On the Existence of Quantum Signature for Quantum Messages

Qin Li · Wai Hong Chan · Chunhui Wu · Zhonghua Wen

Received: 21 February 2013 / Accepted: 16 July 2013 / Published online: 9 August 2013
© Springer Science+Business Media New York 2013

Abstract Quantum signature (QS) is used to authenticate the identity of the originator, ensure data integrity and provide non-repudiation service with unconditional security. Depending on whether a trusted third party named arbitrator is involved or not, QS is classified as arbitrated QS and true QS. This paper studies existence problem about the two kinds of QS and contributes to two points: (1) a basic framework is provided to analyze the possibility of arbitrated QS on signing quantum messages; (2) disagreement between the impossibility of true QS and an existing true QS scheme is solved.

Keywords Quantum cryptography · Quantum signature

1 Introduction

Digital signature, as an analogy to hand-written signature for authenticating the origin of a message and ensuring the message not modified during transmission, is an essential cryptographic primitive. It has been being widely used in various security-related fields, particularly in secure electronic commerce. As Rivest, one of the three inventors of the RSA algorithm, predicted, digital signature may become one of the most fundamental and useful...
inventions of modern cryptography [1]. However, all of the existing classical (digital) signature schemes were threatened by last-increasing power of computers and innovative techniques such as quantum computation since their security depends on the difficulty of solving some hard mathematical problems. Once quantum computers is successfully built, most of classical signature schemes will be cracked through Shor’s algorithm [2]. On the other hand, development of quantum physics has thrown some light on the study of cryptography for obtaining unconditional security [3–8]. So, researchers turn to investigate quantum counterpart of classical signature. They hope that quantum signature (QS) can provide unconditional security, namely the attacker (or the malicious receiver) cannot forge the signature, and the signatory cannot deny the signature even though unlimited computing resources are available.

QS is expected to sign both classical and quantum messages, and the form of each quantum message can be a known quantum state or an unknown one. Since known quantum states can be characterized with classical information, only the quantum messages of the form of unknown quantum states are considered in this paper. In 2001, Gottesman and Chuang proposed the first QS scheme based on quantum one-way function, which is unconditionally secure even against quantum attacks [9]. But this scheme works only on classical messages, and seems not practicable as it use up \( O(m) \) qubits of the public key for signing an \( m \)-bit message. Subsequently, Barnum et al. showed that unconditionally secure QS for quantum messages cannot be achieved [10]. This negative result did depress some researchers pursuing positive application of QS. Fortunately, Zeng and Keitel presented a QS scheme signing both classical and quantum messages by introducing a trust third party named arbitrator [11] (this kind of QS was named arbitrated QS thereafter), and the scheme was improved later [12, 13]. Afterwards, Li et al. observed that the GHZ states used in [13] could be replaced by Bell states, and then put forward a more efficient scheme in [14]. But, Zou et al. proved the two schemes proposed in [13] and [14] are both insecure because they could be repudiated by the receiver Bob, and further presented two arbitrated QS schemes to fix the defect [15]. Some other typical arbitrated QS schemes were also presented since the study of arbitrated QS initiated by Zeng and Keitel [16–20].

Recently, almost all typical arbitrated QS schemes designed for quantum messages were found to have security problems of different extents [21–26]. So, whether QS can provide unconditional security for quantum messages is the key problem many researchers cared. To solve this doubt, we shall present a detailed analysis of the reasons why unconditionally secure arbitrated QS for quantum messages is possible and this does not contradict with Barnum et al.’s conclusion. Note that some related preliminary reasons were simply mentioned by Li et al. in [14]. In addition, Zeng et al. presented a true QS scheme in 2007 and claimed it can sign quantum messages with unconditional security [27]. This result stimulated the nerves of researchers in the field, and a question emerge: is Barnum et al.’s conclusion in [10] wrong or Zeng et al.’s scheme in [27] insecure? We shall answer this question by showing the insecurity of Zeng et al.’s scheme.

The rest of the paper is organized as follows. Section 2 briefly reviews Burnum et al.’s conclusion about the impossibility for signing quantum messages. Then the arbitrated QS is shown to be able to sign quantum messages in Sect. 3, and the disagreements between the impossibility of true QS and an existing true QS scheme for quantum messages is solved in Sect. 4. The last section concludes the paper.
2 Review of a Negative Result on Signing Quantum Messages

This section briefly reviews Barnum et al.’s conclusion claiming that signing quantum messages is impossible to realize [10].

