A Note On Gottesman-Chuang Quantum Signature Scheme

Zhengjun Cao

Department of Mathematics, Shanghai University, China

caozhj@yahoo.cn

Abstract In 2001, Gottesman and Chuang proposed a quantum signature scheme. Unlike classical signature schemes, the public keys in the scheme can only be used once. The authors claim that the scheme is somewhat cumbersome but it serves as a good model and suggests novel research directions for the field of quantum cryptography. In this note, we remark that the Gottesman-Chuang quantum signature scheme is so commonplace and cumbersome that it can not suggest the potential for quantum public key cryptography. The authors ignore an ultimate fact, namely, the cost to grantee the authenticity of a user's public key is expensive in the scenario of Public Key Infrastructure. It entails that a user's public key should be repeatedly usable in the life duration.

Keywords quantum signature, creditability, durability

1 Introduction

A digital signature of a message is a number dependent on the content of the message being signed and on some secret known only to the signer. Signatures must be verifiable; if a dispute arises as to whether a party signed a document, an unbiased third party should be able to resolve the matter equitably, without requiring access to the signer's secret information [10]. Digital signatures have many applications including authentication, data integrity, and non-repudiation.

In the scenario of Public Key Infrastructure (PKI), authenticity of public keys must be guaranteed. To bind the identity of an entity to its public key, it is usual to introduce a trusted third party (TTP). The TTP is generally assumed to be honest and fair but it does not have access to the secret or private keys of users [10]. Before creating a public-key certificate for Alice, the TTP must take appropriate measures to verify the identity of Alice and the fact that the public key to be certificated actually belongs to Alice. To this end, it is usual that *Alice*

has to appear before the TTP with a conventional passport as proof of identity, and submit her public key along with evidence that she knows the corresponding private key.

Explicitly, a user's public key has to satisfy:

(1) Creditability. It should be authenticated by a certification authority.

(2) Accessibility. It should be easily accessible to any user.

(3) Durability. It should be repeatedly usable in the life duration because the cost to generate and distribute a user's public key is expensive.

In 2001, Gottesman and Chuang [5] proposed a quantum digital signature scheme. To sign a classical bit b, the signer has to unveil the secret keys $k_b^1, k_b^2, \cdots, k_b^j$, where $k_b^i, 1 \leq i \leq j$ are L-bit strings, j, L are security parameters. The authors point out the scheme is somewhat cumbersome but the underlying principles suggest novel research directions for the field of quantum cryptography.

In this note, we investigate the Gottesman-Chuang quantum signature scheme, and remark that the scheme is so commonplace and cumbersome that it can not suggest the potential for quantum public key cryptography. The authors ignore an ultimate fact, namely, the cost to grantee the authenticity of a user's public key is expensive in the scenario of PKI. It entails that a user's public key should be repeatedly usable in the life duration.

2 Review of Gottesman-Chuang quantum signature scheme

The Gottesman-Chuang quantum signature scheme [5] can be described as follows.

> [Setup] Set f be an appropriate quantum one-way function, and c, j, L be the security parameters. All participants in the protocol know how to implement the map $k \rightarrow |f_k\rangle$. Alice randomly chooses L-bit strings $k_0^i, k_1^i, 1 \leq i \leq j$. The strings will be Alice's private keys. The corresponding states $|f_{k_0^i}\rangle, |f_{k_1^i}\rangle, 1 \leq i \leq j$, will be Alice's public keys.
>
> [Signing] To sign a single-bit message b, Alice generates $(b, k_b^1, k_b^2, \cdots, k_b^j)$, and sends it over an insecure classical channel. Thus, Alice reveals the identity of half of her public keys. Alice also discards all used and unused private keys.
>
> [Verifying] The verifier checks each of the revealed public keys to verify that $k_b^i \rightarrow |f_{k_b^i}\rangle$. Count the number of incorrect keys and let this be s. Accept it as valid if $s \leq cj$.

3 Remarks on Gottesman-Chuang quantum signature scheme

3.1 On the accessibility of the signer's public key

In the classical case, we know, to distribute public keys is of comparatively low cost because any participant can extract other's authentic public key from a public directory.

