Parameter Analysis in Continuous-Variable Quantum Key Distribution with Arbitrary Modulation

João dos Reis Frazão[1], Aaron Albores-Mejia[1], Boris Škorić[1], and Chigo Okonkwo[1]

[1] Eindhoven Hendrik Casimir Institute, Eindhoven University of Technology, the Netherlands

Continuous-variable quantum key distribution (CV-QKD) represents a solution to distribute quantum-secure secret random keys, where weak coherent states can be encoded with Gaussian or discrete modulation. Using readily available and mature commercial off-the-shelf components, it is possible to achieve high secret key rates for practical short-reach optical communications. From the security proof perspective, it is possible to analyse the Gaussian modulation performance considering finite size effects. More recently, a security proof for arbitrary discrete modulation was proposed, but only in the asymptotic regime. In this work, finite size effects and confidence intervals are included in the models in order to get realistic bounds for relevant hardware implementation parameters for CV-QKD with arbitrary modulation. Furthermore, the optimum secret key rates were studied according to different Alice/Bob implementation parameters such as receiver clearance, channel loss, system excess noise, signal/LO lasers phase noise, signal modulation variance and quantum/calibration data lengths, with the Gaussian linear channel assumption.

Introduction

The first CV-QKD protocol to make use of coherent states with Gaussian modulation [1] was introduced in 2002, with security against individual attacks. The security proof was further extended and improved to that of composable security against collective and coherent attacks in [2]. In order to lower the complexity of CV-QKD, discrete modulation formats like BPSK and QPSK have been proposed in [3] considering security against collective attacks. However, their performance is reduced when compared to Gaussian modulation, due to the lower cardinality of BPSK and QPSK. To close the gap between Gaussian and discrete modulations, an analytical bound for the asymptotic secret key ratio (SKR) of protocols with arbitrary modulation has been proposed [4]. In this work, we analyse such analytical bounds under a realistic scenario with trusted noise and finite-size effects.

Protocol & optimisation

In CV-QKD, Alice starts the protocol by randomly encoding a finite number of weak coherent states, according to the modulation format and optimised modulation variance (V_A). She transmits the data to Bob via the quantum channel, that has a length/loss according to each use case. To measure the quantum states, Bob uses double homodyne detection with maximised quantum efficiency and optimised clearance, the ratio between receiver shot and electronic noise. Excess noise due to Alice's equipment or Eve's attack cannot be distinguished or calibrated. For the post-processing steps, Alice and Bob use an authenticated classical channel to publicly share information for parameter estimation, error correction (EC) and privacy amplification (PA). In parameter estimation, Alice and Bob estimate the secret key ratio by publicly revealing 50% of the data. Here, the quantum block length needs to be optimised according to the impact of finite-size effects and limitations of the system. Lastly, Alice and Bob perform error correction and privacy amplification to make sure they have the same key and to minimize Eve's potential knowledge. In error correction and privacy amplification, the algorithms need to be as

efficient as possible to prevent further degradation of the protocol's performance. The key management service (KMS) should be implemented with minimized key consumption processes. A summary of the parameter requirements is presented in Table 1, where the ↑ and ↓ mean maximize and minimize, while ∗ means the parameter requires optimisation according to theoretical model or use case.

Transmitter (Alice)	Quantum channel	Receiver (Bob)	Post-Processing
Modulation Format ↑	Distance ↑	Clearance ∗	Block length∗
Modulation Variance ∗	Fiber type	Quantum Efficiency ↑	EC/PA efficiency ↑
Symbolrate ∗	Channel Loss ↓	Total Excess Noise ↓	KMS consumption ↓

Tab. 1: CV-QKD requirements for transmitter, quantum channel, receiver and post-processing.

