Amplitude-Phase Modulated CVQKD Protocol

Micael Andrade Dias and Francisco Marcos de Assis

Abstract— Here we report the performance of a discrete modulated Continuous Variable Quantum Key Distribution protocol based on eight and sixteen state optimal Amplitude Phase Keying constellations with pure loss quantum channel transmission. Our constellations use the same amplitudes and state probability as in an optimal four-state unidimensional constellation model and apply amplitude/phase modulation to the quadratures of coherent states. We compare the obtained results with the performance of conventional m-PSK and m-APK constellations. The results presented show that protocols that use the proposed constellations outperform the ones based on conventional constellations in both secret key rate and link distance. In special, our protocol is able to accomplish viable SKR's in low transmittance regime, $\tau < 0.2$.

Keywords— CVQKD, Discrete Modulation, Constellation Shaping.

I. INTRODUCTION

Quantum Key Distribution (QKD) protocols, one of the most promising Quantum Information practical implementations, are mainly divided into protocols based on discrete variable quantum systems, represented by finite dimensional Hilbert spaces, and on continuous variable quantum systems with infinite dimensional Hilbert spaces [1]. The first class is known as Discrete Variable QKD (DVQKD) protocols and naturally applies discrete modulation to encode information as in, for example, the BB84 protocol with single photon polarization and detection [2]. These protocols are extremely sensitive during quantum communication phase but allows the use of simple error correction schemes such as CASCADE protocol [3]. The QKD protocols with continuous variables (CVQKD protocols) usually use coherent or squeezed quantum states and, at first, applied discrete modulation [4] (finite set of transmitted quantum states) but, with the GG02 protocol [5], Gaussian modulation of quadratures became a reference system for CVQKD. These continuous variable based protocols are, in principle, compatible with off-the-shelf optical networks devices (modulators, detectors, multiplexers, etc.) but demands well-designed continuous-to-discrete operations and state-of-the-art capacity achieving error correcting codes [6–10].

In the last decade, research on QKD has turned to a hybrid solution, intending to harvest the best characteristics of both families, by applying discrete modulation on continuous variable quantum systems (DM-CVQKD). With these protocols, there is no need for a continuous-to-discrete conversion and the compatibility with current optical network devices is maintained by using coherent states. This conversion from continuous (analog) to discrete (digital) modulation is a process already experienced in classical communication systems where Gaussian modulation, which matches the statistical behavior of an Aditive White Gaussian Noise (AWGN) channel and reaches the channel capacity, is approximated by digital signaling schemes such as Phase Shift Keying (PSK), Amplitude Shift Keying (ASK), Amplitude Phase Keying (APK) and Quadrature Amplitude Modulation (QAM), also known as constellations [11].

Although digitally modulated protocols come as a practical solution for deploying QKD, a price is payed as non-Gaussian modulation is suboptimal for secret key rates [12]. Although the ultimate secret key rate is reached theoretically by Gaussian modulation on both quadratures, several DM-CVQKD protocols were proposed based on m-PSK constellations, each one presenting different security proofs and the conditions for which the secrete key rate is close to a Gaussian modulated protocol [13–17].

In the classical context, some measures can be taken to reduce the effects of using digital modulation. Firstly, one can increase the number of states in the signal set (the constellation). A more sophisticated solution is to adjust the constellation shape and assign different probabilities to the states, which is known as geometric and probabilistic shaping, respectively. Several constellation shapes of unidimensional (UD) constellations were analyzed in [18] and it was shown that the ones applying some kind of shaping have a better convergence towards Gaussian modulation performance as its cardinalities increase than the ones with no geometric and/or probabilistic shaping. This capability of approximating Gaussian modulation by shaping the constellation is also translated to QKD protocols, as it was shown in [19] where the authors used the UD constellations in [18] and compared with an UD Gaussian modulation [20], and they concluded that capacity archiving[1] UD constellations also reaches the performance of Gaussian modulated UD protocol. The authors also presented optimal four state constellations obtained by an exhaustive search on its geometry and probability for each transmittance in the interval $\tau \in \,]0, 1[$.

