

Long-Distance Continuous-Variable Quantum Key Distribution with Advanced Reconciliation of a Gaussian Modulation

L. Gyongyosi^{*a,b}, S. Imre^a

^a Quantum Technologies Laboratory, Department of Telecommunications, Budapest University of Technology and Economics, 2 Magyar tudosok krt, H-1111, Budapest, Hungary;

^b MTA-BME Information Systems Research Group, Hungarian Academy of Sciences, H-1518, Budapest, Hungary

^{*}Electronic address: gyongyosi@hit.bme.hu

ABSTRACT

The two-way continuous-variable quantum key distribution (CVQKD) systems allow higher key rates and improved transmission distances over standard telecommunication networks in comparison to the one-way CVQKD protocols. To exploit the real potential of two-way CVQKD systems a robust reconciliation technique is needed. It is currently unavailable, which makes it impossible to reach the real performance of a two-way CVQKD system. The reconciliation process of correlated Gaussian variables is a complex problem that requires either tomography in the physical layer that is intractable in a practical scenario, or high-cost calculations in the multidimensional spherical space with strict dimensional limitations. To avoid these issues, we propose an efficient logical layer-based reconciliation method for two-way CVQKD to extract binary information from correlated Gaussian variables. We demonstrate that by operating on the raw-data level, the noise of the quantum channel can be corrected in the scalar space and the reconciliation can be extended to arbitrary high dimensions. We prove that the error probability of scalar reconciliation is zero in any practical CVQKD scenario, and provides unconditional security. The results allow to significantly improve the currently available key rates and transmission distances of two-way CVQKD. The proposed scalar reconciliation can also be applied in one-way systems as well, to replace the existing reconciliation schemes.

Keywords: continuous-variable quantum key distribution, reconciliation, Gaussian variables, Gaussian modulation, quantum cryptography, quantum Shannon theory.

1. INTRODUCTION

The QKD (Quantum Key Distribution) systems represent one of the most important practical applications of quantum information theory. The QKD schemes allow unconditionally secret communication between distant parties by exploiting the fundamental attributes of quantum mechanics. The QKD protocols can be classified into two main classes: DV (Discrete-Variable) and CV (Continuous-Variable) QKD systems. The firstly introduced QKD protocols were based on discrete variables, such as photon polarization. Since the polarization of single photons cannot be encoded and decoded efficiently because of the technological limitations of current physical devices, the CVQKD systems were proposed. In a CVQKD system, the information is encoded on continuous variables by a Gaussian modulation, such as in the position or momentum quadratures of coherent states. In comparison to DVQKD, the modulation and decoding of continuous variables does not require specialized devices and can be implemented efficiently by standard telecommunication networks and technologies that are currently available and in widespread use. As follows, the CVQKD systems can be integrated into the current telecommunication networks by using well-established optical fiber networks and practical devices. The CVQKD protocols can be further classified into one-way and two-way systems. In a one-way CVQKD system, Alice, the sender transmits her continuous variables to the receiver, Bob, over a quantum channel [9-11]. In a two-way system, Bob starts the communication, Alice adds her internal secret to the received message, and this is then sent back to Bob (e.g., one mode of the coupled beam that is outputted from a beamsplitter is transmitted back to Bob).

The two-way CVQKD systems were introduced for practical reasons to exceed the limitations of one-way CVQKD, such as low key rates and short communication distances [1-8]. The two-way CVQKD protocols exploit the benefits of multiple channel uses and allow the leak of only lower valuable information to the eavesdropper, and they are also

equipped with significantly stronger capabilities in comparison to one-way protocols. Turning our attention to two-way CVQKD from one-way CVQKD is definitely reasonable, since one-way schemes have almost reached their physical limitations, and no significant further improvements can be realized in the secret key rates and transmission distances, neither by applying more robust post-processing nor by more powerful reconciliation techniques.

The CVQKD schemes use continuous-variable Gaussian modulation which provably provides optimal key rates against collective attacks at finite-size block lengths [1-11] and also maximizes the mutual information between Alice and Bob. The security of CVQKD has also been proven against collective attacks in the asymptotic regime with infinite block sizes, while the analysis of arbitrary attacks in the finite-size regime is currently in progress [9]. One of the most critical points in regard to CVQKD is the post-processing [1-11]. The post-processing is aimed to correct the errors of the quantum channel that are cumulated in the raw data. The raw data is a correlated binary bitstring at Alice's and Bob's side, generated by the random quadrature measurements at the parties. Each quadrature measurement results in a unit in the raw data. The raw data itself contains no secret key; it consists only of the results of the random quadrature measurements. The secret key is a uniformly distributed long binary string that will be combined with the raw data elements, and will be added to the picture only in the stage of logical layer manipulations. The logical layer-based post-processing phase uses purely classical tools: precisely a classical-authenticated communication channel and classical error-correction algorithms. The logical-layer based post-processing basically does the same in the logical layer as the tomography does in the physical layer, and it consists of two main phases: the reconciliation procedure with several error-correction steps, and privacy amplification. The aim of reconciliation is to extract as much valuable information from the correlated raw data as possible and to generate an error-free key between Alice and Bob. The privacy amplification operates on the shared, error-corrected common secret to extract the final key between the parties, and the aim of this phase is to reduce to zero the possible knowledge of an eavesdropper from the elements of the key. The implementation of tomography in the physical layer is a complex problem, and it is intractable in a practical scenario. But, fortunately, well-characterized solutions can be proposed in the logical layer for the same purpose of giving an analogous, and also more valuable answer to the reconciliation of correlated Gaussian variables than the physical-layer tomography ever could. The theoretical background that makes the logical layer-based reconciliation possible also allow us to view the noisy physical quantum channel as a binary Gaussian channel in the logical layer [9-11]. This has the immediate consequence that very efficient binary error-correction tools can be integrated from the world of traditional communication theory into CVQKD—which would not be available for the physical-layer tomography to extract binary information from the correlated Gaussian variables.

The raw data shared over the quantum channel is noisy, and this must be corrected to distill the final secret key. Since a large amount of raw data bits have to be shared between the parties, the complexity of the post-processing phase is a critical point in CVQKD protocols, and it has to be in order to be as low as possible. The existing logical layer-based solutions require high-complexity calculations in the high-dimensional spherical space for the reconciliation of Gaussian variables [9-11]. Since a complex reconciliation is so undesirable, the aim is to find a more efficient solution in the logical layer. Basically, the error correction in the reconciliation phase consists of two phases: First, the binary-channel codes (such as LDPC – Low Density Parity Check, turbo codes, polar codes, etc. [9-11]) that are used for the transmission of the classical bits in the reconciliation phase are corrected. Second, the real Gaussian noise on the received raw-data vector must be corrected, which noise arises from the effect of the quantum channel (i.e., from Eve's optimal Gaussian attack, which is considered in CVQKD protocols [1-11]). In this work we focus on the second phase of reconciliation, which has crucial role in CVQKD, since this phase makes it possible to correct the errors incurred on the quantum channel and to share an error-free key between Alice and Bob. Since the raw data is formulated by binary bitstrings resulted from quadrature measurements at the parties, the reconciliation problem is analogous to the well-known subject of binary-channel coding that operates on binary-channel codes. It also follows that the complicated and difficult to implement physical-layer tomography can be replaced in the logical level by binary error-correction schemes that are easier to implement. At this point we arrived to a critical security requirement of QKD. In the reconciliation phase, only uniform distribution can be transmitted over the classical channel, otherwise the information theoretic security of the protocol cannot be proven [1-13]. The raw data itself follows Gaussian random distribution because these arise from a Gaussian random source; however, by applying some trivial operations on the raw data units, the desired uniform distribution can be reached, and the reconciliation can be performed with unconditional security.

