

Documents

Nagy, M., Nagy, N.

General quantum encryption scheme based on quantum memory

(2013) *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 8273 LNCS, pp. 169-180. Cited 1 time.

Abstract

In cryptography, 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 protocol 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 simpler, cleaner, faster and computationally more efficient than the two-step scenario with a quantum distributed classical key. The probability of catching a potential eavesdropper can be made arbitrarily large by increasing the length of the signature string attached to the message. © 2013 Springer-Verlag.

2-s2.0-84892426969

Document Type: Conference Paper

Publication Stage: Final

Source: Scopus