Despite the good performance of digital UD modulation, finding bidimensional efficient constellations is still quite challenging. In this paper we propose new eight and sixteen-states amplitude-phase shifted constellations based CVQKD protocol. The proposed constellations are based on the optimal UD four-state constellations presented in [19], where we used the four-state constellation amplitudes and probabilities while applying several rotations to obtain proper eight/sixteen-states constellations. We analyze the protocol performance assuming reverse reconciliation and a noiseless quantum channel.

Micael Andrade Dias and Francisco Marcos de Assis, Center of Electrical Engineering and Informatics, Federal University of Campina Grande (UFCG), Campina Grande-PB, Brazil. E-mails: micael.souza@ee.ufcg.edu.br, fmarcos@dee.ufcg.edu.br.

---

[1]By capacity achieving the authors mean a modulation scheme whose performance in the AWGN channel reaches the information-theoretic limit of continuous Gaussian modulation.

The results indicate that our proposed protocol outperforms standard PSK and APK based protocols in the secret key rate and reachable range. These results imply that the way to obtain better performances for discrete modulated CVQKD protocols goes through managing the constellation geometry and the state probability.

The paper is structured as follows. Section II presents the general framework of a discrete modulated QKD protocol with continuous variables. Section III introduces the optimized constellations and the main results. In Section IV we give the final considerations and perspectives for future work.

II. DISCRETE MODULATED PROTOCOLS

Any QKD protocol consists on two legitimate parties (Alice and Bob) intending to establish a secret random stream of symbols to be used as cryptographic key and, for that, they use quantum systems to transmit classical information. This phase of preparing, transmitting and detecting quantum states is called the protocol's quantum stage and is where most differences between many kinds of QKD protocols lie. In a Gaussian Modulated Coherent State (GMCS) protocol, Alice will draw realizations q_i and p_i of normally distributed random variables $\mathcal{Q}$ and $\mathcal{P}$ to define the complex amplitude $\alpha_i = q_i + ip_i$ of a coherent state, which will be prepared, transmitted and detected by Bob with homodyne or heterodyne setups. After state preparation/detection, the complex amplitudes α_i and detection outcomes β_i are continuous valued and then require some quantization process in order to result on binary strings. This quantizer must be well designed and works alongside with the error correction protocol. This continuous-to-discrete operation added to error correction provides a bottleneck on the protocol's performance.

A discrete modulated CVQKD protocol dismiss the quantization process and works as follows. Instead of drawing realizations out of normal random variables, define an alphabet of $N = 2^K$ letters to be drawn randomly by Alice according to some suitable probability distribution $\mathcal{P} = \{p_i\}$, each letter corresponding to a binary word of K bits, and a set of complex amplitudes $\mathcal{A}$ with $|\mathcal{A}| = N$. Each letter is mapped unambiguously to a coherent state $|\alpha_i\rangle$ whose complex amplitude $\alpha_i \in \mathcal{A}$ and we call $C(\mathcal{A}, \mathcal{P})$ a constellation *geometric shaped* by $\mathcal{A}$ and *probabilistic shaped* by $\mathcal{P}$. Different constellations define distinct DM-CVQKD protocols although they may share the same classical post-processing protocols[2] (parameter estimation, information reconciliation and security amplification). Then, by randomly drawing the letters, Alice chooses the coherent state that will be prepared on mode A, she sends it through a quantum channel whose output mode B will be detected by Bob. We consider the quantum channel to be a pure-loss channel and Bob's detection to be heterodyne, as depicted in Figure 1.

---

[2]The security analysis should consider the set of states prepared by Alice in order to estimate the correlations between Alice, Bob and Eve data after quantum state transmission. The protocols in [13–15, 17] uses constellations with different cardinalities and have its security analysis made from distinct perspectives. Once quantum state transmission is finished, Alice and Bob have correlated binary sequences and, at first, classical post-processing becomes independent of which constellation was used.
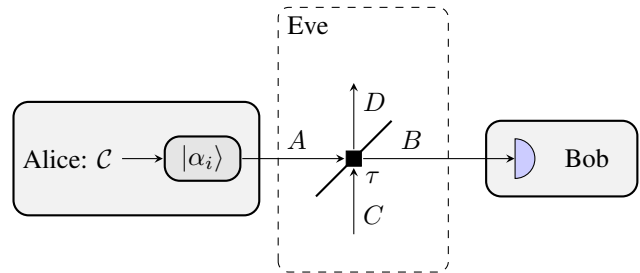

Fig. 1: Pure loss quantum channel model for a DM-CVQKD protocol.

