QUANTUM DIGITAL SIGNATURE BASED ON QUANTUM ONE-WAY FUNCTIONS

Xin Lü
State Key Laboratory of Information Security
Graduate School of Chinese Academy of Sciences
Beijing, 100039,China
email: lxdcs@hotmail.com

Deng-Guo Feng
State Key Laboratory of Information Security
Software Institute of Chinese Academy of Sciences
Beijing, 100080,China

ABSTRACT

A quantum digital signature scheme based on quantum mechanics is proposed in this paper. The security of the protocol relies on the existence of quantum one-way functions by fundamental quantum principles. Our protocol involves a so-called arbitrator who validates and authenticates the signed message. This scheme uses public quantum keys publicized by the signatory to verify the validity of the signature and uses quantum one-time pad to ensure the security of quantum information on channel. To guarantee the authenticity of the transmitted quantum states, a family of quantum stabilizer code is employed. The proposed scheme presents a novel method to construct secure quantum signature systems for future secure communications.

KEY WORDS

Information security; Digital signature; Quantum cryptography; Error correction code; Quantum one-way functions

1 Introduction

Quantum cryptography aims at providing information security that relies on the main properties of quantum mechanics. The most successful topic of quantum cryptography is quantum key distribution (QKD), which was firstly invented by Bennett and Brassard in 1984 [1]. QKD is believed to be the first practical quantum information processor and its unconditional security has been proven [2, 3].

Other than QKD, quantum cryptography protocols are widely studied in these years, such as quantum digital signature and quantum message authentication. Digital signature is a main task in modern cryptography and is widely used in today's communication systems. Digital signature cares about the "authenticity" data on channel [4]. Informally, an unforgeable signature scheme requires that each user be able to efficiently generate his(her) own signature and verify the validity of another user's signature on a specific document, and no one be able to efficiently generate the signatures of other users to documents that those users didn't sign.

Gottesman and Chuang proposed a quantum digital system [5] based on quantum mechanics, and claimed that the scheme was absolutely secure, even against an adversary having unlimited computational resources. The scheme, however, can only sign classical bits string and can't deal with general quantum superposition states. Zeng presented an arbitrated quantum signature scheme, the security of which is due to the correlation of the GHZ triplet states and utilization of quantum one-time pad [6].In an arbitrated signature scheme, all communications involve a so called arbitrator who has access to the contents of the messages [7]. The security of most arbitrated signature schemes depends heavily on the trustworthiness of the arbitrators. Zeng's protocol signs quantum messages which are known to the signatory. It seems impossible to sign a general unknown quantum state [5, 6, 8].

In this paper, we present a novel arbitrated quantum digital signature scheme which can sign general quantum states, the security of which is based on a family of quantum one-way functions by quantum information theory. The rest of the article is arranged as follows.

Section 2 introduces some definitions and preliminaries we will use in the article. Section 3 describes the proposed quantum signature scheme. The security is considered in Section 4. Section 5 gives discussions and conclusions.

2 Preliminaries

2.1 Quantum one-way function

This section introduces a class of quantum one-way functions based on the fundamental principles of quantum mechanics, which was proposed by Gottesman and Chuang [5] and the definitions are presented as below.

Definition 1 (quantum one-way function) *A function $f : |x\rangle_{n_1} \mapsto |f(x)\rangle_{n_2}$ where $x \in F_2^{n_1}$ and $n_1 \gg n_2$, is called a quantum one-way function under physical mechanics if*

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

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

What should be pointed out for the above definition is that the condition $n_1 \gg n_2$ is necessary. By Holevo's theorem [10], no more than n classical bits of information can be obtained by measuring n qubits quantum states. Several means to construct quantum one-way function were introduced by Gottesman and Chuang [5] and here we choose the quantum fingerprinting function [11] for the candidate. The quantum fingerprinting function of a bit string $u \in F_2^w$ is

