An Arbitrated Quantum Signature Scheme Based on W States

Yu-ting Jiang and Zhi-wen Mo(✉)

College of Mathematics and Software Science, Sichuan Normal University, Chengdu 610066, China
mozhiwe@sicnu.edu.cn

Abstract. Arbitrated quantum signature(AQS) is a cryptographic scenario. There are three participants in this scheme. Sender(signer) Alice generates the signature of a message. Receiver(verifier) Bob verifies the signature. A trusted arbitrator helps Bob verify the signature. In this paper, we propose an arbitrated quantum signature scheme with W states. The W states are used for quantum signature and verification. The W states have stronger robustness than the GHZ states in the loss of the quantum bits. Finally, we also discuss its security against forgery and disavowal.

Keywords: Quantum cryptography · Quantum signature · Arbitrated quantum signature · W states

1 Introduction

Quantum cryptography is new cross subject with the combination of classic cryptography and quantum information. It is a new type of cryptographic system that uses quantum effects to realize the information exchange of unconditional security. The ideology of quantum cryptography can be traced back to the earliest Wiesner Stephen article in 1983 [1]. Bennet et al. designed the first quantum cryptography scheme named BB84 [2]. Since then, quantum cryptography has developed rapidly. Quite a few branches of quantum cryptography have been pointed out, including quantum key distribution(QKD) [3–7], quantum secure direct communication(QSDC) [8–11], quantum secret sharing(QSS) [12–15] and so on.

The principle of quantum signature is a combination of quantum theory and the principle of digital signature. Gotteman et al. [16] and Buhrman et al. [17] proposed quantum digital signatures in 2001. Zeng and Keitel proposed and designed the first arbitration quantum signature scheme by using the classical signature and the entanglement of the Greenberger-Horne-Zeilinger(GHZ) triplet states [18]. Li et al. modified the signature of Zeng and Keitel by using Bell states instead of GHZ states, which is more efficient and more convenient [19]. Zou and Qiu proposed an AQS scheme with a public board which can avoid being disavowed for the integrality of the signature by Bob [20]. With the continuous

B.-Y. Cao (ed.), *Fuzzy Information and Engineering and Decision*,
Advances in Intelligent Systems and Computing 646, DOI 10.1007/978-3-319-66514-6_12

development and application of the arbitration quantum signature, many practical quantum signature protocols have been put forward, such as quantum proxy signature [21,22] ,quantum group signature [23,24], quantum blind signature [25,26], quantum multi signature [27,28], etc.

In 2000, Dür et al. proposed a new entangled state, and found that the W states have stronger robustness than the GHZ states in the loss of the quantum bits [29]. In the case of the loss of particles, the W states can maintain the quantum entanglement properties well. In this paper, we propose an arbitrated quantum signature scheme based on W states with public board. And we also discuss its security against forgery and disavowal.

This paper is arranged as follows. In Sect. 2, we introduce the general principle we demand for this AQS scheme. In Sect. 3, we describe the basic scheme including an initial phase, a signing phase and a verifying phase. In Sect. 4, we make security analyses on the proposed scheme to show neither to be disavowed by the signatory nor to be deniable for the receiver. In Sect. 5, we give a brief conclusion.

2 Preliminaries

There are four Bell basis shown as below

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

There are three participants in the protocol, the signer Alice, the receiver Bob and the arbitrator Trent. Alice need to sign the message $|P\rangle$ with a appropriate signature $|S\rangle$. We assume n qubits in the string, such that $|P\rangle = (|p_1\rangle, |p_2\rangle, \cdots, |p_n\rangle)$. Any qubit $|p_i\rangle$ can be expressed as below

$$|p_i\rangle = \alpha_i|0\rangle + \beta_i|1\rangle \tag{2}$$

where α_i, β_i are complex numbers with $|\alpha_i|^2 + |\beta_i|^2 = 1$. And $|P\rangle$ can be known or unknown. In advance, three participants share a three-particle W state

$$|\varphi\rangle_{ATB} = \frac{1}{2}(|000\rangle + |110\rangle + |101\rangle + |011\rangle)_{ATB} \tag{3}$$

where the subscripts A correspond to Alice, T correspond to Trent and B correspond to Bob. Alice implements a Bell measurement on $|p_i\rangle$ and the particle she owns in W state, the system is expressed as follows

