A novel error correction scheme in quantum key distribution (QKD) protocol

ABSTRACT

Ideally, in any quantum key distribution (QKD) communication system, each sifted key is expected to be received without error. However in practice, due to infeasibility of generating pure single photon and device impairment problem, some of the sifted key may experience errors. This results to the increment of quantum bit error rate (QBER) that requires error reconciliation for correcting error. The main concept in error reconciliation is very much related to the capability of correcting all errors while minimizing eavesdrop information. The quantum error correcting code such as Hamming code which used in Winnow protocol is found to be more attractive. However the Winnow protocol can only correct one error out of seven bits. In this paper, a modified Hamming encoder/decoder to improve Winnow protocol by correcting two errors out of seven bits which leads to reducing the QBER is presented. This design utilizes a pair of forward and reverse order syndromes for error pattern recognition. A new reconciliation protocol has been developed to enhance the error correcting capability in BB84 protocol. It is carried out in a simple structure which can correct up to double erroneous bits and detect four erroneous bits for each seven bits.

Keyword: Cryptography; Hamming code; Error correction; QKD; Reconciliation protocol; BB84 protocol; Winnow protocol