Int J Theor Phys (2017) 56:609–616
DOI 10.1007/s10773-016-3202-9

High-Efficient Arbitrated Quantum Signature Scheme Based on Cluster States

Negin Fatahi[1] · Mosayeb Naseri[1] · Li-Hua Gong[2] · Qing-Hong Liao[2]

Received: 13 June 2016 / Accepted: 21 November 2016 / Published online: 6 December 2016

Abstract The arbitrated quantum signature characteristics including the security and the efficiency are investigated and a new efficient and secure arbitrated quantum signature is proposed. It is shown that the proposed scheme exhibits an efficiency of 64 %. Furthermore, to gain a higher security, the decoy photons security checking is employed.

Keywords Quantum communication · Quantum signature · Cluster state

1 Introduction

Since the presentation of the first quantum key distribution protocol by Bennett and Brassard in 1984 [1], quantum information and quantum computation have spurred a number of theoretical and practical researches. In recent decade, researches on quantum computation and quantum information make it possible to be used in real-life world scenario applications related to information security [2–12].

In classical communication protocols, the digital signature plays an important role by offering authenticity, integrity of messages and forestalls disavowal of transmitted messages. In addition to the above mentioned requirement, in some specific applications such as electronic voting and electronic cash systems, the privacy of the message owners had to be protected. To preserve such conditions on secure communication, the concepts of blind signature and arbitrated signature schemes were proposed. Blind signature schemes provide a

✉ Negin Fatahi
n83fatahi@yahoo.com

Mosayeb Naseri
m.naseri@iauksh.ac.ir

[1] Department of Physics, Kermanshah Branch, Islamic Azad University, Kermanshah, Iran

[2] School of Information Engineering, Nanchang University, Nanchang, 330031, China

type of solution that the manager signs the message blindly and the voter then converts it to the signature of the original message for anyone who would probably verify it. The manager signs the message in such a way that he can neither know the content of the message nor recollect the message and the corresponding signature he has signed. In an arbitrated signature scheme, every signed message from the sender, S, to the receiver, R, goes to an arbiter, A, first. The arbitrator confirms the origin of the message and signature after subjecting them to the number of tests and sends them to the receiver.

Up to now many quantum blind signature and arbitrated quantum signature (AQS) schemes have been presented [13–22]. The AQS model by using the correlation of Greenberger-Horne-Zeilinger (GHZ) triplet states and the Leung quantum one-time pad (L-QOTP) algorithm [13] was first introduced by Zeng et al. [14]. Li et al. presented a more efficient AQS scheme by replacing GHZ states with Bell states [15]. However, Zou and Qiu [16] showed that both these two AQS schemes above were insecure because they could be disavowed by the receiver, and further proposed two improved AQS schemes. However, Hwang et al. [17] showed that the same security flaw still exists in Zou et al.'s schemes. Some other security problems and improvements were also introduced in Refs. [18–23]. Obviously, the construction and the cryptanalysis of AQS schemes are two important branches of AQS and can be mutually reinforcing.

Recently, an interesting research regarding the arbitrated quantum signature scheme based on cluster state has been done by Yang et al. [24], where the cluster states are employed for quantum key distribution and quantum signature. Motivated by this work, this paper a new arbitrated quantum signature scheme is proposed to make the original protocol not only more efficient but also more secure. The paper is organized as follows:

The next section introduces the basic preliminaries, which is involved in presenting the new improved protocol. Our improved protocol for quantum arbitrated signature is presented in Section 3. The security of the proposed protocol is analyzed in Section 4. Finally, a short discussion and a brief conclusion are given in Section 5.

