CV-QKD Security Limits Using Higher-Order Probabilistic Shaped Regular M-APSK Constellations

Margarida Almeida[1,2], Daniel Pereira[1,2], Nelson J. Muga[1], Margarida Facão[3], Armando N. Pinto[1,2], Nuno A. Silva[1]

[1]Instituto de Telecomunicações, University of Aveiro,
Campus Universitário de Santiago, 3810-193, Aveiro, Portugal

[2]Department of Electronics, Telecommunications and Informatics, University of Aveiro,
Campus Universitário de Santiago, 3810-193, Aveiro, Portugal

[3]Department of Physics and I3N, University of Aveiro,
Campus Universitário de Santiago, 3810-193, Aveiro, Portugal

{mralmeida,danielfpereira,muga,mfacao,anp,nasilva}@ua.pt

Abstract. *In this work we study the performance of M-symbol (M-)Amplitude and Phase Shift Keying (APSK) constellations for Continuous-Variable Quantum Key Distribution systems. Despite the gap still observed between the performance of higher order regular M-APSK constellations with binomial distribution for probabilistic shaping and the optimal performance of Gaussian Modulation, regular 128-APSK's performance is better than irregular 256-APSK's and almost the same as for regular 256-APSK. Moreover, higher-order regular M-APSK is secure for longer distances and higher values of mean number of photons per symbol, and is more resistant to excess noise.*

1. Introduction

Quantum Key Distribution (QKD) can establish a secure key between two legitimate users of a communication system, often called Alice and Bob [Li et al. 2014]. This even against an eavesdropper with unlimited computing power [Bennett and Brassard 2014]. Continuous-Variable (CV)-QKD uses coherent states and coherent detection to provide high detection efficiencies and key rates [Ghorai et al. 2019]. Moreover, CV-QKD schemes are compatible with telecommunication's components [Huang et al. 2014], thus being very attractive for practical implementations.

The theoretically optimal Gaussian Modulation (GM) was initially proposed for CV-QKD [Grosshans and Grangier 2002, Ghorai et al. 2019]. However, its security proofs require ideal GM, which is very difficult to obtain in practice [Denys et al. 2021]. Discrete Modulation (DM) overcomes these limitations [Leverrier and Grangier 2011], being experimentally simpler to implement [Ghorai et al. 2019, Lin and Lütkenhaus 2020]. Early DM-CV-QKD protocols considered small-order constellations, such as 4-Phase Shift Keying (PSK) [Leverrier et al. 2010]. Nonetheless, their performance is far away from the one achievable with GM. Security proofs were obtained for arbitrary DM formats using semi-definite programs mainly in the asymptotic case [Ghorai et al. 2019]. Moreover, the use of semi-definite programs is computationally expensive, turning their application

beyond small M-symbol (M-)PSK constellations hardly achievable. [Denys et al. 2021] recently proposed an explicit analytical formula for the secret key rate of DM-CV-QKD, allowing the study of arbitrary modulation of coherent states. This allowed the study of M-Quadrature Amplitude Modulation (QAM) constellations in the asymptotic regime [Denys et al. 2021]. Nonetheless, M-QAM constellations require higher bandwidths and higher peak-to-average power ratios than M-Amplitude and Phase Shift Keying (APSK) constellations. Consequently, [Almeida et al. 2021] studied irregular M-APSK constellations in the finite-size scenario.

In this paper we applied higher-order regular M-APSK constellations to a CV-QKD system under the finite-size effect regime. We obtain security limits of probabilistic shaped higher-order M-APSK constellations, taking into account both the transmission distance and the excess noise. Irregular M-APSK's security bounds (studied in [Almeida et al. 2021]) were also computed for comparison purposes. We have considered the binomial distribution for probabilistic shaping. CV-QKD systems using regular M-APSK are more robust to eavesdropper attacks than systems using irregular M-APSK, being secure for longer distances. The present report is organized as follows. Section 2 briefly describes the computation of the security bounds of CV-QKD systems. Section 3 analyses the security limits of considering higher-order probabilistic shaped regular and irregular M-APSK. Finally, Section 4 summarizes the main conclusions.

