Security Problems in the Quantum Signature Scheme with a Weak Arbitrator

X. Zou[1] D. Qiu[2,3] F. Yu[2] P. Mateus[3]

[1]School of Mathematics and Computational Science, Wuyi University, China

[2]Department of Computer Science, Sun Yat-sen University, China

[3]SQIG–Instituto de Telecomunicações,
Departamento de Matemática, Instituto Superior Técnico, University of Lisbon

Abstract

Very recently, a quantum signature scheme with weak arbitrator was presented [Int. J. Theor. Phys. (2012) **51**:2135–2142]. A weak arbitrator is only involved in the disagreement case, which means that the scheme is costless. In this paper, the security of the quantum signature scheme with weak arbitrator is analyzed. We show that attackers can counterfeit a signature for any message, which will pass the verification for the signer. In addition, they can counterfeit a signature for any one of the 4^L (L is the length of the intercepted quantum message) messages by employing the known message attack, which will pass the verification for the signed message. In particular, by employing the Z-transform attack, the attackers can forge a signature for any one of the 2^L messages, which will pass the verifications for both the signer and the signed message successfully.

1 Introduction

The digital signature is a primitive component of cryptography. A digital signature scheme is a mathematical scheme that demonstrates the authenticity of a digital message or document. It can be used to authenticate the identity of the sender of a message or the signer of a document, and to ensure that the original content of the message or the document received is unchanged. In other words, a valid digital signature makes the receiver believe that the message was indeed created by a known sender and not altered in the transmission. The digital signature is commonly used in software distributions and financial transactions where it is important to detect forgery or tampering. Most classical digital signature schemes base on the public key cryptography, which can be broken by Shor's quantum algorithm [1]. Therefore, many researchers turn to investigate quantum signature and authentication, which are supposed to be able to provide an alternative scheme with unconditional security. The first quantum digital signature scheme was proposed by Gottesman and Chuang [2]. Thereafter, progresses have been made [3–16]. Zeng and Keitel [5] proposed an *arbitrated quantum signature* (AQS) scheme, which has many merits such as that it can sign both known and unknown quantum states. This scheme has been further studied in [17, 18]. It was claimed in [19, 20] and in [21] that the unconditional security can be ensured by using the correlation of Greenberger-Horne-Zeilinger (GHZ) triplet states and quantum one-time pads, respectively. Li *et al.* [6] presented an arbitrated quantum signature scheme using Bell states instead of GHZ states. The scheme preserves the advantages of the original scheme [5] while providing a higher efficiency in transmission and reducing the complexity of implementation. It was pointed out in [16] that the existing AQS schemes [5, 6] can be repudiated by the receiver. Two improved AQS schemes in [16] were then proposed in order to overcome this deficiency. In particular, one of them does not utilize entangled states in the phases of both signing and verification.

Very recently, Luo *et al.* [22] pointed out that there is no need to involve an arbitrator in the signing phase of AQS [5, 6], and single qubits are enough for such schemes. According to this, they suggested *quantum signature scheme with weak arbitrator*, a signature scheme without arbitrage which is similar to most classical signatures with asymmetric techniques [22]. The weak arbitrator is required only when there is a dispute between the signer and the verifier. However, in this paper, we will show that a malicious verifier in the quantum signature scheme with weak arbitrator can counterfeit a valued signature by employing several known message attacks.

The remainder of this paper is organized as follows. First, in Section 2, we recall the security conditions of quantum signatures and the technique of comparing two unknown quantum states presented in Ref. [23]. Then, in Section 3, we briefly review the quantum signature scheme with weak arbitrator [22]. Several attacks are suggested to apply on it and analysis is made in Section 4. Finally in Section 5, we make a conclusion.

2 Preliminaries

In this section, the security conditions of the (arbitrated) quantum signature is first recalled. Then, the algorithm of comparing two unknown quantum states, which was first presented in Ref. [23] and discussed further in Ref. [6, 16], is introduced.

2.1 Security conditions

A secure (arbitrated) quantum signature scheme should satisfy two conditions [5, 6, 16, 18, 22]:

(1) The signature should not be forged by the attacker (including the malicious receiver).