The entire communication (either quantum or classical) is under the presence of a powerful eavesdropper (Eve) whose capabilities are only bounded by the laws of quantum mechanics. Eve will intend to acquire information about the exchanged states by Alice and Bob by performing some information attack during the quantum communication stage[3]. This attack comprises the coupling setup, i.e., how she intercept each state sent by Alice, and how she interacts with the states (individual, collective or coherent coupling/detection). In the case of a pure-loss channel, Eve replaces the quantum channel by a beam splitter (BS) with controlled transmittance τ. This BS couples Alice's state to a vacuum state (mode C) and one of its outputs ports goes to Bob (mode B) while the other is Eve's (mode D). When Eve couples Alice's state to a two-mode squeezed vacuum state, the pure-loss channel becomes a thermal-loss channel and constitutes the entangling cloner attack.

A. The Secret Key Rate

To compute the Secret Key Rate (SKR) of a discrete modulated CVQKD protocol, it is needed to define (or assume) which way to interact with Alice states was chosen Eve. Here we assume the following: (a) pure-loss channel, (b) collective attacks and (c) reverse reconciliation direction. By collective attacks we mean that Eve will interact individually with each state but she can store her ancilla mode in a quantum memory to perform a collective delayed measurement. This strategy allows her to use some information of the reconciliation phase to adjust her measurement apparatus so her obtained information can reach the Holevo bound. The reverse reconciliation direction indicates that during error correction (information reconciliation), Alice will adjust her raw key to Bob's one, forcing Eve to relate her states to Bob's outcomes.

Given the above assumptions, the SKR formula for reverse reconciliation under collective attacks is

$$K_{coll} = I(A;B) - \chi(B,E), \qquad (1)$$

where $I(A;B)$ is the Shannon mutual information between Alice and Bob's classical random variables and $\chi(B,E)$ is Holevo's bound on Eve's accessible information on Bob's states [21–23]. To compute the mutual information, one needs

---

[3]The eavesdropper attempts during classical error correction of the key post-processing are still considered but the classical channel is assumed to be authenticated, meaning that Eve can not modify the error correction messages or to pass by Alice or Bob.

to note that Alice's random variable is a discrete one, the set of amplitudes $\mathcal{A}$ and the probabilities assigned to each amplitude, and Bob's variable is continuous and, in the case of heterodyne measurement, one has that the probability of Bob's outcome b given Alice sent α_i is $p(b|\alpha_i) = e^{-|b-\sqrt{\tau}\alpha_i|^2}/\pi$. Then, the mutual information can be computed using the factorization

$$I(A;B) = H(\mathcal{P}) - \int_{\mathbb{C}} H(A|B=b)\, \mathrm{d}^2 b, \qquad (2)$$

where $H(\cdot)$ is the Shannon entropy and the integral is in the complex plane. The Holevo bound gives the maximal classical mutual information between Eve's measurements and Bob's outcomes. This implies that Eve performs the optimal measurement on her states and is computed by

$$\chi(B,E) = S(\hat{\rho}_E) - \int_{\mathbb{C}} p(b) S(\hat{\rho}_{E|b})\, \mathrm{d}^2 b, \qquad (3)$$

where $\hat{\rho}_E$ is Eve's average state,

$$\hat{\rho}_E = \sum p_i \, |\sqrt{1-\tau}\alpha_i\rangle\langle\sqrt{1-\tau}\alpha_i|, \qquad (4)$$

and $\hat{\rho}_{E|b}$ is Eve's average state conditioned to Bob's measurement outcome b,

$$\hat{\rho}_{E|b} = \sum p(\alpha_i|b) \, |\sqrt{1-\tau}\alpha_i\rangle\langle\sqrt{1-\tau}\alpha_i|. \qquad (5)$$

Here, $S(\cdot)$ is the von Neumann entropy of a quantum state defined as $S(\hat{\sigma}) = -\operatorname{tr}(\hat{\sigma}\log\hat{\sigma})$. If the state $\hat{\sigma}$ has a spectral decomposition $\hat{\sigma} = \sum_k \lambda_k |\sigma_k\rangle\langle\sigma_k|$, where $\Lambda = \{\lambda_k\}$ are the eigenvalues of $\hat{\sigma}$ (non-negative and summing up to 1) and $|\sigma_k\rangle$ eigenvectors, then $S(\hat{\sigma}) = H(\Lambda)$. In the Equation (3) where must be computed the entropy for the states in Equations (4) and (5), which are mixtures of nonorthogonal states, its entropy can be computed using the Gram-Schmidt orthogonalization procedure, as explained in the Appendix.

