Security of Post-selection based Continuous Variable Quantum Key Distribution against Arbitrary Attacks

Nathan Walk¹, Timothy C. Ralph¹, Thomas Symul² and Ping Koy Lam²
¹Department of Physics, University of Queensland, St Lucia, QLD 4072, Australia
²Quantum Optics Group, Department of Physics, Faculty of Science, Australian National University, ACT 0200, Australia

We analyse the security and performance of a continuous variable quantum key distribution protocol using post selection, deriving results that are unconditionally secure in the sense of no longer restricting the eavesdroppers attack.

Quantum Key Distribution; Post-selection; Continuous Variable; Non-Gaussian Attacks;

I. INTRODUCTION

Quantum key distribution (QKD) is the process of sharing a key, simply a random string, between two parties by encoding the information in a quantum communications protocol. The power of this method is that the security of the key distribution, and the subsequent communication via a one-time pad, is established by imposing only physical limitations upon a potential eavesdropper making no assumptions about their technological capabilities.

There are two main families of QKD, discrete variable (DV) and continuous variable (CV) which are realised by encoding and then detecting single photons and the quadrature variables of the optical field respectively [1].

Initially it was thought that CV-QKD was insecure in principle for channel losses of greater than 50% but this problem has been circumvented by two different protocols, reverse reconciliation [2] and post-selection [3] which both, in principle, allow secure communication even for arbitrarily high losses.

II. SECURITY OF CV-QKD

In general security proofs for CV-QKD protocols proceed by noting that protocols involving the preparation and transmission of a classical distribution of quantum states are equivalent to entanglement based schemes in which an entangled state is prepared one half of which is kept and projectively measured while the other is sent through the eavesdroppers domain.

Using this method both reverse reconciliation and post-selection have been proved to be secure assuming collective Gaussian attacks and powerful result in [4] showed that a hard lower bound could be placed upon the rate of secure transmission by assuming that the final bipartite state shared by Alice and Bob was Gaussian. Up until now the highly non-Gaussian nature of post-selection meant it was unclear how to correctly construct the corresponding entanglement based protocol.

In this work we introduce exactly this equivalent protocol by implementing the post-selection as a quantum filter rather than a classical operation allowing us to apply the Gaussian extremality arguments of [4] to obtain an unconditional lower bound on the rate of secure communication. We further demonstrate how this method can be used to prove the security of a post-selection protocol based only upon quantities directly measured in an experiment.

Finally the performance of the protocol is examined for a lossy channel imposing small amounts of Gaussian noise, which is most commonly encountered scenario. The parameters of the equivalent Gaussian channel are calculated and it is found the post-selection acts as a kind of amplification, increasing the effective channel transmission at the cost of larger effective noise. We compare our unconditional results to those for the same situation but where the eavesdroppers attack was assumed to be Gaussian [5] and as one would expect there is performance penalty associated with this more rigorous proof. However we still find that the post-selection protocol allows provably secure communication for experimentally realistic levels of noise and for losses on the order of 90%.

REFERENCES

[1] V. Scarani et al. The security of practical quantum key distribution. Reviews of Modern Physics, 81(3):1301, 2009.

[2] F. Grosshans and P. Grangier. Continuous variable quantum cryptography using coherent states. Physical Review Letters, 88(5):057902, 2002.

[3] Ch. Silberhorn, T.C. Ralph, N. Lutkenhaus and G. Leuchs. Continuous variable quantum cryptography: beating the 3dB loss limit. Physical Review Letters, 89(16):167901, 2002.

[4] R. Garcia-Patron and N. Cerf. Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. Physical Review Letters, 97(19):190503, 2006.

[5] T. Symul et al. Experimental demonstration of post-selection-based continuous-variable quantum key distribution in the presence of Gaussian noise. Physical Review A, 76(3):030303, 2007.