quantum capabilities, $n-1$ classical users, $Bob_2, ..., Bob_n$ only measures in the Z basis, and one trusted classical user, Bob_1 has only limited quantum capabilities, such as applying X or I unitary operations and performing the Z basis measurement on qubits. To make the following analysis manageable, we assume that the quantum channel is insecure and that there is an eavesdropper who has full quantum capabilities but can eavesdrop on an authenticated classical channel without altering the information. The CSQSS protocol is described as follows. The framework of the CSQSS is given in Fig. 1.

Step 1 (preparation): Alice generates a sufficiently large number (L) of $n+2$ ($n=2k$, where k is a positive integer) entangled particle states, denoted by Eq. (3),

$$\begin{aligned}|\varphi\rangle_{a_1a_2b_1\cdots b_n} =&\frac{1}{2}[|000\rangle|0\rangle^{\otimes(n-1)} + |010\rangle|1\rangle^{\otimes(n-1)}\\ &+ |101\rangle|0\rangle^{\otimes(n-1)} + |111\rangle|1\rangle^{\otimes(n-1)}]_{a_1a_2b_1\cdots b_n},\end{aligned} \tag{3}$$

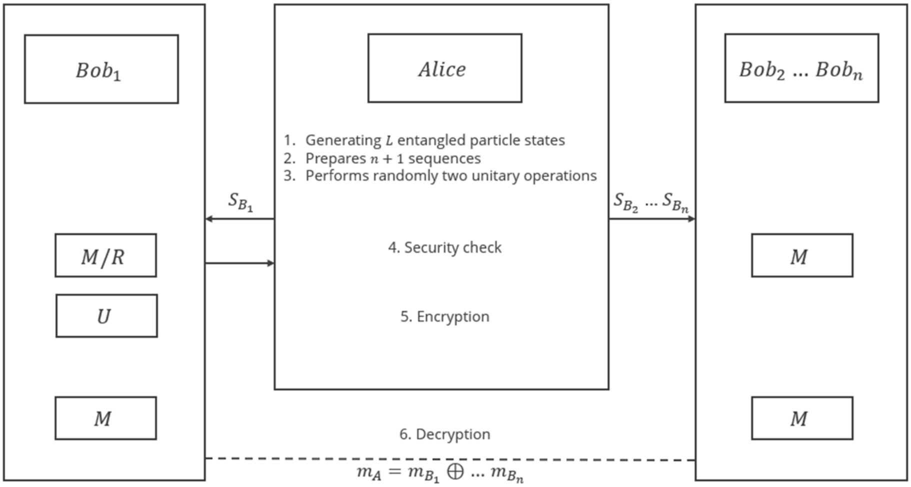
Bob_1
$Alice$
$Bob_2 \ldots Bob_n$
1. Generating L entangled particle states
2. Prepares $n+1$ sequences
3. Performs randomly two unitary operations
S_{B_1}
$S_{B_2} \ldots S_{B_n}$
M/R
U
M
4. Security check
5. Encryption
M
M
6. Decryption
$m_A = m_{B_1} \oplus \ldots m_{B_n}$

Fig. 1 The framework of CMSQSS

where $a_1a_2b_1...b_n$ represent the $n+2$ qubits in an $n+2$ entangled particle state. These entangled particle states can be defined in L groups as $[P^1_{a_1a_2b_1...b_n}, P^2_{a_1a_2b_1...b_n}, ..., P^L_{a_1a_2b_1...b_n}]$. Alice chooses some groups at random to check the security of the quantum channel. She then divides the series of entangled particle states into $n+1$ sequences. For each entangled state, Alice holds the first and second qubits in her hands and randomly performs two unitary operations (H operation or I operation) on every particles of the selected groups. Alice then sends $S_{B_1}, S_{B_2}, ..., S_{B_n}$ to $Bob_1, Bob_2, ...$ and Bob_n respectively.

$$\begin{aligned}
S_A &= (P^1_{a_1}P^1_{a_2}, P^2_{a_1}P^2_{a_2}, ..., P^L_{a_1}P^L_{a_2}) \\
S_{B_1} &= (P^1_{b_1}, P^2_{b_1}, ..., P^L_{b_1}) \\
S_{B_2} &= (P^1_{b_2}, P^2_{b_2}, ..., P^L_{b_2}) \\
&\vdots \\
S_{B_n} &= (P^1_{b_n}, P^2_{b_n}, ..., P^L_{b_n})
\end{aligned}$$

Step 2 (Security check): when all users have reported that they have received the sequences, Alice declares the order of the particles by an authenticated classical channel. According to Alice's declaration, Bob_i selects these particles and then, $Bob_2, Bob_3, ..., Bob_n$ measure their particle in the Z basis. Then, Bob_1 randomly chooses either to measure the particle in the Z basis, or to reflect it back to Alice without any modification. After Alice receives the particles from Bob_1, she measures the particles that depends on her choices. If she applied I operation on the particles in the preparation phase, she will measure her particles and the received particles with the Z basis; otherwise she will measure the particles with the X basis. According to Table 1, the measurement results of all users should be correlated. If there is no eavesdropper, proceed to the next step; otherwise, if the error rate exceeds the predefined threshold, abort the protocol.

Step 3 (encryption): after the eavesdropping check, Alice determines her specific message and measures her two qubits. According to her results, she asks Bob_1 as a controller to perform a proper unitary operation, defined in Table 2, on his qubit.