Gaussian channel & Finite-size effects

This paper uses the assumption that Alice's (x) and Bob's (y) data follow the normal linear model: $y = tx + z$ with $t = \sqrt{\eta T/2}$ and Gaussian noise z, with variance $\sigma_z^2 = \frac{\eta T}{2}\xi_A + N_0 + \nu_{el}$.Where T corresponds to the transmittance of the channel, $N_0 + \nu_{el}$ the receiver trusted noise and ξ_A the excess noise at Alice's output, where the optimal attack by Eve is performed. Finite-size effects are considered according to [5]. A lower bound on the secret key ratio is obtained assuming the worst-case estimators with confidence intervals for excess noise, transmittance and trusted noise. The following expression is used to evaluate the secret key ratio assuming reverse reconciliation and collective attacks with ϵ security : $K_{finite} = \frac{n}{N}[\beta I_{BA} - \chi_{EB} - \Delta]$. The fraction $\frac{n}{N}$ is the amount of data after parameter estimation, β the reconciliation efficiency, I_{BA} the mutual information between Alice and Bob, χ_{EB} the Holevo bound and Δ a parameter related to the security of privacy amplification. The analytical bound for a discrete modulation format is given in [4].

Receiver Trusted Noise

In a realistic CV-QKD scenario, one can assume that the receiver side is safe from an attacker (Eve)[3]. This means Bob operates under the trusted noise assumption and calibrates his detectors regularly by disconnecting the quantum channel and measuring his total and electronic receiver noise with the LO on and off, respectively [6]. Bob can further analyse the shot noise and clearance levels of the receiver to calibrate his data accordingly. From the perspective of a theoretical model, the trusted quantities are perceived as quantum efficiency η, shot noise N_0 and electronic noise ν_{el}. These parameters are used to obtain the final excess noise expression: $\xi_A = \frac{2}{\eta T}(\sigma_z^2 - N_0 - \nu_{el})$.

Modulation Format

At the transmitter, Alice needs to either implement a Gaussian or discrete modulation format. In Gaussian modulation, the coherent state is an arbitrary complex number chosen according to a Gaussian probability distribution. One discrete example is quadrature amplitude modulation (QAM), where the constellation consists of M points distributed over a square grid. It is important that each coordinate of the coherent state is chosen independently according to a discrete Gaussian distribution (Probabilistic Constellation Shaping). The coherent states are centered at M possible equidistant points of the form $\alpha = x + ip$ with probability: $p_{x,p} \approx exp(-\nu(x^2 + p^2))$. By fixing the overall variance per coordinate to $\frac{Va}{4}$, the probability distribution depends only on the free parameter ν, which is numerically optimised according to Fig. 1a. An analysis of the impact of the worst-case assumption and clearance levels is given in Fig. 2, with enhanced ν for 64/256 QAM.

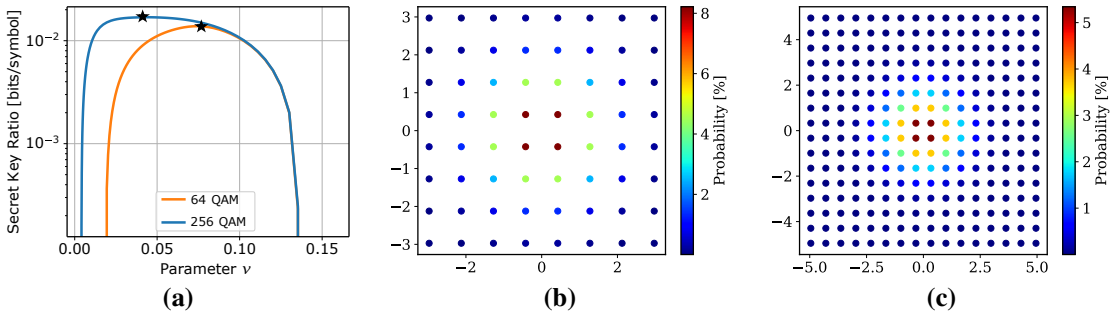

Fig. 1: (a) Optimisation of ν for maximum secret key ratios. Fixed parameters: distance = 30 km, $\alpha = 0.2$ dB/km, $V_A = 4.6$ SNU, $\xi_B = 0.01$ SNU, $\nu_{el} = 0.05$ SNU, $N = 2 \times 10^7$, $N_{cal} = 10^6$, $\eta = 60\%$, $\beta = 95\%$, $\epsilon = 10^{-10}$. (b) Probabilistic constellation shaping 64 QAM with $\nu = 0.0747$. (c) Probabilistic constellation shaping 256 QAM with $\nu = 0.046$.

