International Journal of Quantum Information
Vol. 7, No. 6 (2009) 1205–1209

World Scientific
www.worldscientific.com

A NOTE ON AN ARBITRATED QUANTUM SIGNATURE SCHEME

ZHENGJUN CAO

Département d'informatique,
Université Libre de Bruxelles, Belgium

Department of Mathematics, Shanghai University, China
zhencao@ulb.ac.be

OLIVIER MARKOWITCH

Département d'informatique,
Université Libre de Bruxelles, Belgium
Olivier.Markowitch@ulb.ac.be

Received 18 May 2009

Zeng and Keitel proposed an arbitrated quantum signature scheme in 2002. Recently, Curty and Lütkenhaus pointed out that the protocol is not operationally specified. In a reply, Zeng gave more details of the scheme. The author also claimed that the scheme is suitable for unknown messages. In this letter, we remark that the invented scenario in the original scheme is artificial. This is because its security entirely depends on the presence of a trustworthy arbitrator. Moreover, the claim that the original scheme is suitable for unknown messages is not sound.

Keywords: Quantum digital signature; blind signature; arbitrator.

1. Introduction

A digital signature of a message is a number dependent on some secret known only to the signer, and, additionally, on the content of the message being signed.[1] Signatures must be verifiable; if a dispute arises as to whether a party signed a document (caused either by a lying signer trying to repudiate a signature it did create, or a fraudulent claimant), an unbiased third party should be able to resolve the matter equitably, without requiring access to the signer's secret information (private key). The importance of digital signatures to modern electronic commerce has become overwhelming such that Rivest[2] has written that "[they] may prove to be one of the most fundamental and useful inventions of modern cryptography."

The security of all public key digital signature schemes presently depends on the inability of a forger to solve certain difficult mathematical problems, such as factoring large numbers.[3] Regretfully, with a quantum computer, factoring becomes

tractable,[4] thus allowing signatures to be forged. In 2001, Gottesman and Chuang[5] proposed a quantum digital signature scheme whose security is based on fundamental principles of quantum physics. It allows a sender (Alice) to sign a message in such a way that the signature can be validated by a number of different people, and all will agree either that the message came from Alice or that it has been tampered with. The public keys in the scheme can be used only once, unlike more sophisticated digital signature schemes. So this simple protocol can serve as a model for a quantum scheme.

In 2002, Zeng and Keitel[6] proposed an arbitrated quantum signature scheme (AQSS for short). The suggested algorithm is implemented by a symmetrical quantum key cryptosystem and Greenberger–Horne–Zeilinger (GHZ)[7] triplet states. Its security relies on the availability of an arbitrator. In 2008, Curty and Lütkenhaus[8] pointed out that the protocol is not clearly operationally defined and several steps are ambiguous. Moreover, they argued that the security statements are incorrect. In the reply,[9] the author gave more detailed presentations and proofs of the scheme. He also claimed that the scheme is suitable for unknown messages.

In this letter, we revisit the scheme using a general technique and show that the invented scenario in Ref. 9 is artificial. The claim that the original scheme is suitable for unknown messages is not sound. This is because it is unreasonable that in a signature scheme, the final verifier cannot know the content of the signed message.

2. Review of the AQSS

We now briefly review the AQSS in Ref. 6. The following description follows that in Ref. 9.

Step I1: Obtaining keys K_a and K_b. The lengths of these keys depend on the chosen cryptographic algorithms in the signing and verifying phases.

Step I2: Distributing GHZ triplet states ψ.

Step S1: Alice presents a message state $|P\rangle = \{|p_1\rangle, |p_2\rangle, \ldots, |p_n\rangle\}$, with $|p_i\rangle = \alpha_i|0\rangle + \beta_i|1\rangle$.

Step S2: Alice generates $|R\rangle = \{|r_1\rangle, |r_2\rangle, \ldots, |r_n\rangle\}$.

Step S3: Alice obtains a four-particle state $|\phi\rangle_i$ via entangling the message state $|p_i\rangle$ and the GHZ state $|\psi\rangle$ according to Eq. (8) defined in Ref. 6.

Step S4: Alice executes a Bell measurement on $|\phi\rangle_i$ and obtains the results $\mathcal{M}_a$ expressed in Eq. (9) of Ref. 6.

Step S5: Alice creates the signature $|S\rangle$ of the message $|P\rangle$ via encrypting the Bell measurement results $\mathcal{M}_a$ and the generated $|R\rangle$ using a quantum symmetrical key cryptosystem, e.g. the quantum one-time pad algorithm.

Step S6: Alice sends $|P\rangle$ followed by the signature $|S\rangle$ to Bob.

Step V1: Bob measures his GHZ particles and obtains the results $\mathcal{M}_b$, then he encrypts $\mathcal{M}_b$, $|S\rangle$, and $|P\rangle$ with his key K_b to obtain y_b. After that, Bob sends y_b to the arbitrator.

Step V2: The arbitrator generates a verification parameter γ according to Eq. (13) of Ref. 6.
Step V3: The arbitrator sends his GHZ particles and the encrypted result $y_{tb} = K_b(\mathcal{M}_a, \mathcal{M}_b, \gamma, |S\rangle)$ to Bob.
Step V4: Bob obtains the arbitrator's GHZ particles. In addition, he obtains $\mathcal{M}_a, \mathcal{M}_b, |S\rangle$, and γ via decrypting the received y_{tb}.
Step V5: Bob performs the initial verification via the parameter γ.
Step V6: Bob performs the further verification via comparing $|P\rangle$ and $|P'\rangle$, where $|P'\rangle$ is obtained according to the correlation of the GHZ triplet state.

