International Journal of Theoretical Physics (2019) 58: 1036–1045
https://doi.org/10.1007/s10773-018-03995-4

Arbitrary Quantum Signature Based on Local Indistinguishability of Orthogonal Product States

Dong-Huan Jiang[1] · **Yan-Long Xu**[1] · **Guang-Bao Xu**[1]

Received: 4 September 2018 / Accepted: 22 December 2018 / Published online: 4 January 2019

Abstract
Digital signature plays an important role in cryptography. Many quantum digital signature (QDS) schemes have been proposed up to now since the security of classic digital signature (CDS) schemes becomes more and more vulnerable with the development of quantum computing algorithms. Most of the existing quantum signature schemes are based on probabilistic comparison of quantum states, which makes the schemes very complicated. In this paper, we propose a new QDS scheme based on local indistinguishability of orthogonal product states. In the scheme, the receiver cooperates with the arbitrator to verify the valid of the signature. The analysis of security and efficiency shows that our scheme is secure and efficient.

Keywords Digital signature · Quantum digtial signature · Local indistinguishability

1 Introduction

Classical digital signature (CDS) can authenticate the integrity of a signed message and the identity of a signatory. It has been widely used in many practical occasions [1, 2], such as e-payment system, e-government, and so on. As we know, the security of classical digital signature (CDS) generally depends on the assumption of computational complexity (e.g. the factoring problem and discrete logarithm problem). However, the security of CDS is seriously challenged because of rapid development of quantum algorithms. Fortunately, quantum digital signature, which is based on the laws of quantum mechanics, is attracting a lot of attention since it can resist the attacks of quantum algorithms.

To achieve different purposes, various quantum signature schemes, such as arbitrated quantum signature (AQS) [3–9], quantum group signature (QGS) [10–12], quantum proxy signature (QPS) [13–15], quantum blind signature (QBS) [16–19], have been proposed. In Ref. [3], Zeng et al. gave the first AQS model by using the correlation of Greenberger-Horne-Zeilinger (GHZ) triplet states. Inspired by this pioneering work, Li et al. [7] replaced

✉ Guang-Bao Xu
xu_guangbao@163.com

[1] College of Mathematics and Systems Science, Shandong University of Science and Technology, Qingdao, 266590, China

GHZ states with Bell states to give a more efficient AQS scheme. Later, Zou et al. [8] pointed out that these two schemes are insecure since the receiver can deny a valid signature and presented two new AQS schemes. Gao et al. [20] and Hwang et al. [21] pointed out that most of the previous signature schemes cannot resist a known message attack of the receiver. Recently, Yang et al. presented an AQS scheme [22] with cluster states. This scheme can achieve an efficiency of 100%. Inspired by the work [22], Fatahi et al. proposed a high-efficient arbitrated quantum signature scheme based on cluster states. However, these schemes are very difficult to implement since it is very difficult to prepare these cluster states under current conditions.

The local distinguishability of orthogonal product states is an important research topic in the field of quantum information. In recent years, many results about the local distinguishability of orthogonal product states have been proposed [23–28]. As we know, the preparation of product states consumes less resources compared with entangled states.

In this paper, we propose an AQS scheme which is based on the local indistinguishability of orthogonal product states. In this scheme, different particles of a state that comes from a set of indistinguishable product states are transmitted separately, which can improve the security of the scheme. The rest of the paper is organised as follows. In Section 2, some fundamental preliminaries are introduced. In Section 3, we give a detailed description for the proposed AQS scheme. In Section 4, We discuss the security and efficiency of the proposed scheme. At last, a short conclusion is given in Section 5.

2 Preliminaries

In this section, we introduce some preliminaries that are used in what follows. We say a set of orthogonal product states is locally indistinguishable [28, 29] if it cannot be perfectly distinguished by local operations and classical communications (LOCC).

Theorem 1 *The set of orthogonal product states (1)*

$$\begin{aligned}
|\psi_1\rangle &= |0\rangle_1|0\rangle_2|0\rangle_3,\\
|\psi_2\rangle &= |1\rangle_1|1\rangle_2|1\rangle_3,\\
|\psi_{3,4}\rangle &= \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)_1|0\rangle_2|1\rangle_3,\\
|\psi_{5,6}\rangle &= \frac{1}{\sqrt{2}}|1\rangle_1(|0\rangle \pm |1\rangle)_2|0\rangle_3,\\
|\psi_{7,8}\rangle &= \frac{1}{\sqrt{2}}|0\rangle_1|1\rangle_2(|0\rangle \pm |1\rangle)_3
\end{aligned} \tag{1}$$

cannot be perfectly distinguished by LOCC.

