International Journal of Theoretical Physics (2019) 58:3239–3251
https://doi.org/10.1007/s10773-019-04199-0

Semi-Quantum Bi-Signature Scheme Based on W States

Xing-Qiang Zhao[1] · Hua-Ying Chen[2] · Yun-Qian Wang[1] · Nan-Run Zhou[3]

Received: 18 March 2019 / Accepted: 27 June 2019 / Published online: 13 July 2019

Abstract
A semi-quantum bi-signature scheme based on W states is designed, in which two signers sign the same message. The unconditional security of the new semi-quantum bi-signature scheme is guaranteed with the teleportation of W states and semi-quantum key distribution (SQKD) protocol. From the aspects of hardware requirement and efficiency, the proposed semi-quantum bi-signature scheme is more efficient and convenient than many typical quantum signature schemes.

Keywords Quantum signature · Semi-quantum bi-signature scheme · Teleportation · W state · Semi-quantum key distribution

1 Introduction

Quantum cryptography has made a significant breakthrough, however how to ensure the authenticity of quantum information is still an essential problem. Therefore, quantum authentication [1–3] has been taken seriously. As an important part of quantum authentication, quantum signature (QS) [4–7] could solve the problem to some extent.

In 2001, Zeng et al. proposed the first quantum signature scheme based on the correlation of GHZ triplet states, which finished signature and verification with key [1]. In the same year, Gottesman and Chuang firstly brought out the idea of quantum digital signature (QDS) [8] and popularized the classical Lamport's signature scheme [9] to quantum one with quantum one-way function and quantum public-key. Since then, many kinds of quantum signature schemes have been put forward [10–14], and a number of scholars analyzed and studied these schemes [15–18]. Nevertheless, Li et al. pointed out that some security flaws still existed in some proposed quantum signature schemes [18]. In 2014, Dunjko et al. proposed one quantum signature scheme just with linear optics, where no quantum memory was required [19]. To resolve the security problem, Amiri et al. invented a secure quantum signature scheme via insecure quantum channels and the

✉ Nan-Run Zhou
nrzhou@ncu.edu.cn

[1] Department of Computer Science and Technology, Nanchang University, Nanchang 330031, China

[2] Department of Physics, Nanchang University, Nanchang 330031, China

[3] Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China

transmission of significantly fewer quantum states [20], which is unconditionally secure against most general coherent attacks. In 2018, Chen et al. proposed one public-key quantum digital signature scheme with one-time pad private-key and public-key cryptosystem [21], which was easier to realize than many other quantum signature schemes. In the same year, Guo et al. presented a trusted third-party e-payment protocol based on quantum blind signature without entanglement [22]. Inspired by Guo et al., Zhao et al. proposed the concept of "bi-signature" to realize the signature scheme, where two people sign their signatures on the same message [23]. However, it is hard to require all participants to own quantum computing ability in the above quantum protocols. Fortunately, Boyer et al. first proposed the conception of "semi-quantum" [24] and the method of semi-quantum was successfully applied into semi-quantum key distribution (SQKD) protocols [25–28] and semi-quantum key agreement (SQKA) protocols [29, 30]. Obviously, semi-quantum is also suitable for QS and the first semi-quantum bi-signature scheme with two quantum signers and just one classical verifier is designed.

The structure of this paper is as follows. In Section 2, SQKD and the teleportation of W state are introduced. In Section 3, the semi-quantum bi-signature scheme is proposed. In Section 4, the analyses of security and efficiency are provided. In Section 5, a brief conclusion is reached.

2 Preliminary Theory

2.1 Semi-Quantum Key Distribution

Semi-quantum key distribution protocols, first introduced in 2007 by Boyer et al. [24], have the same goal: the establishment of a secret key, secure against an all-powerful adversary [31]. However now, instead of allowing both A and B to manipulate quantum resources (e.g., prepare and measure qubits in a variety of bases) as is permissible in a typical QKD protocol, only A is allowed such liberties while B is limited to performing certain "classical" or "semi-quantum" operations (what operations B is limited to are discussed shortly). In this scenario, A is called the quantum user while B is called the classical user (in a fully quantum protocol, such as BB84 [32], both A and B are fully quantum).

2.2 W State

With entanglement classification [33], Dur et al. presented a class of W states [34], i.e.,

$$|W\rangle = \frac{1}{\sqrt{2\alpha+2}}\left(|100\rangle + \sqrt{\alpha}e^{i\theta_1}|010\rangle + \sqrt{\alpha+1}e^{i\theta_2}|001\rangle\right), \tag{1}$$

where α is a positive real parameter, θ_1 and θ_2 are phases. If α=1 and $\theta_1 = \theta_2 = 0$, Eq. (1) will become the most common W state:

$$|W\rangle_{123} = \frac{1}{2}\left(|100\rangle + |010\rangle + \sqrt{2}|001\rangle\right)_{123}. \tag{2}$$

If someone chooses one group of orthogonal bases [35].

