MedCrave
Step into the World of Research

Physics & Astronomy International Journal

Review Article

Open Access

CrossMark

Secure electronic voting scheme by the new quantum signature-masked authentication

Abstract

Signature-masked authentication is a type of authentication that a user can obtain services when the service provider ensured that the user has the corresponding credentials issued by a trusted central authentication (CA). In this paper, we introduce a new quantum signature-masked authentication scheme based on private key, in which, the centre of CA exports not only the original credential that certificates for the user by adding the user's secret information but also private key between the user Alice and the service provider Bob. The shared private key makes it possible for the communicators to protect their encoded quantum message from CA cheating. It is proved that the scheme can resist the forgery attack, impersonation attack and outside attack. Also, as a potential application of the scheme, an electronic voting method by using signature-masked authentication is introduced.

Keywords: signature-masked authentication, quantum key distribution, greenberger-horne-zeilinger, digital video broadcasting

Volume 2 Issue 6 - 2018

Negin Fatahi, Hamid Reza Afsheh
Department of Physics, Islamic Azad University, Kermanshah Branch, Iran

Correspondence: Negin Fatahi, Department of Physics, Islamic Azad University, Kermanshah Branch, Iran,
Email fatehi@iauksh.ac.ir

Received: October 25, 2018 | **Published:** December 17, 2018

Introduction

The most successful subject of quantum cryptography is quantum key distribution (QKD), which was firstly constructed by Bennett et al.[1] in 1984. It is believed that QKD is the first applied quantum information processing and its unconditional security has been proven.[2,3] Most recently, in addition to QKD, quantum cryptography protocols have been widely studied in many fields such as quantum digital signature, quantum message authentication, quantum image encryption and quantum steganography. Quantum digital signature is an important topic and a primitive component of modern cryptography. The digital signature is a mathematical scheme that maintains the authenticity of the data and digital document in channel.[4] A secure quantum signature scheme requires that each user is able to generate his (her) own signature effectively and verifies the validity of another user's signature on a specific document. Also, no one is able to efficiently generate the signatures of other users on documents that those users didn't sign. Therefore, it can be used to guarantee the authenticity, integrity and non-disavowal of transmitted messages or the signer of a document.

Digital signature is commonly used in software distributions and financial transactions where it is important to detect forgery or tampering. The first quantum digital signature scheme was proposed by Gottesman, et al.[5] Then, research made several advances. The problem of how to authenticate quantum information sent through a quantum channel between two communicating parties with the minimum amount of resources is addressed by M Curty, et al.[7] and they define that one elementary quantum message (a qubit) can be authenticated with a key of minimum length. An algorithm by using a symmetrical quantum key cryptosystem and Greenberger-Horne-Zeilinger (GHZ) triplet states relies on the availability of an arbitrator suggested by G Zeng, et al.[8] Based on two-particle entangled Bell states, Q Li, et al.[9] proposed an arbitrated quantum signature scheme while providing a higher efficiency in transmission and reducing the complexity of implementation. In 2004 H Lee, et al.[10] presented two quantum signature schemes with message recovery which relies on the availability of an arbitrator that one of them by using a public board while the others does not. However both schemes provide confidentiality of the message and a higher efficiency in transmission. A quantum digital signature scheme was proposed based on quantum mechanics by using public quantum keys publicized by the signatory to verify the validity of the signature introduced by X Lu, et al.[11] A prototype of quantum signature scheme using single photons and its extensions were presented.[12] A protocol which can be used in multi-user quantum signature was based on the correlation of GHZ states and the controlled quantum teleportation proposed by X Wen, et al.[13] Also, a true quantum signature algorithm based on continuous-variable entanglement state is proposed[14] and by employing the signature key, a message state is encoded into a 2k-particle entangled state and a two-particle entangled state is prepared. The resulting states are exploited as a signature of the message state. Yang[15] proposed a multi-proxy quantum group signature scheme with threshold shared verification. In 2010, Naseri[16] revisited a weak blind signature scheme based on the correlation of Einstein-Padolsky-Rosen pairs and was shown that the scheme in its original form does not complete the task of a blind signature fairly. In addition, two papers in this field were presented.[17,18]

In many cryptography applications, there is a trusted centre of CA that exports the credential certificates to the qualified users. The user can obtain its services, when the service provider is ensured that users have the corresponding credentials issued by the CA. This type of authentication is called signature-masked authentication. In quantum signature-masked authentication scheme, the user can not send signature of the CA directly to the service provider while the service provider can be convinced that the user is legitimate and really knows the signature. Signature-masked authentication is widely used in many systems such as the identity authentication between Digital Set-Top-Box (DSTB) and smart card in secure Digital Video Broadcasting (DVB) service system.

