Soft-Decoding Reverse Reconciliation in Discrete-Modulation CV-QKD

Marco Origlia, Emanuele Parente, and Marco Secondini, *Senior Member, IEEE*

***Abstract*—In continuous-variable quantum key distribution, information reconciliation is required to extract a shared secret key from correlated random variables obtained through the quantum channel. Reverse reconciliation (RR) is generally preferred, since the eavesdropper has less information about Bob's measurements than about Alice's transmitted symbols. When discrete modulation formats are employed, however, soft information is available only at Bob's side, while Alice has access only to hard information (her transmitted sequence). This forces her to rely on hard-decision decoding to recover Bob's key.**

In this work, we introduce a novel RR technique for PAM (and QAM) in which Bob discloses a carefully designed soft metric to help Alice recover Bob's key, while leaking no additional information about the key to an eavesdropper. We assess the performance of the proposed technique in terms of the achievable secret key rate (SKR) and its bounds, showing that the achievable SKR closely approaches the upper bound, with a significant gain over hard-decision RR. Finally, we implement the scheme at the coded level using binary LDPC codes with belief-propagation decoding, assess its bit-error rate through numerical simulations, compare the observed gain with theoretical predictions from the achievable SKR, and discuss the residual gap.

***Index Terms*—Information Theory, Reverse Reconciliation, QKD, PAM, LDPC**

I. Introduction

Information reconciliation is the process by which two parties, holding correlated random sequences, communicate over a public channel to correct discrepancies between their data and obtain two identical sequences. This is particularly useful in all applications where these sequences are employed as symmetrical keys, and the correlated sequences are obtained from data transmission schemes of various natures. Ensuring secrecy is therefore a fundamental requirement in such kinds of applications. A possible scenario of shared randomness generation is quantum key distribution (QKD), in which the correlated sequences are obtained from the transmission of quantum states over a quantum channel [2].

Following the initial phase of random data transmission, reconciliation serves to resolve discrepancies between the correlated sequences. It is typically assumed that the remote parties are provided with an authenticated noiseless public channel for this purpose. Finally, a privacy amplification stage is applied to purge any information potentially leaked during the previous phases.

This work has been partially supported by PNRR MUR project PE0000023-NQSTI, by the QUASAR project and by the SMARTQKD scholarship funded by SMA-RTY Italia SRL and CNR-IEIIT.

This paper is an extended version of our previous work presented at the 14th International ITG Conference on Systems, Communications and Coding (SCC), Karlsruhe, Germany, 2025 [1].

Depending on which party performs error correction, two reconciliation strategies can be distinguished. In direct reconciliation (DR), the sender (Alice) defines the key based on her data and discloses some redundant information, usually a syndrome, associated with it. The receiver (Bob) then uses the shared information, along with his received data, to recover Alice's key. Conversely, in reverse reconciliation (RR), Bob defines the key based on his received data and discloses the redundant information associated with it, while Alice uses this information and her transmitted data to recover Bob's key.

When a potential attacker is taken into account, the direction of the reconciliation matters. In fact, the data potentially leaked during transmission usually have larger mutual information with the transmitted data than with the received data. As a result, RR generally results in lower information leakage compared to DR, overcoming the 3dB limitation of DR—which consists of a disruption of the key exchange protocol due to the eavesdropper being able to perfectly reconstruct the secret key by obtaining more than half of the transmitted power—and enabling higher secret key rates (SKR) and longer distances [2], [3].

For the phase of data transmission, different signaling techniques may be employed. For instance, in the realm of QKD, the existing protocols may adopt single photons (discrete-variable (DV) QKD) [4], or coherent states (continuous-variable (CV) QKD) [5]. Unlike DV-QKD, CV-QKD does not require single photon sources and detectors and can use the same devices and modulation/detection schemes commonly employed in classical coherent optical communications [6].

The choice of the information carrier is not only a matter of implementation, as it also affects the kind of variables with which Alice and Bob are provided at the beginning of the reconciliation procedure. In the GG02 protocol [5], Alice and Bob share correlated Gaussian random variables. The most well-known reconciliation procedures for Gaussian variables are slice reconciliation [7] and multidimensional reconciliation [8], [9], [10].

Despite its theoretical appeal, communication based on Gaussian variables poses several practical challenges, such as the limited range and finite resolution of modulators [11], [12], and the limited reconciliation efficiency [13]. This has motivated the exploration of CV-QKD protocols utilizing discrete constellations [14], [15]. Among these, a particularly promising approach uses probabilistically-amplitude-shaped quadrature amplitude modulation (PAS-QAM), which allows the protocol to closely approach the SKR achievable by GG02 [16], [17], [18]. When the transmitted symbols are drawn from a discrete constellation, DR can be formulated as a

classical error correction problem over an additive white Gaussian noise (AWGN) channel, with slight modifications due to Alice and Bob working within an arbitrary coset of a given code. After Alice publicly reveals the particular coset by disclosing the syndrome of the key (equal to the transmitted sequence in this case), Bob uses this syndrome and the soft information available on his side (the AWGN channel output) to infer the most likely transmitted sequence. For this task, efficient codes and soft-decoding algorithms—such as low-density parity-check (LDPC) codes and belief propagation [19], [20]—are available to closely approach channel capacity. On the other hand, RR—usually preferred over DR, as discussed above—is made more difficult by the lack of soft information on Alice's side. After Bob defines the key based on the received data (e.g., by using thresholds to select the most probable symbols transmitted by Alice) and discloses the corresponding syndrome, Alice has access only to hard information (her transmitted sequence) to recover Bob's decisions through error correction. In this scenario, where the reconciliation protocol exclusively involves discrete random variables, secrecy against general attacks is guaranteed by security proofs based on the entropy accumulation theorem [21], [22]. However, discarding the soft information contained in Bob's continuous measurement outcomes inevitably reduces the mutual information (MI) between Alice and Bob, and it is unclear whether a possible reduction of Eve's Holevo information can systematically compensate for this MI loss. Moreover, [23] argues that channel codes closely approaching the capacity of continuous-output channels at very low SNR can be obtained by applying simple constructions, which are not as effective when applied to discrete-output channels.

For BPSK and QPSK constellations, a soft RR procedure has been proposed by Leverrier [24], in which Bob discloses the amplitude of the received samples. In this case, the amplitude gives no information to a potential eavesdropper (Eve) about Bob's decisions (which depend only on the phase), but enables Alice to perform soft decoding as in the DR scheme (and with the same efficiency). Unfortunately, this procedure cannot be extended to general discrete constellations (e.g., QAM), for which disclosing the received amplitude would reveal also relevant information about the key.

To overcome this issue, in this work:

- We introduce a novel RR procedure with soft information (RRS) that can be applied to PAM (and QAM) signaling;
- We analyze the achievable SKR of the scheme without an eavesdropper acting on the quantum channel, derive its theoretical bounds, and show that the achievable SKR closely approaches the upper limit, yielding a substantial improvement over RR based exclusively on hard information (RRH for short);
- We derive a lower bound for the SKR against collective attacks when an eavesdropper is present on the quantum channel. Our SKR bound corresponds to a modified version of the Devetak–Winter bound [25], where the proposed reconciliation procedure solely improves the MI term between Alice and Bob, leaving the Holevo term between Bob and Eve unchanged;
- We validate the proposed approach through a coded-level implementation using LDPC codes and belief-propagation decoding with 4-PAM and 8-PAM constellations, and assess its performance through numerical simulations, confirming its advantage over RRH;
- We show the advantage of RRS over RRH in terms of SKR in the scenario of collective attacks on a linear quantum channel.

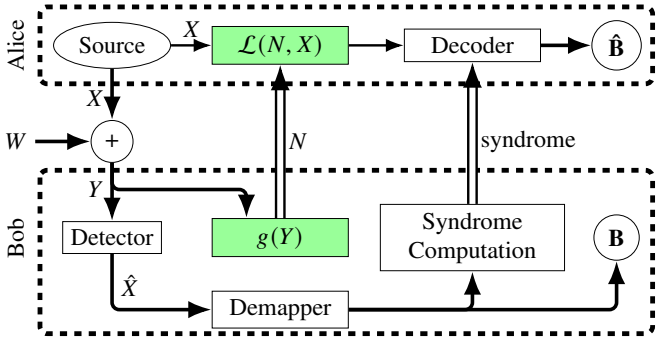


Fig. 1. System overview of the scheme. The highlighted blocks enable the reverse reconciliation with soft information. Bob generates a soft metric N from the symbol Y he received and Alice uses it to generate the log-*a posteriori* probability ratios ($\mathcal{L}(N,X)$) of the corresponding bits for the subsequent syndrome-based error correction.

The proposed reconciliation scheme involves Bob disclosing a soft metric that enables Alice to perform soft decoding, without revealing any additional information to Eve beyond the syndrome normally required for error correction.

The paper is organized as follows. After providing a brief overview of the proposed reconciliation scheme in Section II, we dive deep into the formal aspects of the problem in Section III, presenting a solution in Section III-D. In Section IV, we investigate through numerical simulations the performance of the proposed solution. Finally, we draw some conclusions in Section V.

II. Reconciliation Scheme Overview

Fig. 1 illustrates the working principle of a system employing the proposed RRS procedure, and Table I summarizes its steps. In the initial signaling phase, Alice transmits random symbols X to Bob over an AWGN channel (step 1). Upon receiving Y as the channel output (step 2), Bob makes decisions, denoted as $\hat{X}$ (step 2 (a)).

