Contribution ID: **32** Type: **Poster Presentation**

Security proof of a generic three party Quantum Key Distribution protocol

Tuesday, 4 July 2017 17:10 (1h 50m)

Quantum cryptography or more specifically Quantum key distribution (QKD) is the emerging technology that has shown to be provably secure for transmitting messages between the communicating parties. The security of a QKD protocol is mainly based on the laws of quantum mechanics. In this work, we present a simple security proof for a three party generic QKD protocol. The protocol is implemented using the GHZ states and each party has to perform a single particle measurement either on the computational basis or the Hadamard basis. The security analysis of our protocol is based on the collective attacks and we used one way information reconciliation and privacy amplification to extract the key. Eve's information is conditioned on the random variable V, which provide all the projective measurements on the density operator ρ_ABC. The value obtained for the error bound is ϵ≈0.031.

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

Yes

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

N/A

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

Yes

Primary author: Mr SEKGA, Comfort (Department of Physics and Astronomy, Botswana International University fo Science and Technology, Private Bag 16 Palapye, Botswana)

Co-author: Dr MAFU, Mhlambululi (Botswana International University of Science and Technology)

Presenters: Mr SEKGA, Comfort (Department of Physics and Astronomy, Botswana International University fo Science and Technology, Private Bag 16 Palapye, Botswana); Dr MAFU, Mhlambululi (Botswana International University of Science and Technology)

Session Classification: Poster Session 1

Track Classification: Track G - Theoretical and Computational Physics