$$|\kappa^{\pm}\rangle = \frac{1}{2}\Big(|010\rangle + |001\rangle \pm \sqrt{2}|100\rangle\Big), \tag{3}$$

$$|\gamma^{\pm}\rangle = \frac{1}{2}\Big(|110\rangle + |101\rangle \pm \sqrt{2}|000\rangle\Big), \tag{4}$$

and he/she makes use of these bases to measure Particles 1, 2 in $|W\rangle_{123}$ and a single particle a in state $|\varphi\rangle_a = (\alpha|0\rangle + \beta|1\rangle)_a$, then the measurement outcomes can be expressed as

$$\begin{aligned}|\varphi\rangle_a|W\rangle_{123} &= \Big(\alpha|0\rangle + \beta|1\rangle\Big)_a \otimes \frac{1}{2}\Big(|100\rangle + |010\rangle + \sqrt{2}|001\rangle\Big)_{123} \\ &= \frac{1}{2}\Big[\alpha\Big(|010\rangle + |001\rangle\Big)_{a12}|0\rangle_3 + \sqrt{2}\alpha|000\rangle_{a12}|1\rangle_3 + \\ &\quad \beta\Big(|110\rangle + |101\rangle\Big)_{a12}|0\rangle_3 + \sqrt{2}\beta|100\rangle_{a12}|1\rangle_3\Big] \\ &= \frac{1}{2}\Big[|\kappa^{+}\rangle_{a12}\Big(\alpha|0\rangle + \beta|1\rangle\Big)_3 + |\kappa^{-}\rangle_{a12}\Big(\alpha|0\rangle - \beta|1\rangle\Big)_3 + \\ &\quad |\gamma^{+}\rangle_{a12}\Big(\alpha|1\rangle + \beta|0\rangle\Big)_3 + |\gamma^{-}\rangle_{a12}\Big(-\alpha|1\rangle + \beta|0\rangle\Big)_3\Big]\end{aligned} \tag{5}$$

By recalling the four local unitary operations $\sigma_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\sigma_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\sigma_3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $\sigma_4 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, Eq. (5) can also be written as [35].

$$|\varphi\rangle_a|W\rangle_{123} = \frac{1}{2}\Big(|\kappa^{+}\rangle_{a12}\sigma_1|\varphi\rangle_3 + |\kappa^{-}\rangle_{a12}\sigma_4|\varphi\rangle_3 + |\gamma^{+}\rangle_{a12}\sigma_2|\varphi\rangle_3 + |\gamma^{-}\rangle_{a12}\sigma_3|\varphi\rangle_3\Big). \tag{6}$$

3 The Semi-Quantum Bi-Signature Scheme

In the proposed semi-quantum bi-signature scheme, signers Alice and Bob have quantum computing ability, while receiver and verifier Charlie has no quantum computing ability. Remarkably, Charlie can only measure, prepare and send particles with fixed quantum bases $\{|0\rangle, |1\rangle\}$. Eve is an impostor or attacker. M is the set of the message. The semi-quantum bi-signature scheme is composed of initialization phase, signature phase and verification phase, and the entire semi-quantum bi-signature scheme is shown in Fig. 1.

3.1 Initialization Phase

In the initialization phase, the message is processed and the states and semi-quantum keys are prepared to meet the needs of other two phases.

Step 1 Processing of the Message Alice generates Sequence s_m in a single particle state $\{s_m = |\varphi_{m_i}\rangle | i = 1, 2, \ldots, n.\}$ according to the message $M = \{m_1, m_2, \ldots, m_n\}$, $m_i \in \{0, 1\}$. If $m_i = 0$, $|\varphi_{m_i}\rangle = |0\rangle$; if $m_i = 1$, $|\varphi_{m_i}\rangle = |1\rangle$.

