An arbitrated quantum signature protocol using rotation and permutation operators

Kai Wen, Shihui Zheng\(^1\) and Bin Sun

School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing, 100876, China

\(^1\)Email: shihuizh@bupt.edu.cn

Abstract. The existing improved arbitrated quantum signature (AQS) protocols still have some security problems. First, the security of one AQS protocol is analysed, including existential forgery attack and the signer’s disavowal attack. To resist these attacks, a novel AQS protocol using rotation and permutation operators is proposed. And the analysis shows that the protocol can resist all the known forgery attacks and the signer’s disavowal attacks.

1. Introduction

Digital signature is used to protect data integrity, identity authentication and non-repudiation. However, most classical digital signature schemes used in practice are insecure because of Shor’s algorithm [1]. While the security of quantum signature is guaranteed by quantum physics principles. As with classical digital signature, quantum signature can also be classified into general quantum signature and arbitrated quantum signature (AQS) [2].

Zeng et al [3] proposed the first AQS protocol with GHZ state in 2002, including a credible arbitrator Trent to provide signature verification service for the signer Alice and receiver Bob. In 2009, Li et al [4] proposed another AQS protocol by simplifying the GHZ state to Bell state. One year later, Zou et al [5] also proposed an AQS protocol without entanglement. The basic model of AQS was formed since then, and the latter protocols [6-9] are improvements based on them.

However, in recent years, many attacks on these AQS protocols were presented, such as the receiver’s forgery and the signer’s disavowal. For the receiver’s forgery, Gao [10] et al first found that the protocols [4, 5] used quantum one-time pad algorithm (QOTP) [11], thus the malicious receiver Bob can utilize the commutativity of Pauli operators to achieve existential forgery. For the signer’s disavowal, Gao [10] et al pointed out that, in the protocols [4, 5], Alice can modify the communication data from Trent to Bob in verifying phase to deny her signature because QOTP is a qubit-by-qubit algorithm. Recently, we also find one improved AQS protocol has the above drawbacks, which are described in Sect. 2.

So far, the improvements are mainly divided into two kinds: the scheme based on improved QOTP algorithm [6, 9, 12-15] and the scheme based on chained CNOT algorithm [7, 8]. The latter belongs to the multi-qubit system by using controlled operations between qubits, which can resist the known attacks to some extent. However, its ensemble operation mode increases its complexity in physical implementation. In this paper, from a new perspective, a novel AQS protocol using rotation and permutation operators is proposed, and the analysis shows that the protocol can resist forgery attack and the signer’s disavowal attack.
The rest of the paper is organized as follows: In Sect. 2, the security problems of one AQS protocol are analyzed. In Sect. 3, a novel AQS protocol using rotation and permutation operators is presented. In Sect. 4, the security of the protocol in Sect. 3 is analyzed. In Sect. 5, some conclusions and discussions are given.

2. Security analysis on one AQS protocol

In this section, the attack results to one AQS protocol [9] are given, including existential forgery in Sect. 2.2, the signer’s disavowal in Sect. 2.3. In order to describe the attack process clearly, the basic model of AQS is introduced first.

2.1. The basic model of AQS

As described in Refs. [3-9], an AQS protocol includes the following four phases.

Initializing phase:
(11) Let \( P_i = \bigotimes_{i=1}^{N} p_i \), \( p_i = \alpha |0\rangle + \beta |1\rangle, |k\rangle + |\bar{k}\rangle = 1 \) is a quantum message, \( \text{Sign} \) is the signature algorithm, \( \text{Sign}^{-1} \) is the inverse of \( \text{Sign} \), and \( \text{Ver} \) is the verification algorithm.

(12) The signer Alice and receiver Bob share keys \( K_{AT} \) and \( K_{BT} \) with the arbitrator Trent, respectively.

Signing phase:
Alice generates the signature \( |S_A\rangle = \text{Sign}_{K_{AT}} (|P_i\rangle) \) then sends \( (|P_i\rangle, |S_A\rangle) \) to Bob.