(2) The signature should not be disavowed by the signatory and the receiver.

2.2 The technique of comparing two unknown quantum states

The comparison of known quantum states can be definitely made while the comparison of unknown quantum states cannot. Nevertheless, by using the method proposed in [6, 16, 23], the error probability of determining whether or not two qubit strings are identical can be minimized.

Now, we review the technique of comparing two unknown quantum states [23]. Suppose we need to compare whether or not two states $|\phi\rangle$ and $|\psi\rangle$ are identical. This is accomplished with one-sided error probability by the procedure that measures and outputs the first qubit of the state

$$(H \otimes I \otimes I)(\text{c-SWAP})(H \otimes I \otimes I)|0\rangle|\phi\rangle|\psi\rangle.$$

Here H is the Hadamard transform which maps $|b\rangle \rightarrow \frac{1}{\sqrt{2}}[|0\rangle + (-1)^b|1\rangle]$, I is the identity transform, SWAP is the operation $|\phi\rangle|\psi\rangle \rightarrow |\psi\rangle|\phi\rangle$, and c-SWAP is the controlled-SWAP (controlled by the first qubit). The circuit for this procedure is illustrated in Figure 1. By tracing through the execution of

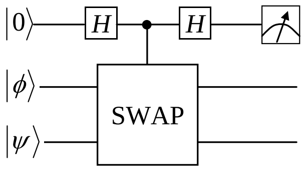

Figure 1: The circuit of comparing two unknown quantum states.

this circuit, one can determine that the state before the final measurement is

$$\frac{1}{2}|0\rangle(|\phi\rangle|\psi\rangle + |\psi\rangle|\phi\rangle) + \frac{1}{2}|1\rangle(|\phi\rangle|\psi\rangle - |\psi\rangle|\phi\rangle). \tag{1}$$

Measuring the first qubit of this state will produce two outcomes $|0\rangle$ and $|1\rangle$. The former will let one infer that the compared two states is equal. Otherwise, they are determined to be unequal. An error occurs when $|\phi\rangle = |\psi\rangle$ but the outcome is $|1\rangle$ (In this case, $|0\rangle$ is the right outcome.). The probability $\frac{1}{2} - \frac{1}{2}(\langle\phi|\psi\rangle)^2$ of it is larger than 0 because $(\langle\phi|\psi\rangle)^2 = \delta^2 > 0$. Therefore, the test has an one-sided error $\frac{1}{2}(1+\delta^2)$.

3 The quantum signature scheme with weak arbitrator

In this section, we briefly review the quantum signature scheme with weak arbitrator [22].

Assume that the messages are a qubit string $|\mathbf{m}\rangle = \{|m_1\rangle, |m_2\rangle, \ldots, |m_L\rangle\}$ with $|m_i\rangle = a_i|0\rangle + b_i|1\rangle$ $(1 \leq i \leq L)$. Alice can prepare arbitrary copies if she knows these states; otherwise, she needs at least three copies for any one's verification and checking. Based on the quantum trapdoor function in Section 2 of Ref. [22], Alice chooses a traceless Hermitian matrix $\mathbf{H}$ to generate one parameter unitary groups $\mathbf{U}_t = e^{it\mathbf{H}}$. For simulation, one can choose $\mathbf{H}$ from the Pauli matrices $\{\sigma_X, \sigma_Y, \sigma_Z\}$. She also randomly chooses $\mathbf{t}_N = (t_{N,1}, t_{N,2}, \ldots, t_{N,L})$ from $\mathbb{Z}^L_{2^N}/2^N$. Alices public key is $\{|\mathbf{P}\rangle = \otimes_{i=1}^L \mathbf{U}_{t_N,i}|\mathbf{0}\rangle\}$, her secret key is $\mathcal{D} = \{t_N, \mathbf{H}\}$. Here, $\mathbf{H}$ is secret to strengthen the security and

$$\mathbf{U}_{t_{N,i}} = \begin{pmatrix} \alpha_i & -\beta_i \\ \beta_i^* & \alpha_i^* \end{pmatrix} \tag{2}$$

where α_i and β_i are complex which are dependent of $t_{N,i}$. This unitary group can be obtained from two special one-parameter unitary groups with the generators $\mathbf{H}_1 = -i\sigma_Y$ and $\mathbf{H}_2 = \mathrm{diag}(\theta_1, \theta_2)$.

