Arithmetic Reconciliation for CVQKD Protocols

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

Abstract— **Quantum key distribution allows the distribution of a secret key with applications to cryptography. Specially, continuous variable quantum key distribution presents some advantages over its discrete counterpart and involves a reconciliation protocol where the continuous variable must be transformed to a binary sequence common to both trusted parties. Recently proposed, Arithmetic Reconciliation is one of the possible schemes. In this paper, we evaluate the performance of this scheme both mathematically and through simulations, as also achieve expressions and simulations for the obtained reconciliation efficiencies. These results suggest that Arithmetic Reconciliation is a promising technique in continuous variable quantum key distribution.**

Keywords— **Reconciliation, CVQKD, Cryptography, Distributional Transform.**

I. Introduction

It is a well known fact that one-time pad is an encryption technique that provides no information about the original message to an untrusted party. In 1917, using an electrical system, Gilbert Vernam implemented the one-time pad scheme for crytography [1], and its perfect secrecy was proved by Claude Shannon in 1949 [2]. However, one-time pad requires a secret key that has at least the same length of the message, which imposes difficulty to its usage. Quantum key distribution (QKD) schemes, such as BB84 [3], allow a secure distribution of the key, by the no-cloning theorem of quantum mechanics, which guarantees that any measurement from an untrusted part (Eve) in the quantum channel would disturb the coherent state [4].

QKD schemes may be performed with discrete or continuous variables. Specifically, continuous variable QKD (CVQKD) may use the quadratures of quantized electromagnetic fields [5], [6], [7], [8] and presents some advantages over the discrete variable QKD. Mainly, it is relatively easy to implement with the existing telecommunications equipments, allows higher secret rates [9], [10], [11], [12], and may be used with room temperatures [4].

In CVQKD, the trusted parties to achieve the secret key, Alice and Bob, share a noisy quantum channel. Thus, their continuous variables will differ, and the reconciliation protocol is one step in which one of these variables is discretized to a random binary sequence (which will be the secret key). Alice and Bob will exchange reconciliation messages publicly in order to achieve a common secret key, and a posterior step of privacy amplification must be performed to guarantee that Eve will not gain information about the key through these reconciliation messages [9].

One of the proposed reconcilition schemes is Arithmetic Reconciliation [13]. Firstly introduced in [14], it was further defined and explored in reference [15], based in results from the copula and information theories. Specifically, reference [15] shows that the technique achieves maximum efficiency, in reverse reconciliation, greater than 0.9, in a regime with SNR less than -3.6 dB (with heterodyne measurements). The aim of this paper is to highlight its performance with the use of more subchannels, introducing the mathematical and simulated values of bit error probability, considering a realistic scenario where the maximum efficiency is not necessarily achieved.

In order to do so, in Section II, we summarize the Arithmetic Reconciliation protocol. In Section III we present the bit error probabilities for the second subchannel mathematically and for other subchannels in a similar SNR range that is found in optical channels. In Section IV we present the calculation and simulations for reconciliation efficiency. Finally, Section V concludes the paper.

II. Arithmetic Reconciliation

Considering the quantum channel as an Additive White Gaussian Noise (AWGN) channel, after the sifting step, it is assumed that Alice and Bob share two correlated Gaussian sequences, denoted respectively by X and Y, referred to as raw keys, with mutual information greater than zero, i.e., $I(X;Y) > 0$ [5]. Alice holds N realizations of X, corresponding to her prepared quantum states, while Bob holds N realizations of $Y = X + \sqrt{N}Z$, where $X, Z \sim \mathcal{N}(0,1)$, $X \perp Z$ and $N = 1/SNR$.

To ensure that the keys match, an information reconciliation step is required, in which the Gaussian values are quantized and error correction is applied — typically through a Binary Correction Protocol (BCP) [9]. Error correction is generally performed using LDPC codes, as they operate close to the Shannon limit even under low-SNR conditions (around 0 dB) and offer lower decoding complexity compared to other powerful code families, such as Turbo Codes [16], [17], [18].