Verifying phase:
(V1) Bob calculates \( |Y_{BT}\rangle = \text{Sign}_{K_{BT}} (|P_i\rangle, |S_A\rangle) \) and sends \( |Y_{BT}\rangle \) to Trent;

(V2) After receiving \( |Y_{BT}\rangle \), Trent first calculates \( (|P_i\rangle, |S_A\rangle) = \text{Sign}^{-1}_{K_{AT}} (|Y_{BT}\rangle) \). Second, he calculates \( |V_t\rangle = \text{Ver}_{K_{AT}} (|P_i\rangle, |S_A\rangle) \in \{0\}, 1\} \), where \(|V_t\rangle = |1\rangle\) indicates \( (|P_i\rangle, |S_A\rangle) \) is valid, otherwise not. Then he calculates \( |Y_{TB}\rangle = \text{Sign}_{K_{AT}} (|P_i\rangle, |S_A\rangle, |V_t\rangle) \) and sends \( |Y_{TB}\rangle \) to Bob;

(V3) After receiving \( |Y_{TB}\rangle \), Bob calculates \( (|P_i\rangle, |S_A\rangle, |V_t\rangle) = \text{Sign}^{-1}_{K_{AT}} (|Y_{TB}\rangle) \). If \(|V_t\rangle = |1\rangle\), he accepts the signature, otherwise, he rejects.

Arbitrating phase:
When a dispute occurs between Alice and Bob later, Trent asks Bob for \( (|P_i\rangle, |S_A\rangle) \), then he calculates \( |V_t\rangle = \text{Ver}_{K_{AT}} (|P_i\rangle, |S_A\rangle) \in \{0\}, 1\} \). If \(|V_t\rangle = |1\rangle\), he declares that Alice had signed the message \( |P_i\rangle \), otherwise, it is Bob’s forged signature.

It can be seen that the algorithm \( \text{Sign} \) is used for both generating signatures and authenticating the communication between legitimate users. Thus, the security of AQS depends on the security of \( \text{Sign} \).

2.2. Existential forgery

For the protocol [9], the malicious receiver Bob can easily achieve existential forgery by the commutativity of unitary operators. Bob’s forgery is described as follows.

In signing phase, Alice generates the signature \( |S_A\rangle \) for \( |P_i\rangle = \bigotimes_{i=1}^{N} p_i \):

\[
|S_A\rangle = \text{Sign}_{K_{AT}} (|P_i\rangle) = \bigotimes_{i=1}^{N/2} X^{k_{AT}^{i}} \bigotimes_{i=1}^{N/2} Z^{k_{AT}^{i}} \bigotimes_{i=1}^{N/2} V^{k_{AT}^{i}} |P_i\rangle
\]

where \( N \) is even, \( X, Z \) are Pauli operators, \( H \) is the Hardmard operator, and \( V = (X-Z)/\sqrt{2} \).

After receiving \( (|P_i\rangle, |S_A\rangle) \) from Alice, Bob can perform unitary operators \( U_i \in \{I, iY\}, i^2 = -1 \) on \( (|P_i\rangle, |S_A\rangle) \) to forge a new pair \( (|P_i\rangle, |S_A\rangle) \), where \( Y = iXZ \) is another Pauli operator.

2
\[
\left| F' \right> = \bigotimes_{i=1}^{N} U_i |p_i> \\
\left| S_{\alpha}^\prime \right> = \bigotimes_{i=1}^{N/2} U_{2i-1} X^{\alpha_{2i-1}} H^{\alpha_{2i-1}} |p_{2i-1}> \bigotimes_{i=1}^{N/2} U_{2i} Z^{\alpha_{2i}} V^{\alpha_{2i}} |p_{2i}> 
\]

(2)

In verifying phase, after receiving \((\left| P' \right>, \left| S_{\alpha}^\prime \right>)\) from Bob, Trent calculates \(\left| V_T \right>\) as follows:

First, as \(XY = -XY, YH = -HY, YZ = -ZY, YV = -VY\), he calculates

\[
\left| S_T \right> = \bigotimes_{i=1}^{N/2} X^{\alpha_{2i}} H^{\alpha_{2i}} U_{2i-1} |p_{2i-1}> \bigotimes_{i=1}^{N/2} Z^{\alpha_{2i}} V^{\alpha_{2i}} U_{2i} |p_{2i}> = \bigotimes_{i=1}^{N/2} \pm U_{2i-1} X^{\alpha_{2i}} H^{\alpha_{2i}} |p_{2i-1}> \bigotimes_{i=1}^{N/2} \pm U_{2i} Z^{\alpha_{2i}} V^{\alpha_{2i}} |p_{2i}>
\]

(3)

Second, Trent compares \(\left| S_T \right>\) and \(\left| S_{\alpha}^\prime \right>\) bitwise under quantum swap test circuit (QSTC) [16]. Because global phase \(\pm 1\) could be negligible, he obtains \(\left| S_T \right> = \left| S_{\alpha}^\prime \right>\) and \(\left| V_T \right> = \left| 1 \right>\), thus \((\left| P' \right>, \left| S_{\alpha}^\prime \right>)\) can pass Trent’s verification. Since \(U_i\) may be \(I\) or \(i\) \(Y\), there are \(2^N - 1\) non-trivial combinations as Equation (3) for the message with length \(N\).

2.3. The signer’s disavowal
In this subsection, Alice could easily deny her signature in the protocols [9].

In verifying phase, the communication data from Trent to Bob is

\[
\left| Y_{TB} \right> = \text{Sign}_{K_{at}} \left( \left| P' \right> \otimes \left| S_{\alpha}^\prime \right> \otimes \left| V_T \right> \right) 
\]

(4)

Because \(\text{Sign}_{K_{at}}\) is a qubit-by-qubit algorithm as Equation (1), the position of signature qubits in \(\left| Y_{TB} \right>\) is determined. Alice can modify the signature qubits while leave other qubits unchanged. Suppose Bob obtains \((\left| P' \right>, \left| S_{\alpha}^\prime \right>, \left| V_T \right>\) from the modified \(\left| Y_{TB} \right>\), where \(\left| S_{\alpha}^\prime \right>\) denotes the modified signature. Without \(K_{at}\), he cannot find Alice’s modification on \(\left| S_{\alpha}^\prime \right>\). However, in arbitrating phase, Trent asks Bob for \((\left| P' \right>, \left| S_{\alpha}^\prime \right>)\), which could not pass verification, so Alice can deny her signature.

3. An AQS protocol using rotation and permutation operators
The existing improved schemes [6, 9, 12-15] for AQS are based on QOTP by modifying the Pauli operators to resist forgery attacks. In quantum computation, one important kind of operators are rotation operators. In 2008, Nikolopoulos [17] et al proposed a public key quantum encryption scheme by using y-type rotation operators. Inspired by this, in this section, a novel AQS protocol using rotation and permutation operators is presented. First, the two operators are defined as follows.

Let \(\left| P \right> = \bigotimes_{i=1}^{N} |p_i>\) be an \(N\)-qubit string, and \(R_x(\theta), R_y(\theta)\) are two unitary operators:

\[
R_x(\theta) = \left( \begin{array}{cc} \cos(\theta/2) & -\sin(\theta/2) \\ -\sin(\theta/2) & \cos(\theta/2) \end{array} \right), \quad R_y(\theta) = \left( \begin{array}{cc} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{array} \right), \quad \theta \in \mathbb{R}, i^2 = -1
\]

(5)

Definition 1 The rotation operator \(\text{Rot}_x\) is defined as follows:

\[
\text{Rot}_x \left( \left| P' \right> \right) = \bigotimes_{i=1}^{N} R_x(\alpha_i \theta_i) |p_i>
\]

(6)

where \(\Omega = \{\alpha_1, \ldots, \alpha_N\}, \alpha_i \in \mathbb{R}\) is an array, \(\alpha_i \in \{x, y\}\), \(\theta_i \in \mathbb{R}\).

The rotation operator \(\text{Rot}_x\) is reversible, and the inverse of \(\text{Rot}_x\) is

\[
\text{Rot}_x^{-1} \left( \left| P' \right> \right) = \bigotimes_{i=1}^{N} R_x(-\alpha_i \theta_i) |p_i>
\]

(7)

Let \(\sigma_j\) is a permutation in \(N\)-order permutation group \(S_N\). Then \(\sigma_j\) and its inverse permutation \(\sigma_j^{-1}\) are denoted as
\[ \sigma_j = \left[ \begin{array}{cccc} 1 & \cdots & i & \cdots & N \\ \sigma_j(l) & \cdots & \sigma_j(i) & \cdots & \sigma_j(N) \end{array} \right] \quad \sigma_j^{-1} = \left[ \begin{array}{cccc} 1 & \cdots & i & \cdots & N \\ \sigma_j^{-1}(l) & \cdots & \sigma_j^{-1}(i) & \cdots & \sigma_j^{-1}(N) \end{array} \right] \] (8)

**Definition 2** The permutation operator \( \text{Per} \) is defined as follows:

\[ \text{Per}_{\sigma_j}(\{|P\}\}) = \left| p_{\sigma_j(0)} \right\rangle \otimes \cdots \otimes \left| p_{\sigma_j(i)} \right\rangle \otimes \cdots \otimes \left| p_{\sigma_j(N)} \right\rangle \] (9)

where \( \left| p_{\sigma_j(i)} \right\rangle \) denotes the \( \sigma_j(i) \)-th qubit of \( |P\rangle \).