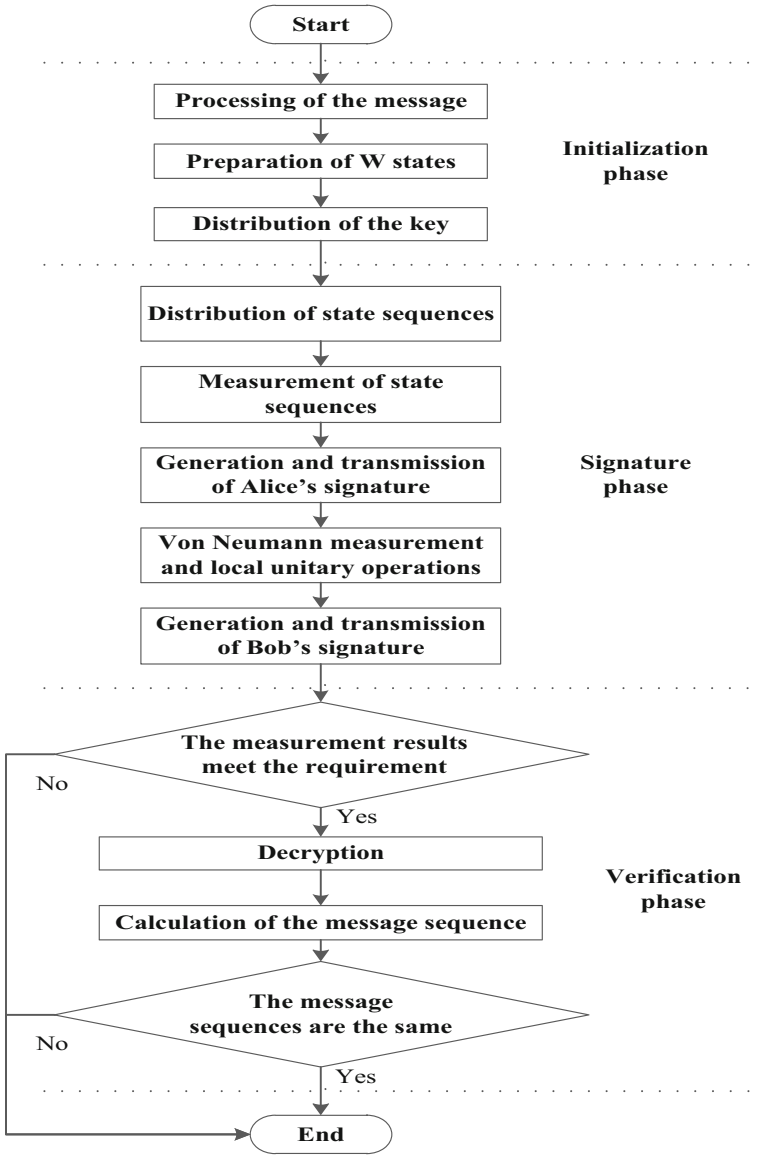

Fig. 1 Process of the semi-quantum bi-signature scheme

Step 2 Preparation of W States Bob prepares n W states as Eq. (2) and divides these states into three sequences s_1, s_2 and s_3. Alice prepares n W states as Eq. (7) and divides these states into three sequences s_4, s_5 and s_6. Besides, Sequence s_i includes all the particles labeled i in W states.

$$|W\rangle_{456} = \frac{1}{2}\left(|100\rangle + |010\rangle + \sqrt{2}|001\rangle\right)_{456}, \tag{7}$$

Step 3 Distribution of the Key Alice and Charlie have pre-shared a semi-quantum key K_{AC} as the private key while Bob and Charlie have pre-shared a private semi-quantum key K_{BC}.

Krawec's protocol [31] is adopted as the way of SQKD in this paper. Concurrently, as long as one makes use of the private semi-quantum key K_{AC} or K_{BC} to communicate, the person is honest.

3.2 Signature Phase

In this phase, the signatures of Alice and Bob are generated, and then Alice and Bob send their signatures and other messages to Charlie. The transmissions of the sequences and messages are shown in Fig. 2.

Step 1 Distribution of State Sequences Alice sends Sequences s_5 and s_6 to Bob and Charlie, respectively (Please refer to Fig. 3). Bob sends Sequences s_1 and s_2 to Alice (Please refer to Fig. 4).

Step 2 Measurement of State Sequences Alice, Bob, and Charlie measure Sequences s_4, s_5, and s_6 with Z-basis to generate the measurement results $A = \{|A_1\rangle, |A_2\rangle, \ldots, |A_n\rangle\}$, $B = \{|B_1\rangle, |B_2\rangle, \ldots, |B_n\rangle\}$ and $C = \{|C_1\rangle, |C_2\rangle, \ldots, |C_n\rangle\}$, respectively.

Step 3 Generation and Transmission of Alice's Signature Alice generates her private sequence $S_A^{'} = \{|s_A^i\rangle | i = 1, 2, \ldots, n.\}$ with measurement outcome A_i and message sequence