Next, the core phase of RRS begins. Based on the channel output Y, Bob computes a side-information variable N and transmits it to Alice over a noiseless public side channel (step 2 (b)). This variable is designed to provide Alice, who knows the transmitted symbols X, with soft information about Bob's decision $\hat{X}$. At the same time, N is carefully constructed to reveal no information about $\hat{X}$ to any potential eavesdropper who does not know X, as discussed in Section III-A. The specific transformation $N = g(Y)$ used to compute this side information is detailed in Section III-D.

Alice then uses the side channel information N, along with her knowledge of the transmitted symbol X, to compute the log-*a posteriori* probability ratios (LAPPRs) for the bits corresponding to Bob's decisions (step 3), as detailed in Section III-F.

TABLE I
SUMMARY OF OUR REVERSE RECONCILIATION SCHEME WITH SOFT INFORMATION (RRS).

1	Alice randomly draws a symbol X out of a possibly discrete constellation and sends it over the quantum channel.
2	Bob receives a noisy copy Y of the transmitted symbol, and processes it: (a) He discretizes Y to $\hat{X}$, and he maps $\hat{X}$ to a bit vector according to a labeling rule. (b) He applies a transformation function $g(Y)$ and he discloses the result N over the public channel.
3	Alice computes the LAPPRs $\mathcal{L}(X, N)$ associated to this bit vector, taking N into account.
1–3	Steps 1–3 are repeated a sufficient number of times, so that Bob has collected a binary vector $\mathbf{B}$, and Alice has computed the associated LAPPRs.
4	Bob computes and discloses the syndrome of $\mathbf{B}$.
5	Alice uses the syndrome and the computed LAPPRs for coset decoding, obtaining $\hat{\mathbf{B}}$.

In the subsequent error correction phase, Alice and Bob use a previously agreed-upon error correction code (for simplicity, we assume here a binary code). After collecting a sufficient number of decisions $\hat{\mathbf{X}}$, Bob computes the syndrome of the binary sequence $\mathbf{B}$ corresponding to $\hat{\mathbf{X}}$ and sends it to Alice over the side channel (step 4). Alice feeds the decoder with the syndrome and the LAPPRs to produce an estimate $\hat{\mathbf{B}}$ of the binary sequence $\mathbf{B}$ (step 5).

Finally, privacy amplification (not shown in the scheme) is performed to remove any information potentially leaked through the syndrome and produce the final shared key.

III. THEORY

In this section, we focus our analysis on a PAM signaling system. The analysis can be readily applied to QAM signaling by considering independently the in-phase and quadrature PAM signal components.

Alice, the sender, selects a random sample X from a PAM alphabet $\mathcal{A} = \{a_1, \ldots, a_M\}$ according to the probability mass function (PMF)[1] $\mathrm{P}_X(a_i)$ and sends it over an AWGN channel. This PMF is arbitrary, therefore the following analysis holds when PAS-QAM is employed [16], [17], even though we will use uniform input probabilities in our simulations as a proof of concept. Similarly, the channel noise need not be Gaussian, as long as its distribution is known both to Alice and Bob. The noise sample added by the channel is $W \sim \mathcal{N}\left(0, \frac{N_0}{2}\right)$. The noise variance is supposed to be known by Alice and Bob, for instance after channel estimation. The channel output is $Y = X + W$, with conditional distribution

$$f_{Y|X}(y|a_i) = \frac{1}{\sqrt{\pi N_0}} \exp\left(-\frac{(y-a_i)^2}{N_0}\right) \tag{1}$$

and marginal distribution

$$f_Y(y) = \frac{1}{\sqrt{\pi N_0}} \sum_{a_j \in \mathcal{A}} \mathrm{P}_X(a_j) \exp\left(-\frac{(y-a_j)^2}{N_0}\right). \tag{2}$$

[1]Throughout this work, we will denote the probability density function of a generic random variable A with f_A, and the corresponding cumulative distribution function (CDF) with F_A. For PMFs, we will use $\mathrm{P}_A(a) := \mathrm{P}\{A = a\}$.

Based on Y and a set of intervals $\{D_i \subset \mathbb{R} : \bigcup_{i=1}^{M} D_i = \mathbb{R},\ D_k \bigcap D_j = \emptyset\ \forall k \neq j\}_{i=1}^{M}$ that partition the set of real numbers, Bob makes a decision on $\hat{X}$

$$\hat{x} = \begin{cases} a_1, & y \in D_1 \\ \vdots & \\ a_M, & y \in D_M. \end{cases} \tag{3}$$

The choice of the intervals D_i (or equivalently, the decision thresholds, corresponding to their infimum and supremum points) is arbitrary. For example, they may depend on the noise variance N_0, or they could be fixed. Furthermore, even though in this work we assume that the size of the *output* alphabet matches the size of the *input* alphabet, the analysis of this reconciliation scheme still applies when input and output alphabets have different sizes. When both X and $\hat{X}$ belong to the same alphabet $\mathcal{A}$, the intervals D_i may be chosen, for instance, to maximize the *a posteriori* probabilities of the transmitted symbol X (MAP criterion).

Once a sufficient number of decisions have been collected, Bob demaps the resulting sequence $\hat{\mathbf{X}}$ to a bitstring $\mathbf{B}$, e.g., assuming a Gray mapping. Then he evaluates its syndrome according to a code previously agreed upon, and supposed to be publicly known. The syndrome is sent to Alice, who will use it to perform the error correction processing and get $\hat{\mathbf{B}}$, possibly identical to $\mathbf{B}$.

To assist Alice in decoding $\hat{\mathbf{B}}$, Bob provides her with additional side information derived from Y. Since this information is shared over a public channel, its design must ensure that no information about Bob's decisions $\hat{X}$ is leaked to a potential eavesdropper unaware of X.

To achieve this, Bob applies a deterministic transformation to Y, generating a random variable N that is sent to Alice. Without loss of generality, we define the transformation between Y and N through the piecewise function

$$n = g(y) = \begin{cases} g_1(y), & y \in D_1 \\ \vdots & \\ g_M(y), & y \in D_M. \end{cases} \tag{4}$$

When the eavesdropper has no side information, the achievable SKR is $I(X;Y)$ [26, Prop. 1], [27, Th. 2]. In the DR case, the raw key coincides with the input sequence $\mathbf{X}$ transmitted by Alice, and Bob can exploit the continuous (soft) outputs $\mathbf{Y}$ to recover it. This reduces to the classical problem of reliable communication over a discrete-input AWGN channel, whose capacity can be closely approached with well-established techniques (e.g., Alice discloses the syndrome of $\mathbf{X}$ based on an LDPC code, and Bob uses it with soft information from $\mathbf{Y}$ in a belief-propagation decoder).

In the RR case—the most relevant for QKD—Bob derives the raw key[2] $\hat{\mathbf{X}}$ from $\mathbf{Y}$, while Alice only has hard information (her sequence $\mathbf{X}$) to recover it. Proceeding symmetrically to

[2]In contrast to MDR, where the raw key is locally generated by Bob, in RRS it is derived from a discretization of the channel output. MDR employs the channel output to perform multidimensional rotations on a transformed version of the raw key to produce a soft metric, whereas in RRS the soft metric is directly derived from the channel output, as we will explain shortly.

the DR case, i.e., with Bob sharing only the syndrome of $\hat{\mathbf{X}}$ and Alice using it with $\mathbf{X}$ to recover $\hat{\mathbf{X}}$, the achievable rate is limited to $I(\hat{X};X)$, with significant loss compared to the ultimate rate $I(X;Y)$. If, however, Bob publicly discloses additional side information N, as in the RRS scheme of Fig. 1, the achievable SKR becomes $I(\hat{X};X|N)$ [26, Th. 3]. This can be higher or lower than $I(\hat{X};X)$, depending on whether N reveals more (or less) information to Alice than to Eve. We will refer to $I(\hat{X};X)$ and $I(\hat{X};X|N)$ as the achievable SKRs for the RRH and RRS schemes, respectively. In QKD, further side information may be gathered by Eve by tampering with the quantum channel, and must therefore be included in the computation of the SKR [25].

A. Constraint on Information Leakage

A well-designed transformation g, according to the discussion above, should maximize $I(\hat{X};X|N)$. First note that

$$I(\hat{X};X|N) = I(\hat{X};X,N) - I(\hat{X};N). \tag{5}$$

Whereas the optimal transformation g may be hard to devise, it is reasonable to first minimize the second term $I(\hat{X};N)$, which represents the information about the raw key $\mathbf{B}$ leaked through the disclosed metric N. As the MI is non-negative, we can reasonably impose the constraint

$$I(\hat{X};N) = 0. \tag{6}$$

The mutual information between two random variables is zero if and only if they are independent. Therefore, to satisfy (6) the function pieces g_i in (4) must be selected such that, given the decision $\hat{X} = a_i$, the distribution of the resulting variable N is independent of the decision a_i itself, i.e.,

$$f_{N|\hat{X}}(n|a_i) = f_{N|\hat{X}}(n|a_j) = f_N(n) \quad \forall\, a_i,\, a_j \in \mathcal{A}. \tag{7}$$

Imposing (6) does not guarantee the optimality of the solution. However, as we will see in the results, the remaining degrees of freedom allow us to closely approach the upper bound $I(X;Y)$ as discussed in the following section.