2. Discrete Modulation CV-QKD Security Bounds

In the quantum channel, Alice and Bob only share a finite number of states, N, upper bounding the secret key rate of the CV-QKD system as [Leverrier et al. 2010]

$$K = \frac{n}{N}\left[\beta I_{\mathrm{BA}} - \chi_{\mathrm{BE}} - \Delta\left(n\right)\right]. \tag{1}$$

Here n is the number of states allocated to information reconciliation, β is the reconciliation efficiency, I_{BA} is the mutual information between Bob and Alice, and χ_{BE} is the Holevo bound between Bob and Eve, assuming reverse reconciliation. The impossibility of transmitting an infinite number of states is associated to a worst estimation of the channel transmission and excess noise. This can be accounted for by considering the lower and upper bound of the channel transmission and excess noise, respectively, with a probability of at least $1 - \epsilon_{\mathrm{PE}}$, as provided in [Leverrier et al. 2010]. The finite-size effects related with the privacy amplification step are accounted for in $\Delta\left(n\right)$, which is given by

$$\Delta\left(n\right) = 7\sqrt{\frac{\log_2\left(2/\bar{\epsilon}\right)}{n}} + \frac{2}{n}\log_2\left(1/\epsilon_{\mathrm{PA}}\right), \tag{2}$$

where $\bar{\epsilon}$ is a *smoothing* parameter, and ϵ_{PA} is the failure probability of the privacy amplification procedure [Leverrier et al. 2010]. The mutual information between Alice and Bob, I_{BA}, for GM can be found in [Almeida et al. 2021], while the computation of the mutual information between Alice and Bob for DM, namely M-APSK constellations, can be found in [Essiambre et al. 2010]. The Holevo bound between Bob and Eve is computed as described in [Almeida et al. 2021], assuming collective Gaussian attacks.

3. Security Limits of M-APSK Constellations

The M-APSK constellations consist of M coherent states in the form $|\alpha_{p,k}\rangle = \left|\beta_p|\alpha_R|\,\mathrm{e}^{i(k\theta_p+\theta_p/2)}\right\rangle$, with $p = 1, 2, ..., R$, and $k = 0, 1, ..., M_p - 1$, where

$\beta_p = \frac{p}{R}$, $|\alpha_R|$ is the radius of the outer ring, $\theta_p = \frac{2\pi}{M_p}$, M_p is the number of points in ring p, and R is the total number of rings. All points inside some specific ring are considered to have equal probability, given by $P_k = 1/M_p$. Probabilistic shaping considering the binomial distribution is given by $P_p = \frac{2}{2^{(2R-1)}}\binom{2R-1}{R-p}$, for the rings probability, where $\binom{n}{k}$ gives the number of ways to choose k elements from a set of n elements. The probability associated to each state of the constellation is $P_{p,k} = P_p/M_p$, and the mean number of photons per symbol, $\langle n \rangle = |\alpha|^2$, is given by $\sum_p P_p \langle \beta_p \rangle^2 |\alpha_R|^2$. Here, irregular M-APSK is defined as in [Almeida et al. 2021], with the successive rings containing 4, 12, 16, 32, 64, 128, and 256 states from the inner ring to the outer one. In regular M-APSK, here referred to as M-APSK (M_p), all rings have an equal number of states, M_p.

Fig. 1 presents the secret key rate as a function of the transmission distance (Fig. 1a) and of the excess noise (Fig. 1b) for GM and regular M-APSK with M between 16 and 256 with the binomial distribution for probabilistic shaping. The performance of regular M-APSK constellations increase with the number of states M, getting closer to the optimum performance of GM. Moreover, with increasing M, generally, the performance improvement decreases, until reaching a saturation point. In terms of the maximum achievable transmission distance, this saturation point is reached for 128-APSK (16) (Fig. 1a), which is also very close from 256-APSK (32) in terms of the maximum acceptable excess noise (Fig. 1b). As such, there is still a gap between the performance of regular M-APSK and GM's optimal performance.

