Scopus

Documents

Nagy, M., Nagy, N.

Quantum-based secure communications with no prior key distribution
(2016) *Soft Computing*, 20 (1), pp. 87-101. Cited 3 times.

Abstract
Current quantum cryptographic protocols aim to distribute a classical secret key to be used afterwards in classical encryption/decryption schemes. We show in this paper that quantum information processing can be used to do much more than just key distribution. Simple quantum transformations augmented with the ability to store qubits in a quantum memory are the building blocks of a class of protocols allowing two parties to communicate secretly by encoding/decoding the exchanged message directly through quantum means, without the need to establish a secret encryption/decryption key first. Consequently, our quantum mechanical process of securely transmitting a message through a public channel is conceptually simpler than the two-step scenario with a quantum distributed classical key. In addition, since the encrypted message is only transmitted through a quantum channel, copying and off-line analysis of the transmission is impossible. Our algorithms rely on the common assumption that public information can be authenticated. In terms of security, the protocol using three encoding bases achieves the maximum detection rate of 33 % per qubit tested. The probability of catching a potential eavesdropper can be brought as close to 1 as desired by increasing the length of the signature string attached to the message. © 2014, Springer-Verlag Berlin Heidelberg.

2-s2.0-84952978172
Document Type: Article
Publication Stage: Final
Source: Scopus