B. Bounds on the SKR $I(\hat{X};X|N)$

It is useful to establish upper and lower bounds for the SKR of RRS.

$$I(\hat{X};X) \le I(\hat{X};X|N) \le I(X;Y). \tag{8}$$

Proof: For the lower bound we first use (6) in (5) to get

$$I(\hat{X};X|N) = I(\hat{X};X,N). \tag{9}$$

From the chain rule and the non-negativity of MI

$$I(\hat{X};X,N) = I(\hat{X};X) + I(\hat{X};N|X) \ge I(\hat{X};X). \tag{10}$$

For the upper bound we have

$$\begin{aligned} I(X;Y) &= I(\hat{X},N;X) && (11)\\ &= I(\hat{X};X|N) + I(N;X) && (12)\\ &\ge I(\hat{X};X|N), && (13) \end{aligned}$$

where

- (11) follows from the fact that Y and the pair $(\hat{X},N)$ are related by a deterministic invertible function;
- (12) is the chain rule for mutual information;
- the inequality in (13) is based on the non-negativity of mutual information.

■

Remark. The proof of the lower bound uses constraint (6). On the other hand, the proof of the upper bound does not, therefore it holds in general.

As expected, sharing N over a public channel cannot increase the SKR beyond the limit imposed by [26, Prop. 1]. At the same time, if N satisfies (6), the SKR achievable by RRS is not lower than the SKR achievable by RRH.

C. SKR with a Quantum Eavesdropper

In this section we analyze how the presence of an attacker, namely Eve, would impact the computation of the SKR under the framework of collective attacks and infinite key length. In this scenario, the maximum achievable SKR K can be lower bounded as

$$K \ge I(\hat{X};X|N) - \chi\left(Y;E\right), \tag{14}$$

where χ is the Holevo bound on the information that Eve can extract [28, p. 622].

Proof: The amount of secret information that can be extracted by Alice and Bob, provided that the disclosed metric N is known both by Alice and by Eve, is [8], [25], [2]

$$K = I(\hat{X};X,N) - \chi\left(\hat{X};E,N\right), \tag{15}$$

where E is a random variable that summarizes the eavesdropper's collected information. Since $\hat{X}$ and N are independent classical random variables, it follows that [8, Lemma 1]

$$\chi\left(\hat{X};E,N\right) \le \chi\left(\hat{X},N;E\right). \tag{16}$$

Since g is invertible in each region D_i, each pair $(\hat{X},N)$ is statistically equivalent to Y. Then,

$$\chi\left(\hat{X},N;E\right) = \chi\left(Y;E\right). \tag{17}$$

Putting (15), (16), and (17) together, we can conclude that

$$\begin{aligned} K &\ge I(\hat{X};X,N) - \chi\left(Y;E\right) && (18)\\ &= I(\hat{X};X|N) - \chi\left(Y;E\right), && (19) \end{aligned}$$

where the last equality follows from (5) and (6). ■

This result implies that the soft metric we introduced impacts the MI between Alice and Bob, thus the reconciliation efficiency, and it does not affect the Holevo bound.

D. Transformation Functions

To construct a solution to (7), we begin by arbitrarily specifying the target output distribution $f_N(n)$ as the uniform distribution over the interval $[0,1]$. To preserve as much information as possible about the channel output Y and ease the analytical calculation of the LAPPRs (Section III-F), we further require each g_i to be continuously differentiable and invertible (therefore monotonic) in its domain D_i.

We are left with an additional degree of freedom for each function g_i, i.e., the direction of monotonicity—increasing or decreasing. We first consider the case in which all functions are monotonically increasing. A generalization to arbitrary monotonicity configurations is provided in Section III-G.

It is straightforward to verify that, conditioned on $Y \in D_i$, the transformation

$$g_i(y) = F_{Y|\hat{X}}(y|a_i) = \frac{F_Y(y) - F_Y(\inf D_i)}{\mathrm{P}_{\hat{X}}(a_i)}, \tag{20}$$

corresponding to the conditional CDF of Y given $\hat{X} = a_i$, produces a uniformly distributed output over the interval $[0, 1]$.[3] Here, $F_Y(y) = \int_{-\infty}^{y} f_Y(z)dz$ is the CDF of the channel output Y, whose distribution $f_Y(y)$ is given in (2); $\mathrm{P}_{\hat{X}}(a_i) = F_Y(\sup D_i) - F_Y(\inf D_i)$ is the probability that $Y \in D_i$, i.e., that Bob makes the decision $\hat{X} = a_i$; and, for conciseness, we define

$$F_Y(\inf D_i) = \lim_{\tilde{y} \to \inf D_i} F_Y(\tilde{y}), \tag{21}$$

and similarly for $F_Y(\sup D_i)$. Consequently, defining the global transformation $g(y)$ in (4) by assigning each g_i as in (20) for $i = 1, \ldots, M$, satisfies the constraint in (7). In other words, the conditioned random variables $N_i := N|\{\hat{X} = a_i\}$ are all statistically equivalent, i. e., $\forall i, j: \; N_i \cong N_j \cong N \sim \mathcal{U}([0, 1])$. Moreover, each function g_i in (20) is invertible and differentiable over its domain D_i, with

$$g_i^{-1}(n) = F_Y^{-1}\left(n \cdot \mathrm{P}_{\hat{X}}(a_i) + F_Y(\inf D_i)\right), \tag{22}$$

$$g_i'(y) = \frac{f_Y(y)}{\mathrm{P}_{\hat{X}}(a_i)}. \tag{23}$$

E. Secret Key Rate

We can assess the performance of RRS by its SKR, or equivalently by the mutual information $I(\hat{X}; X, N)$ (as proved earlier, see (9)):

$$I(\hat{X}; X, N) = H(\hat{X}) - H(\hat{X}|X, N), \tag{24}$$

where $H(\hat{X}|X, N) = H(\hat{X}, N|X) - H(N|X)$ can be written as

$$H(\hat{X}|X, N) := \mathop{\mathbb{E}}_{\hat{X},X,N} \left\{ \log_2 \left(\frac{\sum_{a_k \in \mathcal{A}} f_{N,\hat{X}|X}(N, a_k|X)}{f_{N,\hat{X}|X}(N, \hat{X}|X)} \right) \right\}, \tag{25}$$

which is entirely expressed in terms of $f_{N,\hat{X}|X}$. Since the event $\{N = n, \hat{X} = a_i\}$ corresponds to the event $\{Y = g_i^{-1}(n)\}$, this distribution can be obtained through a change of variable as [29, Th. 2.1.8]

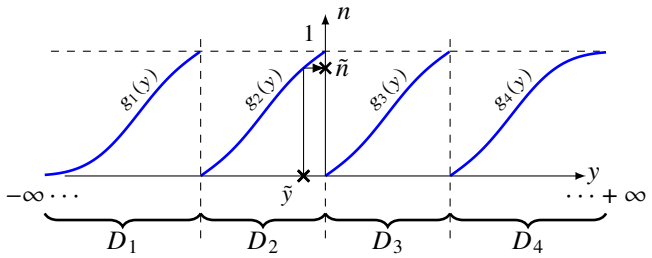
$$f_{N,\hat{X}|X}(n, a_i|a_j) = \frac{f_{Y|X}(g_i^{-1}(n)|a_j)}{|g_i'(g_i^{-1}(n))|}. \tag{26}$$

We remark that, so far, we have at no point assumed a particular distribution of the noise. We just assumed that it is known. In the case of Gaussian noise distribution, the above distribution can be expressed as

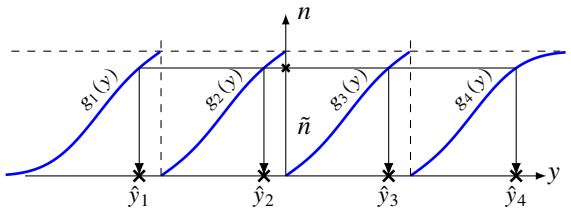
$$f_{N,\hat{X}|X}(n, a_i|a_j) = \frac{\mathrm{P}_{\hat{X}}(a_i)}{\sum_{a_k \in \mathcal{A}} \mathrm{P}_X(a_k) e^{-\frac{(2g_i^{-1}(n) - a_j - a_k)(a_j - a_k)}{N_0}}}, \tag{27}$$

where we replaced the expressions for $g_i'(y)$ from (23), for $f_Y(y)$ from (2), and for $f_{Y|X}$ from (1).

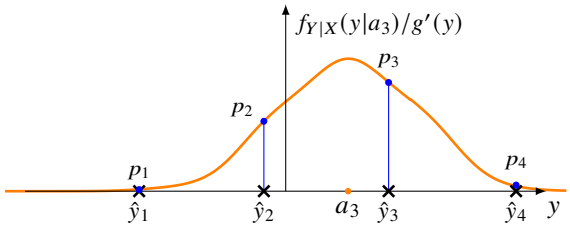
[3] A formal proof follows from the probability integral transform [29, Th. 2.1.10].



(a) Bob receives $y = \tilde{y}$, so he decides on $\hat{x} = a_2$, applies g_2 to compute $\tilde{n} = g_2(\tilde{y})$, and sends it to Alice.



(b) Alice (and Eve) receives $\tilde{n}$ from Bob and applies the inverse transformation function within each region to infer the possible channel outputs $\hat{y}_i = g_i^{-1}(\tilde{n})$ that Bob may have observed.



(c) Since Alice knows what she transmitted, e.g. $x = a_3$, she can compute the *a posteriori* probabilities of $\hat{X}$ given X, by the samples $p_i \propto \mathrm{P}_{\hat{X}|X,N}(a_i|a_3, \tilde{n})$ of (26) (plotted here as a function of y) at $\hat{y}_i$.