2 Cluster States

In general, an N-qubit cluster state is given by [25]

$$|C_N\rangle = \frac{1}{2^{\frac{N}{2}}} \otimes_{a=1}^{N} (|0\rangle_a \sigma_z^{a+1} + |1\rangle_a) \tag{1}$$

where σ_z is Pauli operator. So. the four-particle cluster states can be described by

$$|C_4\rangle = |\phi^{00}\rangle_{1234} = \frac{1}{2}(|0000\rangle + |0110\rangle + |1001\rangle - |1111\rangle)_{1234} \tag{2}$$

The four-particle cluster states were proven to be useful in many fields of quantum communication [26–29]. The usefulness of this state for arbitrated quantum signature is as follows. By performing Pauli operators on qubits 2 and 4, an orthonormal basis can be constructed as

$$FMB = |\phi^{ij}\rangle_{1234} = \sigma_2^i \sigma_4^j |\phi^{00}\rangle_{1234} | i, j = 0, 1, 2, 3 \tag{3}$$

Here, Pauli operators σ_2^i, σ_4^j act on the 2 and 4 particles in cluster states and they are one of the four Pauli operators:

$$\sigma^0 = I = |0\rangle\langle 0| + |1\rangle\langle 1|, \sigma^1 = \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1| \tag{4}$$

$$\sigma^2 = \sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|, \sigma^3 = i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0| \tag{5}$$

The state $|\phi^{00}\rangle_{1234}$ can be rewritten in the following form by rearranging terms:

$$|\phi^{00}\rangle_{1234} = \frac{1}{2}\left(|0+\rangle|+0\rangle + |0-\rangle|-0\rangle + |1-\rangle|+1\rangle + |1+\rangle|-1\rangle\right)_{1234} \quad (6)$$

$$|\phi^{00}\rangle_{1234} = \frac{1}{2}\left(|+0\rangle|0+\rangle + |-0\rangle|0-\rangle + |-1\rangle|1+\rangle + |+1\rangle|1-\rangle\right)_{1234} \quad (7)$$

where $|0+\rangle$ and $|+0\rangle$ are the abbreviated expression of tensor product of $|0\rangle$ and $|+\rangle$:

$$|0+\rangle = |0\rangle \otimes |+\rangle \quad , \quad |+0\rangle = |+\rangle \otimes |0\rangle$$

Thus, we have two groups of different measurement bases for the two-qubit Hilbert space:

$$AMB_1 = |0+\rangle, |0-\rangle, |1-\rangle|1+\rangle$$

$$AMB_2 = |+0\rangle, |-0\rangle, |-1\rangle|+1\rangle$$

Four possible measurement results $|0+\rangle|+0\rangle, |0-\rangle|-0\rangle, |1-\rangle|+1\rangle, |1+\rangle|-1\rangle$ can be obtained with equal probability $\frac{1}{4}$, if one measures the qubits (1,3) in the basis AMB_1 and the qubits (2,4) in the basis AMB_2, respectively. Obviously, a similar conclusion can be derived if one measures the qubits (1,3) in the basis AMB_2 and the qubits (2,4) in the basis AMB_1, respectively. Using this property, Alice, Bob and the arbitrator can check eavesdropping in the quantum transmission.

3 High-Efficient AQS Scheme Based on the Cluster States

In this section, we introduce the new protocol for arbitrated quantum signature by using the cluster states. In this new scheme, the decoy state particle security checking is employed for guarding every eavesdropping in the first phase. Furthermore, it will be shown that the present scheme indicates more efficiency.

The proposed AQS scheme includes three participants, Alice is the signer, Trent is the arbitrator and Bob is the verifier. The protocol consists of three phases: the initializing, the signing and the verifying phases.

The initializing phase is accomplished as follows:

3.1 Initializing Phase

- The arbitrator Trent prepares and sends the secret keys K_{AT} and K_{BT} based on $|0\rangle, |1\rangle$ to Alice and Bob, respectively.
- Trent prepares a large enough number of four-qubit cluster states. He sends particles 1 and 3 for Alice and Bob, respectively and possesses particles 2 and 4 with himself.
- Before sending particle 1 to Alice and particle 3 to Bob, Trent prepares the non-orthogonal decoy particles each randomly in one of the four-state $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ and inserts the decoy particles into the sequence. Then, Trent sends particle 1 and decoy particles to Alice while particle 3 and decoy particles to Bob.
- After confirming Alice and Bob have received the sequences, Trent announces publicly the positions and the states of the decoy particles. Then, Alice and Bob perform a suitable measurement on each decoy particle with the same basis as Trent chosen for preparing it. By comparing his measurement results with Alice and Bob's announcements, Trent can then evaluate the error rate of the transmission of the sequence. If the error rate exceeds the specified threshold, they abort this communication and repeat the protocol from the beginning. Otherwise, they continue to the next step.