The permutation operator is also reversible, and the inverse of \( \text{Per} \) is

\[ \text{Per}_{\sigma_j}^{-1}(\{|P\}\}) = \left| p_{\sigma_j^{-1}(0)} \right\rangle \otimes \cdots \otimes \left| p_{\sigma_j^{-1}(i)} \right\rangle \otimes \cdots \otimes \left| p_{\sigma_j^{-1}(N)} \right\rangle \] (10)

where \( \left| p_{\sigma_j^{-1}(i)} \right\rangle \) denotes the \( \sigma_j^{-1}(i) \)-th qubit of \( |P\rangle \).

Our AQS protocol includes the following four phases:

**Initializing phase:**

(I1) Trent chooses a number \( n \geq 2 \) as a public security parameter, then the unit rotation angle \( \theta_n = \pi / 2^{n-1} \) is obtained. Besides, he announces a public string \( C = \{c_1, \ldots, c_{2^n+1}\}, c_i = \{x, y \mod 2 = 1 \} \).

(I2) Through quantum key distribution, Trent, Alice and Bob share a pair of classical keys \( \{K_{A1}^1, K_{A2}^1\} \), \( \{K_{B1}^1, K_{B2}^1\} \), and \( \{K_{AB}^1, K_{AB}^2\} \), respectively, where \( K_{A1}^1, K_{A2}^1 \in \{0,1\}^{n^2}, K_{B1}^1 \in \{0,1\}^{2^{2n+1}}, K_{B2}^1 \in \{0,1\}^{2^{2n+1}}, K_{AB}^1 \in \{0,1\}^{2^{2n+1}}, K_{AB}^2 \in \{0,1\}^{2n^2} \).

(I3) Transform each pair of keys into a decimal string and a permutation. Take \( \{K_{A1}^1, K_{A2}^1\} \) for example:

(I3-1) Alice converts each \( n \) bits of \( K_{A1}^1 \) into a decimal number \( k^1_{AT} \in \mathbb{Z}_{2^1} \), then a decimal string \( K_{A1}^\text{Dec} = \{k^1_{AT}, \ldots, k^1_{AT}, \ldots, k^1_{AT}\} \) is obtained.

(I3-2) Alice constructs an injection \( f \) from \( \{0,1\}^N \) to \( S_N \), i.e., \( f: K_{A1}^2 \mapsto \sigma_{k_{AT}} \in S_N \), then a permutation \( \sigma_{k_{AT}} \) is obtained.

Similarly, Bob and Trent do the same operations above to transform their keys, i.e., \( K_{A2}^1 \mapsto K_{AB}^\text{Dec}, K_{B1}^2 \mapsto K_{AB}^\text{Dec}, K_{B2}^2 \mapsto \sigma_{k_{AB}} \in S_{2n^2+1} \) and \( K_{AB}^2 \mapsto \sigma_{k_{AB}} \in S_N \).

(I4) Alice and Trent pre-share a serial number \( r \in \mathbb{Z}_{2^n} \) and a classical hash function \( H_n \) with an \( N \)-length output. Besides, they negotiate an synchronization rule: \( r \equiv r+1 \).

**Signing phase:**

(S1) Alice prepares four copies of the message \( |P\rangle = \bigotimes_i^n |p_i\rangle \);

(S2) Alice generates two copies of signatures with two copies of \( |P\rangle \):

\[ |S_i\rangle = \text{Per}_{\sigma_{k_{AT}}} \left( \text{Rot}_{\theta_n} \left( |P\rangle \right) \right) = \text{Per}_{\sigma_{k_{AB}}} \left( \bigotimes_i^n (k_{AT}^i \theta_n) |p_i\rangle \right) \] (11)

where \( K_{AT}^\ast = H_n (K_{AT}^2 || r) \), and the two copies of \( |S_i\rangle \) are denoted as \( |S_i\rangle_T \) and \( |S_i\rangle_B \), respectively.

(S3) Alice calculates \( |Y_{AB}\rangle_T = \text{Per}_{\sigma_{k_{AB}}} \left( \text{Rot}_{k_{AB}} \left( |P\rangle \right) \right) \) with the third copy of \( |P\rangle \) and calculates \( |Y_{AB}\rangle_B = \text{Per}_{\sigma_{k_{AB}}} \left( \text{Rot}_{k_{AB}} \left( |S_i\rangle_B \right) \right) \) and then sends \( |P\rangle \otimes |Y_{AB}\rangle_T \otimes |S_i\rangle_T \otimes |Y_{AB}\rangle_B \) to Bob.