Recently, some signature masked authentication has been proposed successively. The security of Zhang's scheme analyze and a new quantum signature-masked authentication scheme proposed that in this scheme a semi-trusted center of CA issues the original credential

certificates for a user and the final credential certificates is generated by adding her secret information.[19] By using the Weil pairing based cryptographic primitives, signature-masked authentication schemes can be developed. In such a scheme, a legitimate user obtains a signature from a Certificate Authority, and for getting services from a service provider, he convinces the service provider that he has the signature without transmitting the original signature of the provider.[20] A secure quantum identification system combining a classical identification procedure and quantum key distribution is proposed.[21] For user authenticated quantum key distribution in jammable public channel between Alice and Bob via an arbitrator Trent, the secure protocols provide data integrity and mutual identification of the messenger and recipient.[22] A secure quantum key verification scheme, which can simultaneously distribute the quantum secret key and verify the communicators identity proposed.[23] Also in references[24–26] quantum image encryption based on generalized Arnold transforms, quantum image XOR operations and generalized affine transform and logistic map was proposed by NR Zhou, et al.[24] Three protocols of quantum steganography based on probability measurements, the tensor product of Bell states and via a GHZ(4) state proposed in references.[27,28] In addition, an arbitrated Quantum Signature Scheme based on Cluster States with high-Efficient was proposed in reference.[29] what's more, in relation to the quantum information a lot of research has been done[30–34] that these methods can be used to exchange information in a safe way. This paper is organized as follows: In section 2, we introduce a quantum identity authentication based on public key as Zhang's scheme[35] and we use the elementary method of this scheme in our new protocol. In section 3, we propose a quantum signature-masked authentication scheme based on the private key. In section 4, the security of the new protocol is analyzed. In section 5, a new electronic voting scheme proposed by using the protocol that is introduced in section 3. Conclusion is given in the last section.

Zhang's scheme for quantum signature-masked authentication

In this section, we review the Zhang's protocol. This protocol includes three participants, Alice as a user, Bob as a service provider and a centre of CA. Three phases of Zhang's protocol are preparation phase, signature phase and authentication phase, which are as follows:

Preparation phase

Alice randomly selects a public key $K_a = (a_1, b_1, a_2, b_2, a_n, b_n)$ for identity and sends it to CA. Then CA examines the qualification of Alice, if CA accepts Alice as a legitimate user, CA generates a private key $K_b = (e_1, f_1, e_2, f_2, e_n, f_n)$ and sends it to Alice in a secure way. Also CA calculates $K = K_a \oplus K_b = (k_1^a, k_1^b, k_2^a, k_2^b, .. k_n^a, k_n^b)$ and secretly stores it, where $(a_i, b_i, e_i, f_i, k_i^a, k_i^b) \in \{0,1\}$, and $\oplus$ represents bitwise exclusive-OR.

Signature phase

Suppose that an authentication message of Alice is $M = (c_1, c_2, c_n)$, where C_i in $\{0,1\}$. Alice generates a quantum state encoded with K_b expressed by $|\phi\rangle = |\varphi_{c_1 \oplus e_1, f_1}\rangle \otimes |\varphi_{c_2 \oplus e_2, f_2}\rangle \otimes \otimes |\varphi_{c_i \oplus e_i, f_i}\rangle$, where a qubit $|\varphi_{c_i \oplus e_i, f_i}\rangle, i = (1, 2, n)$ is one of the following states:

$$|\varphi_{0,0}\rangle = |0\rangle \quad (1)$$
$$|\varphi_{1,0}\rangle = |1\rangle$$
$$|\varphi_{0,1}\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$
$$|\varphi_{1,1}\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

According to values of f_i, the quantum basis are selected. If $f_i = 0$, then $c_i \oplus e_i$ is encoded in the Z-basis $\{|0\rangle, |1$ and if $f_i = 1$, then $c_i \oplus e_i$ is encoded in the X-basis $\{|+\rangle, |$