Fig. 2. Usage of the transformation function.

F. A Posteriori Probability Ratios

To apply the RRS scheme described above, we finally detail the computation of the LAPPRs that Alice can feed to a syndrome-aware decoder to recover the raw key $\hat{\mathbf{B}}$.

For the sake of clarity, we will follow a concrete example, sketched in Fig. 2. Suppose that Bob receives the channel output $\tilde{y} \in D_2$, as shown in Fig. 2a. Therefore, he assigns $\hat{x} = a_2$ according to (3), and computes $\tilde{n} = g(\tilde{y}) = g_2(\tilde{y})$ based on (4). Finally, he publicly discloses $\tilde{n}$.

Fig. 2b shows that both Alice and Eve can now apply the set of locally inverse functions to $\tilde{n}$, and formulate M (in our example, $M = 4$) different hypotheses $\hat{y}_1, \ldots, \hat{y}_M$ for the channel output that Bob may have received, where $\hat{y}_i = g_i^{-1}(\tilde{n})$.

Note that the true channel output $\tilde{y}$ is included among these hypothetical values.

From Eve's perspective, $\tilde{n}$ alone provides no information about Bob's decision $\hat{x}$. In fact, she could use a soft decoder with a soft input computed from $\mathrm{P}_{Y|N}(\hat{y}_i|\tilde{n}) = \mathrm{P}_{\hat{X}|N}(a_i|\tilde{n})$. However, such input reduces to the *a priori* probability $\mathrm{P}_{\hat{X}}(a_i)$ due to (7) and the uniform distribution of N over $[0,1]$.

On the other hand, Alice knows which symbol x she transmitted. Therefore, unlike Eve, she can combine this knowledge with $\tilde{n}$ to estimate and compare the *a posteriori* probabilities of the M possible decisions made by Bob. In the example of Fig. 2c, $x = a_3$, meaning that, due to channel noise, Alice's transmitted symbol differs from Bob's decision $\hat{x} = a_2$. However, by substituting $x = a_3$ into (26), Alice obtains $f_{Y|X}(y|a_3)/g'(y)$ (the orange curve), and can evaluate it at $y = \hat{y}_i$ to derive the (unnormalized) *a posteriori* probabilities $p_i \propto \mathrm{P}_{\hat{X}|X,N}(a_i|a_3,\tilde{n})$ for $i = 1,\dots,4$. These probabilities indicate that, although her transmitted symbol a_3 remains the most likely, the decision a_2—Bob's actual choice—has a comparable probability, which may help Alice's decoder correct the discrepancy.

In general, the (normalized) *a posteriori* probability required by Alice's decoder can be expressed as

$$\mathrm{P}_{\hat{X}|X,N}(a_i \mid a_j,\ n) = \frac{f_{N,\hat{X}|X}(n,a_i|a_j)}{f_{N|X}(n|a_j)}. \tag{28}$$

For bitwise decoding, the LAPPR associated with the l-th bit B_l of the label assigned to $\hat{X}$ is

$$\begin{aligned}\mathcal{L}_l(n,a_j) &:= \log\left(\frac{\mathrm{P}_{B_l|X,N}(0|a_j,n)}{\mathrm{P}_{B_l|X,N}(1|a_j,n)}\right)\\ &= \log\left(\frac{\sum_{a_i\in\mathcal{A}_0(l)}\mathrm{P}_{\hat{X}|X,N}(a_i \mid a_j,\ n)}{\sum_{a_i\in\mathcal{A}_1(l)}\mathrm{P}_{\hat{X}|X,N}(a_i \mid a_j,\ n)}\right)\\ &= \log\left(\frac{\sum_{a_i\in\mathcal{A}_0(l)} f_{N,\hat{X}|X}(n,a_i|a_j)}{\sum_{a_i\in\mathcal{A}_1(l)} f_{N,\hat{X}|X}(n,a_i|a_j)}\right),\end{aligned} \tag{29}$$

where $\mathcal{A}_0(l), \mathcal{A}_1(l) \subset \mathcal{A}$ partition $\mathcal{A}$ according to the value of the l-th bit (0 or 1, respectively), based on a specific symbol-to-bit labeling rule—Gray labeling, for instance.

The denominator $f_{N|X}(n|a_j)$ in (28) ensures proper normalization of the probabilities. However, this term cancels out in the computation of the LAPPRs, as shown in the last equality of (29). Consequently, Alice can directly use unnormalized probabilities; in the example of Fig. 2c, she computes $\mathcal{L}_l(\tilde{n},a_3)$ by using the samples p_i shown in the figure.

Remark. Compared to RRH, RRS requires the additional computation of the soft metric by Bob and its inverse for the computation of the LAPPRs by Alice. In practice they involve the computation of functions of a single real variable that look like the plot of Fig. 2, which can be implemented with low complexity through lookup tables.

G. Direction of the Monotonicity

If N_i, as defined in Section III-D, is uniformly distributed in $[0,1]$, so is the random variable $\bar{N}_i = 1 - N_i$. The latter can be obtained through the modified transformation

$$\bar{g}_i(y) = \frac{F_Y(\sup D_i) - F_Y(y)}{\mathrm{P}_{\hat{X}}(a_i)} = 1 - g_i(y) \tag{30}$$

corresponding to the complementary conditional CDF of Y given $\hat{X} = a_i$. By construction, $\bar{g}_i$ is also invertible and differentiable in its domain D_i, with

$$\bar{g}_i^{-1}(n) = F_Y^{-1}\left(F_Y(\sup D_i) - n\cdot\mathrm{P}_{\hat{X}}(a_i)\right), \tag{31}$$

$$|\bar{g}_i'(y)| = -\bar{g}_i'(y) = \frac{f_Y(y)}{\mathrm{P}_{\hat{X}}(a_i)}. \tag{32}$$

Since $\bar{N}_i$ has the same uniform distribution as N_i, Alice and Bob can agree on using either of them independently on each interval, i.e., if they agree to use N_i for channel outputs that lie in D_i, they can arbitrarily agree to use either N_j or $\bar{N}_j$ when Y lies is another interval D_j. Either choice complies with constraint (7) and is therefore still a valid solution to our problem, i.e., no information about Bob's decision is obtained from observing N alone.

On the other hand, the set of monotonicity directions chosen in the various intervals does impact the distinguishability of the hypothetical channel outputs from Alice's point of view.

We define a *configuration* $C^{[b]}$ as an M-tuple of monotonicity directions, one for each decision interval. Each of the 2^M possible configurations is identified by a superscript $[b]$, where $b \in 0,1,\dots,2^M-1$. The monotonicity direction in each decision interval D_i is characterized by the binary representation of b, i.e., $C^{[b]} = (b_M,\dots,b_1)$: $b_i = 0$ indicates that the transformation is monotonically increasing ($\nearrow$) in D_i; $b_i = 1$ indicates that it is monotonically decreasing ($\searrow$). For instance, for $M = 4$ (4-PAM), we have $2^4 = 16$ different configurations, e.g., the "base" configuration, whose index has binary representation $C^{[0]} = (0,0,0,0)$, and the "alternating" configuration , whose index has binary representation $C^{[5]} = (0,1,0,1)$. Each configuration $C^{[b]}$ defines a different transformation $G^{[b]}$, which is a piecewise function over the decision intervals (analogously to (4))

$$n = G^{[b]}(y) = \begin{cases} G_1^{[b]}(y), & y \in D_1\\ \vdots & \\ G_M^{[b]}(y), & y \in D_M. \end{cases} \tag{33}$$

where

$$G_i^{[b]}(y) = \begin{cases} g_i(y) & \text{if } b_i = 0\\ 1 - g_i(y) & \text{if } b_i = 1. \end{cases} \tag{34}$$

For instance, the aforementioned "base" and "alternating" configurations, would visually look like

$$G^{[0]} \sim [\nearrow,\nearrow,\nearrow,\nearrow] \tag{35}$$

$$G^{[5]} \sim [\searrow,\nearrow,\searrow,\nearrow]. \tag{36}$$

The analysis of the SKR in Section III-E still applies, where g_i is simply replaced by $G_i^{[b]}$ in (26).

Some monotonicity configurations are *equivalent*, in the sense that they yield identical SKRs when used in the RRS scheme. As shown in appendix A, equivalent configurations also produce the same conditional distribution (26). Therefore

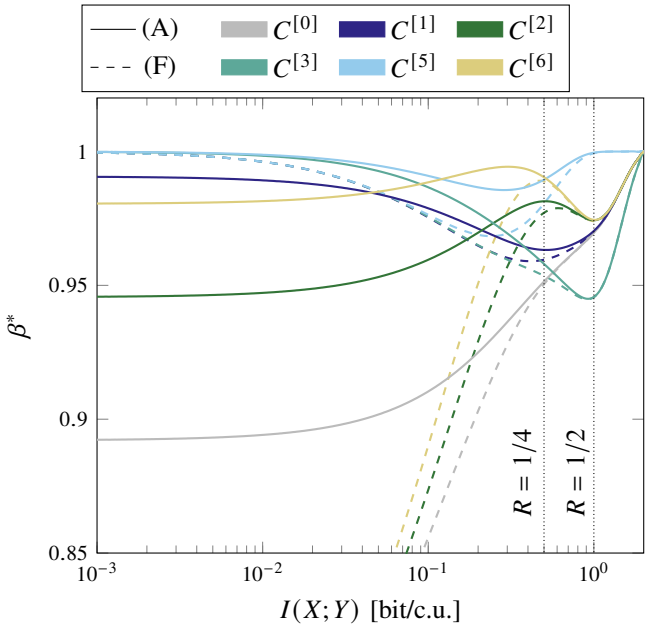


Fig. 3. Achievable reconciliation efficiency β^* of the RRS scheme with 4-PAM, for different configurations $C^{[b]}$ and threshold selection strategies (A/F).

the LAPPR distribution remains unchanged, and the BER performance is identical across all equivalent configurations.

