International Journal of Quantum Information
Vol. 15, No. 3 (2017) 1750023 (13 pages)

DOI: 10.1142/S021974991750023X

Quantum secret sharing with identity authentication based on Bell states

Hussein Abulkasim*

Faculty of Science, Assiut University,
New Valley Branch, El-Kharja 72511, Egypt
hussein@scinv.au.edu.eg

Safwat Hamad†, Amal Khalifa‡ and Khalid El Bahnasy§

Faculty of Computer and Information Sciences,
Ain Shams University, 11566 Cairo, Egypt
†*shamad@cis.asu.edu.eg*
‡*Amal_Khalifa@cis.asu.edu.eg*
§*khaled.bahnasy@cis.asu.edu.eg*

Received 29 April 2016
Accepted 30 March 2017
Published 4 May 2017

Quantum secret sharing techniques allow two parties or more to securely share a key, while the same number of parties or less can efficiently deduce the secret key. In this paper, we propose an authenticated quantum secret sharing protocol, where a quantum dialogue protocol is adopted to authenticate the identity of the parties. The participants simultaneously authenticate the identity of each other based on parts of a prior shared key. Moreover, the whole prior shared key can be reused for deducing the secret data. Although the proposed scheme does not significantly improve the efficiency performance, it is more secure compared to some existing quantum secret sharing scheme due to the identity authentication process. In addition, the proposed scheme can stand against participant attack, man-in-the-middle attack, impersonation attack, Trojan-horse attack as well as information leaks.

Keywords: Quantum secret sharing; quantum dialogue; Bell states; authentication; quantum cryptography.

1. Introduction

Since the pioneer work of Bennett and Brassard,[1] several quantum cryptographic protocols have been introduced for solving several security issues. For example, quantum key distribution (QKD),[2,3] quantum secure direct communication (QSDC),[4,5] semi-quantum cryptographic protocols (SQC),[6–8] quantum teleportation

*Corresponding author.

(QT),[9,10] quantum private comparison (QPC),[11,12] quantum secret sharing (QSS)[13] and so on.

QSS has become a significant topic of quantum cryptography that merges classical secret sharing with the principles of quantum mechanics. Secret sharing[14] can be defined as a technique for sharing a secret key among n parties, where each party holds a share of the secret key and only enough number of legitimate parties can recover that secret key. The essential feature of secret sharing lies in the fact that the honest party can prevent the dishonest one from damaging or stealing the secret. However, as one of the most classical cryptosystems that depends on mathematical assumptions, eavesdropping problem decreases the efficiency of secret sharing. Fortunately, QSS can keep illegitimate parties from acquiring useful information.

In March 1999, Hillery *et al.*[13] introduced the first QSS protocol for securely sharing secret information by a three-particle Greenberger–Horne–Zeilinger (GHZ) state or a four-particle GHZ state. Subsequently, numerous QSS protocols have been introduced with entangled states[15–18] and without entangled states[19,20] in both theoretical studies[21–23] and experimental applications.[24,25] Zhou *et al.*[26] proposed a multi-party QSS protocol based on a single decoy photon protocol and pure entangled states for sharing a private key. Du and Bao[27] presented a QSS protocol using the three-element phase-shift operations which can stand against some of the well-known attacks including a cheating attack. Long *et al.*[28] proposed an efficient QSS scheme which enables three parties to share three bits using a six-qubit state. Shi *et al.*[29] introduced a multi-party QSS protocol. Their protocol enables the participants to acquire the shared information by performing Bell measurements and without using any local unitary operations. Tan and Jiang[30]; on the other hand, presented a QSS protocol using unitary operations based on Bell states. They also employed the single decoy photon technique to prevent eavesdropper.

Furthermore, the process of quantum identity authentication (QIA)[31–34] is necessary for QSS schemes to prevent attackers from performing impersonation attack and man-in-the-middle attack. Yang *et al.*[35] in 2008 presented two multiparty quantum identity authentication schemes based on secret sharing method to share classical information. Zhang and Ji[36] indicated that Yang *et al.*'s schemes are vulnerable to participant attack. In 2015, Qin *et al.*[37] presented a (t, n) QSS protocol to share a quantum state based on phase shift operation. They showed that an identity authentication process should be employed to avoid impersonation attack and man-in-the-middle attack.

In 2004, Nguyen[38] proposed a quantum dialogue (QD) protocol to achieve the process of quantum identity authentication. According to Nguyen's protocol, the participants can simultaneously exchange their secret information in a direct way. Since then, many QD protocols have been proposed such as Ye[39] and Lin *et al.*[40] who independently presented two QD protocols for preventing information leaks. They used a prior shared key between participants for deciding the measuring bases.