Alice sends the encoded quantum state $|\phi\rangle$ to CA (to check eavesdropping, Alice inserts some decoy particles S_{el} in the quantum state $|\phi\rangle)$. As soon as receiving $|\phi\rangle$, CA applies $W^{[1]}$ to $|\phi\rangle$ according to K

$$W^{[1]} : |\phi\rangle \to |\phi'\rangle,$$

where $W^{[1]}$ is defined as

$$W^{[1]} = U_1^{[1]} V_1^{[1]} \otimes U_2^{[1]} V_2^{[1]} \otimes .. \otimes U_n^{[1]} V_n^{[1]} \quad (2)$$

and

$$U_i^{[1]} = U(k_i^a), V_i^{[1]} = V(k_i^b)$$
$$U(1) = i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0| \quad (3)$$
$$U(0) = |0\rangle\langle 0| + |1\rangle\langle 1|$$
$$V(1) = H = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\langle 0| + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\langle 1|$$
$$V(0) = |0\rangle\langle 0| + |1\rangle\langle 1|.$$

CA encodes quantum state $|\phi'\rangle$, and he/she forms M sequence. For eavesdropping check CA prepares and inserts some decoy photons randomly in one of the states in eq. (1) into the sequence. Afterwards, CA sends quantum state $|\phi'\rangle$ and all decoy photons to Bob.

Authentication phase

When Bob receives all photons and states, CA announces publicly the positions and the states of decoy photons. Therefore, using the decoy photon security checking method, they can check if the quantum channel is secure or not.[17,18] If they are confirmed that the channel is secure, Bob applies $W^{[2]}$ to $|\phi'\rangle$ according to K_a

$$W^{[2]} : |\phi'\rangle \to |\phi''\rangle,$$

where

$$W^{[2]} = U_1^{[2]} V_1^{[2]} \otimes U_2^{[2]} V_2^{[2]} \otimes .. \otimes U_n^{[2]} V_n^{[2]} \quad (4)$$

and

$$U_i^{[2]} = U(a_i), V_i^{[2]} = V(b_i) \quad (5)$$
$$U(1) = i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$$
$$U(0) = |0\rangle\langle 0| + |1\rangle\langle 1|$$
$$V(1) = H = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\langle 0| + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\langle 1|$$
$$V(0) = |0\rangle\langle 0| + |1\rangle\langle 1|.$$

Bob measures $|\phi''\rangle$ on the basis (0,0,0) and gets message $(c_1''c_2, .c_n)'$. If $(c_1, c_2, c_n) = (c_1''c_2, .c_n')$ the signature is valid. Otherwise, the signature is invalid.

Citation: Fatahi N, Afsheh HR. Secure electronic voting scheme by the new quantum signature-masked authentication. *Phys Astron Int J.* 2018;2(6):586–591. DOI: 10.15406/paij.2018.02.00146

Prior to present our scheme, let us say few words about the security of Zhang's protocol. There are two objections to this Protocol, which are forgery attack and impersonation attack.[19]

Forgery attack

One means that Alice knows public key K_a and private key K_b namely $K = K_a \oplus K_b$, therefore CA and also Alice similarly can make the signature $|\phi'\rangle$ which is called credential certificates in the traditional cryptography. Therefore, when Bob reserves the signature $|\phi'\rangle$, he cannot recognize the true source of quantum state $|\phi'\rangle$, which may be Alice sent or CA. If Alice is malicious, she can forge valid signature by herself to get some services from the services provider Bob.

Impersonation attack in this protocol CA may be untrusted. In the preparation phase CA got public key K_a from Alice. An impersonation attack refers to an attack in which CA generates a quantum state $|\phi\rangle$ and obtain Alice's signature (credential certificates) without Alice's participation. Therefore, CA wants to get Alice's privacy information by forging her credential certificates, but Zhang's scheme cannot check the malicious CA from the legitimate user Alice.

Because of these two attacks, Zhang's scheme is limited in many network systems.[19] For example, in many cryptographic application when a user wants to some services from a service provider (e.g. a user applies for a driving license from the traffic management department), firstly he has to prove to the service provider that he is eligible (e.g. he has passed the driving examination) he has a credential certificate issued by a trusted center of CA. Therefore, the service provider prepares the service to the user. So the Zhang's scheme is not secure. Considering the disadvantages of the Zhang's scheme, in the next section, by using a private key, a new secure protocol for quantum signature-masked authentication is proposed and a new method of electronic voting is introduced by this scheme.

