

Impact of SNR Mismatch on Induced BSCs in CV-QKD Systems Quantized with Arithmetic Reconciliation

Rávilla R. S. Leite, Juliana M. de Assis and Francisco M. de Assis

Abstract—Arithmetic Reconciliation (AR) is a recently proposed reconciliation protocol for Continuous-Variable Quantum Key Distribution (CV-QKD) systems operating in low-SNR regimes. Since the channel signal-to-noise ratio (SNR) directly affects the statistical characterization of the induced binary subchannels, inaccuracies in SNR estimation may significantly impact reconciliation performance. In this work, we investigate the effects of SNR mismatch on the Kullback-Leibler (KL) distance, Bit Error Rate (BER), capacities of the BSC subchannels induced by AR quantization and the secret key rate provided by the protocol. The obtained results show that the most significant subchannels are considerably more sensitive to mismatch conditions, especially at moderate and high SNR values. Furthermore, SNR underestimation leads to the selection of excessively robust low-rate error-correcting codes, increasing computational complexity and reducing spectral efficiency, whereas SNR overestimation degrades the effective decoding performance due to insufficient redundancy. These results demonstrate the importance of accurate SNR estimation for reliable and efficient practical implementations of CV-QKD systems employing AR.

Keywords—CV-QKD Reconciliation, Arithmetic Reconciliation, Parameter Estimation, SNR Mismatch.

I. INTRODUCTION

Quantum Key Distribution (QKD) protocols enable the distribution of secret keys between two distant parties that must be known only to the users involved, usually referred to as Alice and Bob. This key must be used only once — in applications known as “one-time pad” — and during its generation, as little information as possible must be leaked to an eavesdropper — usually called Eve — so that the key obtained is said to be “unconditionally secure”.

Early QKD protocols were based on discrete-variable quantum states, in which the secret information is encoded into the preparation basis of single photons. According to the quantum uncertainty principle, Bob must choose a measurement basis, increasing the certainty about one observable while inherently increasing the uncertainty about its conjugate counterpart. Any eavesdropping attempt introduces detectable disturbances into the system, since quantum states cannot be perfectly copied or amplified as classical signals [1]. Therefore, the security of

QKD systems relies fundamentally on the laws of quantum physics rather than on computational complexity assumptions.

Recent advances have enabled the development of Continuous-Variable Quantum Key Distribution (CV-QKD) protocols, in which the secret information is encoded into the amplitude and phase quadratures of the quantized electromagnetic field. An important advantage of CV-QKD lies in its compatibility with commercially available optical communication components. These protocols may employ either Gaussian modulation [2], [3] or discrete modulation schemes [4], [5]. Gaussian-modulated protocols already possess well-established security proofs in the literature [6]. However, they require an additional quantization stage after the quantum transmission phase, so that binary error-correcting codes, such as Low-Density Parity-Check (LDPC) codes [7], can be applied during reconciliation in order to align Alice’s and Bob’s raw keys.

The quantization of Gaussian variables is commonly performed through Slice Error Correction (SEC) [8] for signal-to-noise ratio (SNR) regimes above 0 dB, or through Multi-dimensional Reconciliation (MD) [9] in lower-SNR scenarios. More recently, [10] proposed Arithmetic Reconciliation (AR), initially referred to as the Distributional Transform Expansion, is an alternative quantization strategy for CV-QKD reconciliation. Compared to SEC and MD, AR presents lower computational complexity, since SEC needs to estimate the slicing functions and MD, the rotation matrices. Furthermore, AR has demonstrated competitive reconciliation efficiencies for its induced subchannels, particularly in negative-SNR operating regions [10], [11], [12].

In computer simulations, it is common to assume that the SNR is perfectly known, which leads to an ideal estimate of channel capacity. However, in practical situations, the SNR is obtained from the transmittance Γ and the excess noise ξ , calculated during the Parameter Estimation stage, which leads to a discrepancy from the ideal SNR, which may result in inadequate decoding conditions and a suboptimal code design, affecting the secret key rate (SKR) generated by the protocol.