This paper is organized as follows. In Section 2, some preliminary findings of two-way CVQKD are summarized. In Section 3, we introduce the proposed reconciliation scheme. Section 4 provides the error analysis of the reconciliation scheme. Finally, in Section 5, we conclude the paper. For further details and information see [27].

2. DIRECT CODING IN THE PHASE SPACE

Let us denote the quadratures of the i -th signal $S_{Alice,i}$ in the phase space \mathcal{S}_A by $x_{A,i}, p_{A,i}$, and the quadratures of Bob's signal $S_{Bob,i}$ in the phase space \mathcal{S}_B by $x_{B,i}, p_{B,i}$, where $x_{A,i}, p_{A,i} \in \mathbb{N}(0, \sigma_\omega^2)$ and $x_{B,i}, p_{B,i} \in \mathbb{N}(0, \sigma_\omega^2)$ are drawn from a Gaussian random distribution with mean $\mu = 0$, and variance σ_ω^2 , where σ_ω^2 is the modulation variance [1-10]. The coherent states $S_{Alice,i} = |x_{A,i} + ip_{A,i}\rangle \in \mathcal{S}_A$ and $S_{Bob,i} = |x_{B,i} + ip_{B,i}\rangle \in \mathcal{S}_B$ are encoded by Gaussian modulation with dedicated centers $(x_{A,i}, p_{A,i}) \in \mathcal{S}_A$ and $(x_{B,i}, p_{B,i}) \in \mathcal{S}_B$, respectively (Note: Each S_i define a zero-mean, circular symmetric complex Gaussian random variable $\mathcal{CN}(0, \sigma_{S_i}^2)$ with variance $\sigma_{S_i}^2 = \mathbb{E}[|S_i|^2]$ in the phase space \mathcal{S} , with i.i.d. real and imaginary components $x_i, p_i \in \mathbb{N}(0, \sigma_\omega^2)$, thus $\sigma_{S_i}^2 = \mathbb{E}[|S_i|^2] = 2\sigma_\omega^2$. The squared magnitude $|S_i|^2$ is exponentially distributed with density $f(|S_i|^2) = 1/\sigma_{S_i}^2 \exp(-|S_i|^2/\sigma_{S_i}^2), |S_i|^2 \geq 0$.) The two beams are correlated at Alice's BS, which results in a combined signal in the combined phase space $\mathcal{S}_{A \times B}$. The modulation noise $\partial \in \mathcal{CN}(0, \sigma_\partial^2)$, is precisely centered around $(x_{A,i} + x_{B,i}, p_{A,i} + p_{B,i}) \in \mathcal{S}_{A \times B}$ and $(x_{A,i} - x_{B,i}, p_{A,i} - p_{B,i}) \in \mathcal{S}_{A \times B}$ in $\mathcal{S}_{A \times B}$.

After the two beams $S_{Alice,i}$ and $S'_{Bob,i}$ are correlated at a BS at Alice's side, where $S'_{Bob,i}$ is the noisy version of $S_{Bob,i}$, Alice applies a random quadrature measurement M_1 on the first mode of the beam, while the second mode is transmitted back to Bob over quantum channel \mathcal{N}_2 . Alice's state in the combined phase space $\mathcal{S}_{A \times B}$ is as follows:

$$|\varphi_i\rangle = |x_{A,i} + x'_{B,i} + i(p_{A,i} + p'_{B,i})\rangle \in \mathcal{CN}(0, \sigma_{\varphi_i}^2) \in \mathcal{S}_{A \times B}, \quad (1)$$

with Gaussian random quadrature components $\mathbb{N}(0, 2\sigma_\omega^2 + \sigma_{\mathcal{N}_1}^2)$, where $2\sigma_\omega^2$ is the cumulated modulation variance, $\sigma_{\mathcal{N}_1}^2$ is the variance of \mathcal{N}_1 , $x'_{B,i}, p'_{B,i}$ are Bob's noisy quadratures modified by \mathcal{N}_1 , while $\sigma_{\varphi_i}^2 = \mathbb{E}[|\varphi_i|^2]$. Assuming a homodyne measurement M_1 , Alice gets an X_i unit of her raw data, which is a binary string. If she measured in the position quadrature basis she obtains:

$$X_i = x_{A,i} + x'_{B,i} \quad (2)$$

or, if she used the momentum quadrature basis she gets

$$X_i = p_{A,i} + p'_{B,i}. \quad (3)$$

The second mode of the combined signal in $\mathcal{S}_{A \times B}$ is transmitted directly back to Bob over the noisy channel \mathcal{N}_2 , given as:

$$|\phi_i\rangle = |x_{A,i} - x'_{B,i} + i(p_{A,i} - p'_{B,i})\rangle \in \mathcal{CN}(0, \sigma_{\phi_i}^2) \in \mathcal{S}_{A \times B}, \quad (4)$$

with $\mathbb{N}(0, 2\sigma_\omega^2 + \sigma_{\mathcal{N}_1}^2)$ Gaussian random quadratures, and $\sigma_{\phi_i}^2 = \mathbb{E}[|\phi_i|^2]$. The Gaussian noise of the quantum channel \mathcal{N}_2 defines a noise vector $\Delta_i \in \mathcal{CN}(0, \sigma_{\Delta_i}^2) \in \mathcal{S}_{A \times B}$, with noise components $\Delta_{x_i} \in \mathbb{N}(0, \sigma_{\mathcal{N}_2}^2)$, $\Delta_{p_i} \in \mathbb{N}(0, \sigma_{\mathcal{N}_2}^2)$ which results in the noisy state $|\xi_i\rangle \in \mathcal{S}_{A \times B}$ as follows:

$$|\xi_i\rangle = |\phi_i\rangle + \Delta_i = |x'_{A,i} - x''_{B,i} + i(p'_{A,i} - p''_{B,i})\rangle \in \mathcal{CN}(0, \sigma_{\xi_i}^2) \in \mathcal{S}_{A \times B}, \quad (5)$$

with $\mathbb{N}\left(0, 2\sigma_\omega^2 + \sigma_{\mathcal{N}_1}^2 + \sigma_{\mathcal{N}_2}^2\right)$ distributed Gaussian random quadratures, and $\sigma_{\xi_i}^2 = \mathbb{E}\left[|\xi_i|^2\right]$.

