Enhancing Continuous-Variable Quantum Key Distribution by State Preparation With Shannon-Kotel'nikov Maps

Edmar J. Nascimento and Francisco M. de Assis

***Abstract*—We propose a continuous-variable quantum key distribution protocol that uses Shannon-Kotel'nikov maps for preparing coherent quantum states. Our protocol has similarities with the no-switching protocol in the sense that it requires that both quadratures need to be measured. It is also a Gaussian modulated protocol, because the secret key is to be extracted from Gaussian parameters. The use of this kind of map in the preparation of coherent states allows the increase in the source-to-distortion ratio (SDR) between Alice and Bob, thus making information reconciliation easier. This increase in SDR is due to the use of nonlinear maps of higher dimension instead of simply raising Alice's variance. We analyze here two kind of maps: the uniform Archimedes' spiral and the geodesics on a flat torus. We assess the security of our protocol through simulations. In order to do that, we simulate the optimal feedforward attack together with a maximum-likelihood receiver, then we use Kraskov's first algorithm to estimate the mutual information.**

***Index Terms*—Quantum cryptography, Continuous-variable quantum key distribution, Shannon-Kotel'nikov maps, No-switching protocol.**

I. Introduction

Cryptographic protocols require a shared secret key in order to allow two parties Alice and Bob to communicate in secrecy. By carrying out a quantum key distribution (QKD) protocol successfully, Alice and Bob can share a secret key even if they are far apart and linked through an insecure communication channel. The security of their communication is guaranteed by quantum mechanics [1]. QKD can be implemented either with discrete variables or continuous variables. While discrete variables protocols require specialized equipment like APDs, continuous-variable quantum key distribution (CVQKD) protocols can be implemented with standard telecom components [2].

In CVQKD, the information is encoded in the quadratures x and p of a quantized electromagnetic field [3]. There is a diversity of continuous-variable protocols which differs on how modulation, state preparation and measurement are realized [2]. Protocols with practical implementations are mostly based on the coherent state protocol GG02 [4], [5]. In this protocol, the quadratures of a coherent state are modulated according to a Gaussian distribution, then this state is sent to Bob. After receiving it, Bob chooses randomly to measure one of the quadratures by homodyne detection. If X denotes the quadrature sent by Alice and Y denotes the Bob's measured quadrature, then $Y = X + Z$, where Z is Gaussian with variance σ_Z^2 and X has power P. So X and Y are described by a Gaussian channel with signal-to-noise ratio (SNR) given by P/σ_Z^2. In order to get a secret key from the random variables X and Y, it is still necessary to carry out the classical procedures of information reconciliation and privacy amplification. Besides GG02, it is also possible to measure both quadratures of the coherent states as it is done in the no-switching (NS) protocol [6], [7]. In this case, both quadratures contribute to generate the secret key at the expense of adding one shot noise unit to the measured outputs.

Security proofs for Gaussian modulated protocols are well established. These protocols are proven secure against collective attacks which turn out to be the most powerful type of attack [8]. Thus, at least theoretically, if reverse reconciliation (RR) is employed, it is possible to distribute a secret key for larger distances (hundreds of kilometers) using CVQKD as long as the excess noise is below a given threshold [5].

When considering practical implementations of Gaussian modulated protocols, a more severe limitation for CVQKD is the inefficiency of reconciliation protocols. This is mostly due to the fact that reconciliation protocols for Gaussian variables rely on classical error correcting codes that need to operate close to the channel capacity in order to achieve higher efficiencies [9], [10]. Codes that are suitable for reconciliation have long length, which results in a complex and computationally demanding decoding process [11].

Extending CVQKD to larger distances requires efficient reconciliation protocols at low SNRs. In [12], CVQKD was implemented over a 25km link of optical fiber. The reconciliation was accomplished by using multilevel coding and multistage decoding (MLC/MSD) [9] together with low-density parity check (LDPC) codes of 200,000 block length, resulting in an overall reconciliation efficiency $\beta = 0.898$ for a SNR of 3.38 (5.3dB). Improvements in reconciliation efficiency were reached in [13] keeping MLC/MSD together with the same block length but employing a different design for LDPC codes. In this case, $\beta = 0.937$ was reached for a SNR of 3 (4.77dB). Further improvements can be attained by designing specific codes for each coding level as in [14]. In this case, LDPC codes of large length (more than a million bits) allowed a $\beta = 0.934$ for a SNR of 0.55 (-2.6dB). For even low SNRs, higher reconciliation efficiencies can be obtained with the

Edmar J. Nascimento is with the Department of Electrical Engineering, Federal University of Vale do Sao Francisco (Univasf), email: edmar.nascimento@univasf.edu.br

Francisco M. de Assis is with the Department of Electrical Engineering, Federal University of Campina Grande (UFCG), email: fmarcos@dee.ufcg.edu.br

Digital Object Identifier: 10.14209/jcis.2019.11

multidimensional reconciliation technique [15], [16], allowing practical implementations of CVQKD in a range of 80km [17].

Instead of trying to improve the performance of CVQKD through reconciliation, another possibility is to increase the SNR at Bob's side. This approach became theoretically possible with the concept of a heralded noiseless linear amplifier (NLA) [18]. In the context of CVQKD, considering an ideal model and the GG02 protocol, a NLA of gain g could allow $20\log_{10} g^2$dB extra losses before the secret key rate drops to zero [19]. When imperfections are considered, simulations done for the no-switching protocol show that a non-ideal LNA could still provide gains in distance and tolerable excess noise [20]. It is not necessary to build a physical LNA to improve the performance of CVQKD. In [21], [22], it is shown that noiseless amplification operations can be simulated in the classical data postprocessing stage.

In this paper, we follow a different approach in order to improve the performance of CVQKD. We aim to increase the source-to-distortion ratio (SDR) at Bob's side through the use of analog encoding in the preparation of coherent states. In our approach, the SDR plays the role of the SNR for traditional CVQKD protocols. We then make use of a geometrical interpretation of nonlinear modulations given in [23], [24]. According to that, the preparation of coherent states can be viewed as a mapping of a given parameter to some point belonging to a curve in a N-dimensional space. The noisy measurement results are projected back in this curve and an estimate of the encoded parameter is obtained. The fidelity between the parameter and its estimate depends on the noise level and properties of the curve like length and curvature. In [25], we proposed a CVQKD protocol using this idea and analyzed it for a uniform Archimedes' spiral mapping under a feedforward attack. Here, we extend our previous analysis by detailing some theoretical aspects and exploring mappings of higher dimension. It is worth saying that such kinds of mappings have been used for security purposes in a totally different scenario. In [26], the physical layer security was analyzed for a wireless classical channel.

The paper is organized as follows: In Sect. II, we describe the theory of Shannon-Kotel'nikov maps and the two kinds of mappings that are used in our scheme. In Sect. III, we review the Gaussian modulated CVQKD protocols and build a simulation model for our protocol. In Sect. IV, our proposed protocol is described. In Sect. V, we discuss some simulation results obtained for our system. Finally in Sect. VI, some conclusions about our work are presented.

