# Arbitrated quantum signature scheme using Bell states

Qin Li,[1,2,*] W. H. Chan,[2] and Dong-Yang Long[1]
[1]*Department of Computer Science, Sun Yat-sen University, Guangzhou 510275, China*
[2]*Department of Mathematics, Hong Kong Baptist University, Kowloon, Hong Kong, China*
(Received 1 January 2009; published 21 May 2009)

In an arbitrated quantum signature scheme, the signatory signs the message and the receiver verifies the signature's validity with the assistance of the arbitrator. We present an arbitrated quantum signature scheme using two-particle entangled Bell states similar to the previous scheme using three-particle entangled Greenberger-Horne-Zeilinger states [G. H. Zeng and C. H. Keitel, Phys. Rev. A **65**, 042312 (2002)]. The proposed scheme can preserve the merits in the original scheme while providing a higher efficiency in transmission and reducing the complexity of implementation.

DOI: 10.1103/PhysRevA.79.054307 PACS number(s): 03.67.Dd, 03.65.Ud

## I. INTRODUCTION

Classical signature is an essential cryptographic primitive and has been employed in various applications, particularly in secure electronic commerce. However, if quantum computers could be available someday, Shor's algorithm [1] would break most of the classical signature schemes, whose security depends on the intractability of factoring large numbers or solving discrete logarithms. Researchers and scholars turn to investigate quantum signature, which is supposed to provide an alternative with unconditional security. Recently, some progress has been made on quantum signature [2–9].

In a recent paper, an arbitrated quantum signature scheme providing many merits was proposed [3]. In such a scheme, both known and unknown quantum states could be signed, and the unconditional security was ensured by using the correlation of Greenberger-Horne-Zeilinger (GHZ) triplet states [10] and quantum one-time pads. However, we observe that although the scheme in Ref. [3] takes advantage of the correlation of GHZ states, the correlation between the arbitrator and the other two parties has not been used. The arbitrator is unnecessary to be entangled and thus the GHZ states used in Ref. [3] can be replaced with Bell states. Moreover, the preparation and distribution of two-particle entangled Bell states are much easier to be implemented than that of three-particle entangled GHZ states with the present-day technologies. Therefore, we present an efficient arbitrated quantum signature scheme using two-particle entangled Bell states while retaining the advantages of the original scheme.

This Brief Report is organized as follows. First, in Sec. II, we give an arbitrated quantum signature scheme similar to that in Ref. [3] using Bell states. In Sec. III, we discuss the security and the efficiency of the proposed scheme. Finally, in Sec. IV, we make a conclusion.

## II. ARBITRATED QUANTUM SIGNATURE USING BELL STATES

From the arbitrated quantum signature scheme in Ref. [3], we observe that the main functions of the arbitrator are distributing reliable GHZ states and deciphering the ciphertext encrypted with the key $K_A$ to help the receiver Bob verify the signature. The arbitrator has nothing to do with the correlation caused by the three-particle entangled GHZ states but just sends his GHZ particles to Bob in step V3 of the verifying phase [11]. Thus, the arbitrator is unnecessary to be entangled with the other two participants and the three-particle entangled GHZ states used in the scheme can be displaced by two-particle entangled Bell states.

In the following, according to the original scheme proposed in Ref. [3] and the corresponding comments on this scheme [11,12], we present an efficient arbitrated quantum signature scheme using two-particle entangled Bell states, which can maintain the advantages of the scheme in Ref. [3]. The proposed scheme can be applied to both known and unknown quantum states and still provides unconditional security by utilizing the correlation of Bell states and quantum one-time pads.

The presented scheme also involves three participants, namely, signatory Alice, receiver Bob, and the arbitrator, and includes three phases, the initializing phase, the signing phase, and the verifying phase.

### A. Initializing phase

*Step I1*. Alice shares her secret key $K_A$ with the arbitrator through quantum key distribution protocols [13–15], which were proved to be unconditionally secure [16,17]. Likewise, Bob obtains his secret key $K_B$ shared with the arbitrator.

