Security analysis of continuous-variable quantum key distribution using m-PSK classical modulation schemes

Yupeng Gong[1], Anran Jin[1], He Li[1], Adrian Wonfor[1] and Richard Penty[1]
[1]*Centre for Advanced Photonics and Electronics, 9 JJ Thomson Ave, University of Cambridge, Cambridge, CB3 0FA*
yg311@cam.ac.uk

Abstract: We theoretically prove the security of using classical m-psk modulation protocol for the transmission of continuous-variable quantum key distribution and discuss the performance of classical digital communication protocols for CVQKD

OCIS codes: Quantum communications (270.5565), Quantum cryptography (270.5568), Quantum information and processing (270.5585)

1. Introduction

Quantum key distribution (QKD), one of the most mature applications of quantum information theory, allows two authenticated users, Alice and Bob to share a sequence of random numbers for classical symmetric encryption over an insecure channel [1]. QKD can be categorized into two classes of protocols, namely continuous variable (CV) and discrete variable (DV) protocols, based on the dimension of the Hilbert space that the information is encoded onto. Unlike DVQKD which has a rather complete security analysis for different protocols against coherent attacks [1], only the Gaussian modulated CVQKD protocol has been proved theoretically secure based on Gaussian optimality [2]. However, CVQKD using discrete modulation (DM) has many intrinsic advantages in practical applications, e.g., more compatible with classical coherent communication technologies, potentially higher key rate and easier post-processing and error correction. However, owing to the difficulty of security analysis for CV quantum states, the development of CVQKD using efficient classical digital communication schemes has been severely delayed.

In [3], convex optimization has been explored to prove the security of four-state CVQKD. By extending the security to higher dimensions, one could further enhance the secure key rate and exploit the merits of various classical digital communication protocols, e.g. m-PSK, QAM etc. In this paper, we present and compare the results of security analysis for CVQKD using m-PSK classical modulation schemes, i.e. BPSK, QPSK and 8PSK and discuss the potential advantages of using classical digital communication protocols for the generation of CV quantum keys.

The general process of m-PSK CVQKD can be summarized as follows:

1. *Quantum state preparation*: Alice prepares coherent state $\left|\alpha e^{i\frac{2\pi k}{m}}\right\rangle$ according to the probability, where m is m-PSK modulation, and α is the amplitude of the coherent state. E.g., for BPSK modulation, Alice sends coherent state $|\alpha\rangle$ and $|-\alpha\rangle$ to Bob with 50% probability over a quantum channel.
2. *Measurement*: Bob measures the received state using homodyne detection. With probability p_B, Bob chooses to measure the x or p quadrature.
3. *Sifting and parameter estimation*: After N rounds of communication, Alice and Bob communicate via a classical authenticated channel to disclose the quadrature Bob chose to measure and Alice reveals a small subset of her states to Bob for estimating the channel security condition.
4. *Information reconciliation and privacy amplification*: Bob performs a key map with certain post-selection thresholds over his received quantum states of his raw keys. Then Alice and Bob communicate via a classical channel using classical error correction and privacy amplification process to agree on a series of final key.

2. Security analysis method

A general method for proving the security of quantum key distribution is based on the proving a non-zero key rate using the Devetak-Winter formula [4] against collective attacks. And in the reverse reconciliation case, the equation is given by

$$R^{\infty} = p_{pass}[I(A;B) - \max_{\rho \in S} \chi(B:E)], \qquad (1)$$

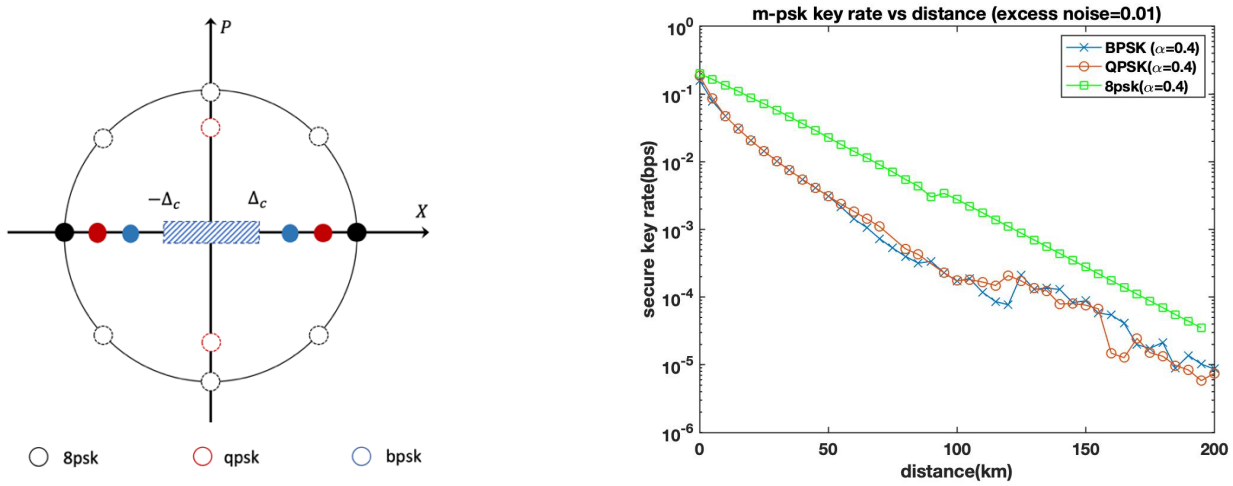
where p_{pass} is the postprocessing probability, $I(X;Z)$ is the classical mutual information between Alice and Bob's string, and $\max_{\rho \in S} \chi(B:E)$ is the maximum Holevo information that quantifies Eve's knowledge of Bob's information. The set S includes all possible density matrices regarding the quantum states received by Bob. As discussed in [3], this problem can be converted into a convex optimization problem by using the quantum relative entropy as:

$$R^{\infty} = \min_{\rho_{AB} \in S} D(\mathcal{G}(\rho_{AB}) || \mathcal{Z}[\mathcal{G}(\rho_{AB})]) - p_{pass}\delta_{EC}, \qquad (2)$$

where the function $D(\rho||\sigma)$ is the quantum relative entropy, the function $\mathcal{G}(\rho_{AB})$ is the function that describes the post-processing, detection, key mapping step of Bob's system, the function $\mathcal{Z}[\mathcal{G}(\rho_{AB})]$ is the readout process of the key mapping and δ_{EC} is the classical error between Alice's and Bob's information.

Specifically, we first find a near minimum value of $\min_{\rho_{AB}\in S} D(\mathcal{G}(\rho_{AB})||\mathcal{Z}[\mathcal{G}(\rho_{AB})])$ over all possible density matrices in the feasible set using semidefinite programming, and then convert it to a reliable lower bound of the minimum value based on duality [5]. If the reliable lower-bound of the minimum key is non-zero, we thus prove the security of the corresponding protocol. The detailed constraints and approximation methods that we employed in the analysis will be discussed at the conference.

3. Results and discussion



(a) (b)

Figure 1: (a) Constellation diagram for BPSK, QPSK and 8PSK CVQKD, where the black, red and blue circle represent the 8PSK, QPSK and BPSK respectively. The dashed area is the post-selection area for no-key generation. (b) The secure key rate for BPSK, QPSK and 8PSK CVQKD using homodyne detection

In this section, we present our convex optimization based security analysis of CVQKD with BPSK, QPSK, and 8PSK modulation schemes. In figure 1(a), we illustrate the constellation diagram, key mapping and post-selection thresholds of our analyzed protocols. For example, in the 8PSK scheme (black circles), eight states are employed which are shown on the outer circle. In addition, the hollow circles represent the states used for channel security estimation and only the filled circle, i.e. state $|\boldsymbol{\alpha}\rangle$ and $|-\boldsymbol{\alpha}\rangle$ are used for secure key generation. In the middle, the post-selection threshold (dashed area) could be defined to further enhance the key rate to remove states with higher error rates. To calculate the convex optimization problem, the feasible region of $\boldsymbol{\rho_{AB}}$ is confined by the sent and received quantum states' properties, e.g. being semidefinite and satisfy the quadrature operators.

In figure 1(b), the secure key rates at different distances are shown for the three modulation scheme with the same parameters, i.e. fixed state $\boldsymbol{\alpha = 0.4}$, excess noise $\boldsymbol{\xi = 0.01}$, with the same post-selection threshold and fixed calculation precision. As can be seen, all three protocols are proved secure over a 200km channel (40dB). In addition, the 8PSK protocol has the highest secure key rate while QPSK and BPSK have a similar secure key rate. This is because for 8PSK, 6 additional states are employed for channel parameter estimation and generate a much tighter lower bound over the feasible set. It is noteworthy that, even for the BPSK protocol, both $\langle\hat{\boldsymbol{x}}\rangle$ and $\langle\hat{\boldsymbol{p}}\rangle$ quadratures are measured and used for parameter estimation, causing the protocol to have a similar feasible region as QPSK and resulting in similar key rate. In our calculation, we assume an asymmetric key generation where Alice doesn't send the states with equal probability and most of the states are $|\boldsymbol{\alpha}\rangle$ and $|-\boldsymbol{\alpha}\rangle$ for an optimal key rate.

In conclusion, we have successfully proved the security of CVQKD using classical m-PSK modulation scheme. In addition, this method can be further extended to higher dimensions, e.g., 16PSK or including amplitude modulation also, e.g., 16QAM. Moreover, by simply changing the key mapping and post-selection threshold, the feasible region can be confined tighter with an even higher secure key rate.

Acknowledgement: This work has been funded by the UK EPSRC Quantum Communications Hub EP/T001011/1.

Reference

1. Xu, F., et al., *Secure quantum key distribution with realistic devices.* Reviews of Modern Physics, 2020. **92**(2): p. 025002.
2. García-Patrón, R. and N.J. Cerf, *Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution.* Physical Review Letters, 2006. **97**(19): p. 190503.
3. Lin, J., T. Upadhyaya, and N. Lütkenhaus, *Asymptotic Security Analysis of Discrete-Modulated Continuous-Variable Quantum Key Distribution.* Physical Review X, 2019. **9**(4): p. 041064.
4. Devetak, I. and Winter, A., *Distillation of Secret Key and Entanglement from Quantum States*, Proc. R. Soc. A, 2005. 461, 207
5. Boyd, S. and L. Vandenberghe, *Convex Optimization*. 2004, Cambridge: Cambridge University Press.