The reconciliation step occurs over an authenticated classical channel, assumed to be error-free, through which the eavesdropper may observe the exchanged messages but cannot tamper with them. Let $I(X;Y)$ denote the mutual information between Alice and Bob's raw keys; in practice, only a fraction $\beta I(X;Y)$ of this mutual information can be extracted, with $\beta < 1$ representing the reconciliation efficiency [19], [13]. Therefore, assuming a sufficiently efficient BCP-based reconciliation scheme, the protocol is expected to yield $\beta I(X;Y) - \chi_{AE}$ bits per transmitted state under direct reconciliation, and $\beta I(X;Y) - \chi_{BE}$ under reverse reconciliation where χ_{AE} and

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).

χ_{BE} are the Holevo bounds for the information accessible to Eve about Alice's and Bob's keys, respectively [19], [15]. The reconciliation efficiency β depends on both the quantization technique and the error-correcting code employed.

The most widely adopted reconciliation techniques include the Slice Error Correction (SEC) protocol [9], [19] and Multidimensional Reconciliation (MD-Reconciliation) [20], [10], which enable the generation of binary sequences from continuous values, allowing the subsequent application of error-correcting codes. An alternative to these protocols is the quantization technique proposed by Araújo and Assis [13], which is based on Lemma 1, derived from Arithmetic Source Coding and inspired by the Shannon-Fano-Elias coding scheme [21]. This method significantly simplifies the process by eliminating the need for optimal estimator search for slicing functions (as required in SEC) and for algebraic multidimensional rotations (as required in MD-Reconciliation). The technique is comprehensively described in [13], [15], [22].

Lemma 1: Let V be a random variable with a continuous distribution function $F(V)$, define $U = F_V(V)$ its cumulative distribution function. So, U is uniformly distributed on $[0,1]$.

Lemma 1 is known in Copula Theory as the "Distributional Transform" [15], and ensures that transforming a random variable with a continuous distribution function (CDF) through its own cumulative distribution function (CDF) always results in a uniform distribution over the interval $[0,1]$. The bits resulting from the binary expansion of a random variable with distribution $unif \sim [0,1]$ are independent and Bernoulli ($\frac{1}{2}$) [21]. Figure II illustrates the configuration considered during the quantization step, where the quantum channel is modeled as an AWGN channel with correlation $\rho(X,Y)$, followed by the mappings $X \mapsto F_X(X) \mapsto U$ and $Y \mapsto F_Y(Y) \mapsto V$, such that each realization of X is transformed into a corresponding bit sequence with m-bit precision: $x_i \mapsto u_1 u_2 \ldots u_m$ (similarly for $y_i \mapsto v_1 v_2 \ldots v_m$).

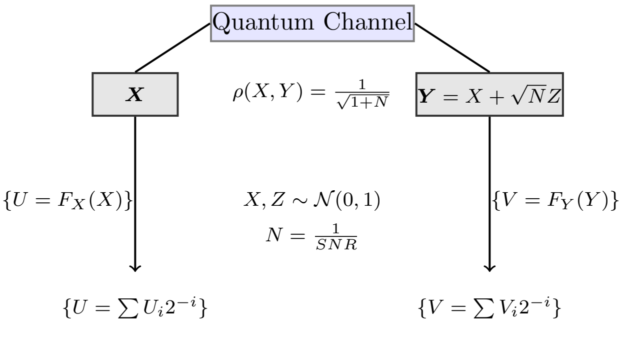
Quantum Channel
$\boldsymbol{X}$
$\rho(X,Y) = \frac{1}{\sqrt{1+N}}$
$\boldsymbol{Y} = X + \sqrt{N}Z$
$\{U = F_X(X)\}$
$X, Z \sim \mathcal{N}(0,1)$
$N = \frac{1}{SNR}$
$\{V = F_Y(Y)\}$
$\{U = \sum U_i 2^{-i}\}$
$\{V = \sum V_i 2^{-i}\}$

Fig. 1. Initial setup of Arithmetic Reconciliation, modeling the quantum channel as an AWGN channel with correlation $\rho(X,Y)$, where X represents Alice's sequence and Y corresponds to Bob's. Alice and Bob compute the cumulative distribution functions (CDFs) of their respective Gaussian sequences, and subsequently perform binary expansions of the resulting values, yielding the variables U and V, respectively.