**Verifying phase:**
(V1) After receiving $|P\rangle \otimes |Y_i\rangle \otimes |S_{\lambda_i} \rangle \otimes |Y_{bf}\rangle$ , Bob calculates $|P^*\rangle = \text{Rot}_{K^A_{ic}}^{-1} \left( \text{Per}_{e_{ic}}^{-1} \left( |Y_{AB}\rangle \langle P| \right) \right)$, and then uses bitwise QSTC to decide whether $|P^*\rangle = |P\rangle$ or not. If $|P^*\rangle \neq |P\rangle$ , the protocol continues; otherwise, Bob rejects and the protocol stops.

(V2) Bob calculates $|Y_{bf}\rangle = \text{Per}_{e_{ic}} \left( \text{Rot}_{K^B_{ic}}^{-1} \left( |P\rangle \otimes |S_{\lambda_i} \rangle \right) \right)$ and sends $|Y_{bf}\rangle$ to Trent;

(V3) After receiving $|Y_{bf}\rangle$ , Trent performs the following steps:

(V3-1) First he calculates $|P\rangle \langle S_{\lambda_i} |) = \text{Rot}_{K^B_{ic}}^{-1} \left( \text{Per}_{e_{ic}}^{-1} \left( |Y_{bf}\rangle \langle S_{\lambda_i} | \right) \right)$ and

$$|S_{\lambda_i} | = \text{Per}_{e_{ic}} \left( \text{Rot}_{K^B_{ic}}^{-1} \left( |P\rangle \langle S_{\lambda_i} | \right) \right)$$

Then he compares $|S_{\lambda_i} |$ and $|S_{\lambda_i} \rangle$ bitwise under QSTC, if $|S_{\lambda_i} \rangle = |S_{\lambda_i} \rangle$, let $V_t = 1$, otherwise, $V_t = 0$. Then he calculates $|P\rangle = \text{Rot}_{K^A_{ic}}^{-1} \left( \text{Per}_{e_{ic}}^{-1} \left( |S_{\lambda_i} \rangle \langle S_{\lambda_i} | \right) \right)$ (note that $|P\rangle$ can be recovered if $|S_{\lambda_i} \rangle = |S_{\lambda_i} \rangle$).

(V3-2) After that, he calculates $|Y_{bf}\rangle = \text{Per}_{e_{ic}} \left( \text{Rot}_{K^B_{ic}}^{-1} \left( |P\rangle \otimes |S_{\lambda_i} \rangle \otimes |V_t\rangle \right) \right)$ and sends $|Y_{bf}\rangle$ to Bob.

(V4) After receiving $|Y_{bf}\rangle$ , Bob calculates $|P^*\rangle \otimes |S_{\lambda_i} \rangle \otimes |V_t\rangle = \text{Rot}_{K^B_{ic}}^{-1} \left( \text{Per}_{e_{ic}}^{-1} \left( |Y_{bf}\rangle \langle S_{\lambda_i} | \langle V_t \rangle \right) \right)$, if $V_t = 1$, $|P^*\rangle = |P\rangle$ and $|S_{\lambda_i} \rangle = |S_{\lambda_i} \rangle$, he accepts the signature, otherwise, he rejects.

**Arbitrating phase:**

When a dispute occurs between Alice and Bob later, Trent asks Bob for $(|P\rangle, |S_{\lambda_i} \rangle)$, and then Trent calculates $|S_{\lambda_i} \rangle$ as Equation (11) and compares $|S_{\lambda_i} \rangle$ and $|S_{\lambda_i} \rangle$. If $|S_{\lambda_i} \rangle = |S_{\lambda_i} \rangle$, Trent declares that the Alice had indeed signed the message, otherwise, it is Bob’s forged signature.

### 4. Security analysis

In this section, the security of the protocol in Sect. 3 is analyzed from two aspects: the unforgeability and non-repudiation.

#### 4.1. Unforgeability

From the security analysis in Sect. 2.2, the existential forgery is based on the commutativity of unitary operators. To prove the security of the protocol under this forgery strategy, the following two theorems are given.