New quantum signature-masked authentication scheme based on private key

In the reference[19] a quantum signature-masked authentication scheme introduced which seems very complicated. In this paper by removing some parts of previous method and making the necessary changes, we propose a quantum signature-masked authentication scheme based on the private key. This new introduced method is just as secure and is simpler than the previous one. Then by using this new method we introduce secure electronic voting scheme in the next section. Similar to the Zhang's scheme, our protocol involves a user Alice, a service provider Bob and a center of CA and includes but the following is set up, signature-masked and authentication phases.

Set up phase

Alice and Bob select a public key P_A and P_B respectively:

$$P_A = (a_1^A, b_1^A, a_2^A, b_2^A, a_n^A, b_n^A) \tag{6}$$

$$P_B = (a_1^B, b_1^B, a_2^B, b_2^B, a_n^B, b_n^B)\ , \tag{7}$$

where $a_i^A, b_i^A, a_i^B, b_i^B \in \{0,1\}, 0 \le i \le n$. Alice and Bob send P_A and P_B to CA, while they insert sufficiently large number of decoy particles into them for eavesdropping check.

Once CA receives P_A and P_B, Alice and Bob announce publicly the positions and the states of the decoy particle. CA performs a suitable measurement on each decoy particle with the same basis as Alice and Bob chose. Then, comparing his measurement results with Alice's and Bob's announcement, CA can examine the qualification of Alice and Bob. If the CA accepts Alice and Bob as legitimated users, he/she generates private keys S_A and S_B for Alice and Bob respectively and sends them in a secure quantum way:

$$S_A = (c_1^A, d_1^A, c_2^A, d_2^A, c_n^A, d_n^A) \tag{8}$$

$$S_B = (c_1^B, d_1^B, c_2^B, d_2^B, c_n^B, d_n^B)\ , \tag{9}$$

where $c_i^A, d_i^A, c_i^B, b_i^B \in \{0,1\}, 0 \le i \le n.$

CA calculates and secretly stores $E_C = S_A \oplus S_B = (e_1, f_1, e_2, f_2, , e_n, f_n)$ where $(e_i, f_i) \in \{0,1\}$ and $\oplus$ represents bitwise exclusive-OR.

Signature-masked phase

Alice's authentication message is:

$$M = (m_1, m_2, . m_n)\ , \tag{10}$$

where $m_i \in \{0,1\}, 0 \le i \le n$. Alice generates an encoded quantum state $|\phi\rangle$ according to S_A:

$$|\phi\rangle = |\varphi_{m_1 \oplus c_1^A, d_1^A}\rangle \otimes |\varphi_{m_2 \oplus c_2^A, d_2^A}\rangle \otimes .....\otimes |\varphi_{m_n \oplus c_n^A, d_n^A}\rangle\ , \tag{11}$$

where for each $i = 1, 2, n$, a qubit $|\varphi_{m_i \oplus c_i^A, d_i^A}\rangle$ is one of the following states:

$$|\varphi_{0,0}\rangle = |0\rangle$$

$$|\varphi_{1,0}\rangle = |1\rangle$$

$$|\varphi_{0,1}\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$|\varphi_{1,1}\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

Alice selects a private key $R_A = (g_1, h_1, g_2, h_2, .. g_n, h_n)$ where $g_i, h_i \in \{0,1\}, 0 \le i \le n$ and sends it to Bob in a secure quantum channel. In this part Alice again uses decoy particles eavesdropping check method for sending R_A to Bob.

Alice applies $W^{[1]}$ to $|\phi\rangle$ according to R_A and obtains the signature $|\phi'\rangle$.

$$W^{[1]} : |\phi\rangle \to |\phi'\rangle,$$

$W^{[1]}$ is defined as

$$W^{[1]} = U_1^{[1]} V_1^{[1]} \otimes U_2^{[1]} V_2^{[1]} \otimes .. \otimes U_n^{[1]} V_n^{[1]} \tag{12}$$

where

$$U_i^{[1]} = U(g_i), V_i^{[1]} = U(h) \tag{13}$$

$$U(1) = i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$$

$$U(0) = |0\rangle\langle 0| + |1\rangle\langle 1|$$

$$V(1) = H = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\langle 0| + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\langle 1|$$

$$V(0) = |0\rangle\langle 0| + |1\rangle\langle 1|.$$

Then Alice sends $|\phi'\rangle$ to CA through a secure quantum channel.