In this work, we propose a new QSS scheme that combines the advantages of both QSS protocol and QD protocol. The proposed QSS scheme allows two parties to

simultaneously perform mutual identity authentication. The idea of the proposed QSS scheme is inspired by the protocols in Refs. 30 and 40. Nevertheless, the prior shared key is prepared in a more secure way and is reused to recover the final shared master key. Finally, the proposed QSS scheme is proved to be more secure than some of the existing QSS schemes as well as some QIA protocols that are based on the technique of secret sharing.[35]

The rest sections of this paper are organized as follows. Section 2 describes the proposed QSS scheme. The security and efficiency analysis are then given in Secs. 3 and 4, respectively. Section 5 introduces the multiparty case of the proposed QSS scheme. Comprehensive comparisons between the proposed QSS scheme and other existing QSS schemes are given in Sec. 6. At the end, Sec. 7 summarizes the final results and conclusions.

2. The Proposed QSS Scheme

This work assumes that Alice wants to share, with her agents Bob and Charlie, a master key $K_M = PK \oplus K$, i.e. $K_M, PK, K \in \{0,1\}^{4n}$ where n is an even number. Here, PK is a prior shared key with Bob and Charlie, and K is a secret key prepared by Alice. Alice, Bob and Charlie will employ a two-phase approach to share K: the first phase is QSS phase and the second one is QD phase. In the first phase, a QSS scheme will be considered for distributing K among Alice, Bob and Charlie as in Ref. 30. While in the second phase, a QD protocol will be considered between Bob and Charlie for authenticating the identity of each other based on PK as in Ref. 40. Bob and Charlie will divide PK into two equal parts PK_1 and PK_2, where $PK_1 \oplus PK_2 = PK^*$, i.e. $PK_1, PK_2, PK^* \in \{0,1\}^{2n}$. They then will use the sequence of PK^* to determine the initial states of the Bell states in the QD phase. In addition, the first n bits of PK will be used to represent the measuring bases. Finally, PK will be reused to deduce the master key K_M. Moreover, the four Pauli operators will take the form: $\{U_{00} = I = |0\rangle\langle 0| + |1\rangle\langle 1|,\ U_{01} = \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|,\ U_{10} = \sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|,\ U_{11} = i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|\}$. These operators should be known for both Alice, Bob and Charlie. In addition, they should agree on the four unitary operations $\{U_{00}, U_{01}, U_{10}, U_{11}\}$ to represent the four classical bits $\{00, 01, 10, 11\}$, respectively.

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

The following steps describe the proposed scheme as depicted in Fig. 1:

(1) Alice prepares $2n$ Bell states, all in $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$. Then, she divides these states into two ordered sequences of qubits $S_b = \{b_1, b_2, \ldots, b_{2n}\}$ and

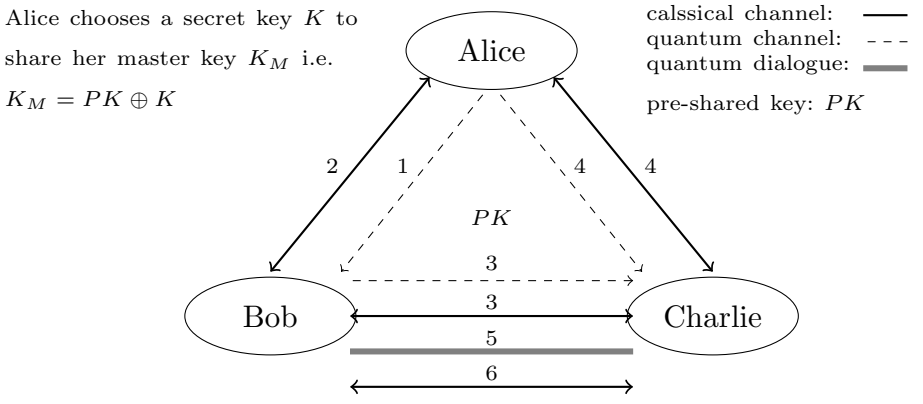

Fig. 1. The proposed scheme.

$S_c = \{c_1, c_2, \ldots, c_{2n}\}$, where S_b is the sets of the first photons of all Bell states and S_c is the sets of the second photons of all Bell states. Then, Alice inserts decoy photons l_1, at random positons, into S_b with each photon randomly in one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Now, the sequence S_b is ready to be sent to Bob by Alice.

(2) Upon receiving the qubits in S_b, Alice declares to Bob the positions of each decoy photon in S_b and its initial states. Then Bob measures these decoy photons by a suitable measuring basis (Z basis $\{|0\rangle, |1\rangle\}$ or X basis $\{|+\rangle, |-\rangle\}$). Now, Alice and Bob should be ready to compare the outcomes of the measurement with the initial states. Hence, they will be able to confirm the security of the communications by calculating the error rate value.