II. Shannon-Kotel'nikov maps

We consider a system as depicted in Fig. 1 in which we want to transmit time-discrete symbols of a continuous source through an additive white gaussian noise (AWGN) channel. These symbols are mapped directly onto channel symbols by the transmitter. The receiver, in turn, produces an estimate of the transmitted symbols in order to satisfy some optimality criterion such as the mean-squared error (MSE). This joint source-channel system can be given a geometric interpretation where a parameter $m \in \mathbb{R}^M$ is mapped onto a point $s(m)$

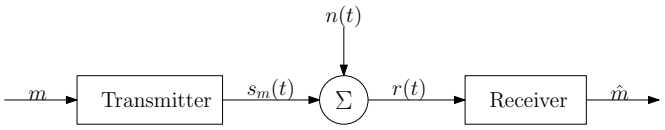


Fig. 1. Source symbols m are mapped by the transmitter onto channel waveforms $s_m(t)$. The channel simply adds some noise to its input. The receiver gives an estimate $\hat{m}$ of the transmitted symbols.

in a curve in $\mathbb{R}^N$ [23]. Such maps are referred as Shannon-Kotel'nikov (SK) maps [27]. When $N > M$, SK maps act like analog error correcting codes, allowing the reduction of the MSE between the source symbols and their respective estimates.

In this paper, we are interested in $1 : N$ mappings. More specifically, we map a source real parameter $m \in [-1, 1]$ onto N channel coordinates through a chosen nonlinear mapping scheme. Using the well known equivalence between vectors and waveforms, for a given orthonormal basis $\{\varphi_i\}_{i=1}^N$, channel waveforms can be represented as vectors

$$\mathbf{s}(m) \quad = \quad [s_1(m)\ s_2(m)\ \cdots\ s_N(m)]. \tag{1}$$

When m is varied along its support, the tip of the vector $\mathbf{s}(m)$ moves along a twisted curve as depicted in Fig. 2. Analogously, the noise process can be represented by a vector $\mathbf{n}$ in such a way that the received signal by the receiver is given by $\mathbf{r} = \mathbf{s}(m) + \mathbf{n}$. For an AWGN channel with power spectral density σ_n^2, a maximum likelihood (ML) receiver produces an estimate $\hat{m}$ that maximizes the likelihood function

$$f(\mathbf{r}|m) = f(\mathbf{r} - \mathbf{s}(m)) = \frac{\exp\left\{-\frac{\|\mathbf{r}-\mathbf{s}(m)\|^2}{2\sigma_n^2}\right\}}{(2\pi\sigma_n^2)^{N/2}}. \tag{2}$$

This function is maximized by the value of m that minimizes $\|\mathbf{r}-\mathbf{s}(m)\|$, that is, the closest point of the curve to the received point.

According to Ziv [28], there is not a single map that reaches the best performance in terms of MSE for all SNRs. The optimal performance theoretically attainable (OPTA) bound gives us a clue on the behavior of optimal maps when dimensions M and N are modified. Considering an AWGN channel with average power P and noise variance σ_n^2, we can define the channel signal-to-noise ratio (CSNR) as $P/(N\sigma_n^2)$. Similarly, for a Gaussian source of variance σ_m^2 and MSE D between source samples and their estimates, we define the source-to-distortion ratio (SDR) as σ_m^2/D. The OPTA bound is obtained by equating the rate-distortion function and the channel capacity [29]. For the Gaussian source and the AWGN channel, the OPTA bound is given by

$$\frac{\sigma_m^2}{D} = \left(1 + \frac{P}{N\sigma_n^2}\right)^{\frac{N}{M}}. \tag{3}$$

As noted in [27], practical mapping performances are far away from OPTA bounds. However, the trend of better SDR performances for higher CSNRs is still verified. From Eq. 3, we can also see that SDR can be improved for a fixed CSNR if we allow N to grow. Such result is known in classical telecommunications as a trade-off between performance and bandwidth expansion. Expressions for the MSE D of generic

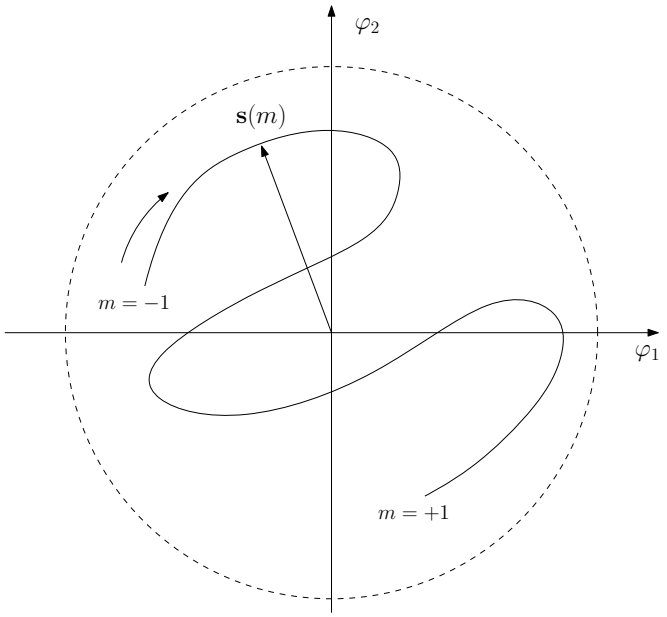


Fig. 2. Representation of a general two-dimensional mapping. Source symbols $m \in [-1, 1]$ are mapped onto channel waveforms. The tip of the vector $\mathbf{s}(m)$ goes through the signal locus.

mappings are usually obtained under the assumption of low noise levels. In this case, the distance between curve folds must be greater than three or four times $\sqrt{N\sigma_n^2}$.

Assuming that a source symbol m_0 corresponds to a mapped point $\mathbf{s}(m_0)$. Under the low noise assumption, the received point $\mathbf{r}$ will lie close to $\mathbf{s}(m_0)$ with high probability. In this way, the signal curve can be approximated by the straight line

$$\mathbf{s}(m) \approx \mathbf{s}(m_0) + (m - m_0)\mathbf{s}'(m_0). \tag{4}$$

The ML estimate can be approximated by the projection of the received point $\mathbf{r}$ onto this line. Then, it can be shown that the conditional MSE is given by

$$E\{(m - \hat{m})^2 | m = m_0\} = \frac{\sigma_n^2}{\|\mathbf{s}'(m_0)\|^2}. \tag{5}$$

If the probability density function (pdf) of m is denoted by f_m, then the MSE is obtained by averaging Eq. 5 over all values of m, that is

$$D = E\{(m - \hat{m})\} = \sigma_n^2 \int_{-1}^{1} f_m \|\mathbf{s}'(m)\|^{-2} dm. \tag{6}$$