Stage 1. Signing phase

The signer performs the CNOT transform on each message particle A_i (in the state $|m_i\rangle$) and the corresponding auxiliary particle B_i (in the state $|0\rangle$):

$$\mathrm{CNOT}(|\mathbf{m}\rangle \otimes |\mathbf{0}\rangle) = \bigotimes_{i=1}^{L}(a_i|00\rangle + b_i|11\rangle)_{A_iB_i}, \tag{3}$$

where the message qubits are the controlling qubits while the auxiliary qubits are the goals. Then, the signer performs $\mathbf{U}_{t_{N,i}}$ on each A_i in Eq. (3) and obtains

$$\begin{aligned}|\mathbf{SM}\rangle &:= \left(\bigotimes_{i=1}^{L}(\mathbf{U}_{t_{N,i}}\otimes I)\right)\left(\bigotimes_{i=1}^{L}(a_i|00\rangle + b_i|11\rangle)_{A_iB_i}\right) && (4)\\ &= \bigotimes_{i=1}^{L}(a_i\alpha_i|00\rangle + a_i\beta_i^*|10\rangle - b_i\beta_i|01\rangle + b_i\alpha_i^*|11\rangle) && (5)\\ &= \bigotimes_{i=1}^{L}[a_i(\alpha_i|0\rangle + \beta_i^*|1\rangle)|0\rangle + b_i(-\beta_i|0\rangle + \alpha_i^*|1\rangle)|1\rangle], && (6)\end{aligned}$$

where I is the second-order identity matrix. Finally, he/she obtains the signature $\{|\mathbf{m}\rangle, |\mathbf{SM}\rangle\}$.

Stage 2. Verifying the signer phase

In order to verify whether it is Alice who signed the state $|\mathbf{SM}\rangle$, Bob performs the Von Neumann measurement (vNM measurement) on all B_is. The measurement will collapse each A_i to $\alpha_i|0\rangle + \beta_i^*|1\rangle$ or $-\beta_i|0\rangle + \alpha_i^*|1\rangle$, corresponding to the outcome state $|0\rangle$ or $|1\rangle$, respectively.

Then, for the outcome $|0\rangle$, Bob takes use of the unknown quantum states comparison algorithm [23] to compare the collapsed state with the public key state $|\mathbf{P}\rangle$ of Alice. Otherwise, he determines whether or not the collapsed state is orthogonal to $|\mathbf{P}\rangle$.

Stage 3. Verifying the signed message phase

Bob performs the CNOT transform on $|\mathbf{SM}\rangle$ and obtains:

$$\begin{aligned}&\bigotimes_{i=1}^{L}\mathrm{CNOT}_{A_i,B_i}|\mathbf{SM}\rangle\\ &\quad= \bigotimes_{i=1}^{L}(a_i\alpha_i|00\rangle + b_i\alpha_i^*|10\rangle - b_i\beta_i|01\rangle + a_i\beta_i^*|11\rangle)\\ &\quad= \bigotimes_{i=1}^{L}[(a_i\alpha_i|0\rangle + b_i\alpha_i^*|1\rangle)|0\rangle\\ &\qquad + (-i\sigma_Y)(a_i\beta_i^*|0\rangle + b_i\beta_i|1\rangle)|1\rangle]. \qquad (7)\end{aligned}$$

(Each A_i is the controlling particle while the corresponding B_i is the goal). Then, he performs the vNM measurement on each B_i, making A_i collapse to $(a_i\alpha_i|0\rangle + b_i\alpha_i^*|1\rangle)|0\rangle$ or $(a_i\beta_i^*|0\rangle + b_i\beta_i|1\rangle)|1\rangle$ corresponding to the outcome state $|0\rangle$ or $|1\rangle$, respectively.