We denote the entangled tetrads as the sequences $P_i : [p_i^1, p_i^2, p_i^3, ..., p_i^n] , i = 1, 2, 3, 4$. Here $(p_1^j, p_2^j, p_3^j, p_4^j)$ is an entangled tetrad in the same cluster state $|\phi^{00}\rangle_{1234}$ for $1 \leq j \leq n$.

The signing phase is completed as follows:

3.2 Signing Phase

- Alice measures the particles in the sequence P_1 according to the message $m = (m(1, m(2), ..., m(n))$, where $m(i) \in \{0, 1\}$. If $m(i) = 0$, she measures the corresponding particle p_1^i in the $|0\rangle, |1\rangle$ basis otherwise, she chooses the $|+\rangle, |-\rangle$ basis.
- Alice translates her measurement results into classical bits; that is, $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ correspond to 00,01,10,11, respectively. She denotes the classical bits as R_A.
- Alice encrypts R_A with her key K_{AT} to generate her signature $S_A = E_{K_{AT}}(m, R_A)$ and sends her signature S_A to Trent.

The verifying phase is performed as follows:

3.3 Verifying Phase

- Trent decrypts S_A with K_{AT} to obtain m and R_A.
- Trent measures the corresponding particles p_2^i and p_4^i in P_2 and P_4 in his hand in the measurement basis corresponding to the message m; *i.e.*, if $m(i) = 0$, he chooses the basis AMB_2; otherwise, he chooses the basis AMB_1. Trent translates the eight states $|+0\rangle, |-0\rangle, |+1\rangle, |-1\rangle, |0+\rangle, |0-\rangle, |1+\rangle, |1-\rangle$ into classical bits 000,001,010,011,100,101,110,111, respectively. The encoded results can be denoted as R_T.
- Trent can deduce Alice's measurement results $R_A^{'}$ from his own measurement results according to the correlation in (6) and (7). For example, if his measurement result is $|+0\rangle_{24}$, Trent can infer that Alice's measurement result should be $|0\rangle_1$, and $R_A^i = 00$. He compares R_A with $R_A^{'}$. If $R_A \neq R_A^{'}$, Trent judges that Alice's signature S_A is not valid; otherwise, he accepts the signature. To ensure the data integrity during the transmission, Trent selects a proper hash function $H(\bullet)$ to compute the hash function of S_A. Then he encrypts m, S_A, $H(S_A)$, and R_T with the key K_{BT}, then he sends $E_{K_{BT}}(m, S_A, H(S_A), R_T)$ to the verifier Bob.
- Bob decrypts $E_{K_{BT}}(m, S_A, H(S_A), R_T)$ with the key K_{BT} and obtains m, S_A, $H(S_A)$, and R_T. Then he measures the particles in the sequence P_3 with the suitable measurement basis. If $m(i) = 0$, he measures the particle p_3^i in the basis $|+\rangle, |-\rangle$; otherwise, he chooses the $|0\rangle, |1\rangle$ basis. He encodes the four states $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ into classical bits 00,01,10,11, respectively, and then he denotes the encoded results as R_B.
- Bob can verify the validity of R_T by checking the consistence between R_B and R_T according to the correlation in (6) and (7). The relationship among R_A, R_B, and R_T is shown in Table 1. If the consistence occurs, he proceeds to step (6).
- Bob further verifies the integrity of S_A by computing the hash value of S_A and comparing it with $H(S_A)$. If the two values are equal, Bob will accept the signature S_A as the valid signature for the message m, otherwise, he rejects it.

Needless to say that, in this section Bob can ensure the data integrity and check the eavesdropping by using the classical bits R_B. Since, R_B and R_T are related to each other according to (6) and (7), Bob simply can verify the validity of R_T.