In this paper, we investigate the impact of SNR mismatch on the bit error probability of AR-induced virtual subchannels and consequently on the degradation of their capacities, and on the secret key rate (SKR) provided by the AR with binary symmetric channels. We then discuss the implications of CV-QKD reconciliation performance, both for the choice of error-correcting codes and for the SKR generated by the protocol.

After this section, the paper is organized as follows: Sec. II

Rávilla R. S. Leite and Francisco M. de Assis, Department of Electrical Engineering, Federal University of Campina Grande (UFCG), Campina Grande-PB, Brazil. E-mails: ravilla.leite@ee.ufcg.edu.br, fmarcos@dee.ufcg.edu.br; Juliana M. de Assis, Federal University of Pernambuco (UFPE), Recife-PE, Brazil. E-mail: juliana.massis@ufpe.br. This work was partially financed by CNPq (311680/2022-4 and 140827/2022-6) and Fundação de Amparo à Ciência e Tecnologia do Estado de Pernambuco - FACEPE (APQ-1341-1.02/22).

describes the channel model and AR; Sec. III presents the main results about the Kullback-Leibler distance of mismatched distributions, error probability of induced BSC subchannels and Capacity. At the end, Sec. IV concludes the paper.

II. SYSTEM MODEL AND RECONCILIATION FRAMEWORK

A. Gaussian CV-QKD Channel Model

Gaussian-modulated CV-QKD protocols may employ either homodyne detection [2], in which Bob measures only one quadrature of Alice's quantum states at a time — requiring a sifting stage to discard non-matching bases — or heterodyne detection [3], where both quadratures are measured simultaneously, resulting in bidimensional random variables at the cost of an additional 50% loss introduced by the 50:50 beam splitter.

After the quantum measurement and sifting stages (in the case of homodyne detection), it is assumed that Alice and Bob share two correlated Gaussian random variables, X and Y respectively, such that the mutual information satisfies $I(X; Y) > 0$. These variables correspond to the so-called *raw keys*. Bob's received signal can be modeled as

$$Y = X + \frac{1}{\sqrt{\text{SNR}}}Z, \quad (1)$$

where $Z \sim \mathcal{N}(0, 1)$ denotes the noise in the quantum channel, assumed to be an Additive White Gaussian Noise (AWGN) channel, with Z statistically independent of X .

Assuming an optical-fiber Prepare-and-Measure (PM) implementation, the transmitted variable can be expressed as $X \sim \mathcal{N}(0, V_m)$, where V_m denotes Alice's modulation variance. The total variance is given by $V = V_m + V_0 = V_m + 1$, where $V_0 = 1$ corresponds to the vacuum shot-noise variance. The channel transmittance is defined as

$$\Gamma = 10^{-\alpha d/10}, \quad (2)$$

where $\alpha = 0.2$ dB/km is the optical-fiber attenuation coefficient and d denotes the transmission distance in kilometers. Under homodyne detection, the signal-to-noise ratio is given by

$$\text{SNR}_{\text{hom}} = \frac{\Gamma V_m}{1 + \xi}. \quad (3)$$

B. Arithmetic Reconciliation

AR, in summary, computes the cumulative distribution function (CDF) of Alice's and Bob's raw keys, mapping the realizations of X and Y uniformly onto the unit interval, i.e., $X, Y \mapsto U, V \in [0, 1]$. The binary expansion of a uniformly distributed RV over $[0, 1]$ generates i.i.d. (independent and identically distributed) bit sequences following a Bernoulli (1/2) distribution. Fig. 1 illustrates the overall AR procedure, considering a reverse reconciliation scheme in which Alice corrects her sequence to match Bob's, by using Slepian-Wolf LDPC coding. In the Slepian-Wolf scheme, Bob's sequence is compressed by the syndrome calculation, instead the traditional channel coding.