III. AMPLITUDE-SHIFTED CONSTELLATION DESIGN

The design of QKD protocols compatible with current communication devices is a crucial step towards practical implementation and the application of discrete modulation to coherent state based protocols provides a solid advance in this direction. Although non-Gaussian modulation is always suboptimal in the SKR, its performance can be improved with well-designed modulations schemes, which implies the search for constellations that maximizes the protocol performance. In the classical context, finding optimal bidimensional constellations is not a simple task and one can only expect that it is no different in a quantum information protocol.

Four types of unidimensional constellations were examined in [18] for different signal-to-noise ratios and increasing cardinalities. The performance of such constellations in a QKD context were investigated in [19] and they also presented an optimal four-state unidimensional constellation. The search for these optimal four-state constellations was made exhaustively in the following way. Define $\mathcal{C}^{(4)}$ to be the set of all constellations of four coherent states in the form $\{|\alpha_1\rangle, |-\alpha_1\rangle, |\alpha_2\rangle, |-\alpha_2\rangle\}$, $\alpha_i \in \mathbb{R}$ and $\alpha_2 > \alpha_1$, with probabilities $\{p_1, p_1, p_2, p_2\}$, where $p_1 > p_2 = \frac{1}{2} - p_1$. Call
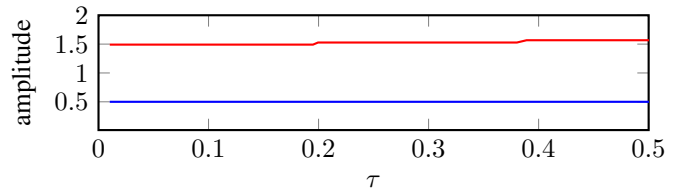
(a) Optimal amplitudes α_1 (lower) and α_2 (upper).
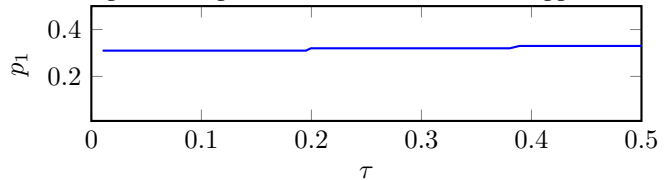
(b) Optimal probability p_1.

Fig. 2: Parameters α_1, α_2 and p_1 for the optimal ensemble that maximizes the SKR in of a four-state UD-CVQKD protocol.

$\hat{\rho}_m$ the average state representing an arbitrary ensemble of $\mathcal{C}^{(4)}$ restricted to the energy constrain $\operatorname{tr}(\hat{\rho}_m \hat{n}) = 1$. Let $I(A;B)(\hat{\rho}_m)$ and $\chi(E,B)(\hat{\rho}_m)$ to be Alice and Bob's mutual information and Eve's accessible information, both assuming the protocol used the constellation represented by $\hat{\rho}_m$. Therefore, the maximal SKR for a four-state unidimensional protocol is given by

$$R_{max}^{(4)} = \max_{\substack{\hat{\rho}_m \in \mathcal{C}^{(4)} \\ \operatorname{tr}(\hat{\rho}_m \hat{n})=1}} \{I(A;B)(\hat{\rho}_m) - \chi(E,B)(\hat{\rho}_m)\}. \qquad (6)$$

Indeed, by setting the values of α_1 and p_1 the constellation is completely defined and the search task will look for the pair (α_1, p_1) that maximizes the SKR at a given transmittance τ with fixed energy constrain. The optimized parameters are replicated in Figure 2 in the interval $0 < \tau < 0.5$. One can see that, in the presented transmittance range, the amplitude values and the probabilities remained almost unchanged. It can be said that the optimal constellations are slightly geometric shaped (the states are equally spaced) while the probability distribution is not uniform.