In [10], Barnum et al. proved a theorem that quantum authentication implies encryption. This means that any scheme ensuring the authenticity of quantum messages must also encrypt them almost perfectly. However, in a QS scheme, the receiver should learn something about the contents of the quantum message but is not allowed to changed it. It follows that the theorem results in the impossibility of signing quantum messages: any non-trivial information obtained from encrypted quantum messages is only possible at the cost of introducing disturbance to them which implies the authenticity of quantum messages is destroyed.

To be better understanding, one can assume the receiver is allowed to efficiently extract the original quantum message $\rho$, then it is easy to show the receiver can generate a valid signature of a new message $\rho'$ favorable to him by the following steps. First suppose the receiver can extract the original message $\rho$ via the transformation $U$ and leave the auxiliary state as $\phi$ which may not be hold entirely by the receiver. Since $\rho$ should have been entangled with a reference system, $\phi$ must be independent of $\rho$. Then the receiver implements the transformation $U^\dagger$, the inverse process of $U$, on $\rho'$ and his part of $\phi$ to get a valid signature. Obviously, this contradicts with the security of QS.

3 Possibility of Arbitrated QS for Quantum Messages

In this section, we analyze why it is possible to design an arbitrated QS scheme to sign quantum messages. It does not disagree with Barnum et al.’s conclusion [10] and can provide unconditional security if it is properly devised. We also give a basic framework of such a scheme as an example.

As mentioned in Sect. 2, Barnum et al. showed any protocol allowing a receiver to read a quantum message also allows the receiver to modify the message without the risk of being detected, therefore all potential receivers of an authenticated message must be trustworthy. Obviously this will not happen for a general QS protocol. However, in an arbitrated QS scheme, the arbitrator is always supposed to be trusted by both signatory and receiver. We assume that the real recipient of the authenticated message is the arbitrator who is in charge of the verification of the signature. After verifying the signature, the arbitrator can send a parameter to indicate whether the signature is valid. The receiver would obtain the indication parameter, and only check whether the parameter and other information come from the real arbitrator.

Recently, almost all existing arbitrated QS schemes were cracked [21–26], but it does not mean that arbitrated QS cannot provide unconditional security. The failures of the previous schemes are mainly due to imperfections of design. For example, some schemes just employed quantum one-time pad to encrypt, but ignored to authenticate the transmitted quantum messages. Quantum encryption does not imply authentication, even though the converse is true [10].

Based on the above analysis, we give a basic framework of an unconditional secure arbitrated QS scheme for quantum messages, which is composed of the following three phases.

- **The initial phase:** The signatory Alice shares a key $K_A$ with the arbitrator using an unconditionally secure quantum key distribution protocol. The receiver Bob also has a key $K_B$ shared with the arbitrator in the same way.
The signing phase: Alice generates the signature $\text{Sig}_{K_A}(P)$ of the message $P$ via a non-commutative transformation which means that there does not exist a unitary operation $U$ to satisfy $U(\text{Sig}_{K_A}(P)) = \text{Sig}_{K_A}(UP)$. Then Alice computes $\sigma = \text{Aut}(\text{Sig}_{K_A}(P), P)$ for authentication. Note that $\text{Aut}(\cdot)$ denotes unconditionally secure authentication is used such as the quantum authentication scheme given in [10] for quantum information, and Wegman-Carter authentication scheme for classical information in [28]. The authenticated signature state $\sigma$ is sent to Bob.

The verification phase: After Bob receives $\sigma$, he can implement the verification with the aid of the arbitrator using the following three steps:

1. Bob makes a random transformation on $\sigma$ to obtain $\text{Trans}_{K_B}(\sigma)$ according to the key $K_B$. Then he produces the authenticated state $Y = \text{Aut}(\text{Trans}_{K_B}(\sigma))$ and transmits it to the arbitrator.
2. After having received $Y$, the arbitrator checks the authenticity of $\text{Trans}_{K_B}(\sigma)$. If there is anything wrong, she would abort the protocol immediately; otherwise, she would recover $\sigma$ from $\text{Trans}_{K_B}(\sigma)$ using the key $K_B$ shared with Bob. Similarly, the arbitrator examines whether $\text{Sig}_{K_A}(P)$ and $P$ are tamped or not. If not, the arbitrator would verify whether $\text{Sig}_{K_A}(P)$ is a valid signature of the message $P$. If the verification process is passed, the arbitrator sets the verification parameter $r = 1$; otherwise, sets $r = 0$. Finally, the arbitrator computes $T = \text{Aut}(P, \text{Sig}_{K_A}(P), r)$ and sends it to Bob.
3. Finally, Bob authenticates what he received. If the authentication test is passed and $r = 1$, he would accept $\text{Sig}_{K_A}(P)$ as the signature of $P$.