(3) Bob randomly chooses one of the four local unitary operations $\{U_{00}, U_{01}, U_{10}, U_{11}\}$, say $U_{x_1x_2}$, to be applied on S_b, where $x_1, x_2 \in \{0, 1\}$. He also inserts randomly decoy photons l_2 among the qubits in S_b producing S_b^*. Then, the new sequence S_b^* is sent to Charlie. Upon receiving the qubits in S_b^*, Bob informs Charlie of the positions of l_2 and its initial states to check the security of the quantum channel they are using. If the quantum channel is not secure, they should cancel the communication. Otherwise, they can continue to the upcoming step.

(4) Alice encodes her secret K by applying one of the four local unitary operations on S_c, say $U_{k_1k_2}$, where $k_1, k_2 \in \{0, 1\}^{2n}$ and $U_{k_1k_2}$ represent K. She inserts

randomly decoy photons l_3 among the qubits in S_c producing S_c^*. Alice then sends the new sequence S_c^* to Charlie. Upon receiving the qubits in S_c^*, Alice informs Charlie of the positions of l_3 and its initial states to check the security of the quantum channel they are using. If the quantum channel is not secure, they should cancel the communication. Otherwise, they can continue to the upcoming step.

(5) Quantum dialogue:

(i) According to PK^*, Bob generates n Bell states, these states selected from the states in Eq. (1). Both Bob and Charlie agree on the four states $\{|\Phi^+\rangle, |\Psi^+\rangle, |\Psi^-\rangle, |\Phi^-\rangle\}$ to represent the classical bits $00, 01, 10, 11$, respectively. Subsequently, Bob divides the n Bell states into two ordered sequences of qubits $S_B = \{B_1, B_2, \ldots, B_n\}$ and $S_C = \{C_1, C_2, \ldots, C_n\}$, where S_B is the sets of the first photons of all Bell states, and S_C is the sets of the second photons of all Bell states.

(ii) Bob retains only the sequence of S_B in his possession, and sends the sequence S_C to Charlie.

(iii) Upon receiving S_C, Charlie chooses $\frac{n}{2}$ photons form the sequence S_C, called C_{C1}, to be used as checking photons. He then declares their positions to Bob.

(iv) Bob picks up $\frac{n}{2}$ photons from S_B, called C_{B1}, corresponding to the positions of C_{C1}, and measures C_{B1} according to the measuring bases obtaining the measuring result $MR_{C_{B1}}$. He then picks up the remaining $\frac{n}{2}$ photons from S_B, called C_{B2}, to be used as checking photons. Bob then provides Charlie with $MR_{C_{B1}}$ and the positions of C_{B2}.

(v) Upon receiving $MR_{C_{B1}}$ and the positions of C_{B2}, Charlie measures C_{C1} according to the measurement bases obtaining the measuring result $MR_{C_{C1}}$. Charlie then checks whether $MR_{C_{C1}}$ and $MR_{C_{B1}}$ have a deterministic correlation or not. If not, Charlie should terminate the protocol. Otherwise, Charlie immediately authenticates Bob's identity. Charlie then picks up $\frac{n}{2}$ photons from S_C, called C_{C2}, corresponding to the position of C_{B2}. Then, he measures these photons according to the measuring bases obtaining $MR_{C_{C2}}$. Finally, Charlie sends $MR_{C_{C2}}$ to Bob.

(vi) After receiving $MR_{C_{C2}}$, Bob measures the photons C_{B2} according to the measuring bases to get the measuring result $MR_{C_{B2}}$. Bob then checks whether $MR_{C_{C2}}$ and $MR_{C_{B2}}$ have a deterministic correlation or not. If not, Bob should terminate the protocol. Otherwise, Bob immediately authenticates Charlie's identity.

(6) After Bob and Charlie successfully authenticate their identity, they collaborate for deducing the secret key of Alice, i.e. $U_{k_1 k_2}$. Finally, Bob and Charlie perform an XOR operation to get the master key of Alice, i.e. $K_M = PK \oplus K$.