*Step I2*. The arbitrator that should be trusted by both Alice and Bob generates $N$ Bell states $|\psi\rangle=(|\psi_1\rangle,|\psi_2\rangle,\ldots,|\psi_N\rangle)$ with $|\psi_i\rangle=\frac{1}{\sqrt{2}}(|00\rangle_{AB}+|11\rangle_{AB})$, where the subscripts $A$ and $B$ correspond to Alice and Bob, respectively. Then the arbitrator distributes one particle of each Bell state to Alice and the other to Bob employing a secure and authenticated method [18,19]. This step can also be achieved as follows: first, the arbitrator and Alice can share $N$ Bell sates of almost perfect fidelity even if they are far away from each other [16] through the use of quantum repeaters [20,21] and fault-tolerant quantum computation [22,23], then the arbitrator sends his own particle of each Bell state to Bob in a secure and authenticated way [18,19].

*liqin805@163.com

 

TABLE I. The quantity of the transmitted qubits for the arbitrated quantum signature (AQS) when signing $N$-qubit message.

| Transmission | AQS using GHZ states in Ref. [3][a] | AQS using Bell states |
|---|---|---|
| Alice → Bob | $4N$ | $4N$ |
| Bob → The arbitrator | $5N$ | $4N$ |
| The arbitrator → Bob | $7N+1$ | $6N+1$ |

[a]Note that the quantity here differs from that counted in Ref. [4] since we count $N$ Bell states as $2N$ qubits.

### B. Signing phase

*Step S1*. Alice obtains a qubit string $|P\rangle=(|p_1\rangle,|p_2\rangle,\ldots,|p_N\rangle)$ related to the message with $|p_i\rangle=\alpha_i|0\rangle+\beta_i|1\rangle$. Here note that if known quantum states are to be signed, $|P\rangle$ can be prepared any copies and if unknown quantum states are to be signed, three copies of $|P\rangle$ are necessary (one to be combined with the Bell states, one to produce the secret qubit string $|R_A\rangle$, and the other to be sent to Bob), but if the dimension of $|P\rangle$ is not sufficiently large, more copies are needed to obtain a lower error probability of comparison tests for unknown quantum states and then reduce the failure probability of the verifying phase. Besides, the message states are provided depending on the specific applications. If Alice knows the information of the states, she can prepare them many copies, if Bob knows, he can provide many copies of the message states to Alice, and if the identities of the states are unknown to both Alice and Bob, the third party who needs Alice's signature of certain message to be verified by Bob is required to offer Alice the message states.

*Step S2*. Alice transforms the qubit string $|P\rangle$ into a secret qubit string $|R_A\rangle$ in terms of the key $K_A$. For instance, assume that the key $K_A$ is related to a collection of unitary operators $M_{K_A}=(M_{K_A^1}^1,M_{K_A^2}^2,\ldots,M_{K_A^N}^N)$. If $K_A^i=0$, she applies the bit flip operation $\sigma_x$, namely, $M_{K_A^i}^i=\sigma_x$, and if $K_A^i=1$, she applies the phase flip operation $\sigma_z$, namely, $M_{K_A^i}^i=\sigma_z$. Here notice that unitary operations are preferable since the encrypted states with $M_{K_A}$ can be decrypted with the corresponding Hermitian conjugate operators $M_{K_A}^\dagger$, while measurement operations are not usually reversible. Denote $|R_A\rangle=M_{K_A}(P)=(|r_1\rangle,|r_2\rangle,\ldots,|r_N\rangle)$ with $|r_i\rangle=M_{K_A^i}^i(p_i)$.

*Step S3*. Alice combines each message state and the Bell state by carrying out a joint measurement on both states and obtains the three-particle entangled state,

$$\begin{aligned}|\phi_i\rangle &= |p_i\rangle\otimes|\psi_i\rangle \\ &= \tfrac{1}{2}\{|\psi_{12}^+\rangle_A(\alpha_i|0\rangle_B+\beta_i|1\rangle_B)+|\psi_{12}^-\rangle_A(\alpha_i|0\rangle_B-\beta_i|1\rangle_B) \\ &\quad +|\phi_{12}^+\rangle_A(\alpha_i|1\rangle_B+\beta_i|0\rangle_B)+|\phi_{12}^-\rangle_A(\alpha_i|1\rangle_B-\beta_i|0\rangle_B)\},\end{aligned} \quad (1)$$

where $|\psi_{12}^+\rangle_A$, $|\psi_{12}^-\rangle_A$, $|\phi_{12}^+\rangle_A$, and $|\phi_{12}^-\rangle_A$ represent the four Bell states [24].