The arbitrated QS scheme of the above framework is secure since it satisfies two security properties: impossibility of forgery and non-repudiation of signatory. First, without the knowledge about signing key, an attacker cannot directly produce a signature of a new quantum message directly. Furthermore, as the signature process is noncommutative, an attacker cannot change the received signature state to be that of another quantum message favorable for him by implementing appropriate unitary operations. Second, the key information of the signatory is included in a signature state, which cannot be changed due to the use of authentication during the verification phase, so the signatory cannot deny what she has signed. In addition, under the assumption that the arbitrator is trustworthy and is the real person who can verify $\text{Sig}_{K_A}(P)$ with all the information he holds, thus the arbitrated QS scheme under the proposed framework does not disobey Barnum et al.’s conclusion. This also tells that the verification made by the arbitrator is indispensable to an arbitrated QS scheme.

4 Building a Bridge Between Two Contradictory Results on Signing Quantum Messages

From the above section, we know Barnum et al.’s conclusion [10] on the impossibility of signing quantum messages does not include arbitrated QS, so it just aimed at true QS. However, Zeng et al. presented a true QS scheme recently in [27], which was claimed to be able to sign quantum messages with unconditional security. Then people wondered whether Barnum et al.’s conclusion is wrong or Zeng et al.’s scheme is not secure. In this section, we clarify this question. At first, we review Zeng et al.’s true QS scheme [27]. Then, we show the insecurity of the scheme by attacking it successfully using similar method presented by Barnum et al. in [10].
4.1 Review of the True QS Scheme Proposed by Zeng et al.

Zeng et al. proposed a true QS scheme for the purpose of signing quantum messages recently [27] and claimed that the scheme is unconditionally secure. We briefly describe the three main phases of their scheme as follows (more details can be found in [27]).

– In the initial phase, the main goal is to generate a signing key $K_s$ and a verification key $K_v$ by constructing a one-way function $G : \{L, X, T_{ij}\} \rightarrow \{U, \|T\|^{1/2}\}$, where $L$ is a linear transformation mapping $x = (x_0, x_1, \ldots, x_{k-1}) \in \mathbb{R}^k$ to $y(X) = y_0(x) = [y_0(x_1), \ldots, y_{2k-1}(x)]^T \in \mathbb{R}^{2k}$ and making any $k$-element subset of $\{x_0, x_1, \ldots, x_{2k-1}\}$ linearly independent, $T$ makes $T[y_{r_1}, y_{r_2}, \ldots, y_{r_k}]^T = T[x_0, y_{r_{k+1}}, \ldots, y_{2k-1}]^T$, and $U$ satisfies $U|y_{r_1}\rangle_r \langle y_{r_2}|_r \cdots |y_{r_k}\rangle_r = |x_0\rangle_r |y_{r_{k+1}}\rangle_r \cdots |y_{2k-1}\rangle_r$. $K_s$ is expressed as $K_s = \{L, X\}$ and $K_v$ is set as $K_v = \{U, \|T\|^{1/2}\}$.

– In the signing phase, according to $K_s$, the signatory Alice prepares $2k - 1$ ancilla states $|\omega(X)\rangle = |y_1(X)\rangle \cdots |y_{2k-1}(X)\rangle^\perp_{k-1}$ and encodes the message state $P$ with a wave function $\langle x_0|P\rangle$ as $|\tilde{S}\rangle = \int \langle P|\omega\rangle dx$. Then Alice prepares a two-particle entangled state $|\tilde{\Omega}\rangle = \int_\mathbb{R} |y_{k+1}\rangle_r |y_{k+1}\rangle_{r_k} dx$ in terms of $K_s$ and generates a signature state $|\tilde{S}\rangle = |\tilde{\Omega}\rangle \otimes |\tilde{\Omega}\rangle$. Finally $|\tilde{S}\rangle$ and $|P\rangle$ are sent to the receiver Bob.