It is still necessary to define how source symbols m are mapped onto the signal locus. For a given modulation method, this locus corresponds to a curve of length L. If we introduce an intermediate variable $l(m)$ denoting the length along the locus, it can be shown that [24]

$$D = \sigma_n^2 \int_{-1}^{1} f_m \left| \frac{dl}{dm} \right|^{-2} dm. \tag{7}$$

The minimum MSE is attained if $l(m)$ is chosen as

$$l(m) = L \frac{\int_{-1}^{m} f_u^{1/3} du}{\int_{-1}^{1} f_u^{1/3} du} - \frac{L}{2}. \tag{8}$$

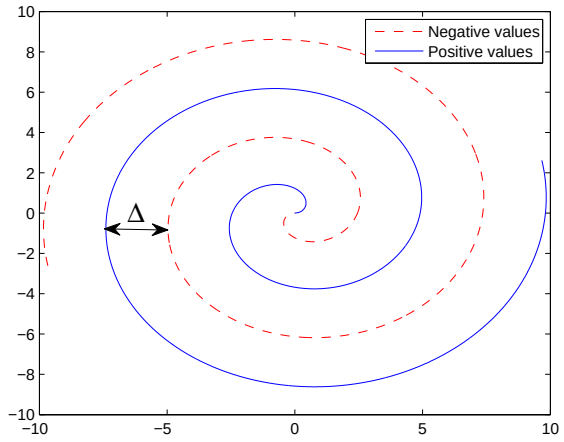


Fig. 3. General plot of an uniform Archimedes' spiral. Dashed line represents negative parameters while solid line represents positive parameters. In this picture, we set $P = 10$, $\Delta = 2.45$ and $\sigma_m = 0.25$.

This operation is referred as a compander or a stretching function. An SK mapping operation is often interpreted as the combination of stretching followed by the bending of the curve. Substituting Eq. 8 into Eq. 7, we get an expression for the minimum MSE given by

$$D_{min} = \frac{\sigma_n^2}{L^2} \left[\int_{-1}^{1} f_m^{1/3} dm \right]^3. \tag{9}$$

It can be seen in Eq. 9 that the MSE can be reduced by increasing the length of the curve. However, due to the power restriction, increasing curve length makes curve folds get closer. In this situation, the threshold effect appears, which makes the MSE to increase rapidly because received points are decoded in different folds of the curve with high probability. Next, we analyze two SK mappings: the uniform Archimedes' spiral [27] and the geodesics on flat tori [30]. The former is a $1:2$ mapping while the latter is a $1:2k$ $(k \geq 2)$ one.

A. *Uniform Archimedes' spiral*

A 1:2 mapping using the uniform Archimedes' spiral is illustrated in Fig. 3. It can be seen that the image of the mapping consists of two intertwined spirals: one for positive source values and the other for negative ones. The distance between spiral's arms is constant and denoted by Δ. Thus, the design of the mapping consists of finding a Δ that maximizes the performance for a given CSNR subjected to an average channel power restriction P.

Instead of using a stretch function like the one in Eq. 8, it was used in [27] the inverse curve length approximation $\varphi(x) = \pm\sqrt{|x|/(0.16\Delta)}$. This choice makes tangent vectors along the curve have equal length, then assuring mutual independence between signal and noise. The spiral map is then given by

$$\mathbf{s}(m) = \operatorname{sgn}(m) \frac{\Delta}{\pi} \sqrt{\frac{g_s|m|}{0.16\Delta}} \begin{pmatrix} \cos \sqrt{\frac{g_s|m|}{0.16\Delta}} \\ \sin \sqrt{\frac{g_s|m|}{0.16\Delta}} \end{pmatrix}, \tag{10}$$

where $\mathrm{sgn}(\cdot)$ is the sign function and g_s is a gain factor that is necessary to keep the power constraint. As previously mentioned, we assume that the source values are truncated into the interval $m \in [-1, 1]$. This means that source distribution parameters have to be chosen properly so as truncation effects might be neglected. For a gaussian source of variance σ_m^2, g_s is given by

$$g_s = \frac{0.16P\sqrt{2\pi^5}}{\sigma_m \Delta(1 - e^{-1/(2\sigma_m^2)})}. \quad (11)$$

For a fixed P, a smaller Δ means a spiral with a larger length (more folds) and, consequently, a better SDR as noted in Eq. 9. However, if Δ is chosen too small compared to the channel noise, the threshold effect becomes dominant, so degrading the system's performance. So, there is a tradeoff that allows an optimal value for Δ to be found. In [27], an expression for the optimal Δ as a function of the CSNR and P is given. For $\sigma_m = 0.25$, this expression is given by

$$\Delta_{opt} = 5.223\sqrt{P}e^{-(3.10^{-4}\mathrm{CSNR}_{dB}^2 + 0.0801\mathrm{CSNR}_{dB})}, \quad (12)$$

where dB points out decibel units. It should be pointed out that the threshold effect can be quite severe for this mapping if the spiral is used for noise levels above designed thresholds. The reason for this is that jumps in decoded arms may represent transitions between signs for source parameters.

B. Geodesics on flat tori

Geodesic curves on a flat torus were used for analog error correction in [31]. Such curves have constant curvature and turn around a flat torus like a helix on a cylinder. For a flat torus in $\mathbb{R}^{2k}$, geodesics are generically described by

$$\begin{aligned} \mathbf{s}_\theta(\alpha) &= [r_1\cos(\omega_1\alpha), r_1\sin(\omega_1\alpha), \cdots \\ &\quad \cdots, r_k\cos(\omega_k\alpha), r_k\cos(\omega_k\alpha)], \end{aligned} \quad (13)$$

where $\theta = \{r_1, r_2, \cdots, r_k, \omega_1, \omega_2, \cdots, \omega_k\}$ is a parametrization for the curve and α is the output of a stretching function (Eq. 8). A twisted curve requires that the elements ω_i be different [30]. Besides, specific constraints for θ must be taken in account in designing analog codes.

In the context of CVQKD, we are interested in good performances for low CSNRs. Then, a bigger distance between curve folds is more valuable than simply extending the curve length. In [32], geodesics parameters were optimized so as to achieve good performances for low CSNRs. This was done by maximizing the global circumradius function over θ. The minimum value of the global circumradius function can be interpreted as the radius of a tube centered along the curve that prevents self intersection [33]. Thus, the minimum distance between curve folds is guaranteed to be twice the minimum value of the global circumradius function.