Proof Now we prove these states (1) cannot be perfectly distinguished by LOCC. To distinguish these eight product states, one of the three parties must start with a positive-operator-valued measure (POVM). Without loss of generality, suppose that the first party goes first with a set of general 2×2 POVM elements $\{M_k^\dagger M_k;\ k = 1, 2, \ldots, l_1\}$, where

$$M_k^\dagger M_k = \begin{bmatrix} m_{00}^k & m_{01}^k \\ m_{10}^k & m_{11}^k \end{bmatrix}$$

under the basis $\{|0\rangle, |1\rangle\}$. It is noted that the postmeasurement states must be pairwise orthogonal for making further discrimination feasible. That is, the states that are orthogonal on the first side should maintain the orthogonality on the first side after the measurement.

For the states $|\psi_5\rangle$ and $|\psi_7\rangle$, we have

$$\langle\psi_5|M_k^\dagger M_k \otimes (I_{2\times 2}^\dagger I_{2\times 2}) \otimes (I_{2\times 2}^\dagger I_{2\times 2})|\psi_7\rangle = 0$$

and

$$\langle\psi_7|M_k^\dagger M_k \otimes (I_{2\times 2}^\dagger I_{2\times 2}) \otimes (I_{2\times 2}^\dagger I_{2\times 2})|\psi_5\rangle = 0.$$

Thus, we can get

$$\frac{1}{2}\langle 1|M_k^\dagger M_k|0\rangle[(\langle 0| + \langle 1|)I_{2\times 2}^\dagger I_{2\times 2}|1\rangle][\langle 0|I_2^\dagger I_{2\times 2}(|0\rangle + |1\rangle)] = 0$$

and

$$\frac{1}{2}\langle 0|M_k^\dagger M_k|1\rangle[\langle 1|I_{2\times 2}^\dagger I_{2\times 2}(|0\rangle + |1\rangle)][(\langle 0| + \langle 1|)I_{2\times 2}^\dagger I_{2\times 2}|0\rangle] = 0.$$

So, we have

$$m_{10}^k = 0, \tag{2}$$

$$m_{01}^k = 0. \tag{3}$$

For the states $|\psi_3\rangle$ and $|\psi_4\rangle$, we have

$$\langle\psi_3|M_k^\dagger M_k \otimes (I_{2\times 2}^\dagger I_{2\times 2}) \otimes (I_{2\times 2}^\dagger I_{2\times 2})|\psi_4\rangle = 0.$$

Thus,

$$\frac{1}{2}[(\langle 0| + \langle 1|)M_k^\dagger M_k[|0\rangle - |1\rangle][\langle 0|I_{2\times 2}^\dagger I_{2\times 2}|0\rangle][\langle 1|I_{2\times 2}^\dagger I_{2\times 2}|1\rangle] = 0.$$

So, we have

$$m_{00}^k = m_{11}^k. \tag{4}$$

This means that any of the POVM elements of the first party should be in the form

$$M_k^\dagger M_k = \begin{bmatrix} m_{00}^k & 0 \\ 0 & m_{00}^k \end{bmatrix}. \tag{5}$$

Consider the product states $|\psi_6\rangle$ and $|\psi_8\rangle$. If the first party discriminates these states outright then for one of states $|\psi_6\rangle$ and $|\psi_8\rangle$,

$$\langle\psi_i|M_k^\dagger M_k \otimes (I_{2\times 2}^\dagger I_{2\times 2}) \otimes (I_{2\times 2}^\dagger I_{2\times 2})|\psi_i\rangle = 0.$$

But given (5),

$$\langle\psi_i|M_k^\dagger M_k \otimes (I_{2\times 2}^\dagger I_{2\times 2}) \otimes (I_{2\times 2}^\dagger I_{2\times 2})|\psi_i\rangle = m_{00}^k.$$

Therefore, $m_{00}^k = 0$ and, since POVM elements must be positive, $M_k^\dagger M_k$ is the null matrix.

According to the above analysis, all of the first party's POVM elements must be proportional to the identity. Thus, the first party cannot go first; by the symmetry of states (1), neither the second party nor the third party can do it. Therefore, these states are locally indistinguishable. This completes the proof. □

3 The Proposed AQS Scheme

The proposed scheme involves three participants, namely, the signatory Alice, the receiver Bob and the arbitrator Trent. It should be noted that the arbitrator Trent is a disinterested third party and is trusted by Alice and Bob. The scheme is composed of three phases: initializing phase, signing phase, and verifying phase.

3.1 Initializing Phase

Suppose that $m = \{m_1, m_2, \cdots, m_n\}$ is a $3n$-bit message to be signed, where $m_i \in \{000, 001, 010, 011, 100, 101, 110, 111\}$ for $i = 1, 2, \ldots, n$.