The transformation of X and Y by calculating the CDF preserves the initial mutual information, i.e. $I(X;Y) = I(F_X(X);F_Y(Y))$ because mutual information is invariant to homeomorphisms and the CDF is considered to be one of them [23]. Alice and Bob can then use this technique to produce correlated binary sequences from the continuous data of their raw keys. Since the bits generated in the binary expansion are independent of each other, the sequences $U_i = u_1, ..., u_j$ and $V_i = v_1, ..., v_j$, for $1 \leq i \leq n$ and $j = 1, ..., m$, the bits of the j-th position in U and V are correlated and can be treated as memoryless BSC (Binary Symmetric Channel) channels with inversion probability $e_j = Pr[U_{i(j)} \neq V_{i(j)}]$ [24], which can be obtained analytically or computationally.

III. Performance of the Arithmetic Reconciliation Subchannels

A. Performance analysis for the second Subchannel

In [25] we considered the bit error probability for the first subchannel ($j = 1$). Now we will specialize to the second subchannel ($j = 2$).

The following remark will be useful soon. Consider the numbers 2^{-i}, $i = 1, 2, \ldots$, let us compute the reals $y_i = F_Y^{-1}(2^{-i})$ in terms of the standard normal distribution.

$$\begin{aligned}
2^{-i} &= \int_{-\infty}^{y_i} \frac{1}{\sqrt{2\pi(N+1)}} e^{-\frac{1}{2}\frac{u^2}{N+1}} du \\
&= \int_{-\infty}^{y_i/\sqrt{N+1}} \frac{1}{\sqrt{2\pi}} e^{-\frac{v^2}{2}} dv \\
&= \Phi\Big(\frac{y_i}{\sqrt{N+1}}\Big) \\
&= \Phi\left(\frac{F_Y^{-1}(2^{-i})}{\sqrt{N+1}}\right)
\end{aligned}$$

From the last equality, inverting the the distribution function $\Phi(\cdot)$ we obtain

$$\begin{aligned}
y_i &= F_Y^{-1}\left(2^{-i}\right) = \sqrt{1+N}\,\Phi^{-1}\Big(2^{-i}\Big) && (1)\\
&= \sqrt{1+\frac{1}{\text{SNR}}}\,\Phi^{-1}\Big(2^{-i}\Big) && (2)\\
&= \sqrt{1+\frac{1}{\text{SNR}}}\,x_i, && (3)
\end{aligned}$$

where, for ease the notation we set $x_i = \Phi^{-1}\Big(2^{-i}\Big)$.

Now, let us define the event :

$$E = \{U_2 = 0, V_2 = 1\}$$

Event E can happen in four mutually exclusive ways:

$$\begin{aligned}
E_1 &= \{F_X(X) < 1/4 \cap 1/4 < F_Y(Y) < 1/2\}\\
E_2 &= \{F_X(X) < 1/4 \cap F_Y(Y) > 3/4\}\\
E_3 &= \{1/2 < F_X(X) < 3/4 \cap 1/4 < F_Y(Y) < 1/2\}\\
E_4 &= \{1/2 < F_X(X) < 3/4 \cap F_Y(Y) > 3/4\}\\
E &= \cup_{i=1}^{4} E_i,
\end{aligned}$$

and we will describe them in terms of the variables X and Z, considering the correct limits of integration of the bivariate normal density f_{XZ}, as shown next (and illustrated in Figure 2).

$$\begin{aligned}
\Pr[E_1] &= \Pr[X < \Phi^{-1}(1/4), F_Y^{-1}(1/4) < Y < F_Y^{-1}(1/2)] \\
&= \Pr\left[X < x_2, y_2 < X + \sqrt{N}Z < 0\right] \\
&= \Pr\left[X < x_2, \frac{y_2 - X}{\sqrt{N}} < Z < -\frac{X}{\sqrt{N}}\right]
\end{aligned}$$

$$\begin{aligned}
\Pr[E_1] &= \int_{-\infty}^{x_2} \int_{\frac{y_2 - x}{\sqrt{N}}}^{\frac{-x}{\sqrt{N}}} \frac{1}{2\pi} e^{-\frac{x^2+z^2}{2}} dz dx \\
&= \int_{-\infty}^{x_2} \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}} \left(\Phi\left(\frac{-x}{\sqrt{N}}\right) - \Phi\left(\frac{y_2 - x}{\sqrt{N}}\right) \right) dx \\
&= \int_{-\infty}^{x_2} \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}} \Bigg(\Phi(-\sqrt{SNR}x) \\
&\quad -\Phi(\sqrt{SNR+1}x_2 - \sqrt{SNR}x) \Bigg) dx
\end{aligned}$$

