



Contribution ID: 505

Type: Oral Presentation

## Finite-size key in QKD protocols for Renyi entropies

Wednesday, 10 July 2013 11:30 (20 minutes)

### Abstract content <br> &nbsp; (Max 300 words)

A realistic quantum key distribution protocol necessarily runs with finite resources. This is in contrast to the existing quantum key distribution security proofs which are asymptotic, in the sense that they only work if certain parameters are exceedingly large as compared to practical realistic values. In this paper, we spell out the bounds and formalism to derive bounds on the secret key rates for the B92 protocol [Phys. Rev. Letter, 68. 3121 1992] which includes a preprocessing step. This is expressed as an optimization problem by using the recent results on the uncertainty relation and the smooth Renyi entropies.

### Apply to be<br> considered for a student <br> &nbsp; award (Yes / No)?

Yes

### Level for award<br>&nbsp;(Hons, MSc, <br> &nbsp; PhD)?

PhD

### Main supervisor (name and email)<br>and his / her institution

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

### Would you like to <br> submit a short paper <br> for the Conference <br> Pro- ceedings (Yes / No)?

Yes

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

**Co-authors:** Prof. PETRUCCIONE, Francesco (Centre for Quantum Technology, University of KwaZulu-Natal); Mr GARAPO, Kevin (University of KwaZulu-Natal)

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

**Session Classification:** Theoretical

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