Table 1 Relationship among R_A, R_B, and R_T

m(message)	R_A	R_T	R_B
0	$00(\|0\rangle)$	$000(\|+0\rangle)$	$10(\|+\rangle)$
	$00(\|0\rangle)$	$001(\|-0\rangle)$	$11(\|-\rangle)$
	$01(\|1\rangle)$	$011(\|-1\rangle)$	$10(\|+\rangle)$
	$01(\|1\rangle)$	$010(\|+1\rangle)$	$11(\|-\rangle)$
1	$10(\|+\rangle)$	$100(\|0+\rangle)$	$00(\|0\rangle)$
	$10(\|+\rangle)$	$111(\|1-\rangle)$	$01(\|1\rangle)$
	$11(\|-\rangle)$	$101(\|0-\rangle)$	$00(\|0\rangle)$
	$11(\|-\rangle)$	$110(\|1+\rangle)$	$01(\|1\rangle)$

4 Efficiency and Security

In this section, the efficiency and the security of the proposed scheme are analyzed. At first, the efficiency of the proposed protocol is considered. By using Cabello's definition of the efficiency [30], the information theoretical efficiency of a protocol is

$$\eta = \frac{b_s}{q_t + b_t} \tag{8}$$

where b_s is the expected number of secret bits received by Bob, q_t is the number of qubits transmitted through the quantum channel, and b_t is the number of classical bits exchanged over the public channel.

In the present arbitrated quantum signature scheme, Bob receives the signature S_A containing $8n$ secret bits R_A and n bits of the message m, while $12n$ classical bits R_T are exchanged over the public channel and $2n$ qubits are transmitted among Alice, Bob and Trent during the initializing phase. Therefore, $b_s = 9n, q_t = 2n, b_t = 12n$ and the efficiency can be calculated as 64 %.

Now let us analyze the security of the proposed scheme. Needless to say, any secure quantum signature scheme, in addition to resistance again external attacks, which are done by an outside eavesdropper, should satisfy two the requirements: (1) The signature had not been forged by the attacker (including the malicious receiver); (2)The signature could not be disavowed by the signatory and the receiver [31–33]. Before considering the above cases it should be noted that in our scheme the arbitrator Trent shares the signing key K_{AT} and K_{BT} with the signer Alice and the verifying Bob. Trent as the arbitrator, is very important in two aspects, one is that he can help the receiver Bob to verify the signature; the other is that he can arbitrate some disputes between Alice and Bob. Also, Trent as the authenticated channel between Alice and Bob would avoid the vulnerability of the protocol against the distrustfulness of Trent, because Trent as an arbitrator, he must be perfectly trustworthy in our scheme. In the following discussion, we will show that the proposed scheme not only resists again an external eavesdropping, but also exhibits the above mentioned two properties.

4.1 Outside Attack

Assume an eavesdropper called Eve, who knows the procedure of our proposed quantum signature. Due to the no-cloning theorem, it is impossible for Eve to make a perfect copy of

a qubit without knowing the basis, in which has initially been created. Hence, if an attacker, who is outside the protocol, wants to forge Alice's signature, he/she needs to obtain the initial secret key K_{AT} shared between Alice and Trent. However, it is impossible since the key is shared through unconditional secure quantum key distribution before transmitting the particles 1 and 3 to Alice and Bob. Furthermore, in the initializing phase, Trent inserts decoy particles to the sequence to guard for eavesdropping. The states and the positions of the decoy photons are unknown for Eve. Therefore, any eavesdropping done by Eve will inevitably disturb the states of the decoy particles and ultimately be detected by the two legitimate users Alice and Bob.

Also, even if the attacker obtains the key K_{AT}, he/she still cannot forge the signature successfully since he/she cannot get the classical bits R_A corresponding to Alice's measurement result in the signing phase. In the signing phase, Alice encrypts her signature S_A with classical bits R_A and her key K_{AT}. Therefore, Eve cannot forge the signature.