The circumradius function may be written as

$$\rho(\alpha_1, \alpha_2) = \frac{\|\mathbf{s}(\alpha_1) - \mathbf{s}(\alpha_2)\|}{2|\sin\angle(\mathbf{s}(\alpha_1) - \mathbf{s}(\alpha_2), \mathbf{s}'(\alpha_2))|}, \quad (14)$$

where $\angle(\cdot,\cdot)$ denotes the angle between two vectors. For a smooth curve like the one in Eq. 13, the global circumradius function is given by

$$\rho_g(\alpha) = \min_{\alpha_2} \rho(\alpha, \alpha_2). \quad (15)$$

Then, the minimum distance between curve folds is given by

$$d_{min} = 2\min_{\alpha} \rho_g(\alpha). \quad (16)$$

Optimal θ were found in [32] for a given k by maximizing Eq. 16 subjected to the following restrictions:

$$\|\mathbf{s}_\theta(\alpha)\| = \sum_{i=1}^{k} r_i^2 = 1, \quad (17)$$

$$\|\mathbf{s}_\theta(\alpha)'\| = \sum_{i=1}^{k} r_i^2\omega_i^2 = 1, \quad (18)$$

$$\omega_i = i\omega_i, i = 1, \cdots, k, \quad (19)$$

$$\int_{\alpha=-L/2}^{L/2} \|\mathbf{s}_\theta(\alpha)'\| d\alpha = L. \quad (20)$$

The two first restrictions are usual in designing torus related curves. The third one simplifies the search by restricting it to harmonic frequencies. Finally, the last one avoids the curve to repeat itself at each period by restricting its path length.

III. Gaussian modulated CVQKD protocols

In Gaussian modulated CVQKD protocols with coherent states, Alice prepares and sends coherent states $|x_A + ip_A\rangle$ to Bob. For these states, the displacement values x_A and p_A for the quadratures x or p, respectively, are chosen from a Gaussian distribution of zero mean and variance $V_A N_0$, where N_0 is the shot-noise (vacuum noise) variance and V_A is a scale factor. Bob gets his set of data by measuring randomly one quadrature (GG02 protocol) or both quadratures (NS protocol) for each state sent by Alice. After exchanging some classical information through a public authenticated channel, they end up with two sets of correlated data from which they can distill a secret key. In order to achieve this goal, they have to do some classical data processing that involves channel parameters estimation, information reconciliation and privacy amplification.

As CVQKD protocols are usually designed for fiber optics physical channels, the channel model used to describe them is the lossy channel [2]. In this case, the channel is characterized by the transmission T (the fraction of power that arrives at Bob's, i.e. $0 \leq T \leq 1$) and the excess noise ϵ. After estimating these parameters, Alice and Bob can compute their mutual information I_{AB}. As our construction requires measuring both quadratures, we report next some already known results for the NS protocol.

For the NS protocol, I_{AB}^{NS} has the contribution of both quadratures. Assuming that T and ϵ are the same for both x and p, I_{AB}^{NS} is given by [34]

$$I_{AB}^{NS} = \log\Big(\frac{T(V+\chi)+1}{T(\chi+1)+1}\Big) = \log\Big(1 + \frac{TV_A}{2+T\epsilon}\Big), \quad (21)$$

where $V = V_A + 1$ and $\chi = 1/T - 1 + \epsilon$.

A lower bound to the key generation rate is obtained when we get an upper bound for Eve's knowledge, that means considering an optimal attack that maximizes Eve's information. Eve's bounds depend on the direction of the reconciliation protocol that is being used. When Bob tries to estimate Alice's

data from his data set and some side information, reconciliation protocols are said to employ direct reconciliation (DR). When Alice and Bob roles are reversed, reconciliation protocols are said to employ reverse reconciliation (RR). For the NS protocol, the feedforward attack is proven to be an optimal individual attack that reaches the bound

$$\begin{aligned} I_{AE}^{NS} &= \frac{1}{2}\log\left(\frac{V+\chi_{X_{E_1}}}{1+\chi_{X_{E_1}}}\right)+\frac{1}{2}\log\left(\frac{V+\chi_{P_{E_2}}}{1+\chi_{P_{E_2}}}\right) \\ &= \log\left(\frac{V+\chi_E^{min}}{1+\chi_E^{min}}\right), \end{aligned} \tag{22}$$

for DR, where E_1 and E_2 denote Eve's modes related to the Eve's measured quadratures X_{E_1} and P_{E_2}, respectively. For RR, the bound [35] is given by

$$\begin{aligned} I_{BE}^{NS} &= \frac{1}{2}\log\left(\frac{V_B}{V_{X_B|X_{E_1}}}\right)+\frac{1}{2}\log\left(\frac{V_B}{V_{P_B|P_{E_2}}}\right) \\ &= \log\frac{(V+\chi_E^{min})[T(V+\chi)+1]}{(1+\chi_E^{min})(V+1)}, \end{aligned} \tag{23}$$

where

$$V_B = \frac{T(V+\chi)+1}{2}N_0, \tag{24}$$

$$V_{X_B|X_{E_1}} = \frac{1}{2}(V_{X_{B'}|X_{E_1}}+N_0), \tag{25}$$

$$V_{P_B|P_{E_2}} = \frac{1}{2}(V_{P_{B'}|P_{E_2}}+N_0), \tag{26}$$

$$V_{X_{B'}|X_{E_1}} = V_{P_{B'}|P_{E_2}} \equiv V_{B'|E}^{min} = \frac{V\chi_E^{min}+1}{V+\chi_E^{min}}N_0, \tag{27}$$

$$\begin{aligned} \chi_{X_{E_1}} &= \chi_{P_{E_2}} \equiv \chi_E^{min} \\ &= \frac{T(2-\epsilon)^2}{(\sqrt{2-2T+T\epsilon}+\sqrt{\epsilon})^2}+1. \end{aligned} \tag{28}$$

The asymptotic secret key rate bounds for the NS protocol when considering individual attacks and perfect reconciliation are then given by

$$\Delta I_{DR} \geq I_{AB}^{NS} - I_{AE}^{NS}, \tag{29}$$

$$\Delta I_{RR} \geq I_{AB}^{NS} - I_{BE}^{NS}, \tag{30}$$

where equalities are reached for an optimal attack like the feedforward attack. In an ideal case, $\Delta I_{RR} > 0$ for arbitrary distances if the excess noise is kept below a given threshold. In practical situations, I_{AB}^{NS} is penalized by the reconciliation efficiency β, so that the effective secret key rate for RR is given by

$$\Delta I_{RR}^{eff} = \beta I_{AB}^{NS} - I_{BE}^{NS}.$$

As can be seen in Fig. 4, if CVQKD is to be deployed in a given distance, a $\beta < 1$ limits Alice's variance V_A. In general, a weak signal sent by Alice decreases both I_{AB}^{NS} and I_{BE}^{NS}, but Eve is more affected than Bob. Therefore, the attainability of positive secret key rates for larger distances may be achieved by improving β through reconciliation and limiting V_A.