Table 1 contains the maximum achievable transmission distance and maximum (back-to-back) secret key rate for $\xi = 0.005$ SNU, and the maximum acceptable excess noise value and maximum (no eavesdropping) secret key rate for $d = 10$ km for GM and regular 64, 128 and 256-APSK with the binomial distribution for probabilistic shaping. For a better comparison between regular and irregular M-APSK, Table 1 also contains results for irregular 64, 128 and 256-APSK with the binomial distribution, with some of the results been taken from Table 1 of [Almeida et al. 2021]. Regular 256-APSK (32) can achieve only $0.7\,\mathrm{km}$ more than irregular 256-APSK. Nonetheless, regular

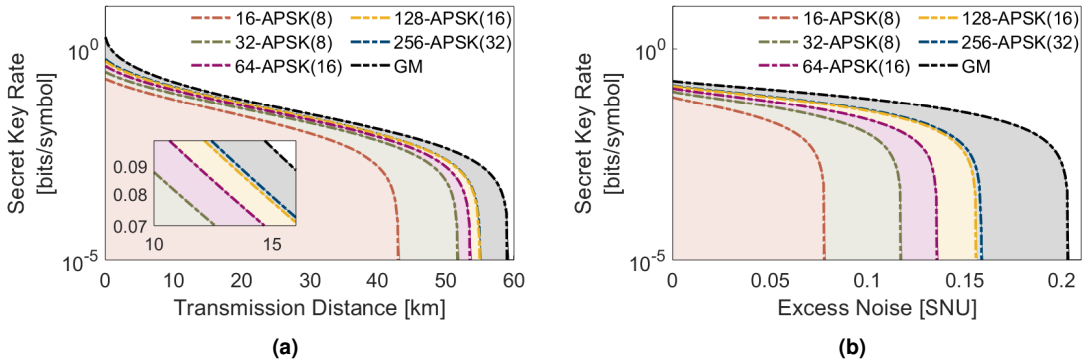

Figure 1. Secret key rate for GM and regular M-APSK with M between 16 and 256, considering binomial distribution for probabilistic shaping, with the mean number of photons per symbol optimized and considering the finite size effects, as a function of (a) the transmission distance and (b) the excess noise. Here it was considered $d = 10$ km, $\eta = 0.6$, $\beta = 0.95$, $\xi = 0.005$ SNU, $\xi_{\mathrm{thermal}} = 0.04$ SNU, $\epsilon = \epsilon_{\mathrm{PA}} = \epsilon_{\mathrm{PE}} = 10^{-10}$, $N = 10^8$ points, $n/N = 1/2$.

Table 1. Maximum achievable transmission distance and maximum (back-to-back) secret key rate for $\xi = 0.005$ SNU; and maximum acceptable excess noise and maximum (no eavesdropping) secret key rate for $d = 10$ km. Results are presented for GM, and regular and irregular 64-APSK, 128-APSK and 256-APSK with the binomial distribution for probabilistic shaping. Here the mean number of photon per symbol was optimized, and it was considered $\eta = 0.6$, $\beta = 0.95$, $\xi_{\text{thermal}} = 0.04$ SNU, $\epsilon = \epsilon_{\text{PA}} = \epsilon_{\text{PE}} = 10^{-10}$, $N = 10^8$ points, $n/N = 1/2$. *Results from [Almeida et al. 2021].

	Gaussian Modulation	Regular M-APSK			Irregular M-APSK		
		64-APSK (16)	128-APSK (16)	256-APSK (32)	64-APSK	128-APSK	256-APSK
Maximum Achievable Transmission Distance [km] for $\xi = 0.005$ SNU	58.9	53.5	54.9	54.9	52.0*	53.6*	54.2*
Maximum Secret Key Rate [bits/symbol] for $\xi = 0.005$ SNU	1.908	0.399	0.516	0.574	0.309	0.361	0.402
Maximum Acceptable Excess Noise [SNU] for $d = 10$ km	0.203	0.136	0.156	0.159	0.121	0.134	0.141
Maximum Secret Key Rate [bits/symbol] for $d = 10$ km	0.173	0.116	0.132	0.137	0.101	0.111	0.118