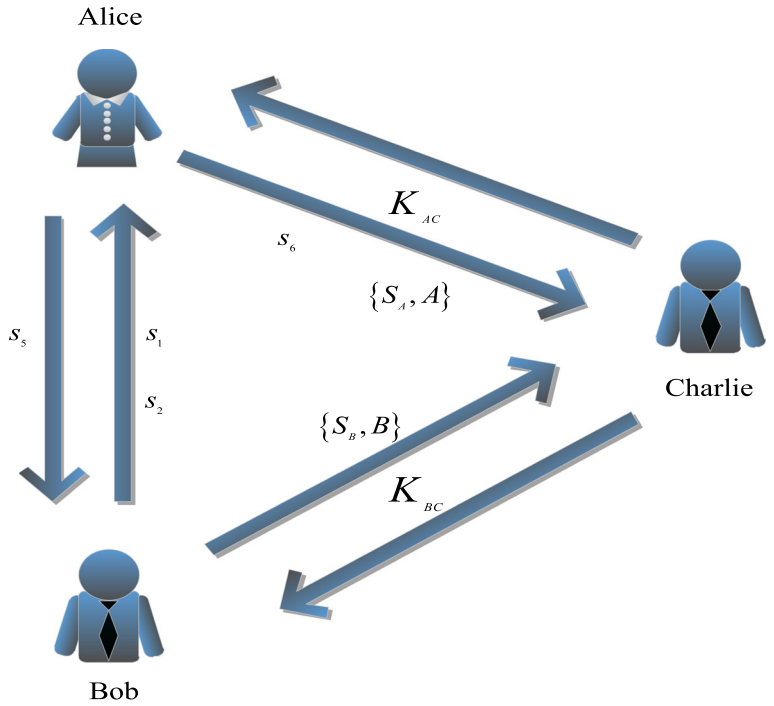

Fig. 2 The transmission of the sequences and the message

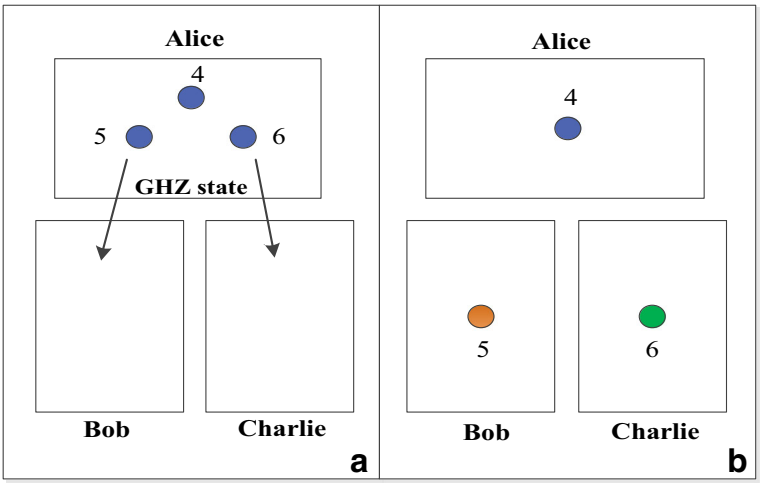

Fig. 3 Distribution of W states that Alice prepared

M, and the specific rule is shown in Table 1. Then Alice produces her signature S_A as $K_{AC} \oplus S_A^{'}$. Alice sends $\{S_A, A\}$ to Charlie.

Step 4 Von Neumann Measurement and Local Unitary Operations (a) Alice measures Sequences s_m, s_1, s_2 with the orthogonal bases $\{|\kappa^{\pm}\rangle, |\gamma^{\pm}\rangle\}$ (Please refer to Fig. 5) and tells Bob the measurement results. (b) According to Alice's measurement outcomes, Bob chooses the local operation from $\{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ and executes it on the state in Sequence s_3 one by one, then Sequence s_3 can be converted to s_m. (d) Bob measures Sequence s_m with Z-basis and gains the message sequence M.

Step 5 Generation and Transmission of Bob's Signature (a) Bob generates his private sequence $S_B^{'} = \{|s_B^i\rangle | i = 1, 2, \ldots, n.\}$ with measurement outcome B_i and message sequence M, the specific signature rule is same as that of Alice. (b) Bob encrypts the private sequence $S_B^{'}$ with K_{BC} to generate his signature $S_B = K_{BC} \oplus S_B^{'}$. (c) Bob sends $\{S_B, B\}$ to Charlie.

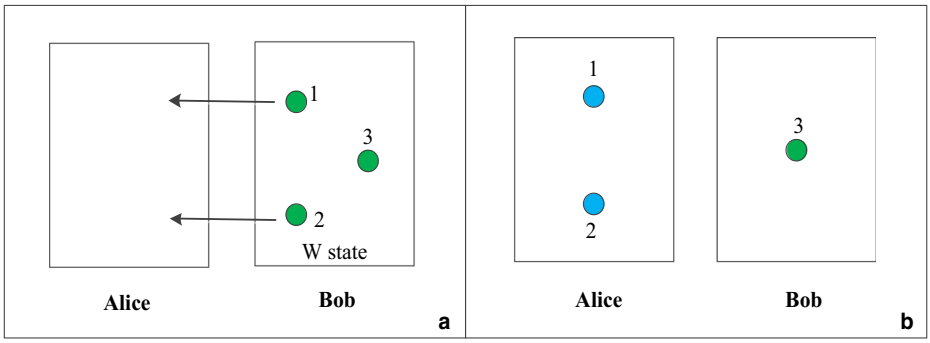

Fig. 4 Distribution of W states that Bob prepared

Table 1 The specific signature rule

	$m_i = 0$	$m_i = 1$
$A_i = 0$	$s_A^i = 1$	$s_A^i = 0$
$A_i = 1$	$s_A^i = 0$	$s_A^i = 1$

3.3 Verification Phase

In this phase, Charlie verifies the signatures of Alice and Bob.

Step 1 Comparison of Measurement Results Charlie compares the measurements A, B and C to determine whether the measurements meet the measurement requirement of W state. If the measurements do not satisfy the requirement, the signatures are both abandoned; otherwise, Charlie performs the next step.

Step 2 Decryption Charlie produces Sequences $S_A^{'}$ and $S_B^{'}$ by decrypting S_A and S_B with K_{AC} and K_{BC}, respectively.

Step 3 Calculation of the Message Sequence Charlie calculates the message sequence M_A of Alice by Sequences $S_A^{'}$ and A while he estimates the message sequence M_B of Bob by Sequences $S_B^{'}$ and B.

