World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:12, No:09, 2018

FPGA Implementation of the BB84 Protocol

Authors : Jaouadi Ikram, Machhout Mohsen

Abstract : The development of a quantum key distribution (QKD) system on a field-programmable gate array (FPGA) platform is the subject of this paper. A quantum cryptographic protocol is designed based on the properties of quantum information and the characteristics of FPGAs. The proposed protocol performs key extraction, reconciliation, error correction, and privacy amplification tasks to generate a perfectly secret final key. We modeled the presence of the spy in our system with a strategy to reveal some of the exchanged information without being noticed. Using an FPGA card with a 100 MHz clock frequency, we have demonstrated the evolution of the error rate as well as the amounts of mutual information (between the two interlocutors and that of the spy) passing from one step to another in the key generation process.

Keywords : QKD, BB84, protocol, cryptography, FPGA, key, security, communication
Conference Title : ICCTCAA 2018 : International Conference on Coding Theory, Cryptology and Advanced Applications
Conference Location : Rome, Italy
Conference Dates : September 17-18, 2018