Implementation of Quantum Message Authentication Scheme

Min-Sung Kang[1,2] , Yung-Su Kim[3], Osung Kwon[3], Chun Seok Yoon[4], Hyung Jin Yang[1,2,4], Sang-Wook Han[3] and Sung Moon[3]

[1]*Center for Information Security Technologies (CIST), Korea University, Seoul, Rep. of Korea*
[2]*Graduate School of Information Security, Korea University, Anam 5-ga Sungbuk-gu, Seoul, Rep. of Korea*
[3]*Center for Quantum Information, Korea Institute of Science and Technology (KIST), Seoul, 136-791, Rep. of Korea*
[4]*Department of Physics, Korea University, Sejong, 339-700, Rep. of Korea*
E-mail address: ykhmss@korea.ac.kr

Modern cryptography requires a cryptosystem to have four functions of confidentiality, authentication, integrity and non-repudiation [1, 2]. Likewise, the quantum cryptography should provide these four functions for complete secure communications. Although various quantum key distribution protocols including BB84 [3] have been suggested and developed, these only provide confidentiality, yet. In order to be a complete quantum cryptosystem, the development of the quantum authentication and the quantum signature protocol should be proceeded [4].

We theoretically presented a quantum signature scheme using challenge-response protocol and unitary operators [5]. In this research, we implement a quantum message authentication scheme which is a base technique for realizing the quantum authentication and the quantum signature. In the proposed scheme, the swap test confirming the agreement of two quantum states is implemented using the Hong-Ou-Mandel interference [6]. And the optimal (U,V) or (I, H)-type quantum encryption [5, 7] is performed by the combination of wave-plates.

Our quantum message authentication scheme can be further expanded to the quantum signature protocol by adding a trusted third party in the middle of Alice and Bob. Also, if our quantum message signature scheme uses arbitrated states, it can be utilized as the quantum entity authentication protocol.

References

1. Menezes. A. J., et al. “Handbook of Applied Cryptography”, CRC Press: Boca Raton (1996)
2. Stinson. D. R., “Cryptography: Theory and Practice”, CRC Press Third Edition (2005)
3. Bennett. C. H., "Quantum cryptography: Public key distribution and coin tossing", In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 175, 8, New York (1984)
4. Kang. M. S., et al. "Comment on “Quantum Signature Scheme with Weak Arbitrator”", Int. J. Theor. Phys. 53(6), 1862-1866 (2014)
5. Kang. M. S., et al. "Quantum Signature Scheme Using a Single Qubit Rotation Operator", Int. J. Theor. Phys. 54(2), 614-629 (2015)
6. Garcia-Escartin, J. C., et al. "Swap test and Hong-Ou-Mandel effect are equivalent", Phys. Rev. A 87, 052330 (2013)
7. Choi. J. W., et al. “Security problem on arbitrated quantum signature schemes”, Phys. Rev. A 84, 062330 (2011)