In the next phase, Bob applies a random quadrature measurement M_2 (assumed to be homodyne) and gets block Y_i . If he used a position quadrature basis, he gets

$$Y_i' = x_{A,i}' - x_{B,i}'' \quad (6)$$

and for the momentum quadrature basis he obtains:

$$Y_i' = p_{A,i}' - p_{B,i}'' \quad (7)$$

Bob, calibrating his resulted block Y_i' by $2x_{B,i}$ or $2p_{B,i}$ (depending on the used quadrature measurement), gets back the noisy version X_i' of Alice's raw data unit X_i as:

$$X_i' = Y_i' + 2x_{B,i} = x_{A,i}' - x_{B,i}'' + 2x_{B,i} = x_{A,i}' + x_{B,i}'', \quad (8)$$

and

$$X_i' = Y_i' + 2p_{B,i} = p_{A,i}' - p_{B,i}'' + 2p_{B,i} = p_{A,i}' + p_{B,i}'', \quad (9)$$

which is referred as Bob's *raw data unit*. The noise of the quantum channel is analogous to the addition of a non-standard Gaussian random noise vector Δ_i to Alice's raw data block X_i .

Alice's and Bob's modes in the combined phase space $\mathcal{S}_{A \times B}$ right after being outputted from the BS are $|\varphi_i\rangle$ and $|\phi_i\rangle$, as shown in Fig. 1. Alice obtains the first mode of the beam, $|\varphi_i\rangle$, the second mode $|\phi_i\rangle$ is sent back to Bob. The noise that exists in $\mathcal{S}_{A \times B}$ arises from the modulation noise $\partial \in \mathbb{CN}(0, \sigma_\partial^2)$ (already included in the quadrature distributions) and the two channel uses, \mathcal{N}_1 and \mathcal{N}_2 . The measurements performed on $|\varphi_i\rangle$ and $|\xi_i\rangle$ result in raw data units $X_i \in \mathbb{N}(0, \sigma_X^2)$ and $X_i' \in \mathbb{N}(0, \sigma_{X'}^2)$. The noise of the first channel changes the Gaussian random distribution of the quadratures from $\mathbb{N}(0, 2\sigma_\omega^2)$ to $\mathbb{N}(0, 2\sigma_\omega^2 + \sigma_{\mathcal{N}_1}^2)$ in the combined phase space $\mathcal{S}_{A \times B}$, with mean $\mu = 0$, and results X raw data level variance $\sigma_X^2 = (2\sigma_\omega^2 + \sigma_{\mathcal{N}_1}^2)$, and where noise variance $\sigma_{\mathcal{N}_1}^2$ arises from the first channel use. The quadratures of the second mode of the coupled beam is also characterized by the same variance, i.e., $|\phi_i\rangle \in \mathbb{CN}(0, \sigma_{\phi_i}^2)$.

The noise of \mathcal{N}_2 transforms $|\phi_i\rangle \in \mathcal{S}_{A \times B}$ into $|\xi_i\rangle \in \mathcal{S}_{A \times B}$ and further modifies the distribution, so finally Bob's received quadratures will follow a Gaussian distribution $\mathbb{N}(0, 2\sigma_\omega^2 + \sigma_{\mathcal{N}_1}^2 + \sigma_{\mathcal{N}_2}^2)$. The X' raw data level variance is evaluated as $\sigma_{X'}^2 = (2\sigma_\omega^2 + \sigma_{\mathcal{N}_1}^2 + \sigma_{\mathcal{N}_2}^2)$, which fact arises from the *cumulated* Gaussian random noise of \mathcal{N}_1 and \mathcal{N}_2 . At this point, one can recognize that on the raw data level, only the *difference* of the variance of Alice's and Bob's raw data σ_X^2 and $\sigma_{X'}^2$ has relevance and $\sigma_{\mathcal{N}_1}^2$ vanishes from the picture. This difference is, indeed, $\sigma_{\mathcal{N}_2}^2$. In the level of raw data manipulations Alice's X_i will serve as a *reference unit* to correct Bob's noisy unit, X_i' . In other words, the first channel use will have no relevance in the raw data-level calculations, hence the noise of \mathcal{N}_1 can be excluded from the error-correction process. Precisely, the use of \mathcal{N}_1 has only one consequence: it increases the initial variance $2\sigma_\omega^2$ by $\sigma_{\mathcal{N}_1}^2$, which finally results in $\mathbb{N}(0, \sigma_X^2)$ on the level of raw data blocks. In particular only \mathcal{N}_2 will have significance in the whole scenario, and, in fact, only the noise of the second channel use has to be corrected in the reconciliation phase. (*Note:* Throughout the manuscript, the noise will be modeled on the quadrature-level by a real vector, and the notation of \mathbb{CN} will be simplified to \mathbb{N} .)

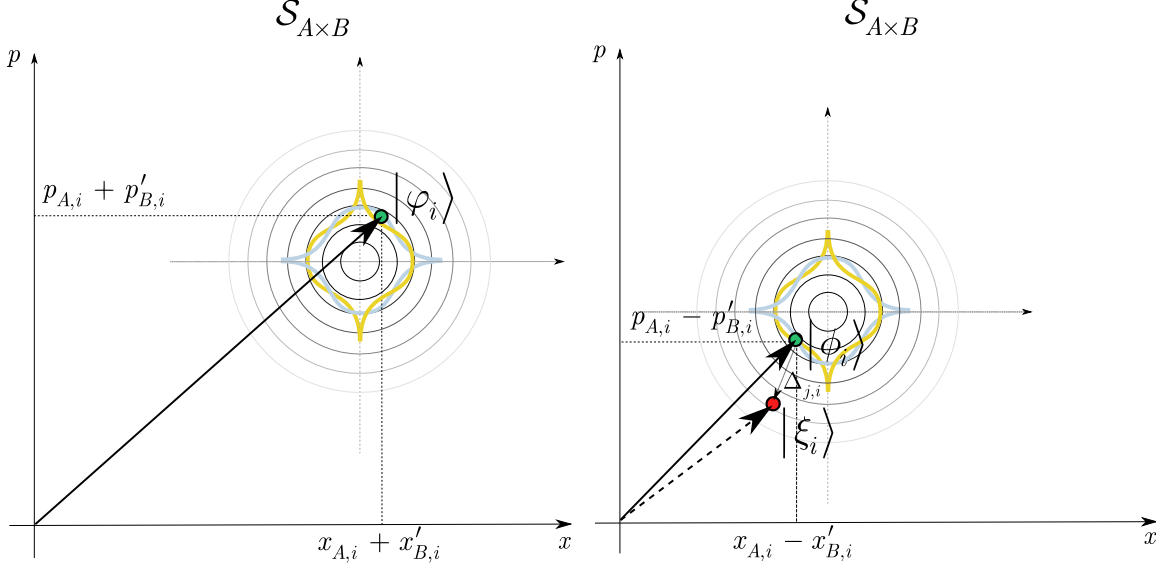


Figure 1. The combined signals $|\varphi_i\rangle \in \mathcal{CN}(0, \sigma_{\varphi_i}^2)$ and $|\phi_i\rangle \in \mathcal{CN}(0, \sigma_{\phi_i}^2)$ in the combined phase space, $\mathcal{S}_{A \times B}$. The modulation noise $\partial \in \mathcal{CN}(0, \sigma_{\partial}^2)$ in the combined signal space $\mathcal{S}_{A \times B}$ is illustrated by the Gaussian curves. The noise $\Delta_i \in \mathcal{N}(0, \sigma_{\mathcal{N}_2}^2)$ of quantum channel \mathcal{N}_2 distorts the distribution of the quadratures from $\mathcal{N}(0, 2\sigma_{\omega}^2 + \sigma_{\mathcal{N}_1}^2)$ into $\mathcal{N}(0, 2\sigma_{\omega}^2 + \sigma_{\mathcal{N}_1}^2 + \sigma_{\mathcal{N}_2}^2)$. Alice's raw data variance is $\sigma_X^2 = (2\sigma_{\omega}^2 + \sigma_{\mathcal{N}_1}^2)$, while Bob's raw data variance is $\sigma_{X'}^2 = (2\sigma_{\omega}^2 + \sigma_{\mathcal{N}_1}^2 + \sigma_{\mathcal{N}_2}^2)$.