Table 1 The corresponding measurement results

Bob_1's,..., Bob_n's states	Bob_1's operation	Alice's operation	Alice's basis	Alice's state (a_1a_2R)
$\|0\rangle\|0\rangle^{\otimes(n-1)}$	$M(REF)$	Z	I	$\|00\rangle(\|0\rangle)$
$\|0\rangle\|1\rangle^{\otimes(n-1)}$	$M(REF)$	Z	I	$\|01\rangle(\|0\rangle)$
$\|1\rangle\|0\rangle^{\otimes(n-1)}$	$M(REF)$	Z	I	$\|10\rangle(\|1\rangle)$
$\|1\rangle\|1\rangle^{\otimes(n-1)}$	$M(REF)$	Z	I	$\|11\rangle(\|1\rangle)$
$\|0\rangle^{\otimes(n)}$ or $\|1\rangle^{\otimes(n)}$	M	X	H	$\|{+}{+}\rangle$
$\|0\rangle^{\otimes(n)}$ or $\|1\rangle^{\otimes(n)}$	M	X	H	$\|{+}{-}\rangle$
$\|0\rangle^{\otimes(n)}$ or $\|1\rangle^{\otimes(n)}$	M	X	H	$\|{-}{+}\rangle$
$\|0\rangle^{\otimes(n)}$ or $\|1\rangle^{\otimes(n)}$	M	X	H	$\|{-}{-}\rangle$
$\|0\rangle^{\otimes(n-1)}$ or $\|1\rangle^{\otimes(n-1)}$	REF	X	H	$\|{+}{+}\rangle\|+\rangle$
$\|0\rangle^{\otimes(n-1)}$ or $\|1\rangle^{\otimes(n-1)}$	REF	X	H	$\|{+}{-}\rangle\|+\rangle$
$\|0\rangle^{\otimes(n-1)}$ or $\|1\rangle^{\otimes(n-1)}$	REF	X	H	$\|{-}{+}\rangle\|-\rangle$
$\|0\rangle^{\otimes(n-1)}$ or $\|1\rangle^{\otimes(n-1)}$	REF	X	H	$\|{-}{-}\rangle\|-\rangle$

R Received particle from Bob_1 to Alice, M measure, REF reflect

Step 4 (decryption): all users, Bob_1, Bob_2,..., Bob_n measure their qubits and publish their results on an authenticated classical channel. Finally, the users can recover Alice's secret by performing an exclusive OR operation on their results only if they cooperate.

As an example of this CSQSS protocol, suppose Alice wants to send "1" as a specific message. When the result of her measurement is $|11\rangle$, she asks Bob_1 to perform an X operation on the corresponding particle in his hand. Then, all the classical users perform a Z basis measurement on their particles. In this way, all classical users can cooperate to obtain the shared secret message m_A by calculating $m_A = r_{B_1} \oplus r_{B_2} \oplus \cdots \oplus r_{B_n} = 0 \oplus 1 \oplus \cdots \oplus 1 = 1$

4 The extension of the proposed CSQSS

In this section, we propose an improvement to the proposed CSQSS protocol in which Alice, as a quantum user can send m-bit specific messages $K(k_1, k_2, ..., k_m)$ to n classical users.

Step 1 (preparation): Alice prepares a sufficiently large number (L) of $m(n+2)$ ($n = 2k$, where k is a positive integer) entangled particle pairs to exchange messages as in Eq. (4),

$$\begin{aligned}
&|\varphi\rangle_{a_1^1 a_2^1 a_1^2 a_2^2 ... a_1^m a_2^m b_1^1 b_2^1 ... b_n^1 b_1^2 b_2^2 ... b_n^2 ... b_1^m b_2^m ... b_n^m} \\
&= \frac{1}{2^{\frac{2m}{2}}} \Big[|0\rangle^{\otimes 2m} |0\rangle^{\otimes (m-1)n} |0\rangle^{\otimes n} + |0\rangle^{\otimes (2m-1)} |1\rangle |0\rangle^{\otimes (m-1)n} |0\rangle |1\rangle^{\otimes (n-1)} \\
&+ |0\rangle^{\otimes (2m-2)} |10\rangle |0\rangle^{\otimes (m-1)n} |1\rangle |0\rangle^{\otimes (n-1)} + |0\rangle^{\otimes (2m-2)} |11\rangle |0\rangle^{\otimes (m-1)n} |1\rangle^{\otimes n} \\
&+ |0\rangle^{\otimes (2m-3)} |100\rangle |0\rangle^{\otimes (m-2)n} |0\rangle |1\rangle^{\otimes (n-1)} |0\rangle^{\otimes n} \\
&+ |0\rangle^{\otimes (2m-3)} |101\rangle |0\rangle^{\otimes (m-2)n} |0\rangle |1\rangle^{\otimes (n-1)} |0\rangle |1\rangle^{\otimes (n-1)} \\
&+ |0\rangle^{\otimes (2m-3)} |110\rangle |0\rangle^{\otimes (m-2)n} |0\rangle |1\rangle^{\otimes (n-1)} |1\rangle |0\rangle^{\otimes (n-1)} \\
&+ |0\rangle^{\otimes (2m-3)} |111\rangle |0\rangle^{\otimes (m-2)n} |0\rangle |1\rangle^{\otimes (n-1)} |1\rangle^{\otimes n} \\
&+ \cdots + |1\rangle^{\otimes (2m-2)} |00\rangle |1\rangle^{\otimes (m-1)n} |0\rangle^{\otimes n} + |1\rangle^{\otimes (2m-2)} |01\rangle |1\rangle^{\otimes (m-1)n} |0\rangle |1\rangle^{\otimes (n-1)} \\
&+ |1\rangle^{\otimes (2m-1)} |0\rangle |1\rangle^{\otimes (m-1)n} |1\rangle |0\rangle^{\otimes (n-1)} + |1\rangle^{\otimes 2m} |1\rangle^{\otimes (m-1)n} |1\rangle^{\otimes (n)} \Big],
\end{aligned} \tag{4}$$

