A Simple Deniable Authentication Protocol Based on Quantum Key Distribution

Chen-hui JIN[1], Zhi-yong LI[2,*] and Su-hua LIAO[3]

[1] School of Medical Technology and Nursing, Shenzhen Polytechnic, Shenzhen 518055, China

[2] School of Digital Creation and Animation, Shenzhen Polytechnic, Shenzhen 518055, China

[3] Peking University Shenzhen Hospital, ShenZhen 518036

*Corresponding author

Keywords: Deniable, Authentication, Quantum key distribution.

Abstract. A deniable authentication protocol enables a receiver to identify the true source of given message, but not to prove the identity of the sender to a third party. This property is very useful for providing secure negotiation over the Internet. Recently, Shi et al. proposed a quantum deniable authentication protocol based on the property of unitary transformation and quantum one-way function. A trusted center (TC) is introduced in their protocol, and a much amount of quantum resources, such as entanglement, quantum memory and quantum one-way function, are required. In this paper, a deniable authentication protocol without a trust center is proposed based on the quantum key distribution (QKD). In the presented protocol, the QKD is used firstly to share a secret key between the sender and the receiver. Then, the shared key is used to identify the true source of sender's message by the receiver. Finally, the simulation based proof shows that the receiver cannot prove the identity of the sender to any third party.

Introduction

Privacy of communications has been one of the main objects of study in cryptography for centuries. Its goal is to establish secure channels between authenticated parties and prevent unauthorized parties from accessing secret or confidential information. Today, with the transfer of our personal, social, economic and political lives to digital form, privacy has become a much wider and central notion. In this paper, we focuses on an important aspect of privacy: deniable authentication.

Deniable authentication refers to authentication between a sender Alice and a receiver Bob where the Bob himself can be confident in the authenticity of the message, but it cannot be proven to a third party after the event. This should be the case even if Alice herself is trying to prove the existence of the conversation to such a third party.

Communications with deniability has been a central concern in personal and business communications, such as online negotiation, shopping over the internet and electronic voting system.

We take online negotiation for example. Suppose a customer wants to order goods from a trader. Then the customer makes a price offer M to the trader and creates the authenticator of M. It is desirable for the customer to be able to prevent the trader from showing this offer M to a third party in order to obtain greater benefits. Otherwise, it is unfair to the customer.

The above example shows that the customer's (sender's) identity should be revealed only to the intended trader (receiver). Therefore, deniable authentication protocol has the following two basic features:(1)Completeness: It enables an intended receiver to identify the source of a given message; (2) Deniability: The intended receiver can not prove to any third party the identity of the sender.

The concept of deniable authentication protocol was initially introduced by Dwork et al. [1], which is based on the concurrent zero knowledge proof. Another notable scheme which was presented by Aumann and Rabin [2] is based on the intractability of the factoring problem. In 2001, Deng et al. [3] also proposed two deniable authentication protocols based on the factoring and the discrete logarithm problem respectively. In 2002, Fan et al. [4] proposed a simple deniable authentication protocol based on Diffie-Hellman key distribution protocol. Unfortunately, Yoon et al. [5] found that their protocol suffers from the intruder masquerading attack and subsequently proposed their enhanced version. Thereafter, various deniable authentication protocols have been devised [6,7] . However, the security of these protocols are mainly based on the assumptions of computational complexity, and they are vulnerable to the strong ability of some advanced quantum algorithms [8,9]. Fortunately, this difficulty can be overcome by quantum cryptography, whose security is based on the quantum mechanics. Owing to its higher security, quantum cryptography has draw a great deal of attention now.

