ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **9** (2020), no.4, 1803–1810
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.4.36 Spec. Issue on NCFCTA-2020

IMPROVE SECURITY OF QUANTUM PROXY SIGNATURE SCHEME USING QUANTUM ONE-WAY FUNCTION AND BELL STATES

MANOJ KUMAR, SUDHANSHU SHEKHAR DUBEY[1], PRATIK GUPTA, AND YOGESH KHANDELWAL

ABSTRACT. With the advancement of the quantum cryptography, it is unconditional secure to transfer data between two remote parties. The present paper proposes a new quantum proxy signature scheme using quantum one-way function (OWF) and EPR quantum entanglement. Quantum one-way function can be computed polynomial time but are hard to invert in polynomial time. It is easy to compute on every input but hard to invert. The quantum key distribution, OWF and one-time-pad encryption algorithm guarantee the unconditional security of this scheme.

1. INTRODUCTION

Quantum cryptography providing information security, the most successful topic of quantum cryptography is quantum key distribution (QKD). QKD firstly proposed by Bennett and Brassard [1] in 1984, which provide the unconditional security. Quantum cryptography protocol is widely studied in these years, such as quantum digital signature and quantum message authentication. Gottesman and Chuang [2] develop a quantum digital system based on quantum mechanics, this protocol claim that the scheme is perfectly secure. Digital signature is an

[1]*corresponding author*

2010 *Mathematics Subject Classification.* 94A60, 14G50.

Key words and phrases. Quantum cryptography, Entanglement, one-way function, Proxy signature, Unitary transformation, Quantum key distribution.

important branch of cryptography has widely used in E-payment system, mobile communication [3, 4] and grid computing, mobile agent. In the recent years, several researchers studied various kind of quantum signature such as quantum blind signature, quantum proxy signature [5–7] and quantum arbitrated signature.

The concept of one-way function (OWF) is fundamental tools for cryptography. Quantum OWF has several categories such as "classical-to-classical", "classical-to-quantum", and "quantum-to-classical". They are mostly used for post quantum cryptography or quantum cryptography.

The rest of the paper arranged in the following way. In section 2 introduces some definition and notation of the OWF. Section 3 consists of the proposed quantum proxy signature scheme and correctness of this scheme in section 4. The security analysis of this scheme defined in section 5. Finally the last section concludes the research work.

2. Some Basic Definitions and Notations

This section contains some basic definitions and notations about quantum one-way function and quantum fingerprinting function.

Definition 2.1 (Quantum one-way function)**.** *Quantum one-way function based on the principles of quantum mechanics and proposed by Gottesman and Chuang [2]. A function* $f : |x\rangle_{n_1} \rightarrow |f(x)\rangle_{n_2}$ *where* $n_1 >> n_2$ *and* $x \in F_2^{n_1}$*, is called a quantum one-way function under physical mechanics if*

(i) *Easy to compute: there is a quantum polynomial-time-algorithm* A *such that on input* $|x\rangle$ *outputs* $|f(x)\rangle$*.*

(ii) *Hard to invert: given* $|f(x)\rangle$*, it is impossible to invert* x *by virtue of fundamental quantum information theory.*

Definition 2.2. *(Quantum fingerprinting function) Quantum fingerprinting function of bit string* $v \in F_2^w$ *is*

$$|f(v)\rangle = \frac{1}{\sqrt{m}} \sum_{l=1}^{m} (-1)^{E_l(v)} |l\rangle$$

where $E : \{0,1\}^w \rightarrow \{0,1\}^m$ *is a collection of error correcting code with fixed* $c > 1, 0 < \delta < 1$ *and* $m = cw$*. The distance between* $E(u_1)$ *and* $E(u_2)$ *is at*

least $(1-\delta)\, m$. *Since two distinct coding words can be equal in at most* δm *positions, for any* $v_1 \neq v_2$ *we have* $\langle f(v_1) \mid f(v_2) \rangle \leq \frac{\delta m}{m} = \delta$.

3. Proposed Scheme

The proposed quantum deniable authentication protocol (QDAP) involving three entities: an original signatory Alice, a proxy signatory (receiver) Bob and a trusted center (TC). The current scheme contains the following four phases known as initialization phase, key exchange phase, authentication phase.