3. Security Analysis

In the QSS phase, the boss Alice uses the unitary operations $U_{k_1 k_2}$ for encoding her secret information K. In collaboration with Bob, Charlie compares Bob's unitary operation, $U_{x_1 x_2}$, and his measuring result $|\phi_{r,s}\rangle$, where $|\phi_{r,s}\rangle = \frac{1}{\sqrt{2}}(|0r\rangle + (-1)^s|1\bar{\mathrm{r}}\rangle)$. Here $r, s \in \{0, 1\}$, $\bar{\mathrm{r}} = r \oplus 1$ and the symbol $\oplus$ denotes addition modulo 2. Hence, both of Bob and Charlie are able to get the secret key K, where $k_1 = x_1 \oplus r$ and $k_2 = x_2 \oplus s$. Moreover, PK is a part of deducing the master key process and only known to Alice, Bob and Charlie. Therefore, Eve will be unable to reveal the master key K_M without knowing PK. Thus, we can say that there is no information leakage in the proposed scheme. In addition, the encrypted sequence PK^* is used instead of the original prior shared key PK as indicated in Step (5)(i). This definitely increases the security by ensuring the concept of avoiding information leaks. For example, assume that the prior shared key $PK = 00011011$, hence $PK_1 = 0001$, $PK_2 = 1011$, so $PK^* = 1010$. Bob will employ PK^* to generate the initial Bell sates, i.e. $\{|\Psi^-\rangle, |\Psi^-\rangle\}$, which will be used to authenticate the identity of Bob and Charlie as indicated in Step (5)(i). The measuring bases will be decided by the first n bits in the sequence PK, i.e. 00, where each bit determines the measuring bases for each Bell states (Z-basis $\{|0\rangle, |1\rangle\}$ when the bit value is 0 and X-basis $\{|+\rangle, |-\rangle\}$ when the bit value is 1). Accordingly, Z-basis will be selected to measure the two states $\{|\Psi^-\rangle, |\Psi^-\rangle\}$. Then, Bob and Charlie should check whether their measurements have deterministic correlation or not (note that this work assumes that the quantum information is transmitted over lossless and noiseless quantum channels, and over public classical channels as well).

In the QSS phase, the quantum information is transmitted over the quantum channels in one-way from Alice to Bob, from Alice to Charlie and from Bob to Charlie. As well, in the QD phase, the quantum information is transmitted from Bob (Charlie) to Charlie (Bob). Thus, we can say that the proposed QSS scheme is secure against Trojan-horse attacks.[40–44] Also, the proposed scheme is secure against impersonation attacks, man-in-the-middle attacks, modification attacks, entangled-and-measure attacks as well as participant attacks as indicated below.

3.1. *Man-in-the-middle attack*

In the QD phase, Eve may try to pass the process of identity authentication by making two independent communications with Bob and Charlie for stealing the quantum information. She will try to achieve this strategy by preparing n Bell states, she then divides these states into two ordered sequences $\{S_{EB}, S_{EC}\}$ as Bob does in Step (5)(i). Afterwards, she may employ some of man-in-the-middle attacks strategies for intercepting the transmitted particles between Bob and Charlie, and replacing them with new particles. However, Eve is unable to successfully pass the process of identity authentication because she does not know PK, where PK is used to prepare the initial Bell states as well as the measuring bases.

3.2. *Impersonation attack*

Lets consider that Eve has two potential scenarios to acquire useful information from Bob and Charlie's communications as follows:

(i) Impersonating Bob. Eve may send forged initial Bell states (S_{EC}) to Charlie to impersonate Bob's identity. However, Charlie will detect Eve's attack in Step (5) (ii), because her sequence S_{EC} is not corresponding to S_C, where S_C is based on PK and Charlie already knows S_C. On very rare occasions, Eve may guess the correct initial Bell states and send Charlie identical photons (S_C). However, Eve cannot select the proper measuring bases which are decided based on PK. Therefore, Eve's attack will be detected in Step (5)(v), where Charlie checks whether $MR_{C_{C1}}$ and $MR_{C_{B1}}$ have a deterministic correlation or not. In this proposed scheme, $\frac{3}{4}$ is the probability for Eve to successfully pass the identity authentication process. Thus, the probability of detecting Eve's attack is $(1-(\frac{3}{4})^{\frac{n}{2}})$, here $\frac{n}{2}$ is the minimum number of used particles to check Eve's attack for each round. Accordingly, the probability of detecting Eve's attack can be very close to 1 using large enough n.

(ii) Impersonating Charlie. Eve may try to impersonate Charlie by sending the measuring result $MR_{C_{E2}}$. Since Eve does not have PK she cannot decide the correct measuring bases. Thus, she will send an invalid measuring result $MR_{C_{E2}}$ to Bob. Subsequently, Bob compares the measuring result $MR_{C_{E2}}$ with $MR_{C_{B2}}$ and detects that they are not in deterministic correlation. The probability of detecting Eve's attack is $(1-(\frac{3}{4})^{\frac{n}{2}})$, here $\frac{n}{2}$ is the minimum number of used particles to check Eve's attack for each round. Accordingly, the probability of detecting Eve's attack can be very close to 1 using large enough n.