4.2 Forgery Attack

The signature forgery attack means that the attacker has the ability to create a fake pair of a message and a signature that the message has not been signed over the past by the legitimate signer. Suppose that the verifier Bob is malicious and tries to forge Alice's signature.

A possible strategy is to obtain the secret key K_{AT} and classical bits R_A to generate S_A in initializing phase. However, the task is impossible because the key is distributed through the quantum key distribution and if Bob wants to acquire R_A, he must wield an attack strategy on particle 1, but he will be detected during the security check with decoy particles in the initializing phase, also he doesn't know the basis measurement of Alice in the signing phase. Thus the proposed AQS scheme is secure against the forgery attack.

4.3 Disavowal Attack

Disavowal attack means that Alice signed a signature S_A for a message m, and then wants to disavow that she has signed this signature. In our scheme, detecting Alice's cheat is easy for Trent, because Alice's signature S_A encrypts with the secret key K_A. Therefore, if a dispute occurs between Alice and Bob, Bob needs to take the message signature pair (m, S_A) to Trent to make a fair judgement. The signature S_A has been absolutely generated by Alice, if and only if contain the secret key K_A.

Moreover, in the verifying phase, the action of dishonest Alice who wants to modify S_A after Trent's action on the signature, will be found. In the check of data integrity, the hash function plays an important role. Because Alice cannot know any information about K_{BT}, when Bob computes the hash value of S_A and compares it with $H(S_A)$, her action will be found. Therefore, a disavowal attack by the signer will not work in our scheme.

5 Conclusion and Discussion

An arbitrate quantum signature scheme based on cluster states is proposed. With the decoy photon technique in security checking, it is shown that the protocol is secure not only against the outside attack which would be done by an eavesdropper outside of the participants but also it is secure against the two types of internal attacks, i.e., the forgery attack and the disavowal attack. Furthermore by using the Cabello's definition of the efficiency, it indicates the efficiency of 64 % confirms that the present protocol is more efficient.

Acknowledgments This work is supported by Kermanshah Branch, Islamic Azad University, Kermanshah, IRAN, the National Natural Science Foundation of China (Grant No. 61561033), and the Natural Fundation of Jiangxi Province (Grant No. 2015IBAB207002).

