Contribution ID: **280** Type: **Oral Presentation**

Derivation of the quantum-bit-error rate for the BB84 protocol based on the phase-covariant-cloning machine

Wednesday, 11 July 2012 08:20 (20 minutes)

Abstract content
   (Max 300 words)

Quantum key distribution provides the only physically secure and proven method for the transmission of a secret key between two distant parties, Alice and Bob who are connected by an authenticated classical channel and insecure quantum channel [1]. Based on the laws of physics in particular the no-cloning theorem [2], quantum key distribution makes possible the distribution of the secret key such that the third party, Eve cannot clone the quantum states of the BB84 protocol sent by Alice and then re-send a perfect copy to the receiver (Bob) without it being de- tected. However, the phase-covariant-cloning machine [3] seems to be the best cloning machine for the BB84 quantum states. Therefore, we high- light that there is a trade-off between the quality of the clone and the amount of information that Eve can gain but still the protocol remaining secure. By using the phase-covariant-cloning machine to illustrate strate- gies performed by the eavesdropper, we arrive at a quantum bit-error-rate of 0.1464 for the BB84 protocol which agrees with previous results [4, 5].

References

[1] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Du˘sek, Norbert Lu¨tkenhaus, and Momtchil Peev. The security of practi- cal quantum key distribution. Rev. Mod. Phys., 81(3):1301–1350, Sep 2009.

[2] M.A. Nielsen and I.L. Chuang. Quantum Computation and Quantum Infor- mation. Cambridge University Press, 2002.

[3] D. Bruss, M. Cinchetti, G. Mauro DAriano, and C. Macchiavello. Phase- covariant quantum cloning. Physical Review A, 62(1):12302, 2000.

[4] P.W. Shor and J. Preskill. Simple proof of security of the bb84 quantum key distribution protocol. Physical Review Letters, 85(2):441–444, 2000.

[5] C. Branciard, N. Gisin, B. Kraus, and V. Scarani. Security of two quantum cryptography protocols using the same four qubit states. Physical Review A, 72(3):32301, 2005.

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

Yes

Level for award
 (Hons, MSc,
   PhD)?

MSc

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

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

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

Yes

Primary author: Mr MAFU, Mhlambululi (Quantum Research Group, UKZN)

Co-author: Prof. PETRUCCIONE, Francesco (Quantum Research Group, National Institute for Theoretical Physics and School of Chemistry and Physics, University of KwaZulu-Natal)

Presenter: Mr MAFU, Mhlambululi (Quantum Research Group, UKZN)

Session Classification: Theoretical

Track Classification: Track G - Theoretical and Computational Physics