**Theorem 1** The same type of rotation operators are commutative.

Proof: \( \forall \theta_1, \theta_2 \in \mathbb{R} \), the rotation operators around \( x, y, z \) axis are denoted as respectively

\[
R_x(\theta) = \begin{pmatrix}
\cos(\theta / 2) & -\sin(\theta / 2) \\
\sin(\theta / 2) & \cos(\theta / 2)
\end{pmatrix},
\quad
R_y(\theta) = \begin{pmatrix}
\cos(\theta / 2) & \sin(\theta / 2) \\
-\sin(\theta / 2) & \cos(\theta / 2)
\end{pmatrix},
\quad
R_z(\theta) = \begin{pmatrix}
1 & 0 \\
0 & e^{i\theta / 2}
\end{pmatrix}
\]

(13)

It is not difficult to verify that the same type of rotation operators are commutative, because the commutators are all zeros:

\[
\left[ R_x(\theta_1), R_x(\theta_2) \right] = R_x(\theta_1) R_x(\theta_2) - R_x(\theta_2) R_x(\theta_1) = 0
\]

\[
\left[ R_y(\theta_1), R_y(\theta_2) \right] = R_y(\theta_1) R_y(\theta_2) - R_y(\theta_2) R_y(\theta_1) = 0
\]

\[
\left[ R_z(\theta_1), R_z(\theta_2) \right] = R_z(\theta_1) R_z(\theta_2) - R_z(\theta_2) R_z(\theta_1) = 0
\]

(14)

Proof completed.

**Theorem 2** Two different types of rotation operators are commutative if and only if they are Pauli operators, or one type of rotation operator is an identity operator when ignoring a global phase factor.

Proof: Rotation operators around \( x, y, z \) are commutative if \( \exists \theta_1, \theta_2, \theta_3 \in \mathbb{R}, c_1, c_2, c_3 \in \mathbb{C}, |c_i| = 1 , s.t.
According to Equation (13), to expand Equation (15), it is easy to get the following solutions:

$$\begin{align*}
R_i(\theta) &= \pm I \text{ and } R_i(\theta) = \pm iX \text{ or } R_i(\theta) = \pm iY \\
R_i(\theta) &= \pm iX \text{ and } R_i(\theta) = \pm iY \text{ or } R_i(\theta) = \pm Z
\end{align*}$$

(16)

where $X,Y,Z$ are Pauli operators. Proof completed.

In the following, based on Theorem 1 and 2, it will be illustrated that the protocol can resist the forgery strategy by the commutativity of unitary operators in Sect. 2.2. In the other words, if Bob performs unitary operators on the message and signature qubits, the probability of his successful forgery can be negligible, i.e., the probability $P_{\text{for}} = 1/ f(N)$, where $f(N)$ is an exponential function about $N$, $N$ is the length of a message.

First, suppose Bob receives a valid pair $|P\rangle, |S_{\lambda}\rangle$ from Alice, he can perform bitwise unitary operator on each qubit of $|P\rangle$ and $|S_{\lambda}\rangle$ to obtain new pair:

$$\begin{align*}
|P'\rangle &= \left( \bigotimes_{i=1}^{N} U_i \right) |P\rangle = \left( \bigotimes_{i=1}^{N} U_i \right) |p_i\rangle \\
|S'_{\lambda}\rangle &= \left( \bigotimes_{i=1}^{N} Q_i \right) |S_{\lambda}\rangle = \text{Per}_{e_{k_i}} \left( \bigotimes_{i=1}^{N} Q_{k_i}^{-1} R_i \left( k_{i \lambda}^i, \theta_i \right) |p_i\rangle \right)
\end{align*}$$

(17)

where $U_i$ and $Q_i$ are unitary operators. If $|P'\rangle, |S'_{\lambda}\rangle$ can pass Trent's verification, the forgery is considered successful.

Thus, in verifying or arbitrating phase, after receiving $|P'\rangle, |S'_{\lambda}\rangle$, Trent calculates $|S_r\rangle$ as Equation (12):

$$|S_r\rangle = \text{Per}_{e_{k_i}} \left( \text{Rot}_{k_i} |P'\rangle \right) = \text{Per}_{e_{k_i}} \left( \bigotimes_{i=1}^{N} R_i \left( k_{i \lambda}^i, \theta_i \right) |U_i |p_i\rangle \right)$$

(18)

and then he compares $|S_r\rangle$ and $|S'_{\lambda}\rangle$ bitwise under QSTC, if $|S_r\rangle \approx |S'_{\lambda}\rangle$, then $|P'\rangle, |S'_{\lambda}\rangle$ is considered valid. Here, $|S_r\rangle \approx |S'_{\lambda}\rangle$ indicates $|S_r\rangle$ equals to $|S'_{\lambda}\rangle$ when ignoring global phases.