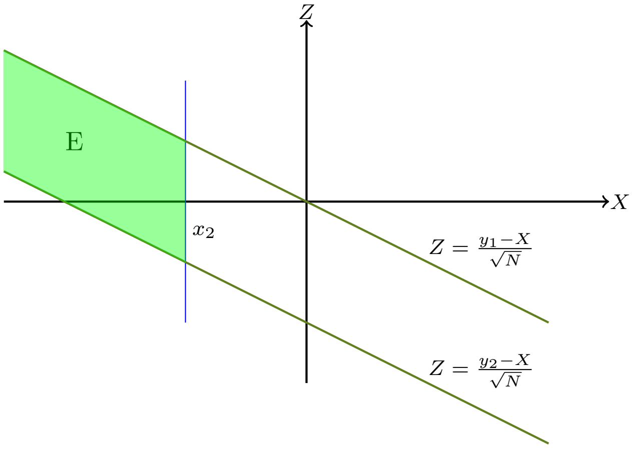
Z
E
X
x_2
$Z = \frac{y_1 - X}{\sqrt{N}}$
$Z = \frac{y_2 - X}{\sqrt{N}}$

Fig. 2. Integration region for event E_1.

Similarly, we may evaluate the probabilities associated with E_2, E_3 and E_4.

Figure 3 illustrates the evaluated bit error probability, as also the curve for the simulated channel (as expected, both curves achieve similar values).

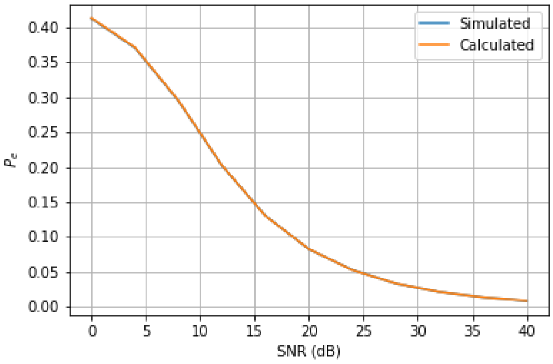

Fig. 3. Simulated and calculated ($2 \times P_E$ versus SNR) bit error probabilities for the second channel.

B. Performance of the other subchannels

Figure 4 shows the error probability for 7 BSC channels obtained with quantization in a very low SNR region (from -20 to 2 dB). Figure 5 shows the capacity of each channel, calculated by $C_j = 1 - h(e_j)$, where $h(e_j)$ is the binary entropy $h(e) = -e\log(e) - (1-e)\log(1-e)$.

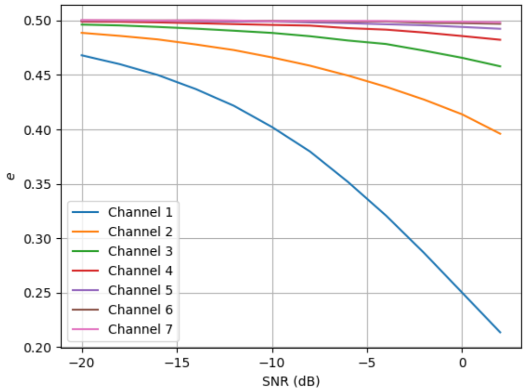

Fig. 4. Average error probability of each subchannel for $m = 7$, obtained through simulations with 1000 samples for each SNR value in the range from -20 to 2 dB.

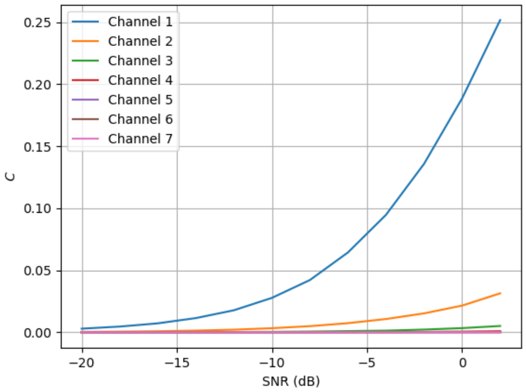

Fig. 5. Capacity of each BSC channel obtained after quantization, in SNR region from -20 to 2 dB, calculated from the error probabilities obtained previously.