$$\begin{aligned}|\Psi\rangle_{iATB} &= |p_i\rangle \otimes |\varphi\rangle_{ATB} \\ &= \frac{1}{2\sqrt{2}}\{|\phi^+\rangle_A[\alpha_i(|00\rangle + |11\rangle)_{TB} + \beta_i(|10\rangle + |01\rangle)_{TB}] \\ &\quad + |\phi^-\rangle_A[\alpha_i(|00\rangle + |11\rangle)_{TB} - \beta_i(|10\rangle + |01\rangle)_{TB}] \\ &\quad + |\psi^+\rangle_A[\alpha_i(|10\rangle + |01\rangle)_{TB} + \beta_i(|00\rangle + |11\rangle)_{TB}] \\ &\quad + |\psi^-\rangle_A[\alpha_i(|10\rangle + |01\rangle)_{TB} - \beta_i(|00\rangle + |11\rangle)_{TB}]\}\end{aligned} \tag{4}$$

where $|\phi^+\rangle_A, |\phi^-\rangle_A, |\psi^+\rangle_A, |\psi^-\rangle_A$ represent the Bell states in Eq. (1). At present, Trent uses $\{|0\rangle, |1\rangle\}$ in the basis to implement a single-measurement, and sends the outcomes to Bob. Then, Bob can apply a proper unitary operation to recover the message.

Suppose Alice's measurement result is $|\phi^+\rangle_A$. After the Trent's measurement, the particles of Trent and Bob collapse into the state as follows

$$|0\rangle_T(\alpha_i|0\rangle + \beta_i|1\rangle)_B + |1\rangle_T(\alpha_i|1\rangle + \beta_i|0\rangle)_B \tag{5}$$

If Trent's measurement result is $|0\rangle$, Bob's particle will be $\alpha_i|0\rangle + \beta_i|1\rangle$. Bob can use local unitary operation I to recover the message $|p_i\rangle$. If Trent's measurement result is $|1\rangle$, Bob's particle will be $\alpha_i|1\rangle + \beta_i|0\rangle$. Bob can use unitary operation σ_x to recover the message $|p_i\rangle$, where

$$\begin{aligned} I &= |0\rangle\langle 0| + |1\rangle\langle 1| \\ \sigma_x &= |0\rangle\langle 1| + |1\rangle\langle 0| \\ i\sigma_y &= |0\rangle\langle 1| - |1\rangle\langle 0| \\ \sigma_z &= |0\rangle\langle 0| - |1\rangle\langle 1| \end{aligned} \tag{6}$$

All possibilities of the scheme are shown in Table 1. $|M_A\rangle$ means Alice's measurement results in Table 1. $|M_T\rangle$ means Trent's measurement result. $|\phi_B\rangle$ means Bob's collapse state and U_B means the unitary operation which Bob needs to recover the Alice's message.

Table 1. Relation between the local unitary operations and measurement results

$\|M_A\rangle$	$\|M_T\rangle$	$\|\phi_B\rangle$	U_B
$\|\phi^+\rangle_A$	$\|0\rangle_T/\|1\rangle_T$	$\alpha\|0\rangle + \beta\|1\rangle/\alpha\|1\rangle + \beta\|0\rangle$	I/σ_x
$\|\phi^-\rangle_A$	$\|0\rangle_T/\|1\rangle_T$	$\alpha\|0\rangle - \beta\|1\rangle/\alpha\|1\rangle - \beta\|0\rangle$	$\sigma_z/i\sigma_y$
$\|\psi^+\rangle_A$	$\|0\rangle_T/\|1\rangle_T$	$\alpha\|1\rangle + \beta\|0\rangle/\alpha\|0\rangle + \beta\|1\rangle$	σ_x/I
$\|\psi^-\rangle_A$	$\|0\rangle_T/\|1\rangle_T$	$\alpha\|1\rangle - \beta\|0\rangle/\alpha\|0\rangle - \beta\|1\rangle$	$i\sigma_y/\sigma_z$

3 Arbitrated Quantum Signature Based on W States

There are three participants in the protocol, the signer Alice, the receiver Bob and the arbitrator Trent. Trent is absolutely trusted by Alice and Bob. The two sides share classical keys with arbitrator respectively. The key is stored by the communication terminal, which can be used for a long time. We also use public board to avoid being disavowed by Bob. The presented scheme includes three phases, initializing phase, signing phase, and verifying phase.

3.1 Initializing Phase

Step $I1$. Alice shares the secret keys K_A with arbitrator Trent through the quantum key distribution [3–7], which were proved to be unconditionally secure [7,30]. Similarly, Bob shares the secret keys K_B with Trent.