According to Equations (17, 18), if $|S_r\rangle = |S_{\lambda}^r\rangle$, there must be

$$Q_{\sigma_{k_{\lambda}^r}}^{-1} R_i \left( k_{i \lambda}^r, \theta_i \right) = R_i \left( k_{i \lambda}^r, \theta_i \right) U_i$$

(19)

Thus, according to Equation (19), to obtain the correct operators $U_i$ and $Q$ requires knowing the correct permutation $\sigma_{k_{\lambda}^r}$. Therefore, the probability of Bob's forgery is discussed in two cases, i.e., Bob guess the correct permutation or not.

Case 1: Bob guesses the correct permutation

In this case, Bob guess the correct $\sigma_{k_{\lambda}^r}$, with probability of $p_1 = 1/2^N$, and Bob also obtains the correct operators $U_i$ and $Q$, with probability of $p_2$, therefore, the probability of Bob's successful forgery is $P_{\text{for}} = p_1 \cdot p_2 \leq 1/2^N$.

Case 2: Bob guesses the wrong permutation

In this case, Bob guesses the wrong $\sigma_{k_{\lambda}^r}$, with probability of $p_3 = 1 - 1/2^N$. And according to Theorem 1 and 2, to make the probability of Bob's successful forgery as large as possible, there must be
If $U = X$, according to Theorem 1 and Equation (14), if the signature qubits are generated by $R_x(k_{AX}^i \theta_n^i), i = 1,3,\ldots,N - 1$, then $XR_y(k_{AX}^i \theta_n^i) = R_y(k_{AX}^i \theta_n^i)X$, so half of the signature qubits can pass Trent’s verification.

However, if the signature qubits are generated by $R_y(k_{AX}^i \theta_n^i), j = 2,4,\ldots,N$, then these signature qubits could pass verification if and only if $XR_y(k_{AX}^i \theta_n^i) = R_y(k_{AX}^i \theta_n^i)X$. In addition, according to Theorem 2, there must be $k_{AX}^i = 0.2^{m-1}$, and the probability is $p_s = 1/2^{m-1}$. Since half of the signature qubits are generated by $R_y(k_{AX}^i \theta_n^i)$, the probability of Bob’s successful forgery is:

$$P_{fs} = p_s \cdot p_s^{N/2} = \left(1 - \frac{1}{2^N}\right)^{N/2} \leq \frac{1}{2^{N(e-1)/2}}$$  \hspace{1cm} (20)

Similarly, if $U = Y$, the probability of Bob’s successful forgery is also as Equation (20).

Overall, the probability of Bob’s successful forgery can be negligible.

### 4.2. Non-repudiation

Similar with the analysis in Sect. 2.3, for the protocol, Alice successfully denies her signature if she modifies $|Y_{TB}\rangle$ in verifying phase without being found, while in arbitrating phase, Trent detects that there is one pairs of qubits different between $|S_i\rangle$ and $|S_i\rangle$.

In the protocol, $|Y_{TB}\rangle$ can be denoted as

$$|Y_{TB}\rangle = Per_{Y_{TB}} \left( \bigotimes_{i=1}^N R_{i}^x(k_{AX}^i \theta_n^i) |p_{i1}, \ldots, p_{iN}\rangle \bigotimes_{i=1}^N R_{i=1}^{x,y} \left( k_{B\tau Ax/u}^i \theta_n^i \right) \right) \bigotimes_{i=1}^N R_{i=1}^{x,y} \left( k_{B\tau Ax/u}^i \theta_n^i \right) |V_T\rangle.$$ \hspace{1cm} (21)

Because $|Y_{TB}\rangle$ is generated with a permutation in the permutation group $S_{2N+1}$, thus, the message, signature, and verification qubits are confused together. Alice cannot determine which qubits are derived from signature qubits because the permutation is unknown to her.

If Alice randomly modifies one qubit in $|Y_{TB}\rangle$, the probabilities that she modified the qubits of the message and the signature are both $N/(2N+1) = 1/2$. However, according to the step (V4), the modified $|Y_{TB}\rangle$ could pass Bob’s verification if $V_T = 1$, $|P^\prime\rangle = |P\rangle$ and $|S_{i1}\rangle = |S_{i1}\rangle$. Therefore, whatever Alice modified the message or the signature, it will always lead to the result $|P^\prime\rangle \neq |P\rangle$ or $|S\rangle \neq |S\rangle$, that is, Alice’s modifying will be discovered by Bob, so Bob could reject the signature, and our proposed protocol could resist Alice’s disavowal attack.