References

1. Bennett, C.H., Brassard. G.: In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, p. 175. IEEE, New York (1984)
2. Zhang. Y.S., Li. C.F., Guo. G.C.: Quantum key distribution via quantum encryption. Phys. Rev. A. **64**, 024302 (2001)
3. Zhou, N., Zeng, G., Zeng, W., Zhu, F.: Cross-center quantum identification scheme based on teleportation and entanglement swapping. Opt. Commun. **254**, 380 (2005)
4. Zhou, N., Liu, Y., Zeng, G., Xiong, J., Zhu, F.: Novel qubit block encryption algorithm with hybrid keys. Physica A. **375**, 693 (2007)
5. Naseri, M.: Comment on: secure direct communication based on ping-pong protocol, Quantum Inf. Process. **8**, 347 (2009); Quantum Inf. Process. **9**, 693–698 (2010)
6. Zhou, N.R., Wang, L.J., Ding, J., Gong, L.H.: Quantum deterministic key distribution protocols based on the authenticated entanglement channel. Phys. Scr. **81**, 045009 (2010)
7. Naseri, M.: A weak blind signature based on quantum cryptography. Int. J. Phys. Sci. **6**, 5051 (2011)
8. Sheikhehi. F, Naseri. M: Probabilistic bidirectional quantum secure communication based on a shared partially entangled states. Int. J. Quantum Inf. **9** (supp01), 357–365 (2011)
9. Liu, D., Chen, J.L., Jiang, W.: High-Capacity Quantum Secure Direct Communication with Single Photons in Both Polarization and Spatial-Mode Degrees of Freedom. Int. J. Theor. Phys. **51**, 2923–2929 (2012)
10. Gu, B., et al: Robust Quantum Secure Communication with Spatial Quantum States of Single Photons. Int. J. Theor. Phys. **52**, 4461–4469 (2013)
11. Zhang, Q.N., Li, C.C., Li, Y.H., Nie, Y.Y.: Quantum Secure Direct Communication Based on Four-Qubit Cluster States. Int. J. Theor. Phys. **52**, 22–27 (2013)
12. Naseri, M., et al: A scheme for secure quantum communication network with authentication using GHZ-like states and cluster states controlled teleportation. Quantum Inf. Process. **14**, 4279–4295 (2015)
13. Leung, D.W.: Quantum Vernam cipher. Quantum Inf. Comput. **2**, 14–34 (2002)
14. Zeng, G.H., Keitel, C.H.: Arbitrated quantum-signature scheme. Phys. Rev. A. **65**, 042312 (2002)
15. Li, Q., Chan, W.H., Long, D.Y.: Arbitrated quantum signature scheme using Bell states. Phys. Rev. A. **79**, 054307 (2009)
16. Zou, X.F., Qiu, D.W.: Security analysis and improvements of arbitrated quantum signature schemes. Phys. Rev. A. **82**, 042325 (2010)
17. Hwang, T., Luo, Y.P., Chong, S.K.: Comment on security analysis and improvements of arbitrated quantum signature schemes. Phys. Rev. A. **85**, 056301 (2012)
18. Gao, F., Qin, S.J., Guo, F.Z., Wen, Q.Y.: Cryptanalysis of the arbitrated quantum signature protocols. Phys. Rev. A. **84**, 022344 (2011)
19. Li, Q., Du, R.G., Long, D.Y., Wang, C.J., Chan, W.H.: Entanglement enhances the security of arbitrated quantum signature. Int. J. Quantum Inf. **7**, 913–925 (2009)
20. Li, Q., Li, C.Q., Wen, Z.H., Zhao, W.Z., Chan, W.: On the security of arbitrated quantum signature schemes. J. Phys. A Math. Theor. **46**, 015307 (2013)
21. Guo, W., Zhang, J.z., Li, Y.P., An, W.: Multi-proxy Strong Blind Quantum Signature Scheme. Int. J. Theor. Phys. **55**, 3524–3536 (2016)
22. Guo, Y., Feng, Y., Huang, D., Shi, J.: Arbitrated quantum signature scheme with Continuous-Variable coherent states. Int. J. Theor. Phys. **55**, 2290–2302 (2016)
23. Choi, J.W., Chang, K.Y., Hong, D.: Security problem on arbitrated quantum signature schemes. Phys. Rev. A **84**, 062330 (2011)
24. Yang, Y.G., Lei, A.H., Liu, A.Z., Zhou, Y.H., Shi, W.: M.,arbitrated quantum signature scheme based on cluster states. Quantum Inf. Process. **15**, 2487–2497 (2016)
25. Raussendorf, R., Harrington, J.: Fault-tolerant quantum computationwith high threshold in two dimensions. Phys. Rev. Lett. **98**, 190504 (2007)
26. Dur, W., Briegel, H.J.: Stability of macroscopic entanglement under decoherence. Phys. Rev. Lett. **92**, 180403 (2004)
27. Schlingemann, D., Werner, R.F.: Quantum error-correcting codes associated with graphs. Phys. Rev. A. **65**, 012308 (2001)

28. Sun, Z.W., Long, D.Y.: Quantum private comparison protocol based on cluster states. Int. J. Theor. Phys. **52**, 212–218 (2013)
29. Cao, W.F., Yang, Y.G., Wen, Q.Y.: Quantum secure direct communication with cluster states. Sci. Chin. Ser. G Phys. Astron. **53**, 1271–1275 (2010)
30. Cabello, A. Phys. Rev. Lett. **85**, 5635 (2000)
31. Zeng, G.H., Keitel, C.H.: Arbitrated quantum-signature scheme. Phys. Rev. A. **65**, 042312 (2002)
32. Zeng, G.H.: Reply to Comment on Arbitrated quantum-signature scheme. Phys. Rev. A. **78**, 016301 (2008)
33. Li, Q., Chan, W.H., Long, D.Y.: Arbitrated quantum signature scheme using Bell states. Phys. Rev. A. **79**, 054307 (2009)