(1) Trent establishes an n-bit shared secret key $K_{AT} = \{K_{AT}^1, K_{AT}^2, \ldots, K_{AT}^n\}$ with Alice and an n-bit shared secret key $K_{BT} = \{K_{BT}^1, K_{BT}^2, \ldots, K_{BT}^n\}$ with Bob by quantum key distribution protocol [30–36].
(2) Alice establishes an n-bit shared secret key $K_{AB} = \{K_{AB}^1, K_{AB}^2, \ldots, K_{AB}^n\}$ with Bob by quantum key distribution protocol [30–36].

3.2 Signing Phase

(1) Alice encodes the message m as a quantum sequence $|S\rangle$ according to the following rules:

$$
\begin{aligned}
&m_i = 000 : \longmapsto |S^i\rangle = |\psi_1\rangle = |0\rangle_1|0\rangle_2|0\rangle_3,\\
&m_i = 111 : \longmapsto |S^i\rangle = |\psi_2\rangle = |1\rangle_1|1\rangle_2|1\rangle_3,\\
&m_i = 001 : \longmapsto |S^i\rangle = |\psi_3\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_1|0\rangle_2|1\rangle_3,\\
&m_i = 010 : \longmapsto |S^i\rangle = |\psi_4\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)_1|0\rangle_2|1\rangle_3,\\
&m_i = 100 : \longmapsto |S^i\rangle = |\psi_5\rangle = \frac{1}{\sqrt{2}}|1\rangle_1(|0\rangle + |1\rangle)_2|0\rangle_3,\\
&m_i = 011 : \longmapsto |S^i\rangle = |\psi_6\rangle = \frac{1}{\sqrt{2}}|1\rangle_1(|0\rangle - |1\rangle)_2|0\rangle_3,\\
&m_i = 101 : \longmapsto |S^i\rangle = |\psi_7\rangle = \frac{1}{\sqrt{2}}|0\rangle_1|1\rangle_2(|0\rangle + |1\rangle)_3,\\
&m_i = 110 : \longmapsto |S^i\rangle = |\psi_8\rangle = \frac{1}{\sqrt{2}}|0\rangle_1|1\rangle_2(|0\rangle - |1\rangle)_3,
\end{aligned}
\tag{6}
$$

where $|S^i\rangle$ is the i-th product state of the sequence $|S\rangle$ for $i = 1, 2, \ldots, n$.
(2) Alice firstly generates the quantum sequence $|S\rangle$. Then, she picks out the j-th particle of each product state of $|S\rangle$ to form the sequence $|S_{(j)}\rangle$ for $j = 1, 2, 3$.
(3) For the first sequence $|S_{(1)}\rangle$, Alice performs the following unitary operation on the i-th particle $|S_{(1)}^i\rangle$ according to the i-th bit of K_{AB} to get a new particle $|\overline{S}_{(1)}^i\rangle$, i.e., $H^{K_{AB}^i}|S_{(1)}^i\rangle = |\overline{S}_{(1)}^i\rangle$, where

$$
H \equiv \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}
$$

is the Hadamard gate, $H^{K^i_{AB}} = I$ (unit operator) if $K^i_{AB} = 0$ and $H^{K^i_{AB}} = H$ (Hadamard gate) if $K^i_{AB} = 1$ for $i = 1, 2, \cdots, n$.

By this step, Alice changes the sequence $|S_{(1)}\rangle$ to a new sequence $|\overline{S}_{(1)}\rangle$.

(4) For the second sequence $|S_{(2)}\rangle$, Alice performs the following unitary operation on the i-th particle $|S^i_{(2)}\rangle$ according to the i-th bit of K_{AT} to get a new particle $|\overline{S}^i_{(2)}\rangle$, i.e., $H^{K^i_{AT}}|S^i_{(2)}\rangle = |\overline{S}^i_{(2)}\rangle$, where H is the Hadamard gate, $H^{K^i_{AT}} = I$ (unit operator) if $K^i_{AT} = 0$ and $H^{K^i_{AT}} = H$ (Hadamard gate) if $K^i_{AT} = 1$ for $j = 1, 2, \cdots, n$.

By this step, Alice changes the sequence $|S_{(2)}\rangle$ to a new sequence $|\overline{S}_{(2)}\rangle$.

(5) Firstly, Alice generates $3l$ decoy particles that are randomly in one of the four states: $|0\rangle$, $|1\rangle$, $|+\rangle$ and $|-\rangle$ for checking eavesdropping, where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Next she randomly inserts these $3l$ decoy particles into the quantum sequences $|\overline{S}_{(1)}\rangle$, $|\overline{S}_{(2)}\rangle$, $|S_{(3)}\rangle$ and gets three corresponding sequences: $|\overline{S}'_{(1)}\rangle$, $|\overline{S}'_{(2)}\rangle$ and $|S'_{(3)}\rangle$. Then she encrypts m with K_{AB} to get an encrypted message $C = E_{K_{AB}}(m)$. Finally, Alice sends $\{|\overline{S}'_{(1)}\rangle, |\overline{S}'_{(2)}\rangle, |S'_{(3)}\rangle, C\}$ to Bob.