The resulting quantization with m bits of precision induces m binary symmetric channels (BSCs), whose crossover probabilities are defined as

$$e_i = \Pr(V_i^j \neq U_i^j), \quad (4)$$

for $1 \leq i \leq m$ e $1 \leq j \leq n$, where n is the number of samples. From the crossover probability, the binary entropy of each subchannel can be computed as

$$H(e_i) = -e_i \log(e_i) - (1 - e_i) \log(1 - e_i), \quad (5)$$

which allows the corresponding subchannel capacity to be calculated as $C_i = 1 - H(e_i)$.

C. SNR Mismatch Model

Equation 3 shows that the channel SNR is determined from the transmittance Γ and the excess noise ξ . In practical implementations, device imperfections and parameter-estimation inaccuracies may lead to discrepancies between the real and estimated SNR values, denoted by SNR and $\hat{\text{SNR}}$, respectively. This mismatch can be expressed as

$$\delta_{\text{SNR}} = \text{SNR} - \hat{\text{SNR}}, \quad (6)$$

or equivalently in terms of the noise variance as

$$\delta = 1 - \frac{\sigma_r^2}{\hat{\sigma}_r^2} \quad (7)$$

where δ denotes the relative deviation with respect to the real system's variance, σ_r^2 denotes the real noise's variance and $\hat{\sigma}_r^2$ represents the estimated variance.

To quantify the statistical discrepancy introduced by SNR mismatch, the Kullback-Leibler (KL) divergence was calculated between the actual channel distribution and the mismatched estimates at different SNR values.

The SNR mismatch directly affects the bit error probability e_i of each induced subchannel and, consequently, impacts both the bit error probability and the estimated subchannel capacities. As a result, the parametrization of the error-correcting codes employed during reconciliation is also affected, since the code rate is typically selected according to the estimated channel capacity. Furthermore, belief-propagation decoding algorithms rely on the computation of log-likelihood ratios (LLRs), which depend directly on e_i [13]:

$$\text{LLR}(U_i^j) = \log \frac{p(U_i^j = 0)}{p(U_i^j = 1)} \equiv (1 - 2 \cdot U_i^j) \log \frac{1 - e_i}{e_i}, \quad (8)$$

where U_i^j denotes Alice's j -th bit associated with the i -th subchannel. In this reverse reconciliation Slepian-Wolf framework [13], Alice's bits are employed as side information during the decoding process.

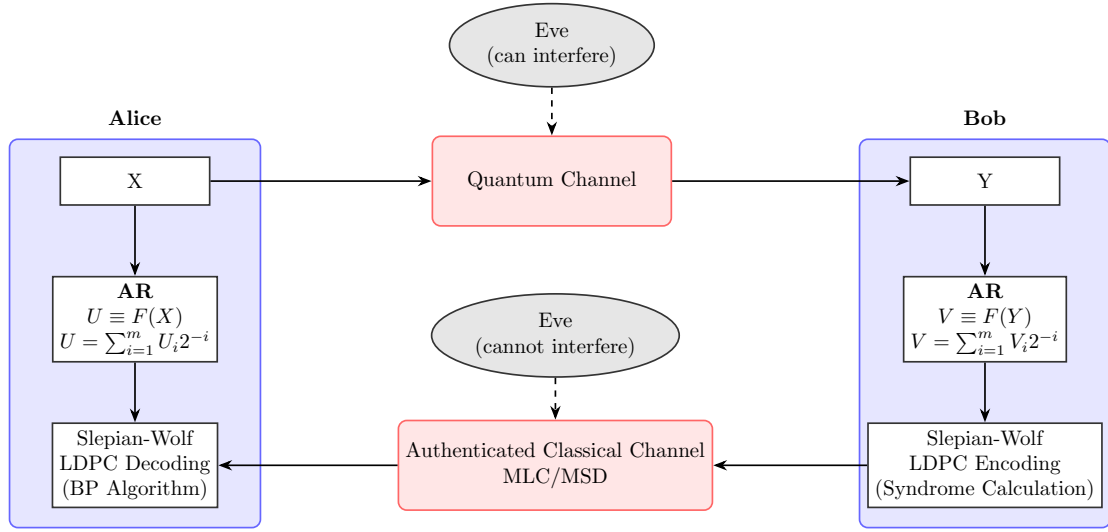


Fig. 1. General scheme of Arithmetic Reconciliation, illustrating how both Alice and Bob map their Gaussian variables onto the unit interval through the computation of the cumulative distribution function (CDF), followed by binary expansion, which generates statistically independent Bernoulli (1/2) bits. Finally, LDPC codes are employed within a multi-level coding/multi-stage decoding (MLC/MSD) reverse reconciliation framework, in which Alice corrects her sequence in order to match Bob's observations [?].