Step $I2$. Trent generates n W triplet states $|\varphi\rangle_{ATB} = (|\varphi_1\rangle, |\varphi_2\rangle, \cdots, |\varphi_n\rangle).|\varphi_i\rangle$ is the same as Eq.(3).

$$|\varphi_i\rangle_{ATB} = \frac{1}{2}(|000\rangle + |110\rangle + |101\rangle + |011\rangle)_{ATB} \tag{7}$$

where the subscripts A, T and B correspond to Alice, Trent and Bob. Trent distributes corresponding particles to Alice and Bob.

Step $S1$. Alice need to sign a qubit string $|P\rangle = (|p_1\rangle, |p_2\rangle, \cdots, |p_n\rangle)$ related to the message with $|p_i\rangle = \alpha_i|0\rangle + \beta_i|1\rangle$. Alice prepares three copies of $|P\rangle$ necessarily. Then, Alice uses four unitary operators on the $|P\rangle$ for local operation.

$$|P'\rangle = \sigma|P\rangle = (\sigma_1|p_1\rangle, \sigma_2|p_2\rangle, \cdots, \sigma_n|p_n\rangle) \tag{8}$$

where $\sigma_i \in \{I, \sigma_x, i\sigma_y, \sigma_z\}, i = 1, 2, \cdots, n$. Here notice that $|P'\rangle$ return to the original states perfectly because of Hermitian conjugate operators of unitary operators, while measurement operations are not usually reversible.

Step $S2$. Alice transforms the qubit string $|P'\rangle$ into a secret qubit string $|R_A\rangle$ in terms of the key K_A.

$$|R_A\rangle = E_{K_A}|P'\rangle \tag{9}$$

For example, assume that the key K_A is related to a collection of unitary operators $R_{K_A} = (R^1_{K^1_A}, R^2_{K^2_A}, \cdots, R^n_{K^n_A})$. If $R^i_{K^i_A} = 0$, Alice applies the unitary operation σ_x, namely, $R^i_{K^i_A} = \sigma_x$. If $R^i_{K^i_A} = 1$, Alice applies the unitary operation σ_z, namely, $R^i_{K^i_A} = \sigma_z$. So $|R_A\rangle = R_{K_A}(P) = (|r_1\rangle, |r_2\rangle, \cdots, |r_n\rangle)$ with $|r_i\rangle = M^i_{K^i_A}(p_i)$.

Step $S3$. Alice combines each secret message state $|P'\rangle$ and the W states. Then, she implements a Bell measurement on her particles. It shows in Eq.(4). And she can obtain $|M_A\rangle = (|M^1_A\rangle, |M^2_A\rangle, \cdots, |M^n_A\rangle)$, where $|M^i_A\rangle$ represents one of the four Bell states in Eq.(1).

Step $S4$. Alice generates the signature $|S'\rangle = E_{K_A}(|M_A\rangle, |R_A\rangle)$ of the message $|P'\rangle$ with the secret key K_A by using the quantum one-time pad algorithm.
Step $S5$. Alice transmits the signature $|S'\rangle$ and $|P'\rangle$ to Bob.

3.2 Verifying Phase

Step $V1$. Bob encrypts $|S'\rangle$ and $|P'\rangle$ with the secret key K_B and sends the resultant outcomes $|Y_B\rangle = E_{K_B}(|S'\rangle, |P'\rangle)$ to the arbitrator Trent.
Step $V2$. Trent decrypts with K_B and gets $|S\prime\rangle$ and $|P'\rangle$. Then he decrypts $|S'\rangle$ with K_A and gets $|M_A\rangle$ and $|R_A\rangle$. Trent encrypts $|P'\rangle$ by using K_A and gets $|R'_A\rangle$. The operation is same as Alice in Step $S2$. Then Trent compares $|R_A\rangle$ with $|R'_A\rangle$ through swap [17]. If $R_A\rangle = |R'_A\rangle$, Trent sets the verification parameter $r = 1$; otherwise, he sets $r = 0$.
Step $V3$. Trent implements a measurement in the basis $\{|0\rangle, |1\rangle\}$ and obtains $|M_T\rangle = (|M_T^1\rangle, |M_T^2\rangle, \cdots, |M_T^n\rangle)$. All possibilities of the measurement results are shown in Table 1.
Step $V4$. Trent sends the encrypted results $|Y_T\rangle = E_{K_B}(|S'\rangle, |P'\rangle, |R'_A\rangle, |M_T\rangle, r)$ to Bob.
Step $V5$. Bob decrypts $|Y_T\rangle$ and gets $|S'\rangle, |P'\rangle, |R'_A\rangle, |M_T\rangle$ and r. If $r = 0$, obviously the signature has been forged and Bob rejects it directly. If $r = 1$, Bob goes on the next step.
Step $V6$. Bob combines the $|R'_A\rangle$ and $|M_T\rangle$ and implements the corresponding unitary operation according to Table 1. Bob obtains $|P'_B\rangle$. He makes comparisons between $|P'_B\rangle$ and $|P'\rangle$. This method is still swap [17]. If $|P'_B\rangle \neq |P'\rangle$, Bob rejects the signature; otherwise he informs Alice by the public board to publish σ, which Alice used in Eq.(8).
Step $V7$. Alice publishes σ by the public board.
Step $V8$. Bob gets back $|P\rangle$ from $|P'\rangle$ and holds $|S\rangle = (|S'\rangle, \sigma)$ as Alice's signature for quantum message $|P\rangle$.