Table 2 Relation between the secret, measurement results, and Bob_1's operation

Secret	Alice's result	Bob_1's result	Bob_2's,..., Bob_n's results	Bob_1's operation
0	$\|00\rangle$	$\|0\rangle$	$\|0\rangle^{\otimes(n-1)}$	I
0	$\|01\rangle$	$\|0\rangle$	$\|1\rangle^{\otimes(n-1)}$	σ_x
0	$\|10\rangle$	$\|1\rangle$	$\|0\rangle^{\otimes(n-1)}$	σ_x
0	$\|11\rangle$	$\|1\rangle$	$\|1\rangle^{\otimes(n-1)}$	I
1	$\|00\rangle$	$\|0\rangle$	$\|0\rangle^{\otimes(n-1)}$	σ_x
1	$\|01\rangle$	$\|0\rangle$	$\|1\rangle^{\otimes(n-1)}$	I
1	$\|10\rangle$	$\|1\rangle$	$\|0\rangle^{\otimes(n-1)}$	I
1	$\|11\rangle$	$\|1\rangle$	$\|1\rangle^{\otimes(n-1)}$	σ_x

where $a_1^1a_2^1a_1^2a_2^2...a_1^ma_2^mb_1^1b_2^1...b_n^1b_1^2b_2^2...b_n^2...b_1^mb_2^m...b_n^m$ represent the $2m+mn$ qubits in a $2m + mn$ entangled particle state as a quantum channel. The channel has 4^m terms. The first $2m$ qubits indicate the order of Alice's possible secret messages, which take values from 0 to 2^{2m-1}, respectively. The remaining mn qubits are divided into m groups of n qubits. Each n-qubit group takes one of four possible states ($|0\rangle|0\rangle^{\otimes(n-1)}$, $|0\rangle|1\rangle^{\otimes(n-1)}$, $|1\rangle|0\rangle^{\otimes(n-1)}$ and $|1\rangle|1\rangle^{\otimes(n-1)}$). There are 4^m possibilities for ordering these states for n classical users which are related to $b_1^1b_2^1...b_n^1b_1^2b_2^2...b_n^2...b_1^mb_2^m...b_n^m$.

These $2m + mn$ entangled particle states can be defined in L groups as:

$$\begin{aligned}&[P^1_{a_1^1a_2^1a_1^2a_2^2...a_1^ma_2^mb_1^1b_2^1...b_n^1b_1^2b_2^2...b_n^2...b_1^mb_2^m...b_n^m},\\ &P^2_{a_1^1a_2^1a_1^2a_2^2...a_1^ma_2^mb_1^1b_2^1...b_n^1b_1^2b_2^2...b_n^2...b_1^mb_2^m...b_n^m}, ...,\\ &P^L_{a_1^1a_2^1a_1^2a_2^2...a_1^ma_2^mb_1^1b_2^1...b_n^1b_1^2b_2^2...b_n^2...b_1^mb_2^m...b_n^m}].\end{aligned}$$

Alice chooses some groups at random to check the security of the quantum channel. She then divides the series of entangled particle states into $n + 1$ sequences. For each entangled state, Alice takes all the first $2m$ qubits in her hands and performs two unitary operations (X operation and I operation) at random on the other particles of the selected groups. Then, she transmits $S_{B_1}, S_{B_2}, ..., S_{B_n}$ to $Bob_1, Bob_2, ...$ and Bob_n, respectively as follows:

$$\begin{aligned}S_A &= (P^1_{a_1}P^1_{a_2}...P^{2m}_{a_1}P^{2m}_{a_2}, P^2_{a_1}P^2_{a_2}...P^{2m}_{a_1}P^{2m}_{a_2}, ..., P^L_{a_1}P^L_{a_2}...P^{2m}_{a_1}P^{2m}_{a_2})\\ S_{B_1} &= (P^1_{b_1}...P^m_{b_1}, P^2_{b_1}...P^m_{b_1}...P^L_{b_1}...P^m_{b_1})\\ S_{B_2} &= (P^1_{b_2}...P^m_{b_2}, P^2_{b_2}...P^m_{b_2}, ..., P^L_{b_2}...P^m_{b_2})\\ &\vdots\\ S_{B_n} &= (P^1_{b_n}...P^m_{b_n}, P^2_{b_n}...P^m_{b_n}, ..., P^L_{b_n}...P^m_{b_n})\end{aligned}$$

Step 2 (security check): this step is the same as Step 2 in Sect. 3.

Step 3 (encryption): after the eavesdropping check, Alice determines her m-bit specific messages and measures her $2m$ qubits based on the Z basis. Based on her results and secrets, she asks Bob_1 as a controller to perform an appropriate unitary operation on his particles, as follows:

$$\begin{aligned}k_1 &= R^1_{a_1} \oplus R^1_{a_2} \oplus k'_1\\ k_2 &= R^2_{a_1} \oplus R^2_{a_2} \oplus k'_2\\ &\vdots\\ k_m &= R^m_{a_1} \oplus R^m_{a_2} \oplus k'_m,\end{aligned} \tag{5}$$

where $R^j_{a_i}$ are the measurement results in the Z basis of the qubits $P^j_{a_i}$, and k'_j refers to an appropriate unitary operation, $U_{b_1^j}$. According to Eq. (5), k'_j is specified by Alice. The operator applied to the jth qubit is equal to $X^{k'_j}$, that is, if $k'_j = 0$ or $k'_j = 1$, the corresponding Bob_1 must apply $U_{b_1^j} = I$ or $U_{b_1^j} = \sigma_x$ on his particles, respectively. Table 3 shows the results in more detail.