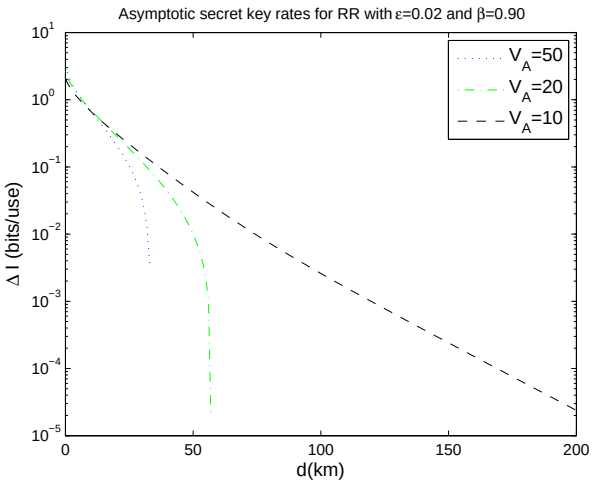


Fig. 4. ΔI_{RR}^{eff} versus distance for the NS protocol. If $\beta = 0.9 < 1$, as V_A is increased, the maximum distance for CVQKD is diminished.

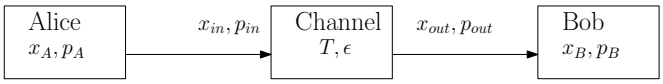


Fig. 5. Simplified model for quadrature variables. Alice's and Bob's quadratures are denoted respectively by (x_A, p_A) and (x_B, p_B). (x_{in}, p_{in}) and (x_{out}, p_{out}) denote the quadratures at the channel input and output, respectively.

A. Simulation Model

In this paper, we assess the gain and security of our protocol through simulations. Therefore, it is necessary to describe how quadrature variables evolve throughout the channel, beam splitters and measurement devices. As it is often assumed, we follow a common approach in which the Alice to Bob channel does not mix quadratures x and p [35]. In this way, quadratures are treated as two independent channels.

In Fig. 5, we give a representation of our model. x_A and p_A denote quadrature variables chosen by Alice, while x_B and p_B denote variables measured by Bob. The quadratures of coherent states at the input and output of the channel are indicated by x_{in}, p_{in} and x_{out}, p_{out}, respectively. The relationship among these variables is given by

$$x_{in} = x_A + x_{vac}^{(a)}, \tag{31}$$

$$x_{out} = \sqrt{T}(x_{in} + B_x), \tag{32}$$

$$\langle B_x^2 \rangle = \chi N_0 = (1/T - 1 + \epsilon)N_0, \tag{33}$$

$$\langle x_{in}^2 \rangle = V N_0 = (V_A + 1)N_0, \tag{34}$$

$$\langle x_{out}^2 \rangle = (TV_A + 1 + T\epsilon)N_0, \tag{35}$$

where $x_{vac}^{(a)}$ denotes the shot noise added to quadrature x in the preparation of coherent states by Alice and $\langle\cdot\rangle$ denotes the expectation value. Similar equations are obtained for quadrature p if we replace x by p in Eqs. 31-35.

Bob's measurement involves splitting the incoming signal in a beamsplitter, followed by a homodyne detection in each output. Assuming an ideal homodyne detector and a real

beam splitter with transmissivity $1/2$ [36], Bob's measured quadratures are described by

$$\begin{aligned} x_B &= \frac{1}{\sqrt{2}}(x_{out} + x_{vac}^{(b)}) \\ &= \sqrt{\frac{T}{2}}(x_A + x_{vac}^{(a)} + \frac{x_{vac}^{(b)}}{\sqrt{T}} + B_x), \qquad (36) \\ p_B &= \frac{1}{\sqrt{2}}(-p_{out} + p_{vac}^{(b)}) \\ &= \sqrt{\frac{T}{2}}(-p_A - p_{vac}^{(a)} + \frac{p_{vac}^{(b)}}{\sqrt{T}} + B_p), \qquad (37) \end{aligned}$$

where $x_{vac}^{(b)}$ and $p_{vac}^{(b)}$ denote the shot noise added to quadratures in the beamsplitter. From Eqs. 36 and 37, it is clear that Bob's measured quadratures are made up of a signal component and noise, so we can define a CSNR representing the Alice to Bob channel as

$$CSNR_{AB} = CSNR_{AB(x)} = CSNR_{AB(p)} = \frac{TV_A}{2 + T\epsilon}. \qquad (38)$$

Following a similar approach, Eve's measured quadratures x_E and p_E can be characterized when she implements the feedforward attack described in Fig. 6. In this kind of attack, Eve reproduces the channel parameters T and ϵ, so remaining undetected. To accomplish this task, Eve has a beamsplitter of transmissivity T_E and a gain factor g_E for their measurement results that must be set to

$$\begin{aligned} g_E &= \sqrt{\epsilon T}, \qquad (39) \\ T_E &= \frac{4T(2 - \sqrt{\epsilon(2 - 2T + T\epsilon)})}{(2 + T\epsilon)^2} - \frac{T(2-\epsilon)}{2 + T\epsilon}. \qquad (40) \end{aligned}$$

In the first beamsplitter, the transmitted and reflected quadratures are represented by

$$\begin{aligned} x_{TE} &= \sqrt{T_E}x_{in} + \sqrt{1 - T_E}x_{vac}^{(e1)}, \qquad (41) \\ x_{RE} &= -\sqrt{1 - T_E}x_{in} + \sqrt{T_E}x_{vac}^{(e1)}. \qquad (42) \end{aligned}$$

Expressions for p_{TE} and p_{RE} are obtained by replacing x by p in Eqs. 41 and 42, respectively. The reflected part of the signal is measured by Eve, resulting in the outputs x_E and p_E given by

$$\begin{aligned} x_E &= \frac{1}{\sqrt{2}}(x_{RE} + x_{vac}^{(e2)}) \\ &= \sqrt{\frac{1 - T_E}{2}}(-x_A - x_{vac}^{(a)} + \frac{\sqrt{T_E}x_{vac}^{(e1)} + x_{vac}^{(e2)}}{\sqrt{1 - T_E}}), \qquad (43) \\ p_E &= \frac{1}{\sqrt{2}}(-p_{RE} + p_{vac}^{(e2)}) \\ &= \sqrt{\frac{1 - T_E}{2}}(p_A + p_{vac}^{(a)} - \frac{\sqrt{T_E}p_{vac}^{(e1)} - p_{vac}^{(e2)}}{\sqrt{1 - T_E}}). \qquad (44) \end{aligned}$$

Similarly to Eq. 38, a CSNR representing the Alice to Eve channel is given by

$$CSNR_{AE} = CSNR_{AE(x \text{ or } p)} = \frac{(1 - T_E)V_A}{2}. \qquad (45)$$

As shown in Fig. 6, the remaining part of the feedforward attack consists of applying a gain g_E to x_E and p_E, then

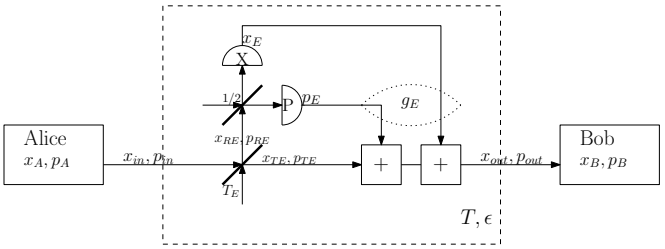


Fig. 6. Feedforward attack. Eve captures a fraction $1-T_E$ of the input signal, then she measures both quadratures of this fraction. Measurement results are used to translate the transmitted fraction T_E of the input.

using this result to translate x_{TE} and p_{TE}. Finally, Bob's input quadratures are given by

$$\begin{aligned} x_{out} &= -g_E x_E + x_{TE}, \qquad (46) \\ p_{out} &= g_E p_E + p_{TE}. \qquad (47) \end{aligned}$$

If g_E and T_E are chosen according to Eqs. 39 and 40, respectively, then Eqs. 46 and 47 reproduce the same statistics of the original physical channel.