M-APSK have higher key rates for all distance range. In fact, for small distances regular 64-APSK (16) has a higher secret key rate associated, namely $0.399\,\text{bits/symbol}$ in a back-to-back situation, than irregular 128-APSK, which has $0.361\,\text{bits/symbol}$, being only $0.003\,\text{bits/symbol}$ away from irregular 256-APSK. The differences between considering regular or irregular M-APSK constellations are even more noticeable in terms of the excess noise, with regular 128-APSK (16) and 256-APSK (32) being able to accept $0.015\,\text{SNU}$ and $0.018\,\text{SNU}$ more than irregular 256-APSK. As such, regular M-APSK outperforms irregular M-APSK either in terms of secret key rate, in terms of maximum achievable transmission distances and in terms of maximum acceptable excess noise. Remark that no practical advantage of irregular M-APSK constellations over regular M-APSK, considering QKD practical applications, has been found. Future research may focus on the comparison between both these modulation formats alongside a practical implementation of the CV-QKD system.

Fig 2a contains the secret key rate as a function of the mean number of photons per symbol for GM and regular M-APSK with M between 16 and 256 considering the binomial distribution for probabilistic shaping. For small values of mean number of photons per symbol, the key rates obtained considering regular M-APSK approximate the optimum ones of GM. With increasing number of states, M, the curves for regular M-APSK becomes flatter, as also observed for irregular M-APSK, allowing more flexibility in terms of the mean number of photons per symbol in the system, without compromising the secret key rate. Moreover, regular M-APSK has a larger range of usable mean number of photons per symbol, than irregular M-APSK. From Fig. 8 of [Almeida et al. 2021], irregular M-APSK cannot consider values of mean number of photons higher than $7\,\text{photons per symbol}$, while both regular 128-APSK (16) and 256-APSK (32) can extract keys using more than $8\,\text{photons per symbol}$.

In Fig. 2b we present the maximum excess noise as a function of the transmission distance for GM and regular M-APSK with M between 16 and 256. The use of higher-order M-APSK allows the increase of the key rate, and as such the increase of

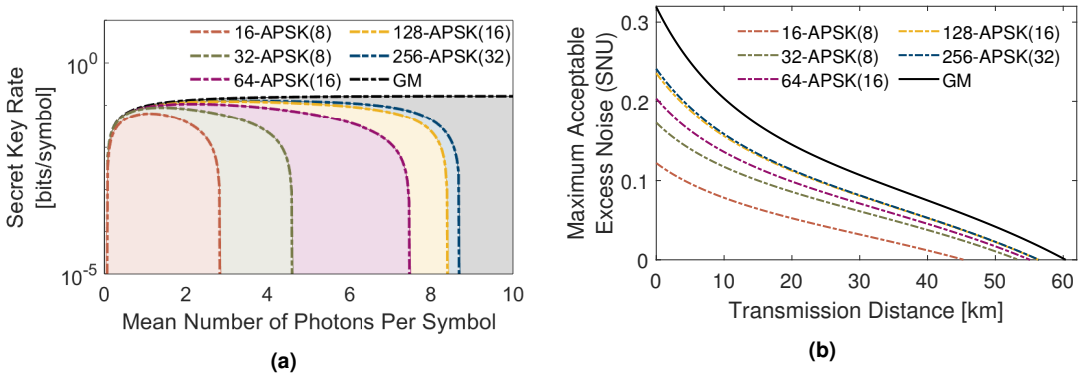

Figure 2. (a) Secret key rate as a function of the mean number of photons per symbol; and (b) Maximum acceptable excess noise as a function of the transmission distance with the mean number of photons per symbol optimized. This for GM and regular M-APSK with M between 16 and 256 considering the binomial distribution for probabilistic shaping. The results were obtained considering $d = 10$ km, $\eta = 0.6$, $\beta = 0.95$, $\xi = 0.005$ SNU, $\xi_{\text{thermal}} = 0.04$ SNU, $\epsilon = \epsilon_{\text{PA}} = \epsilon_{\text{PE}} = 10^{-10}$, $N = 10^8$ points, $n/N = 1/2$.

the achievable distances and of the robustness to attacks (Fig. 1 and Table 1), independently of the transmission distance and excess noise value considered (Fig. 2b). Higher transmission distances are associated to smaller accepted excess noise values (Fig. 2b). Similarly, higher values of excess noise mean that the CV-QKD system is only secure for a smaller range of distances. Nonetheless, the relation between the maximum acceptable excess noise and the transmission distance is not linear (Fig. 2b). The maximum acceptable excess noise decreases more for smaller distances. Remark that, with increasing transmission distance, the difference between the amount of eavesdropping accepted by the different constellations decreases.