3.3. *Entangled-and-measure attack*

In Steps (1), (3) and (4), Alice sends the sequence S_b to Bob, and sends the sequence S_c^* to Charlie and Bob sends the sequence S_b^* to Charlie, respectively. To recover Alice's secret, Eve prepares some ancillas $E=\{|E_0\rangle,|E_1\rangle,\ldots\}$, she then entangles them with the checking particles by a unitary operation U (i.e. $U.U^\dagger = U^\dagger.U = I$), which produces the result in Eq. (2):

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

where $|\alpha^2|+|\beta^2| = |\gamma^2|+|\delta^2| = 1$, and $\{|e_{00}\rangle, |e_{01}\rangle, |e_{10}\rangle, |e_{11}\rangle\}$ are ancillas states prepared by Eve. In entangled-and-measure attack, Eve has to perform two

procedures to pass eavesdropping check. Firstly, she has to set $\beta = \gamma = 0$ if the used checking photons are $|0\rangle$ or $|1\rangle$. Secondly, she has to set $\alpha|e_{00}\rangle - \beta|e_{01}\rangle + \gamma|e_{10}\rangle - \delta|e_{11}\rangle = \alpha|e_{00}\rangle + \beta|e_{01}\rangle - \gamma|e_{10}\rangle - \delta|e_{11}\rangle = 0$ if the used checking photons are $|+\rangle$ or $|-\rangle$. However, preparing $\beta = \gamma = 0$ gives $\alpha|e_{00}\rangle - \delta|e_{11}\rangle = 0$, which means that $\alpha|e_{00}\rangle = \delta|e_{11}\rangle$. As a result, Eve cannot differentiate between $\alpha|e_{00}\rangle$ and $\delta|e_{11}\rangle$. Therefore, Eve cannot reveal K. Moreover, even if she was clever enough to get K; Eve is still incapable of deducing K_M because PK is required and she does not know it (i.e. $K_M = PK \oplus K$). Therefore, entangled-and-measure attacks are prevented.

3.4. *Participant attack*

The outer attacks are much less threatening than internal attacks because dishonest participants already know shadows of the secret. Thus, the security against participant attacks is pivotal to QSS schemes. In the proposed QSS scheme, Alice sends Bob, the sequence S_b protected by l_1, also Alice sends Charlie the sequence S_c^* protected by l_3 (l_1 and l_3 are single decoy photons, which are randomly chosen from the states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$). Thus, when a dishonest participant, say Bob (Charlie), adopts an attack strategy such as intercept-and-resend attack for intercepting $S_c^*(S_b)$ and resends a new sequence, he will be detected easily in Step (4) (Step (2)); because dishonest Bob (dishonest Charlie) does not neither know the polarization states of the photons in l_3 (l_1) nor their positions. In addition, the decoy photons and the photons in $S_c^*(S_b)$ are in maximally mixed state. So, Bob (Charlie) cannot differentiate between the decoy photons and the photons in $S_c^*(S_b)$. The probability for dishonest Bob (Charlie) to pass the public discussion is $\frac{3}{4}$, and the probability of detecting Bob's attack is $1 - (\frac{3}{4})^{l_3}$ (the probability of detecting Charlie's attack is $1 - (\frac{3}{4})^{l_1}$). Accordingly, the probability of detecting Bob's (Charlie) attack can be very close to 1 using large enough $l_3(l_1)$. Hence, the proposed QSS scheme is proved to be secure against participant attacks.

3.5. *Modification attack*

In the QD phase, Eve may perform a unitary operation (e.g. $i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$) on photons in S_C for modifying Charlie's sequence without being detected. Therefore, the initial two states $\{|\Psi^-\rangle, |\Psi^-\rangle\}$ will be changed to $\{|\Phi^+\rangle, |\Phi^+\}\rangle$, respectively. Since Charlie already knows the PK, he is expecting values of the received initial states. Indubitably, Charlie will detect the modification of the initial states immediately. In the QSS phase, Eve may perform a unitary operation (e.g. $i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$) on photons in $S_c^*(S_b)$ for modifying Charlie's (Bob's) sequence without being detected. However, she will be detected easily in Step (4) (Step (2)). Therefore, the proposed scheme can efficiently resist modification attacks.

4. Efficiency Analysis

In 2000, Cabello[45] defined the information-theoretical efficiency as: $\eta = b_s/(q_t + b_t)$, where b_s is the secret bits to be received, b_t is the used classical bits between participants and q_t is the used qubits in the quantum communications. The proposed protocol's information-theoretical efficiency is $4n/(6n + 4n) = 40\%$ (note, classical bits and qubits which are used for security checks and identity authentication are not being considered). Compared to protocols in Refs. 30, 46 and 47, the efficiency performance of the proposed QSS scheme is higher than those in Refs. 46 and 47 (i.e. 33.3%), and equal to the efficiency performance registered in Ref. 30. However, the proposed scheme is more secure as it is obviously enhanced by the features of identity authentication and a prior shared key.