In 2008, Curty and Lütkenhaus[8] pointed out that it is unclear what the real advantages of this protocol are if all the parties know the state $|P\rangle$. In the reply,[9] the author acknowledged:

> The AQSS works for known messages even though it is not very useful or efficient, which was never claimed. The main aims of the AQSS are to present another application of the entanglement in cryptology and to prove the possibility of a quantum-signature. Based on the AQSS, we expected some further investigation of the quantum-signature.

Finally, the author stressed that the AQSS is, in principle, also suitable for the unknown message. He explained:

> The unknown message signature scheme is always called the "blind signature" in classic cryptology. The blind signature considers the cases where Alice or Bob, or even both Alice and Bob, do not know the content of the message to be signed and verified.

3. Analysis of the AQSS

We now revisit the AQSS by a general technique.

Step I1': Obtaining keys K_a and K_b.
Step S1': Alice presents a message state $|P\rangle$.
Step S2': Alice creates $|S\rangle = K_a(|P\rangle)$ and sends the signature $|S\rangle$ to Bob.
Step V1': Bob creates $y_b = K_b(|S\rangle)$ and sends y_b to the arbitrator.
Step V2': The arbitrator decrypts y_b with the key K_b to obtain $|S'\rangle$. He then decrypts $|S'\rangle$ with the key K_a to obtain $|P'\rangle$. If $|P'\rangle = |P\rangle$, he sets $\gamma = 1$. Otherwise, $\gamma = 0$. The arbitrator then creates $y_{tb} = K_b(|P'\rangle, \gamma)$ and sends y_{tb} to Bob.
Step V3': Bob decrypts y_{tb} with the key K_b to obtain $|P''\rangle, \gamma'$. He then checks if $\gamma' = 0$. If $\gamma' = 0$, he rejects it. If $\gamma' = 1$, he performs the further verification via checking if $|P\rangle = |P''\rangle$. If $|P\rangle = |P''\rangle$, he accepts it. Otherwise, he rejects it.

By the simplified protocol, we find that the requirement for the costly GHZ triplet-particle can be removed. Why can the simple protocol work well? This is because the arbitrator knows all private keys of the involved users. Actually, in the presence of an *absolutely* trustworthy arbitrator, almost cryptographic primitives become easy to achieve. The authors of Ref. 6 *misunderstand* the term "arbitrator" in cryptology. This leads them to a peculiar protocol (the arbitrator shares the keys K_a and K_b with Alice and Bob, respectively). As for the role of an arbitrator in cryptographic protocols, we refer to Ref. 10:

> An arbitrator is a disinterested third party trusted to complete a protocol. Trusted means that all people involved in the protocol accept what he says as true, what he does as correct, and that he will complete his part of the protocol. Arbitrators can help complete protocols between two mutually distrustful parties.

Notice that an arbitrated protocol does not necessarily mean that the arbitrator knows all private keys of the involved users.

In the reply,[9] the author claimed that the original scheme is suitable for unknown messages. We now argue that the claim is false. First, we claim that it is unreasonable that the final verifier cannot know the content of the signed message. In fact, the ultimate motive of a signature is to assure the authorship (or at least agreement with the contents) of the signed message to the final verifier. Second, the author[9] also misunderstands the scenario for a classical blind signature. In cryptography, a blind signature, as introduced by D. Chaum,[11] is a form of digital signature in which the content of a message is disguised (blinded) before it is signed. The resulting blind signature can be publicly verified against the original, unblinded message, in the manner of a regular digital signature. Therefore, we stress that the final verifier must know the content of the signed message.

4. Conclusion

In this letter, we have remarked that the Zeng–Keitel arbitrated quantum signature scheme is artificial. We have also clarified that in a blind signature scheme, the final verifier knows the content of the signed message.

Acknowledgments

We acknowledge the Cryptasc Project (Institute for the Encouragement of Scientific Research and Innovation of Brussels), the National Natural Science Foundation of China (Project 60873227), the Innovation Program of the Shanghai Municipal Education Commission and the Shanghai Leading Academic Discipline Project (S30104).

References

1. A. Menezes, P. Oorschot and S. Vanstone, *Handbook of Applied Cryptography* (CRC, 1996).
2. R. Rivest, *Cryptography*, Vol. 1 (Elsevier, 1990), pp. 717–755.
3. R. Rivest, A. Shamir and L. Adleman, *Comm. Assoc. Comput. Mach.* **21** (1978) 120–126.
4. P. Shor, *SIAM J. Comp.* **26**(5) (1997) 1484–1509.
5. D. Gottesman and I. Chuang, [arXiv:quant-ph-0105032].
6. G. Zeng and C. Keitel, Arbitrated quantum-signature scheme, *Phys. Rev. A* **65** (2002) 042312.
7. D. Greenberger, M. Horne and A. Zeilinger, *Bell's Theorem, Quantum Theory, and Conceptions of the Universe* (Kluwer Academic, Dordrecht, 1989).
8. M. Curty and N. Lütkenhaus, *Phys. Rev. A* **77** (2008) 046301.
9. G. Zeng, *Phys. Rev. A* **78** (2008) 016301.
10. B. Schneier, *Protocols, Algorithms, and Source Code in C* (Wiley, New York, 1996).
11. D. Chaum, *Advances in Cryptology — Crypto '82* (Springer-Verlag, Berlin, 1983), pp. 199–203.