

A single photon quantum user bi-directional authentication scheme over noiseless channel

ABSTRACT

In this paper, we propose a quantum user authentication protocol with single photon based on short shared secret key and quantum bit error ratio verification. In this scheme, usage of proposed deterministic quantum key distribution technique and simple verification in a public channel culminate reduced photon transmission. Security analysis proves our proposed scheme is resistant to impostors' attacks and eavesdropper. Furthermore, our proposed protocol can extend to multiparty environment and permits to re-use many times of the shared secret key without revealing it.

Keyword: Quantum cryptography; Quantum user authentication; Single photon quantum key distribution