Next, Bob asks Alice to verify the message. In detail, Bob performs a series of CNOT transforms on the collapsed states and the auxiliary states $|\mathbf{0}\rangle$ to obtain $\bigotimes_{i=1}^{L}|\psi_i\rangle$, where $|\psi_i\rangle$ is $a_i\alpha_i|00\rangle + b_i\alpha_i^*|11\rangle$ or $a_i\beta_i^*|00\rangle + b_i\beta_i|11\rangle$. Then, he sends one particle and the measurement outcome k_i(0 or 1 corresponding to the outcome state $|0\rangle$ or $|1\rangle$, respectively.) to Alice.

Alice remotely teleports a series of rotations $R_{j,k}$ on her qubit [24] (for its experimental realization), where

$$\mathbf{R}_{j,1} = \mathrm{diag}(1, e^{i2\theta_{j,1}}), \quad \mathbf{R}_{j,2} = \mathrm{diag}(e^{i2\theta_{j,2}}, 1) \tag{8}$$

with $\alpha_j = |\alpha_j|e^{i\theta_{j,1}}$ and $\beta_j = |\beta_j|e^{i\theta_{j,2}}$. The remotely entangled states are then changed into $\bigotimes_{i=1}^{L}(a_i|00\rangle + b_i|11\rangle)$ (up to a global phase factor) since $a_i\alpha_i|00\rangle + b_ie^{i2\theta_{i,1}}\alpha_i^*|11\rangle = \alpha_i(a_i|00\rangle + b_i|11\rangle)$, $a_ie^{i2\theta_{i,2}}\beta_i^*|00\rangle + b_i\beta_i|11\rangle = \beta_i(a_i|00\rangle + b_i|11\rangle)$. Then, she sends her particles back to Bob. Now, Bob obtains $\bigotimes_{i=1}^{L}(a_i|00\rangle + b_i|11\rangle)$ (up to a global phase factor). Finally, he performs CNOT transforms to disentangle the particles A_is and the unknown quantum states comparison algorithm [23] to verify whether or not the changed states are the message states $|\mathbf{m}\rangle$.

4 Analysis of the Quantum Signature Scheme with Weak Arbitrator

In this section, we analyze the quantum signature scheme with weak arbitrator and its potential weakness. It is stated in [22] that the scheme takes use of the classical known state comparison algorithm to do the comparison. However, it is known that a quantum state can not be known without being measured. Therefore, the quantum states to be compared in the quantum signature scheme [22] must be unknown quantum states. Accordingly, the algorithm doing the comparison must be an algorithm which can compare two unknown quantum states as described in Subsection 2.2. In fact, the procedure described in Fig. 1 of Ref. [22] is exactly for comparing two unknown quantum states like that in Ref. [23].

4.1 Problems in the phase of verifying the signer

According to the quantum signature scheme [22], the vNM measurements are performed in both phases of verifying the signer and the signed message. Therefore, a verifier can only do the verification for either the signer or the signed message with respect to the same signature $|\mathbf{SM}\rangle$. Then, it is possible for an attacker, say Eve, to perform his/her attack on two same signatures made independently for either verification. First, we show that Eve can have at least two options to forge the signature in order to pass the verification for the signer.

Eve intercepts the particles and applies the vNM measurement on each B_i. The collapsed state $|S_i\rangle$ of each A_i will be $\alpha_i|0\rangle+\beta_i^*|1\rangle$ or $-\beta_i|0\rangle+\alpha_i^*|1\rangle$ corresponding to the outcome state $|0\rangle$ or $|1\rangle$ of A_i, respectively. She can then build a new signature $|\widetilde{\mathbf{SM}}\rangle = \bigotimes_{i=1}^{L} |\widetilde{\mathbf{SM}}_i\rangle$, where

$$|\widetilde{\mathbf{SM}}_i\rangle = \begin{cases} |S_i\rangle|0\rangle, & \text{if the outcome state is } |0\rangle, \\ |S_i\rangle|1\rangle, & \text{if the outcome state is } |1\rangle. \end{cases} \tag{9}$$

According to the mechanism of the quantum signature scheme [22], this forged signature will pass the verification for the signer performed by Bob.