4. Conclusion

In this work the performance in CV-QKD systems of regular M-APSK constellations was studied and compared with the performance of irregular M-APSK. We show that regular M-APSK can achieve higher secret key rates than irregular M-APSK, thus getting closer to the GM's optimal performance. In a practical implementation, regular and irregular M-APSK are similar, turning regular M-APSK constellations more relevant for CV-QKD purposes. The higher-order regular M-APSK can achieve higher distances, being more resistant to the excess noise. Nonetheless, a gap can still be observed, independently of the transmission distance and of the excess noise, between the performance of the higher-order regular M-APSK constellations and GM, with the curve of regular 128-APSK (16) being almost overlapped with the curve of regular 256-APSK (32). As such, there is no relevant gain in considering regular 256-APSK (32) over regular 128-APSK (16). Regular 128-APSK (16) achieves almost 93% of GM's maximum achievable transmission distance (in a no eavesdropper situation), and accepts almost 76% GM's maximum acceptable excess noise (in a back-to-back situation), showing greater performance than irregular 256-APSK for all distance and excess noise values. Further analysis of both regular and irregular M-APSK constellations in terms of the practical implementation of CV-QKD systems is left as future work.

Acknowledgments: This work was supported in part by Fundação para a Ciência e a Tecnologia (FCT) through national funds, by the European Regional Development Fund (FEDER), through the Competitiveness and Internationalization Operational Programme (COMPETE 2020) of the Portugal 2020 framework, and when applicable co-funded EU funds under the project UIDB/50008/2020-UIDP/50008/2020 (actions DigCORE, QUESTS, and QuRUNNER), and by FCT through the PhD Grant SFRH/BD/139867/2018.

References

Almeida, M., Pereira, D., Muga, N. J., Facão, M., Pinto, A. N., and Silva, N. A. (2021). Secret key rate of multi-ring M-APSK continuous variable quantum key distribution. *Optics Express*, 29(23):38669–38682.

Bennett, C. H. and Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11.

Denys, A., Brown, P., and Leverrier, A. (2021). Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation. *Quantum*, 5:540. arXiv: 2103.13945.

Essiambre, R.-J., Kramer, G., Winzer, P. J., Foschini, G. J., and Goebel, B. (2010). Capacity Limits of Optical Fiber Networks. *Journal of Lightwave Technology*, 28(4):662–701.

Ghorai, S., Grangier, P., Diamanti, E., and Leverrier, A. (2019). Asymptotic Security of Continuous-Variable Quantum Key Distribution with a Discrete Modulation. *Physical Review X*, 9(2):021059.

Grosshans, F. and Grangier, P. (2002). Continuous variable quantum cryptography using coherent states. *Physical Review Letters*, 88(5):057902. arXiv: quant-ph/0109084.

Huang, P., Fang, J., and Zeng, G. (2014). State-discrimination attack on discretely modulated continuous-variable quantum key distribution. *Physical Review A*, 89(4):042330.

Leverrier, A. and Grangier, P. (2011). Continuous-variable quantum key distribution protocols with a non-Gaussian modulation. *Physical Review A*, 83(4):042312. arXiv: 1101.3008.

Leverrier, A., Grosshans, F., and Grangier, P. (2010). Finite-size analysis of a continuous-variable quantum key distribution. *Physical Review A*, 81(6):062343.

Li, Z., Zhang, Y.-C., Xu, F., Peng, X., and Guo, H. (2014). Continuous-Variable Measurement-Device-Independent Quantum Key Distribution. *Physical Review A*, 89(5):052301. arXiv: 1312.4655.

Lin, J. and Lütkenhaus, N. (2020). Trusted Detector Noise Analysis for Discrete Modulation Schemes of Continuous-Variable Quantum Key Distribution. *Physical Review Applied*, 14(6):064030.