IV. Reconciliation Efficiency

The reconciliation efficiency depends on the quantization efficiency and the error-correcting code used in each channel. With regard to quantization, the aim is to maximize the mutual information between the bits produced for each realization of X, U, and the Gaussian values of Y, $I(U;Y)$. The quantization efficiency indicates how much of the mutual information $I(X;Y)$ has been preserved. Considering a multilevel coding (MLC) scheme, each channel obtained from quantization will be coded independently from the syndrome calculation (Slepian-Wolf Coding), using a LDPC code with rate R_i $(1 \leq i \leq m)$. Although the use of Slepian-Wolf coding transforms the problem into a case of Distributed Source Coding (DSC), where syndrome computation is treated as a form of source compression, [22] shows that the decoding algorithm can only successfully recover the sequences when the capacity of the Binary Symmetric Channel (BSC) exceeds the code rate — thus characterizing it as a channel coding problem. Since this rate is limited by the capacity of each channel, the use of real codes will introduce another source of inefficiency.

In a similar way to the calculation of the SEC protocol's Reconciliation Efficiency presented by Jouguet and others [19], Dias and Assis [15] derived the expressions for the maximum reconciliation efficiency achievable with Arithmetic Reconciliation, i.e. when ideal codes are used with $R_i = C_i$. Considering a direct reconciliation scheme, the maximum quantization efficiency $\beta_q^{\rightarrow}$ is given by:

$$\beta_{q\ max}^{\rightarrow} = \frac{I(U;Y)}{I(X;Y)} = \frac{\sum_{i=1}^{m} I(U_j;Y)}{I(X;Y)}, \tag{4}$$

where $U = \sum_{i=1}^{m} U_i 2^{-i}$ and

$$I(U;Y) = H(U) - H(U|Y). \tag{5}$$

$H(U|Y)$ is the minimum amount of information that Alice can transmit over the classical channel (maximum compression) that allows Bob to reconstruct U. Assuming that there are d quantization intervals on the unit interval, with $d = 2^m$, so $p(d)$ is the same for all intervals, and that the bits in the binary expansion are equiprobable, then:

$$\begin{aligned} H(U) &= \sum_{i=1}^{m} H(U_i) \\ &= -\sum_{d=1}^{2^m} p(d) \cdot \log_2 p(d) = m. \end{aligned} \tag{6}$$

Substituting 5 in 4 and considering the approximation $H(U|Y) \approx \sum_{i=1}^{m} h(e_i)$, as occurs in [9], $I(U;Y)$ can be rewritten as:

$$I(U;Y) = m - \sum_{i=1}^{m} h(e_i). \tag{7}$$

Since $C_i = 1 - h(e_i)$:

$$I(U;Y) = \sum_{i=1}^{m} C_i. \tag{8}$$

$\beta_{q\ max}^{\rightarrow}$ will be given by:

$$\beta_{q\ max}^{\rightarrow} = \frac{\sum_{i=1}^{m} C_i}{I(X;Y)}. \tag{9}$$

Similarly, the maximum quantization efficiency for a reverse reconciliation scheme can be calculated by:

$$\beta_{q\ max}^{\leftarrow} = \frac{\sum_{i=1}^{m} I(V_i;X)}{I(X;Y)}. \tag{10}$$

The Lemma 1 guarantees that $F_Y(Y)$ has a uniform distribution on $[0,1]$, and that therefore the d intervals in the calculation of V are also equiprobable, even if the noise makes the limits $(\tau_1, \ldots, \tau_{t-1})$ in Y different from those in X. Therefore, the same considerations - $H(V) = m$ and $H(V;X) = \sum_{i=1}^{m} h(e_i)$ - can be made:

$$\begin{aligned} \beta_{q\ max}^{\leftarrow} &= \frac{H(V) - H(V|X)}{I(X;Y)} \\ &= \frac{m - m + \sum_{i=1}^{m} C_i}{I(X;Y)} \\ &= \frac{\sum_{i=1}^{m} C_i}{I(X;Y)}. \end{aligned} \tag{11}$$

It can then be seen that there is symmetry between direct and reverse reconciliation, leading to the same performance, i.e. $I(U;Y) = I(V;X)$ [15].