Step 4 (decryption): finally, all classical users cooperate to recover the secret K $(k_1, k_2, ..., k_m)$ by

$$
\begin{aligned}
k_1 &= R^1_{b_1} \oplus R^1_{b_2} \oplus \cdots \oplus R^1_{b_n}\\
k_2 &= R^2_{b_1} \oplus R^2_{b_2} \oplus \cdots \oplus R^2_{b_n}\\
&\vdots\\
k_m &= R^m_{b_1} \oplus R^m_{b_2} \oplus \cdots \oplus R^m_{b_n},
\end{aligned}
\tag{6}
$$

where $R^j_{b_i}$ is the measurement results in the Z basis of qubits $P^j_{b_i}$. For example, suppose Alice wants to send “110” as 3-bit specific messages. When the results of her measurements become $|000010\rangle$; she asks Bob_1 to perform X operation on the corresponding particles in his hand. Then, all the classical users perform a Z basis measurement on their particles. In this way, all users (Bob_1, Bob_2,..., Bob_n) can cooperate together to obtain the common secret message $K(k_1, k_2, k_3)$ by calculating

$$
\begin{aligned}
k_1 &= R_{b^1_1} \oplus R_{b^1_2} \oplus \cdots \oplus R_{b^1_n} = 1 \oplus 0 \oplus \cdots \oplus 0 = 1\\
k_2 &= R_{b^2_1} \oplus R_{b^2_2} \oplus \cdots \oplus R_{b^2_n} = 1 \oplus 0 \oplus \cdots \oplus 0 = 1\\
k_3 &= R_{b^3_1} \oplus R_{b^3_2} \oplus \cdots \oplus R_{b^3_n} = 0 \oplus 0 \oplus \cdots \oplus 0 = 0
\end{aligned}
$$

Table 3 Relation between the secrets, classical users’s measurement results, and Bob_1’s operations

Secrets	Alice’s results	Bob_1’s results	Bob_2’s,..., Bob_n’s results	Bob_1’s operations
0...00	$\lvert 0\rangle^{\otimes 2m}_{a^1_1 a^1_2 a^2_1 a^2_2 ... a^m_1 a^m_2}$	$\lvert 0\rangle^{\otimes m}_{b^1_1 b^2_1 ... b^m_1}$	$\lvert 0\rangle^{\otimes m(n-1)}_{b^1_2 ... b^1_n ... b^m_2 ... b^m_n}$	$I \otimes ... \otimes I \otimes I$
0...00	$\lvert 0\rangle^{\otimes(2m-1)}\lvert 1\rangle$	$\lvert 0\rangle^{\otimes m}$	$\lvert 0\rangle^{\otimes(n-1)}\lvert 1\rangle^{\otimes(m-1)(n-1)}$	$I \otimes ... \otimes I \otimes \sigma_x$
..	..	..	..	..
0...00	$\lvert 1\rangle^{\otimes 2m}$	$\lvert 1\rangle^{\otimes m}$	$\lvert 1\rangle^{\otimes m(n-1)}$	$I \otimes ... \otimes I \otimes I$
0...01	$\lvert 0\rangle^{\otimes 2m}$	$\lvert 0\rangle^{\otimes m}$	$\lvert 0\rangle^{\otimes m(n-1)}$	$I \otimes ... \otimes I \otimes \sigma_x$
0...01	$\lvert 0\rangle^{\otimes(2m-1)}\lvert 1\rangle$	$\lvert 0\rangle^{\otimes m}$	$\lvert 0\rangle^{\otimes(n-1)}\lvert 1\rangle^{\otimes(m-1)(n-1)}$	$I \otimes ... \otimes I \otimes I$
..	..	..	..	..
0...01	$\lvert 1\rangle^{\otimes 2m}$	$\lvert 1\rangle^{\otimes m}$	$\lvert 1\rangle^{\otimes m(n-1)}$	$I \otimes ... \otimes I \otimes \sigma_x$
0...10	$\lvert 0\rangle^{\otimes 2m}$	$\lvert 0\rangle^{\otimes m}$	$\lvert 0\rangle^{\otimes m(n-1)}$	$I \otimes ... \otimes \sigma_x \otimes I$
0...10	$\lvert 0\rangle^{\otimes(2m-1)}\lvert 1\rangle$	$\lvert 0\rangle^{\otimes m}$	$\lvert 0\rangle^{\otimes(n-1)}\lvert 1\rangle^{\otimes(m-1)(n-1)}$	$I \otimes ... \otimes \sigma_x \otimes \sigma_x$
..	..	..	..	..
0...10	$\lvert 1\rangle^{\otimes 2m}$	$\lvert 1\rangle^{\otimes m}$	$\lvert 1\rangle^{\otimes m(n-1)}$	$I \otimes ... \otimes \sigma_x \otimes I$
..	..	..	..	..
..	..	..	..	..
..	..	..	..	..
1...11	$\lvert 0\rangle^{\otimes 2m}$	$\lvert 0\rangle^{\otimes m}$	$\lvert 0\rangle^{\otimes m(n-1)}$	$\sigma_x \otimes ... \otimes \sigma_x \otimes \sigma_x$
1...11	$\lvert 0\rangle^{\otimes(2m-1)}\lvert 1\rangle$	$\lvert 0\rangle^{\otimes m}$	$\lvert 0\rangle^{\otimes(n-1)}\lvert 1\rangle^{\otimes(m-1)(n-1)}$	$\sigma_x \otimes ... \otimes \sigma_x \otimes I$
..	..	..	..	..
1...11	$\lvert 1\rangle^{\otimes 2m}$	$\lvert 1\rangle^{\otimes m}$	$\lvert 1\rangle^{\otimes m(n-1)}$	$\sigma_x \otimes ... \otimes \sigma_x \otimes \sigma_x$

5 Security analysis

The security of the proposed CSQSS protocol is discussed in this section. In general, two types of attackers, external and internal attackers, need to be considered in the security analysis of the CSQSS protocol. We show that the proposed CSQSS protocol is secure against both types of attacks.

