

# Security of coherent state quantum cryptography against collective attacks in the presence of gaussian channel noise

Matthias Heid (1) and Norbert Lütkenhaus (2)

1: Quantum Information Theory Group, Institut für Theoretische Physik I and Max-Planck Research Group, Institute of Optics, Information and Photonics, Universität Erlangen-Nürnberg, Staudtstr. 7/B2, 91058 Erlangen, Germany

2: Institute for Quantum Computing, University of Waterloo, 200 University Avenue West, Waterloo, Ontario N2L 3G1, Canada

## Abstract

We analyze the security of a continuous variable quantum key distribution scheme in a realistic setting. The quantum channel connecting the two honest parties is assumed to be lossy and imposes Gaussian noise on the observed quadrature distributions. Secret key rates are given for direct and reverse reconciliation schemes including postselection. The effect of a non-ideal error correction is also taken into account.

## A Gaussian modulated Protocol

We assess the security of a quantum key distribution (QKD) scheme in the continuous variables setting. The sender Alice prepares coherent states  $|\alpha\rangle$  and sends them through a quantum channel possibly controlled by an eavesdropper Eve to the receiver Bob. The input amplitudes  $\alpha$  are drawn at random from a Gaussian probability distribution. Bob performs a heterodyne measurement upon the received states, which is equivalent to a projection onto a coherent state  $|\beta\rangle$ . Alice encodes a logical bit value 0 (1) whenever the real part  $\alpha_x$  of the sent coherent amplitude  $\alpha$  is positive (negative). Consequently, Bob assigns the bit value 0 if the real part  $\beta_x$  of the measured amplitude  $\beta$  is positive. We assume that Alice and Bob share a common phase reference, which cannot be manipulated by Eve.

## Collective Attacks

In our approach, Eve may only perform collective attacks. However, there has been recent work [4] to extend these results through quantum de Finetti type arguments [5] to unconditional security. Also, arguments of optimality of Gaussian attacks are used for the same purpose [6]. The collective attack consists of an individual unitary interaction of Eve's ancilla system with the signals. After this attack, her knowledge about the signals is summarized in holding quantum states  $\rho_E^i$ . She may keep these states after the classical post-processing step of the protocol is completed. Since Alice and Bob use an insecure but authenticated classical channel in this step, Eve may listen and use any gained information to optimize her measurement. In this scenario, a lower bound on the secret key rate is given by Devetak and Winter [1]

$$G \geq I_{A:B} - \chi, \quad (1)$$

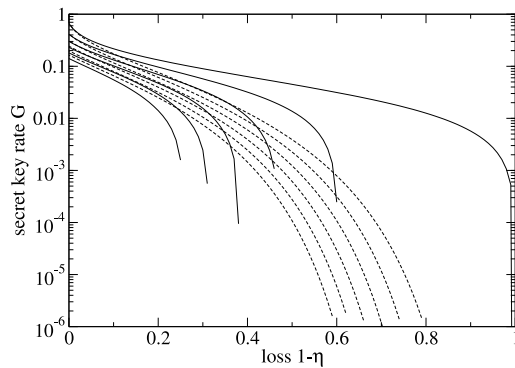
where  $I_{A:B}$  denotes the mutual information between Alice and Bob. The Holevo quantity  $\chi$  quantifies the amount of privacy amplification needed to obtain secret bit strings and is a function of the quantum states  $\rho_E^i$ .

## Quantum Channels imposing Gaussian Noise

In order to construct Eve's quantum states, we assume that the quantum channel is lossy and imposes Gaussian excess noise on the conditional probability distribution  $p(\beta|\alpha)$  seen by Bob. Therefore, the observed probability distributions are still of Gaussian shape, but are broadened by a factor of  $\delta$ , the so-called excess noise, above the vacuum noise level. Here, we do not take quantum channels into account, that could impose arbitrary noise onto the exchanged signals. However, Gaussian noise is typically seen in experiments [7, 8]. Moreover, Alice and Bob can in principle check the validity of the Gaussian assumption in the asymptotic key limit: the described prepare-and-measure scheme can be reformulated in an entanglement based scheme where the exchange of quantum states corresponds to Alice and Bob performing heterodyne measurements onto a shared quantum state  $\rho_{AB}$ . As heterodyne measurements are tomographic complete, Alice and Bob can reconstruct the shared state  $\rho_{AB}$ . Eve might have at most a purification of  $\rho_{AB}$ . Since the two party state  $\rho_{AB}$  is fixed by the tomographic measurements, Eve's purification is determined up to a unitary onto her system. This fixes Eve's knowledge about the signals. Moreover, it follows that all attacks compatible with the observation of a certain amount of excess gaussian noise and loss are equivalent.