*Step S4*. Alice implements a Bell measurement on each three-particle entangled state $|\phi_i\rangle$ and obtains $M_A=(M_A^1,M_A^2,\ldots,M_A^N)$, where $M_A^i$ represents one of the four Bell states.

*Step S5*. Alice generates the signature $|S\rangle=E_{K_A}(M_A,|R_A\rangle)$ of the message $|P\rangle$ by encrypting $M_A$ and $|R_A\rangle$ with the secret key $K_A$ using the quantum one-time pad algorithm. Note that $M_A$, even if sometimes depicted by classical bits, can be transformed into qubits $|M_A\rangle$ according to the Bell basis. Then both $|M_A\rangle$ and $|R_A\rangle$ can be encrypted by quantum one-time pad algorithms [25].

*Step S6*. Alice transmits the signature $|S\rangle$ followed by the message $|P\rangle$ to Bob.

### C. Verifying phase

*Step V1*. Bob encrypts $|S\rangle$ and $|P\rangle$ using the key $K_B$ and sends the resultant outcomes $|Y_B\rangle=E_{K_B}(|S\rangle,|P\rangle)$ to the arbitrator.

*Step V2*. The arbitrator decrypts $|Y_B\rangle$ with $K_B$ and gets $|S\rangle$ and $|P\rangle$. Then he decrypts $|S\rangle$ using $K_A$ and obtains $M_A$ and $|R_A'\rangle$ which should be compared with $|R_A\rangle=M_{K_A}|P\rangle$. If $|R_A'\rangle=|R_A\rangle$, the arbitrator sets the verification parameter $r=1$; otherwise sets $r=0$.

Notice that this step includes quantum state comparison. The comparison of known quantum states can be made definitely, while the comparison of unknown quantum states cannot. Nevertheless, the error probability of determining whether two quantum bit strings are identical can be made small enough by adopting the approach in Ref. [26]. The approach was restated as follows.

Let $\varepsilon_i(i=1,2,\ldots,N)$ be the modulus of the inner product of the $i$th pair qubits in $|R_A'\rangle$ and $|R_A\rangle$. If $N$ is not sufficiently large sometimes, many copies (i.e., $3m$ copies) of $|P\rangle$ are required, $2m$ copies to produce two copies of the extensive message state $|\bar{P}\rangle=\otimes_{i=1}^m|P\rangle$, and the other $m$ copies to form the extensive secret qubit string $|\bar{R}_A\rangle=\otimes_{i=1}^m|R_A\rangle$ in the signing phase. For the $i$th pair qubits in $|R_A'\rangle$ and $|R_A\rangle$, we compare $|R_A'^i\rangle^{\otimes m}$ and $|R_A^i\rangle^{\otimes m}$ ($m$ copies of each pair). Let $n=(2m)!$ and $\sigma_0,\sigma_1,\ldots,\sigma_{n-1}$ comprise all the permutations on $2m$ items. Besides, a $n$-dimensional ancilla system $Q$ in the state $|0\rangle$ is introduced. We first perform the $n$-dimensional quantum Fourier transform $F$ on the ancilla system $Q$ which maps

$$|0\rangle\rightarrow\frac{1}{\sqrt{n}}\sum_{j=0}^{n-1}|j\rangle. \quad (2)$$

Then applying permutation $\sigma_j$ in one-to-one correspondence with the value of $Q$ being $|j\rangle$ on $|R_A'^i\rangle^{\otimes m}|R_A^i\rangle^{\otimes m}$, the state of the entire system should be

$$\frac{1}{\sqrt{n}}\sum_{j=0}^{n-1}|j\rangle\sigma_j(|R_A'^i\rangle\cdots|R_A'^i\rangle|R_A^i\rangle\cdots|R_A^i\rangle). \quad (3)$$

