

Testing Quantum Devices: Entanglement Verification in Optical Systems

Hauke Häselser, Tobias Moroder and Norbert Lütkenhaus

Inst. for Quantum Computing, University of Waterloo, 200 University Ave. W., Waterloo ON N2L 3G1, Canada

Universität Erlangen-Nürnberg, Staudtstr. 7/B2, 91058 Erlangen, Germany

(hhaseler@iqc.ca)

Abstract

We present a method to test quantum behavior of quantum information processing devices, such as quantum memories, teleportation devices, channels and quantum key distribution protocols. The test of quantum behavior can be phrased as the verification of effective entanglement. Necessary separability criteria are formulated in terms of a matrix of expectation values in conjunction with the partial transposition map. Our method is designed to reduce the resources for entanglement verification. A particular protocol based on coherent states and homodyne detection is used to illustrate the method. A possible test for the quantum nature of memories using two non-orthogonal signal states arises naturally. Furthermore, closer inspection of the measurement process in terms of the Stokes operators reveals a security threat for quantum key distribution involving phase reference beams.

Introduction

Many quantum information processing protocols have classical counterparts, but can in principle perform the desired task “better”. In experimental implementation, it is therefore essential to demonstrate that this advantage is not lost by inevitable imperfections. Imagine that the processing of the quantum information is described by a channel which takes input quantum states ρ_i^{in} to the desired output quantum states ρ_i^{out} . The corresponding classical counterpart would be a quantum-classical-quantum (qcq) channel which first converts the quantum information to classical information by suitable destructive measurements and then re-prepares quantum states according to the measurement outcomes. A verifier asked to validate an implementation of a quantum device can now choose suitable sets of test states $\{\rho_i^{in}\}$ and measurements $\{\pi_i\}$ to perform on the output states and can then collect data. The implementation is successful only if the verifier can find sets $\{\rho_i^{in}\}$ and $\{\pi_i\}$ such that his collected data cannot be reproduced by a corresponding (optimized) classical strategy.

Quantum Key Distribution

In the context of quantum key distribution (QKD), it is imperative to test the quantum channel as described, since a qcq channel corresponds to an intercept-resend attack during which all key information leaks to an eavesdropper (Eve) in an undetected manner. In the QKD context, however, the possible test states and measurements on the output states are constrained to those used for the key distillation protocol. Although the construction of explicit intercept-resend at-

tacks may be a simple way of revealing a channel to be useless for secure key distillation, proving the opposite - that a channel can be used - will involve an optimization over all possible intercept-resend attacks, which is typically a much harder task.

There is an alternative way of validating a QKD channel, which builds on the realization that all qcq channels are entanglement-breaking. Therefore, if entangled states are available as test states, a suitable entanglement criterion can be used to check whether the channel breaks entanglement. This is indeed possible even if entangled states are not available, since every source of non-orthogonal signal states admits an *entanglement-based* description, in which case we will refer to effective entanglement. Difficulties arise in this formalism due to the fact that dimension of the effective entangled states depends on the number of signal states for the sender (Alice) and on the dimension of the output Hilbert space for the receiver (Bob). Since the number of signal states used in an experiment is necessarily finite, continuous-variable implementations require an entanglement criterion for discrete-continuous systems.

In particular, we will investigate a continuous-variable version of the B92-protocol with the signal states $|\alpha\rangle$ and $|-\alpha\rangle$ [1]. An entanglement criterion applicable to these qubit-mode states was introduced in Ref. [2], and was developed further and proven to be based on partial transposition in Ref. [3]. This so-called *expectation value matrix* method shows that for the protocol in question with homodyne detection and recording of the first and second moments of two orthogonal quadrature components, the presence of effective entangle-

ment can be verified for a large range of experimentally feasible parameters.

The Phase Reference

However, care must be taken when homodyne detection is involved in practical QKD. Not only does the eavesdropper have access to the signal state mode, but also to the phase reference necessary for Bob's detection. This local oscillator beam is typically sent along the same channel as the signal to ensure phase stability and consequently passes through the insecure domain controlled by Eve. To make assumptions about its state at Bob's detector is hence not justified and the homodyne detection setup should be considered a two-mode measurement, giving the first two moments of two Stokes operators, say \hat{S}_2 and \hat{S}_3 (see Ref. [3]). For this scenario, an expectation value matrix can be constructed as in the quadrature measurement case, but it does not detect *any* entanglement. In fact, an explicit intercept-resend attack can be constructed, which can explain all possible measurement outcomes, in the limit of a strong local oscillator beam leaving Alice's source. This attack reduces the total intensity of both modes while keeping Bob's measured expectation values invariant, thus counteracting the introduction of excess noise. Clearly, no secret key can be distilled from such data.

There are two simple additional measurements which essentially allow us to interpret the homodyne detection as a quadrature measurement again. One is to measure the intensity difference between signal and local oscillator mode, i.e. the third Stokes operator \hat{S}_1 . The other way is to monitor the intensity of the local oscillator separately as it enters the detector, which allows us to bound $\langle \hat{S}_1 \rangle$ from below. In both cases, the expectation value matrix can be extended to include all three Stokes operators and the results essentially coincide with those for quadrature detection.

Although the ability to verify entanglement is easily restored by performing additional measurements, the analysis shows the necessity for careful considerations of the underlying assumptions involved in any implementation of QKD protocols.

References

- [1] S. Lorenz, J. Rigas, M. Heid, U. L. Andersen, N. Lütkenhaus, and G. Leuchs, Phys. Rev. A **74**, 042326 (2006).
- [2] J. Rigas, O. Gühne, and N. Lütkenhaus, Phys. Rev. A **73**, 012341 (2006).
- [3] H. Häselser, T. Moroder, and N. Lütkenhaus, Phys. Rev. A **77**, 032303 (2008).