2009 Sixth International Conference on Information Technology: New Generations

# Security Analysis of One Quantum Digital Signature Scheme

Zhengjun Cao[1,2] Olivier Markowitch[1]
1 Departement D'informatique, Université Libre de Bruxelles, Belgium
2 Department of Mathematics, Shanghai University, China
zhencao@ulb.ac.be

## Abstract

*We point out that the quantum digital signature scheme proposed in ICACT 2005 has three problems. According to the original description of the scheme, we find: (1) the quantum one-way function is not specified clearly; (2) the signer Alice does not use her private key in the signing process; (3) both the signing and the verification can not work well.*

## 1 Introduction

Digital signatures are very important to modern electronic commerce. Rivest [5] said that "they may prove to be one of the most fundamental and useful inventions of modern cryptography." Digital signatures are equivalent to traditional handwritten signatures in many respects; properly implemented digital signatures are more difficult to forge than the handwritten type. A digital signature scheme typically consists of three algorithms: (1) A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key. (2) A signing algorithm which, given a message and a private key, produces a signature. (3) A verifying algorithm which given a message, public key and a signature, either accepts or rejects.

Two main properties are required for a digital signature scheme. First, a signature generated from a fixed message and fixed private key should verify on that message and the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party who does not possess the private key.

The security of common public key digital signature schemes depends on the inability of a forger to solve certain difficult mathematical problems, such as factoring large numbers [6]. But these common signature are not secure against a quantum computer attack. In order to resist powerful quantum cheating strategies, Gottesman and Chuang [2] proposed a quantum digital signature in 2001. The scheme has some drawbacks: (1) the public keys can only be used once unlike more sophisticated digital signature schemes; (2) it is not efficient because it signs the message in the mode of bit by bit. In 2002, Zeng and Keitel [7] proposed an arbitrated quantum signature scheme. The scheme uses the correlation of Green-Horne-Zeilinger states [3], various qubit operations, and a symmetrical quantum key cryptosystem. Its security depends heavily on the trustworthiness of the arbitrator.

In ICACT 2005, Lü and Feng [4] put forward a quantum digital signature. The author claim that its security relies on the existence of quantum one-way functions. In this note, we point out that the quantum digital signature scheme has three problems. According to the original description of the scheme, we find: (1) the quantum one-way function is not specified clearly; (2) the signer Alice does not use her private key in the signing process; (3) both the signing and the verification can not work well.

## 2 Review of the quantum digital signature scheme

The proposed scheme is a cryptographic protocol involving three entities: a signer 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 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 signer can't disavow the message that she has signed.
4. It is infeasible to produce signatures of other users' messages they haven't signed.

978-0-7695-3596-8/09 $25.00 © 2009 IEEE
DOI 10.1109/ITNG.2009.38

### 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.

2. Signature key generation. Alice generates $4n$ random secret strings $u_{i,j} \in F_2^{2n}$ and computes

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

Here $f : |x\rangle \mapsto |f(x)\rangle$ is a quantum one-way function, which is specified as

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

where $E : \{0,1\}^{2n} \to \{0,1\}^m$ is a family of error correcting code with fixed $c > 1, 0 < \delta < 1$ and $m = 2cn$. $E_l(u)$ denotes the *lth* bit of $E(u)$. Alice generates $4n$ key pairs of $\{u_{i,j}, |y_{i,j}\rangle\}_{j\in\{0,1\}}^{1\le i\le 2n}$ and then publicly announces $\{|y_{i,j}\rangle\}_{j\in\{0,1\}}^{1\le i\le 2n}$ as her public key and keeps $\{u_{i,j}\}_{j\in\{0,1\}}^{1\le i\le 2n}$ as her private key.

### 2.2 Signing

1. Suppose Alice has a quantum state $|\psi\rangle \in H_{2^n}$ 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 $\rho$ using $x$. Alice encodes $\rho$ according to $\{Q_k\}$ with syndromes $s$ and obtains $\pi$.

2. Alice computes

$$X = (x_{pre_{|s|}} \oplus y)||(x_{suf_{2n-|s|}}) \qquad (2)$$

where $x_{pre_{|s|}}$ denotes the first $|s|$ bits of $x$ and $x_{suf_{2n-|s|}}$ denotes the last $2n - |s|$ 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.

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

$$\begin{aligned} |\sum_K(X)\rangle &= |y_{1,X_1} \otimes \cdots \otimes y_{2n,X_{2n}}\rangle \\ &= |a_1 \otimes \cdot \otimes a_{2n}\rangle = |a\rangle \end{aligned} \qquad (3)$$

Alice sends $\pi$ and two copies of $|\sum_K(X)\rangle$ to Bob. At the same time, she encrypts $\{s, k, x\}$ as $C_1$ using $K_{AT}$ and sends $C_1$ and two copies of $|\sum_K(X)\rangle$ to Trent.

### 2.3 Verification

1. Trent receives $C_1'$ and two copies of $|\sum_K'(X)\rangle = |a'\rangle$. Trent checks whether these two copies of $|\sum_K'(x)\rangle$ he recieved are equivalent by performing a quantum swap test circuit. 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 $|\sum_K(X)_{(T)}\rangle$ according to $x_T$ and Alice's public keys. Trent compares $|\sum_K(X)_{(T)}\rangle = |a\rangle_T$ to $|\sum_K'(X)\rangle$. 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.