– Bob implements the verification process by the following four steps: (1) Bob checks whether the state $|\tilde{S}\rangle$ is a $2k$-particle QECC by performing a syndrome measurement on it. (2) In terms of $K_v$, Bob decodes $|\tilde{S}\rangle$ as

$$K_v |S\rangle \rightarrow U |\tilde{S}\rangle = J \|T\|^{1/2} \int \{ |P|_{r_1} |y_{r_{k+1}}\rangle_{r_2} |y_{r_{k+1}}\rangle_{r_{k+1}} \cdots \otimes |y_{r_{2k-1}}\rangle_{r_k} |y_{r_{2k-1}}\rangle_{r_{2k-1}} \} dX = J \|T\|^{1/2} |P|_{r_1} |\Omega\rangle_{r_2,r_{k+1}} |\Omega\rangle_{r_3,r_{k+2}} \cdots |\Omega\rangle_{r_{k-1},r_{2k-1}},$$

(1) where $J$ is the Jacobian for the transformation from $X$ to $y(X)$, and $|\Omega\rangle_{i,j} = \int_\mathbb{R} |y_i\rangle_j |y_i\rangle_j dx$ ($i = r_2, \ldots, r_k, j, l = r_{k+1}, \ldots, r_{2k-1}$) is an entanglement state of particles $i$ and $j$. (3) Bob verifies the entanglement properties of $k - 1$ states $|\Omega\rangle_{r_2,r_{k+1}}$, $|\Omega\rangle_{r_3,r_{k+2}}$, $\ldots$, $|\Omega\rangle_{r_{k-1},r_{2k-1}}$, respectively. (4) Bob checks whether the decoded message state is the same as the received message state, and tests the equality of the decoded two-particle entangled state $|\Omega\rangle_{r_2,r_{k+1}}$ and the received two-particle entangled state $|\Omega\rangle$. If there is a failure in any step, Bob will reject $|\tilde{S}\rangle$ and stop the protocol.

4.2 Cryptanalysis of the Reviewed True QS Scheme

The above scheme used for signing quantum messages [27] does not involve a trustable arbiter to help the receiver verify the signature. Any receiver who is not always trustworthy can verify the validity of the signature directly. This scheme obviously violates Barnum et al.’s conclusion [10] which stated that signing quantum messages is impossible since any scheme which allows one receiver to read a quantum message also allows the receiver to modify the message without the risk of being detected, and therefore all potential receivers of an authenticated message must be trustworthy. Therefore, if Barnum et al.’s conclusion is right, Zeng et al.’s scheme cannot be secure; or the other way round.

In the following, we show that Barnum et al.’s conclusion also adapts to Zeng et al.’s scheme and the scheme is insecure. Firstly, we assume the receiver Bob gets the message $P$ and the corresponding valid signature $|S\rangle = |\tilde{S}\rangle \otimes |\tilde{\Omega}\rangle$ using Zeng et al.’s scheme. We then show Bob can forge a valid signature $|S'\rangle$ of another message $P'$ beneficial to him using the following three steps:
– After decoding $|\tilde{S}\rangle$ using the way expressed in Eq. (1), Bob replaces the decoded message state $|P\rangle$ with a new message state $|P'\rangle$, and the state of the whole system is changed to $|\Phi\rangle = J ||^{\frac{1}{2}} |P'\rangle_{r_2,r_{k+1}} |\Omega\rangle_{r_3,r_{k+2}} \cdots |\Omega\rangle_{r_k,r_{2k-1}}$.

– Bob applies $U^\dagger$, the inverse transformation of $U$, on $|\Phi\rangle$ to get $|\tilde{S}'\rangle = U^\dagger |\Phi\rangle$.

– Bob generate the signature state $|S'\rangle = |\tilde{S}'\rangle \otimes |\tilde{\Omega}\rangle$ of $|P'\rangle$ by combing $|\tilde{S}'\rangle$ and $|\tilde{\Omega}\rangle$.

The new message-signature pair $(P',|S'\rangle)$ is valid as it is shown to pass the four steps of the verification phase due to the following points: (1) $|S\rangle$ Bob holds is supposed to be a valid signature, so the entanglement properties of $|\Omega\rangle_{r_2,r_{k+1}}, |\Omega\rangle_{r_3,r_{k+2}}, \ldots, |\Omega\rangle_{r_k,r_{2k-1}}$ are kept and the decoded state $|\Omega\rangle_{r_2,r_{k+1}}$ will be the same as $|\tilde{\Omega}\rangle$. That means Step (3) and Step (4) can be passed; (2) Due to $U|\tilde{S}'\rangle = UU^\dagger |\Phi\rangle = |\Phi\rangle$, Step (2) should also be passed; (3) Suppose $|S''\rangle = |\tilde{S}''\rangle \otimes |\tilde{\Omega}\rangle$ is the correct signature of $|P'\rangle$, then $|\tilde{S}''\rangle$ must be a 2k-particle QECC. As $U|\tilde{S}''\rangle = |\Phi\rangle = U|\tilde{S}'\rangle$, $|\tilde{S}'\rangle$ is identical to $|\tilde{S}''\rangle$ and also is a 2k-particle QECC which implies that Step (1) will be passed.