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

where $E : \{0,1\}^w \rightarrow \{0,1\}^m$ is a family of error correcting code with fixed $c > 1, 0 < \delta < 1$ and $m = cw$. $E_l(u)$ denotes the lth bit of $E(u)$. The distance between distinct code words $E(u_1)$ and $E(u_2)$ is at least $(1-\delta)m$. Since two distinct code words can be equal in at most δm positions, for any $u_1 \neq u_2$ we have $\langle f(u_1)|f(u_2)\rangle \leq \delta m/m = \delta$. Here $f(u)$ can be regarded as a class of quantum one-way functions, which are easy to compute, but difficult to reverse.

2.2 Quantum stabilizer codes

Quantum error correction code (QECC) is a way of encoding quantum data (having m qubits) into n qubits (m<n), which protects quantum states against the effects of noise. Quantum stabilizer code is an important class of QECC and has been used to the other subject of quantum information, such as quantum cryptography [10].

The Pauli operators $\{\pm I, \pm\sigma_x, \pm\sigma_y, \pm\sigma_z\}$ constitute a group of order 8. The n-fold tensor products of single qubit Pauli operators also form a group $G_n = \pm\{I, \pm\sigma_x, \pm\sigma_y, \pm\sigma_z\}$, of order 2^{2n+1}. We refer to G_n as the n-qubit Pauli group. Let S denote an abelian subgroup of the n-qubit Pauli group G_n. Then the stabilizer codes $H_S \subseteq H_{2^{2n}}$ satisfy,

$$|\psi\rangle \in H_S, iff \ \ M|\psi\rangle = |\psi\rangle \ \ for \ \ all \ \ M \in S \qquad (2)$$

The group S is called the stabilizer of the code, since it preserves all of the codewords.

For stabilizer codes [[n, k, d]], the generators M_i and the errors E_a, write

$$M_i E_a = (-1)^{S_{ia}} E_a M_i, i = 1, \cdots, n-k \qquad (3)$$

The $s_{ia}'s$ constitute a syndrome for the error E_a, as $(-1)^{S_{ia}}$ will be the result of measuring M_i if the error E_a happens. For a nondegenerate code, $s_{ia}'s$ will be distinct for all $E_a \in \varepsilon$, so that measuring the $n-k$ stabilizer generators will diagnose the error completely.

3 The Proposed Protocol

3.1 Security requirements

The proposed scheme is a cryptographic protocol involving three entities: a signatory Alice, a receiver Bob, and an arbitrator Trent who authenticates and validates the signed message. The security of the signature scheme depends much on the trustworthiness of the arbitrator who has access to the contents of the messages. The quantum digital signature discussed in this article should meet the following security conditions:

1. Each user (Alice) can efficiently generate her own signature on messages of his choice;
2. A receiver Bob can efficiently verify whether a given string is a signature of another user's on specific message with Trent's help;
3. The signatory can't disavow the message that she has signed;
4. It is infeasible to produce signatures of other users' messages they haven't signed.

3.2 The protocol

3.2.1 Key generation

1. Key distribution. Alice, Bob and Trent agree on some random bits K_{AT}, K_{AB} and K_{TB} as their private keys. K_{AT} is shared between Alice and Trent, K_{AB} is shared between Alice and Bob and K_{TB} between Trent and Bob .

   To ensure that the scheme is unconditionally secure, the keys can be generated using quantum key distribution protocols, such as BB84 or EPR protocol[1, 10].

2. Signature key generation. Alice generates $2k$ random secret strings $u_{i,j} \in F_2^w$ and computes

$$|y_{i,j}\rangle = |f(u_{i,j})\rangle, 1 \leq i \leq 2n, j \in \{0,1\} \quad (4)$$

   Here $f : |x\rangle \mapsto |f(x)\rangle$ is a class of quantum one-way functions introduced in section 2. Alice generates $4n$ key pairs of $\{u_{i,j}, |y_{i,j}\rangle\}_{j\in\{0,1\}}^{1\leq i\leq 2n}$ and then publicly announces $\{|y_{i,j}\rangle\}_{j\in\{0,1\}}^{1\leq i\leq 2n}$ as her public key and keeps $\{u_{i,j}\}_{j\in\{0,1\}}^{1\leq i\leq 2n}$ as her private key.

