2006 Vol.46 No.3 pp.443-446 DOI:

Quantum Privacy Amplification for a Sequence of Single Qubits

DENG Fu-Guo[1,2] and LONG Gui-Lu[3,4]

[1] The Key Laboratory of Beam Technology and Material Modification of Ministry of Education and Institute of Low-Energy Nuclear Physics, Beijing Normal University, Beijing 100875, China
[2] Beijing Radiation Center, Beijing Normal University, Beijing 100875, China
[3] Key Laboratory for Quantum Information and Measurements and Department of Physics, Tsinghua University, Beijing 100084, China
[4] Key Laboratory for Atomic and Molecular NanoSciences, Tsinghua University, Beijing 100084, China
(Received: 2006-1-10; Revised:)

Abstract: We present a scheme for quantum privacy amplification (QPA) for a sequence of single qubits. The QPA procedure uses a unitary operation with two controlled-not gates and a Hadamard gate. Every two qubits are performed with the unitary gate operation, and a measurement is made on one photon and the other one is retained. The retained qubit carries the state information of the discarded one. In this way, the information leakage is reduced. The procedure can be performed repeatedly so that the information leakage is reduced to any arbitrarily low level. With this QPA scheme, the quantum secure direct communication with single qubits can be implemented with arbitrarily high security. We also exploit this scheme to do privacy amplification on the single qubits in quantum information sharing for long-distance communication with quantum repeaters.

PACS: 03.67.Hk, 03.67.Dd
Key words: quantum privacy amplification, quantum secure direct communication