

Quantum Key Distribution with Multi Letter Phase-Shift Keying

Denis Sych and Gerd Leuchs

Institute of Optics, Information and Photonics, Max Planck Research Group, University of Erlangen-Nuremberg, Günther-Scharowsky-Str. 1, Building 24, 91058 Erlangen, Germany
denis.sych@physik.uni-erlangen.de

Abstract

We present a new protocol for quantum key distribution using discrete phase-shift encoding with continuous variables. The novelty of the protocol is multi letter alphabets represented by coherent states of light with fixed amplitude and variable phase. Information is encoded in the phase of a coherent states which can be chosen from a regular discrete set consisting of an arbitrary number of letters. We evaluate the security of the protocol against the beam splitting attack. As a results we show the advantage of the proposed protocol over the standard two letter coherent state protocol, especially in the case when losses in the communication channel are low.

Introduction

In the case of discrete variables it has been shown that extensions of the standard BB84 [1] to higher dimensions or to higher number of letters in the alphabet can improve secrecy of QKD [2, 3]. In the case of continuous variables (CV QKD) the protocol based on two coherent states encoding [4] is a CV analogy of the discrete B92 protocol [5]. Based on the idea of improving properties of QKD by use of higher number of letters in a quantum alphabet [6], we perform a straightforward generalization of the two states CV QKD protocol [4] to a higher number of states. Namely, instead of just two coherent states $|\pm\alpha\rangle$ which have phases 0 and π , we use N coherent states $|\alpha_k\rangle=|a \exp(2\pi k/N)\rangle$ which have different phases $(2\pi k)/N$ and a fixed amplitude a . We show how the number of letters affects the security of the protocol.

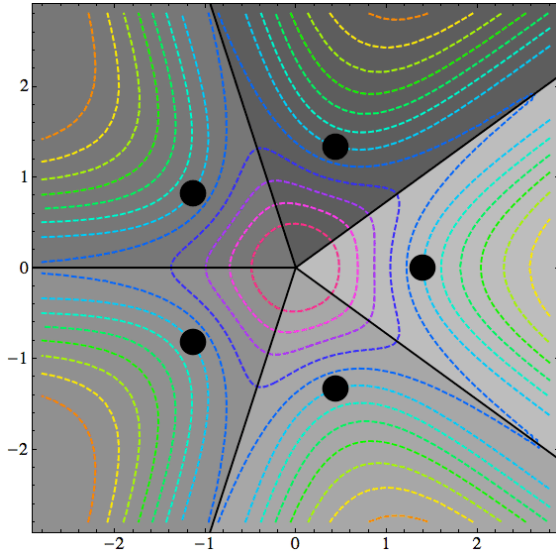


Figure 1: Phase space representation of the 5 letter protocol. Dots represent letters (coherent states with the amplitude $a=1.4$). Regions, where a measured value is assigned with a certain number, are shown as greyshaded sectors. Colourful dashed lines show borders of the post selection area for different values of attenuation.

Description of the protocol

The sender (Alice) chooses a random letter k and sends the respective coherent state $|\alpha_k\rangle=|a \exp(2\pi k/N)\rangle$. The receiver (Bob) obtains a state $|\beta\rangle$ using a double homodyne measurement. Then he assigns a classical number m to the measured state $|\beta\rangle$ by finding the maximal value of $|\langle\alpha_m|\beta\rangle|^2$ among the alphabet. In phase space representation the alphabet looks like a regular constellation, and the region, where a state $|\alpha_m\rangle$ is assigned to the result of Bob's measurement $|\beta\rangle$, looks like a sector with an angle $2\pi/N$. As an example we show a 5 letter alphabet in Fig. 1 and its Q-function in Fig. 2.

After the measurement Bob can use the post selection idea [4], when he decides whether to keep the transaction depending on the value $|\beta\rangle$. It is quite intuitive that if the measured state $|\beta\rangle$ is close to the centre of phase space or to the border between neighbouring sectors, the probability to confuse the transmitted letter k with the reconstructed value m is higher then if $|\beta\rangle$ lies in the centre of sector. Thus Bob's information significantly depends on the value of $|\beta\rangle$. If Bob omits the low-informational part of trans-

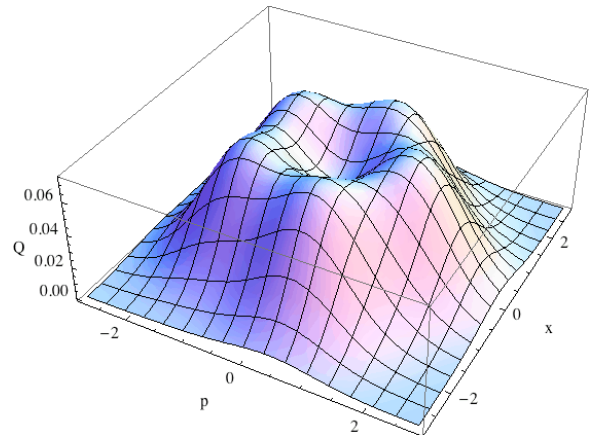


Figure 2: Phase space representation of the Q-function of the 5 letter protocol with the amplitude $a=1.4$ and the channel transmittance $\eta=1$ (loss-less case).

actions, he can increase the average information per transaction of the remaining part. As an example we show the exact post selection regions for the 5 letter protocol and for different values of attenuation using the fixed amplitude $a=1.4$ (dashed colourful lines in Fig. 1).