Finally we perform $F^\dagger$ on $Q$ and measure it with the projection operator $|0\rangle\langle 0|\otimes I$. If $|R_A'^i\rangle=|R_A^i\rangle$, the measurement outcome must be 0; otherwise, the probability of obtaining 0 (the error probability) is

$$\left\| \frac{1}{\sqrt{n}} \sum_{j=0}^{n-1} \langle 0|F^{\dagger}|j\rangle \sigma_j (|R_A'^i\rangle \cdots |R_A'^i\rangle |R_A^i\rangle \cdots |R_A^i\rangle) \right\|^2$$
$$= \left\| \frac{1}{n} \sum_{j=0}^{n-1} \sigma_j (|R_A'^i\rangle \cdots |R_A'^i\rangle |R_A^i\rangle \cdots |R_A^i\rangle) \right\|^2$$
$$= \frac{(m!)^2}{(2m)!} \sum_{k=0}^{m} \binom{m}{k}^2 \varepsilon_i^{2k} \leq \frac{(m!)^2}{(2m)!} (1+\varepsilon_i)^{2m}$$
$$\sim \sqrt{\pi m} \left( \frac{1+\varepsilon_i}{2} \right)^{2m}. \quad (4)$$

Suppose the attacker should successfully forge $l(l \leq N)$ qubits for passing the comparison tests and $\varepsilon = \max\{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_N\}$. The error probability after all the comparison tests must be $\bar{p}_e \leq \sqrt{\pi m}(\frac{1+\varepsilon^2}{2})^{2lm}$ which can be made small enough by choosing a suitable $l$ and $m$.

*Step V3.* The arbitrator obtains $|P\rangle$ from $|R_A\rangle$ according to the key $K_A$. This process can be accomplished by carrying out Hermitian conjugate operations $M_{K_A}^{\dagger}$ on $|R_A\rangle$, that is, $|P\rangle = M_{K_A}^{\dagger}|R_A\rangle = M_{K_A}^{\dagger} M_{K_A}|P\rangle$.

*Step V4.* The arbitrator sends the encrypted results $|Y_{aB}\rangle = E_{K_B}(M_A, |S\rangle, |P\rangle, r)$ to Bob.

*Step V5.* Bob decrypts $|Y_{aB}\rangle$ and obtains $M_A$, $|S\rangle$, $|P\rangle$, and $r$. If $r=0$, Bob considers that the signature has been obviously forged and rejects it; otherwise, Bob goes on the further verification.

*Step V6.* According to Alice's measurement outcomes $M_A$ and Eq. (1), Bob obtains $|P'\rangle$ by implementing the corresponding transformations denoted as Eq. (5) on his particles of the Bell states. For example, if Alice's measurement result is $|\psi_{12}^{+}\rangle_A$, then the state in Bob's hand must be $\alpha_i|0\rangle_B + \beta_i|1\rangle_B$. Thus Bob can obtain $|P'\rangle$ by applying the identity transformation $I$. The other transformations can be elaborated in the similar way. Then he makes comparisons between $|P'\rangle$ and $|P\rangle$. Here the way of comparing $|P'\rangle$ and $|P\rangle$ is the same as that of comparing $|R_A'\rangle$ and $|R_A\rangle$ in step V2. If $|P'\rangle = |P\rangle$, Bob accepts the signature $|S\rangle$ of the message $|P\rangle$; otherwise he rejects it.

$$|\psi_{12}^{+}\rangle_A \to I, \quad |\psi_{12}^{-}\rangle_A \to \sigma_z,$$
$$|\phi_{12}^{+}\rangle_A \to \sigma_x, \quad |\phi_{12}^{-}\rangle_A \to \sigma_z\sigma_x. \quad (5)$$