In the field of quantum cryptographic, there have been a lot of quantum identity authentication (QIA) protocol [10-16]. However, these proposed QIA protocols only involved authentication between two participants. In some scenario, such as online negotiation, online shopping and electronic voting etc., the deniability capability is often desired. In 2014, Shi et al. [17] first proposed an efficient quantum deniable authentication protocol based on quantum one-way function and the correlation of GHZ states. And, a trusted centre (TC) is also needed in their protocol. In this paper, however, we will show that there exist a simple solution to the deniable authentication problem which are basically classical protocol with the assistance of quantum key distribution. Therefore, the quantum resources, such as entanglement, unitary operation, quantum memory, decoy states, quantum one-way function etc. are not required, which makes our protocol more efficient and feasible with current technology. Besides, the TC is not needed in our protocol, which avoids information leaking to TC.

The remainder of this paper is organized as follows. Next section describes in detail our deniable authentication protocol. Then, the security of the presented protocol is analyzed. Finally, we give a conclusion and discussion.

Quantum Deniable Authentication Protocol

Our proposed protocol involves two participants: a sender Alice with message m and a intended receiver Bob. M has n bits, i.e. |m| = n. Let p be a prime, with |p| < n. Then Z_p forms a field modulo p with respect to {+, -, *, /}. Our protocol is described as follows.

Setup: Alice and Bob first run a QKD protocol [18] to share a secret key K=(a, b, c), where $(a,b,c) \in Z_p \otimes Z_p \otimes Z_p$.

Generation: Alice uses the shared secret key (a,b) to compute MAC = a*m+b (mod p)[24]. Then, MAC is encoded as quantum state |S> according to the secret key c, i.e., if c_i=0, the i-th bit of MAC 0 (1) is encoded as $|0\rangle$ ($|1\rangle$); otherwise, the i-th bit of MAC 0

(1) is encoded as $|+\rangle$ ($|-\rangle$), where c_i is the i-th bit of the key c, and $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. The message authentication code on m is $|S\rangle$.

Send: Then, Alice sends $\varphi = \{|S\rangle, m, T\}$ to Bob using a secure channel. Here, T is the time stamp.

Authentication: After receiving $\varphi = \{|S\rangle, m, T\}$, Bob first verify whether the time stamp T is valid. If T is invalid, Bob aborts the protocol; otherwise, he first decodes MAC from $|S\rangle$ according to secret key c. Then, he computers $\mathrm{MAC}' = a * m + b(\bmod p)$. If $\mathrm{MAC}' = \mathrm{MAC}$, he accepts m; otherwise Bob reject it.

Security Analysis of The Proposed Protocol

Note that our protocol is mainly composed of two parts: the secret key sharing part and the authentication code generation part. Therefore, given that QKD is composable secure [19], the security of our protocol is mainly depended on the security of the MAC.

Note that most previous results of QKD consider only stand-alone security. The stand-alone security means that the protocol is secure during a single execution of it in an isolated environment. The stand-alone security is often proven by showing that the mutual information between honest party and malicious party is exponentially small. However, the stand-alone security is not sufficient if we consider a protocol in a broader and hence more realistic scenario. Ref.[20] has pointed out that even if the accessible information is small, the key might not be enough secure if it is used in the one-time pad encryption, due to the locking [21]. If we want to guarantee the security of QKD in such a broader context, we must show it is composable secure. The composable security means the QKD protocol is secure even if it is used many times as subroutines of a larger protocol. Fortunately, it has been proven that QKD is universal composable (UC) secure [22,23].

Additionally, the MAC used in our protocol is one-time MAC, and it has been proven to be unconditionally secure as long as the key is used at most once [24]. Therefore, our protocol is unconditionally secure as long as the key is used at most once. This means that our protocol can withstand all the attacks, such as forgery attack, impersonation attack, inter-resend attack, and so on.

In the following, we will show that the presented deniable authentication protocol has the following features: (1) Completeness: It enables an intended receiver to indentity the source of a given message; (2) Deniability: The intended receiver can not prove to any third party the identity of the sender.

Theorem 1 The proposed protocol achieves the authentication between the sender Alice and the intended receiver Bob.

Proof: In our protocol, if Bob accepts the authentication message φ, he can always identify the source of the message. If an adversary wants to impersonate Alice, he can obtain a timestamp T, a message m and the prime p. But, it is not enough for Eve to construct a valid MAC. On the one hand, since the QKD protocol is universal composable (UC) secure [22,23], the generated key K will be still secure when it is used in the MAC.