We then used the optimal parameters found by the optimization in Equation (6) to design optimal Amplitude-Phase modulations (OAPK) schemes with eight and sixteen states. We denote by N_1/N_2OAPK the Optimal Amplitude Phase Keying constellation with N_1 states of energy α_1^2 and N_2 states of energy α_2^2. From the probabilities $\{p_1, p_2\}$ we define that the state with energy α_i^2 is prepared with probability $q_i = 2p_i/N_i$. Such constellations are shown in Figure 3.

In Figure 4 we plot the SKR for the eight and sixteen state OAPK constellations together with conventional 8PSK, 16PSK, 4/4APK and 8/8APK constellations. At first, the results show that the proposed constellations applied to QKD outperform PSK and APK based protocols. It can be seen that our eight-state protocol provides greater SKR in the entire transmittance range and reaches longer distances (positive SKR's for low transmittance) than the other eight-state protocols. However, the 4/4OAPK protocol performance
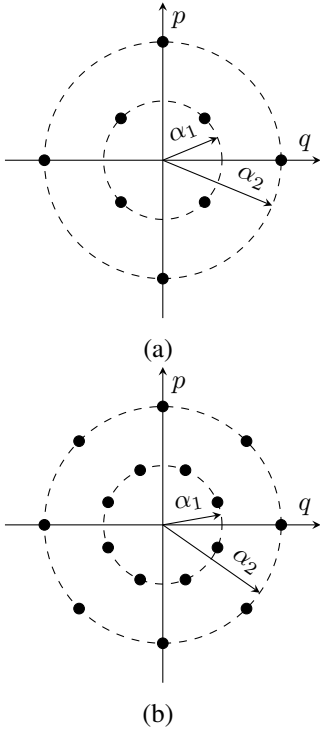
(a)

(b)

Fig. 3: Eight (a) and sixteen (b) state OAPK constellations designed from the optimal 4UD constellation parameters given by Equation (6).
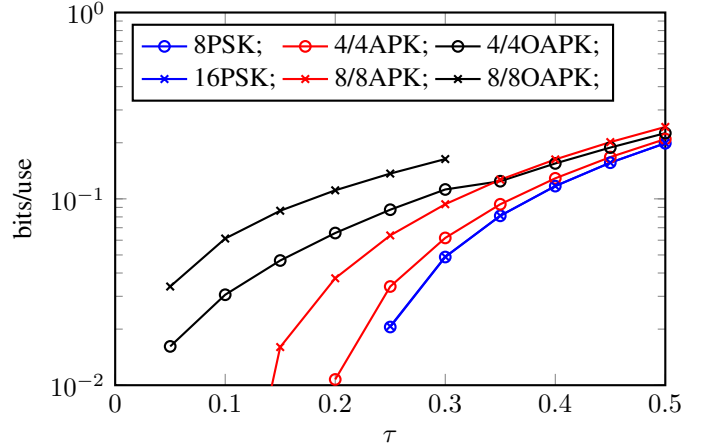

Fig. 4: Secret key rates for the discrete modulated CVQKD protocol based on PSK, APK and our proposed optimized APK constellations with eight (circle marker) and sixteen (cross marker) states. All constellations have fixed unit average energy.

gets a little diminished for $\tau > 0.3$ and we can address this issue to the fact that as the transmittance increases, the states received by Bob becomes more distinguishable by him and the eavesdropper is able to retrieve more information about his states.

When we turn to the proposed sixteen-state protocol, two things call attention. First, increasing the cardinality of our OAPK protocol considerably increases the secret key rate and, second, there is no significant difference between the 8PSK and 16PSK constellations. The 16APK constellation presents a performance enhancement but still remains undermined by both 4/4OAPK and 8/8OAPK constellations. One can conclude that m-PSK based protocols have a saturation point in its cardinality near to eight states. By comparing the traditional APK and our proposed OAPK constellations, we can conclude that simple adjustments to the constellation geometry and probability distribution results in considerably SKR increasing and allows the protocol to reach longer distances. The 8/8OAPK constellation results for $\tau > 0.3$ where not presented due to numerical issues.

IV. CONCLUSION

We have presented amplitude-phase shifted constellations obtained from unidimensional four-state constellations optimized to CVQKD and analyzed its performance in the reverse reconciliation regime over a pure-loss quantum channel. We computed the secret key rates for the proposed amplitude-phase constellations with eight and sixteen states and compared with conventional m-PSK and m-APK constellations.