Recognizing equivalent configurations is particularly useful when assessing the performance of RRS, as it allows to restrict numerical computations and simulations to a single representative from each equivalence class. For an exhaustive study of equivalence classes, refer to the Appendix.

IV. Simulations and Results

A. Secret Key Rate

To assess the performance of the proposed RRS scheme, we compare its achievable SKR $I(\hat{X};X|N)$ against the achievable SKR of the RRH scheme $I(\hat{X};X)$ and the SKR upper bound $I(X;Y)$. Results are obtained through a numerical library we developed for this purpose [30].

The M decision intervals in (33) are defined by means of $M-1$ thresholds (the first and last intervals being lower and upper bounded by $-\infty$ and $+\infty$, respectively). In this work, we consider two possible threshold selection strategies:

(F) where thresholds are *fixed* across different SNR values and placed midway between adjacent constellation points. For 4-PAM, with constellation points $\{-3,-1,1,3\}$, the thresholds are at $-2,0,+2$;

(A) where thresholds are *adaptively* selected at each SNR value to produce uniform symbol probabilities after hard decision, thus maximizing the entropy $H(\hat{X})$.[4]

We first consider the case of BPSK modulation ($M=2$), which admits only two non-equivalent configurations, $C^{[0]}$ and $C^{[1]}$ (see Table IV in Appendix B), with the optimal threshold fixed at 0 by symmetry. In this setting, configuration $C^{[1]}$ corresponds to Leverrier's scheme [24], where $|y|$ is remapped from $\mathbb{R}^+$ to $[0,1]$ to serve as n. This scheme was shown to be equivalent to the BI-AWGN channel, and therefore its achievable SKR attains the upper bound $I(X;Y)$. For this reason, the BPSK results are not explicitly plotted.

We then turn to the 4-PAM case. To better illustrate the performance of the proposed scheme, we introduce the *achievable reconciliation efficiency* as the ratio between the achievable SKR and its upper bound[5]

$$\beta^* = \frac{I(\hat{X};X|N)}{I(X;Y)}. \tag{37}$$

The selection of the configuration can be carried out by precomputing the MI for all configuration classes in a broad SNR range, and picking the optimal one for the SNR value of interest. The number of distinct configuration classes is reported in Table VI of Appendix B. Even though it grows rapidly with the modulation order, practical QAM-based CV-QKD systems typically employ up to a 64-QAM format (equivalent to a 8-PAM modulation on each quadrature), and rarely exceed the 256-QAM modulation format, with 16 constellation points per real dimension. For such modulation orders, the aforementioned exhaustive approach is still feasible. Alternatively, one can always select the configuration with alternating monotonicities in adjacent decision intervals ($C^{[5]}$ for 4-PAM, and $C^{[85]}$ for 8-PAM). Even though it is not always optimal, experimental results indicate that it exhibits good achievable reconciliation efficiency also for higher modulation orders. Further investigation is required.

Fig. 3 shows β^* for a representative from each configuration equivalence class of 4-PAM, listed in Table V, and for both fixed and adaptive thresholds. At rate $R=1/2$ (and higher), the difference between the two threshold selection strategies is negligible (for high SNR, the fixed thresholds already yield almost uniform symbol probabilities), and the alternating configuration $C^{[5]}$ attains the highest efficiency (≈ 1). For lower rates, the choice of the threshold selection strategy becomes more important, and the adaptive strategy is always more efficient. At rate $R=1/4$, $C^{[5]}$ with adaptive thresholds still achieves the highest efficiency, on par with $C^{[6]}$ and only slightly below 1. Indeed, $C^{[5]}$ is the best configuration for almost any rate (except for the range 0.1–0.25, where $C^{[6]}$ has a slightly higher efficiency) and is asymptotically optimal for both low and high rates. For this reason, from now on we will only show results for configuration $C^{[5]}$ with adaptive thresholds.

Fig. 4 shows the achievable SKR of the RRS and RRH schemes (both with same adaptive thresholds) compared with the upper bound $I(X;Y)$, as a function of the SNR E_b/N_0. For RRH, the minimum E_b/N_0 is about -0.95dB (- - - -), with a gap of about 0.64dB towards the upper bound (·····). At

[4]Maximizing $H(\hat{X})$ does not guarantee the maximization of the SKR in (24), which depends also on $H(\hat{X}|X,N)$. In principle, a joint optimization of (24) over both the input probabilities $\mathrm{P}_X(a_j)$ and the decision thresholds would be required to maximize the SKR, but this is beyond the scope of this work.

[5]The reconciliation efficiency β is commonly defined in the literature as the ratio between the actual rate achieved with a practical code and its upper bound. Here, instead, we add the superscript "*" and refer to β^* as *achievable* to emphasize that it is an information-theoretic metric, which does not account for the performance of a specific error-correction code.

TABLE II
SIMULATION PARAMETERS

Modulations	4-PAM, 8-PAM
Code rates	1/2, 1/4
Block length	64800
Max LDPC iterations	50

TABLE III
GAP COMPARISON

		Gain [dB]	Residual gap [dB]
BER	(10^{-3}, $R = 1/2$)	1.39	0.04
SKR	(1 b/cu)	1.2	0
BER	(10^{-3}, $R = 1/4$)	0.53	0.36
SKR	(0.5 b/cu)	0.63	0.07

higher rates (shown in Fig. 4b), the gap increases to more than 1dB. Consistently with the efficiency curve shown in Fig. 3, the RRS scheme (——) nearly closes this gap, tightly approaching the upper bound at both low and high rates, and showing just a small gap at intermediate rates.

To illustrate the advantage of RRS over RRH also in the presence of an eavesdropper performing a collective attack, we computed the corresponding secret key rate as a function of the distance, following the approach described in [18]. We assumed a linear quantum channel model [31], [32], [33], and a standard optical fiber with 0.2dB/km loss. The results are reported in Fig. 5 for excess noise values of $\xi = 0.01$ and $\xi = 0.03$ shot noise units. In both cases, RRS (—○—/—●—) yields a higher SKR and reaches a longer range then RRH (- -□- -/- -■- -), tightly approaching the upper bound when employing 4-PAM transmissions with uniform input probabilities (·····△·····/·····▲·····). Further improvements towards the GG02 bound are possible by applying probabilistic shaping of the constellation.

B. Bit Error Rate

A second set of simulations shows the performance of the proposed RRS scheme in terms of bit error rate (BER) for 4-PAM and 8-PAM coded transmission over an AWGN channel. In these simulations, we consider Gray mapping, DVB-S2 LDPC codes with rates 1/2 and 1/4 and a blocklengh of 64800 [34], and implement the RRS scheme with adaptive thresholds and alternating configurations ($C^{[5]}$ for 4-PAM and $C^{[85]}$ for 8-PAM). The LDPC decoder [35] implements the sum-product algorithm [19], [36] and takes into account the syndrome when processing check node inputs to produce the messages for the connected variable nodes. Simulation parameters are summarized in Table II.

The corresponding BER curves are shown in Fig. 6. As benchmarks, we also report the BER obtained with the RRH scheme and with direct reconciliation, where Bob recovers Alice's sequence using the channel output Y and the syndrome, as in a classical communication scheme. We take the latter as a reference because it represents the case where soft information is fully available at the decoder, and the corresponding SKR is equal to the upper bound for the SKR of RRS.

With a rate-1/2 code employed in the 4-PAM scenario (Fig. 6a), RRH has a gap of about 1.4dB from DR. This large gap is almost completely filled by RRS, which lies within 0.04dB from DR. This is consistent with the behavior observed for the SKR curves in Fig. 4b. For reference, in Fig. 6a we also report the result we obtained in our recent work [1], where we a gain of roughly 1dB w.r.t. RRH was observed, further improved by resolving numerical issues.

With a rate-1/4 code (Fig. 6b), the gap between RRH and DR reduces to about 0.9dB, and is only partially filled by RRS, which however still provides a relevant gain of more than 0.5dB over RRH. The gains of the RRS scheme over RRH and its residual gap to DR are summarized in table III. For reference, gaps and gains measured on the SKR curves in Fig. 4b are reported, too. The gains are roughly the same, but the residual gaps appear larger in the BER curves than in the SKR curves, particularly at lower rate. This larger residual gap may be caused by the mismatched bit-wise decoding implemented by the belief propagation decoder, and could potentially be reduced through symbol-wise decoding, non-binary codes, or optimized bit-labeling strategies. This aspect is currently under investigation and will be addressed in future work.

Regarding the 8-PAM modulation, at rate $R = 1/2$ (Fig. 6c) the BER of our scheme lays within 0.1dB from the BER of the DR scheme. When a rate-1/4 code is employed (Fig. 6d), the improvement is less strong, but the RRS still has a positive impact. In fact, despite the fact that the gap to the BER of the direct reconciliation amounts to about 0.35dB, a gain of at least 0.1dB with respect to RRH is still present.