Residual Phase noise

Initial CV-QKD implementations multiplexed the quantum signal with strong transmitter-side LO (TLO). This, enables a shot-noise calibration attack on the distributed LO, compromising the security [7]. To circumvent this problem, Bob uses an independent laser to provide the LO (LLO). With pilot-tone-aided techniques, Bob can recover the relative phase between both lasers. Even so, excess phase noise exists which cannot be compensated [8] given by: $\xi_{phase} = 2V_A(1 - e^{-V_{est}/2})$ where, V_{est} is the variance of the residual phase noise after phase estimation/correction. For a sequential-LLO scheme, V_{est} depends on, the symbol rate, the amplitude of reference signal (or pilot) and the sum of the linewidths of the two free-running lasers. In order to minimize the impact of ξ_{phase} on the secret key ratio, these parameters need to be optimised as shown in Fig. 3.

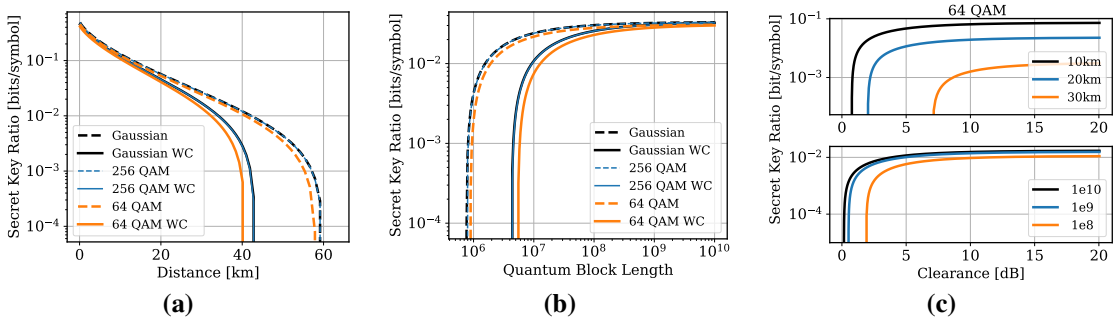

Fig. 2: (a) Impact of worst-case (WC) scenario on SKR vs Distance. (b) Worst-case analysis of SKR vs Quantum block length. (c) SKR for 64 QAM Modulation versus Clearance for different transmission distances and block lengths. Same fixed parameters as Fig. 1.

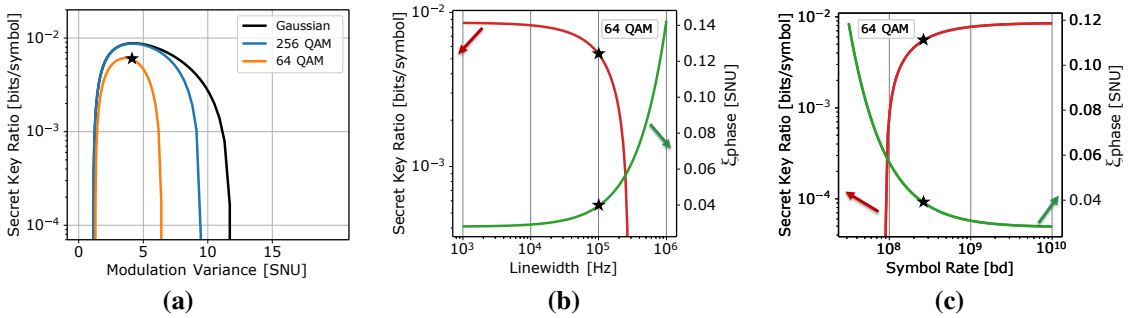

Fig. 3: (a) Comparison of SKR vs V_A for different modulation formats. (b) SKR (left) and ξ_{phase} (right) variation with LO linewidth. (c) SKR (left) and ξ_{phase} (right) for different symbol rates. Same fixed parameters as Fig. 1 with 250 Mbaud and 50 kHz linewidth for both lasers.