3.1. **Initialization Phase:**

Step (I). Trusted center (TC) shares secret key K_{TA} with Alice and secret key K_{TB} with Bob. The secret key K_{AB} is shared between Alice and Bob.

$$K_{AB} = \{p_1, q_1, p_2, q_2, \ldots, p_n, q_n\}$$

$$K_{TA} = \{r_1, s_1, r_2, s_2, \ldots, r_n, s_n\}$$

$$K_{TB} = \{t_1, u_1, t_2, u_2, \ldots, t_n, u_n\}$$

where p_i, q_i,r_i, s_i, t_i, $u_i$are in Z_2. Here $Z_2 = \{0, 1\}$ additive group of modulo 2 and $1 \leq i \leq n$.

Step (II). TC measure $2n$ EPR pairs $\{|A_1\rangle, |A_2\rangle, ..., |A_n\rangle\}$ then describes the sequence of particle $|A_p\rangle = \{|A_{p_1}\rangle, |A_{p_2}\rangle, \ldots, |A_{p_{2n}}\rangle\}$ to Alice and

$$|A_q\rangle = \{|A_{q_1}\rangle, |A_{q_2}\rangle, \ldots, |A_{q_{2n}}\rangle\}$$

to Bob. Here $|A_i\rangle = \frac{1}{\sqrt{2}}\left(|0_{p_i} 0_{q_i}\rangle + |1_{p_i} 1_{q_i}\rangle\right)$, where $i = 1, 2, \ldots, 2n$. For the distribution of $|A_p\rangle$and $|A_q\rangle$by using block-transmission protocol [17, 18] ensure the security of the channel.

Step (III). Using the secret key K_{TA} and K_{TB}, the new quantum state generates by TC and it can be written as

$$|B_T\rangle = |A_{r_1,u_1}\rangle \otimes |A_{r_2,u_2}\rangle \otimes \ldots \otimes |A_{r_n,u_n}\rangle \tag{3.1}$$

where $i = 1, 2, \ldots, n$ and $|A_{r_i,u_i}\rangle$ is taken from the following states:

$$|A_{0,0}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

$$|A_{0,1}\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |11\rangle)$$
$$|A_{1,0}\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)$$
$$|A_{1,1}\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle)$$

According to one-time pad encryption algorithm [19], using the secret keyK_{TA}, TC computes $E_{K_{TA}}\{|B_T\rangle\}$and sends it to Alice by a proper quantum channel.

Step (IV). Let Mbe the signer message such that $M = (m_1, m_2, \ldots, m_n)$ where $m_i \in Z_2 = \{0, 1\}$ and $i = 1, 2, \ldots, n$. Trusted centre (TC) computes

$$v_i = m_i \oplus r_i \oplus t_i$$

where $v = (v_1, v_2, \ldots, v_n)$ and $\oplus$ is XOR operation. After compute v_i then, we have to apply quantum one way function discussed in section 2. $|f(v)\rangle$ where

$$f : |x\rangle \to |f(x)\rangle$$

3.2. **Key Exchange Phase:**

Step (I): Alice computes the quantum states $|B_w\rangle = \{|B_w^1\rangle, |B_w^2\rangle, \ldots, |B_w^{2n}\rangle\}$ and each $|B_w^i\rangle \in \{|0\rangle, |1\rangle\}$ where

$$i = 1, 2, \ldots, 2n.$$

Step (II): After put on the Bell measurement by Alice on $|B_w^i\rangle$. If $|B_w^i\rangle$is $|0\rangle$ then Alice calculate $|A_{p_i}\rangle$ with the base $Z = \{|0\rangle, |1\rangle\}$.Otherwise he uses the base $X = \{|+\rangle, |-\rangle\}$, (where $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$) to calculate $|A_{p_i}\rangle$ and Alice write down the data as new state $|B_E\rangle$.

Step (III): Alice collect $E_{K_{TA}}\{|B_T\rangle\}$ from trusted centre (TC), decrypts with $K_{TA}$and give $|B_T\rangle$. After Alice performs $F^{(1)}$ to $|B_T\rangle$ and $F^{(1)}$is defined as

$$F^{(1)} = U^{(1)}_{p_1,q_1} \otimes U^{(1)}_{p_2,q_2} \otimes \ldots \otimes U^{(1)}_{p_n,q_n}$$

where $U^{(1)}_{p_i,q_i} = U_{p_i,q_i}$is one of the four Pauli operators:

$$U_{0,0} = I = |0\rangle\langle 0| + |1\rangle\langle 1|$$
$$U_{0,1} = \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$$
$$U_{1,0} = \sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$$
$$U_{1,1} = i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$$