The other option that Eve can have is as follows. In order to verify the signer, Bob performs the unknown quantum states comparison algorithm [23] to determine whether or not the collapsed state $|S_i\rangle$ is equal(orthogonal) to $|\mathbf{P}\rangle$, if the measurement outcome state of B_i is $|0\rangle(|1\rangle)$. However, the algorithm for determining the orthogonality between $|S_i\rangle$ and $|\mathbf{P}_i\rangle$ is not clarified. To our knowledge, there is no such an algorithm that can determine the orthogonality between two unknown quantum states. (The authors of [22] think that the orthogonality of $|S_i\rangle$ and $|\mathbf{P}_i\rangle$ can be determined because they mistakenly believe that $|S_i\rangle$ and $|\mathbf{P}_i\rangle$ are known quantum states.) Therefore, Bob is unable to verify the signer when the i-th measurement result is $|1\rangle$. This means that Bob can only verify the signer when the i-th measurement result is $|0\rangle$. Since $|\mathbf{P}\rangle$ is Alice's public key, Eve can get $|\mathbf{P}\rangle$ easily and forge a signature $|\widetilde{\mathbf{SM}}\rangle$ as follows:

(1) She generates a random quantum string $|\phi\rangle = \bigotimes_{i=1}^{L} |\phi_i\rangle$ with $|\phi_i\rangle \in \{|0\rangle, |1\rangle\}$.

(2) She constructs $|\widetilde{\mathbf{SM}}\rangle = \bigotimes_{i=1}^{L} |\widetilde{\mathbf{SM}}_i\rangle$ as

$$|\widetilde{\mathbf{SM}}_i\rangle = \begin{cases} |\mathbf{P}_i\rangle|\phi_i\rangle, & \text{if } |\phi_i\rangle = |0\rangle, \\ (\sigma_Z|\mathbf{P}_i\rangle)|\phi_i\rangle, & \text{if } |\phi_i\rangle = |1\rangle. \end{cases} \tag{10}$$

From the discussion above, the forged signature $|\widetilde{\mathbf{SM}}\rangle$ can pass the verification for the signer performed by Bob.

4.2 Problems in the phase of verifying the signed message

Eve can also perform her attack in the phase of verifying the signed message, given that she has gained the control over the quantum channel between Alice and Bob and has obtained the message-signature pair $(|\mathbf{m}\rangle, |\mathbf{SM}\rangle)$.

4.2.1 The X-transform attack

If she performs the X transform on both $|\mathbf{m}_i\rangle$ and the two particles of $|\mathbf{SM}_i\rangle$, Eve will obtain

$$|\widetilde{\mathbf{m}}_i\rangle = \sigma_X|\mathbf{m}_i\rangle = b_i|0\rangle + a_i|1\rangle \tag{11}$$

and

$$|\widetilde{\mathbf{SM}}_i\rangle = (\sigma_X \otimes \sigma_X)|\mathbf{SM}_i\rangle = b_i\alpha_i^*|00\rangle + a_i\beta_i^*|01\rangle - b_i\beta_i|10\rangle + a_i\alpha_i|11\rangle, \tag{12}$$

respectively. Then, Eve sends to Bob $|\widetilde{\mathbf{m}}\rangle = \bigotimes_{i=1}^L |\widetilde{\mathbf{m}}_i\rangle$ with the forged signature $|\widetilde{\mathbf{SM}}\rangle = \bigotimes_{i=1}^L |\widetilde{\mathbf{SM}}_i\rangle$.

