Quantum Cryptography Based On Qutrit Bell Inequalities

Dagomir Kaszlikowski,[1] Kelken Chang,[1] D. K. L. Oi,[2] L.C. Kwek,[3,1] and C.H. Oh[1]

[1] *Department of Physics, Faculty of Science, National University of Singapore, Lower Kent Ridge, Singapore 119260, Republic of Singapore*
[2] *Centre for Quantum Computation, Clarendon Laboratory, University of Oxford, Parks Road, Oxford OX1 3PU, UK*
[3] *National Institute of Education, Nanyang Technological University, 1 Nanyang Walk, Singapore 639798*

We present a cryptographic protocol based upon entangled pairs of three-dimensional quantum systems. The presented scheme is a natural generalization of Ekert-91 qubit protocol. We analyze the security of the protocol under a symmetric incoherent attack and show that it is more robust against noise than its qubit counterpart. We also show that the violation of a three dimensional generalization of Clauser-Horne-Shimony-Holt inequality is only a necessary condition for the security of the transmission in this case, i.e., the secure communication is possible even if there is a local realistic description of quantum correlations. This is surprising and may imply that there is no connection between Bell inequalities and security of cryptographic protocols based on entanglement for more than two dimensional quantum systems.

PACS numbers: