|VI WECIQ>
VI Workshop
Escola de
Computação e
Informação
Quântica

Unifal MG
Universidade Federal de Alfenas

# Distributional Transform Based Information Reconciliation

**Micael Andrade Dias[1], Andresso da Silva[2], Francisco M. de Assis[3]**

Federal University of Campina Grande, PB, Brazil

micael.souza@ee.ufcg.edu.br[1], fmarcos@dee.ufcg.edu.br[2], andresso.silva@ee.ufcg.edu.br[3]

## Abstract

We present an information reconciliation protocol designed for continuous variable QKD using the Distributional Transform. By combining tools from copula and information theories, we present a method for extracting independent symmetric Bernoulli bits for Gaussian-modulated CVQKD protocols, which we called the Distributional Transform Expansion (DTE).

**Keywords:** continuous variable QKD; distributional transform; reconciliation protocol.

## Introduction

In a Gaussian modulated CVQKD protocol, Alice prepares a coherent state $|\alpha_i\rangle$, where $\alpha_i = q_i + jp_i$ comes from realizations of i.i.d. random variables $Q \sim P \sim \mathcal{N}(0, \tilde{V}_m)$. She sends it to Bob through a quantum channel and, at reception, Bob will perform homodyne[1] detection, randomly switching between quadratures. After $N$ rounds and excluding a subset of size $m$ used during parameter estimation, Alice and Bob keep the matching values, owning the sequences $X_n = x_1, \cdots, x_n$ and $Y_N = x_1, \cdots, y_n$, respectively, with $n = N - m$. The task is to extract random binary sequences from the real valued vectors $X_n$ and $Y_n$ to be further reconciliated (error correction).

## Objectives

Our main objective is to propose an information reconciliation protocol to solve the problem presented in the previous section.

## Reconciliation Protocol

Our proposed solution begins with the following theorem [1, Theorem 1.2.6].

**Theorem 1.** *Let X be a random variable with distribution function $F_X$ and $F_X^{(-1)}$ its quasi-inverse. Then,*

1. *If $F_X$ is continuous, then $U = F_X(X)$ is uniformly distributed on $[0, 1]$.*
2. *If $U$ is a uniformly distributed random variable on $[0, 1]$, then $Y = F_X^{(-1)}(U)$ has distribution function according to $F_X$.*

The transformation mentioned in the first part of Theorem 1 is known as the Distributional Transform and ensures that transforming a random variable by its continuous distribution function always leads to a uniform distribution on the unit interval. A number $d \in [0, 1]$ can be expanded in the binary basis with $l$ bit precision according to

$$d \mapsto 0.b_1 b_2 \cdots b_l, \qquad \sum_{i=1}^{l-1} b_i \frac{1}{2^i} \leq d \leq \sum_{i=1}^{l-1} b_i \frac{1}{2^i} + \frac{1}{2^l}, \tag{1}$$

and we call $\boldsymbol{b} = b_1 b_2 \cdots b_l$ the corresponding bit sequence.

**Definition 1.** *Let $X$ be a random variable with continuous l distribution function $F_X$ and $\mathcal{Q} : [0, 1] \mapsto \{0, 1\}^l$ a function giving a binary expansion as in Equation (1). The Distributional Transform Expansion (DTE) is defined as*

$$\mathcal{D}(X) = \mathcal{Q}\left(F_X(X)\right). \tag{2}$$

*Once the bits in binary the expansion are independent [2, Lemma 13.3.1], it is possible to factor $\mathcal{D}(X) = \mathcal{D}_1(X) \cdots \mathcal{D}_l(X)$, where $\mathcal{D}_i(X) = \mathcal{Q}_i\left(F_X(X)\right)$ is the function $\mathcal{Q} : [0, 1] \mapsto \{0, 1\}$ computing the $i$-th bit in Equation (1) and $\mathcal{D}_i \sim Bern(\frac{1}{2})$. We call $l - \mathcal{D}(X)$ the DTE expansion of $F$ with length $l$.*

Alice and Bob can use the DTE to produce binary sequences from their continuous-valued data:

1. Alice and Bob has the sequences of Gaussian variables $X = X_1, \ldots, X_n$ and $Y = Y_1, \ldots, Y_n$ after quantum communication and parameter estimation;
2. Alice (Bob in RR) compute $\mathcal{D}(X) = (\mathcal{D}_1(X) \cdots \mathcal{D}_l(X))^T$ (and $\mathcal{D}(Y) = (\mathcal{D}_1(Y) \cdots \mathcal{D}_l(Y))^T$ in RR). The resulting bit sequence can be expressed as the matrices,

$$X \mapsto \begin{pmatrix} \mathcal{D}_1(X_1) & \cdots & \mathcal{D}_1(X_n) \\ \mathcal{D}_2(X_1) & \cdots & \mathcal{D}_2(X_n) \\ \vdots & \cdots & \vdots \\ \mathcal{D}_l(X_1) & \cdots & \mathcal{D}_l(X_n) \end{pmatrix}, \tag{3} \qquad Y \mapsto \begin{pmatrix} \mathcal{D}_1(Y_1) & \cdots & \mathcal{D}_1(Y_n) \\ \mathcal{D}_2(Y_1) & \cdots & \mathcal{D}_2(Y_n) \\ \vdots & \cdots & \vdots \\ \mathcal{D}_l(Y_1) & \cdots & \mathcal{D}_l(Y_n) \end{pmatrix}. \quad (4)$$

3. Each one of the $l$ pairs of sequences $(D_i(X), Y)$ (and $(D_i(Y), X)$ in RR] induce a Binary-Input AWGN channel and Bob (Alice in RR) can retrieve Alice's (Bob's in RR) binary sequences by using an error correcting code.

**Example 1.** *Let $X \sim \mathcal{N}(0, 1)$, $Z \sim \mathcal{N}(0, 0.5)$ with $X \perp Z$ and $Y = X + Z$. Assume the realizations $x = \{0.491, 0.327, -0.652, -1.096, -0.023\}$ and $z = \{-0.722, 0.942, 0.191, 0.198, -0.370\}$. Then,*

$$F_X(x) = (0.688, 0.628, 0.257, 0.136, 0.491) \qquad F_Y(y) = (0.425, 0.850, 0.353, 0.231, 0.374)$$

$$\mapsto \begin{pmatrix} 1\,1\,0\,0\,0 \\ 0\,0\,1\,0\,1 \\ 1\,1\,0\,1\,1 \end{pmatrix} \qquad\qquad \mapsto \begin{pmatrix} 0\,1\,0\,0\,0 \\ 1\,1\,1\,0\,1 \\ 1\,0\,0\,1\,0 \end{pmatrix}$$

## Experimental Results

With the procedure described above, one has a method to extract $l$ independent bits from each raw key elements. The maximal reconciliation efficiency, $\beta^{\leftarrow}_{max} = \sum_{i=1}^{l} I(\mathcal{D}_i(Y); X)/I(X; Y)$ for reverse reconciliation ($X$ and $Y$ are swapped in direct reconciliation), were estimated and plotted in Figure 1.

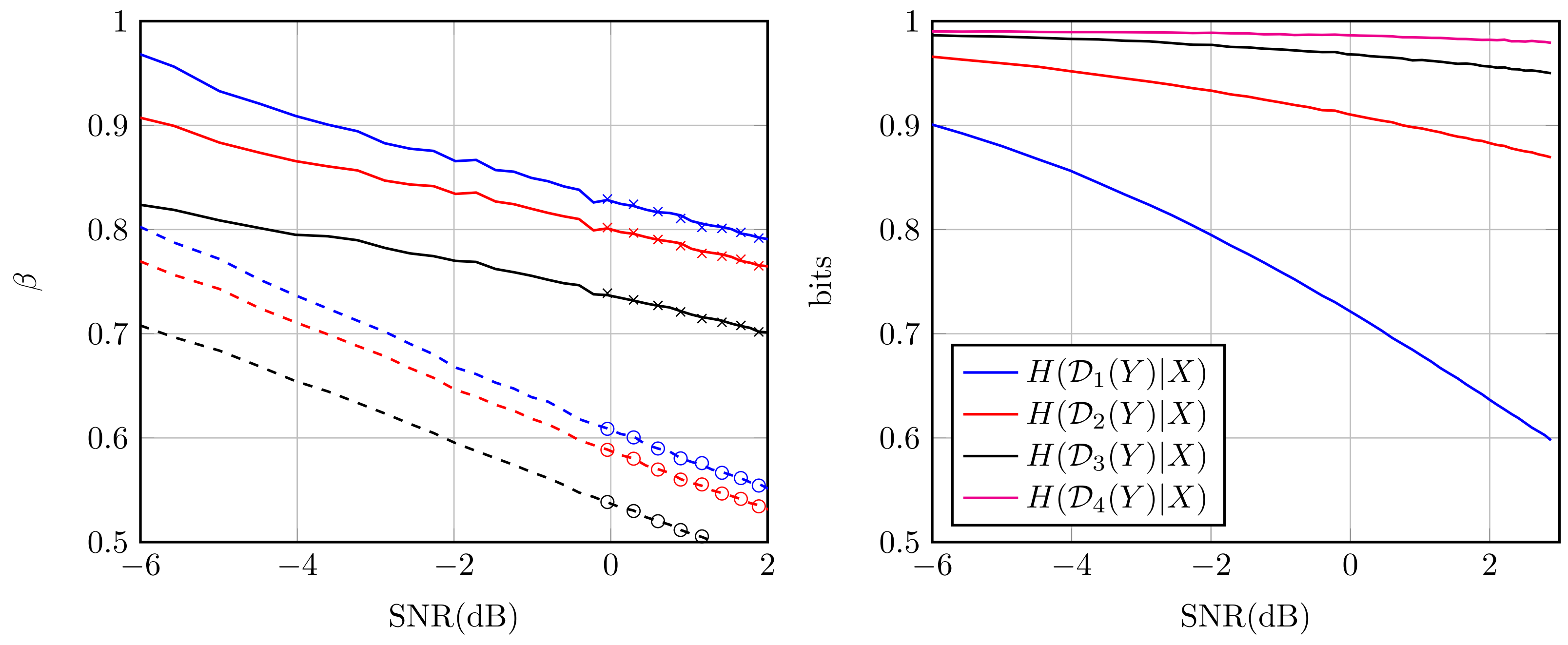

**Figura 1:** (a) Maximum reconciliation efficiency reached by $l$-DTE with $l \in \{2, 3, 4\}$ (black, red and blue plots, respectively), $\tilde{V}_m = 1$ and $\xi = 0.02$. Solid and dashed lines correspond to the efficiency considering RR with heterodyne and homodyne detection, respectively. Cross and circle marks refer to direct reconciliation (heterodyne and homoyne detection, respectively); (b) Conditional entropy $H(\mathcal{D}_i(Y)|X)$.

## Conclusions

We have presented an information reconciliation protocol designed for Continuous-Variable QKD using the Distributional Transform, a tool from copula theory. Together with arguments from information theory, it was made possible to extract bit sequences from Gaussian random variables whose bits are undoubtedly independent. We showed that each bit in the binary expansion can be treated as an independent channel and its capacities where estimated considering direct and reverse reconciliation for homodyne and heterodyne detection. We also derived the expressions for the reconciliation efficiency in both reconciliation directions and the results showed that the maximum efficiency is reached in protocols with heterodyne detection and at low SNR. More specifically, it is possible to reach $\beta^{\leftarrow}_{max} > 0.9$ for $\mathrm{SNR}_{het} < -3.6\,\mathrm{dB}$ with a DTE of four bits. Future work could focus on the design of error correcting codes for the DTE induced sub-channels.

## Referências

[1] F. Durante and C. Sempi, Principles of copula theory. Hoboken: CRC Press, 2016.

[2] J. A. T. Thomas M. Cover, Elements of Information Theory. Wiley John + Sons, 2006.

[1] The problem can be generalized to heterodyne detection with adjusted parameters.