For further information see [27].

3. SCALAR RECONCILIATION OF A GAUSSIAN MODULATION

We start our description from the point at which the quantum states are completely transmitted through the quantum channel from Alice to Bob. At this point all interactions with the quantum channel are closed, and the post-processing phase is being started. First, Alice and Bob exclude from the raw data those measurements that have been performed in different quadratures that results in the N -unit length raw data vectors. Then formulate N/d number of d -dimensional vectors $\mathbf{X}_j \in \mathbb{R}^d$, $\mathbf{X}'_j \in \mathbb{R}^d$. These quantities are introduced as follows.

Let $X \in \mathbb{R}^N$ and $X' \in \mathbb{R}^N$ the N -unit length raw data of Alice and Bob. The d -dimensional vectors $\mathbf{X}_j \in \mathbb{R}^d$ and $\mathbf{X}'_j \in \mathbb{R}^d$, for $j=0, j \leq (N/d) - 1$, of Alice and Bob are defined as:

$$\mathbf{X}_j = (X_{j,0}, \dots, X_{j,d-1})^T \in \mathcal{N}(0, \sigma_X^2)_d \quad (10)$$

and

$$\mathbf{X}'_j = (X'_{j,0}, \dots, X'_{j,d-1})^T \in \mathcal{N}(0, \sigma_{X'}^2)_d, \quad (11)$$

where $X_{j,i} \in \mathcal{N}(0, \sigma_X^2) \in \mathbb{R}$ and $X'_{j,i} \in \mathcal{N}(0, \sigma_{X'}^2) \in \mathbb{R}$ refer to the i -th unit of the j -th vector, respectively. Alice and Bob have to share a common secret by using their correlated raw data. For this purpose, they establish a proper code-alphabet $\mathcal{A} = \{a, b\}$, where $a \in \mathbb{R}$ and $b \in \mathbb{R}$ are two public variables (i.e., Eve also has access to it). In the reverse reconciliation these will be selected *uniformly at random* in the form of several $U_j \in \{a, b\}$ -s at Bob's side, with $\Pr(a) = \Pr(b) = 0.5$. A secret d -dimensional key vector \mathbf{U}_j is drawn from a uniform distribution \mathcal{U} and built up

from d units, $U_{j,i} \in \mathbb{R}$, as:

$$\mathbf{U}_j \in \mathbb{R}^d : (U_{j,0}, \dots, U_{j,d-1})^T, U_{j,i} \in \mathbb{R}, \text{ for } j=0, j \leq (N/d) - 1. \quad (12)$$

The d units $U_{j,i} \in \mathcal{U}$ of \mathbf{U}_j are uniform random variables, as follows:

$$U_j \in \{a, b\} = \sum_{i=0}^{d-1} U_{j,i} \in \mathcal{U}. \quad (13)$$

From (13) follows, that (12) can be rewritten as $\mathbf{U}_j \in \{\mathbf{A}, \mathbf{B}\} \in \mathbb{R}^d$, with vectors \mathbf{A}, \mathbf{B} as:

$$\mathbf{A} : (a_{j,0}, \dots, a_{j,d-1})^T, \left\{ \sum_{i=0}^{d-1} a_{j,i} = a \right\}, \mathbf{B} : (b_{j,0}, \dots, b_{j,d-1})^T, \left\{ \sum_{i=0}^{d-1} b_{j,i} = b \right\}. \quad (14)$$

As follows, Bob granulates the selected a or b into d number of uniformly random variables $U_{j,i}$, so that the sum of the units will be equal to the selected value.

The *full key* \mathbf{K} is built up as:

$$\mathbf{K} \in \mathbb{R}^{N/d} : (U_0, \dots, U_{(N/d)-1})^T. \quad (15)$$

The reconciliation problem in the level of logical layer is summarized as follows. Alice and Bob first agree on d . Bob sends the blocks of $C(\mathbf{X}'_j) \mathbf{U}_j \in \mathbb{R}^d$, for $j=0, j \leq (N/d) - 1$, over the classical channel. Alice then receives the d noisy $U'_{j,i}$ units, and by using her X she has to decode U'_j as [9]

$$\sum_{i=0}^{d-1} U'_{j,i} = \left(\sum_{i=0}^{d-1} C(X'_{j,i}) / \sum_{i=0}^{d-1} C(X_{j,i}) \right) \sum_{i=0}^{d-1} U_{j,i} \quad (16)$$

and then she has to make an error-correction to remove the noise from U'_j .

In comparison to the multidimensional reconciliation, the scalar reconciliation uses a fundamentally different solution to achieve the uniform distribution of the raw data. While the former is based on sophisticated multidimensional spherical operations, our solution requires only the use of a simple function in the scalar space. In our scheme, the *uniformity* of the correlated raw data units is achieved by the *Gaussian Cumulative Distribution Function* (CDF). Another important difference is that the approximation of the logical binary Gaussian channel can be achieved by *arbitrary* dimensional vectors with arbitrary accuracy, which is justified by the *Central Limit Theorem* (CLT).

On Alice's and Bob's side, the Gaussian CDF function can be used to reach the uniform distribution of the correlated raw data. Since we assumed reverse reconciliation let us to start the description from Bob's perspective. Let Bob's raw data unit $X'_{j,i}$ with Gaussian random distribution $\mathbb{N}(0, \sigma_{X'}^2)$. The Gaussian CDF-transformation $C(\cdot) : \mathbb{R} \rightarrow \mathbb{R}$ for a unit $X'_{j,i}$ is as follows:

$$C(X'_{j,i}) = \frac{1}{2} \left(1 + \operatorname{erf} \left(\frac{X'_{j,i}}{\sqrt{2\sigma_{X'}^2}} \right) \right), \text{ for } i \in [d], \quad (17)$$

where

$$\operatorname{erf} \left(\frac{X'_{j,i}}{\sqrt{2\sigma_{X'}^2}} \right) = \frac{2}{\sqrt{\pi}} \int_0^{X'_{j,i}} e^{-t^2} dt \quad (18)$$

is the Gauss error function, and $C(X'_{j,i}) \in \mathbb{R}$ is a real variable from the range of $[0, 1]$, with \mathcal{U} *uniform* distribution (for a plausible example see *Supplementary Information* of [27]). The quantity $C(X'_{j,i})$ will be referred as the *CDF-transformed unit*.