D. Reconciliation Efficiency and Secret Key Rate

Security proofs for QKD protocols can be derived at different levels, each of which considers different types of constraints on the eavesdropper's capabilities. Security against collective attacks is more robust than against individual attacks and is widely used in the literature [6], and for that reason, it will be adopted in this study. In a general way, the secret key rate (SKR) of CV-QKD protocol is obtained by

$$SKR^{\rightarrow} = \beta I_{AB} - \chi_{AE}, \quad (9)$$

$$SKR^{\leftarrow} = \beta I_{AB} - \chi_{BE}, \quad (10)$$

respectively for DR and RR, where β is the reconciliation efficiency. The upper bound on the information accessible to Eva in systems with *one-way* postprocessing, given by the Devetak–Winter Theorem

$$I_{AE} = \max_{Eva} \chi_{AE}, \quad (11)$$

as for I_{BE} in RR. χ_{AE}/χ_{BE} are the Holevo bounds in DR/RR, respectively.

The reconciliation efficiency of AR protocol is shown in [10], [11]:

$$\beta = \frac{\sum_{i=1}^m \beta_c C_i}{I(X; Y)} = \beta_c \beta_q, \quad (12)$$

where $\beta_c = \frac{R_i}{C_i}$ denotes the coding efficiency associated with the employed error-correcting code, with R_i representing its code rate, while $\beta_q = \frac{\sum_{i=1}^m C_i}{I(X; Y)}$ corresponds to the quantization efficiency, and $I(X; Y)$ denotes the Gaussian channel capacity. If we consider ideal codes with $R_i = 1$, β depends only on β_q . Therefore, inaccuracies in the estimated subchannel capacities also directly affect the reconciliation efficiency, degrading the overall system performance.

III. RESULTS AND DISCUSSION

A. KL Divergence Analysis

Simulations were performed considering relative mismatch levels of $\delta \in \{-0.2, 0.2, 0.5\}$ applied to the noise variance of the Gaussian channel, that is: $\delta = 0.2 \rightarrow \sigma_r^2 = 0.8\sigma_r^2$, $\delta = -0.2 \rightarrow \sigma_r^2 = 1.2\sigma_r^2$ and $\delta = -0.5 \rightarrow \sigma_r^2 = 1.5\sigma_r^2$. Initially, the KL divergence between the real Gaussian distributions and the mismatched distributions was evaluated according to the KL distance between two Gaussian distributions with the same mean and different variances. Let, $\phi_1(x) \sim \mathcal{N}(\mu, \sigma_1^2)$ and $\phi_2(x) \sim \mathcal{N}(\mu, \sigma_2^2)$, we have

$$\begin{aligned} D(\phi_1 || \phi_2) &= \mathbb{E}_{\phi_1} \ln \frac{\phi_1}{\phi_2} \\ &= \mathbb{E}_{\phi_1} \ln \frac{\frac{1}{\sqrt{2\pi}\sigma_1} \exp\left\{-\frac{(X-\mu)^2}{2\sigma_1^2}\right\}}{\frac{1}{\sqrt{2\pi}\sigma_2} \exp\left\{-\frac{(X-\mu)^2}{2\sigma_2^2}\right\}} \\ &= \mathbb{E}_{\phi_1} \ln \frac{\sigma_2}{\sigma_1} \exp\left\{-\frac{(X-\mu)^2}{2\sigma_1^2} + \frac{(X-\mu)^2}{2\sigma_2^2}\right\} \\ &= \mathbb{E}_{\phi_1} \ln \frac{\sigma_2}{\sigma_1} + \mathbb{E}_{\phi_1} \left(\frac{(X-\mu)^2}{2\sigma_2^2} - \frac{(X-\mu)^2}{2\sigma_1^2} \right) \\ &= \ln \frac{\sigma_2}{\sigma_1} + \frac{1}{2\sigma_2^2} \mathbb{E}_{\phi_1} (X-\mu)^2 - \frac{1}{2\sigma_1^2} \mathbb{E}_{\phi_1} (X-\mu)^2 \\ &= \ln \frac{\sigma_2}{\sigma_1} + \frac{\sigma_1^2}{2\sigma_2^2} - \frac{1}{2}. \end{aligned} \quad (13)$$