Assuming that in real systems the channel capacity is not fully utilized and the individual error-correcting codes of each subchannel have rate $R_i \leq C_i$, the efficiency over the entire reconciliation system, considering sub-optimal codes, is given by:

$$\beta = \frac{\sum_{i=1}^{m} R_i}{I(X;Y)}. \tag{12}$$

Since the code efficiency $\beta_c = \frac{R_i}{C_i}$ is seen as the ratio between the rate of real codes and ideal ones, β can be rewritten as:

$$\beta = \frac{\sum_{i=1}^{m} \beta_c C_i}{I(X;Y)}. \tag{13}$$

$$\beta = \beta_c \beta_{disc}. \tag{14}$$

It can then be seen that reconciliation efficiency depends directly on the rate of the available codes R_i and how close they are to the capacity of each channel.

Some investigations have been carried out in order to evaluate the reconciliation efficiency of the proposed technique in the range from -20 to 2 dB of SNR and how much the increase in the number of channels adds to the mutual information achieved. Figure 6 shows the mutual information $I(U;Y)$ with $m = 1, \ldots, 7$ bits of quantization precision, compared to the mutual information of the Gaussian channel, which serves as the upper bound. Figure 7 shows the quantization efficiency obtained with the same bit levels. It can be seen that above 3 bits of quantization the gain in mutual information achieved is not significant and that the quantization efficiency improves as the SNR decreases, which makes the technique promising for application in CVQKD protocols.

The results corroborate what was obtained in [13], in which it was shown that from the 4th channel onwards, the high error probabilities between the quantized sequences mean that the channels are not suitable for key sharing. The 3rd and 4th channels, however, can be disclosed without coding to help correct the most significant bits and then discarded, similar to what happens in the SEC protocol [9], [19], depending on the error correction technique to be used.

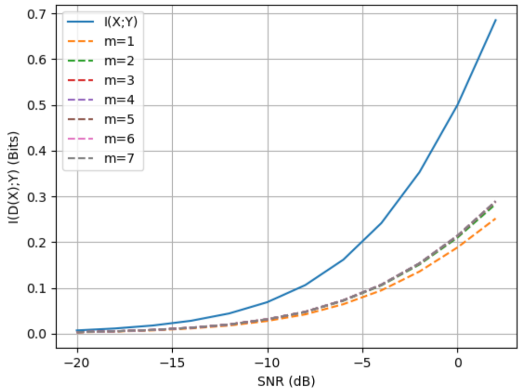

Fig. 6. Mutual information $I(U;Y)$ obtained for different quantization precisions ($m = 1, \ldots, 7$ bits), in comparison with the mutual information of the Gaussian channel, considered the theoretical upper bound.

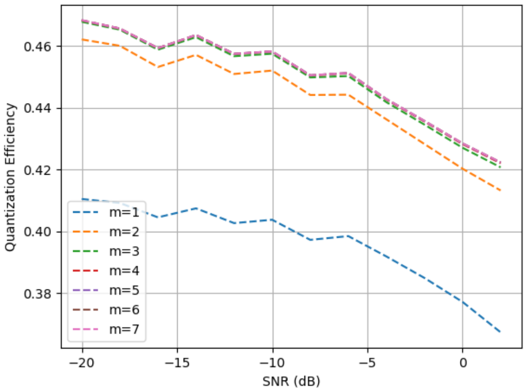

Fig. 7. Quantization efficiency $\beta = I(U;Y)/I(X;Y)$ for varying quantization precisions ($m = 1, \ldots, 7$ bits). The results highlight the diminishing gains in efficiency beyond 3 bits and the improved performance at lower SNR values.

V. Conclusions

In this paper we reviewed the Arithmetic Reconciliation technique, evaluating its performance mathematically and with simulations in regions with low SNRs, as found in real scenarios. We also presented the reconciliation efficiencies expressions and the values obtained in simulations. The results indicate that Arithmetic Reconciliation technique is a promising technique in the context of CVQKD.

Aknowledgements

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] W. Peng, S. Cui, and C. Song, “One-time-pad cipher algorithm based on confusion mapping and dna storage technology,” *Plos one*, vol. 16, no. 1, p. e0245506, 2021.

[2] C. E. Shannon, “Communication theory of secrecy systems,” *The Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[3] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” *International Conference on Computers, Systems, and Signals Processing*, pp. 175–179, 1984.