The results presented a superiority of the proposed constellations over the conventional ones, providing greater secret key rates and capability of reaching longer distances. Such enhancement shows that simple constellation shaping can improve the protocol's performance. Future works can be focused on finding constellations with greater cardinalities and also including the thermal noise effect in the quantum channel.

APPENDIX

Let us define an ensemble of arbitrary coherent states $\mathcal{S} = \{|\alpha_i\rangle, p_i\}_{i=0}^{K-1}$, being $\alpha_i \in \mathbb{C}$ and p_i the probability of the i-th state on $\mathcal{S}$ to be prepared, with $\sum p_i = 1$. From $\mathcal{S}$, one can compute the inner product matrix $V_\mathcal{S}$,

$$V_{ij} = \langle\alpha_i|\alpha_j\rangle = e^{\frac{1}{2}(\alpha_i^*\alpha_j - \alpha_i\alpha_j^*)}e^{-\frac{1}{2}|\alpha_i - \alpha_j|^2}. \qquad (7)$$

By the Gram-Schmidt orthogonalization procedure it is possible to compute, using the states on $\mathcal{S}$, an orthonormal set of states $\mathcal{B} = \{|\psi_0\rangle, \cdots, |\psi_{K-1}\rangle\}$ which is a base to the subspace spanned by $\{|\alpha_i\rangle\}_{i=0}^{K-1}$. Then, one can decompose each $|\alpha_i\rangle$ with $\mathcal{B}$ basis:

$$|\alpha_k\rangle = \sum_{i=0}^{K-1} \langle\psi_i|\alpha_k\rangle |\psi_i\rangle = \sum_{i=0}^{K-1} M_{ki} |\psi_i\rangle, \qquad (8)$$

where $M_{k,i}$ corresponds to the projection of the k-th state $|\alpha_k\rangle$ into the i-th basis element of $\mathcal{B}$. These projections are arranged as a matrix, for which each element may be computed by the following algorithm:

$$M_{k0} = V_{0k} \qquad (9)$$

$$M_{ki} = \frac{1}{M_{ii}}\left(V_{ik} - \sum_{j=0}^{i-1} M_{ij}^* M_{kj}\right) \quad if \ 1 \le i < k \qquad (10)$$

$$M_{ki} = 0 \quad if \ i > k \qquad (11)$$

$$M_{kk} = \left(1 - \sum_{i=0}^{k-1} |M_{ki}|^2\right)^{1/2} \quad for \ k > 0. \qquad (12)$$

4

By the description on Equation (8), the density operators $\hat{\rho}_{\alpha_k}$ and $\hat{\rho}_m$ for the coherent state $|\alpha_k\rangle$ and the whole ensemble $\mathcal{S}$ are, respectively,

$$\hat{\rho}_{\alpha_k} = \sum_{i,j=0}^{k} M_{ki} M_{kj}^* \, |\psi_i\rangle\langle\psi_j| \qquad (13)$$

$$\hat{\rho}_m = \sum_{k=0}^{N-1} p_k \hat{\rho}_{\alpha_k} = \sum_{k=0}^{N-1} p_k \sum_{i,j=0}^{k} M_{ki} M_{kj}^* \, |\psi_i\rangle\langle\psi_j| . \qquad (14)$$

REFERENCES

[1] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information," *Rev. Mod. Phys.*, vol. 84, no. 2, pp. 621–669, 2012.

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, pp. 7–11, 2014. DOI: `10.1016/j.tcs.2014.05.025`.

[3] G. Brassard and L. Salvail, "Secret-Key Reconciliation by Public Discussion," in *EUROCRYPT*, Berlin, Heidelberg: Springer Berlin Heidelberg, 1994, pp. 410–423. DOI: `10.1007/3-540-48285-7_35`.

[4] T. C. Ralph, "Continuous variable quantum cryptography," *Phys. Rev. A*, vol. 61, no. 1, 1999. DOI: `10.1103/physreva.61.010303`.

[5] F. Grosshans and P. Grangier, "Continuous Variable Quantum Cryptography Using Coherent States," *Phys. Rev. Lett.*, vol. 88, no. 5, p. 57902, Jan. 2002. DOI: `10.1103/PhysRevLett.88.057902`.

[6] G. V. Assche, J. Cardinal, and N. J. Cerf, "Reconciliation of a quantum-distributed Gaussian key," *IEEE TIT*, vol. 50, no. 2, pp. 394–400, 2004, ISSN: 0018-9448. DOI: `10.1109/tit.2003.822618`.