V. CONCLUSIONS

In this work we introduced a novel technique that improves the efficiency of RR for CV-QKD protocols that use PAM or QAM alphabets. In this approach, denoted as RRS, Bob computes and discloses a carefully designed soft metric that assists Alice in reconciling her transmitted symbols with Bob's decisions (the key), while not revealing any information about such decisions to a potential eavesdropper. We formalized the concept of *configurations* underlying the construction of the soft metric and analyzed how the choice of the configurations, along with the thresholds used to derive the key from Bob's measurements, affect the achievable SKR.

We demonstrated that the RRS scheme exhibits a significant gain over RR without the soft metric (the RRH scheme) in terms of the achievable SKR, both when no eavesdropper is present on the quantum channel, and when it performs collective attacks in the asymptotic regime on a linear quantum channel.

Furthermore, we implemented and tested a complete version of the proposed RRS scheme, employing binary LDPC codes and bit-wise belief-propagation decoding. Although the BER results generally follow the SKR trends, the observed gains and gaps do not totally reflect those in the SKR. The reason for this discrepancy is currently under investigation, but a likely explanation is the use of bit-wise decoding, whose performance is better predicted by the normalized generalized mutual information (GMI) [37].

In future work, we will compute the GMI of RRS to better understand the impact of symbol-to-bit mapping and

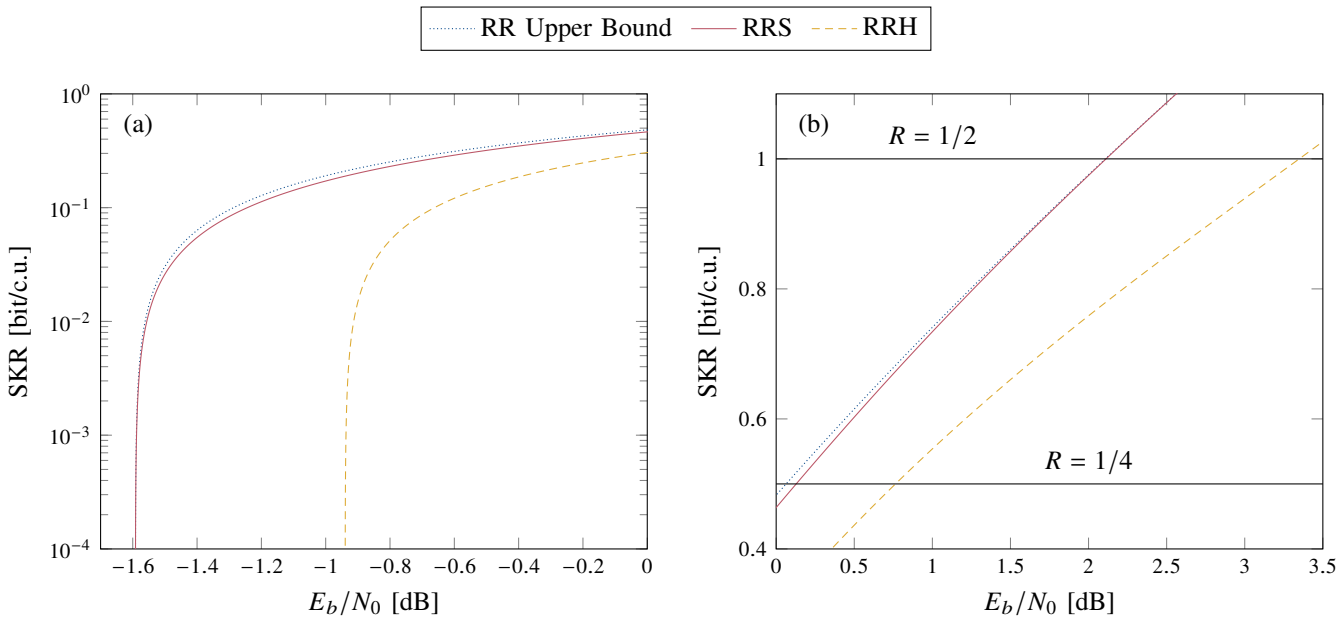


Fig. 4. Achievable SKR for 4-PAM with different reconciliation schemes and adaptive thresholds: (a) low-rate region in log scale; (b) region of interest for our BER simulations employing codes with rates 1/2 and 1/4.

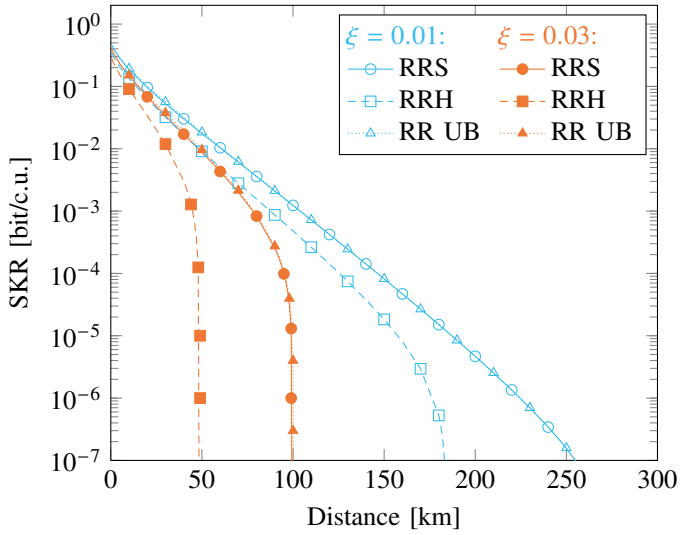


Fig. 5. Secret key rate against collective attacks, computed with different excess noise values, namely $\xi = 0.01$ (blue lines with empty markers) and $\xi = 0.03$ (orange lines with filled markers). We assumed a linear quantum channel model..

bit-wise decoding on performance, and possibly to close the gap between hard and soft decoding also in terms of BER. We will also explore probabilistic constellation shaping and threshold optimization, and focus on the low-rate regime of particular interest for QKD.

Acknowledgement

The authors sincerely thank Erdem Eray Cil (Karlsruhe Institute of Technology) for useful discussions about security proofs.

Appendix

A. Equivalent Configurations and Transformation Functions

In the following we will refer to the soft metric produced by the scheme employing a configuration $C^{[b]}$ with $N^{[b]}$.

1) Flipped functions: A pair $C^{[b]}$ and $C^{[b^{(F)}]}$ of flipped configurations has opposite monotonicity directions in each decision interval, i.e.,

$$\forall i \in \{1, \dots, M\} : b_i^{(F)} = \bar{b}_i \Rightarrow G_i^{[b^{(F)}]} = 1 - G_i^{[b]}. \quad (38)$$

For instance, in the 4-PAM scenario, configurations $C^{[2]}$ and $C^{[13]}$ are equivalent by flipping, and the corresponding transformation functions would look like this:

$$G^{[4]} \sim [\nearrow, \nearrow, \searrow, \nearrow] \quad (39)$$
$$G^{[11]} \sim [\searrow, \searrow, \nearrow, \searrow] \quad (40)$$

Proof: (Equivalence of flipped functions) From (38) it follows that $G_i^{[b^{(F)}]^{-1}}(n^{[b^{(F)}]}) = G_i^{[b]^{-1}}(n^{[b]})$ and for any $y \in D_i$: $|G_i^{[b^{(F)}]'}(y)| = |G_i^{[b]'}(y)|$. This implies that for the flipped configuration it holds that:

$$f_{N^{[b^{(F)}]},\hat{X}|X}(n^{[b^{(F)}]}, a_i|a_j) = \frac{f_{Y|X}(G_i^{[b^{(F)}]^{-1}}(n^{[b^{(F)}]})|a_j)}{|G_i^{[b^{(F)}]'}(G_i^{[b^{(F)}]^{-1}}(n^{[b^{(F)}]})|} = \frac{f_{Y|X}(G_i^{[b]^{-1}}(n^{[b]})|a_j)}{|G_i^{[b]'}(G_i^{[b]^{-1}}(n^{[b]})|} = f_{N^{[b]},\hat{X}|X}(n^{[b]}, a_i|a_j), \quad (41)$$

and the distributions above being equal, $H(\hat{X}|X, N)$ does not change when we replace $N^{[b^{(F)}]}$ by $N^{[b]}$ in (25). Moreover, $H(\hat{X})$ in (24) does not depend on the configuration. So the

