|VI WECIQ>

VI Workshop Escola de Computação e Informação Quântica

Unifal MG Universidade Federal de Alfenas

Secret Key Rates of CVQKD Protocols with Gauss-Quadrature Constellations

Micael Andrade Dias[1], Francisco Marcos de Assis[2]

Federal University of Campina Grande, PB, Brazil

micael.souza@ee.ufcg.edu.br[1], fmarcos@dee.ufcg.edu.br[2]

Abstract

Research in the quantum key distribution (QKD) field has turned to the analysis of protocols using continuous-variable (CV) quantum states with discrete modulation (DM) schemes to generate random secret cryptographic keys, called DM-CVQKD protocols. Despite these protocols being experimentaly convenient, it comes with pertinent open problems concerning the protocol security against arbitrary attacks and which constellations best optimize the protocol's performance. In this extended abstract, we present a QAM constellation based on the Gauss-quadrature modulation and use the results in [2] to compute a lower bound to the secret key rate.

Key-Worlds: Semidefinite Programming, Gauss-Quadrature Constellation, DM-CVQKD.

Introduction

Given a constellation of coherent states with amplitudes α_k and probability distribution p_k, Alice's state is in the mixture represented by $\tau = \sum_k p_k \left|\alpha_k\right\rangle\!\left\langle\alpha_k\right|$, which are transmitted to Bob through the quantum channel. Bob, in his turn, measures the received states and, based on his measurements, Alice and him must infer if it is secure to distill a secret key. This security analysis is better accessed by an equivalent entangled-based protocol. In this case, Alice prepares a bipartite state $\left|\Phi\right\rangle_{AA'}$ which it is a purification of the modulation τ. The problem is, given the observations β_k of Bob, to estimate the correlations between Alice and Bob without making any assumptions about the channel connecting Alice and Bob represented by the map $\mathcal{N}_{A'\to B}$ that transforms the initial state as

$$\hat{\rho}_{AB} = (\mathbb{1}_A \otimes \mathcal{N}_{A'\to B})(\left|\Phi\right\rangle\!\left\langle\Phi\right|_{AA'}). \tag{1}$$

Objectives

Compare the performance of several m-QAM like constellations concerning the secret key rate of CVQKD protocols, given by

$$K = \beta I(X;Y) - \sup_{\mathcal{N}_{A'\to B}} \chi(Y;E) \tag{2}$$

Secret Key Rate Computation

The secret key rate is a function of an upper bound on the eavesdroppper information, which is obtained by lower bounding the correlation between Alice and Bob. One solution for this problem were provided in [2], where the authors defined the following semidefinite program (SDP)

$$\begin{aligned} \text{minimize} \quad & \operatorname{tr}\Big((\hat{\mathbf{a}}\hat{\mathbf{b}} + \hat{\mathbf{a}}^\dagger\hat{\mathbf{b}}^\dagger)\cdot\hat{\rho}_{AB}\Big) \\ \text{subject to} \quad & \operatorname{tr}_B(\hat{\rho}_{AB}) = \tau, \\ & \operatorname{tr}\Big(\hat{\rho}_{AB}(\Pi\otimes\hat{\mathbf{b}}^\dagger\hat{\mathbf{b}})\Big) = n_B, \\ & \operatorname{tr}(\hat{\rho}_{AB}(\textstyle\sum_k \overline{\langle\alpha_k|\hat{\mathbf{a}}_\tau|\alpha_k\rangle}\,|\psi_k\rangle\!\langle\psi_k|\otimes\hat{\mathbf{b}} + \text{h.c.})) = c_1, \\ & \operatorname{tr}(\hat{\rho}_{AB}(\textstyle\sum_k \bar{\alpha}_k\,|\psi_k\rangle\!\langle\psi_k|\otimes\hat{\mathbf{b}} + \text{h.c.})) = c_2, \\ & \hat{\rho}_{AB} \succeq 0. \end{aligned} \tag{3}$$

where $\hat{\mathbf{a}}\hat{\mathbf{b}} + \hat{\mathbf{a}}^\dagger\hat{\mathbf{b}}^\dagger$ is the operator corresponding to the covariance therm of the covariance matrix of $\hat{\rho}_{AB}$, $\hat{\mathbf{a}}_\tau = \tau^{1/2}\hat{\mathbf{a}}\tau^{-1/2}$, $\Pi = \sum_k |\psi_k\rangle\!\langle\psi_k|$ is a projector on the relevant subspace of τ with orthonormal bases $|\psi_k\rangle$, n_B is the average energy measured by Bob and c_1 and c_2 correlation quantities that can be experimentally estimated with $c_1 = \operatorname{Re}\Big\{\sum_k p_k \overline{\langle\alpha_k|\hat{\mathbf{a}}_\tau|\alpha_k\rangle}\beta_k\Big\}$ and $c_2 = \operatorname{Re}\{\sum_k p_k\bar{\alpha}_k\beta_k\}$.

Results

We aim to use the bounds provided by the semidefinite program and compare the performance of the constellations presented in [2] with a Gauss-Quadrature QAM-like constellation. The Gauss-quadrature constellation is defined as follows [3]. For a standard Gaussian density function $p_X(x) = \frac{1}{\sqrt{2\pi}}e^{-x^2/2}$, we denote the N-th Hermite polynomial H_N and the set of weights $\{w_{i,N}\}$ obtained by the N roots $\{x_{i,N}\}$ of H_N. Then, the Gauss quadrature constellation (GQ) is made up of the amplitudes $\mathcal{A}_{GQ} = \{x_{i,N}\}$ and the probability distribution $\mathcal{P}_{GQ} = \{w_{i,N}\}$. As the N roots $\{x_{i,N}\}$ are real valued, a QAM constellation is obtained by the Cartesian product $\mathcal{A}_{GQ}\times\mathcal{A}_{GQ}$. In Figures 1 and 2 we potted the SKR for the GQ m-QAM constellation, alongside the constellations presented in [2], using the lower bound provided by the SDP.