On the other hand, the one-time MAC used in our protocol is unconditionally secure as long as the key is used at most once [24].

Combining the UC secure QKD with the unconditionally secure one-time MAC makes our protocol unconditionally secure too. In other words, Eve can not obtain the secret key, then she can not forge a valid MAC. Thus, she can not impersonate Alice.

Therefore, if the receiver can identify the source of a given message, the message must come from Alice.

Theorem 2 The proposed protocol achieves the property of deniability.

Proof: To prove that our proposed protocol has the property of deniability, we should prove that all transcripts transmitted between Alice and Bob could be simulated by Bob himself in polynomial time algorithm.

We first construct a simulator Γ. Then we use Γ to simulate the communication transcripts. Therefore, the deniable property can be proved via the simulation process of the simulator.

Transcript Simulation

Setup: The simulator Γ runs a "fake QKD" with Bob. They interact with the third party (consider the third party as Eve of the fake QKD protocol) and run verification procedure as in QKD. The fake QKD generates a key, but the fake output key is unused and kept secret from the third party. Since Bob knows the key K=(a, b, c), Γ and Bob output K=(a, b, c) as their shared key.

Send: Γ uses the key K=(a, b, c) to compute $\mathrm{MAC}'' = a * m + b (\bmod p)$, and encodes MAC'' as quantum sequence $|\mathrm{S}'\rangle$ according secret key c. Then, Γ sends $\varphi' = \{|\mathrm{S}'\rangle, \mathrm{m}, \mathrm{T}\}$ to Bob in a secure way.

The communication transcripts could be simulated by a probabilistic polynomial time algorithm. Based on the construction of the simulator, the third party cannot distinguish the generated $|\mathrm{S}'\rangle$ from those of the sender Alice. Thus the protocol has the deniable property.

Clearly, because both Alice and Bob have the same secret key K=(a, b, c), the transcripts $\varphi' = \{|\mathrm{S}'\rangle, \mathrm{m}, \mathrm{T}\}$ is the same as those of Alice in the real deniable authentication protocol. As a result, Bob is not able to prove to a third party that the transcripts were produced by the sender Alice or is created by himself. According to Bob's transcript simulation above, our protocol achieves the property of deniability.

Efficiency Analysis of the Proposed Protocol

In this subsection, we make a brief comparison between Ref.[17]'s and our protocol. The cost of Ref. [17] are 2 quantum one-way functions, 4n CNOT operations, 6n unitary operations, where n is the length of the transmitted message. Besides, quantum entanglement, quantum memory, decoy states and a trusted center are also needed in their protocol. In contrast with the protocol of Ref.[17], only quantum key distribution is used to share a secret key, the rest part of our protocol is almost classical, which requires 2 multiplication (mod p) operations. Therefore, our protocol is more efficient and feasible with current technology. Additionally, our protocol does not need any help of a trusted center, which avoids unnecessary information leakage to other parties.

Summary

In this paper, we present a quantum deniable authentication protocol. Different from the previous QIA protocols, ours can not only provide authentication but also deniability. A merit of our protocol is that no entanglement states is needed. On the contrary, the protocol in Ref. [17] requires a much greater amount of quantum resources, such as entanglement, quantum memory, decoy states, quantum one-way function, etc. Therefore, our protocol is more feasible and efficient. Furthermore, compared with Ref. [17], our protocol does not need any help of a TC, which avoids information leaking to

TC. Finally, the security analysis shows that our protocol is unconditionally secure. And the simulation based proof shows that the receiver cannot prove the identity of the sender to any third party. The algorithm in this paper can be widely used and applied in remote interaction such as remote medical and remote diagnosis field.

Acknowledgement

This work was financially supported by Science and Technology Plan Project Foundation of Shenzhen(No.JCYJ20140508155916428,No.JCYJ20140828152830610 and No. CXZZ20140418182638764).