2. Bob has received Alice's information $[\pi', |\sum_K''(X)\rangle = |a''\rangle], \pi'$ and Trent's message $C_2'$ now. **He deciphers $C_2'$ as $\{k_B, x_B\}$ and computes $X_B$ according to Eq.(2)**. He measures the syndrome $s_B$ of the stabilizer code $Q_k$ on $\pi'$ and decodes the qubits as $\rho'$. 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 $|\sum_K''(X)\rangle$ are equivalent by performing the QSTC. He computes quantum states $|\sum(X)\rangle_B = |a\rangle_B$ using $X_B$ and Alice's public keys $\{|y_{i,j}\rangle\}_{j\in\{0,1\}}^{1\le i\le 2n}$. He verifies Alice's signature according to

$$\begin{aligned} & V_K(X_B, |\sum_K{}'(X)\rangle) = True \\ \Leftrightarrow \quad & \{|a_i'\rangle = |y_{i,X_i}\rangle = |a_i''\rangle_B\}_{1\le i\le 2n} \end{aligned}$$

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

## 3 Analysis

Like the Zeng-Keitle quantum signature, the scheme introduces an entity Arbitrator. But it removes the requirement for the correlation of Green-Horne-Zeilinger states. Whereas, it introduces a quantum one-way function $f$. Regretfully, we find it has three problems according to its original description.

### 3.1 The quantum one-way function is not specified clearly

By the representation of Eq.(1) and its context, we find that the authors do not specify the quantum states

$$|1\rangle, \cdots, |m\rangle$$

Thus, one can not complete the calculation of the function $|f(u)\rangle$. To fix it, we can take a base of $H_{2^m}$ as the states.

### 3.2 The signer Alice does not use her private key in the signing process

By the key generation process, we know that the signer's public key is

$$\{|y_{i,j}\rangle\}_{j\in\{0,1\}}^{1\leq i\leq 2n}$$

and its corresponding private key is

$$\{u_{i,j}\}_{j\in\{0,1\}}^{1\leq i\leq 2n}$$

Combining the signing process, we find that the signer Alice does not use her private key $\{u_{i,j}\}_{j\in\{0,1\}}^{1\leq i\leq 2n}$. It's an apparent error.

One can argue that the $y$ in the equation

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

should be replaced by the private key. But it is impossible because Bob has to recover $X$ in the verification process (see the boldface sentence in step 2 of the verification).

### 3.3 Both the signing and the verification can not work well

In the step 2 of the signing process, Alice has to compute

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

But the authors do not specify the string $y$ through out the paper. By its context, one can argue that the string $y$ should be the string $s$. Regretfully, if that, the private key $\{u_{i,j}\}_{j\in\{0,1\}}^{1\leq i\leq 2n}$ remains unused. Moreover, the authors have specified that the $s$ is the syndrome of the the stabilizer code $Q_k$.

Likewise, in the step 2 of the verification process, Bob cannot complete the calculation of $X_B$ though he has $k_B, x_B, \pi$ and two copies of $|\sum_K(X)\rangle$ obtained from Trent and Alive, respectively.

Incidentally, the data $C_3$ sent by Bob is not used in the later steps. The purpose of calculation of $C_3$ is obscure.

## 4 Conclusion

In this note, we analyze the quantum digital signature scheme put forward in ICACT 2005. To the best of our knowledge, it seems difficult to fix and improve the scheme in the original model. By the way, in 2002, Barnum et al [1] pointed out that quantum cryptography cannot be used to design signature schemes though it is possible to use quantum algorithm in conventional signature schemes.

## 5 Acknowledgement

Supported by Cryptasc Project (Institute for the encouragement of Scientific Research and Innovation of Brussels), National Natural Science Foundation of China (Project 60873227), Innovation Program of Shanghai Municipal Education Commission, Shanghai Leading Academic Discipline Project (J50101), Key Disciplines of Shanghai Municipality (S30104).

## References

[1] H. Barnum, C. Crepeau, D. Gottesman, A. Smith, A. Tapp, Authentication of quantum messages, 43rd Annual IEEE Symposium on Foundations of Computer Science FOCS, 2002, pp. 449-458

[2] D. Gottesman, I. Chuang, Quantum digital signatures, http://arxiv.org/abs/quant-ph/0105032, 2001

[3] D. Greenberger, M.A. Horne, A. Shimony, and A. Zeilinger, Am. J. Phys. 58, 1990, 1131

[4] X. Lü, D. Feng, Quantum digital signature based on quantum one-way functions, Advanced Communication Technology 2005, ICACT 2005. 514-517 (It is also accessible at http://arxiv:quant-ph/04030462)

[5] R. Rivest, Cryptography, vol.1. Elsevier, 1990, pp. 717-755

[6] R. Rivest, A. Shamir, L. Adleman, A method of obtaining digital signatures and public-key cryptosystems. Comm. Assoc. Comput. Mach. 21 (1978), 120-126

[7] G. Zeng, C. Keitel, Arbitrated quantum signature scheme, Physical Review A, vol 65, 2002, 042312