CA applies $W^{[2]}$ to $|\phi'\rangle$ according to $E_C = S_A \oplus S_B$ and obtains the signature $|S\rangle$.

Citation: Fatahi N, Afsheh HR. Secure electronic voting scheme by the new quantum signature-masked authentication. *Phys Astron Int J.* 2018;2(6):586–591. DOI: 10.15406/paij.2018.02.00146

$W^{[2]}:|\phi'\rangle \to |S\rangle,$

$W^{[2]}$ is defined as

$$W^{[2]} = U_1^{[2]}V_1^{[2]} \otimes U_2^{[2]}V_2^{[2]} \otimes .. \otimes U_n^{[2]}V_n^{[2]} \quad (14)$$

where

$$U_i^{[2]} = U(e_i), V_i^{[2]} = U(f) \quad (15)$$

$$U(1) = i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$$

$$U(0) = |0\rangle\langle 0| + |1\rangle\langle 1|$$

$$V(1) = H = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\langle 0| + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\langle 1|$$

$$V(0) = |0\rangle\langle 0| + |1\rangle\langle 1|.$$

Finally, CA sends signature $|S\rangle$ to Bob.

Authentication phase

Bob authenticates Alice's individuality, then applies $W^{[3]}$ to $|S\rangle$ according to $Z_b = S_B \oplus R_A = (q_1, t_1, q_2, t_2, q_n, t_n)$ obtains the signature $|S'\rangle$, where:

$W^{[3]}:|S\rangle \to |S'\rangle,$

$$W^{[3]} = U_1^{[3]}V_1^{[3]} \otimes U_2^{[3]}V_2^{[3]} \otimes \otimes U_n^{[3]}V_n^{[3]} \quad (16)$$

and

$$U_i^{[3]} = U(q_i), V_i^{[3]} = V(t) \quad (17)$$

$$U(1) = i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$$

$$U(0) = |0\rangle\langle 0| + |1\rangle\langle 1|$$

$$V(1) = H = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\langle 0| + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\langle 1|$$

$$V(0) = |0\rangle\langle 0| + |1\rangle\langle 1|.$$

Bob measures $|S'\rangle$ on the basis (0,0,0) and gets message $M' = (m_1''m_2, .. m_n)'$. If $(m_1, m_2, ., m_n) = (m_1'm_2', . m_n')$ the signature is valid. Otherwise, the signature is invalid.

We can show correctness of the proposed quantum signature-masked authentication scheme based on private key as follow.

The initial quantum state $|\phi\rangle$ generated according to S_A by Alice. During the signature-masked and authentication phases, it passes the following process:

$$message\, M \to^{S_A} |\phi\rangle \to^{R_A} |\phi'\rangle \to^{S_A \oplus S_B} |S\rangle \to^{S_B \oplus R_A} |S'\rangle. \quad (18)$$

By equations (8), (9) and R_A we have:

$$d_i^A = h_i \oplus d_i^A \oplus d_i^B \oplus d_i^B \oplus h_i \quad (19)$$

$$d_i^A = h_i \oplus d_i^A \oplus d_i^B \oplus d_i^B \oplus h_i. \quad (20)$$

As previously noted, Bob can measure $|S'\rangle$ on the basis $(|0\rangle, |0\rangle, .. |0\rangle)$ and get $(m_1'm_2', m_n')$, and it is easy to verify $(m_1', m_2', . m_n') = (m_1, m_2, m_n)$ holds.

Security analysis

In this section, a security of the proposed scheme is analyzed and it has been shown that the protocol withstands forgery attack, impersonation attack and outside attack. First of all, it's noted that all states and keys are transferred in secure quantum channel and sent by using the decoy particles eavesdropping check method. Therefore, the probability of an attack is low. It is also possible one of the user, the service provider or the center of authentication is untrustworthy.

Alice forgery attack

Let us discuss how the proposed protocol withstands the Alice forgery attack.