In order to verify whether or not it is Alice's signature for $|\widetilde{\mathbf{m}}\rangle$, Bob performs the CNOT transform on $|\widetilde{\mathbf{SM}}\rangle$:

$$\begin{aligned}
&\bigotimes_{i=1}^L \mathrm{CNOT}_{A_i,B_i}|\widetilde{\mathbf{SM}}\rangle \\
&=\bigotimes_{i=1}^L (b_i\alpha_i^*|00\rangle + a_i\alpha_i|10\rangle + a_i\beta_i^*|01\rangle - b_i\beta_i|11\rangle) &(13)\\
&=\bigotimes_{i=1}^L [(b_i\alpha_i^*|0\rangle + a_i\alpha_i|1\rangle)|0\rangle + (-i\sigma_Y)(b_i\beta_i|0\rangle + a_i\beta_i^*|1\rangle)|1\rangle]. &(14)
\end{aligned}$$

Next, Bob performs the vNM measurement on the second particle in Eq. (13). Then, he performs a series of CNOT transforms on the collapsed states and the auxiliary states $|\mathbf{0}\rangle$ in order to obtain $\bigotimes_{i=1}^L |\psi_i\rangle$ where $|\psi_i\rangle$ is $b_i\alpha_i^*|00\rangle + a_i\alpha_i|11\rangle$ or $b_i\beta_i|00\rangle + a_i\beta_i^*|11\rangle$. After that, he sends one of the entangled particles and the measurement outcome k to Alice.

Note that Eve now gains the control over the quantum channel. She may send this particle through an X-gate. This will change $|\psi_i\rangle$ to $|\psi_i'\rangle$, which is $b_i\alpha_i^*|10\rangle + a_i\alpha_i|01\rangle$ or $b_i\beta_i|10\rangle + a_i\beta_i^*|01\rangle$.

Alice remotely teleports a series of rotations $R_{j,k}$ on her qubits [24], where

$$\mathbf{R}_{j,1} = \mathrm{diag}(1, e^{i2\theta_{j,1}}), \quad \mathbf{R}_{j,2} = \mathrm{diag}(e^{i2\theta_{j,2}}, 1) \tag{15}$$

with $\alpha_j = |\alpha_j|e^{i\theta_{j,1}}$ and $\beta_j = |\beta_j|e^{i\theta_{j,2}}$. $|\psi_i'\rangle$ is then transformed into $|\psi_i''\rangle$, which is $b_i|10\rangle + a_i|01\rangle$ or $b_i|10\rangle + a_i|01\rangle$ (up to a global phase factor). Then, she sends the particle back to Bob.

Eve intercepts this particle again and sends it through an X-gate, which converts its state $|\psi_i''\rangle$ into $|\psi_i'''\rangle = b_i|00\rangle + a_i|11\rangle$.

Now, Bob obtains $\bigotimes_{i=1}^{L}(b_i|00\rangle + a_i|11\rangle)$. Next, he takes CNOT transforms in order to disentangle the particles A_i. Finally, he will obtain $\bigotimes_{i=1}^{L}(b_i|0\rangle + a_i|1\rangle)$. By using the quantum comparison algorithm [23], he can verify that the state is $\bigotimes_{i=1}^{L}(b_i|0\rangle + a_i|1\rangle)$, which is exactly the message states $|\widetilde{\mathbf{m}}\rangle$.

4.2.2 The Z-transform attack

If she performs the Z transform on both $|\mathbf{m}_i\rangle$ and the first particle of $|\mathbf{SM}_i\rangle$, Eve will obtain

$$|\widetilde{\mathbf{m}}_i\rangle = \sigma_Z|\mathbf{m}_i\rangle = a_i|0\rangle - b_i|1\rangle \tag{16}$$

and

$$|\widetilde{\mathbf{SM}}_i\rangle = (I \otimes \sigma_Z)|\mathbf{SM}_i\rangle = a_i\alpha_i|00\rangle + a_i\beta_i^*|10\rangle + b_i\beta_i|01\rangle - b_i\alpha_i^*|11\rangle, \tag{17}$$

respectively. Then, Eve sends to Bob $|\widetilde{\mathbf{m}}\rangle = \bigotimes_{i=1}^{L}|\widetilde{\mathbf{m}}_i\rangle$ with the forged signature $|\widetilde{\mathbf{SM}}\rangle = \bigotimes_{i=1}^{L}|\widetilde{\mathbf{SM}}_i\rangle$.