5. Multiparty Case

The proposed QSS scheme is easy to extend to a multiparty case. Suppose that Alice divided her secret into $N + 1$ agents, i.e. (Bob_1, Bob_2, ..., Bob_N, $Charlie$)). In the QSS phase, the boss Alice sends the sequence S_b to Bob_1, Bob_1 randomly applies a unitary operation on S_b and sends it to Bob_2, and so on until Bob_N. Finally, Bob_N randomly applies a unitary operation on his sequence and sends it to Charlie. Subsequently, Alice and Charlie carry out Step (4). Then, they move to the QD phase. As in Step (5), Bob_1 generate n initial Bell states based on the prior shared key for authenticating the identity of Bob_2. Similarly, any authenticated agent (Bob_1 or Bob_2) authenticates the identity of Bob_3 and so on until authenticating the identity of Charlie. Finally, all the agents cooperate to recover Alice's master key as in Step (5).

6. Comparisons

Comparisons are made between the proposed QSS scheme and the schemes in Refs. 27–30, 34, 46, 50, 53 and 54. The results of the comparisons are indicated in Table 1 and discussed in detail as follows.

Table 1. Comparisons between the proposed QSS protocol and previous QSS protocols.

	Quantum resource	Identity authentication	Secure against participant attack
Refs. 27, 29 and 54	Bell state	No	No
Ref. 28	Six-qubit entangled state	No	Yes
Ref. 30	Bell state	No	Yes
Ref. 35	Single photon	Yes	No
Ref. 46	GHZ state	No	No
Ref. 50	Single photon and Bell state	No	No
Ref. 53	GHZ state	Yes	Yes
The proposed scheme	Bell state	Yes	Yes

6.1. *Comparison with Ref. 27*

Du and Bao[27] presented a QSS scheme based on Bell sates, they claimed that their scheme can resist well-known attacks as well as cheating attack. However, Liu *et al.* shown in Ref. 48 that Du and Bao's scheme could not prevent participant attack. The proposed scheme can efficiently resist participant attack as Alice uses independently decoy photon sequences to protect each agent's shadow. Therefore, the secret key is transmitted securely not only against Eve's attack but also against participant attack.

6.2. *Comparison with Ref. 28*

Long *et al.*[28] proposed an efficient QSS protocol based on genuinely maximally six-qubit entangled states, where the dealer shares three classical bits among three participants using a six-qubit state. They showed that their protocol is invulnerable to eavesdropping. However, Qin and Liu[51] pointed out that Long *et al.*'s protocol suffers from partly information leaks. In contrast, the proposed scheme is secure against information leaks, where a prior shared key is used for deducing the final master key. In addition, the proposed QSS scheme adopts the process of quantum identity authentication for preventing impersonation attacks and man-in-the-middle attacks.

6.3. *Comparison with Ref. 29*

Shi *et al.*[29] introduced a high efficient QSS scheme using Bell states. In Shi *et al.*'s scheme, all the participants are not required to generate entangled states or perform a local unitary operation. However, Wang *et al.*[49] pointed out that their scheme is not secure against participant attacks, where the first participant can collaborate with last one to reveal the secret. While in the proposed scheme, revealing the secret cannot be achieved without mutual help from all participants.

6.4. *Comparison with Ref. 30*

Tan and Jiang[30] proposed a QSS scheme based on Bell states, their QSS scheme is secure against participant attacks and can reduce implementation complexity. Also, Tan and Jiang's scheme and the proposed QSS scheme have the same efficiency performance as computed in Sec. 4. However, the proposed scheme is more secure than Tan and Jiang's scheme due to the identity authentication process, where authenticating the identity of the participants is an indispensable process as a defense against man-in-the-middle attacks and impersonation attacks.[56]

6.5. *Comparison with Ref. 35*

Yang *et al.*[35] proposed two quantum identity authentication schemes based on secret sharing and single photons, where all participant can be authenticated by a trusted

third party's help. In their protocol, the third party encodes a sequence of particles with a random key and sends it to all participants, then each participant applies the corresponding sequence of unitary operations on the sequence of particles sequentially. However, Zeng and Ji[36] indicated that Yang *et al.*'s scheme is vulnerable to participant attacks, while the proposed scheme is completely secure against participant attacks as mentioned in Sec. 6.1. In addition, the security of Yang *et al.*'s scheme relies on the honesty of the third party, while the participants of the proposed scheme perform the identity authentication process by themselves. Also, Yang *et al.*'s scheme shares only classical information, while the proposed scheme shares quantum information.