5 Conclusion

In this paper, we have shown arbitrated QS does not disobey Barnum et al.’s conclusion about the impossibility of QS for quantum messages [10], and the arbitrated QS under the proposed framework is possible to sign quantum messages with unconditional security. In addition, we have also explained that the existing true QS scheme presented by Zeng et al. [27] cannot get away from the restriction of Barnum et al.’s conclusion since the scheme is shown to be insecure. Nevertheless, Barnum et al.’s negative result does not preclude the possibility of QS for classical messages. So, how to construct efficient QS schemes to sign classical messages deserve further work.

Acknowledgements This work was partially supported by Natural Science Foundation of China (Grant Nos. 61202398, 61272295, and 61070232), Internal Research Grant of The Hong Kong Institute of Education (Grant No. RG 66/11-12), and the Foundation for Distinguished Young Talents in Higher Education of Guangdong (Grant No. LYM11093).

References

1. Rivest, R.: Cryptography, vol. 1, Chap. 13, pp. 715–755. Elsevier, Amsterdam (1990)
2. Shor, P.W.: In: Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science, pp. 124–134 (1994)
3. Bennett, C.H., Brassard, G.: In: Proceedings of the IEEE International Conference on Computers. Systems and Signal Processing, pp. 175–179 (1984)
4. Ekert, A.K.: Phys. Rev. Lett. 67, 661 (1991)
5. Brassard, G.: SIGACT News 20, 78 (1989)
6. Lo, H.K., Chau, H.F.: Science 283, 2050 (1999)
7. Bennett, C.H., Devincenzo, D.P.: Nature 404, 247 (2000)
8. Mayers, D.: J. ACM 48, 351 (2001)
9. Gottesman, D., Chuang, I.L.: Quantum Digital Signatures (2001). arXiv:quant-ph/0105032
10. Barnum, H., Crepeau, C., Gottesman, D., Smith, A., Tapp, A.: In: Proceedings of the 43th Annual IEEE Symposium on Foundations of Computer Science, pp. 449–458 (2002)
11. Zeng, G.H., Keitel, C.H.: Phys. Rev. A 65, 042312 (2002)
12. Curty, M., Lütkenhaus, N.: Phys. Rev. A 77, 046301 (2008)
13. Zeng, G.H.: Phys. Rev. A 78, 016301 (2008)
14. Li, Q., Chan, W.H., Long, D.Y.: Phys. Rev. A 79, 054307 (2009)
15. Zou, X.F., Qiu, D.W.: Phys. Rev. A 82, 042325 (2010)
16. Lee, H., Hong, C., Kim, H., Lim, J., Yang, H.J.: Phys. Lett. A 321, 295 (2004)
17. Lü, X., Feng, D.G.: In: Proceedings of the 1st International Symposium on Computational and Information Science, pp. 1054–1060 (2004)
18. Lü, X., Feng, D.G.: In: Proceedings of the 7th International Conference on Advanced Communication Technology, pp. 514–517 (2005)
19. Wang, J., Zhang, Q., Tang, C.J.: In: Proceedings of the 8th International Conference on Advanced Communication Technology, pp. 1375–1378 (2006)
20. Yang, Y.G., Wen, Q.Y.: Opt. Commun. 283, 3198 (2010)
21. Gao, F., Qin, S.J., Guo, F.Z., Wen, Q.Y.: Phys. Rev. A 84, 022344 (2011)
22. Choi, J.W., Chang, K.Y., Hong, D.: Phys. Rev. A 84, 062330 (2011)
23. Sun, Z.W., Du, R.G., Wang, B.H., Long, D.Y.: Improving the security of arbitrated quantum signature protocols (2011). Available at arXiv:1107.2459 [quant-ph]
24. Hwang, T., Luo, Y.P., Chong, S.K.: Phys. Rev. A 85, 056301 (2012)
25. Chong, S.K., Luo, Y.P., Hwang, T.: Opt. Commun. 284, 893 (2011)
26. Li, Q., Li, C.Q., Wen, Z.H., Zhao, W.Z., Chan, W.H.: J. Phys. A, Math. Theor. 46, 015307 (2013)
27. Zeng, G.H., Lee, M., Guo, Y., He, G.Q.: Int. J. Quantum Inf. 5, 553 (2007)
28. Wegman, M.N., Carter, L.: J. Comput. Syst. Sci. 22, 265 (1981)