# SAIP2012

Contribution ID : 281

## Upper bound to accessible information for the six-state quantum key distribution protocol

Tuesday 10 Jul 2012 at 17:30 (02h00')

**Abstract** :

Quantum key distribution allows two distant parties, traditionallyknown as Alice and Bob who are connected by an authenticated clas-sical channel and insecure quantum channel to establish a secure random cryptographic key under the intervention of an eavesdropper, Eve [1]. It is necessary for any quantum key distribution protocol to have an unconditional security proof which is robust against any kinds of attack that are allowed by the laws of physics. This is the main advantage of quantum key distribution schemes over classical ones aiming to achieve the same task. We derive the upper bound on the achievable information that an eavesdropper may obtain. Instead of the known method of conditioning on the random variable, we express Eve's information about the raw key as a function of the error since it is related to the secret key fraction. The proposed method reproduces the upper bound that was derived previously [2, 3].References[1] Nicolas Gisin, Gr□egoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. Rev. Mod. Phys., 74(1):145{195, Mar 2002.[2] H.K. Lo. Proof of unconditional security of six-state quatum key distribution scheme. Quantum Information and Computation, 1(2):81{94, 2001.[3] Renato Renner, Nicolas Gisin, and Barbara Kraus. Information-theoretic security proof for quantum-key-distribution protocols. Phys. Rev. A,72:012332, Jul 2005.

**Award** :

Yes

**Level** :

MSc

**Supervisor** :

Prof. Francesco Petruccione

**Paper** :

Yes

**Primary authors** : Mr. MAFU, Mhlambululi (Quantum Research Group)

**Co-authors** : Prof. PETRUCCIONE, Francesco (Quantum Research Group, National Institute for Theoretical Physics and School of Chemistry and Physics, University of KwaZulu-Natal)

**Presenter** : Mr. MAFU, Mhlambululi (Quantum Research Group)

**Session classification** : Poster Session

**Track classification** : Track G - Theoretical and Computational Physics

**Type** : Poster Presentation