[4] M. Milicevic, C. Feng, L. M. Zhang, and P. G. Gulak, “Key reconciliation with low-density parity-check codes for long-distance quantum cryptography,” *ArXiv*, 2017.

[5] F. Grosshans and P. Grangier, “Continuous variable quantum cryptography using coherent states,” *Phys. Rev. Lett.*, vol. 88, p. 057902, Jan 2002.

[6] F. Grosshans, G. Van Assche, and J. e. a. Wenger, “Quantum key distribution using gaussian-modulated coherent states,” *Nature*, vol. 421, pp. 238–241, Jan 2003.

[7] 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.

[8] Y.-M. Li, X.-Y. Wang, Z.-L. Bai, W.-Y. Liu, S.-S. Yang, and K.-C. Peng, “Continuous variable quantum key distribution,” *Chinese Physics B*, vol. 26, no. 4, p. 040303, 2017.

[9] G. V. Assche, J. Cardinal, and N. J. Cerf, “Reconciliation of a quantum-distributed gaussian key,” *IEEE Transactions on Information Theory*, vol. 50, Feb 2004.

[10] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, “Long-distance continuous-variable quantum key distribution with a gaussian modulation,” *Physical Review A*, vol. 84, Dec 2011.

[11] P. Jouguet and S. Kunz-Jacques, “High performance error correction for quantum key distribution using polar codes,” *Quantum Info. Comput.*, vol. 14, p. 329–338, mar 2014.

[12] 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.

[13] L. M. C. d. Araújo, “Novo método de quantização para protocolos de reconciliação de chaves secretas geradas quanticamente utilizando códigos ldpc no sentido slepian-wolf,” 2017.

[14] L. M. C. Araújo, F. M. de Assis, and B. B. Albert, “Novo protocolo de reconciliação de chaves secretas geradas quanticamente utilizando códigos ldpc no sentido slepian-wolf,” in *Anais do XXXVI Simpósio Brasileiro de Telecomunicações e Processamento de Sinais - SBrT2018*, (Campina Grande, Brasil), pp. 885–889, Sociedade Brasileira de Telecomunicações, 2018.

[15] M. A. Dias and F. M. d. Assis, “Distributional transform based information reconciliation,” *Journal of Communication and Information Systems*, vol. 39, no. 1, 2024.

[16] T. J. Richardson, M. A. Shokrollahi, and R. L. Urbanke, “Design of capacity-approaching irregular low-density parity-check codes,” *IEE Transactions on Information Theory*, vol. 47, pp. 619–637, feb 2001.

[17] A. Leverrier and P. Grangier, “Continuous-variable quantum key distribution protocols with a discrete modulation,” jan 2011.

[18] S. J. Johnson, *Iterative Error Correction. Turbo, Low-Density Parity-Check and Repeat-Accumulate Codes*. Cambridge University Press, 2010.

[19] P. Jouguet, D. Elkouss, and S. Kunz-Jacques, “High-bit-rate continuous-variable quantum key distribution,” *Phys. Rev. A*, vol. 90, p. 042329, Oct 2014.

[20] 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.

[21] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. John Willey & Sons, 2nd ed., 2006.

[22] R. R. S. Leite and F. M. d. Assis, “Cvqkd reconciliation based on distributional transform and slepian-wolf coding,” in *Anais do XLII Simpósio Brasileiro de Telecomunicações e Processamento de Sinais - SBrT2024*, (Belém, Brasil), Sociedade Brasileira de Telecomunicações, 2024.

[23] P. Czyż, F. Grabowski, J. Vogt, N. Beerenwinkel, and A. Marx, “Beyond normal: On the evaluation of mutual information estimators,” *Advances in Neural Information Processing Systems*, vol. 36, 2024.

[24] R. R. S. Leite and F. M. d. Assis, “Cvqkd reconciliation with bit-flipping decoding ldpc slepian-wolf codes,” in *VII Workshop Escola de Computação, Comunicação e Informação Quântica*, (Rio de Janeiro, Brasil), pp. 91–95, 2024.

[25] M. A. Dias, F. M. de Assis, and J. M. de Assis, “A novel technique for generation of correlated bit sequences with application to gaussian channels,” in *Anais do XLII Simpósio Brasileiro de Telecomunicações e Processamento de Sinais - SBrT2024*, (Belém, Brasil), Sociedade Brasileira de Telecomunicações, 2024.