(6) After confirming that Bob has received $\{|\overline{S}'_{(1)}\rangle, |\overline{S}'_{(2)}\rangle, |S'_{(3)}\rangle, C\}$, Alice announces the positions and the initial states of the decoy particles in the quantum sequences $|\overline{S}'_{(1)}\rangle$, $|\overline{S}'_{(2)}\rangle$ and $|S'_{(3)}\rangle$. Then for each of the decoy particles, Bob measures it with the corresponding basis and compares the measurement outcome with its initial state. If there exist no errors, Bob continues to the next step; otherwise, he restarts the protocol.

(7) After checking eavesdropping, Bob can recover the quantum sequences $|\overline{S}_{(1)}\rangle$, $|\overline{S}_{(2)}\rangle$ and $|S_{(3)}\rangle$. For the i-th particle $|\overline{S}^i_{(1)}\rangle$ of $|\overline{S}_{(1)}\rangle$, Bob performs the operation $H^{K^i_{AB}}$, where $H^{K^i_{AB}} = I$ if $K^i_{AB} = 0$ and $H^{K^i_{AB}} = H$ if $K^i_{AB} = 1$ for $i = 1, 2, \ldots, n$. Thus Bob can get the sequence $|S_{(1)}\rangle$ since $H^{K^i_{AB}}|\overline{S}^i_{(1)}\rangle = |S^i_{(1)}\rangle$. For the i-th particle $|S^i_{(3)}\rangle$ of $|S_{(3)}\rangle$, Bob performs the operation $H^{K^i_{BT}}$. Thus Bob can get the sequence $|\overline{S}_{(3)}\rangle$ according to $H^{K^i_{BT}}|S^i_{(3)}\rangle = |\overline{S}^i_{(3)}\rangle$ for $i = 1, 2, \ldots, n$.

(8) Bob decrypts C to get the message m by $m = D_{K_{AB}}(C)$ and encrypts m to get $\overline{C}$ by $\overline{C} = E_{K_{BT}}(m)$.

Bob stores $S_A = \{|S_{(1)}\rangle, |\overline{S}_{(2)}\rangle, |\overline{S}_{(3)}\rangle, \overline{C}\}$ as Alice's signature about the message m.

3.3 Verifying Phase

(1) For checking eavesdropping, Bob generates $3l$ decoy states that are randomly in one of the four states: $|0\rangle$, $|1\rangle$, $|+\rangle$ and $|-\rangle$, where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Then he randomly inserts these $3l$ decoy states into the quantum sequences $|S_{(1)}\rangle$, $|\overline{S}_{(2)}\rangle$ and $|\overline{S}_{(3)}\rangle$ to get three quantum sequences $|S''_{(1)}\rangle$, $|\overline{S}''_{(2)}\rangle$ and $|\overline{S}''_{(3)}\rangle$. Bob sends the quantum sequences $\{|S''_{(1)}\rangle, |\overline{S}''_{(2)}\rangle, |\overline{S}''_{(3)}\rangle\}$ and the encrypted message $\overline{C}$ to Trent.

(2) After confirming that Trent has received the quantum sequences $\{|S''_{(1)}\rangle, |\overline{S}''_{(2)}\rangle, |\overline{S}''_{(3)}\rangle\}$ and the encrypted message $\overline{C}$, Bob announces the positions and the initial states of the decoy particles in these three sequences. Then for each of the decoy particles, Bob measures it with the corresponding basis and compares the measurement outcome with

its initial state. If there exist no errors, Trent continue to the next step; otherwise, he restarts the protocol.

(3) After checking eavesdropping, Trent can recover the quantum sequences $|S_{(1)}\rangle$, $|\overline{S}_{(2)}\rangle$ and $|\overline{S}_{(3)}\rangle$. For the i-th particle $|\overline{S}^i_{(2)}\rangle$ of $|\overline{S}_{(2)}\rangle$, Trent performs the operation $H^{K^i_{AT}}$, where $H^{K^i_{AT}} = I$ if $K^i_{AT} = 0$ and $H^{K^i_{AT}} = H$ if $K^i_{AT} = 1$ for $i = 1, 2, \ldots, n$. Thus Trent can recover the sequence $|S_{(2)}\rangle$ since $H^{K^i_{AT}}|\overline{S}^i_{(2)}\rangle = |S^i_{(2)}\rangle$. For the i-th particle $|\overline{S}^i_{(3)}\rangle$ of $|\overline{S}_{(3)}\rangle$, Trent performs the operation $H^{K^i_{BT}}$, where $H^{K^i_{BT}} = I$ if $K^i_{BT} = 0$ and $H^{K^i_{BT}} = H$ if $K^i_{BT} = 1$ for $i = 1, 2, \ldots, n$. Thus Trent can recover the sequence $|S_{(3)}\rangle$.

