Contribution ID: **317** Type: **Poster Presentation**

Privacy amplification for a quantum key ditribution

Thursday, 28 June 2018 15:00 (2 hours)

Quantum key distribution (QKD) is a process of encoding information in quantum carrier such photons that is shared between legitimate users (usually referred to as Alice and Bob) in the presence of an eavesdropper (usually referred to as Eve) [1]. Alice (sender) and Bob (receiver) are connected via two channels namely a quantum channel and classical channel. A quantum channel can be an optical fibre or free space; it enables users to exchange quantum information (single photons). A classical channel can be a computer network or a telephone line; it is used for the analysis of the transmitted information, the evaluation of the efficiency of the system and elimination of any error committed during the communication [1].
Since the introduction of QKD, many protocols have been proposed which can ensure the security of exchanging information [2-5]. The implementation of these protocols exploits the laws of Physics by using binary encoding based on phase, polarisation or time-bin degrees of freedom and achieves a secret key rate of at least one bit per photon [1, 6].

The implementation of a QKD system requires the execution of two major processes, such as quantum transmission and post-processing procedure. The second process is composed with 3 steps namely error estimation, error reconciliation and privacy amplification. This research project focuses on the privacy amplification where the size of the reconciled key is reduced in order to eliminate any information an eavesdropper could have gained.

References

1. Gisin, N., et al., Quantum cryptography. Reviews of modern physics, 2002. 74(1): p. 145.
2. Bennett, C.H., Quantum cryptography using any two nonorthogonal states. Physical review letters, 1992. 68(21): p. 3121.
3. Ekert, A.K., Quantum cryptography based on Bell's theorem. Physical review letters, 1991. 67(6): p. 661.
4. Scarani, V., et al., Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. Physical review letters, 2004. 92(5): p. 057901.
5. Gisin, N., et al., Towards practical and fast quantum cryptography. arXiv preprint quant-ph/0411022, 2004.
6. Scarani, V., et al., The security of practical quantum key distribution. Reviews of modern physics, 2009. 81(3): p. 1301.

Please confirm that you
have carefully read the
abstract submission instructions
under the menu item
"Call for Abstracts"
(Yes / No)

Yes

Consideration for
student awards
Choose one option
from those below.
N/A
Hons
MSc
PhD

PhD

Supervisor details
If not a student, type N/A.
Student abstract submision
requires supervisor permission:
please give their name,
 institution and email address.

Prof. Francesco Petruccione, University of KwaZulu-Natal, petruccione@ukzn.ac.za

Primary author: Ms UMUHIRE, Marie Louise (University of Kwazulu Natal, School of Chemistry and Physics, Westville Campus, Durban, South Africa)

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

Presenter: Ms UMUHIRE, Marie Louise (University of Kwazulu Natal, School of Chemistry and Physics, Westville Campus, Durban, South Africa)

Session Classification: Poster Session 2

Track Classification: Track F - Applied Physics