Step (IV): Alice obtains $|B_{TA}\rangle$by using the unitary transformation $F^{(1)} : |B_T\rangle \rightarrow |B_{TA}\rangle$. According to one time pad algorithm, Alice creates a message $|S_A\rangle$ using the secret key K_{AB} and it sends to Bob through proper quantum channel. Here $|S_A\rangle = E_{K_{AB}}$which is the encryption of $|B_A\rangle$, $|B_w\rangle$ and $|B_{TA}\rangle$.
Step (V): Bob receives $|S_A\rangle$ and decrypts with K_{AB} and get the states $|B_A\rangle$, $|B_w\rangle$and$|B_{TA}\rangle$. After Bob first examine the quantum state $|B_w\rangle$is exact to step (I), then the process is continuous to next steps. Otherwise Bob terminate the signature.

Step (VI): Bob calculate his particle sequence $|A_{q_i}\rangle$ according to $|B_w^i\rangle$, where $i = 1, 2, \ldots, 2n$. If the value of $|B_w^i\rangle$ is $|0\rangle$, using the Z basis $\{|0\rangle, |1\rangle\}$ Bob calculates $|A_{q_i}\rangle$. Otherwise, Bob uses Xbasis $\{|+\rangle, |-\rangle\}$ to calculates $|B_{q_i}\rangle$. After that Bob put down the data as $|B_E^*\rangle$.

Step (VII): After step (VI) Bob justification between $|B_E\rangle$and $|B_E^*\rangle$. If $|B_E\rangle$and $|B_E^*\rangle$ are similar that is$|B_E\rangle = |B_E^*\rangle$, Bob accepts the proxy signature, otherwise Bob discards the signature.

3.3. **Key Updating Phase:**

Step (I). Bob randomly selects a sequence of private key

$$K_B = \{g_1, h_1, g_2, h_2, \ldots, g_n, h_n\}$$

and g_i, h_i are in Z_2. Here $Z_2 = \{0, 1\}$ additive group of modulo 2 and $1 \leq i \leq n$.

Step (II). Bob prepare K_{PB} and publish his private key

$$K_{PB} = K_B \oplus K_{AB} \oplus K_{TB}$$

$$K_{PB} = \{a_1, b_1, a_2, b_2, \ldots, a_n, b_n\} \tag{3.2}$$

Step (III). He put in $F^{(2)}$ to $|B_{TA}\rangle$ using private key $K_B$and obtains the proxy signature$|S\rangle$

$$F^{(2)} : |B_{TA}\rangle \rightarrow |S\rangle$$

here$F^{(2)}$ is defined as

$$F^{(2)} = U^{(2)}_{g_1,h_1} \otimes U^{(2)}_{g_2,h_2} \otimes \ldots \otimes U^{(2)}_{g_n,h_n}$$

where $U^{(2)}_{g_i,h_i} = U_{g_i,h_i}$ is one of the four Pauli operators:

$$U_{0,0} = I = |0\rangle\langle 0| + |1\rangle\langle 1|$$

$$U_{0,1} = \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$$

$$U_{1,0} = \sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$$

$$U_{1,1} = i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$$

3.4. **Authentication Phase:** Now suppose any verifier V can verify the proxy signature $|S\rangle$ of the following steps:

Step (I). Verifier V operate $F^{(3)}$ to $|S\rangle$ by using K_{PB} then obtains the verifier signature $|S_V\rangle$

$$F^{(3)} : |S\rangle \to |S_V\rangle$$

here $F^{(3)}$ is defined as

$$F^{(3)} = U^{(3)}_{a_1,b_1} \otimes U^{(3)}_{a_2,b_2} \otimes \ldots \otimes U^{(3)}_{a_n,b_n}$$

where $U^{(3)}_{a_i,b_i} = U_{a_i,b_i}$ is one of the four Pauli operators:

$$U_{0,0} = I = |0\rangle\langle 0| + |1\rangle\langle 1|$$

$$U_{0,1} = \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$$

$$U_{1,0} = \sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$$

$$U_{1,1} = i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$$

Step (II). On the basis $(|0\rangle, |0\rangle, \ldots, |0\rangle)$, V computes $|S_V\rangle$ and give $(\lambda_1, \lambda_2 \ldots, \lambda_n)$. After verifier computes

$$v_i^* = \lambda_i \oplus m_i$$

where $v^* = (v_1^*, v_2^*, \ldots, v_n^*)$.