6.6. *Comparison with Ref. 46*

Hwang *et al.*[46] introduced a high efficient multiparty QSS protocol using the GHZ state. According to Hwang *et al.*'s protocol, they used the dense coding scheme on GHZ states in which each GHZ state is able to carry two classical bits. Also, they proved that their protocol is secure against several kinds of attacks. However, Liu and Pan[47] pointed out that Hwang *et al.*'s protocol is insecure against participant attack, where one participant may reveal half of the secret information without performing any attack strategy. Whereas the proposed QSS scheme is secure against dishonest participant as mentioned in Secs. 6.1 and 6.3.

6.7. *Comparison with Ref. 50*

Lin and Hwang[50] presented circular QSS protocol using CNOT gate for remote agent that is secure against Trojan-horse attack, intercept-resend attack and entangled-and-measure attack. However, according to their scheme, the first agent can collaborate with the last one to obtain the secret message as pointed out in Ref. 52. In the multiparty case of the proposed scheme, any illegally attempt to recover the secret shared data will fail because each participant applies random unitary operations on his/her share before sending it to another participant. Thus, all participants must collaborate to deduce the master key.

6.8. *Comparison with Ref. 53*

Yang *et al.*[53] presented a flexible multiparty simultaneous QIA scheme based on GHZ states. According to Yang *et al.*'s protocol, the identity of the participants can be authenticated by a third party who must be trusted. While in the proposed QSS scheme, the identity authentication process is only achieved by the participants as mentioned in Sec. 6.5. Additionally, Yang *et al.*'s scheme uses GHZ states, whereas the proposed QSS scheme uses Bell states that is more simple and easy to implement. Moreover, the authentication key in Yang *et al.*'s scheme is used only for performing the identity authentication process. In contrast, the authentication key in the

proposed QSS scheme is used twice: one to authenticate the identity of participants, the second to deduce the master key.

6.9. *Comparison with Ref. 54*

Yuan *et al.*[54] presented a multiparty QSS scheme based on Bell states and using continuous variable operations. However, Zhang and Qin[55] pointed out that their scheme is not secure when the first participant is dishonest or being conspired with another participant, as opposed to the proposed QSS scheme that is proved to be secure against participant attacks as mentioned in Secs. 6.1 and 6.3.

7. Conclusion

In this work, we have proposed an authenticated QSS protocol based on Bell sates. To share a master key, Alice prepares a secret key and encodes it using unitary operations before she shares it with her agents. Before the agents authenticate their identity using a prior shared key, they encode the prior shared key using an XOR operation. Eventually, the participants perform the XOR operation on the prior shared key and the secret key to deduce Alice's master key. The proposed QSS scheme has the following features: (1) the participants authenticate their identity using a prior shared key without a help of a third party; (2) for avoiding information leakage, the participants encrypt the prior shared key before they use it in the authentication process and the security checks process. When compared to some existing QSS schemes, the proposed scheme proved an impressive performance in terms of defense against participant attack, modification attack, entangled-measure attack, man-in-the-middle attack, impersonation attack and Trojan-horse attack.

Acknowledgements

The authors would like to thank the anonymous referees for their valuable suggestions and comments that improved the clarity of the manuscript.

References

1. C. H. Bennett and G. Brassard, Quantum cryptography: Public-key distribution and coin tossing, in *Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing* (Bangalore, India, 1984), pp. 175–179.
2. P. W. Shor and J. Preskill, *Phys. Lett. A* **85** (2000) 441.
3. G. Guo and G. Guo, *Phys. Lett. A* **310** (2003) 247.
4. J. Cai, Z. Pan, T. J. Wang, S. Wang and C. Wang, *Int. J. Quantum Inform.* **14** (2016) 1650043.
5. L. Han, Y. Liu, J. Liu and Z. Zhang, *Opt. Commun.* **281** (2008) 2690.
6. X. Zou and D. Qiu, *Sci. China Phys. Mech. Astron.* **57** (2014) 1696.
7. X. Zou, D. Qiu, L. Li, L. Wu and L. Li, *Phy. Rev. A* **79** (2009) 052312.
8. X. Zou, D. Qiu, S. Zhang and P. Mateus, *Quantum Inf. Process.* **14** (2015) 2981.