In this scheme, Alice may be dishonest. We show that she cannot forge $|S\rangle$. The verifying process of the signature $|\phi'\rangle$ must use the private keys S_A and S_B, so the receiver Bob can confirm Alice's legation with the help of CA. An effective $|S\rangle$ needs using the knowledge of the Bob's private key S_B, because Alice does not know the value of S_B, she cannot forge signature $|S\rangle$. Concluding, a malicious Alice cannot forge credential certificates by herself to get some services from the service provider Bob.

Bob forgery attack

Suppose that, an attacker wants to impersonate the service provider Bob to verify Alice's identity in order to provide some false services. In the verify phase, a verifier has to use his private key S_B and the shared private keys R_A between Alice and Bob to verify the validity of Alice's credential certificates $|S'\rangle$. Only the service provider Bob has the two keys S_B and R_A. So no one can verify the validity of Alice's credential certificates except Bob. As well as, one possible strategy for the malicious Bob that tries to forge Alice's signature is to obtain the private key R_A to generate $|\phi'\rangle$, however, since the key is distributed through quantum key distribution, it would be impossible, . Moreover, the service provider Bob does not know Alice's private key S_A, therefore Alice's credential certificates $|\phi\rangle$ cannot be forged by the service provider.

Impersonation attack

The new proposed scheme based on private key can withstand the impersonation attack. May be, an attacker may impersonate the user Alice in order to use some services from the service provider Bob. Firstly, CA may forge Alice's credential certificates $|\phi'\rangle$, then impersonate Alice to obtain some services from the service provider Bob, actually CA may be destructive. CA can not generate a valid $|\phi'\rangle$, because an effective $|\phi'\rangle$ needs using the knowledge of the shared key R_A that is transmitted between Alice and Bob in secure quantum channel. So, the quantum state $|\phi'\rangle$ is unknown to CA and CA cannot impersonate the user Alice to get some services from the service provider Bob.

Outside attack

Alice, Bob and CA as the participants, are still unable to forge signatures, let assume an outsider attacker Eve. All the keys, quantum states and messages transmitted through quantum channel are encrypted by using a decoy particles encryption algorithm. Also, in our proposed scheme based on a private key, the CA issues the original signature for the qualified Alice. Because no one knows the two private keys S_A and S_B except CA, only CA can generate $|S\rangle$. Therefore, our scheme is manageable and withstands the outside attack.

Secure electronic voting scheme

In this section, we proposed a new method of Electronic voting by

Citation: Fatahi N, Afsheh HR. Secure electronic voting scheme by the new quantum signature-masked authentication. *Phys Astron Int J.* 2018;2(6):586–591. DOI: 10.15406/paij.2018.02.00146

using the quantum signature- masked authentication based on private key that introduced in previous section. Electronic voting includes the following several parties:

1. Elector and owner of the vote message is the voter Alice.
2. Charlie is the vote management center and signer that checks the qualification of voters, distributes ballots.
3. Bob is the center of counting votes and teller.
4. Diana is a scrutineer that supervises the behaviour of Charlie. Charlie and Diana will verify the messages and signatures.

Proposed Electronic voting contains three phases:

a) Setup

b) Vote stage

c) Counting ballots and supervising.

Set up phase

First, the voter Alice sends her identification information to the vote management center Charlie. Then Charlie checks whether Alices identity is eligible and whether this vote is the first one. If not, he will refuse to award tickets. Conversely, if Alice satisfies the vote conditions, the vote management center will randomly assign Alice a unique vote ID and this means that the voter registration is successful. After registration, the public keys P_A and P_B and private keys S_A and S_B such as (6), (7), (8), (9) share between Alice, Bob and Charlie. Charlie calculates and secretly stores $E_C = S_A \oplus S_B$.

Vote stage

Alice converts the vote message M into a n-bit binary sequence. That is

$$M = (m_1, m_2, . m_n), \tag{21}$$

where $m_i \in \{0,1\}, 0 \le i \le n$. The vote message M is blind to quantum state $|\phi\rangle$ according to S_A as defined in previous section by (11). Alice sends $|\phi\rangle$ to scrutineers Diana.

Alice selects a serial number as binary sequences $R_A = (g_1, h_1, g_2, h_2, , g_n, h_n)$ where $g_i, h_i \in \{0,1\}, 0 \le i \le n$ and sends it to the center of counting votes Bob.