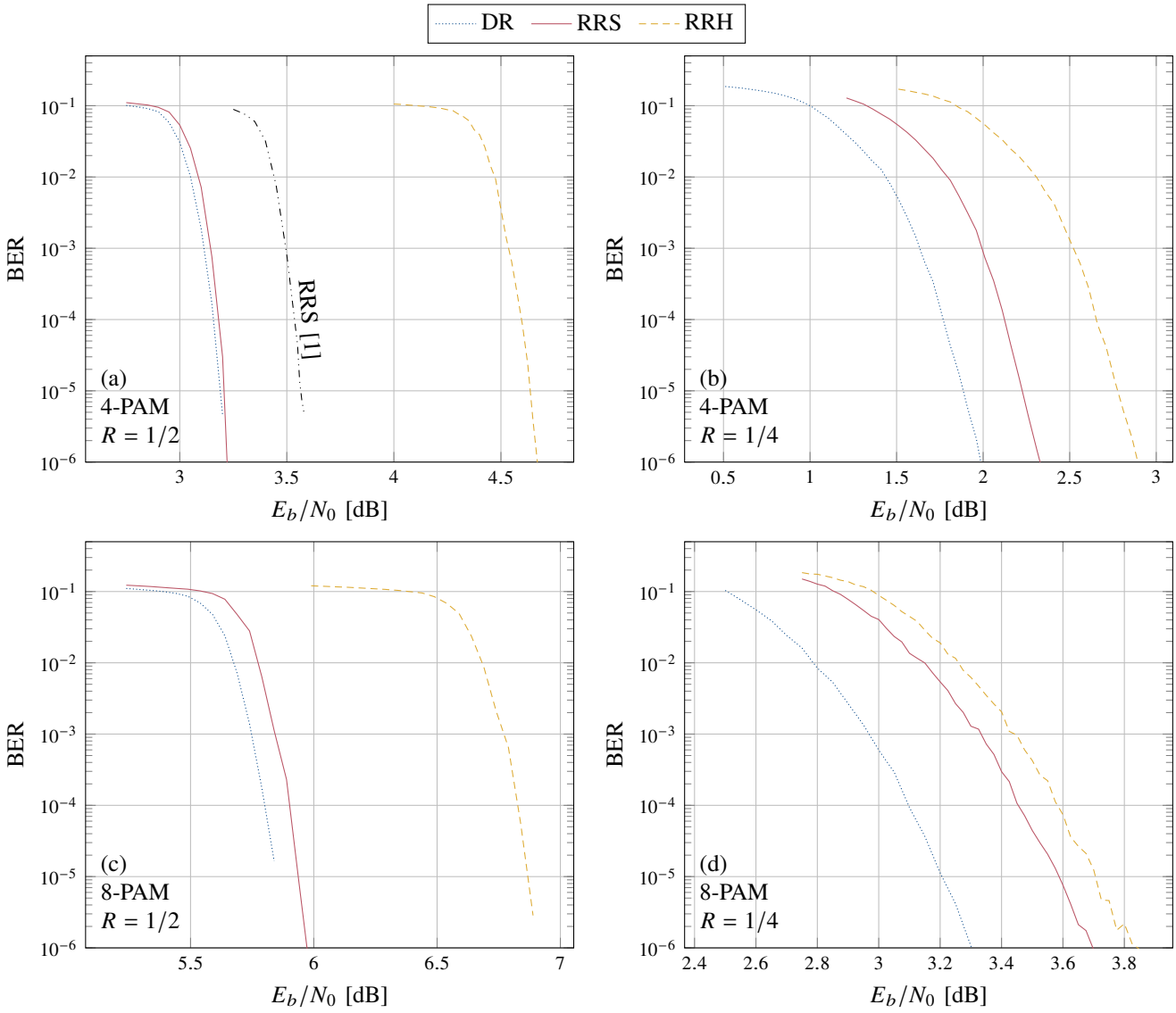


Fig. 6. BER plots for 4-PAM and 8-PAM at $R = 1/2$ and $R = 1/4$. For reference, in each sub-plot we report the BER curve of the DR, as the corresponding SKR (Fig. 4 for 4-PAM) is an upper bound for the SKR in the RRS setting.

mutual information of RRS that employs either of them does not change, i.e.,

$$I(\hat{X}; X|N^{[b^{(F)}]}) = I(\hat{X}; X|N^{[b]}). \tag{42}$$

■

2) Mirrored functions: A mirrored function is obtained by mirroring a transformation function, i.e.,

$$G_i^{[b^{(M)}]}(y) = G_{M+1-i}^{[b]}(-y). \tag{43}$$

For instance, in the 4-PAM scenario, configurations $C^{[4]}$ and $C^{[13]}$ are equivalent by mirroring, as the corresponding transformation functions would look like this:

$$G^{[4]} \sim [\nearrow, \nearrow, \searrow, \nearrow] \tag{44}$$
$$G^{[13]} \sim [\searrow, \nearrow, \searrow, \searrow] \tag{45}$$

In the following we will assume that the input distribution and the decision regions D_i are symmetric, i.e.,

$$\forall a_i \in \mathcal{A}: \ \mathrm{P}\{X = a_i\} = \mathrm{P}\{X = -a_i = a_{M+1-i}\} \tag{46}$$
$$\inf D_i = \sup D_{M+1-i}, \quad \sup D_i = \inf D_{M+1-i}, \tag{47}$$

so $y \in D_i \iff -y \in D_{M+1-i}$.

Proof: (Equivalence of mirrored functions) The first step is to prove that

$$f_{N^{[b^{(M)}]},\hat{X}|X}(n, a_i|a_j) = f_{N^{[b]},\hat{X}|X}(n, a_{M+1-i}|a_{M+1-j}). \tag{48}$$

We can immediately establish the following relationships from definition (43)

$$G_i^{[b^{(M)}]^{-1}}(n) = -G_{M+1-i}^{[b]^{-1}}(n), \tag{49}$$
$$G_i^{[b^{(M)}]'}(y) = -G_{M+1-i}^{[b]'}(-y). \tag{50}$$

By applying (50) to (49), we obtain

$$|G_i^{[b^{(M)}]'}(G_i^{[b^{(M)}]^{-1}}(n))| = |G_{M+1-i}^{[b]'}(G_{M+1-i}^{[b]^{-1}}(n))| \tag{51}$$

By using the symmetry of the PAM constellation, i.e., $-a_j = a_{M+1-j}$, and (49) again, we obtain

$$\left(G_i^{[b^{(M)}]^{-1}}(n) - a_j\right)^2 = \left(G_{M+1-i}^{[b]^{-1}}(n) - a_{M+1-j}\right)^2 \tag{52}$$

$$\Rightarrow f_{Y|X}(G_i^{[b^{(M)}]^{-1}}(n)|a_j) = f_{Y|X}(G_{M+1-i}^{[b]^{-1}}(n)|a_{M+1-j}). \tag{53}$$

Dividing (53) by (51) term by term, as in (26), we prove (48). For the second part of the proof, we write the second term of (24) as

$$H(\hat{X}|X, N^{[b^{(M)}]}) = \int_0^1 \sum_{i=1}^{M/2}\sum_{j=1}^{M/2}\left(\mathcal{F}_{i,j}^{[b^{(M)}]}(n) + \mathcal{F}_{i,M+1-j}^{[b^{(M)}]}(n) + \right.$$
$$\left. + \mathcal{F}_{M+1-i,j}^{[b^{(M)}]}(n) + \mathcal{F}_{M+1-i,M+1-j}^{[b^{(M)}]}(n)\right)\mathrm{d}n \tag{54}$$

where

$$\mathcal{F}_{i,j}(n) = \mathrm{P}_X(a_j) f_{N,\hat{X}|X}(n, a_i|a_j) \cdot \log_2\left(\frac{\sum_{a_k\in\mathcal{A}} f_{N,\hat{X}|X}(n, a_k|a_j)}{f_{N,\hat{X}|X}(n, a_i|a_j)}\right). \tag{55}$$

Because of (48) and the symmetries discussed above, we have that

$$\mathcal{F}_{i,j}^{[b^{(M)}]}(n) = \mathcal{F}_{M+1-i,M+1-j}^{[b]}(n), \tag{56}$$

and we simply obtain a re-arrangement of the sum inside the integral in (54). So, we can conclude that $H(\hat{X}|X, N^{[b^{(M)}]}) = H(\hat{X}|X, N^{[b]})$, therefore

$$I(\hat{X}; X|N^{[b^{(M)}]}) = I(\hat{X}; X|N^{[b]}) \tag{57}$$

■

We can immediately establish the equivalence of (43) to the following equation

$$b_i^{(M)} = \bar{b}_{M+1-i} \tag{58}$$

as it will be useful for proving the last configuration equivalence.

Remark 1. In Section III we claimed that the analysis of the scheme holds for any input PMF $\mathrm{P}_X(a_i)$, however in this proof we assumed that opposite constellation points have the same probability. This is not a very restrictive assumption, because constellation points probabilities are usually shaped to be symmetric.

Remark 2. We proved (48) for the Gaussian noise distribution, however the proof holds for any other additive noise process whose distribution satisfies (48). If this condition is not satisfied, one should simply consider $C^{[b]}$ and $C^{[b^{(M)}]}$ as configurations with distinct performance.

3) Reversed configurations: In this configuration we just reverse the order of the monotonicities, i.e.,

$$b_i^{(R)} = b_{M+1-i} \tag{59}$$

TABLE IV
EQUIVALENT CONFIGURATIONS FOR BPSK

$C^{[b]}$	$C^{[b^{(F)}]}$	$C^{[b^{(M)}]}$	$C^{[b^{(R)}]}$
$C^{[0]}$	$C^{[3]}$	$C^{[3]}$	$C^{[0]}$
$C^{[1]}$	$C^{[2]}$	$C^{[1]}$	$C^{[2]}$

TABLE V
EQUIVALENT CONFIGURATIONS FOR 4-PAM

$C^{[b]}$	$C^{[b^{(F)}]}$	$C^{[b^{(M)}]}$	$C^{[b^{(R)}]}$
$C^{[0]}$	$C^{[15]}$	$C^{[15]}$	$C^{[0]}$
$C^{[1]}$	$C^{[14]}$	$C^{[7]}$	$C^{[8]}$
$C^{[2]}$	$C^{[13]}$	$C^{[11]}$	$C^{[4]}$
$C^{[3]}$	$C^{[12]}$	$C^{[3]}$	$C^{[12]}$
$C^{[5]}$	$C^{[10]}$	$C^{[5]}$	$C^{[10]}$
$C^{[6]}$	$C^{[9]}$	$C^{[9]}$	$C^{[6]}$

