# SAIP 2011

Contribution ID : 398

## Towards the unconditional security proof for the Coherent-One-Way (COW) protocol

Wednesday 13 Jul 2011 at 15:00 (00h15')

**Content** :

Quantum Cryptography, one aspect of which is Quantum Key Distri-bution (QKD), provides the only physically secure and proven methodfor the transmission of a secret key between two distant parties, Alice and Bob. The goal of QKD is to guarantee that a possible eavesdropper (Eve), with access to the communication channel is unable to obtain useful information about the message.The Coherent-One-Way (COW) protocol is one of the most recent practical QKD protocols. However, its security proof still remains unrealized. We therefore present a necessary condition for the security of the COW protocol. In the proof, we describe bob's measurements by non-commuting POVM elements which satisfies this proof.

**Level (Hons, MSc, PhD, other)?** :

PhD

**Consider for a student award (Yes / No)?** :

Yes

**Short Paper** :

Yes

**Primary authors** : Mr. MAFU, Mhlambululi (Centre for Quantum Technology)

**Co-authors** : Ms. MARAIS, Adriana (center for Quantum Technology) ; Prof. PETRUCCIONE, Francesco (Center for Quantum Technology)

**Presenter** : Mr. MAFU, Mhlambululi (Centre for Quantum Technology)

**Session classification** : Theoretical

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

**Type** : Oral Presentation