IV. Mappings in CVQKD

Our idea consists of using the nonlinear mappings like the ones described in Sect. II to prepare the coherent states that are sent by Alice in a Gaussian modulated CVQKD protocol. More specifically, the displacement values x_A and p_A are now chosen as points in a parametric curve. There is a one to one correspondence between points in these curves and random parameters m, which represent the information exchanged in our protocol. If the selected maps fit the channel noise, we can improve the SDR of the Alice to Bob channel, thus making reconciliation easier.

Our protocol is illustrated in Fig. 7 and it is generically described by the following steps:

1) Alice draws a random number m from a Gaussian distribution $\mathcal{N}(0, \sigma_m^2)$, then uses this value to get a mapped point $\mathbf{s}(m) = [s_1(m)\ s_2(m)\ \cdots\ s_N(m)]$ in a selected curve in $\mathbb{R}^N$ $(N = 2k)$;
2) Alice prepares k coherent states $|x_{A(1)} + ip_{A(1)}\rangle, \cdots, |x_{A(k)} + ip_{A(k)}\rangle$, where $s_1(m) = x_{A(1)}$,$s_2(m) = p_{A(1)}$,$\cdots$,$s_{N-1}(m) = x_{A(k)}$,$s_N(m) = p_{A(k)}$, then sends them to Bob;
3) Bob measures both quadratures x e p of the received states, then uses the results and the selected curve to obtain an estimate $\hat{m}$;
4) A secret key is extracted from m and $\hat{m}$ after information reconciliation and privacy amplification.

The SK maps discussed in Sect. II are designed for AWGN channels. In order to convert quadrature channels onto AWGN channels, we must scale Eqs. 36 and 37 as

$$\begin{aligned} x'_B &= \sqrt{\frac{2}{T}}x_B = x_A + n_x, \qquad (48) \\ p'_B &= -\sqrt{\frac{2}{T}}p_B = p_A + n_p, \qquad (49) \end{aligned}$$

where n_x and n_p are Gaussian variables of zero mean and variance $(2/T+\epsilon)N_0$. We assume that Eve knows the mapping

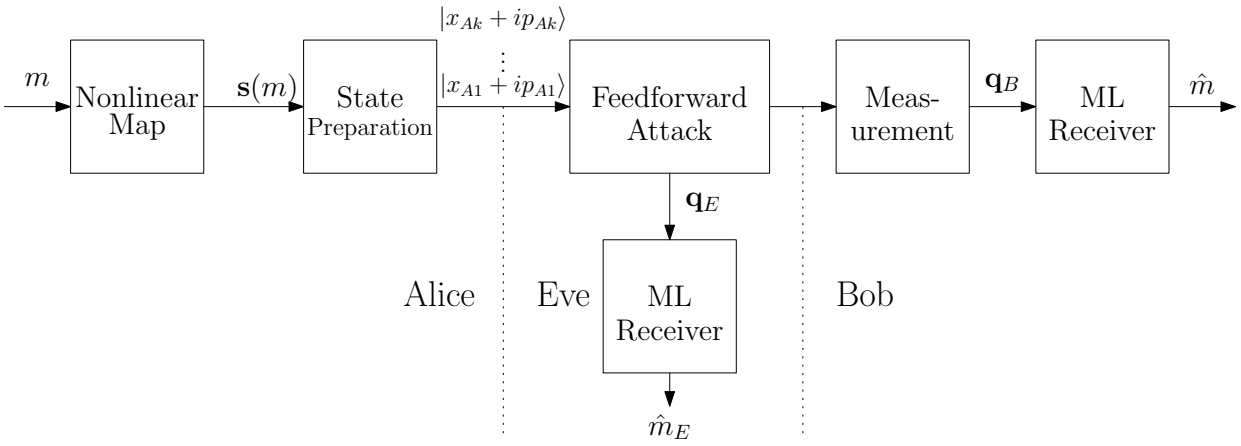


Fig. 7. Block diagram of our protocol. A mapped point of a curve is used for state preparation. Bob and Eve get each an estimate of the parameter sent by Alice through the use of a ML receiver.

that is being used by Alice and Bob, so she can use it to get her own estimate $\hat{m}_E$. As it was done for Alice and Bob, the AWGN channel for Alice and Eve is obtained by scaling x_E and p_E (Eqs. 43 and 44) by $\mp\sqrt{2/(1-T_E)}$.

A. Archimedes' spiral

For the Archimedes' spiral, each parameter m is mapped onto two points according to Eq. 10. This pair of points is used to prepare the coherent state $|x_{A(1)} + ip_{A(1)}\rangle$ that is sent to Bob. In order to have curves of finite length, we restrict the support of the source to the interval $[-1, 1]$. We assume that our information source is Gaussian with zero mean and variance $\sigma_m^2 = (0.25)^2$. By making this choice, truncation effects may be neglected. The variance of quadratures x and p is controlled by adjusting the gain g_S (Eq. 11). We set the average channel power P to $V_A N_0$. This choice results in an average CSNR per quadrature equals to Eq. 38, thus allowing to compare our protocol to the NS protocol.

We design a spiral for each transmission value T, that means calculating a Δ_{opt} (Eq. 12) for each T. The CSNR used in these calculations is given by

$$\text{CSNR}_{des} = \frac{P}{\langle n_x^2\rangle + \langle n_p^2\rangle} = 0.5\frac{V_A T}{2 + T\epsilon}. \tag{50}$$

B. Geodesics on a flat torus

Our simulations regarding curves on a flat torus were carried out for $N = \{4, 6\}$. That means that a point in a curve is used to prepare two or three coherent states. As before, our source has support restricted to the interval $[-1, 1]$ and is Gaussian with zero mean and variance $\sigma_m^2 = (0.25)^2$. Before mapping the source symbols, it is necessary passing them through a compander (Eq. 8). For the sake of comparison to other protocols, we scale the vectors generated according to Eq. 13 by $\sqrt{P}$, where P is the average input channel power. If we set $P = NV_A N_0$, the average CSNR per quadrature equals to Eq. 38. Unlike the spiral mappings that are designed for each value of T, a single curve on a torus is used for all values of T in a simulated range (N fixed). A direct consequence of this choice is that the threshold effect is more pronounced for small values of T.