3.2.2 Signature

1. Suppose that Alice has a quantum state $|\psi\rangle \in \mathcal{H}_{2^n}$ and wants to send it to Bob. Alice randomly selects bits strings $x \in F_2^{2n}$, k for the stabilizer codes $\{Q_k\}$ and s. She q-encrypts $|\psi\rangle$ as ρ using x. Alice encodes ρ according to Q_k with syndromes s and obtains π.

2. Alice computes

$$X = (x_{pre_{|s|}} \oplus y)||(x_{suf_{2n-|s|}})^1 \quad (5)$$

   and generates four copies of $X's$ signature $|\Sigma_K(X)\rangle$ according to her key $K \in \{u_{i,j}, |y_{i,j}\rangle | 1 \leq i \leq 2n, j \in \{0,1\}\}$

$$|\Sigma_K(X)\rangle = |y_{1,X_1} \otimes \ldots \otimes y_{2n,X_{2n}}\rangle$$
$$= |a_1 \otimes \ldots \otimes a_{2n}\rangle = |a\rangle \quad (6)$$

   Alice sends π and two copies of $|\Sigma_K(X)\rangle$ to Bob. At the same time, she encrypts $\{s, k, x\}$ as C_1 using K_{AT} [2] and sends C_1 and two copies of $|\Sigma_K(X)\rangle$ to Trent. We assume that each setting up of a protocol has a unique sequence number.

3.2.3 Verification

1. Trent receives C_1' and two copies of $|\Sigma_K'(X)\rangle = |a'\rangle$. Trent checks whether these two copies of

[1] Supposing $s < 2n$ in the algorithm. Here, $x_{pre_{|y|}}$ denotes the first $|y|$ bits of x and $x_{suf_{2n-|y|}}$ denotes the last $2n - |y|$ bits of x, $a \oplus b$ means the bit-by-bit XOR of the strings a and b, namely $a \oplus b = a_1 \oplus b_1, \cdots, a_m \oplus b_m$. The symbol "$||''$" means concatenation of two binary strings.

[2] In this algorithm, we select classical one-time-pad to encrypt classical message to ensure the unconditional security.

$|\Sigma'_K(x)\rangle$ he recieved are equivalent by performing a quantum swap test circuit (QSTC [11]). If any one of $|a'_i\rangle$'s fails the test, Trent aborts the protocol. Trent decrypts C'_1 using his secure key K_{AT} and obtains $\{s_T, k_T, x_T\}$. He computes $|\Sigma_K(X)_{(T)}\rangle$ according to x_T and Alice's public keys. Trent compares $|\Sigma_K(X)_{(T)}\rangle = |a\rangle_T$ to $|\Sigma'_K(X)\rangle$. If any one of them fails the test, Trent aborts the protocol. Trent encrypts $\{k_T, x_T\}$ as C_2 using K_{TB} and sends the ciphertext to Bob.

The comparison of two quantum states is less straightforward than in the classical case because of the statistical properties of quantum measurements. Another serious problem is that quantum measurements usually introduce a noneligible disturbance of the measured state. Here, we use the quantum swap test circuit (QSTC) proposed in [11] to compare whether $|a_i\rangle_T$ and $|a'_i\rangle$ are equivalent or not. QSTC is a comparison strategy with one-sided error probability $(1+\delta^2/2)$, and each pair of the compared qubits has an inner product with an absolute value at most δ. Because there are $2n$ sets of qubits to be compared, the error probability of the test can be reduced to $(\frac{1+\delta^2}{2})^{2n}$, where $\langle f_i|f_j\rangle \leq \delta$ with $i \neq j$, and n is the security parameter. Let the number of the incorrect keys be e_j, Bob rejects it as invalid signature if $e_j > cM$. Here c is a threshold for rejection and acceptance in the protocol.

