Contribution ID: **108** Type: **Oral Presentation**

Development of Post-Processing Technique for a Quantum Key Distribution System

Thursday, 6 July 2017 16:10 (20 minutes)

Classical Cryptography offers different methods to encrypt messages amongst authorized users by applying some mathematical techniques which require the users to have shared some information initially[1]. These mathematical techniques can be broken as they all rely on the computational complexity[1]. Quantum Key Distribution (QKD) is an alternative means of encrypting information whereby instead of users exchanging an encrypted message; they share first the symmetric-key[2]. QKD relies on the properties of Quantum Mechanics to protect the information transfer from the interference of an eavesdropper. The implementation of QKD demands an appropriate protocol which can enable the users to produce a secure key.
Apart from the key distribution process, post-processing is performed to obtain a final key. This is achieved through an error reconciliation protocol. Post-processing is required to eliminate errors introduced by an eavesdropper in the quantum channel and imperfections of the equipment used[3]. The error reconciliation protocol is hence needed to identify and fix all the errors in the shared key, so that at the end users will have the same identical key.
In this research, the data used for post-processing were obtained from experimental implementation of the Coherent One-Way (COW) protocol using free space as a quantum channel. We applied Cascade error reconciliation protocol to the raw key obtained in the experiment to identify and fix errors obtained in the quantum transmission process. Also Cascade error reconciliation protocol is tested to verify how efficiency of the system.

References

1.Zoller, P., et al., Quantum information processing and communication. The European Physical Journal D-Atomic, Molecular, Optical and Plasma Physics, 2005. 36(2): p. 203-228.

2.Nicolas, G., et al., Quantum cryptography. REVIEWS OF MODERN PHYSICS, 2002. 74(1): p. 145 - 195.

3.Brassard, G. and L. Salvail. Secret-key reconciliation by public discussion. in Workshop on the Theory and Application of of Cryptographic Techniques. 1993. Springer.

Apply to be
 considered for a student
   award (Yes / No)?

yes

Level for award
 (Hons, MSc,
   PhD, N/A)?

MSc

Main supervisor (name and email)
and his / her institution

Prof. Francesco Petruccione
petruccione@ukzn.ac.za

University of Kwazulu-Natal.

Would you like to
 submit a short paper
 for the Conference
 Proceedings (Yes / No)?

Yes

Primary author: Ms UMUHIRE, Marie Louise (University of Kwazulu-Natal, Private Bag X54001, Durban 4000, South Africa)

Co-authors: Prof. PETRUCCIONE, Francesco (UKZN); Dr ISMAIL, Yaseera (UKZN)

Presenter: Ms UMUHIRE, Marie Louise (University of Kwazulu-Natal, Private Bag X54001, Durban 4000, South Africa)

Session Classification: Applied Physics

Track Classification: Track F - Applied Physics