Alice also applies the CDF transformation, and takes into account her raw data variance σ_X^2 for the units of $X_{j,i}$ to get

$C(X_{j,i})$:

$$C(X_{j,i}) = \frac{1}{2} \left(1 + \operatorname{erf} \left(\frac{X_{j,i}}{\sqrt{2\sigma_X^2}} \right) \right), \text{ for } i \in [d], \quad (19)$$

and the result of (17) and (19) is the correlated uniform raw data $C(X_{j,i}) \approx C(X'_{j,i})$. In the reconciliation process, only Alice can correct U'_j into U_j , because nobody knows the CDF-transformed raw data units $C(X_{j,i})$, except Alice. For a given $\mathbf{X}_j \in \mathbb{R}^d$, the CDF function $C(\cdot) : \mathbb{R} \rightarrow \mathbb{R}$ reads as

$$C(\mathbf{X}_j) = C(X_{j,0}), \dots, C(X_{j,d-1}) = \frac{1}{2} \left(1 + \operatorname{erf} \left(\frac{X_{j,i}}{\sqrt{2\sigma^2}} \right) \right) \in \mathbb{R}, \text{ for } i \in [d], \quad (20)$$

Applying the results for Bob's raw data the CDF-transformed vector is:

$$C(\mathbf{X}'_j) = C(X'_{j,0}), \dots, C(X'_{j,d-1}) = \frac{1}{2} \left(1 + \operatorname{erf} \left(\frac{X'_{j,i}}{\sqrt{2\sigma^2}} \right) \right) \in \mathbb{R}, \text{ for } i \in [d]. \quad (21)$$

The CDF-transformed $C(\mathbf{X}_j)$, $C(\mathbf{X}'_j)$ raw data vectors each consist of d real \mathbb{R} variables as:

$$C(\mathbf{X}_j) = \bigcup_{i=0}^{d-1} C(X_{j,i}), \quad C(\mathbf{X}'_j) = \bigcup_{i=0}^{d-1} C(X'_{j,i}). \quad (22)$$

In the multidimensional case, the precision of the approximation of the logical binary Gaussian channel (i.e., the quality of the physical-logical channel conversion) was quantified by the Dirac distribution [9-11]. Since in the scalar reconciliation the spherical space is eliminated, a different solution was needed to analyze the accuracy of the conversion between the physical-logical Gaussian channels. Our answer for the problem is the *Central Limit Theorem* and a mathematical result from the 19th century – the so-called *Lyapunov-condition* [26]. The accuracy of the physical-logical conversion of scalar reconciliation can be maximized and it can be made in arbitrary high dimensions as it is being stated in Lemma 1.

Lemma 1. *The noise variance of the converted logical binary Gaussian channel asymptotically coincidences with the noise variance of the physical quantum channel, which allows to reach the theoretical maximum of the capacity of the converted logical binary channel.*

Proof.

Let $X_{j,i} \in \mathbb{R}$ and $X'_{j,i} \in \mathbb{R}$ the j -th units of Alice's and Bob's raw data, respectively. For a d -dimensional vector $\mathbf{U}_j = (U'_{j,0}, \dots, U'_{j,d-1})^T$, the sum of the independent noise $\{\delta_{j,0}, \dots, \delta_{j,d-1}\}$ units on the secret noisy key units $U'_{j,i} = U_{j,i} + \delta_{j,i}$ will approximate a zero-mean Gaussian random variable with mean $\mathbb{E}[\delta_{j,i}] = \mu_{\delta_{j,i}} = 0$, noise variance $\operatorname{var}[\delta_{j,i}] = \sigma_{\delta_{j,i}}^2$ as follows:

$$\begin{aligned} \text{CLT} : \frac{1}{\sqrt{\sum_{i=0}^{d-1} \sigma_{\delta_{j,i}}^2}} \delta_j &= \frac{1}{\sqrt{\sum_{i=0}^{d-1} \sigma_{\delta_{j,i}}^2}} \left(\sum_{i=0}^{d-1} \delta_{j,i} \right) \rightarrow \mathbb{N}(0, 1)_d \\ \delta_j &= \left(\sum_{i=0}^{d-1} \delta_{j,i} \right) \rightarrow \mathbb{N}\left(0, \sum_{i=0}^{d-1} \sigma_{\delta_{j,i}}^2\right) = \mathbb{N}\left(0, \sigma_{\delta_{j,i}}^2\right)_d. \end{aligned} \quad (23)$$

To show that (23) holds for the d -dimensional noise parameter δ_j , we exploit the Lyapunov-condition [26]. Let $\mathcal{L} > 0$, then

$$\lim_{d \rightarrow \infty} \frac{1}{\left(\sqrt{\sum_{i=0}^{d-1} \sigma_{\delta_{j,i}}^2} \right)^{2+\mathcal{L}}} \sum_{i=0}^{d-1} \mathbb{E} \left[|\delta_{j,i}|^{2+\mathcal{L}} \right] = 0 \quad (24)$$

is satisfied for any $d \rightarrow \infty$, by theory. As follows, the noise on $\mathbf{U}_j \in \mathbb{R}^d$ will converge to

$$\delta_j = \left(\sum_{i=0}^{d-1} \delta_{j,i} \right) \in \mathbb{N}\left(0, \sigma_{\delta_j}^2\right)_d, \quad (25)$$

and the resulting logical channel will be equivalent to a logical binary Gaussian channel with noise variance $\sigma_{\delta_j}^2$. By the same argumentation, the variance of the resulting logical binary Gaussian channel will converge to the variance of the physical Gaussian quantum channel $\sigma_{\mathcal{N}_2}^2$ for $N \rightarrow \infty$.

Let again $\mathcal{L} > 0$, and d is an appropriate dimension for which (24) is satisfied, and let the expected variance of δ_j is

$$\text{var}[\delta_j] = \sigma_{\mathcal{N}_2}^2. \quad (26)$$

Then

$$\lim_{N \rightarrow \infty} \frac{1}{\left(\sqrt{\sum_{j=0}^{(N/d)-1} \sigma_{\mathcal{N}_2}^2} \right)^{2+\mathcal{L}}} \sum_{j=0}^{(N/d)-1} \mathbb{E} \left[|\delta_j|^{2+\mathcal{L}} \right] = 0, \quad (27)$$

is satisfied by theory, from which

$$\begin{aligned} \text{CLT} : \frac{1}{\sqrt{\sum_{j=0}^{(N/d)-1} \sigma_{\mathcal{N}_2}^2}} \left(\sum_{j=0}^{(N/d)-1} \delta_j \right) &\rightarrow \mathbb{N}(0, 1)_{N/d} \\ \left(\sum_{j=0}^{(N/d)-1} \delta_j \right) &\rightarrow \mathbb{N}\left(0, \sum_{j=0}^{(N/d)-1} \sigma_{\mathcal{N}_2}^2\right) = \mathbb{N}\left(0, \sigma_{\mathcal{N}_2}^2\right)_{N/d}, \end{aligned} \quad (28)$$

follows, which proves the statement. Hence one can readily recognize that

$$\lim_{N \rightarrow \infty} \text{var} \left[\delta_{0 \dots (N/d)-1} \right] = \left(\sigma_{\mathcal{N}_2}^2 \right)_{N/d}. \quad (29)$$