Step 4 Comparison of Message Sequences Charlie compares two message sequences M_A and M_B. If M_A is same as M_B, Charlie accepts the signatures of Alice and Bob; otherwise, he refuses these two signatures. Then Charlie sends Alice and Bob $K_{AC} \oplus M_A$ and $K_{BC} \oplus M_B$, respectively.

4 Security Analysis and Discussion

4.1 Security against Forgery

Generally, Eve has three possible ways to forge signatures in the proposed semi-quantum bi-signature scheme.

Eve may forge a new signature and replace the signature of Alice or Bob with her own one after she captures the message from Alice or Bob. If Eve attempts to achieve her purpose, she

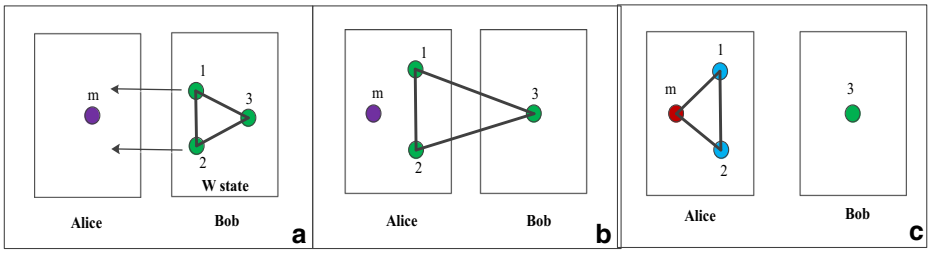

Fig. 5 Process of Von Neumann measurement

has to obtain the message sequence M. However, it is known that Eve cannot gain the message sequence M since it is transmitted by the teleportation of W state. Zhou et al. [36] have proved the teleportation of W state proposed by Agrawal [35] is secure and correct.

Eve may generate a signature of her chosen message to replace the signature of Alice or Bob. Since Eve doesn't know the length of the message sequence M, she can only intercept $\{S_A, A\}$ or $\{S_B, B\}$ to achieve her goal. Obviously, Eve can gain nothing from S_A or S_B since she does not know the key K_{AC} or K_{BC}. Therefore, Eve can only utilize the measurement sequence A or B and her chosen message M_{Eve} to forge the signature of Alice or Bob, and the probability that she can achieve her purpose is

$$\rho_1 = \frac{1}{2^n}. \tag{8}$$

Since the number n is big enough, the probability $\rho_1 \approx 0$.

Eve may intercept the signature of Alice or Bob and send Charlie a new signature. However, the signatures of Alice and Bob are sequences encrypted and Eve knows nothing about the keys K_{AC} and K_{BC}. Apparently, Eve cannot forge the signature of Alice or Bob by intercepting the encrypted sequence S_A or S_B directly.

In addition, the identities of the participants have been verified during the distribution phase of semi-quantum keys K_{AC} and K_{BC}. In other words, if one can correctly communicate with the private semi-quantum key K_{AC} or K_{BC}, he/she is honest.

Therefore, the proposed semi-quantum bi-signature scheme can effectively resist the forgery attack.

4.2 Security against Repudiation

Non-repudiation is an important aspect of the signature scheme. In the proposed semi-quantum bi-signature scheme, Alice and Bob must not deny what they have signed on some previous information. Firstly, the signatures of Alice and Bob are encrypted by the private keys K_{AC} and K_{BC}, so they cannot disavow that they have utilized the keys. Secondly, Alice and Bob transmit the message sequence M by the teleportation of W state and they cannot repudiate the collapse of W state. Likewise, Alice, Bob and Charlie have one sequence of W states respectively, and they cannot disaffirm the collapse of W state.

Concurrently, Charlie cannot repudiate that he has received the signatures of Alice and Bob. On the one hand, in Step 4 of the verification phase, Charlie sends Alice and Bob the messages $K_{AC} \oplus M_A$ and $K_{BC} \oplus M_B$ respectively, so he cannot deny the application of the keys K_{AC} and K_{BC}. On the other hand, Charlie cannot disavow the collapse of W state.

Therefore, the proposed semi-quantum bi-signature scheme can effectively resist the repudiation of signers and verifier.

4.3 Security against Intercept-Resend Attack

On the one hand, Eve may intercept sequences s_1 and s_2 to steal the message. Nevertheless, the message is transmitted by the teleportation of W state. Thus Eve cannot steal any information of the real message by intercepting the sequences s_1 and s_2 according to [36].