References

[1] C. Dwork, M. Naor, and A. Sahai, Concurrent zero-knowledge, in Proc. 30th ACM STOC 98, Dalas TX, USA, (1998), 409-418.

[2] Y. Aumann, and M. O. Rabin, Efficient deniable authentication of long message, Int. Conf. on Theoretical Computer Science in honour of Professor Manuel Blums 60th birthday, (1998).

[3] X. Deng, C. H. Lee, and H. Zhu, Deniable authentication protocols, IEE Proceedings. Computers and Digital Techniques, 148, (2001) 101-104.

[4] L. Fan, C. X. Xu, and J. H. Li, Deniable authentication protocol based on Diffie-Hellman algorithm, Electronics Letters, 38, 705706, (2002).

[5] E. J. Yoon, E. K. Ryu, and K. Y. Yoo, Improvement of Fan et al.'s Deniable Authentication protocol based on Diffie-Hellman Algorithm, Applied Mathematics and Computation, 167, (2005) 274-280.

[6] Y. Aumann, and M. O. Rabin, Authentication, enhanced security and error correcting codes, Crypto'98, Santa Barbara, CA, USA, (1998) 299-303.

[7] W. Lee, C. Wu, and W. Tsaur, A novel deniable authentication protocol using generalized ELGamal signature scheme, Inf. Sci. 177, (2007) 1376-1381.

[8] P. W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, in Proc. 35th Annual Symposium on he Foundations of Computer Science, Santa Fe, New Mexico, (1994) 124-134.

[9] A fast quantum mechanical algorithm for database search, in Proc. 28th Annual ACM Symposium on Theory of Computing, New York, (1996) 212-219.

[10] M. DuSek, O. Haderka, et al., Quantum identification system, Phys. Rev. A, 60, (1999) 149-156.

[11] D. Ljunggren, M. Bourennane and A. Karlsson, Authority-based user authenticaiton in quantum key distribution, Phys. Rev. A, 62, 022305 (2000).

[12] G. H. Zeng and W. P. Zhang, Identity verfication in quantum key distribution, Phys. Rev. A, 61, 022303 (2002).

[13] M. Curty and D. J. Santos, Quantum identification of classical message, Phys. Rev. A, 64, 062309 (2001).

[14] T. Mihara, Quantum identification of classical message, Phys. Rev. A, 65, 05236 (2002).

[15] Z. W. Sun, R. G. Du, D.Y. Long, Quantum secure direct communication with quantum identification, International Journal of Quantum Information. 10(1), (2012) 1250008.

[16] T. Y. Wang, Q. Y. Qiao, and F. C. Zhu, Secure authentication of classical messages with decoherence-free states, Opt. Commun, 282, (2009) 3382-3385.

[17] W. M. Shi, Y. H. Zhou, and Y. G. Yang, quantum deniable authentication, Quantum inf. Process, 13, (2014) 1501-1510.

[18] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, In Proc. of the IEEE Iternational Conference on Computers,Systems and Signal Processing, Bangalore, India, (1984) 175-179.

[19] U. Maurer and R. Renner, Abstract cryptography. In Proceedings of Innovations in Computer Science, ICS, (2011) 1-21.

[20] R. K"onig, R. Renner, A. Bariska, and U. Maurer, Small accessible quantum information does not imply security, Phys. Rev. Lett., 98, 140502 (2007).

[21] D. P. DiVincenzo, M. Horodecki, D. W. Leung, J. A. Smolin, and B. M. Terhal, Locking classical correlations in quantum states, Phys. Rev. Lett., 92, 067902 (2004).

[22] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim, The universal composable security of quantum key distribution, TCC (2005) 386-406.

[23] R. Renner and R K"onig, Universally composable privacy amplification against quantum adversaries, TCC (2005) 407-425.

[24] Simmons, Gustavus, Authentication theory/coding theory, Crypto'84, Berlin, (1985) 411-431.