(4) Firstly, Trent recovers the sequence $|S\rangle$ by $|S_{(1)}\rangle$, $|S_{(2)}\rangle$ and $|S_{(3)}\rangle$. Secondly, Trent measures each product state of $|S\rangle$ with the product basis (1) and records the measurement outcomes. Here we denote the measurement outcomes as $\overline{m}$.

(5) Trent recovers the message m by $m = D_{K_{BT}}(\overline{C})$ and compares m with $\overline{m}$. If $m = \overline{m}$, he announces Alice's signature is valid; while he announces Alice's signature is invalid if $m \neq \overline{m}$.

4 Security and Efficiency Analysis

In this section, we will first discuss the security of the scheme and then analyze the efficiency of the scheme. As we know, a secure AQS should meet two properties:

- *Unforgeability*. Neither an outside attacker nor the signature receiver can generate a valid signature except a legal signatory.
- *Undeniability*. If a signatory had signed a valid signature, he cannot successfully deny the signature.

4.1 Unforgeability

As a signature scheme, unforgeability is an important property. We will show that nobody can forge Alice's valid signature. In fact, there exist two kinds of attacks. One is the outside attacks; the other is the participant's attacks.

(1) Outsider attacks

From the steps of quantum signature, an outside attacker has two chances to attack our proposed scheme. The first time is when Alice sends $\{|\overline{S}'_{(1)}\rangle, |\overline{S}'_{(2)}\rangle, |S'_{(3)}\rangle, C\}$ to Bob. The second time is when Bob sends the quantum sequences $|S''_{(1)}\rangle$, $|\overline{S}''_{(2)}\rangle$ and $|\overline{S}''_{(3)}\rangle$ to Trent. In fact, the sequences $\{|\overline{S}'_{(1)}\rangle, |\overline{S}'_{(2)}\rangle, |S'_{(3)}\rangle\}$ and the sequences $\{|S''_{(1)}\rangle, |\overline{S}''_{(2)}\rangle, |\overline{S}''_{(3)}\rangle\}$ are inserted into decoy particles which are randomly in one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Just like the situation in BB84 protocol [37], if an outside attacker eavesdrops in the transmission process of quantum sequences, his/her eavesdropping actions will inevitably disturb part of the decoy particles. Thus his/her eavesdropping actions must be found by Bob or Trent.

(2) Participant's attacks

We consider the situation that Bob is a dishonest participant who wants to forge a valid signature of Alice. To forge a valid signature, Bob needs to know the shared key K_{AT} of Alice and Trent. Thus Bob should know which state each particle of the

sequence $|\overline{S}_{(2)}\rangle$ is in. Of course Bob couldn't measure these particles directly because he is not sure which basis of the two mutually unbiased bases $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ is correct for each particle of $|\overline{S}_{(2)}\rangle$. Now we consider that Bob uses entanglement-measure attack to get the key K_{AT}. That is, he performs a collective operation U on each particle and an auxiliary system $|\varepsilon\rangle$. Without loss of generality, suppose that the operation U holds:

$$U(|0\rangle|\varepsilon\rangle) = \lambda_1|\xi_1\varepsilon_1\rangle + \lambda_2|\xi_2\varepsilon_2\rangle \tag{7}$$

$$U(|1\rangle|\varepsilon\rangle) = \mu_1|\zeta_1\varepsilon_1'\rangle + \mu_2|\zeta_2\varepsilon_2'\rangle \tag{8}$$

Here, $|\lambda_1|^2 + |\lambda_2|^2 = |\mu_1|^2 + |\mu_2|^2 = 1$, $\langle\xi_1|\xi_2\rangle = \langle\varepsilon_1|\varepsilon_2\rangle = \langle\zeta_1|\zeta_2\rangle = \langle\varepsilon_1'|\varepsilon_2'\rangle = 0$. (The right parts of (7) and (8) are in the forms of Schmidt decomposition.) If Bob wants to extract the useful information to be used to discriminate the particles $|0\rangle$ and $1\rangle$ in $|\overline{S}_{(2)}\rangle$ precisely, the two reduced density matrices of Bob's auxiliary systems $|\lambda_1|^2|\varepsilon_1\rangle\langle\varepsilon_1| + |\lambda_2|^2|\varepsilon_2\rangle\langle\varepsilon_2|$ and $|\mu_1|^2|\varepsilon_1'\rangle\langle\varepsilon_1'| + |\mu_2|^2|\varepsilon_2'\rangle\langle\varepsilon_2'|$ must be discriminated precisely. That means $\langle\varepsilon_i|\varepsilon_j'\rangle = 0$, where $i, j = 1, 2$. With this condition, the unitary transformation of U on the particles $|+\rangle$ and $|-\rangle$ of $|\overline{S}_{(2)}\rangle$ has the universal form