C. Maximum likelihood decoding

When Bob measures both quadratures of the k coherent states sent by Alice, he ends up with the vector $\mathbf{q}_B = [x_{B(1)}, p_{B(1)}, \cdots, x_{B(k)}, p_{B(k)}]$. Before using the ML receiver, he has to scale the components of $\mathbf{q}_B$ as done in Eqs. 48 and 49, so getting $\mathbf{q}'_B$. For an AWGN channel, the ML receiver chooses $\hat{m}$ as the value of m for which the Euclidean distance between $\mathbf{q}'_B$ and $\mathbf{s}(m)$ is minimum. Analogously, when Eve implements the feedforward attack, she ends up with the vector $\mathbf{q}_E$. After scaling $\mathbf{q}_E$ and getting $\mathbf{q}'_E$, she uses her knowledge about the curve to get her own estimate $\hat{m}_E$.

D. Security analysis

As we consider only individual attacks in this paper, a secret key can be distilled from shared data if the secret key rate given by Eqs. 29 or 30 is positive. In our case, we replace the mutual information bounds for the NS protocol by simulated values for our protocol. More specifically, in order to calculate the secret key rate for our protocol, it is necessary to calculate the mutual information among the variables m, $\hat{m}$ and $\hat{m}_E$. We define the followings mutual information for our protocol: $I_{AB}^{SK} = I(m;\hat{m})$, $I_{AE}^{SK} = I(m;\hat{m}_E)$ and $I_{BE}^{SK} = I(\hat{m};\hat{m}_E)$.

In our setup, we assume that Eve implements the feedforward attack, an optimal individual attack for the NS protocol. The quadratures measured by Eve are processed with a ML receiver, then she gets her own estimate of Alice's parameters. From Alice's data together with Bob's and Eve's estimates, the secret key rates for our protocol under DR and RR are given respectively by

$$\Delta I_{DR}^{SK} = I_{AB}^{SK} - I_{AE}^{SK}, \tag{51}$$

$$\Delta I_{RR}^{SK} = I_{AB}^{SK} - I_{BE}^{SK}. \tag{52}$$

It is worth saying that the feedforward attack with parameters given by Eqs. 39 and 40 may not be optimal for our protocol. This happens because the nonlinear structure of the SK maps makes the distribution of Alice's quadratures non-Gaussian. In this way, further analyses are required in order to treat Eqs. 51 and 52 as optimal bounds for our protocol.

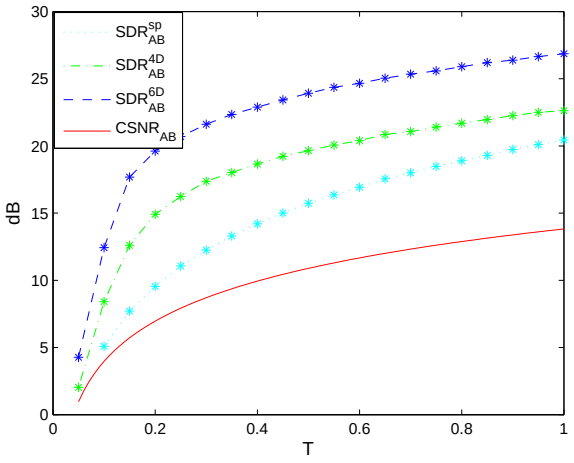


Fig. 8. Simulated values for SDR_{AB} and $CSNR_{AB}$ are plotted against the transmission T . Here, sp stands for spiral while $4D$ and $6D$ stand for the geodesics dimension. It is possible to note the trend of higher gains with higher dimension maps.

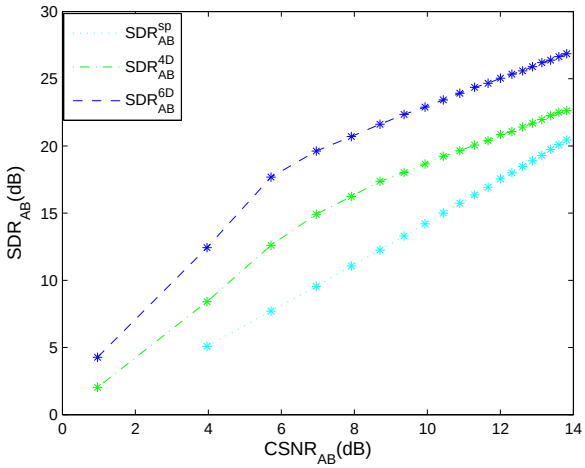


Fig. 9. Simulated values for SDR_{AB} are plotted against $CSNR_{AB}$. Here, sp stands for spiral while $4D$ and $6D$ stand for the geodesics dimension. It is possible to note the trend of higher gains with higher dimension maps.

V. Simulation Results

In order to assess the gains of our protocol, we compare the SDR between Alice's and Bob's variables to the CSNR for the NS protocol (Eq. 38). Thus, we define $SDR_{AB} = \sigma_m^2 / \langle (m - \hat{m})^2 \rangle$, where the denominator represents the distortion between m and $\hat{m}$. From the previously defined I_{AB}^{SK}, I_{AE}^{SK} and I_{BE}^{SK}, we calculate the ratios $\beta_{lim}^{DR}(SK) = I_{AE}^{SK}/I_{AB}^{SK}$ and $\beta_{lim}^{RR}(SK) = I_{BE}^{SK}/I_{AB}^{SK}$ that represent the minimum necessary reconciliation efficiencies for DR and RR, respectively. Similarly, for the NS protocol, we have the ratios $\beta_{lim}^{DR}(NS) = I_{AE}^{NS}/I_{AB}^{NS}$ and $\beta_{lim}^{RR}(NS) = I_{BE}^{NS}/I_{AB}^{NS}$ for DR and RR, respectively. In this case, the ratios are calculated according to bounds given in Sect. III. Mutual information was estimated using Kraskov's first algorithm [37]. This algorithm is based on entropy estimates from p-nearest neighbor distances. In our simulations, we set $p = 5$ for blocks of 10,000 samples. With these choices, we can achieve an estimation error of order 10^{-3} while keeping a reasonable simulation time.

In our simulations, we set $V_A = 50$ and we used $\epsilon = 0.0015V_A$ ([14]) for the excess noise. For the Archimedes' spiral, simulations were done for transmission values $T \in [0.1, 1]$. As previously mentioned, a spiral is designed for each value of T. When dealing with curves on a flat torus, we extended the transmission values to the interval $T \in [0.05, 1]$. If we consider an optical fiber with a 0.2 dB/km attenuation, $T = 0.1$ and $T = 0.05$ correspond to maximum distances $d = 50km$ and $d = 65km$, respectively. For the geodesics on a flat torus, we started from the optimized parameters given in [32] and we made some adjustments in the curves length. When $N = 4$, we have $\theta = \{0.8165, 0.5773, 0.7071, 1.4142\}$ and $L = 7.74$. When $N = 6$, we have $\theta = \{0.69, 0.63, 0.3564, 0.5584, 1.1169, 1.6753\}$ and $L = 10.2$.