Alice applies $W^{[1]}$ according to serial number R_A to $|\phi\rangle$ obtains the signature $|\phi'\rangle$ and sends it to the vote management center Charlie. The $W^{[1]}$ define by (12).

The vote management Charlie applies $W^{[2]} : |\phi'\rangle \rightarrow |S\rangle$ according to $E_C = S_A \oplus S_B$ and sends signature $|S\rangle$ to teller Bob.

Counting ballots and supervising

The center of counting votes Bob after receiving the signed votes and authenticates Alice's individuality, applies $W^{[3]} : |S\rangle \rightarrow |S'\rangle$ according to private key and serial number $Z_b = S_B \oplus R_A = (q_1, t_1, q_2, t_2, q_n, t_n)$.

Bob sends $|S'\rangle$ to scrutineers Diana.

Bob measures $|S'\rangle$ on the basis $(|0\rangle, |0\rangle, |0\rangle)$ and gets $(m'_1, m'_2, ., m'_n)$, if $(m'_1, m'_2, m'_n) = (m_1, m_2, m_n)$ the vote is legible and signature masked can be verified otherwise, vote and signature is invalid.

Under the scrutineer Diana, the teller Bob gets every voter's ballot. Diana as a supervisor compares the signature message $|S'\rangle$ that Bob sent with the $|\phi\rangle$. If these two states are equal, it means the signature masked and vote is valid if not, which indicates the presence of cheating.

For the voters to confirm information later, every voter's ballot number and election contents are posted on bulletin boards.

Finally, if there is no dispute announce to the public that that the election is effective and announce the election results.

The proposed electronic voting is secure because the quantum-signature masked authentication protocol that used for voting is protected under the each kind of attack (as explained in section 4).

Conclusion

In summary, a quantum signature-masked authentication scheme based on private key is pro- posed. Different from previous protocols, by using the private key R_A that is only known by Alice and Bob, the center of CA does not know the contents of the message. The user's final credential certificate is issued by hers and CA together. It has been shown that the proposed protocol can resist not only inside attacks such as the participant's Alice's forgery attack, Bob's forgery attack, impersonation attack but also it is secure against outside attacks which can be widely used in many systems, such as the identity authentication between Digital Set-Top-Box (DSTB) and smart card in secure Digital Video Broadcasting (DVB) service system. Also, we introduce a new electronic voting scheme by using this secure method.

Acknowledgments

This work is supported by Kermanshah Branch, Islamic Azad University

Conflicts of interest

Authors declare there is no conflict of interest.

References

1. CH Bennett, G Brassard. Quantum Cryptography Public Key Distribution and Coin Tossing. In Proceedings of IEEE International Conference on Computers Systems and Signal Processing; 1984 December; India. p. 175−179.
2. D Mayers. Unconditional security in quantum cryptography. *Journal of the ACM*. 2001;48(3):351−406.
3. P Shor, J Priskill. Simple proof of security of the bb84 quantum key distribution protocol. *Physical Review Letters*. 2000;85:441−444.
4. O Goldreich. *Foundations of Cryptography*. UK: Cambridge university press; 2001.
5. D Gottesman, I Chuang. Quantum digital signatures. 2001. p. 8.
6. H Barnum, C Crepeau, D Gottesman, et al. Authentication of quantum messages. The 43rd Annual IEEE Symposium on Foundations of Computer Science; 2002 Nov 19; IEEE: Canada. p. 449−458.
7. M Curty, DJ Santos, E Perez, et al. Qubit authentication. *Physical Review A*. 2002;66(2):022301.
8. G Zeng, CH Keitel. Arbitrated quantum−signature scheme. *Physical Review A*. 2002;65(4):042312.
9. Q Li, WH Chan, DY Long. Arbitrated quantum signature scheme using Bell states. *Physical Review A*. 2009;79(5):054307.