In the quantum signature scheme the signer's public keys are quantum states $|f_{k_0^i}\rangle, |f_{k_1^i}\rangle, 1 \leq i \leq j$. To make sure that any verifier easily accesses to the signer's public keys, the authors [5] suggest a straightforward solution. It assumes the existence of a trusted key distribution center, which has authenticated links to all participants. Alice sends her public keys to the key distribution center, which performs swap tests between corresponding pairs of public keys. If any pair of public keys fails the swap test, the center concludes Alice is cheating; otherwise it forwards a copy of each public key to each recipient.

Apparently, the cost to distribute public keys (quantum states) in the solution is impressive because it requires that the key distribution center has authenticated links to all participants. Actually, if these authenticated links exist, the signer can directly send the signed message to the center via an authenticated channel, the center then forwards it to any recipient via a corresponding authenticated channel. In this case, the key distribution center acts as a creditable courier. There is no necessary for the recipient to certify the origin of the received message because of the presence of a courier.

3.2 On the durability of the signer's public key

The authors point out that the signer can only use his/her private keys once, as well as the corresponding public keys. Whether from the practical point of view or from the theoretical point of view, this is not applicable. The authors ignore an ultimate fact, namely, the cost to grantee the authenticity of a user's public key is expensive in the scenario of PKI. It entails that a user's public key should be repeatedly usable in the life duration.

3.3 On other schemes inspired by Gottesman-Chuang signature

In the past decade, there are some quantum signature schemes [9, 14] directly inspired by the Gottesman-Chuang quantum signature. We observe that the schemes are commonplace [2, 3]. We also observe that the quantum secret sharing schemes [6, 11, 8, 13, 12, 7] are not true secret sharing as claimed, instead they are quantum key distribution schemes [4]. Naturally, they are variations of BB84 scheme [1]. So far, no sophisticated cryptographic primitive has been fulfilled in quantum cryptography. The so-called quantum cryptography consists mainly of the quantum key agreement and quantum encryption.

4 Conclusion

The main difference between classical cryptography and quantum cryptography is that the former depends on pure mathematical principles while the later depends on quantum laws. They are based on two different intractabilities. One is mathematical intractability, the other is physical manipulating intractability. In some senses, the physical manipulating intractability is like the intractability of invisible inks in ancient times. In view of the difference, we think it is usual that some cryptographic primitives achieved in classical cryptography can not be acquired in quantum cryptography.

References

[1] C. Bennet and G. Brassard, *Proc. IEEE Int. Con. Computers, Systems, and Signal Processing* (IEEE Press, New York, 1984) pp. 175-179.

[2] ZJ Cao, O.Markowitch, Security Analysis of One Quantum Digital Signature Scheme, *6th International Conference on Information Technology: New Generations* (ITNG 2009), IEEE CS, pp. 1574-1576.

[3] ZJ Cao, O. Markowitch, A note on an arbitrated quantum signature scheme, *International Journal of Quantum Information*, Vol. 7 (6), 2009. World Scientific Publishing Co., pp. 1205-1209.

[4] ZJ Cao, O. Markowitch, A note on some quantum secret sharing schemes, *International Journal of Quantum Information*. World Scientific Publishing Co. (to appear)

[5] D. Gottesman and I. Chuang, Quantum Digital Signatures. arXiv:quant-ph-0105032

[6] S. Gaertner, C. Kurtsiefer, M. Bourennane and H. Weinfurter, *Phys. Rev. Lett.* **98** (2007) 020503.

[7] M. Hillery, V. Bužek and A. Berthiaume, *Phys. Rev. A* **59** (1999) 1829.

[8] L. Hsu and C. Li, *Phys. Rev. A* **71** (2005) 022321.

[9] X. Lü, DG Feng, Quantum digital signature based on quantum one-way functions, *Advanced Communication Technology 2005* (ICACT 2005). IEEE CS, pp. 514-517.

[10] A. Menezes, P. Oorschot and S. Vanstone, *Handbook of applied cryptography* (CRC Press, 1996)

[11] H. Takesue and K. Inoue, *Phys. Rev. A* **74** (2006) 012315.

[12] L. Xiao, G. Long, F. Deng and J. Pan, *Phys. Rev. A* **69** (2004) 052307.

[13] F. Yan and T. Gao, *Phys. Rev. A* **72** (2005) 012304.

[14] G. Zeng and C. Keitel, Arbitrated quantum-signature scheme, *Phys. Rev. A* **65** (2002) 042312.