### 4.3. Comparison with other protocols

Firstly, as mentioned in the beginning of Sect. 3, the existing improved schemes [6, 9, 12-15] are all based on QOTP to resist forgery attacks. In the other words, these schemes still belong to qubit-by-qubit algorithms, which cannot be extended to multi-qubit signature circumstances and cannot also resist the signer’s disavowal. Our protocol overcomes the above drawbacks of the qubit-by-qubit schemes and it could be signed for multi-qubit message. Moreover, by introducing the permutation operator to reorder the sequence of qubits, it sets barrier for both the receiver to forge and the signer to deny signatures.

Secondly, from the perspective of algorithm efficiency, in the chained CNOT based protocols [7, 8], when generating signatures, it requires performing $N$ sequential controlled operations between qubits. While in our protocol, all $N$ rotation operations could be conducted in parallel. Thus theoretically, our protocol achieves higher efficiency than protocols [7, 8] in algorithm execution.

Thirdly, from the perspective of communication efficiency, Ref. [6] used the strategy of decoy-state-checking to resist forgery and disavowal attacks, thus, qubits transported in the quantum
channel is much more than that in our protocol. Besides, many existing protocols [3, 4, 7] used quantum teleportation to send one copy of the message for Bob’s verification. Instead, our protocol used rotation and permutation operators to authenticate the communication data between Alice and Bob, and also provide one copy of the message for Bob’s verification. Therefore, our protocol requires no consideration for entangled state preparation, distribution and measurement, which contributes to reducing implementation complexity of the protocol.

5. Conclusions and discussions
In this paper, the attack results for one improved AQS protocol are given, including the receiver’s existential forgery and the signer’s disavowal. Then a novel AQS protocol using rotation and permutation operators and the analysis of the protocol are presented. The analysis results show that our protocol can resist forgery attack and the signer’s disavowal attack.

There remain two problems unsolved in this paper. First, a specific example to construct an injection $f$ from $\{0,1\}^N$ into $S_N$ is not given. Second, although our protocol could resist Alice’s disavowal attack, it also requires one more copy of signature compared to the basic model of AQS. Thus, it increases complexity of the protocol. So far, to our knowledge, there are two main solutions to resist the signer’s disavowal, one is to insert decoy states into the communication data from Trent to Bob [6]. However, this method requires lots of checking qubits, which is quite less efficient; another is that Trent stores the message and signature rather than sends back to Bob [10]. However, this method will also bring too much burden to Trent. Whether there are more effective solutions to resist the signer’s disavowal needs further research.

Acknowledgments
This work is supported by the National Natural Science Foundation of China (Grant No. 61502048) and National Science and Technology Major Project (Grant No. 2017YFB0803001).

References
[1] Shor P W 1994 Proceedings of the 35th Annual Symposium on Foundation of Computer Science 124–134
[2] Zeng G H 2008 Physical Review A 78(1) 016301
[3] Zeng G H and Keitel C H 2002 Physical Review A 65 042312
[4] Li Q, Chan W H and Long D Y 2009 Physical Review A 79 054307
[5] Zou X F and Qiu D W 2010 Physical Review A 82 042325
[6] Wang C, Liu J W and Shang T 2014 Chinese Physics B 23(6) 060309
[7] Li F G and Shi J H 2015 Quantum Information Processing 14(6) 2171–2181
[8] Zhang L, Sun H W and Zhang K J et al 2017 Quantum Information Processing 16 70
[9] Guo Y, Sun X and Zhang W 2013 International Journal of Theoretical Physics 11(4) 1350036
[10] Gao F, Qin S J and Guo F Z et al 2011 Physical Review A 84 022344
[11] Boykin P O and Roychowdhury V 2003 Physical Review A 67 042317
[12] Zhang K J, Zhang W W and Li D 2013 Quantum Information Processing 12 2655–2669
[13] Zhang K J, Li D and Su Q 2014 Physica Scripta 89 015102
[14] Kang M S, Choi H W and Pramanik T 2018 Quantum Information Processing 17 254
[15] Kim T Lee H S and Lee S 2017 Physica Scripta 16 268
[16] Buhrman H, Cleve R and Watrous J et al 2001 Physical Review Letters 87(16) 167902
[17] Nikolopoulos G M 2008 Physical Review A 78 019903