



Contribution ID: 398

Type: Oral Presentation

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

Wednesday, 13 July 2011 15:00 (15 minutes)

Quantum Cryptography, one aspect of which is Quantum Key Distribution (QKD), provides the only physically secure and proven method for 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

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

Yes

Primary author: 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