Fig. 2 presents the obtained results, illustrating how the probabilistic model assumed by the receiver progressively diverges from the effective channel distribution under SNR mismatch conditions. It can be observed that the KL divergence reaches its minimum value only when the assumed distribution coincides with the actual channel statistics. In

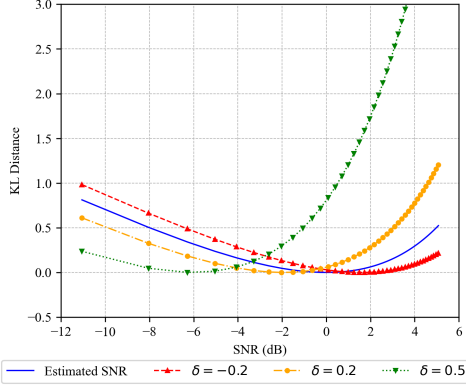


Fig. 2. Kullback–Leibler (KL) distance between the ideal Gaussian distribution and the mismatched distributions as a function of the signal-to-noise ratio (SNR). The mismatch conditions were generated considering deviations of $\delta \in \{-0.2, 0.2, 0.5\}$ in the noise variance.

the ideal scenario, this occurs at the nominal SNR of the system. However, as the SNR increases, the KL divergence rises again, indicating that even small discrepancies between the variances become progressively more relevant from a statistical perspective. This behavior demonstrates that the KL distance is not directly associated with channel quality, but rather with the degree of incompatibility between the probabilistic models under consideration. Furthermore, when the noise variance assumed at the receiver is smaller than the actual channel variance, the minimum-divergence operating point shifts toward positive SNR values.

B. Bit Error Probability and Capacity Degradation

Arithmetic Reconciliation was applied to quantize the Gaussian realizations of X and Y using $m = 4$ bits of precision. Previous studies have shown that with more than 4 channels, the performance gains are almost negligible [11]. For each induced subchannel, the error probability and channel capacity were empirically estimated by comparing the transmitted and received bits.

The parameters used in the simulations were as follows: optical fiber attenuation $\alpha = 0.2$ dB/km, electronic noise at Bob's end $\nu_{el} = 0.041$, efficiency of Bob's detector $\eta_{det} = 0.606$, excess noise relative to the channel input $\xi_A = 0.01$ and transmittance $\Gamma \in [0.02, 0.84]$ with 41 points.

Fig. 3 shows the impact of SNR mismatch on the capacities of BSC subchannels induced by AR quantization. It can be observed that the most significant subchannels ($m = 1$ and $m = 2$) are considerably more sensitive to the effects of mismatch, particularly at higher SNR levels, where the separation between the capacity curves becomes increasingly pronounced. For SNR values below approximately -5 dB, only the first subchannel exhibits a noticeable degradation in capacity, indicating that, under conditions of intense noise, the less significant subchannels are already operating near their minimum achievable capacities, regardless of the level of mismatch considered.

The results indicate that the mismatch introduces a heterogeneous degradation among the subchannels, as can be seen

in Fig. 3, predominantly affecting the most significant bit-planes (subchannels 1 and 2), which originally exhibit lower crossover probabilities (greater capacities).

