



Contribution ID: 378

Type: Oral Presentation

Finite-size key security of Phoenix-Barnett-Chefles 2000 quantum-key-distribution protocol

Thursday, 10 July 2014 10:20 (20 minutes)

**Abstract content
 (Max 300 words)
Formatting &
Special chars**

Based on the post-selection technique which was introduced by Christandl, König and Renner [Phys Rev. Lett. 102, 020504 (2009)] in order to simplify the security of quantum key distribution schemes, we study the security of the Phoenix-Barnett-Chefles 2000 quantum key distribution protocol. The postselection technique has been proposed and some examples have been shortly described in the literature. Therefore, we present the details of the security proof for a specific realistic protocol. We also give bounds on the secret key rates for the Phoenix-Barnett-Chefles 2000 protocol by using the post selection technique when given a finite amount of resources.

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

No

**Level for award
 (Hons, MSc,
 PhD)?**

PhD

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

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

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

No

Primary author: Dr MAFU, Mhlambululi (UKZN)

Co-authors: Prof. PETRUCCIONE, Francesco (UKZN); Mr GARAPO, Kevin (UKZN)

Presenter: Dr MAFU, Mhlambululi (UKZN)

Session Classification: Theoretical

Track Classification: Track G - Theoretical and Computational Physics