The communications in this AQS scheme are described in Fig.1.

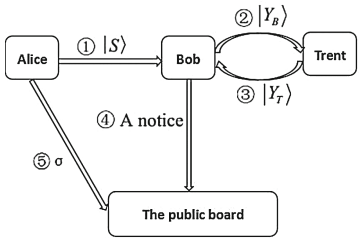

Fig. 1. The communications of the AQS scheme

4 Security Analysis and Discussion

A secure quantum signature scheme should satisfy two requirements: the signature should not be forged by the attacker(including the malicious receiver) and the signature should not be disavowed by the signatory and the receiver. We discuss security of the proposed AQS scheme to against the two attacks.

4.1 Impossibility of Forgery

If the attacker Eve tries to forge Alice's signature $|S'\rangle = E_{K_A}(|M_A\rangle, |R_A\rangle)$ for his own benefit, she has to know Alice's secret keys K_A. However, this is impossible due to the unconditionally security of quantum key distribution [7,30]. Besides, the use of quantum one-time pad algorithm enhances the security. Subsequently the parameter r used in verifying phase will not pass the test.

In the worse situation, for instance, the secret key is exposed to attacker, attacker still cannot forge the signature, since she cannot create appropriate $|M_A\rangle$ and $|M_T\rangle$. Bob would find such forgery, because the further verification about $|P'_B\rangle = |P'\rangle$ could not hold without the correct $|M_A\rangle$ and $|M_T\rangle$.

If the malicious receiver Bob wants to forge Alice's signature $|S'\rangle = E_{K_A}(|M_A\rangle, |R_A\rangle)$ for his own sake, he also should know Alice's secret K_A. It's also impossible because of the unconditionally security of quantum key distribution.

4.2 Impossibility of Disavowal by Signatory and Receiver

Suppose that Alice disavows her signature for her own benefits. In this case, the arbitrator Trent can confirm that Alice has signed the message since Alice's initial secret key k_A in the signature $|S'\rangle = E_{K_A}(|M_A\rangle, |R_A\rangle)$. Thus Alice cannot deny signing the message$|P\rangle$.

Similarly, suppose Bob repudiates the receipt of the signature. Then Trent also can confirm that Bob has received the signature since he needs the assistance of Trent to verify the signature. And if Bob wants to deny the signature by saying $|P'_B\rangle \neq |P'\rangle$, he cannot get σ to recover the message $|P\rangle$. This means that Bob cannot disavow the signature.

5 Conclusion

We have investigated an AQS based on W states in three phases, including initialing phased, signing phase and verifying phase. In the case of the loss of particles, the W states can maintain the quantum entanglement properties well. To avoid being disavowed by Bob, Bob has to ask Alice to publish the encryption key σ which means Bob has no chance to repudiate the signature.

Acknowledgments. This work is supported by the National Natural Science Foundation of China(Grant No. 11671284), Specialized Research Fund for the Doctoral Program of Higher Education (Grant. 20135134110003), Sichuan Provincial Natural Science Foundation of China (Grant No. 2015JY0002) and the Research Foundation of the Education Department of Sichuan Province (Grant No. 15ZA0032).

Recommender: Ming-qiang Bai, College of Mathematics and Software, Sichuan Normal University, Professor.

