



Contribution ID: 169

Type: Oral Presentation

Portable QKD Device Using the COW Protocol

Tuesday, 30 June 2015 11:30 (20 minutes)

Abstract content (Max 300 words) Formatting & Special chars

Quantum Key Distribution (QKD) is an emerging field of information security. To date, this technology has been implemented for large scale financial and voting purposes, but QKD is a versatile solution which can also be utilised to secure personal transactions. The development of low cost, portable QKD devices can further promote the use of quantum encryption in commercial security systems. Research has been done to design hand-held QKD devices for personal use with ATMs. These devices use a short-range free space channel to produce a secret key using the polarisation of single photons as qubits. Free space applications of QKD usually utilise polarisation encoding of single photons since the polarisation states do not deteriorate in the turbulent atmosphere. The proposed device uses the Coherent One Way (COW) protocol to exchange a secret key between the two authenticated parties. The COW protocol is a simple, practical protocol which uses the time of arrival of consecutive weak coherent pulses as the bit encoding. The security of this protocol lies in the coherence between consecutive laser pulses. Should decoherence be observed in the monitoring line, the presence of an eavesdropper is inferred. An advantage of using the COW protocol is the small size and low cost of the setup. This is ideal for a hand-held device used for short-range QKD. The COW protocol is not traditionally used for a free space channel due to the fragility of coherence in a turbulent medium. Since this is a short-range device which will not encounter any turbulence, the coherence of the laser beam is not compromised. It is therefore suitable to use the COW protocol under these conditions. The design of the system in a free space channel and the synchronisation of the system will be discussed.

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

yes

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

PhD

Main supervisor (name and email) and his / her institution

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

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

Yes

**Please indicate whether
this abstract may be
published online
(Yes / No)**

Yes

Primary author: Ms PILLAY, Sharmini (University of KwaZulu-Natal)

Co-authors: Dr MIRZA, Abdul (University of KwaZulu-Natal); Prof. PETRUCCIONE, Francesco (University of KwaZulu-Natal); Dr MARIOLA, Marco (University of KwaZulu-Natal)

Presenter: Ms PILLAY, Sharmini (University of KwaZulu-Natal)

Session Classification: Applied

Track Classification: Track F - Applied Physics