To conclude the situation, in (23) and (28) the variances of δ_j and $\sum_{j=0}^{(N/d)-1} \delta_j$, indeed, are not scaled up by d and N/d , which makes possible to convert the physical Gaussian quantum channel to a logical binary Gaussian channel with noise variance $d\sigma_{\delta_j}^2 \approx \sigma_{\mathcal{N}_2}^2$ for arbitrary d . In other words, these results allow for one to obtain the lowest noise variance and hence, the highest SNR of the logical channel that is possible by theory, because the noise variance $\sigma_{\delta_j}^2$ is lower bounded by $\sigma_{\mathcal{N}_2}^2$, i.e., $\sigma_{\delta_j}^2 \geq \sigma_{\mathcal{N}_2}^2$ holds, by theory. At the resulting SNR, the capacity of the logical binary Gaussian channel also picks up its maximum. From this one can immediately conclude, that, in fact, it is a favorable result because the logical channel is indeed a binary Gaussian channel which is equipped with the same capacity at low SNRs (which is the situation in an experimental long-distance scenario) than the physical Gaussian quantum channel. In our solution, the lower bound $\sigma_{\delta_j}^2 = \sigma_{\mathcal{N}_2}^2$ is precisely reached and is justified by the Lyapunov-condition, which means that our conversion provides the best approximation that is possible.

The key idea is as follows: do the reconciliation in the scalar space to reduce the problem from Γ^{d-1} of \mathbb{R}^d into \mathbb{R} . At this point, the main drawback of the multidimensional reconciliation approaches has to be clear: the processes required the use of spherical space Γ^{d-1} of \mathbb{R}^n to achieve the uniform distribution. As we have found in a CVQKD scenario it is not a required condition, and completely can be eliminated. Why? Because, the fact, that the uniformly distributed elements of \mathbb{R}^d have to be transmitted over the classical authenticated channel, *per se*, does not imply that the reconciliation has to be executed in the spherical space. The spherical correction of the errors of the raw data is a completely undesirable and unwanted event in a practical CVQKD, because it would just cause a further decrease in the very fragile, sensitive, and so strenuously established secret key rates. The use of Γ^{d-1} of \mathbb{R}^d served only one purpose in the multidimensional reconciliation: to guarantee the security requirements of the QKD post-processing phase. From this it immediately can be concluded that the use of spherical space is, in fact, *unnecessary*, and a mathematically equivalent and more efficient solution exists in the scalar space of \mathbb{R} .

At this point, one can recognize *two improvements* in our proposed scheme in comparison to the existing approaches. First, the uniform distribution will be reached by a simple operation, the Gaussian-CDF function applied separately on each unit of the raw data. Second, the approximation of the Gaussian channel will be justified by the CLT, using *arbitrary* dimensional vectors. As follows, the physical-logical channel conversion can be established with arbitrary high precision, since the $d \leq 8$ limitation has also been eliminated from the picture. To conclude, the spherical space can be replaced by the CDF transformation on the raw data units, and the Dirac distribution can be replaced by the CLT. It is clear now that the existing reconciliation methods require a revision since its application just leads to further slow-down in a practical CVQKD scenario. By these reasons, we drop away the spherical space, and instead of it, use the CDF-transformed units. These improvements allow very efficient decoding and error-correction, however, this step does not modify any fine property of the code: in other words, it keeps the desired uniform distribution and guarantees the arbitrary high-precision in the approximation of the logical binary Gaussian channel. Finally, we have to emphasize again that the whole reconciliation procedure is implemented through the logical layer only, without any need of physical-layer tomography. For the further details see [27].

3.1 Run of scalar reconciliation

The run of scalar reconciliation (assuming reverse reconciliation) is sketched as follows. Bob divides his N -unit length raw data X' into $n = N/d$ number of d -dimensional vectors $\mathbf{X}'_j = (X'_{j,0}, \dots, X'_{j,d-1})^T \in \mathbb{R}^d$, where d is the length of the vectors measured in units $X'_{j,i}$ in the raw data. Then for each \mathbf{X}'_j , applies CDF transformation C on the units $X'_{j,i} \in \mathbb{R}$ of \mathbf{X}'_j , for $i = 0, i \leq d-1$, for $j = 0, j \leq (N/d) - 1$. Bob generates $\mathbf{U}_j = (U_{j,0} \dots U_{j,d-1})^T \in \mathbb{R}^d$, $U_{j,i} \in \mathbb{R}$, computes $C(\mathbf{X}'_j)\mathbf{U}_j$, and sends it to Alice over the classical authenticated channel. Alice also divides her N -unit length raw data X , into $n = N/d$ number of d -dimensional vectors $\mathbf{X}_j = (X_{j,0}, \dots, X_{j,d-1})^T \in \mathbb{R}^d$, computes the CDF-transformed vectors $C(\mathbf{X}_j)$ and decodes as

$$\begin{aligned} U'_j &= C(\mathbf{X}'_j)U_j \frac{1}{C(X_j)} \\ &= \sum_{i=0}^{d-1} U'_{j,i} = \frac{\sum_{i=0}^{d-1} C(X'_{j,i})}{\sum_{i=0}^{d-1} C(X_{j,i})} \sum_{i=0}^{d-1} U_{j,i}. \end{aligned} \quad (30)$$

Next, she corrects the Gaussian noise on U'_j to get U_j . From these she rebuilds the error-free full key

$$\mathbf{K} \in \mathbb{R}^{N/d} : \left(U_0, \dots, U_{(N/d)-1} \right)^T. \quad (31)$$

3.2 Security of scalar reconciliation

The scalar reconciliation provides unconditional security. It will be demonstrated for reverse reconciliation. The security of scalar reconciliation is guaranteed by the fact that the transmitted $C(\mathbf{X}'_j)\mathbf{U}_j$ messages have *uniform* distribution, and the multiplied \mathbf{U}_j and \mathbf{X}'_j vectors are also uniform and independent. The following conditional probability holds for each U_j :

$$\Pr(U_j = U_{0\dots 1} | C(\mathbf{X}'_j)\mathbf{U}_j) = \frac{1}{2}. \quad (32)$$

Since $C(\mathbf{X}'_j)\mathbf{U}_j$ are uniformly distributed, and also independent [11], it follows that:

$$\Pr(C(X'_{j,i}) = C(X'_{j,0}) \dots C(X'_{j,N-1})) = \frac{1}{N} \quad (33)$$

and

$$\Pr(U_j = U_{0\dots 1}) = \frac{1}{2}. \quad (34)$$

Since the overall number of d -dimensional $\mathbf{U}_j \in \mathbb{R}^d$ vectors is N/d , the probability that Eve obtains the full key \mathbf{K} is

$$\Pr_{Eve} \left(\mathbf{K} = \left(U_0, \dots, U_{(N/d)-1} \right)^T \right) = \frac{1}{2^{N/d}}. \quad (35)$$

For the further details see [27].