On the other hand, Eve may intercept sequences s_5 and s_6 to steal the real message. For instance, if Eve prepares two auxiliary state sequences in the states $|\varphi\rangle_E^1 = \alpha_1|0\rangle + \beta_1|1\rangle$

($|\alpha_1|^2+|\beta_1|^2=1$) and $|\varphi\rangle_E^2=\alpha_2|0\rangle+\beta_2|1\rangle$ ($|\alpha_2|^2+|\beta_2|^2=1$), respectively. After intercepting state sequences s_5 and s_6, Eve sends these two auxiliary state sequences to Bob and Charlie, respectively. But when Bob and Charlie receive these two state sequences, they will measure them with corresponding bases, respectively. After measuring the states, Bob and Charlie can obtain the measurement outcomes $\{|0\rangle,|1\rangle\}$ of Sequence s_5 and s_6 with probability $|\alpha_1|^2$, $|\beta_1|^2$ and $|\alpha_2|^2$, $|\beta_2|^2$, respectively. Apparently, the error rates for Eve are $|\alpha_1|^2$, $|\beta_1|^2$ of Sequence s_5 and $|\alpha_2|^2$, $|\beta_2|^2$ of Sequence s_6, respectively. Afterwards, the information of Bob (Charlie) can be expressed as [37]:

$$H_{e,i}(B)=H_{e,i}(C)=-|a_i|^2\log_2|a_i|^2-|\beta_i|^2\log_2|\beta_i|^2\leq 1\text{bit},\ (i=1,2.) \tag{9}$$

where $H_{e,i}(X)$ denotes the Shannon entropy. According to the definition, the Shannon entropy can be expressed as:

$$H(X)=-\sum_x p_x\log_2 p_x. \tag{10}$$

where X is a variable and p_x is the presence probability of X [38]. From Eq. (10), it can be obtained that $H_{e,i}(B)=H_{e,i}(C)=1$ if and only if $|\alpha_i|^2=|\beta_i|^2=\frac{1}{2}$. If Eve intercepts Sequences s_5 and s_6, the mutual information between Alice and Bob (Charlie) is

$$I_e(A,B)=H_e(B)-H_e(B|A)<H_e(B)\leq 1\text{ bit}, \tag{11}$$

$$I_e(A,C)=H_e(C)-H_e(\mathrm{C}|A)<H_e(C)\leq 1\text{ bit}, \tag{12}$$

where $H_e(B|A)$ and $H_e(\mathrm{C}|A)$ denote conditional entropy and $H_e(B|A)>0$, $H_e(\mathrm{C}|A)>0$.

According to the Holevo limit [38], if there is no eavesdropper, the mutual information between Alice and Bob (Charlie) is

$$I(A,B)=I(A,C)\leq S(\rho)-\sum_x p_x S(\rho_x), \tag{13}$$

where $S(\rho)=-\mathrm{tr}(\rho\log_2\rho)$ is the von Neumann entropy of state $\rho=\sum_x p_x\rho_x$. If Eve does not intercept Sequences s_5 and s_6, the mutual information between Alice and Bob (Charlie) is

$$I(A,B)=I(A,C)=S(\rho)=-\sum_x \lambda_x\log_2\lambda_x=1\text{ bit}, \tag{14}$$

where λ_x denotes the eigenvalue of state ρ. From Eqs. (11)–(14), it is clear that

$$I_e(A,B)<I(A,B). \tag{15}$$

$$I_e(A,C)<I(A,C). \tag{16}$$

Obviously, the mutual information between Alice and Bob (Charlie) under eavesdropping will be less than that without eavesdropping.

The proposed semi-quantum bi-signature scheme can effectively resist the intercept-resend attack.

4.4 Security against Entangle-Measure Attack

If Eve wants to destroy the signature scheme by the entangle-measure attack, she can only intercept Sequence s_5 or s_6 and entangle it with a pre-prepared intermediate state sequence. After that, Eve resends the intercepted sequence to the corresponding receiver. When the whole semi-quantum bi-signature scheme is finished, Eve measures the intermediate state sequence to extract some useful information about the signature of Alice or Bob. Without loss of generality, Eve's unitary operation U_e can be described as

$$U_e|0\rangle|E\rangle = a_e|0\rangle|e_{00}\rangle + b_e|1\rangle|e_{01}\rangle, \tag{17}$$

$$U_e|1\rangle|E\rangle = c_e|0\rangle|e_{10}\rangle + d_e|1\rangle|e_{11}\rangle, \tag{18}$$

where $|e_{00}\rangle$, $|e_{01}\rangle$, $|e_{10}\rangle$ and $|e_{11}\rangle$ are pure states and $|a_e|^2 + |b_e|^2 = 1$, $|c_e|^2 + |d_e|^2 = 1$. According to the analyses in Ref. [39], it is clear that

$$I_E(A,B) = I_E(A,C) < I_{e,1}(A,B) = I_{e,1}(A,C), \tag{19}$$

where $I_E(A,B)$ and $I_E(A,C)$ denote the mutual information between Alice and Bob and the mutual information between Alice and Charlie, respectively.

From Eq. (19), it is apparent that the mutual information with eavesdropping will be less than that without eavesdropping. Apparently, the proposed semi-quantum bi-signature scheme can resist the entangle-measure attack effectively.

4.5 Security Analysis of Semi-Quantum Key

The semi-quantum keys are generated with the protocol proposed in Ref. [31], and Krawec provided the security proof of the SQKD protocol. Besides, Krawec derived a new lower bound on the key rate in the asymptotic scenario and the adopted protocol can tolerate higher rates of error than previously thought.