$$U(\frac{1}{\sqrt{2}}(|0\rangle + \delta|1\rangle)|\varepsilon\rangle) = \frac{1}{\sqrt{2}}(\lambda_1|\xi_1\varepsilon_1\rangle + \lambda_2|\xi_2\varepsilon_2\rangle + \delta\mu_1|\zeta_1\varepsilon_1'\rangle + \delta\mu_2|\zeta_2\varepsilon_2'\rangle)$$

where $\delta = 1, -1$. Thus the reduced density matrices of auxiliary particles $|+\rangle$ and $|-\rangle$ of Bob are all

$\frac{1}{2}(|\lambda_1|^2|\varepsilon_1\rangle\langle\varepsilon_1| + |\lambda_2|^2|\varepsilon_2\rangle\langle\varepsilon_2) + |\mu_1|^2|\varepsilon_1'\rangle\langle\varepsilon_1'| + |\mu_2|^2|\varepsilon_2'\rangle\langle\varepsilon_2'|)$.

This means that Bob cannot discriminate $|+\rangle$ and $|-\rangle$ of $|\overline{S}_{(2)}\rangle$. Thus, Bob cannot get all the information of the sequence $|\overline{S}_{(2)}\rangle$ by entanglement-measure attack. Therefore, he cannot get the key K_{AT}.

In fact, it means that Bob has a method to discriminate $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ of $|\overline{S}_{(2)}\rangle$ if he can get all the information of the sequence $|\overline{S}_{(2)}\rangle$. However, this is impossible since $|0\rangle, |1\rangle$ and $|+\rangle, |-\rangle$ come from two mutually orthogonal unbiased basis.

4.2 Undeniability

Suppose that Alice has signed a signature S_A for a message m, but she wants to deny that he has signed the signature. In our scheme, it is easy for Trent to detect her deception. This is because the shared key K_{AT} of Alice and Trent is contained in the signature S_A. Once Trent has successfully verified the signature, Alice cannot deny its validity.

On the other hand, Bob cannot deny that he had received Alice's signature after Trent has successfully verified Alice's signature. This is because the sequences that Bob sent to Trent contain the information of the shared key K_{BT} of Bob and Trent. In short, neither Alice nor Bob can deny a valid signature.

4.3 Efficiency Analyses

In Refs. [38, 39], quantum efficiency is introduced to evaluate the efficiency of quantum protocols. For a quantum protocol, quantum efficiency is defined as

$$\eta = \frac{b_s}{q_t + b_t} \tag{9}$$

Table 1 Comparison between the existing schemes and our scheme

	Quantum resource	Quantum efficiency
The scheme of Ref. [22]	Cluster states	$\leq$64%
The scheme of Ref. [40]	Cluster states	64%
Our scheme	Product states	75%

where b_s represents the total number of the transmitted message bits, q_t is the number of the qubits exchanged in the protocol (the qubits used for checking eavesdropping are not counted) and b_t is the number of classical bits exchanged for decoding of the message (classical bits utilized for eavesdropping check are not counted).

In our scheme, Bob receives a $3n$ bits classical message while Trent receives a $3n$ bits classical message and $3n$ qubits. A total of $6n$ qubits are transmitted among Alice, Bob and Trent. It is obvious that $b_s = 9n$, $q_t = 6n$ and $b_t = 6n$. Thus we can get the efficiency of our scheme is $9n/(6n + 6n) = 75\%$.

We compare the efficiency of our scheme with that of Refs. [22] and [40] (See Table 1). It is obvious that our scheme is more efficient. Furthermore, compared with entangled states, product states can be obtained straightforwardly and no ancillary particles are required, thus our scheme is easier to implement than the schemes using cluster states.

5 Conclusions

In this paper, we propose an AQS scheme based on orthogonal product states that cannot be perfectly distinguished by LOCC. The proposed scheme can resist all known attacks. Compared with the existing schemes, our scheme is more efficient and easy to realize since the preparation and storage of orthogonal product states are relatively simple. It should be pointed out that the different particles of each orthogonal product state are separately transmitted in our scheme, which can ensure the security of the scheme.

