Quantum message authentication

M. Curty, David J. Santos, and Esther Pérez
ETSIT, Universidad de Vigo, Campus Universitario s/n, E–36200 Vigo (Spain)

Priscila García-Fernández
Instituto de Óptica, CSIC, Serrano, 123 E-28006 Madrid (Spain)

Abstract

Classical cryptography [1], [2] provides data-origin authentication by means of two general techniques: message authentication codes (MACs) [3], and digital-signature schemes [4]. In both cases, the authentication process is specified by two main algorithms: an encoding, or tagging algorithm (possibly stochastic), and a decoding or verification algorithm. When the sender (Alice) wants to send a certified message to a recipient (Bob), she generates, employing the encoding algorithm, an authentication tag or a signature (a function of the message and a secret encoding-key) and appends it to the message. On the reception side, Bob verifies the authenticity of the message by means of the specified decoding procedure, which depends on the message, the tag, and a decoding-key. This algorithm returns a bit indicating when Bob must regard the message as authentic and accept it as coming from Alice, and when he must discard it.

The main difference between MACs and digital-signature schemes is analogous to the difference between private-key and public-key encryption schemes. It resides in the knowledge Alice has on the identity of the receiver, and her level of trust in him. Typically, MACs are employed when the receiver is predetermined at the time of message transmission, and the decoding-key he owns is secret. Information-theoretic secure MACs have been proposed [3]. On the contrary, in signature schemes, the decoding-key is public, and hence known also to the adversary (Eve). This fact guarantees that anybody can verify the authenticity of data. The degree of security provided by signature schemes depends on unproven assumptions related to the intractability of certain difficult mathematical problems, such as the prime-factorization problem [5]. Unfortunately, if a quantum computer is ever built, Shor's quantum algorithms [6] could break classical signature schemes easily, i.e., in polynomial time.

Recently, several proposals of message authentication using quantum resources have been made. Gottesman and Chuang [7] have proposed a quantum version of classical digital signature schemes. Their technique requires limited circulation of the public key, but it allows unconditionally secure authentication of classical messages. A disadvantage of this protocol, as stated by the authors, is that it requires several non-reusable key bits for each message bit signed. Barnum [8] has addressed the problem of quantum data authentication using a set of quantum error detecting codes. The decoding-key is secret, and his protocols achieve a probability of undetected tampering better than the classical bound (inverse in the square root of the number of keys). Leung [9], in another recent paper, also studies quantum-message authentication. Her protocol requires a two-way classical channel between partners, thus making the overall security dependent on the security of that channel. In a previous article [10] we proposed a class of quantum authentication schemes that allow secure authentication of binary classical messages with one qubit as the authentication key. In this paper we adapt this class of protocols to the authentication of quantum messages (qubits), and study its security. We show that the intrinsic nature of quantum information makes it impossible to detect any unauthorized quantum data manipulation by a potential adversary.

REFERENCES

[1] R. Rivest, *Handbook of Theoretical Computer Science, Volume A: Algorithms and Complexity* (Elsevier and MIT Press, 1990), chap. 13. Cryptography, pp. 717–755.
[2] A. Menezes, P. V. Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, Series on Discrete Mathematics and Its Applications (CRC Press, 1996).
[3] M. Wegman and J. Carter, J. Computer and System Sciences **22**, 265 (1981).
[4] W. Diffie and M. Hellman, IEEE Transactions on Information Theory **IT-22**, 644 (1976).
[5] R. Rivest, A. Shamir, and L. Adleman, Communications of the ACM **21**(2), 120 (1978).
[6] P. Shor, SIAM J. Computing **26**, 1484 (1997).
[7] D. Gottesman and I. Chuang, *Quantum digital signatures*, quant-ph/0105032.
[8] H. Barnum, *Quantum message authentication codes*, quant-ph/0103123.
[9] D. Leung, *Quantum Vernam cipher*, quant-ph/0012077.
[10] M. Curty and D. Santos, *Secure authentication of classical messages with one-ebit quantum key*, quant-ph/0103122.