Results

The star symbol in each plot represents the input value in the theoretical model. For the optimisation of the modulation format, in Fig. 1a, ν is chosen according to the maximum secret key ratio, given the fixed parameters. For 64/256 QAM ν is equal to 0.0747 and 0.046, respectively.

In Fig. 2 we can see the impact of the worst-case estimators on the secret key ratio, with transmission distance in Fig. 2a and quantum block length in Fig. 2b. The larger the block size ($> 10^8$), the less the finite size effects will deteriorate the performance of CV-QKD. However, if the block size is increased, eventually hardware memory and processing speeds will not be sufficient for a realistic implementation. Also, the higher the modulation format the closer performance is to Gaussian, as expected from [4]. The clearance analysis is given in Fig. 2c, where we note that for large distances (>30 km) and reasonable block sizes (2×10^7) high-end low noise receivers will be required. Additionally, if the receiver clearance is low, trade-offs are required by increasing block lengths.

On the transmitter side, Alice optimises the modulation variance according to the security proof and excess phase noise Fig. 3a. For this plot, the increasing excess noise is considered as we increase the modulation variance, and the used optimum value is 4.6 SNU for 30 km and $N = 2 \times 10^7$. Further optimisation to minimize the excess phase noise can be achieved by reducing the linewidth < 10kHz and increasing symbol rates $> 10^8$, as seen in Fig. 3b and Fig. 3c.

Conclusion

In this paper, an in-depth multidimensional optimisation analysis is presented for a practical CV-QKD implementation focusing on modulation format, clearance, block length, symbol rate, linewidth and modulation variance. We showcase significant gains for the secret key ratio extraction in realistic cost-effective CV-QKD. To our knowledge, this is the first time that such optimisation analysis has been realized for these discrete modulation formats considering receiver trusted noise and finite-size effects.

This work was supported by the Dutch Ministry of Economic Affairs and Climate Policy (EZK), as part of the Quantum Delta NL programme.

References

[1] F. Grosshans and P. Grangier, "Continuous Variable Quantum Cryptography Using Coherent States",, vol. 88, no. 5, 057902, p. 057 902, 2002. DOI: 10.1103/PhysRevLett.88.057902.

[2] N. Jain, H.-M. Chin, H. Mani, *et al.*, "Practical continuous-variable quantum key distribution with composable security", *Nature Communications*, vol. 13, Aug. 2022. DOI: 10.1038/s41467-022-32161-y.

[3] A. Leverrier, "Theoretical study of continuous-variable quantum key distribution", Theses, Télécom ParisTech, 2009. [Online]. Available: https://pastel.archives-ouvertes.fr/tel-00451021.

[4] 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, 2021, ISSN: 2521-327X. DOI: 10.22331/q-2021-09-13-540.

[5] P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier, "Analysis of imperfections in practical continuous-variable quantum key distribution", *Phys. Rev. A*, vol. 86, p. 032 309, 3 2012.

[6] M. Rueckmann and C. G. Schaeffer, "Calibration of receiver noise in cv-qkd systems", in *Photonic Networks; 21th ITG-Symposium*, 2020, pp. 1–4.

[7] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, "Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution", *Phys. Rev. A*, vol. 87, p. 062 313, 6 2013. DOI: 10.1103/PhysRevA.87.062313.

[8] A. Marie and R. Alléaume, "Self-coherent phase reference sharing for continuous-variable quantum key distribution", *Phys. Rev. A*, vol. 95, p. 012 316, 1 2017. DOI: 10.1103/PhysRevA.95.012316.