4.6 Comparison with Typical Signature Schemes

The efficiency of the proposed semi-quantum bi-signature scheme can be calculated with the definition $\eta = \frac{b_s}{q_t + b_t}$ [38], where b_s represents the number of useful particles while q_t and b_t denote the total amount of used qubits and the total number of classical bits, respectively. Thus, the efficiency of the proposed bi-signature scheme is $\eta = \frac{2n+2n+2n}{2n+n+3n+3n} = \frac{2}{3} \approx 66.7\%$. Since the teleportation of W state makes full use of the qubits and classical bits, the efficiency of the proposed semi-quantum bi-signature scheme is relatively high. Comparisons of some typical quantum signature schemes or public-key schemes are collected in Table 2, where C and Q denote classical space and quantum space, respectively. If all the participants are quantum parties, the participant attribute is "quantum"; if there is a participant without quantum capability, the participant attribute is "semi-quantum".

It is shown that all the participants are quantum parties in most typical quantum signature schemes while only the two signers are quantum parties in the proposed semi-quantum bi-signature scheme, which reduces the hardware requirements in implementing signature. Since

Table 2 Comparison with typical quantum signature schemes

Scheme	Message space	Signature space	Participant attribute	Symmetry	Efficiency
Ref. [1]	Q	Q	quantum	asymmetric	50%
Ref. [10]	Q	Q	quantum	asymmetric	50%
Ref. [18]	Q	Q	quantum	symmetric	57.1%
Ref. [19]	C	Q	quantum	symmetric	50%
Proposed scheme	C	Q	semi-quantum	asymmetric	66.7%

the proposed semi-quantum bi-signature scheme transmits message with the teleportation of W state rather than with more qubits or classical bits, it is more efficient than some typical quantum signature schemes.

5 Conclusion

Based on the correlation of W state and the teleportation of W state, a semi-quantum bi-signature scheme is designed. Compared with previous quantum signature schemes, the semi-quantum bi-signature scheme with two signers who sign one same message is more useful in real life. The unconditional security is guaranteed by the teleportation of W states and semi-quantum key distribution, and security analyses show that the proposed semi-quantum bi-signature scheme can resist most attacks effectively. Remarkably, the proposed semi-quantum bi-signature scheme is more efficient and convenient than some typical quantum signature schemes.

Acknowledgements This work is supported by the National Natural Science Foundation of China (Grant Nos. 61871205 and 61561033), the Major Academic Discipline and Technical Leader of Jiangxi Province (Grant No. 20162BCB22011), and the Innovation Special Foundation of Graduate Student of Jiangxi Province (Grant No. YC2018-B005).

References

1. Zeng, G., Ma, W., Wang, X., Zhu, H.: Signature scheme based on quantum cryptography [J]. Acta Electron. Sin. **29**(8), 1098–1100 (2001)
2. Nikolopoulos, G.M.: Continuous-variable quantum authentication of physical unclonable keys: security against an emulation attack [J]. Phys. Rev. A. **97**(1), 012324 (2018)
3. Liu, B., Gao, Z., Xiao, D., Huang, W., Liu, X., Xu, B.: Quantum identity authentication in the orthogonal-state-encoding QKD system [J]. Quantum Inf. Process. **18**(5), 137 (2019)
4. Li, Q., Chan, W.H., Long, D.Y.: Arbitrated quantum signature scheme using bell states [J]. Phys. Rev. A. **79**(5), 054307 (2009)
5. Zhang, L., Sun, H.W., Zhang, K.J., Jia, H.Y.: An improved arbitrated quantum signature protocol based on the key-controlled chained CNOT encryption [J]. Quantum Inf. Process. **16**(3), 70 (2017)
6. Yoo, Y., Azarderakhsh, R., Jalali, A., Jao, D., Soukharev, V.: A post-quantum digital signature scheme based on supersingular isogenies [C]. In: International Conference on Financial Cryptography and Data Security, pp. 163–181. Springer, Cham (2017)
7. Safaei, S., Mazziotti, D.A.: Quantum signature of exciton condensation [J]. Phys. Rev. B. **98**(4), 045122 (2018)
8. Gottesman, D., Chuang, I.: Quantum digital signatures [J]. arXiv preprint quant-ph/0105032 (2001)
9. Lamport, L.: Constructing digital signatures from a one-way function [R]. In: Palo Alto: Technical Report CSL-98, SRI International (1979)