10. H Lee, C Hong, H Kim, et al. Arbitrated quantum signature scheme with message recovery. *Physics Letters A*. 2004;321(5−6):295−300.
11. X Lu, D Feng. Quantum digital signature based on quantum one-way functions. The 7th International Conference on Advanced Communication Technology; 2005 July 21−23; South Korea. p. 514−517.
12. J Wang, Q Zhang, C Tang. Quantum signature scheme with single photons. *Optoelectronics Letters*. 2006;2(3):209−212.
13. X Wen, Y Liu, Y Sun. Quantum multi-signature protocol based on teleportation. *Zeitschrift fur Naturforschung A*. 2007;62(3−4)147−151.
14. G Zeng, M Lee, Y Guo, et al. Continuous variable quantum signature algorithm. *International Journal of Quantum Information*. 2007;5(4):553−573.
15. YG Yang. Multi-proxy quantum group signature scheme with threshold shared verification. *Chinese Physics B*. 2008;17(2):415.
16. M Naseri. A weak blind signature based on quantum cryptography. *International Journal of the Physical Sciences*. 2011;6(21):5051−5053.
17. Naseri M. Comment on: "secure direct communication based on ping-pong protocol" [Quantum Inf. Process. 8, 347 (2009)]. *Quantum Information Processing*. 2010;9(6):693−698.
18. Sheikhehi F, Naseri M. Probabilistic bidirectional quantum secure communication based on a shared partially entangled states. *International Journal of Quantum Information*. 2011;9(supp 0l):357−365.
19. WM Shi, YG Yang, YH Zhou. Quantum signature masked authentication schemes. *Optik*. 2015;126(23):3544−3548.
20. FG Zhang, K Kim. Signature-masked Authentication Using the Bilinear Pairings. Cryptology and Information Security Laboratory (CAIS), Information and Communications University, South Korea. 2002.
21. M Dusek, O Haderka, M Hendrych, et al. Quantum identification system. *Physical Review A*. 1999;60:149156.
22. D Ljunggren, M Bourennane, A Karlsson, et al. Authority−based user authenticationin quantum key distribution. *Physical Review A*. 2000;62:022305.
23. GH Zeng, WP Zhang. Identity verification in quantum key distribution. *Physical Review A*. 2001;61:022303.
24. N Zhou, T Hua, L Gong, et al. Quantum image encryption based on generalized Arnold transform and double random phase encoding. *Quantum Information Processing*. 2015;14(4):1193−1213.
25. H Liang, X Tao, N Zhou. Quantum image encryption based on generalized affine transform and logistic map. *Quantum Information Processing*. 2016;15(7):2701−2724.
26. L Gong, X He, Sh Cheng, et al. Quantum image encryption algorithm based on quantum image XOR operations. *International Journal of Theoretical Physics*. 2016;55(7):3234−3250.
27. ZH Wei, XB Chen, XX Niu, et al. A novel quantum steganography protocol based on probability measurements. International *Journal of Quantum Information*. 2013;11(7):1350068.
28. SJ Xu, XB Chen, XX Niu, et al. High-efficiency quantum steganography based on the tensor product of Bell states. *Science China−Physics Mechanics and Astronomy*. 2013;56(9):1745−1754.
29. N Fatahi, M Naseri, LH Gong, et al. High−Efficient Arbitrated Quantum Signature Scheme Based on Cluster States. *International Journal of Theoretical Physics*. 2016;56(2):609−616.
30. M Naseri, Sh Heidari, M Baghfalaki, et al. A new secure quantum watermarking scheme. *Optik*. 2017;139:77−86.
31. M Naseri, M Abdolmaleky, F Parandin, et al. A New Quantum Gray−Scale Image Encoding Scheme, Communication in Theoretical Physics. 2018;69(2):215226.
32. M Naseri, Sh Heidari, R Gheibi, et al. A novel quantum binary images thinning algorithm: A quantum version of the Hilditch' s algorithm. *Optik*. 2017;131:678−686.
33. M Naseri, N Fatahi, A Farouk, et al. Applications of Quantum Mechanics in Secure Communication. In Hassanien A, Elhoseny M, Kacprzyk J, editors. *Quantum Computing: An Environment for Intelligent Large Scale Real Application*. Cham: Springer; 2018; p. 25−40.
34. M Naseri, LH Gong, M Houshmand, et al. An Anonymous Surveying Protocol via Greenberge-Horne-Zeilinger States. *International Journal of Theoretical Physics*. 2016;55(10):4436−4444.
35. XL Zhang. One-way quantum identity authentication based on public key. *Chin Sci Bull*. 2009;54:2018202.

Citation: Fatahi N, Afsheh HR. Secure electronic voting scheme by the new quantum signature-masked authentication. *Phys Astron Int J.* 2018;2(6):586–591. DOI: 10.15406/paij.2018.02.00146