5.1 External attack

In this type of attack, the goal of an external attacker, Eve, is to eavesdrop on the specific messages $K\,(k_1, k_2, ..., k_m)$. If Eve does not attack the particle sequences, she cannot obtain any useful information. Since the particle sequences are only transmitted once in the proposed protocol, Eve must attack the transmission of the particle sequences $S_{B_1}, ..., S_{B_n}$ in Step 1. In the security checking phase, in Step 2, Eve's attack will be detected by Alice. Therefore, the presented CSQSS protocol can protect against external attacks. In the following, two types of Eve's attacks that may utilize in the preparation phase are analyzed.

5.1.1 Intercept-and-resend attack

In this type of attack, since Eve does not know Alice's chosen unitary operation on the particles in the preparation phase, she randomly intercepts and measures the transmitting particles in the Z or X basis and sends the fake particles to the users. The following scenarios could occur:

(1) If Eve chooses the Z basis, while Alice applied the I operation, according to Eq. (3), Eve's attack would not be detected.

(2) If Eve chooses the X basis while Alice's operation was H, according to Eq. (7), her attack will not be detected.

$$\begin{aligned} |\varphi_1\rangle_{a_1a_2b_1\ldots b_n} =&\frac{1}{2}[|++\,+\rangle|+\rangle^{\otimes(n-1)} + |+-+\rangle|-\rangle^{\otimes(n-1)} \\ &+ |-+-\rangle|+\rangle^{\otimes(n-1)} + |---\rangle|-\rangle^{\otimes(n-1)}]_{a_1a_2b_1\ldots b_n}. \end{aligned} \tag{7}$$

(3) If Eve's basis is X and Alice's operation was I, her attack will be detected with probability equal to $\frac{1}{2^n}$. The reason is that, suppose $n = 2$, according to Eq. (8), if Eve obtains $|{++}\rangle$ and Alice's measurement result is $|00\rangle$, since the state that Eve sends to the users is $|+\rangle$, there are four possible combinations of the user's results, and according to Eq. (3), the only results that will be accepted by the users is the case where both users, Bob_1, and Bob_2, obtain $|0\rangle$ based on their measurements. So, with a probability of $\frac{1}{2^2}$, Eve will not be detected.

$$\begin{aligned} |\varphi_2\rangle_{a_1a_2b_1\ldots b_n} = &\frac{1}{2^2}[(|00\rangle + |01\rangle + |10\rangle + |11\rangle)_{a_1a_2}|+\rangle_{b_1}|+\rangle_{b_2} \\ &+ (|00\rangle - |01\rangle + |10\rangle - |11\rangle)_{a_1a_2}|+\rangle_{b_1}|-\rangle_{b_2} \\ &+ (|00\rangle + |01\rangle - |10\rangle - |11\rangle)_{a_1a_2}|-\rangle_{b_1}|+\rangle_{b_2} \\ &+ (|00\rangle - |01\rangle - |10\rangle + |11\rangle)_{a_1a_2}|-\rangle_{b_1}|-\rangle_{b_2}]. \end{aligned} \tag{8}$$

(4) If Eve's basis is Z and Alice's operation was H, her attack will be detected with probability 1/2 only if Bob_1 decided to reflect the particle. Consider the case where $n = 2$, Eve obtains $|00\rangle$ and Alice's measurement result is $|00\rangle$. If Bob_1 reflects the state, Alice may obtain $|-\rangle$ with probability of $\frac{1}{2}$, because the reflected particle is $|0\rangle$ and according to Eq. (9) there is no correlation between the measurement results of Alice and all users. So, Eve will be detected with probability of $\frac{1}{2}$.

$$\begin{aligned}|\varphi_3\rangle_{a_1a_2b_1\ldots b_n} =& \frac{1}{\sqrt{2^{n+1}}}[|+++\rangle(|0\rangle+|1\rangle)^{\otimes(n-1)} + |+-+\rangle(|0\rangle-|1\rangle)^{\otimes(n-1)} \\ &+ |-+-\rangle(|0\rangle+|1\rangle)^{\otimes(n-1)} + |---\rangle(|0\rangle-|1\rangle)^{\otimes(n-1)}]_{a_1a_2b_1\ldots b_n}.\end{aligned} \tag{9}$$

Therefore, the total probability of not detecting Eve is $\frac{1}{2}\left(\frac{1}{2}\left(\frac{1}{2^n}\right)+\frac{1}{2}(0)\right)+\frac{1}{2}\left(\frac{1}{2}\right)\left(\frac{1}{2}+\frac{1}{2}(0)\right)=\frac{1}{8}\left(\frac{1}{2^{n-1}}+1\right)$. As the number of users goes to infinity, the probability of not detecting Eve will be $\frac{1}{8}$, and if the number of the selected groups for the security check is λ, the probability of detecting Eve will be $1-\left(\frac{1}{8}\right)^{\lambda}$. So, if the number of the selected group is large enough, the probability of detecting Eve will be close to one and the communication is secure.