Security analysis

We investigate the security of our protocol against the beam splitting attack [7]. Although this is not the most general and optimal strategy of eavesdropping, it has perfectly agreed with experimental observations. The reason for this is that by beam splitting Eve does not introduce any additional noise on Bob's side, whereas in a more advanced strategies, where Eve creates entanglement with Bob, there is an excess noise on Bob's side. In real communication lines, like optical fibres or free space, excess noise is introduced mainly by imperfections of the experimental setup, and there is almost no excess noise due the channel itself. If the absence of excess noise is checked in experiment, then the eavesdropping strategy based on beam splitting is a quite adequate security proof.

To calculate the secret key rate G we assume that Bob uses double homodyne detection and Eve is not restricted to any practical way of information extraction, thus her potential knowledge is bounded by the Holevo information [8]. For each value of transmittance we optimize the amplitude of the initial signal to maximize the key rate G .

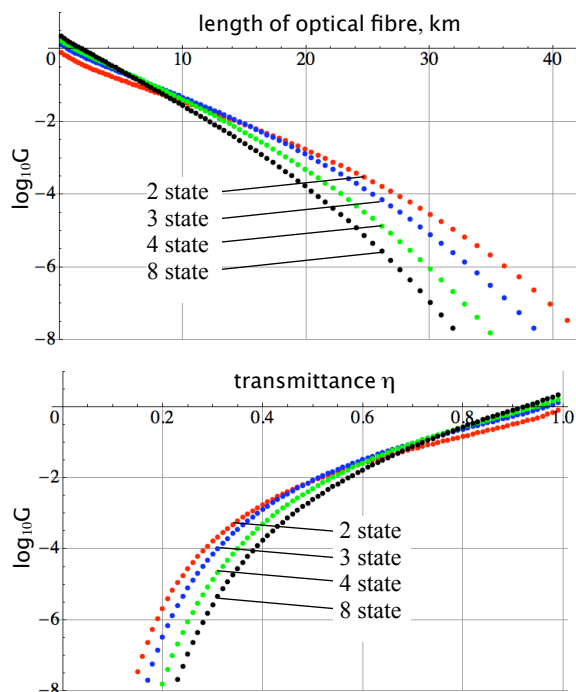


Figure 3: Secret key rate G in \log_{10} scale for 2, 3, 4 and 8 state alphabets after post selection as a function of transmittance (bottom) and length of optical fibre (top).

Results

The calculated secret key rates G for several alphabets are shown in Fig. 3. It is quite interesting that for different values of transmittance there are different optimal alphabets. The intuitive explanation is the following. In the case of low losses Eve has little information, and Alice can increase the amplitude of the signal. With higher amplitude Bob can better distinguish between many letters and increase his information. In the classical limit Bob can get $\log_2 N$ bit per transaction. Therefore, the more letters in the alphabet are, the higher Bob's information is. Thus QKD with multi letter alphabets has an essential advantage over the standard two letter QKD in the case of high transmittance.

On the other hand, when losses are high and the amplitude of the signal is low, it is harder to distinguish between many letters and Bob's information essentially drops, which significantly decreases the key rate. In this case the protocol with minimum number of letters outperforms the multi letter protocol.

We derive the optimal number of letters (among the presented on the Fig. 3): $0 < \eta < 0.5 - 2$, $0.5 < \eta < 0.7 - 3$, $0.7 < \eta < 0.8 - 4$, and $\eta > 0.8 - 8$ letters.

Conclusions and Outlook

We have presented a new CV QKD protocol based on multi letter alphabets. The protocol is shown to be better than the standard two letter protocol under certain conditions.

The future plan is to investigate other ways of post processing, which can further increase the secret key rate of the multi letter protocol.

Another direction of future theoretical research is to investigate other alphabet geometry, different from the constellation-type, and to derive the ultimate security proof for the protocols.

On the practical side, we plan to implement the protocol in experiment both in fibre based and free space channels.

References

1. C. Bennett and G. Brassard, in Proceedings IEEE Int. Conf. on Computers, Systems and Signal Processing, Bangalore, India; IEEE, New York, (1984), 175
2. N. Cerf *et al*, Phys. Rev. Lett. **88** (2002), 127902
3. D. Sych *et al*, Phys. Rev. A **70** (2004), 052331
4. C. Silberhorn *et al*, Phys. Rev. Lett. **89** (2002), 167901
5. C. Bennett, Phys. Rev. Lett. **68** (1992), 3121
6. D. Sych *et al*, Quant. Electron. **35** (2005), 80
7. M. Heid *et al*, Phys. Rev. A **73** (2006), 052316
8. A. Holevo, Probl. Inf. Trans. **9** (1973), 177