Transformations functions with equivalent monotonicities would look like:

$$G^{[4]} \sim [\nearrow, \nearrow, \searrow, \nearrow] \tag{60}$$

$$G^{[2]} \sim [\nearrow, \searrow, \nearrow, \nearrow] \tag{61}$$

Proof: (Equivalence of reversed configurations)

$$b_i^{(R)} = b_{M+1-i} = \tag{62}$$
$$= \bar{\bar{b}}_{M+1-i} = \tag{63}$$
$$= \bar{b}_i^{(M)} = \tag{64}$$
$$= (b^{(M)})_i^{(F)} \tag{65}$$

So, to obtain the reversed configuration corresponding to $C^{[b]}$, instead of reversing the order of the direction of the monotonicities, we can equivalently mirror $C^{[b]}$, and then flip the result. We can now apply the identities we found for the corresponding mutual informations.

$$I(\hat{X}; X|N^{[b^{(R)}]}) := I(\hat{X}; X|N^{[(b^{(M)})^{(F)}]}) \tag{66}$$
$$= I(\hat{X}; X|N^{[(b^{(M)})]}) \tag{67}$$
$$= I(\hat{X}; X|N^{[b]}), \tag{68}$$

where in (67) we used (42) with configurations $C^{[(b^{(M)})^{(F)}]}$ and $C^{[(b^{(M)})]}$, and in (68) we used (57) with configurations $C^{[(b^{(M)})]}$ and $C^{[b]}$. ■

Remark 3. The proof of equivalence of reversed configurations is based on the equivalence of mirrored configurations. Consequently, the claims of *Remark* 2 apply also to reversed configurations.

B. List of Equivalent Configurations

In Tables IV and V we list the equivalent configurations for BPSK and 4-PAM, respectively, the first element of each row being the "reference" configuration.

Configurations $C^{[2]}$ and $C^{[3]}$ for BPSK, and $C^{[4]}$ and $C^{[7]}, \ldots, C^{[15]}$ for 4-PAM are not listed as reference configurations, because they are equivalent to some other one already listed. In fact, it is possible to use the fact that flipping, mirroring and order reversal are self-inverse operations.

TABLE VI
NUMBER OF CONFIGURATION CLASSES VS. PAM MODULATION ORDER.

PAM Order	Number of classes
2-PAM (BPSK)	2
4-PAM	6
8-PAM	72
16-PAM	16512

Proof: (Self-inverse property)

$$\left(b_i^{(F)}\right)^{(F)} = \bar{b}_i^{(F)} = \bar{\bar{b}}_i = b_i \tag{69}$$

$$\left(b_i^{(M)}\right)^{(M)} = \bar{b}_{M-i+1}^{(M)} = \bar{\bar{b}}_{M-(M-i+1)+1} = b_i \tag{70}$$

$$\left(b_i^{(R)}\right)^{(R)} = b_{M-i+1}^{(R)} = b_{M-(M-i+1)+1} = b_i \tag{71}$$

■

In Table VI we report the number of distinct equivalent classes for typical modulation orders.

REFERENCES

[1] M. Origlia and M. Secondini, "Soft reverse reconciliation for discrete modulations," in *2025 14th International ITG Conference on Systems, Communications and Coding (SCC)*, 2025, pp. 1–6.

[2] S. Pirandola *et al.*, "Advances in quantum cryptography," *Adv. Opt. Photon.*, vol. 12, no. 4, pp. 1012–1236, Dec 2020.

[3] F. Grosshans and P. Grangier, "Reverse reconciliation protocols for quantum cryptography with continuous variables," Apr. 2002.

[4] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, pp. 7–11, Dec. 2014.

[5] F. Grosshans and P. Grangier, "Continuous Variable Quantum Cryptography Using Coherent States," *Phys. Rev. Lett.*, vol. 88, no. 5, Jan. 2002.

[6] J. Lodewyck *et al.*, "Controlling excess noise in fiber-optics continuous-variable quantum key distribution," *Physical Review A*, vol. 72, no. 5, art. 050303, 2005.

[7] G. Van Assche, J. Cardinal, and N. Cerf, "Reconciliation of a quantum-distributed gaussian key," *IEEE Transactions on Information Theory*, vol. 50, no. 2, pp. 394–400, 2004.

[8] A. Leverrier *et al.*, "Multidimensional reconciliation for a continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 77, no. 4, Apr. 2008.

[9] X. Liu *et al.*, "OTFS-Based CV-QKD Systems for Doubly Selective THz Channels," *IEEE Transactions on Communications*, vol. 73, no. 8, pp. 6274–6289, Aug. 2025.

[10] Y. Feng *et al.*, "Virtual channel of multidimensional reconciliation in a continuous-variable quantum key distribution," *Physical Review A*, vol. 103, no. 3, p. 032603, Mar. 2021.

[11] P. Jouguet *et al.*, "Analysis of imperfections in practical continuous-variable quantum key distribution," *Physical Review A—Atomic, Molecular, and Optical Physics*, vol. 86, no. 3, art. 032309, 2012.

[12] I. B. Djordjevic, "On the Discretized Gaussian Modulation (DGM)-Based Continuous Variable-QKD," *IEEE Access*, vol. 7, 2019.

[13] A. Leverrier and P. Grangier, "Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation," *Physical Review Letters*, vol. 102, 2009.

[14] ——, "Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation," *Physical review letters*, vol. 102, no. 18, art. 180504, 2009.

[15] T. Hirano *et al.*, "Implementation of continuous-variable quantum key distribution with discrete modulation," *Quantum Science and Technology*, vol. 2, no. 2, art. 024010, 2017.

[16] M. N. Notarnicola *et al.*, "Probabilistic amplitude shaping for continuous-variable quantum key distribution with discrete modulation over a wiretap channel," *IEEE Transactions on Communications*, vol. 72, no. 1, pp. 375–386, 2023.

[17] F. Roumestan *et al.*, "Shaped constellation continuous variable quantum key distribution: Concepts, methods and experimental validation," *Journal of Lightwave Technology*, vol. 42, no. 15, pp. 5182–5189, 2024.

[18] E. Parente *et al.*, "Discrete-modulation continuous-variable quantum key distribution with probabilistic amplitude shaping over a linear quantum channel," Mar. 2026. [Online]. Available: http://arxiv.org/abs/2603.02870

[19] W. Ryan and S. Lin, *Channel codes: classical and modern*. Cambridge university press, 2009.

[20] J. Lodewyck *et al.*, "Quantum key distribution over 25 km with an all-fiber continuous-variable system," *Phys. Rev. A*, vol. 76, no. 4, p. 042305, Oct. 2007.

[21] S. Bäuml *et al.*, "Security of discrete-modulated continuous-variable quantum key distribution," *Quantum*, vol. 8, Jul. 2024.

[22] F. Kanitschar *et al.*, "Finite-Size Security for Discrete-Modulated Continuous-Variable Quantum Key Distribution Protocols," *PRX Quantum*, vol. 4, no. 4, Oct. 2023.

[23] A. Leverrier, "Information reconciliation for discretely-modulated continuous-variable quantum key distribution," Oct. 2023, arXiv:2310.17548 [quant-ph].

[24] ——, "Theoretical study of continuous-variable quantum key distribution," Ph.D. dissertation, Télécom ParisTech, 2009.

[25] I. Devetak and A. Winter, "Distillation of secret key and entanglement from quantum states," *Proceedings of the Royal Society A: Mathematical, Physical and engineering sciences*, vol. 461, no. 2053, pp. 207–235, 2005.

[26] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE Trans. Inform. Theory*, vol. 39, no. 4, Jul. 1993.

[27] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inform. Theory*, vol. 39, no. 3, May 1993.

[28] G. Cariolaro, *Quantum communications*, ser. Signals and communication technology. Cham Heidelberg New York Dordrecht London: Springer, 2015.

[29] G. Casella and R. L. Berger, *Statistical inference*, 2nd ed. Pacific Grove, Calif: Duxbury, 2002.

[30] M. Origlia, "Re2often: (Re)verse (Re)conciliation Softening in Fortran," Apr. 2025. [Online]. Available: https://doi.org/10.5281/zenodo.15222665

[31] Y. Zhang *et al.*, "Continuous-variable quantum key distribution system: Past, present, and future," *Applied Physics Reviews*, vol. 11, no. 1, p. 011318, Mar. 2024.

[32] M. N. Notarnicola, "Quantum communications in continuous variable systems," *International Journal of Quantum Information*, vol. 23, no. 03, p. 2550003, Apr. 2025.

[33] E. Parente, "Probabilistic amplitude shaping for continuous-variable quantum key distribution," Ph.D. dissertation, Dec. 2025. [Online]. Available: https://dta.santannapisa.it/theses/available/etd-11272024-120738/

[34] European Telecommunications Standards Institute (ETSI), *Digital Video Broadcasting (DVB); Second generation framing structure, channel coding and modulation systems for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications; Part 1: DVB-S2*, ETSI Std. EN 302 307-1 V1.4.1, November 2014.

[35] M. Origlia, "Fortran LDPC decoder," Apr. 2025. [Online]. Available: https://doi.org/10.5281/zenodo.15221950

[36] D. J. MacKay, *Information theory, inference and learning algorithms*. Cambridge university press, 2003.

[37] A. Alvarado *et al.*, "Replacing the Soft-Decision FEC Limit Paradigm in the Design of Optical Communication Systems," *Journal of Lightwave Technology*, vol. 33, no. 20, pp. 4338–4352, Oct. 2015.