We also obtain the probability of detecting Eve's attack if Eve chooses only Z basis measurement, regardless of whether Alice's operation is I or H, Eve's attack will be detected with probability equal to $1-\left(\frac{3}{4}\right)^{\lambda}$.

5.1.2 Entangle-and-measure attack

In this attack, Eve tries to recover the specific messages by preparing some auxiliary particles $|E_i\rangle$ and entangling them with the sequences S_{B_i}. Eve uses the unitary operation, U, on the pair of particles $P_{b_i}^{j}$ and her particle $|E_i\rangle$. It can be described as Eq. (10)

$$\begin{aligned}U|0\rangle|E_i\rangle =&\alpha|0\rangle|e_{00}\rangle+\beta|1\rangle|e_{01}\rangle,\\ U|1\rangle|E_i\rangle =&\gamma|0\rangle|e_{10}\rangle+\delta|1\rangle|e_{11}\rangle,\\ U|+\rangle|E_i\rangle =&\frac{1}{2}[|+\rangle(\alpha|e_{00}\rangle+\beta|e_{01}\rangle+\gamma|e_{10}\rangle+\delta|e_{11}\rangle)\\ &+|-\rangle(\alpha|e_{00}\rangle-\beta|e_{01}\rangle+\gamma|e_{10}\rangle-\delta|e_{11}\rangle)],\\ U|-\rangle|E_i\rangle =&\frac{1}{2}[|+\rangle(\alpha|e_{00}\rangle+\beta|e_{01}\rangle-\gamma|e_{10}\rangle-\delta|e_{11}\rangle)\\ &+|-\rangle(\alpha|e_{00}\rangle-\beta|e_{01}\rangle-\gamma|e_{10}\rangle+\delta|e_{11}\rangle)],\end{aligned} \tag{10}$$

where $|e_{ij}\rangle$ indicates the ancillary state of Eve. The unitary operation, U, is described as Eq. (11)

$$\begin{aligned}&U=\begin{bmatrix}\alpha & \beta\\ \gamma & \delta\end{bmatrix},\\ &|\alpha|^2+|\beta|^2=|\gamma|^2+|\delta|^2=1.\end{aligned} \tag{11}$$

After Eve performed unitary operation (for instance on Bob_1 particle), the state of the whole system is described as follows:

$$\begin{aligned}|\Phi\rangle_{a_1a_2b_1\ldots b_nE} =&\frac{1}{2}[\alpha(|000\rangle|0\rangle^{\otimes(n-1)} + |010\rangle|1\rangle^{\otimes(n-1)})|e_{00}\rangle\\ &+ \beta(|001\rangle|0\rangle^{\otimes(n-1)} + |011\rangle|1\rangle^{\otimes(n-1)})|e_{01}\rangle\\ &+ \gamma(|100\rangle|0\rangle^{\otimes(n-1)} + |110\rangle|1\rangle^{\otimes(n-1)})|e_{01}\rangle\\ &+ \delta(|101\rangle|0\rangle^{\otimes(n-1)} + |111\rangle|1\rangle^{\otimes(n-1)})|e_{11}\rangle]_{a_1a_2b_1\ldots b_nE}.\end{aligned} \tag{12}$$

According to Eq. (12) and Table 1, the Eve's existence can be detected with probability equal to $\frac{1}{2}\{|\beta|^2 + |\gamma|^2\}$ probability if the measurement basis is Z.

5.2 Internal attack

The purpose of an internal attack is for one or more dishonest parties to try to obtain the specific messages. In the following, such an internal attack is discussed in more detail from two perspectives.

5.2.1 The participant attack from one dishonest party

The goal of this dishonest party is to determine the specific messages K alone. Without loss of generality, we can consider that Bob_i, where $2 \leq i \leq (n-1)$, to be a dishonest party. If Bob_i wants to get the secret alone; he can only determine $R^m_{b_i}$ by measuring his particle in the Z basis and does not know the results of other particle measurements. This shows that Bob_i cannot obtain any secret. Also, in the proposed CSQSS protocol, there is no qubit transmission between the classical users. If Bob_i wants to achieve his goal, he can try to attack the transmitted particles from Alice to Bob_n. However, this is the same as an external attack, and he will be detected by the security checking phase as discussed in Step 1 with probability equal to $1-\left(\frac{3}{4}\right)^{\lambda}$. If the number of groups for the security check is large enough, the probability is close to one and this type of attack will not be successful.

More specifically, with $\frac{1}{2}$ probability, Alice performs the H operation, and if Bob_1 decides to reflect the particle, since the particle that is measured by the dishonest party is not prepared in the X basis, then with $\frac{1}{2}$ probability, Alice may obtain $|+\rangle$ or $|-\rangle$ according to Eq. (13). Therefore, the measurement results are not correlated if the following cases occur: $\{|++-\rangle_{a_1a_2R}, |+--\rangle_{a_1a_2R}, |-++\rangle_{a_1a_2R}, |--+\rangle_{a_1a_2R}\}$, and the attack will be detected with probability $\frac{1}{4}$. As a result, a dishonest party cannot obtain the specific messages without the help of others.