9. D. Li *et al.*, *Quantum Inf. Process.* **15** (2016) 4819.
10. W. Zhang, D. Qiu and X. Zou, *Quantum Inf. Process.* **15** (2016) 2499.
11. W. Liu, Y. B. Wang and Z. T. Jiang, *Opt. Commun.* **284** (2011) 3160.
12. X. Tan and X. Zhang, *Concurrency Computat., Pract. Exper.* **28** (2016) 3006.
13. M. Hillery, V. Buẑek and A. Berthiaume, *Phys. Rev. A* **59** (1999) 1829.
14. A. Shamir, *Commun. ACM*, **22** (1979) 612.
15. W. Helwig, W. Cui, J. Latorre, A. Riera and H. Lo, *Phys. Rev. A* **86** (2012) 052335.
16. G. Gao, *Int. J. Theor. Phys.* **53** (2014) 2231.
17. L. Zhang, Y. Guo and D. Huang, *Int. J. Internet Protoc. Tech.* **8** (2014) 116.
18. H. Massoud and F. Elham, *Sci. China Phys. Mech. Astron.* **55** (2012) 1828.
19. F. Yan and T. Gao, *Phys. Rev. A* **72** (2005) 012304.
20. X. Chen, X. Niu, X. Zhou and Y. Yang, *Quantum Inf. Process.* **12** (2013) 365.
21. F. Liu, S. Qin and Q. Wen, *Phys. Scr.* **89** (2014) 075104.
22. L. Li, D. Qiu and P. Mateus, *J. Phys. A, Math. Theor.* **46** (2013) 045304.
23. C. Xie, L. Li and D. Qiu, *Int. J. Theor. Phys.* **54** (2015) 3819.
24. C. Schmid *et al.*, *Phys. Rev. Lett.* **95** (2005) 230505.
25. K. Wei, H. Ma and J. Yang, *Opt. Express* **21** (2013) 16663.
26. P. Zhou *et al.*, *Phys. A, Stat. Mech. Appl.* **381** (2007) 164.
27. Y. Du and W. Bao, *Opt. Commun.* **308** (2013) 159.
28. Y. Long, D. Qiu and D. Long, *J. Phys. A, Math. Theor.* **45** (2012) 195303.
29. R. Shi, L. Huang, W. Yang and H. Zhong, *Opt. Commun.* **283** (2010) 2476.
30. X. Tan and L. Jiang, *Int. J. Theor. Phys.* **52** (2013) 3577.
31. M. Dušek, O. Haderka, M. Hendrych and R. Myŝka, *Phys. Rev. A* **60** (1999) 149.
32. M. Curty and D. Santos, *Phys. Rev. A* **64** (2001) 062309.
33. Z. Zhang, G. Zeng, N. Zhou and J. Xiong, *Phys. Lett. A* **356** (2006) 199.
34. P. Huang, J. Zhu, Y. Lu and G. Zeng, *Int. J. Quantum Inform.* **09** (2011) 701.
35. Y. Yang, Q. Wen and X. Zhang, *Sci. China Ser. G Phys. Mech. Astron.* **51** (2008) 321.
36. X. Zhang and D. Ji, *Sci. China Ser. G Phys. Mech. Astron.* **52** (2009) 1313.
37. H. Qin, X. Zhu and Y. Dai, *Quantum Inf. Process.* **14** (2015) 2997.
38. B. Nguyen, *Phys. Lett. A* **328** (2004) 6.
39. T. Ye, *Quantum Inf. Process.* **14** (2015) 3499.
40. C. Lin, C. Yang and T. Hwang, *Int. J. Theor. Phys.* **54** (2014) 780.
41. A. Yin, Z. Tang and D. Chen, *Mod. Phys. Lett. B* **29** (2015) 1550018.
42. Q. Cai, *Phys. Lett. A* **351** (2006) 23.
43. F. Deng, X. Li, H. Zhou and Z. Zhang, *Phys. Rev. A* **72** (2005) 044302.
44. F. Deng, P. Zhou, X. Li, C. Li and H. Zhou, arXiv:quant-ph/0508168.
45. A. Cabello, *Phys. Rev. Lett.* **85** (2000) 5635.
46. T. Hwang, C. Hwang and C. Li, *Phys. Scr.* **83** (2011) 045004.
47. X. Liu and R. Pan, *Phys. Scr.* **84** (2011) 045015.
48. F. Liu, Q. Su and Wen, *Int. J. Theor. Phys.* **53** (2014) 1730.
49. T. Wang, Q. Wen and F. Zhu, *Opt. Commun.* **284** (2011) 1711.
50. J. Lin and T. Hwang, *Quantum Inf. Process.* **12** (2012) 685.
51. S. Qin and F. Liu, *Int. J. Theor. Phys.* **53** (2014) 3116.
52. Z. Zhu, A. Hu and A. Fu, *Quantum Inf. Process.* **12** (2012) 1173.
53. Y. Yang, H. Wang, X. Jia and H. Zhang, *Int. J. Theor. Phys.* **52** (2012) 524.
54. H. Yuan *et al.*, *Int. J. Theor. Phys.* **51** (2012) 3443.
55. K. Zhang and S. Qin, *Int. J. Theor. Phys.* **52** (2013) 3953.
56. H. Tilborg and S. Jajodia, *Encyclopedia of Cryptography and Security* (Springer, 2011).