In order to verify whether or not $|\widetilde{\mathbf{SM}}\rangle$ is Alice's signature for $|\widetilde{\mathbf{m}}\rangle$, Bob performs the CNOT transform on $|\widetilde{\mathbf{SM}}\rangle$:

$$\begin{aligned}
&\bigotimes_{i=1}^{L}\mathrm{CNOT}_{A_i,B_i}|\widetilde{\mathbf{SM}}\rangle \\
&\quad= \bigotimes_{i=1}^{L}(a_i\alpha_i|00\rangle - b_i\alpha_i^*|10\rangle + b_i\beta_i|01\rangle + a_i\beta_i^*|11\rangle) && (18)\\
&\quad= \bigotimes_{i=1}^{L}[(a_i\alpha_i|0\rangle - b_i\alpha_i^*|1\rangle)|0\rangle \\
&\qquad + (-i\sigma_Y)(a_i\beta_i^*|0\rangle - b_i\beta_i|1\rangle)|1\rangle]. && (19)
\end{aligned}$$

According to the quantum signature scheme described in [22], $|\widetilde{\mathbf{SM}}\rangle$ will pass the verification for the signed message.

After the Z-transform attack is performed,

$$\begin{aligned}
|\widetilde{\mathbf{SM}}_i\rangle &= a_i\alpha_i|00\rangle + a_i\beta_i^*|10\rangle + b_i\beta_i|01\rangle - b_i\alpha_i^*|11\rangle && (20)\\
&= a_i(\alpha_i|0\rangle + \beta_i^*|1\rangle)|0\rangle - b_i(-\beta_i|0\rangle + \alpha_i^*|1\rangle)|1\rangle. && (21)
\end{aligned}$$

Obviously, $|\widetilde{\mathbf{SM}}\rangle$ can also pass the verification for the signer.

From the discussions above, we can see that by employing the Z-transform attack, Eve can successfully pass the verifications for both the signer and the signed message.

4.2.3 The Pauli-operators attack

In the previous subsections, we have shown that the quantum signature scheme with weak arbitrator [22] is susceptible to the X-transform and Z-transform attacks. By noting that the Y-transform is the combination of the X-transform and the Z-transform due to the fact that $\sigma_Y = -i\sigma_X\sigma_Z$, the quantum signature scheme with weak arbitrator [22] is also susceptible to the Y-transform attack.

In summary, the quantum signature scheme with weak arbitrator [22] is susceptible to the Pauli-operators attacks. The attacker can forge the signature by performing any Pauli operator on any bit of the intercepted quantum message. In other words, the attacker can forge the signature for any one of 4^L messages as long as he/she intercepts the quantum message-signature pair.

5 Conclusions

In this paper, we have analyzed the security of the quantum signature scheme with weak arbitrator [22]. First, we have showed that the attackers can counterfeit a signature for any message, which will pass the verification for the signer. Then, we have showed that the quantum signature scheme with weak arbitrator [22] is susceptible to the Pauli-operator attack. Such an attacker can forge the signature for any one of the 4^L (L is the length of the intercepted quantum message) messages, which will pass the verification for the signed message. In particular, an attacker who employs the Z-transform attack can forge the signature for any one of 2^L messages, which will pass the verifications for both the signer and the signed message successfully.

Acknowledgements

This work is supported in part by the National Natural Science Foundation (Nos. 61272058, 61073054), the Natural Science Foundation of Guangdong Province of China (No. 10251027501000004), the Specialized Research Fund for the Doctoral Program of Higher Education of China (No.

20100171110042), and the project of SQIG at IT, funded by FCT and EU FEDER projects QSec PTDC/EIA/67661/2006, AMDSC UTAustin/MAT/0057/2008, NoE Euro-NF, and IT Project QuantTel, FCT project PTDC/EEA-TEL/103402/2008 QuantPrivTel, FCT PEst-OE/EEI/LA0008/2011.