$$\begin{aligned}|\varphi_4\rangle_{a_1a_2b_1\ldots b_n} =&\frac{1}{2\sqrt{2}}[|{+}{+}\rangle(|0\rangle + |1\rangle)|+\rangle^{\otimes(n-1)} + |{+}{-}\rangle(|0\rangle + |1\rangle)|-\rangle^{\otimes(n-1)}\\ &+ |{-}{+}\rangle(|0\rangle - |1\rangle)|+\rangle^{\otimes(n-1)} + |{-}{-}\rangle(|0\rangle - |1\rangle)|-\rangle^{\otimes(n-1)}]_{a_1a_2b_1\ldots b_n}.\end{aligned} \tag{13}$$

5.2.2 The participant attack by more than one dishonest parties

There is another common attack strategy where $n-1$ dishonest parties collude together to attack the protocol. To obtain the specific messages, the dishonest parties have two options. First, $Bob_2, ..., Bob_{n-1}$ can determine $R^m_{b_1}, ..., R^m_{b_n}$. The dishonest parties cannot obtain any

Table 4 Qubit efficiency comparison of the MSQSS protocols

Protocol	Quantum resource	Qubit efficiency
Gao et al. (2016)	Bell states	$\frac{1}{4^n}$
Yu et al. (2017)	GHZ-like states	$\frac{1}{6n+4}$
Li et al. (2020)	Bell states	$\frac{1}{5n}$
Ye et al. (2021)	GHZ states	$\frac{1}{3n+1}$
Proposed protocol	Entangled states	$\frac{1}{n+2}$

secrets without the help of Bob_1. Second, if the dishonest parties try to attack the transmitted particles which that Alice sends to Bob_1, their attack can be detected as the external attacker Eve. Therefore, our proposed CSQSS protocol can protect against internal attacks.

6 Comparison and analysis

Here, we give a comparison between our proposed protocol and the existing MSQSS protocols. The qubit efficiency is defined as Eq. (14),

$$\eta = \frac{n}{m}, \tag{14}$$

where n and m are the total number of shared classical bits and the number of qubits, respectively. Table 4 shows the qubit efficiency comparison of our scheme with the existing MSQSS protocols.

As shown in Table 4, the qubit efficiency of our proposed protocol is higher than the previous MSQSS protocols.

Compared to existing MSQSS protocols, the decoy photon technology (Bennett and Brassard 1984b) (each decoy photon is randomly chosen from the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$), is not used in our protocol for eavesdropping check. Also, entangled state measurement is not required for designing the protocol. Thus, the proposed protocol can be achieved at a lower cost.

7 Conclusion

In this paper, a novel controlled semi-quantum secret sharing protocol with entangled state is presented. In the proposed protocol, with the permission of a trusted classical user, Bob_1, Alice as a quantum user, can shares a one-bit specific message to n classical users $(Bob_1, Bob_2, ..., Bob_n)$, and Alice's secret can only be recovered by cooperation of all classical users. Then, the extension of the proposed CSQSS protocol is defined, where Alice can share m-bit specific messages $K(k_1, k_2, ..., k_m)$ to n classical users. Furthermore, the analysis of the proposed CSQSS shows that the protocol is secure against external and internal attackers.

It is worth emphasising that the proposed protocol has the highest qubit efficiency among the existing MSQSS protocols. Compared with previous MSQSS protocols, the proposed protocol can achieve a lower cost due to the fact that it does not use returning qubits to produce the secret message, uses fewer returning qubits for eavesdropping check and does not use entangled state measurement to design the protocol. From an experimental point of view, we hope that the proposed CSQSS protocol will be realised in the near future.

Acknowledgements Majid Haghparast acknowledges supports from the Academy of Finland (Project DEQSE 349945) and Business Finland (Project TORQS 8582/31/2022). Shima Hassanpour acknowledges the financial support by the Federal Ministry of Education and Research of Germany in the programme of "Souverän. Digital. Vernetzt.". Joint project 6 G-life, Project identification number: 16KISK001K.

Author Contributions All authors contributed equally to the conception and design of the study.

Funding The authors have not disclosed any funding.

Data Availability The authors have read and approved the final version of the manuscript and confirm that the data supporting the results of this study are available in the submitted article.

Declarations

Conflict of interest The authors have not disclosed any competing interests.

Ethical approval This declaration is not applicable to the content of this article.

References

Bennett, C.H., Brassard, G.: Quantum cryptography, Proceedings of the international conference on computers, systems and signal processing, 175–179 (1984)

Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. Theoretical Computer Science **560**, 7–11 (2014)

Bin, G., Yu-Gai, H., Xia, F., Cheng-Yi, Z.: A two-step quantum secure direct communication protocol with hyperentanglement. Chin. Phys. B **20**(10), 100309–100312 (2011)

Blakley, G.R.: Safeguarding cryptographic keys. Safeguarding cryptographic keys. Managing requirements knowledge, international workshop on. IEEE Computer Society (1979)

Boyer, M., Kenigsberg, D., Mor, T.: Quantum key distribution with classical Bob, First International Conference on Quantum, Nano, and Micro Technologies (ICQNM'07). IEEE (2007)

Ekert, A.K.: Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. **67**(6), 661–672 (1991)

Gao, G., Wang, Y., Wang, D.: Multiparty semiquantum secret sharing based on rearranging orders of qubits. Mod. Phys. Lett. B **30**(10), 1650130–1650140 (2016)

Gao, X., Zhang, S., Chang, Y.: Cryptanalysis and improvement of the semi-quantum secret sharing protocol. Int. J. Theor. Phys. **56**(8), 2512–2520 (2017)

Hassanpour, S., Houshmand, M.: Efficient controlled quantum secure direct communication based on GHZ-like states. Quantum Inf. Process. **14**(2), 739–753 (2015)

Hassanpour, S., Houshmand, M.: Bidirectional teleportation of a pure EPR state by using GHZ states. Quantum Inf. Process. **15**(2), 905–912 (2016)