This behavior has a direct impact on CV-QKD reconciliation, since the estimated subchannel capacities are used as references for selecting the rate and robustness of the error-correcting codes employed during reconciliation. When the SNR is overestimated, i.e., when the receiver assumes a channel condition better than the actual one, the estimated subchannel capacity becomes artificially higher than the effective channel capacity. Consequently, higher-rate codes with lower redundancy may be selected, even though they are unable to reliably correct the actual channel errors due to the reduced effective capacity. This scenario leads to an apparently improved spectral efficiency, since fewer redundancy bits are transmitted, while simultaneously degrading the effective decoding performance and increasing the probability of decoding failures.

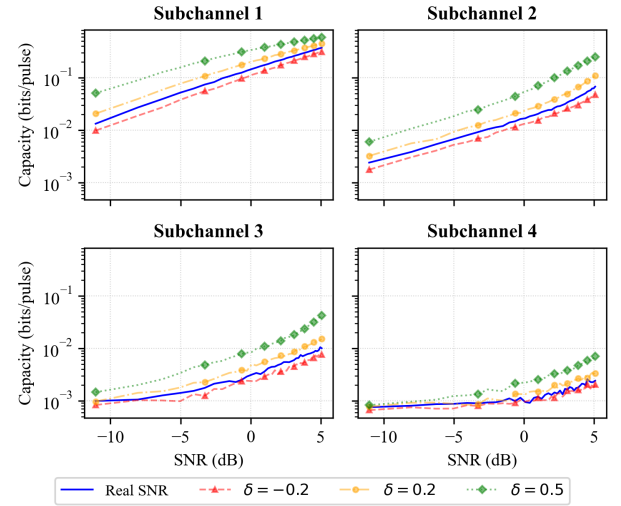


Fig. 3. Capacity of the induced BSC subchannels considering ideal and mismatched SNR conditions. The results were obtained for noise variance deviations of $\delta \in \{-0.2, 0.2, 0.5\}$ relative to the reference variance σ_r^2 .

Conversely, underestimating the SNR leads to conservative capacity estimates, favoring the selection of excessively robust low-rate codes with unnecessary redundancy. Although this approach improves decoding reliability, it also increases computational complexity and reduces the spectral efficiency of the system, unnecessarily limiting the useful information rate, especially considering that redundancy levels in reconciliation procedures are already naturally high. In addition, the unnecessary use of redundancy contributes to a greater leak of information to Eve.

Figure 4 illustrates the impact of SNR mismatch in the SKR provided by the protocol when we consider BSC subchannels. It is important to note that the induced subchannels can also be treated as BIAWGN channels. In this case, the continuous-discrete mutual information $I(X; V_i)$ (RR) or $I(U_i; Y)$ (DR) is obtained from estimators. The BIAWGN case provides greater SKR than the BSC model, but this analysis is outside the scope of this work.

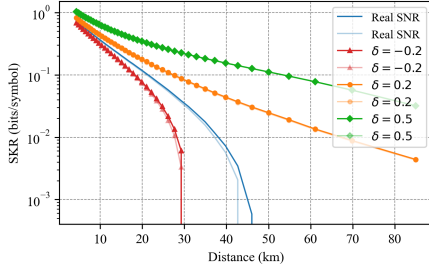


Fig. 4. SKR obtained with BSC subchannels considering ideal and mismatched SNR conditions. The results were obtained for noise variance deviations of $\delta \in \{-0.2, 0.2, 0.5\}$ relative to the reference variance σ_r^2 , that represents the real channel SNR. Solid lines illustrates the behavior when we use 4 channels of quantization and transparent lines, 2 channels of quantization.

The obtained results demonstrate that even small inaccuracies in SNR estimation may produce significant deviations in the statistical characterization of the induced subchannels, directly affecting the trade-off between decoding robustness, spectral efficiency, and computational complexity during CV-QKD reconciliation.

Finally, the fact that the mismatch does not affect all induced subchannels uniformly reinforces the need for distinct error-correcting code parametrizations for each subchannel, further motivating multi-level coding (MLC) reconciliation strategies in practical CV-QKD implementations. These observations highlight the importance of accurate parameter estimation and adaptive reconciliation strategies for reliable low-SNR CV-QKD operation.