References

1. Wiesner, S.: Conjugate coding. ACM SIGACT News **15**(1), 78–88 (1983)
2. Bennett, C.H.: Quantum cryptography: Public key distribution and coin tossing. In: 1984 International Conference on Computer System and Signal Processing, pp. 175–179. IEEE (1984)
3. Abu-Ayyash, A.M., Ajlouni, N.: QKD: recovering unused quantum bit-s. In: 2008 3rd International Conference on Information and Communication Technologies: From Theory to Applications, ICTTA 2008, pp. 1–5. IEEE (2008)
4. Achilles, D., Rogacheva, E., Trifonov, A.: Fast quantum key distribution with decoy number states. J. Mod. Opt. **55**(3), 361–373 (2008)
5. Buttler, W.T., Hughes, R.J., Kwiat, P.G., et al.: Free-space quantum-key distribution. Phys. Rev. A **57**(4), 2379 (1998)
6. Ouellette, J.: Quantum key distribution. Ind. Physicist **10**(6), 22–25 (2004)
7. Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. **85**(2), 441 (2000)
8. Li, Y., Liu, Y.: Quantum secure direct communication based on supervised teleportation. In: Photonics Asia 2007 International Society for Optics and Photonics, vol. 682707-682707-7 (2007)
9. Fei, G., Qiao-Yan, W., Fu-Chen, Z.: Teleportation attack on the QSDC protocol with a random basis and order. Chin. Phys. B **17**(9), 3189 (2008)
10. Su-Juan, Q., Qiao-Yan, W.: Improving the security of secure deterministic communication scheme based on quantum remote state preparation. Chin. Phys. B **19**(2), 020310 (2010)
11. Fei, G., Fen-Zhuo, G., Qiao-Yan, W., et al.: Forcible-measurement attack on quantum secure direct communication protocol with cluster state. Chin. Phys. Lett. **25**(8), 2766 (2008)
12. Peng, J.Y., Bai, M.Q., Mo, Z.W.: Bidirectional quantum states sharing. Int. J. Theor. Phys. **55**(5), 2481–2489 (2016)
13. Xiang, Y., Mo, Z.W.: Quantum secret sharing protocol based on four-dimensional three-particle entangled states. Mod. Phys. Lett. B **30**(02), 1550267 (2016)
14. Guo, G.P., Guo, G.C.: Quantum secret sharing without entanglement. Phys. Lett. A **310**(4), 247–251 (2003)
15. Xiao, L., Long, G.L., Deng, F.G., et al.: Efficient multiparty quantum-secret-sharing schemes. Phys. Rev. A **69**(5), 052307 (2004)
16. Gottesman, D., Chuang, I.: Quantum digital signatures(2001). arXiv preprint quant-ph/0105032
17. Buhrman, H., Cleve, R., Watrous, J., et al.: Quantum fingerprinting. Phys. Rev. Lett. **87**(16), 167902 (2001)
18. Zeng, G., Keitel, C.H.: Arbitrated quantum-signature scheme. Phys. Rev. A **65**(4), 042312 (2002)

19. Li, Q., Chan, W.H., Long, D.Y.: Arbitrated quantum signature scheme using Bell states. Phys. Rev. A **79**(5), 054307 (2009)
20. Zou, X., Qiu, D.: Security analysis and improvements of arbitrated quantum signature schemes. Phys. Rev. A **82**(4), 042325 (2010)
21. Yang, Y.G., Wen, Q.Y.: Threshold proxy quantum signature scheme with threshold shared verification. Sci. China Ser. G: Phys. Mech. Astron. **51**(8), 1079–1088 (2008)
22. Zhou, J.X., Zhou, Y.J., Niu, X.X., et al.: Quantum proxy signature scheme with public verifiability. Sci. China Ser. G: Phys. Mech. Astron. **54**(10), 1828–1832 (2011)
23. Xiaojun, W.: An E-payment system based on quantum group signature. Phys. Scr. **82**(6), 065403 (2010)
24. Zhang, K., Song, T., Zuo, H., et al.: A secure quantum group signature scheme based on Bell states. Phys. Scr. **87**(4), 045012 (2013)
25. Tian-Yin, W., Qiao-Yan, W.: Fair quantum blind signatures. Chin. Phys. B **19**(6), 060307 (2010)
26. Wang, T.Y., Cai, X.Q., Zhang, R.L.: Security of a sessional blind signature based on quantum cryptograph. Quantum Inf. Process. **13**(8), 1677–1685 (2014)
27. Jalalzadeh, S., Ahmadi, F., Sepangi, H.R.: Multi-dimensional classical and quantum cos-mology: exact solutions, signature transition and stabilization. J. High Energy Phys. **2003**(08), 012 (2003)
28. Yu-Guang, Y., Yuan, W., Yi-Wei, T., et al.: Scalable arbitrated quantum signature of classical messages with multi-signers. Commun. Theor. Phys. **54**(1), 84 (2010)
29. D*ür*, W., Vidal, G., Cirac, J.I.: Three qubits can be entangled in two inequivalent ways. Phys. Rev. A 62(6), 062314 (2000)
30. Lo, H.K., Chau, H.F.: Unconditional security of quantum key distribution over arbitrarily long distances. Science **283**(5410), 2050–2056 (1999)