We conclude this section that the proposed arbitrated signature scheme using Bell states is suitable for both known and unknown quantum states as the original scheme in Ref. [3] did. And we emphasize that in the scheme of Ref. [3] and the scheme presented above, the fact that unknown quantum states can be signed is not in contradiction with the consequence given in Ref. [18] that it is impossible to sign unknown quantum states. The significant reason is that a trusted arbitrator is introduced. Barnum *et al.* [18] showed that, since authentication of unknown quantum states requires encryption, signing them is impossible: any protocol which allows one receiver to learn the identity of the state also allows him or her to modify it without risk of detection, and thus all potential receivers of an authenticated state must be trustworthy. In the scheme in Ref. [3] and the scheme we propose, the signature $|S\rangle = E_{K_A}(M_A, |R_A\rangle)$ can be considered as a special kind of authentication. Due to the quantum one-time pad, the receiver Bob or other malicious parties can obtain nothing from $|S\rangle$, while the arbitrator who is trustworthy can verify it. In fact, the verification of the signature is implemented by the arbitrator who gives a parameter to indicate whether the signature is valid. The receiver only gets such parameter and other useful information to complete the further verification.

## III. SECURITY ANALYSIS AND DISCUSSION

A secure quantum signature scheme should satisfy two requirements: one is that the signature should not be forged by the attacker (including the malicious receiver) and the other is the impossibility of disavowal by the signatory and the receiver. We show that the proposed scheme can offer unconditional security as the scheme in Ref. [3] did.

### A. Impossibility of forgery

If the malicious receiver Bob attempts to counterfeit the signatory Alice's signature $|S\rangle = E_{K_A}(M_A, |R_A\rangle)$ to his own benefit, he has to know Alice's secret key $K_A$. However, this is impossible due to the unconditionally secure quantum key distribution. Besides, the use of quantum one-time pad algorithm enhances the security. Thus Bob cannot get the correct $|R_A\rangle$. Subsequently the parameter $r$ used in the verifying phase will not be right, so the arbitrator will discover this forgery.

If the attacker Eve tries to forge Alice's signature $|S\rangle = E_{K_A}(M_A, |R_A\rangle)$ for his own sake, he also should know Alice's secret key $K_A$. However, the public information that he can obtain such as $|S\rangle$, $|P\rangle$, $|Y_B\rangle$, and $|Y_{aB}\rangle$ betrays nothing about the secret key $K_A$. Hence the forgery for Eve is also impossible. In the worse situation, for instance, in which the secret key $K_A$ is exposed to Eve, Eve still cannot forge the signature since he cannot create appropriate $M_A$ related to the new message. Bob would find such forgery using the correlation of the Bell states because the further verification about $|P'\rangle = |P\rangle$ could not hold without the correct $M_A$. But note that if Bob knows the key $K_A$, such forgery will not be avoided.

### B. Impossibility of disavowal by the signatory and the receiver

If the signatory Alice and the receiver Bob disagree with each other, the arbitrated trusted by both of them should be required to make a judgment.

Assume Alice disavows her signature. Then the arbitrator can confirm that Alice has signed the message since the information of Alice's secret key $K_A$ is involved in the signature $|S\rangle = E_{K_A}(M_A, |R_A\rangle)$. Hence Alice cannot deny having signed the message.

Similarly, suppose Bob repudiates the receipt of the signature. Then the arbitrator also can confirm that Bob has received the signature $|S\rangle$ and the message $|P\rangle$ since he needs the assistance of the arbitrator to verify the signature. For instance, the information of his key $K_B$ is included in $|Y_B\rangle$

TABLE II. The complexity of implementing an AQS scheme.

| Complexity of implementation | AQS using GHZ states in Ref. [3] | AQS using Bell states |
|---|---|---|
| Preparing initial entangled states | $N$ GHZ states | $N$ Bell stats |
| Applying joint measurements on message qubits and entangled states | $N$ times | $N$ times |
| Applying Bell measurements | $N$ times | $N$ times |
| Applying von Neumann measurements | $N$ times | 0 times |

$=E_{K_B}(|S\rangle,|P\rangle)$. So Bob cannot disavow that he has received $|S\rangle$ and $|P\rangle$.