The local distinguishability of orthogonal product states has got a lot of attention in the past two decades [23–28]. Our scheme is a useful exploration about the application of local indistinguishable orthogonal product states since there exist a few research results in this field [41–50].

Acknowledgements This work is supported by NSFC (Grant No. 61601171).

References

1. Mambo, M., Usuda, K., Okamoto, E.: Proxy signature: Delegation of the power to sign messages. IEICE Trans. Fundam. **E79**(A(9)), 1338–1353 (1996)
2. Cao, F., Cao, Z.F.: A secure identity-based proxy multi-signature scheme. Inf. Sci. **179**(3), 292–302 (2009)
3. Zeng, G.H., Keitel, C.H.: Arbitrated quantum-signature scheme. Phys. Rev. A **65**(4), 042312 (2002)
4. Curty, M., Lutkenhaus, N.: Comment on arbitrated quantum-signature scheme. Phys. Rev. A **77**(4), 046301 (2008)
5. Cao, Z.J., Markowitch, O.: A note on an arbitrated quantum signature scheme. Int. J. Quantum Inf. **7**(6), 1205–1209 (2009)

6. Zeng, G.H.: Reply to Comment on Arbitrated quantum-signature scheme. Phys. Rev. A **78**(1), 016301 (2008)
7. Li, Q., Chan, W.H., Long, D.Y.: Arbitrated quantum signature scheme using Bell states. Phys. Rev. A **79**(5), 054307 (2009)
8. Zou, X.F., Qiu, D.W.: Security analysis and improvements of arbitrated quantum signature schemes. Phys. Rev. A **82**, 042325 (2010)
9. Yang, Y.G., Wen, Q.Y.: Arbitrated quantum signature of classical messages against collective amplitude damping noise. Opt. Commun. **283**(16), 3198–3201 (2010)
10. Wen, X.J., Tian, Y., Ji, L.P., Niu, X.M.: A group signature scheme based on quantum teleportation. Phys. Scr. **81**(5), 055001 (2010)
11. Xu, R., Huang, L.S., Yang, W., He, L.B.: Quantum group blind signature scheme without entanglement. Opt. Commun. **284**(14), 3654–3658 (2011)
12. Yang, Y.G., Wen, Q.Y.: Quantum threshold group signature. Sci. Chin. Ser. G Phys. Astron. **51**(10), 1505–1514 (2008)
13. Yang, Y.G.: Multi-proxy quantum group signature scheme with threshold shared verification. Chin. Phys. B **17**(2), 415–418 (2008)
14. Wang, T.Y., Wei, Z.L.: One-time proxy signature based on quantum cryptography. Quantum Inf. Process. **11**(2), 455–463 (2012)
15. Shi, J.J., Shi, R.H., Guo, Y., Peng, X.Q., Tang, Y.: Batch proxy quantum blind signature scheme. Sci. Chin. Inf. Sci. **56**(5), 052115 (2013)
16. Wen, X.J., Niu, X.M., Ji, L.P., Tian, Y.: Aweak blind signature scheme based on quantum cryptography. Opt. Commun. **282**(4), 666–669 (2009)
17. Wang, T.Y., Wen, Q.: Fair quantum blind signatures. Chin. Phys. B **19**(6), 060307 (2010)
18. Yin, X.R., Ma, W.P., Liu, W.Y.: A blind quantum signature scheme with χ-type entangled states. Int. J. Theor. Phys. **51**(2), 455–461 (2012)
19. Lou, X.P., Chen, Z.G., Guo, Y.: A weak quantum blind signature with entanglement permutation. Int. J. Theor. Phys. **54**(9), 3283–3292 (2015)
20. Gao, F., Qin, S.J., Guo, F.Z., Wen, Q.Y.: Cryptanalysis of the arbitrated quantum signature protocols. Phys. Rev. A **84**(2), 022344 (2011)
21. 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)
22. Yang, Y.G., Lei, H., Liu, Z.C., et al.: Arbitrated quantum signature scheme based on cluster states. Quantum Inf. Process. **15**, 2487-2497 (2016)
23. Yu, S.X., Oh, C.H.: Detecting the local indistinguishability of maximally entangled states. arXiv:1502.01274v1 [quant-ph] (2015)
24. Wang, Y.L., Li, M.S., Zheng, Z.J., Fei, S.M.: Nonlocality of orthogonal product-basis quantum states. Phys. Rev. A **92**, 032313 (2015)
25. Zhang, Z.C., Gao, F., Cao, Y., Qin, S.J., Wen, Q.Y.: Local indistinguishability of orthogonal product states. Phys. Rev. A **93**, 012314 (2016)
26. Xu, G.B., Wen, Q.Y., Qin, S.J., Yang, Y.H., Gao, F.: Quantum nonlocality of multipartite orthogonal product states. Phys. Rev. A **93**(3), 032341 (2016)
27. Xu, G.B., Yang, Y.H., Wen, Q.Y., Qin, S.J., Gao, F.: Locally indistinguishable orthogonal product bases in arbitrary bipartite quantum system. Sci. Rep. **6**, 31048 (2016)
28. Xu, G.B., Wen, Q.Y., Gao, F., Qin, S.J., Zuo, H.J.: Local indistinguishability of multipartite orthogonal product bases. Quantum Inf. Process. **16**, 276 (2017)
29. Walgate, J., Hardy, L.: Nonlocality, asymmetry, and distinguishing bipartite states. Phy. Rev. Lett. **89**, 147901 (2002)
30. Wang, T.Y., Wen, Q.Y., Chen, X.B.: Cryptanalysis and improvement of a multi-user quantum key distribution protocol. Opt. Commun. **283**(24), 5261–5263 (2010)
31. Salas, P.J.: Security of plug-and-play QKD arrangements with finite resources. Quant. Inf. Comput. **13**, 861–879 (2013)
32. Deng, F.G., Long, G.L., Liu, X.S.: Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pairblock. Phys. Rev. A **68**, 042317 (2003)
33. Chen, X.B., et al.: Cryptanalysis of secret sharing with a single d-level quantum system. Quantum Inf. Process. **17**, 225 (2018)
34. Long, G.L., Liu, X.S.: Theoretically efficient high-capacity quantum-key-distribution scheme. Phys. Rev. A **65**, 032302 (2002)
35. Guo, G.P., Li, C.F., Shi, B.S., Li, J., Guo, G.C.: Quantum key distribution scheme with orthogonal product states. Phys. Rev. A **64**, 042301 (2001)
36. Cai, Q.Y., Tan, Y.G.: Photon-number-resolving decoy-state quantum key distribution. Phys. Rev. A **73**, 032305 (2006)