2. Bob has received Alice's information $[\pi', |\Sigma''_K(X)\rangle = |a''\rangle]$, π' and Trent's message C'_2 now. He deciphers C'_2 as $\{k_B, x_B\}$ and computes X_B according to Eq.(5). He measures the syndrome s_B of the stabilizer code Q_k on π' and decodes the qubits as ρ'. He encrypts s_B as C_3 using parts of K_{TB} and sends it to Trent.

3. Trent encrypts s_T as C_4 using parts of K_{TB} and sends it to Bob.

4. Bob deciphers C'_4 and obtains s_T. He compares s_B to s_T and aborts if any error is detected. Bob checks whether these two copies of $|\Sigma''_K(X)\rangle$ are equivalent by performing the QSTC. He computes quantum states $|\Sigma(X)\rangle_B = |a\rangle_B$ using X_B and Alice's public keys $\{|y_{i,j}\rangle\}_{j\in\{0,1\}}^{1\leq i\leq 2n}$. He verifies Alice's signature according to

$$V_K(X_B, |\Sigma'_K(X)\rangle) = True \Leftrightarrow \{|a'_i\rangle$$

$$= |y_{i,X_i}\rangle = |a''_i\rangle_B\}_{1\leq i\leq 2n} \quad (7)$$

Bob q-decrypts ρ' as $|\psi'\rangle$ according to x_B.

4 Security Analysis

4.1 Correctness

Theorem 1 (Correctness) *Suppose all the entities involved in the scheme follow the protocol, then Eq. (7) holds.*

Proof. The correctness of the scheme can be seen by inspection. In the absence of intervention, Trent will obtain Alice's key s, x, k and her signature of X. Trent verifies the signature and sends x, k secretly to Bob. Bob can successfully decode and decipher the quantum states and verify Alice's signature. Because Alice signs her message according to Eq. (6), it's easy to verify that Eq. (7) holds.

4.2 Security against repudiation

Alice can't deny her signature. When Alice disavows her signature, Bob will resort to Trent. Bob sends one copy of the signature $|\Sigma''_K(X)\rangle$ to Trent. Trent compares s_B and $|\Sigma''_K(X)\rangle$ with s_T and his kept copy of signature $|\Sigma'_K(X)\rangle$ Alice has sent to him. If all these pass the test, Trent reveals that Alice is cheating because $|\Sigma_K(X)\rangle$ contains Alice's signature on her private keys x and s. Otherwise, Trent concludes that the signature has been forged by Bob or other attackers.

4.3 Security against forgery

Theorem 2 *Other entities forge Alice's signature with a successful probability at most* $2^{-[(w-t\lceil log_2 m\rceil)+2n]}$.

Proof. Considering that an adversary (Eve or Bob) controls the communication channels connecting Alice, Trent and Bob and wants to forger Alice's signature. Here we present two strategies that the attack Eve (Bob) can apply.

1. One is that she tries to alter the signed quantum states. Eve intercepts $[\pi', |\Sigma'_K(X)\rangle]$. She keeps π' and selects a random key x_E to encrypt another quantum states $|\phi\rangle$ as τ and sends $[\tau, |\Sigma' K(X)\rangle]$ to Bob. Because Eve knows nothing about the stabilizer code $\{Q_k\}$ and syndrome s, her cheating will be detected by Bob in the fourth step of the verification phase when he compares the syndrome y to y'.