Hillery, M., Bužek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**(3), 1829–1841 (1999)

Khorrampanah, M., Houshmand, M.: Effectively combined multi-party quantum secret sharing and secure direct communication. Opt. Quantam Electron. **54**(4), 213–222 (2022)

Khorrampanah, M., Houshmand, M., Sadeghizadeh, M., Aghababa, H., Mafi, Y.: Enhanced multiparty quantum secret sharing protocol based on quantum secure direct communication and corresponding qubits in noisy environment. Opt. Quantam Electron. **54**(12), 832–840 (2022)

Li, X.-Y., Chang, Y., Zhang, S.-B.: Multi-party semi-quantum secret sharing scheme based on bell states, 6th International Conference, Artificial Intelligence and Security (2020)

Li, X.-H., Deng, F.-G., Zhou, H.-Y.: Efficient quantum key distribution over a collective noise channel. Phys. Rev. A **78**(2), 022321–022331 (2008)

Li, Q., Chan, W.H., Long, D.-Y.: Semiquantum secret sharing using entangled states. Phys. Rev. A **82**(2), 022303–022313 (2010)

Li, L., Qiu, D., Mateus, P.: Quantum secret sharing with classical bobs. J. Phys. A: Math. Theor. **46**(4), 045304–045315 (2013)

Li, Z., Jiang, X., Liu, L.: Multi-party quantum secret sharing based on GHZ state. Entropy **24**(10), 1433–1443 (2022)

Liao, Q., Liu, H., Zhu, L., Guo, Y.: Quantum secret sharing using discretely modulated coherent states. Phys. Rev. A **103**(3), 032410–032423 (2021)

Markham, D., Sanders, B.C.: Graph states for quantum secret sharing. Phys. Rev. A **78**(4), 042309–042319 (2008)

Nielsen, M.A., Chuang, I.: Quantum computation and quantum information, Vol. 2. Cambridge university press (2002)

Saha, D., Panigrahi, P.K.: N-qubit quantum teleportation, information splitting and superdense coding through the composite GHZ-bell channel. Quantum Inf. Process. **11**(2), 615–628 (2012)

Sasaki, T., Yamamoto, Y., Koashi, M.: Practical quantum key distribution protocol without monitoring signal disturbance. Nature **509**(7501), 475–478 (2014)

Shamir, A.: How to share a secret. Commun. ACM **22**(11), 612–613 (1979)

Wang, J., Zhang, S., Zhang, Q., Tang, C.-J.: Semiquantum secret sharing using two-particle entangled state. Int. J. Quantum Inf. **10**(05), 1250050–1250060 (2012)

Wiesner, S.: Conjugate coding. ACM SIGACT News **15**(1), 78–88 (1983)

Wootters, W.K., Zurek, W.H.: A single quantum cannot be cloned. Nature **299**(12), 802–803 (1982)

Xie, C., Li, L., Qiu, D.: A novel semi-quantum secret sharing scheme of specific bits. Int. J. Theor. Phys. **54**(10), 3819–3824 (2015)

Xu, F., Ma, X., Zhang, Q., Lo, H.-K., Pan, J.-W.: Secure quantum key distribution with realistic devices. Rev. Mod. Phys. **92**(2), 025002–025025 (2020)

Yang, C.-W., Hwang, T.: Efficient key construction on semi-quantum secret sharing protocols. Int. J. Quantum Inf. **11**(05), 1350052–1350060 (2013)

Yang, C.-W., Tsai, C.-W.: Efficient and secure dynamic quantum secret sharing protocol based on bell states. Quantum Inf. Process. **19**(5), 1–14 (2020)

Ye, C., Li, J., Chen, X., Yuan, T.: Multi-party semi-quantum secret sharing protocol based on measure-flip and reflect operations, arXiv preprint https://doi.org/10.48550/arXiv.2109.01380 (2021)

Yin, A., Chen, T.: Authenticated semi-quantum secret sharing based on GHZ-type states. Int. J. Theor. Phys. **60**(1), 256–273 (2021)

Yin, A., Fu, F.: Eavesdropping on semi-quantum secret sharing scheme of specific bits. Int. J. Theor. Phys. **55**(9), 4027–4035 (2016)

Yin, H.-L., Fu, Y., Mao, Y., Chen, Z.-B.: Detector-decoy quantum key distribution without monitoring signal disturbance. Phys. Rev. A **93**(2), 022330–022341 (2016)

Yu, K.-F., Gu, J., Hwang, T., Gope, P.: Multi-party semi-quantum key distribution-convertible multi-party semi-quantum secret sharing. Quantum Inf. Process. **16**(8), 1–14 (2017)

Yuan, H., Pan, G.-Z.: Bidirectional quantum-controlled teleportation using six-qubit cluster state without remote joint operation. Mod. Phys. Lett. A **35**(25), 2050192–2050199 (2020)

Zhang, Z.-j, Li, Y., Man, Z.-x: Multiparty quantum secret sharing. Phys. Rev. A **71**(4), 044301–044311 (2005)

Zhang, C.-M., Song, X.-T., Treeviriyanupab, P., Li, M., Wang, C., Li, H.-W., Yin, Z.-Q., Chen, W., Han, Z.-F.: Delayed error verification in quantum key distribution. Chin. Sci. Bull. **59**(23), 2825–2828 (2014)

Zhou, Z., Sheng, Y., Niu, P., Yin, L., Long, G., Hanzo, L.: Measurement-device-independent quantum secure direct communication. Sci. China Phys., Mech. Astron. **63**(3), 1–6 (2020)

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