37. Huang, W., Wen, Q., Liu, B., Gao, F., Sun, Y.: Quantum key agreement with EPR pairs and single-particle measurements. Quantum Inf. Process. **13**(3), 649–663 (2014)
38. He, Y.F., Ma, W.P.: Quantum key agreement protocols with four-qubit cluster states. Quantum Inf. Process. **14**(9), 3483–3498 (2015)
39. Cabello, A.: Quantum key distribution in the Holevo limit. Phys. Rev. Lett. **85**, 5635-5638 (2000)
40. Fatahi, N., Naseri, M., Gong, L.H., Liao, Q.H.: High-efficient arbitrated quantum signature scheme based on cluster states. Int. J. Theor. Phys. **56**, 609–616 (2017)
41. Zhao, Q.L., Li, X.Y.: A bargmann system and the involutive solutions associated with a new 4-order lattice hierarchy. Anal. Math. Phys. **6**(3), 237–254 (2016)
42. Wang, Y.H.: Beyond regular semigroups. Semigroup Forum **92**(2), 414–448 (2016)
43. Zhang, J.K., Wu, X.J., Xing, L.S., Zhang, C.: In Herbert bifurcation analysis of five-level cascaded H-bridge inverter using proportional-resonant plus time-delayed feedback. Int. J. Bifurcat. Chaos. **26**, 11 (2016)
44. Zhang, T.Q., Meng, X.Z., Zhang, T.H.: Global analysis for a delayed siv model with direct and environmental transmissions. J. Appl. Anal. Comput. **6**(2), 479–491 (2016)
45. Meng, X.Z., Wang, L., Zhang, T.H.: Global dynamics analysis of a nonlinear impulsive stochastic chemostat system in a polluted environment. J. Appl. Anal. Comput. **6**(3), 865–875 (2016)
46. Meng, X.Z., Zhao, S.N., Zhang, W.Y.: Adaptive dynamics analysis of a predator-prey model with selective disturbance. Appl. Math. Comput. **266**, 946–958 (2015)
47. Zhao, W.C., Li, J., Meng, X.Z.: Dynamical analysis of SIR epidemic model with nonlinear pulse vaccination and lifelong immunity. Discrete Dyn. Nat. Soc. **2015**, 848623 (2015)
48. Cui, Y.J., Zou, Y.M.: An existence and uniqueness theorem for a second order nonlinear system with coupled integral boundary value conditions. Appl. Math. Comput. **256**, 438–444 (2015)
49. Yu, J., Li, M.Q., Wang, Y.L., He, G.P.: A decomposition method for large-scale box constrained optimization. Appl. Math. Comput. **231**, 9–15 (2014)
50. Jiang, T.S., Jiang, Z.W., Ling, S.T.: An algebraic method for quaternion and complex least squares coneigen-problem in quantum mechanics. Appl. Math. Comput. **249**, 222–228 (2014)