References

[1] Shor, P.W.: Algorithms for quantum computation: Discrete logarithms and factoring. In: Proceedings of Foundations of Computer Science, 1994, The 35th Annual Symposium on, pp. 124–134. IEEE (1994)

[2] Gottesman, D., Chuang, I.: Quantum digital signatures. ArXiv:quant-ph/0105032 (2001)

[3] Barnum, H., Crépeau, C., Gottesman, D., Smith, A., Tapp, A.: Authentication of quantum messages. In: Foundations of Computer Science, 2002, The 43rd Annual IEEE Symposium on, pp. 449–458. IEEE (2002)

[4] Curty, M., Santos, D.J., Pérez, E., García-Fernández, P.: Qubit authentication. Physical Review A **66**(2), 022301 (2002)

[5] Zeng, G., Keitel, C.H.: Arbitrated quantum-signature scheme. Physical Review A **65**(4), 042312 (2002)

[6] Li, Q., Chan, W.H., Long, D.Y.: Arbitrated quantum signature scheme using Bell states. Physical Review A **79**(5), 054307 (2009)

[7] Lee, H., Hong, C., Kim, H., Lim, J., Yang, H.J.: Arbitrated quantum signature scheme with message recovery. Physics Letters A **321**(5), 295–300 (2004)

[8] Lu, X., Feng, D.: Quantum digital signature based on quantum one-way functions. In: Advanced Communication Technology, 2005 (ICACT 2005), The 7th International Conference on, vol. 1, pp. 514–517. IEEE (2004)

[9] Wang, J., Zhang, Q., Tang, C.: Quantum signature scheme with message recovery. In: Advanced Communication Technology, 2006 (ICACT 2006), The 8th International Conference, vol. 2, pp. 1375–1378. IEEE (2006)

[10] Wang, J., Zhang, Q., Tang, C.: Quantum signature scheme with single photons. Optoelectronics Letters **2**(3), 209–212 (2006)

[11] Wen, X., Liu, Y., Sun, Y.: Quantum multi-signature protocol based on teleportation. Zeitschrift fur Naturforschung A **62**(3/4), 147 (2007)

[12] Zeng, G., Lee, M., Guo, Y., He, G.: Continuous variable quantum signature algorithm. International Journal of Quantum Information **5**(4), 553–573 (2007)

[13] Yang, Y.G.: Multi-proxy quantum group signature scheme with threshold shared verification. Chinese Physics B **17**, 415 (2008)

[14] Lü, X., Feng, D.G.: An arbitrated quantum message signature scheme. Computational and Information Science pp. 1054–1060 (2005)

[15] Cao, Z., Markowitch, O.: Security analysis of one quantum digital signature scheme. In: Information Technology: New Generations, 2009 (ITNG'09), The Sixth International Conference on, pp. 1574–1576. IEEE (2009)

[16] Zou, X., Qiu, D.: Security analysis and improvements of arbitrated quantum signature schemes. Physical Review A **82**(4), 042325 (2010)

[17] Curty, M., Lütkenhaus, N.: Comment on "arbitrated quantum-signature scheme". Physical Review A **77**(4), 046301 (2008)

[18] Zeng, G.: Reply to "comment on 'arbitrated quantum-signature scheme' ". Physical Review A **78**(1), 016301 (2008)

[19] Greenberger, D.M., Horne, M.A., Zeilinger, A.: Going beyond Bell's theorem. ArXiv:0712.0921 (2007)

[20] Greenberger, D.M., Bernstein, H.J., Horne, M.A., Shimony, A., Zeilinger, A.: Proposed GHZ experiments using cascades of down-conversions. In: Quantum Control and Measurement, vol. 1, p. 23 (1993)

[21] Boykin, P.O., Roychowdhury, V.: Optimal encryption of quantum bits. Physical Review A **67**(4), 042317 (2003)

[22] Luo, M.X., Chen, X.B., Yun, D., Yang, Y.X.: Quantum signature scheme with weak arbitrator. International Journal of Theoretical Physics **51**, 2135–2142 (2012)

[23] Buhrman, H., Cleve, R., Watrous, J., De Wolf, R.: Quantum fingerprinting. Physical Review Letters **87**(16), 167902 (2001)

[24] Xiang, G.Y., Li, J., Yu, B., Guo, G.C.: Remote preparation of mixed states via noisy entanglement. Physical Review A **72**(1), 012315 (2005)