[7] K.-C. NGUYEN, G. VAN ASSCHE, and N. J. CERF, "Side-information coding with turbo codes and its application to quantum key distribution," in *International Symposium on Information Theory and its Applications*, Parma, Italy, October, Oct. 10, 2004.

[8] M. Bloch, A. Thangaraj, S. McLaughlin, and J.-M. Merolla, "LDPC-based gaussian key reconciliation," in *2006 IEEE Information Theory Workshop*, Punta del Este, Uruguay: IEEE, 2006, pp. 116–120. DOI: `10.1109/ITW.2006.1633793`.

[9] Z. Bai, S. Yang, and Y. Li, "High-efficiency reconciliation for continuous variable quantum key distribution," *Japanese Journal of Applied Physics*, vol. 56, no. 4, p. 44401, Mar. 2017. DOI: `10.7567/jjap.56.044401`.

[10] P. Jouguet, D. Elkouss, and S. Kunz-Jacques, "High-bit-rate continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 90, no. 4, p. 42329, 2014.

[11] J. G. Proakis and M. Salehi, *Digital Communications*, 5th ed. Boston: McGraw-Hill, 2008, ISBN: 978-0-07-295716-7.

[12] M. M. Wolf, G. Giedke, and J. I. Cirac, "Extremality of Gaussian Quantum States," *Phys. Rev. Lett.*, vol. 96, no. 8, p. 080502, Mar. 2006. DOI: `10.1103/PhysRevLett.96.080502`.

[13] Y. B. Zhao, M. Heid, J. Rigas, and N. Lütkenhaus, "Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks," *Phys. Rev. A*, vol. 79, no. 1, pp. 1–14, 2009, ISSN: 10502947. DOI: `10.1103/PhysRevA.79.012307`.

[14] A. Leverrier and P. Grangier, "Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation," *Phys. Rev. Lett.*, vol. 102, no. 18, 2009, ISSN: 00319007. DOI: `10.1103/PhysRevLett.102.180504`.

[15] K. Brádler and C. Weedbrook, "Security proof of continuous-variable quantum key distribution using three coherent states," *Phys. Rev. A*, vol. 97, no. 2, pp. 1–16, 2018, ISSN: 24699934. DOI: `10.1103/PhysRevA.97.022310`.

[16] P. Papanastasiou, C. Lupo, C. Weedbrook, and S. Pirandola, "Quantum key distribution with phase-encoded coherent states: Asymptotic security analysis in thermal-loss channels," *Physical Review A*, vol. 98, no. 1, p. 012340, Jul. 2018, ISSN: 2469-9926, 2469-9934. DOI: `10.1103/PhysRevA.98.012340`.

[17] S. Ghorai, P. Grangier, E. Diamanti, and A. Leverrier, "Asymptotic Security of Continuous-Variable Quantum Key Distribution with a Discrete Modulation," *Physical Review X*, vol. 9, no. 2, p. 021059, Jun. 2019, ISSN: 2160-3308. DOI: `10.1103/PhysRevX.9.021059`.

[18] 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`.

[19] M. Dias and F. Assis, "The Impact of Constellation Cardinality on Discrete Unidimensional CVQKD Protocols," *Quantum Information Processing*, 2021, Manuscript submitted for publication.

[20] V. C. Usenko and F. Grosshans, "Unidimensional continuous-variable quantum key distribution," *Physical Review A*, vol. 92, no. 6, p. 062337, Dec. 2015, ISSN: 1050-2947, 1094-1622. DOI: `10.1103/PhysRevA.92.062337`.

[21] A. S. Holevo, "Statistical problems in quantum physics," in *Proceedings of the Second Japan-USSR Symposium on Probability Theory*, G. Maruyama and Y. V. Prokhorov, Eds., vol. 330, Berlin, Heidelberg: Springer Berlin Heidelberg, 1973, pp. 104–119. DOI: `10.1007/BFb0061483`.

[22] M. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*. 2010, ISBN: 1-107-00217-6. DOI: `10.1017/CBO9780511976667`.

[23] M. M. Wilde, *Quantum Information Theory*, Second. Cambridge University Press, 2017, ISBN: 978-1-107-17616-4.