Step (III). Verifier V measure $|f(v^*)\rangle$ and compare it with $|f(v)\rangle$, if $|f(v)\rangle = |f(v^*)\rangle$ then the signature is authenticate, otherwise delete the signature.

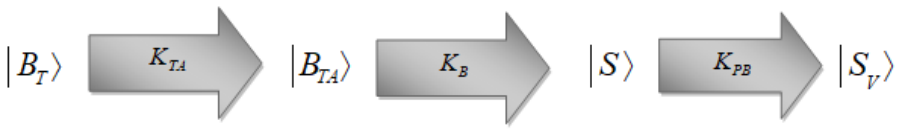

FIGURE 1. Describes the each phase of the proposed scheme

4. CORRECTNESS OF THE PROPOSED SCHEME

The correctness of this scheme is immediately described by inspection. In the initial phase, TC generate a quantum state $|B_T\rangle$ with K_{TA} and K_{TB}. In the same process, Alice obtains $|B_{TA}\rangle$ by using unitary transformation. In the next step, we can find:
By equations (3.1), (3.2) and Pauli operators, we can get

$$\lambda_i = r_i \oplus t_i \tag{4.1}$$

It is easy to verify $|f(v)\rangle = |f(v^*)\rangle$.

5. SECURITY ANALYSIS

In this section, we will analyze how secure are our schemes. Suppose the attacker known as the signature and catch the particles in the quantum channel. So we consider the possible attacks of the proposed schemes.

4.1. Ancillary attack: The proposed scheme resists the ancillary attack. In the initial phase, Eve measure ancillary particles and entangles with the EPR pairs that TC distributed to Alice and Bob. Eve try to obtain any information about Alice's message and Bob's signature by computing the ancillary particles. In this scheme, Alice and Bob not operate unitary operation, so it can be secure of ancillary attack.s

4.2. Intercept-and-resend attack: Since the proposed schemes use particles to protect from any forgery by an Eve, therefore our scheme can oppose intercept-and-resend attack. In this scheme, all the quantum state message transfer through a proper quantum channel, which in encrypted by OTP algorithm. Because of one time pad algorithm secret key are unconditionally secure, Eve cannot obtain in any message, the probability is very low that Eve wants to resend a message and cannot be locate only by approximation.

6. Conclusion

In the proposed scheme, we analyze a quantum proxy signature scheme based on quantum one-way function and Bell states. Quantum one-way function can be computed polynomial time but are hard to invert in polynomial time. It is easy to compute on every input but hard to invert. The quantum key distribution, OWF and one-time-pad encryption algorithm guarantee the unconditional security of this scheme.

References

[1] C. H. Bennett, C. Brassard: *Quantum Cryptography: Public Key Distribution and Coin Tossing*, In Proceedings of IEEE Int. Conf. Comp. Syst. Sign. Proces., **5** (1984), 175–179.

[2] D. Gottesman, I. Chuang: *Quantum Digital Signature*, arXiv:0105032, 2001.

[3] H. Ong, C. P. Schnorr: *Fast Signature Generation with a Fiat-Shamir-Like Scheme*, Proc. Int. Conf. Eurocrpt. Aarhus, Denmark, **2** (1990), 432–440.

[4] S. A. Brands: *Untraceable Off-Line Cash in Wallets with Observers*, Proc. Int. Conf. Crypto., New York, NY, USA, **5** (2017), 302–318.

[5] Y. G. Yang: *Multi-proxy Quantum Group Signature Scheme with Threshold Shared Verification*, Chin. Phys. B, **17** (2008), 415–417.

[6] T. Y. Wang, Z. L. Wei: *One-time Proxy Signature Based on Quantum Cryptography*, Quantum Inf. Process., **11** (2012), 455–417.

[7] M. Kumar, P. Gupta: *An Efficient and Authentication Signcryption Scheme Based on Elliptic Curves*, Matematika, **35**(1) (2019), 1–11.

Department of Mathematics and Statistics, Gurukula Kangri Vishwavidyalaya
Haridwar-249404, Uttarakhand, India
E-mail address: sdmkg1@gmail.com

Department of Mathematics and Statistics, Gurukula Kangri Vishwavidyalaya
Haridwar-249404, Uttarakhand, India
E-mail address: sudhanshusdubey@gmail.com

Department of Mathematics, Mandsaur University
Mandsaur- 458001, Madhya Pradesh, India
E-mail address: pratikgupta1810@gmail.com

Department of Mathematics, Jaipur national University
Jaipur- 302017, Rajasthan, India
E-mail address: yogeshmaths81@gmail.com