4. ERROR ANALYSIS OF SCALAR RECONCILIATION

The error probability $\Pr(\text{error}) = Q\left(\frac{|a-b|}{2} \frac{1}{\eta}\right)$ of scalar reconciliation depends only on $|a-b|$, where $Q\left(\frac{|a-b|}{2} \frac{1}{\eta}\right) = \Pr\left(\frac{|a-b|}{2} \frac{1}{\eta} < g\right)$ is the Q -function (tail function) of a standard Gaussian random variable $g \in \mathbb{N}(0,1)$, and $\eta = \sqrt{\sigma_{\delta_j}^2} = \sqrt{\sum_{i=0}^{d-1} \sigma_{\delta_{j,i}}^2}$ is the standard deviation of the Gaussian noise δ_j . The $\Pr(\text{error})$ exponentially converges to zero for any $|a-b| > 2\eta$.

Let

$$U_j \in \{a, b\} = \sum_{i=0}^{d-1} U_{j,i}, \quad (36)$$

$$C(X_j) = \sum_{i=0}^{d-1} C(X_{j,i}) \quad (37)$$

and

$$C(\Delta_j) = \sum_{i=0}^{d-1} C(\Delta_{j,i}). \quad (38)$$

In the scalar reconciliation process Alice decides on the scalar quantity $U'_j = a$, if:

$$\Pr(U_j = a | U'_j) \geq \Pr(U_j = b | U'_j). \quad (39)$$

Similarly, she decides on $U'_j = b$, if:

$$\Pr(U_j = b | U'_j) \geq \Pr(U_j = a | U'_j). \quad (40)$$

Conditioned on a or b , the received U'_j has mean $\mu_a = a$ or $\mu_b = b$, with $\mathbb{N}(\mu_a, \eta^2)$ and $\mathbb{N}(\mu_b, \eta^2)$.

Applying the maximum-likelihood-based correction rule [15-19], Alice calculates with the following inequalities:

$$\frac{1}{\sqrt{2\pi\eta^2}} e^{-\frac{(U'_j - a)^2}{2\eta^2}} \geq \frac{1}{\sqrt{2\pi\eta^2}} e^{-\frac{(U'_j - b)^2}{2\eta^2}} \quad (41)$$

and:

$$\frac{1}{\sqrt{2\pi\eta^2}} e^{-\frac{(U'_j - b)^2}{2\eta^2}} \geq \frac{1}{\sqrt{2\pi\eta^2}} e^{-\frac{(U'_j - a)^2}{2\eta^2}}, \quad (42)$$

which then leads to:

$$|U'_j - a| < |U'_j - b| \quad (43)$$

and:

$$|U'_j - a| > |U'_j - b|. \quad (44)$$

The received U'_j has mean $\mu_a = a$ or $\mu_b = b$, hence one obtains the following conditional probability for an error

event, conditioned on Bob has sent $U_j = a$:

$$\Pr\left(U'_j = \frac{U_j}{C(X_j)} C(\Delta_j) < \frac{\mu_a + \mu_b}{2} \middle| U_j = a\right) = \Pr\left(U'_j = \frac{U_j}{C(X_j)} C(\Delta_j) > \frac{\mu_a + \mu_b}{2}\right), \quad (45)$$

where $\frac{|\mu_a - \mu_b|}{2}$ assigns a decision boundary. The tail function

$$Q\left(\frac{|a-b|}{2} \frac{1}{\eta}\right) = \Pr\left(\frac{|a-b|}{2} \frac{1}{\eta} < g\right), \quad (46)$$

where $g \in \mathbb{N}(0,1)$, has exponential decay for any $|a - b| > 2\eta$, hence:

$$\frac{1}{\sqrt{2\pi} \left(\frac{|a-b|}{2} \frac{1}{\eta}\right)} \left(1 - \frac{1}{\left(\frac{|a-b|}{2} \frac{1}{\eta}\right)^2}\right) e^{-\frac{\left(\frac{|a-b|}{2} \frac{1}{\eta}\right)^2}{2}} < Q\left(\frac{|a-b|}{2} \frac{1}{\eta}\right) < e^{-\frac{\left(\frac{|a-b|}{2} \frac{1}{\eta}\right)^2}{2}}, \quad (47)$$

which clearly demonstrates that the error probability of scalar reconciliation exponentially converges to zero. As one can readily obtain from (47), for arbitrary large differences between a and b [15-17],

$$Q\left(\frac{|a-b|}{2} \frac{1}{\eta}\right) \rightarrow 0. \quad (48)$$

Alice's error-correction strategy is illustrated in Fig. 2. Alice chooses a if $U'_j < \frac{\mu_a + \mu_b}{2}$, and selects b , if $U'_j > \frac{\mu_a + \mu_b}{2}$ holds.

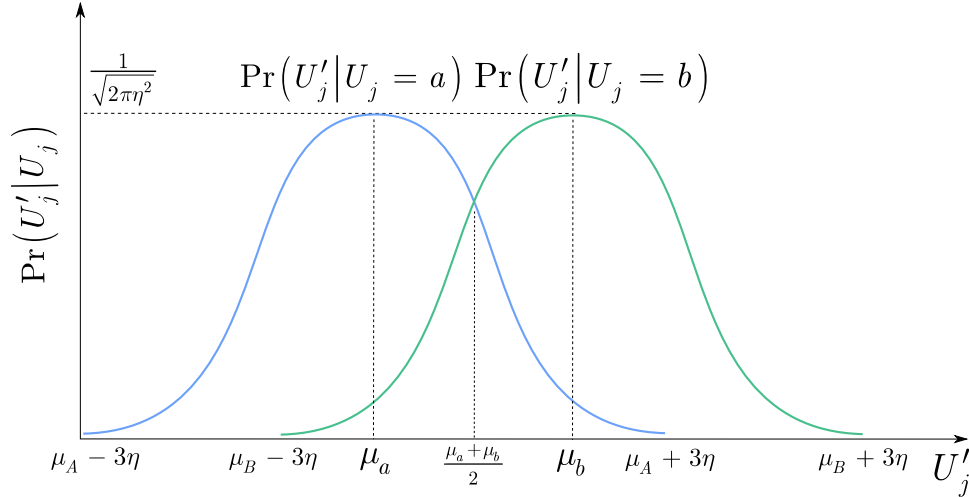


Figure 2. Alice's error correction in the scalar space. Alice corrects each U'_j to rebuild the full key, \mathbf{K} . The noise on a given U'_j has variance η^2 , which arises from the quantum channel. The Gaussian noise of the quantum-level transmission is survived on the raw-data level, and it has distorted Bob's secret U_j into $U'_j = U_j + \delta_j$ on Alice's side.

Thanks to the apparatus provided by maximum-likelihood decision theory and to the application of the Bayes' rule [15-19], for a given U'_j one obtains error probability:

$$\begin{aligned} \Pr\left(U'_j < \frac{\mu_a + \mu_b}{2} \middle| U_j\right) &= \Pr\left(\frac{|a-b|}{2} \frac{1}{\eta} < g\right) \\ &= Q\left(\frac{|a-b|}{2} \frac{1}{\eta}\right) \\ &= \Pr(\text{error}), \end{aligned} \quad (49)$$

which clearly demonstrates that $\Pr(\text{error})$ depends only on the distance $|a - b|$ of a and b . The exponential decay of $\Pr(\text{error})$ is depicted in Fig. 3.