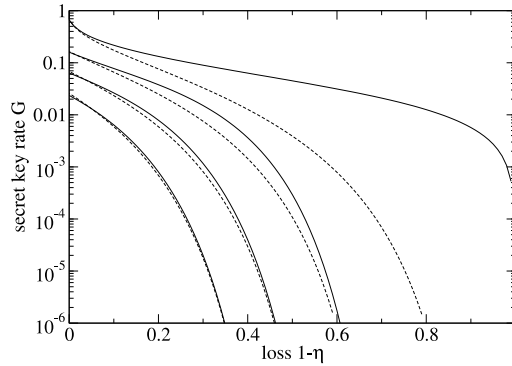
## Secret Key Rate

Strict one-way communication is required in the approach (1). It has been shown [2] that one could either use the classical channel from Alice to Bob or in the opposite direction in the error correction step to obtain two ways of distilling a secret key from shared classical data. We refer to the first case as direct reconciliation (DR), whereas the latter is called reverse reconciliation (RR). Moreover, we allow Bob to postselect his measurement results: he only keeps outcomes if he learns more on average about the sent signal than Eve. Figure (1) summarizes our results for the postselected DR scheme and the RR scheme without postselection. It can be seen that the RR protocol loses quickly its initial advantage with increasing excess noise. Figure (2)

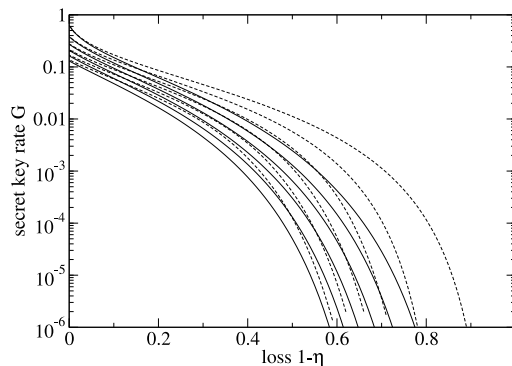


**Figure 1:** Comparison of the secret key rate  $G$  versus loss  $1 - \eta$  for the PS-DR (dashed lines) and the RR (solid lines) scheme. The secret key rates shown correspond to an excess noise  $\delta$  of  $\{0, 0.02, 0.04, 0.06, 0.08, 0.1\}$  and decrease with increasing excess noise.

shows our numerical results for the secret key rates of the postselected protocols: the RR scheme retrieves its advantage over the DR protocol by the introduction of a postselection step. However, it should be noted that this advantage declines with increasing excess noise. Finally, we compute an attainable secret key rates with two way communication and imperfect error correction and postselection. It has already been shown [3] that postselection can help RR protocols to perform stable under the effect of realistic error correction. Two-way communication can be included in our approach by disclosing all error positions to Eve. We assume that the practical error correction procedure can work as efficient as CASCADE. Figure (3) illustrates the robustness of the postselected protocols against non-ideal error correction. Moreover, it can be seen that the advantage of the one-way RR protocol over the attainable two-way protocol declines with increasing excess noise. This work has been published as [9].



**Figure 2:** Combination of postselection and reverse reconciliation. Secret key rates  $G$  are plotted for the PS-DR (dashed lines) and the PS-RR (solid lines) protocols and versus the channel loss  $1 - \eta$ . The excess noise  $\delta$  varies as  $\delta = \{0, 0.1, 0.2, 0.3\}$ .



**Figure 3:** Secret key rates  $G$  for postselected protocols using the two-way error correction scheme CASCADE (solid lines). For comparison, key rates for the PS-RR protocol with one-way codes, that are as efficient as CASCADE are also shown (dashed lines). The excess noise  $\delta$  varies between 0 and 0.1 as in Fig. (1).

- [1] Devetak, I. and Winter, A., Proc. of the Roy. Soc. of London Series A, **461**, 207 (2005)
- [2] Grosshans, F. *et al*, Nature, **421**, 238 (2003)
- [3] Heid, M. and Lütkenhaus, N., Phys. Rev. A **73**, 052316 (2006)
- [4] Renner, R. and Cirac, J. I., arXiv:0809.2243
- [5] Renner, R., PhD thesis, quant-ph/0512258
- [6] Leverrier, A. *et al.*, arXiv:0809.2252
- [7] Lorenz, S., Korolkova, N. and Leuchs, G., Appl. Phys. B **79**, 273 (2004)
- [8] Lorenz, S. *et al.*, Phys. Rev. A **74**, 042326 (2006)
- [9] Heid, M. and Lütkenhaus, N., Phys. Rev. A **76**, 022313 (2007)