10. Zhou, J.X., Zhou, Y.J., Niu, X.X., Yang, Y.X.: Quantum proxy signature scheme with public verifiability [J]. Sci. Chin. Phys. Mechanics and Astronomy. **54**(10), 1828–1832 (2011)
11. Yang, Y.G., Lei, H., Liu, Z.C., Zhou, Y.H., Shi, W.M.: Arbitrated quantum signature scheme based on cluster states [J]. Quantum Inf. Process. **15**(6), 2487–2497 (2016)
12. Li, W., Shi, J., Shi, R., Guo, Y.: Blind quantum signature with controlled four-particle cluster states [J]. Int. J. Theor. Phys. **56**(8), 2579–2587 (2017)
13. Y, Y., Shi, R.H., Guo, Y.: Arbitrated quantum signature scheme with continuous-variable squeezed vacuum states [J]. Chin. Phys. B. **27**(2), 020302 (2018)
14. El Bansarkhani, R., Misoczki, R.G.-M.: A hash-based group signature scheme from standard assumptions [C]. In: International Conference on Post-Quantum Cryptography, pp. 441–463. Springer, Cham (2018)
15. Zou, X., Qiu, D.: Security analysis and improvements of arbitrated quantum signature schemes [J]. Phys. Rev. A. **82**(4), 042325 (2010)
16. Choi, J.W., Chang, K.Y., Hong, D.: Security problem on arbitrated quantum signature schemes [J]. Phys. Rev. A. **84**(6), 062330 (2011)
17. Gao, F., Qin, S.J., Guo, F.Z., Wen, Q.Y.: Cryptanalysis of the arbitrated quantum signature protocols [J]. Phys. Rev. A. **84**(2), 022344 (2011)
18. Li, Q., Li, C., Wen, Z., Zhao, W., Chan, W.H.: On the security of arbitrated quantum signature schemes [J]. J. Phys. A-Math. Theor. **46**(1), 015307 (2012)
19. Dunjko, V., Wallden, P., Andersson, E.: Quantum digital signatures without quantum memory [J]. Phys. Rev. Lett. **112**(4), 040502 (2014)
20. Amiri, R., Wallden, P., Kent, A., Andersson, E.: Secure quantum signatures using insecure quantum channels [J]. Phys. Rev. A. **93**(3), 032325 (2016)
21. Chen, F.L., Liu, W.F., Chen, S.G., Wang, Z.H.: Public-key quantum digital signature scheme with one-time pad private-key [J]. Quantum Inf. Process. **17**(1), 10 (2018)
22. Guo, X., Zhang, J.Z., Xie, S.C.: A trusted third-party e-payment protocol based on quantum blind signature without entanglement [J]. Int. J. Theor. Phys. **57**(9), 2657–2664 (2018)
23. Zhao, X.Q., Wang, Y.Q., Gong, L.H., Zeng, Q.W.: New bi-signature scheme based on GHZ states and W states [J]. Int. J. Theor. Phys. **58**(5), 1555–1567 (2019)
24. Boyer, M., Kenigsberg, D., Mor, T.: Quantum key distribution with classical bob [J]. Phys. Rev. Lett. **99**(14), 140501 (2007)
25. Tan, Y.G., Lu, H., Cai, Q.Y.: Comment on "quantum key distribution with classical bob" [J]. Phys. Rev. Lett. **102**(9), 098901 (2009)
26. Li, C., Yu, K.F., Kao, S., Hwang, T.: Authenticated semi-quantum key distributions without classical channel [J]. Quantum Inf. Process. **15**(7), 2881–2893 (2016)
27. Liu, Z.R., Hwang, T.: Mediated semi-quantum key distribution without invoking quantum measurement [J]. Ann. Phys. **530**(4), 1700206 (2018)
28. Zhu, K.N., Zhou, N.R., Wang, Y.Q., Wen, X.J.: Semi-quantum key distribution protocols with GHZ states [J]. Int. J. Theor. Phys. **57**(12), 3621–3631 (2018)
29. Shukla, C., Thapliyal, K., Pathak, A.: Semi-quantum communication: protocols for key agreement, controlled secure direct communication and dialogue [J]. Quantum Inf. Process. **16**(12), 295 (2017)
30. Liu, W.J., Chen, Z.Y., Ji, S., Wang, H.B., Zhang, J.: Multi-party semi-quantum key agreement with delegating quantum computation [J]. Int. J. Theor. Phys. **56**(10), 3164–3174 (2017)
31. Krawec, W. O: An improved asymptotic key rate bound for a mediated semi-qauntum key distribution protocol [J]. arXiv preprint arXiv:1509.04797 (2015)
32. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing [C]. In: Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, pp. 175–179, Bangalore (1984)
33. Nielsen, M.A.: Conditions for a class of entanglement transformations [J]. Phys. Rev. Lett. **83**(2), 436–439 (1999)
34. Dür, W., Vidal, G., Cirac, J.I.: Three qubits can be entangled in two inequivalent ways [J]. Phys. Rev. A. **62**(6), 062314 (2000)
35. Agrawal, P., Pati, A.: Perfect teleportation and superdense coding with W states [J]. Phys. Rev. A. **74**(6), 062320 (2006)

36. Zhou, Y.S., Wang, F., Luo, M.X.: Efficient superdense coding with W states [J]. Int. J. Theor. Phys. **57**(7), 1935–1941 (2018)
37. Zhou, N.R., Wang, L.J., Gong, L.H., Zuo, X.W., Liu, Y.: Quantum deterministic key distribution protocols based on teleportation and entanglement swapping [J]. Opt. Commun. **284**(19), 4836–4842 (2011)
38. Cabello, A.: Quantum key distribution in the Holevo limit [J]. Phys. Rev. A. **85**(26), 5635 (2000)
39. Zhao, X.Q., Zhou, N.R., Chen, H.Y., Gong, L.H.: Multiparty quantum key agreement protocol with entanglement swapping [J]. Int. J. Theor. Phys. **58**(2), 436–450 (2019)