### C. Comparisons between the two schemes

The proposed arbitrated quantum signature scheme using two-particle entangled Bell states maintains the merits of the scheme using three-particle entangled GHZ states in Ref. [3]. The scheme can be adapted to both known and unknown quantum states and still provides unconditional security by employing the correlation of Bell states and quantum one-time pads. Furthermore, the proposed scheme is more efficient in two aspects: one is that the total number of the transmitted qubits when $N$-qubit message is signed is decreased as described in Table I and the other is that the complexity of implementing the scheme is reduced as depicted in Table II, for example, in the proposed scheme, preparing Bell states is less difficult than preparing GHZ states and performing von Neumann measurements is unnecessary. Thus we conclude that the scheme using Bell states achieves a higher efficiency in transmission and is simpler.

## IV. CONCLUSION

We observe that the arbitrator has nothing to do with the correlation caused by the three-particle entangled GHZ states in the scheme of Ref. [3] and thus propose a similar arbitrated quantum signature scheme employing two-particle entangled Bell states, which not only maintains the advantages of the original scheme but also offers a higher efficiency in transmission and is much easier to implement.

## ACKNOWLEDGMENTS

We would like to appreciate G. H. Zeng and J. X. Li for useful suggestions and discussions. We also want to thank the anonymous referee for constructive comments. This work was sponsored by the National Natural Science Foundation of China (Projects No. 60573039 and No. 60503005) and the Guangdong Provincial Natural Science Foundation (Projects No. 04205407 and No. 5003350), and the Faculty Research (Grant No. FRG2/08–09/070) Hong Kong Baptist University.

[1] P. W. Shor, SIAM Rev. **41**, 303 (1999).
[2] D. Gottesman and I. L. Chuang, e-print arXiv:quant-ph/0105032.
[3] G. H. Zeng and C. H. Keitel, Phys. Rev. A **65**, 042312 (2002).
[4] H. Lee, C. Hong, H. Kim, J. Lim, and H. J. Yang, Phys. Lett. A **321**, 295 (2004).
[5] X. Lü and D. G. Feng, *Proceedings of the First International Symposium on Computational and Information Science* (Springer, Berlin, 2004), p. 1054.
[6] J. Wang, Q. Zhang, and C. J. Tang, *Proceedings of the Eighth International Conference on Advanced Communication Technology* (IEEE, New York, 2006), p. 1375.
[7] X. J. Wen, Y. Liu, and Y. Sun, Z. Naturforsch. A: Phys. Sci. **62a**, 147 (2007).
[8] G. H. Zeng, M. Lee, Y. Guo, and G. Q. He, Int. J. Quantum Inf. **5**, 553 (2007).
[9] Y. G. Yang, Chin. Phys. B **17**, 415 (2008).
[10] D. M. Greenberger, M. A. Horne, and A. Zeilinger, in *Bell's Theorem, Quantum Theory, and Conceptions of Universe*, edited by M. Kaftos (Kluwer, Dordrecht, 1989); D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, Am. J. Phys. **58**, 1131 (1990).
[11] G. H. Zeng, Phys. Rev. A **78**, 016301 (2008).
[12] M. Curty and N. Lütkenhaus, Phys. Rev. A **77**, 046301 (2008).
[13] C. H. Bennett and G. Brassard, *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), p. 175.
[14] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[15] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[16] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[17] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[18] H. Barnum, C. Crépeau, D. Gottesman, A. Smith, and A. Tapp, *Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science* (IEEE, Los Alamitos, 2002), p. 449.
[19] M. Curty, D. J. Santos, E. Pérez, and P. García-Fernández, Phys. Rev. A **66**, 022301 (2002).
[20] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).
[21] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, Nature (London) **414**, 413 (2001).
[22] P. W. Shor, *Proceedings of the 37th Symposium on Foundations of Computer Science* (IEEE, Los Alamitos, 1996), p. 56.
[23] D. Aharonov and M. Ben-Or, *Proceedings of the 29th Annual ACM Symposium on Theory of Computing* (ACM, New York, 1997), p. 176.
[24] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, Phys. Rev. Lett. **75**, 4337 (1995).
[25] P. O. Boykin and V. Roychowdhury, Phys. Rev. A **67**, 042317 (2003).
[26] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, Phys. Rev. Lett. **87**, 167902 (2001).