2. The second strategy is that the attacker tries to recover Alice's private keys and generates a "legal" signature. Because she knows nothing about Alice's private keys x, y, k, K_{AT} and $\{u_{i,j}\}_{j\in\{0,1\}}^{1\leq i\leq 2n}$. She can't compute x, y, k from the mixed state π'. According to Holevo's theorem [10], Eve can obtain at most $t\lceil log_2 m\rceil$ bits of classical information about one of Alice's signature key $\{u_{i,j}\}$ from Alice's public key. Here, t is a small natural number and we let $c = 4$ in our scheme. Since she lacks $w - t\lceil log_2 m\rceil$ bits of information about any private key which Alice hasn't revealed, she will only guess correctly at most $2^{-[w-t\lceil log_2 m\rceil]}$ of it. Therefore, the attacker can forger Alice's signature only with a successful probability less than $2^{-[(w-t\lceil log_2 m\rceil)+2n]}$.

5 Concluding Remarks

Designing quantum digital signature protocol is not trivial because of several fundamental properties of quantum message.

The first and the most important property of quantum information is the no-clone theorem, which forbids the unknown qubits reproduction. For digital signature, how can we verify the signature is indeed the signature on a specific state without generating copies of the original message?

The second is the probability and irreversibility properties of quantum measurement. That brings much troubles to decide whether a state is a legal signature without changing that state.

The last property of secure quantum signature scheme is that it is also a secure encryption scheme, which has been shown by Barnum $et\ al.$ in literature [8].

In this article, we investigate how to span these obstacles and present a quantum digital signature scheme. The security of the scheme relies on the existence of a family of quantum one-way functions by quantum principles. The authenticity of the quantum information is obtained by quantum error correction codes and security of the quantum information on channel is ensured by quantum one-time pad.

Acknowledgments

This work was supported by the Natural Science Foundation of China under Grant No.60273027, the National Grand Fundamental Research 973 Program of China under Grant No. G1999035802 and the National Science Foundation of China for Distinguished Young Scholars under Grant No.60025205.

References

[1] C.H. Bennett and G. Brassard , "Quantum Cryptography: Public Key Distribution and Coin Tossing", In Proceedings of IEEE International Conference on Computers Systems and Signal Processing, Bangalore, India, pp. 175-179, December 1984.

[2] D. Mayers,"Unconditional security in quantum cryptography",Journal of the ACM, Vol. 48 , No. 3, pp. 351-406, May 2001.

[3] P. Shor , J. Priskill, Simple Proof of Security of the BB84 Quantum Key Distribution Protocol, Physical Review Letters, Vol. 85, pp. 441 - 444, 2000.

[4] Goldreich O., Foundations of Cryptography, Cambridge university press, 2001.

[5] D. Gottesman,I. Chuang, "Quantum digital signatures", Technical report, available at http://arxiv.org/abs/quant-ph/0105032, 2001.

[6] G. Zeng and K. Christoph, "An arbitrated quantum signature scheme", Physical review A, Vol. 65, pp. 042312, 2002.

[7] H. Meijer, and S. G. Akl, "Digital Signature Scheme for Computer Communication Networks", In Advances in Cryptography: Crypto 81, pp. 65-70, Santa Barbara, August 1981.

[8] Barnum C, Gottesman D, Smith A $et\ al.$ "Authentication of Quantum Messages", In Proceedings of 43rd Annual IEEE Symposium on the Foundations of Computer Science,Vancouver,pp. 449-458, Canada, November 2002.

[9] I. Jex, E. Andersson and A. Chefles, "Comparing the states of many quantum systems", Technical report, available at http://arxiv.org/abs/quant-ph/0305120, 2003.

[10] M. Nielson , I. Chuang, Quantum computation and quantum Information, Cambridge university press2000.

[11] H. Buhrman, R. Cleve, J. Watrous and R. Wolf, "Quantum fingerprinting", Physical Review Letters,Vol. 87, pp. 167902-167904, 2001.

[12] P. Boykin, V. Roychowdury, "Optimal encryption of quantum bits", Physical review A, Vol. 67, pp. 0423171-0423175, 2003.