Abstract

The basic foundation behind cryptography as a discipline was to research how valuable data, information can be protected from unauthorized parties, such as adversaries. Quantum cryptography is one of the recent advancement occurred within that discipline. However, this cryptographic algorithm still at its early stages, where there is no wide implementation can be seen. Many research papers have been done to develop this algorithm, while others, to propose new implementations of this algorithm to tackle a specific problem. This research paper studies and examines the relationship between the QKDS (Quantum Key Distribution System) and the parity bits. Hence, explore how the use of parity bits can improve the final resolved key.

References

- Nicolas Gisin, Gregoire Ribordy, Wolfgang Tittel, and Hugo Zbinden, "Quantum


- Branciard, Cyril; Gisin, Nicolas; Kraus, Barbara; Scarani, Valerio, &quot;Security of two quantum cryptography protocols using the same four qubit states&quot; Physical Review, 2005, A 72 (3).


- F. T. Sufyan and K. Jasim. Omer, &quot;Reducing the Authentication bits lost in Quantum Cryptography&quot; , The International Conference on Digital Information and Communication Technology and its Applications (PGNET&apos;apos;2011) , Jemors University , Liverpool.


Index Terms

Computer Science Communications
Keywords
Quantum Cryptography  parity bits  BB84 protocol simulation  QKDS