IV. CONCLUSIONS

In this work, we investigated the effects of SNR overestimation and underestimation in Gaussian-modulated CV-QKD systems employing AR, considering that, in practical implementations, the channel SNR must be estimated from the optical-fiber transmittance and excess noise parameters. In particular, the obtained results showed that the most significant induced subchannels are considerably more sensitive to SNR mismatch, exhibiting larger BER and capacity degradations, whereas the least significant subchannels are comparatively less affected by the considered mismatch levels. Furthermore, the results showed important practical implications for the reconciliation stage.

Underestimating the SNR leads to the unnecessary use of excessively robust low-rate error-correcting codes, increasing computational complexity and reducing spectral efficiency, leading to a falsely higher SKR, which could compromise the protocol's security. Overestimating the SNR degrades the effective decoding performance due to insufficient redundancy, leading to a conservative estimate of the SKR, reducing system efficiency. Therefore, the results demonstrate that accurate SNR estimation is a fundamental requirement for the practical implementation of CV-QKD systems employing AR. Future investigations may explore adaptive reconciliation and robust decoding strategies capable of mitigating the effects

of parameter-estimation inaccuracies in low-SNR CV-QKD regimes.

ACKNOWLEDGEMENTS

The authors would like to thank CNPq and COPELE - UFCG for their financial support and IQuanta for the opportunity to carry out this research and for the availability of structure and material support.

REFERENCES

- [1] M. A. Nielsen and I. L. CHUANG, *Quantum Computation and Quantum Information*. Cambridge University Press, 2010.
- [2] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Phys. Rev. Lett.*, vol. 88, p. 057902, Jan 2002.
- [3] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, "Quantum cryptography without switching," *Phys. Rev. Lett.*, vol. 93, p. 170504, Oct 2004.
- [4] 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, June 2019.
- [5] A. Leverrier and P. Grangier, "Unconditional security proof long-distance continuous-variable quantum key distribution with discrete modulation," *Physical Review Letters*, pp. 180504–1–180504–4, May 2009.
- [6] F. Laudenbach, C. Pacher, C. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, "Continuous-variable quantum key distribution with gaussian modulation—the theory of practical implementations," *Advanced Quantum Technologies*, vol. 1, June 2018.
- [7] M. Milicevic, C. Feng, L. M. Zhang, and P. G. Gulak, "Key reconciliation with low-density parity-check codes for log-distance quantum cryptography," *arXiv preprint arXiv:1702.07740*, Feb 2017.
- [8] G. Van Assche, J. Cardinal, and N. J. Cerf, "Reconciliation of a quantum-distributed gaussian key," *IEEE Transactions on Information Theory*, vol. 50, no. 2, pp. 394–400, 2004.
- [9] A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, "Multidimensional reconciliation for a continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 77, p. 042325, Apr 2008.
- [10] M. A. Dias and F. M. de Assis, "Distributional transform based information reconciliation," *Journal of Communication and Information Systems*, vol. 39, p. 74–81, May 2024.
- [11] R. R. S. Leite, J. M. d. Assis, and F. M. d. Assis, "Arithmetic reconciliation for cvqkd protocols," in *to appear in Anais do XLIII Simpósio Brasileiro de Telecomunicações e Processamento de Sinais - SBrT2025*, (Natal, Brasil), Sociedade Brasileira de Telecomunicações, 2025.
- [12] R. R. S. Leite, J. M. de Assis, M. A. Dias, and F. M. de Assis, "Arithmetic reconciliation for cvqkd: Challenges and feasibility," *arXiv preprint arXiv:2602.05526*, 2026.
- [13] A. D. Liveris, Z. Xiong, and C. N. Georghiades, "Compression of binary sources with side information at the decoder using ldpc codes," *IEEE Communications Letters*, vol. 6, Oct 2002.
- [14] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, pp. 1301–1350, Sep 2009.