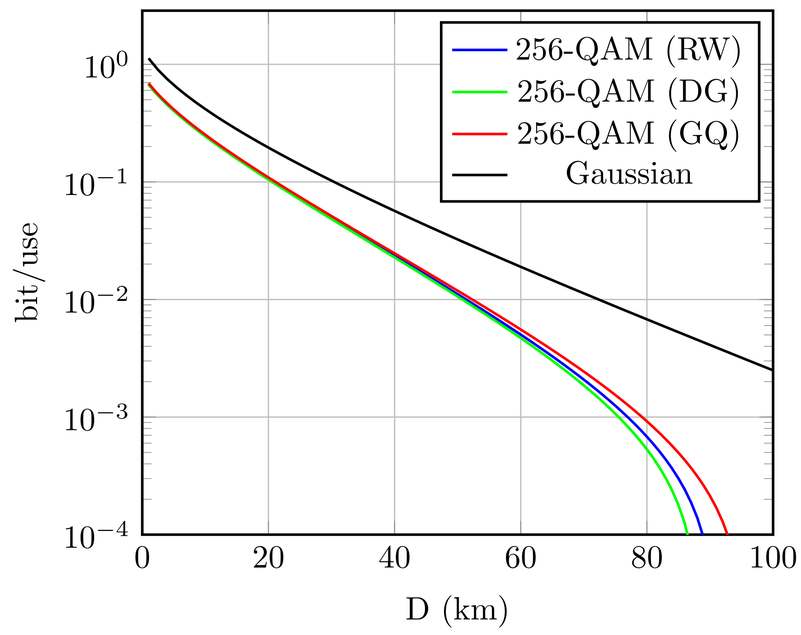

Figura 1: Secret key rate lower bounds for the DG, RW and GQ constellations. The simulated parameters were $\beta = 0.95$, $\xi = 0.06$, $T = 10^{-0.02D}$ and $V_A = 3.8$.

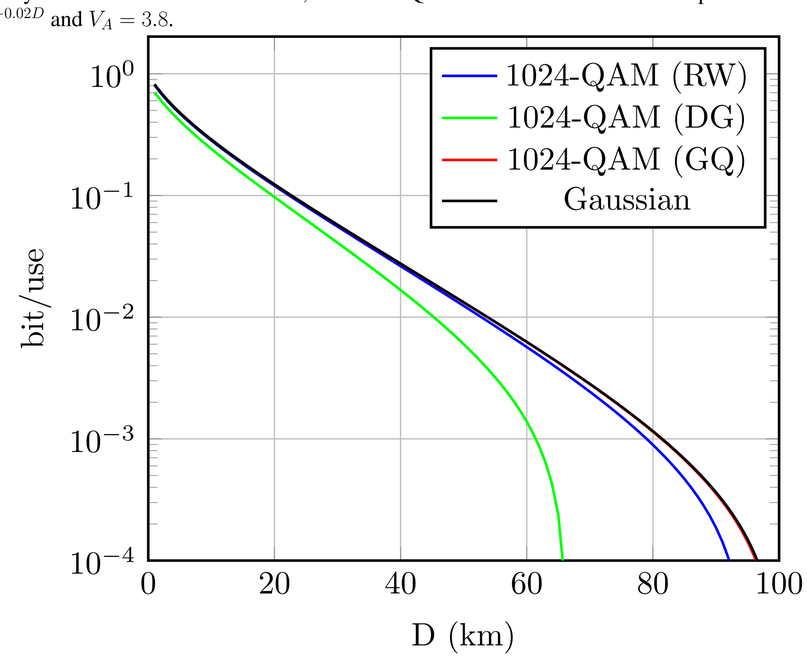

Figura 2: Secret key rate lower bounds for the DG, RW and GQ constellations. The simulated parameters were $\beta = 0.95$, $\xi = 0.06$, $T = 10^{-0.02D}$ and $V_A = 5$.

Conclusions

We plotted in Figures 1 and 2 the secret key rate computed with the SDP for the Gauss-quadrature QAM constellation, as defined above, and compared with the constellations presented in [2], witch are the discrete Gaussian distribution (DG) and the normalized random walk (RW). The results show that the proposed constellation outperforms both the DG and RW and approximates the continuous Gaussian modulation, being almost indistinguishable when the the constellation size is 1024.

Referências

[1] M. A. Dias and F. M. de Assis, "The impact of constellation cardinality on discrete unidimensional CVQKD protocols," Quantum Inf Process, vol. 20, no. 9, p. 284, Sep. 2021, doi: 10.1007/s11128-021-03222-w.

[2] A. Denys, P. Brown, and A. Leverrier, "Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation," Quantum, vol. 5, p. 540, Sep. 2021, doi: 10.22331/q-2021-09-13-540.

[3] Y. Wu and S. Verdú, "The impact of constellation cardinality on gaussian channel capacity," 2010 48th Annual Allerton Conference on Communication, Control, and Computing, Allerton 2010, pp. 620–628, 2010, doi: 10.1109/ALLERTON.2010.5706965.