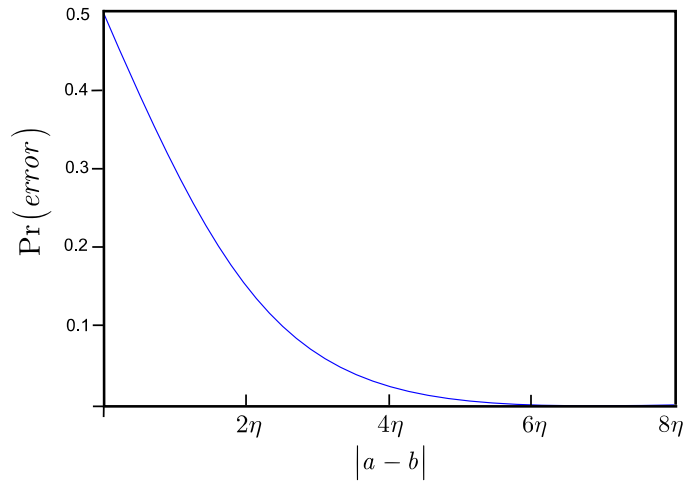


Figure 3. The error probability of the scalar reconciliation process. It converges exponentially to zero as $|a - b| > 2\eta$.

The condition $|a - b| > 2\eta$ can be trivially satisfied by the parties in any practical CVQKD scenario; the proposed results complete the statement. For the further details see [27].

5. CONCLUSIONS

The continuous-variable QKD systems have a great advantage over the DVQKD protocols that can be established over the current telecommunication networks and require only standard network components and devices. The one-way CVQKD protocols have almost reached their physical limits, and no further exploitable resources remain to significantly improve the key rates and transmission distances. The two-way CVQKD protocols are equipped with much stronger hardware in comparison to the one-way protocols, however the lack of the efficient post-processing, up to this point, made it not possible to exploit the real potential of the protocol. The CVQKD protocols are based on Gaussian modulation, and powerful post-processing is needed to maximize the extractable valuable information from the correlated raw data. The physical layer solutions for the reconciliation of Gaussian variables require tomography that is intractable in a practical CVQKD scenario. The reconciliation is also possible in the level of the logical layer by a classical authenticated communication channel and by traditional algorithmical tools. The multidimensional approaches were developed for this purpose, however the use of complex multidimensional calculations is also not desirable in a practical CVQKD scenario, moreover it has strict limitations on the available dimensions. The proposed scalar reconciliation eliminates the use of multidimensional spherical space along with the dimensional boundaries and can be used in arbitrary high dimensions. The scalar reconciliation process neither requires any physical-layer tomography [1-8], and only standard operations and calculations needed in the level of raw data. The method provides unconditional security, and allows a much easier implementation to maximize the extractable valuable binary information from the correlated raw data to significantly boost up the key rates and to improve the distance ranges of two-way CVQKD.

ACKNOWLEDGEMENTS

The results discussed above are supported by the grant TAMOP-4.2.1/B-09/1/KMR-2010-0002, 4.2.2.B-10/1--2010-0009 and COST Action MP1006.

REFERENCES

- [1] S. Pirandola, S. Mancini, S. Lloyd and S. L. Braunstein. *Nature Phys.* 4 726, (2008).
- [2] S. Pirandola, R. Garcia-Patron, S. L. Braunstein and S. Lloyd. *Phys. Rev. Lett.* 102 050503. (2009)
- [3] S. Pirandola, A. Serafini and S. Lloyd. *Phys. Rev. A* 79 052327. (2009).
- [4] S. Pirandola, S. L. Braunstein and S. Lloyd. *Phys. Rev. Lett.* 101 200504 (2008).
- [5] C. Weedbrook, S. Pirandola, S. Lloyd and T. Ralph. *Phys. Rev. Lett.* 105 110501 (2010).
- [6] C. Weedbrook, S. Pirandola, R. Garcia-Patron, N. J. Cerf, T. Ralph, J. Shapiro, and S. Lloyd. *Rev. Mod. Phys.* 84, 621 (2012).
- [7] M. Sun, X. Peng, Y. Shen, H. Guo. *Int. J. Quant. Inf.* 10 1250059 (2012)
- [8] M. Sun, Xiang Peng and Hong Guo. *J. Phys. B: At. Mol. Opt. Phys.* 46 085501 (2013)
- [9] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, *Phys. Rev. A* 84, 062317 (2011).
- [10] P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier, *Phys. Rev. A* 86, 032309 (2012).
- [11] A. Leverrier, R. Alleaume, J. Boutros, G. Zemor, and P. Grangier, *Phys. Rev. A* 77, 042325 (2008).
- [12] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, E. Diamanti, Experimental demonstration of long-distance continuous-variable quantum key distribution, arXiv:1210.6216v1 (2012).
- [13] A. Leverrier, R. Garcia-Patron, R. Renner, and N. J. Cerf, Arxiv preprint arXiv:1208.4920 (2012).
- [14] S. Imre and L. Gyongyosi. *Advanced Quantum Communications - An Engineering Approach*. Wiley-IEEE Press (New Jersey, USA), (2012).
- [15] D. Tse and P. Viswanath. *Fundamentals of Wireless Communication*, Cambridge University Press, (2005).
- [16] J. Hamkins and K. Zeger. Asymptotically efficient spherical codes—Part I: Wrapped spherical codes, *IEEE Trans. Inform. Theory*, vol. 43, pp. 1774–1785, (1997).
- [17] P. F. Swaszek and J. B. Thomas. Multidimensional spherical coordinates quantization, *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 570–576, (1983).
- [18] K. Miller. *Multidimensional Gaussian Distributions*. New York: Wiley, (1964).
- [19] J. Hamkins. Design and analysis of spherical codes, Ph.D. dissertation, Univ. Illinois at Urbana-Champaign, (1996).
- [20] J. H. Conway and D. A. Smith, *On Quaternions and Octonions: Their Geometry, Arithmetic, and Symmetry*, A K Peters/CRC Press, (2003).
- [21] T. Richardson and R. Urbanke, *Modern Coding Theory*, (Cambridge University Press, New York, NY, USA), (2008).
- [22] A. Gersho. Asymptotically optimal block quantization, *IEEE Trans. Inform. Theory*, vol. IT-25, pp. 373–380, (1979).
- [23] D. J. Sakrison. A geometric treatment of the source encoding of a Gaussian random variable, *IEEE Trans. Inform. Theory*, vol. IT-14, pp. 481–486, (1968).
- [24] J. Hamkins and K. Zeger. Gaussian Source Coding With Spherical Codes, *IEEE Trans. Inform. Theory*, vol. 48, no 11, (2002).
- [25] L. Hanzo, H. Haas, S. Imre, D. O'Brien, M. Rupp, L. Gyongyosi. *Wireless Myths, Realities, and Futures: From 3G/4G to Optical and Quantum Wireless*, Proceedings of the IEEE, Volume: 100, Issue: Special Centennial Issue, pp. 1853-1888. (2012).
- [26] J. Rice. *Mathematical Statistics and Data Analysis* (Second ed.), Duxbury Press, ISBN 0-534-20934-3) (1995).
- [27] L. Gyongyosi, Scalar Reconciliation for Gaussian Modulation of Two-Way Continuous-variable Quantum Key Distribution, arXiv:1308.1391 (2013).