In Figs. 8 and 9, we compare the SDR_{AB} for the spiral and the geodesics ($N = 4$ and $N = 6$) to the CSNR for the NS protocol. It is possible to verify the trend of higher gains with higher dimension maps. Besides, geodesics have a more steep graph in low CSNR regions. For $N = 6$, there is a 3.3dB gain in SDR_{AB} compared to $CSNR_{AB}$ for $T = 0.05$. For the same N, when T is doubled, the gain increases to 8.47dB.

In Fig. 10, we plot mutual information for the simulated points. In general, plots exhibit the same tendency of bounds given in Eqs. 21, 22 and 23. For DR, the 3dB point happens around $T = 0.6$. Similarly, for RR, $I_{AB}^{SK} > I_{BE}^{SK}$ in the simulated range. It is worth noting that mutual information values increases with dimension. This is a direct consequence of higher SNR gains for higher dimensions.

In Fig. 11, we plot the ratios $\beta_{lim}^{DR}(SK)$ and $\beta_{lim}^{RR}(SK)$ for our protocol. It is possible to note that SK maps also help Eve to improve her mutual information, thus making necessary the use of more efficient reconciliation protocols for a given T. To compensate this growth in reconciliation efficiency, we could use a lower value for V_A. For $V_A = 50$, geodesics with $N = 6$ requires $\beta_{lim}^{DR}(SK)_{6D} = 98.6\%$ for a $CSNR_{AB} = 0.96dB$ ($T = 0.05$), resulting in a $SDR_{AB} = 4.27dB$. If we have $V_A = 12.5$ for the same $CSNR_{AB} = 0.96dB$ (now $T = 0.20$), we will still have a similar SDR_{AB}, but now with $\beta_{lim}^{DR}(SK)_{6D} = 93.4\%$. This new required efficiency is lower than the ones reported in [14] for this SNR, thus allowing the extraction of a secret key from shared data for our protocol. The cost of lowering V_A in this example was the increase of T. In order to keep low values for T we could use maps of higher dimensions like the geodesics on a flat torus with $N = 8$ or higher.

In Fig. 12, we plot the maximum secret key rates ($\beta = 1$) for our protocol considering the RR scenario. It is possible to note that these simulated curves are below the bound for the NS protocol (Eq. 30). This happens because the mapping also helps Eve to get more information. However, with our protocol, these secret key bits are to be extracted in a higher SNR, which may likely improve the effective secret key rate because it is easier to get a higher β for a higher SNR.

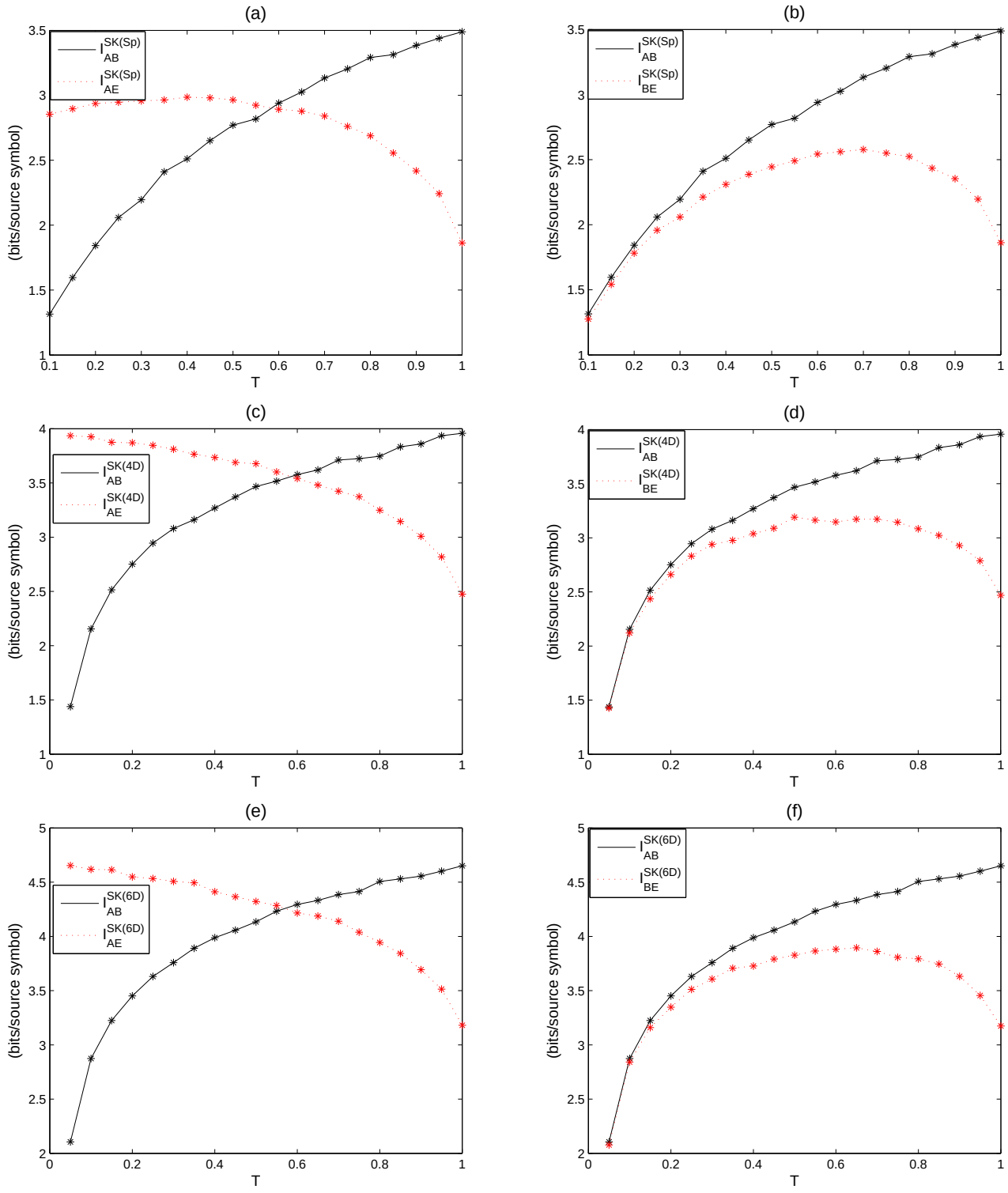


Fig. 10. Simulated mutual information for our protocol. On the left side, it is shown the DR scenario. On the right side, it is shown the RR scenario. (**a**) and (**b**) were obtained for the Archimedes' spiral. (**c**),(**d**) and (**e**),(**f**) were obtained for geodesics on a flat torus with $N = 4$ and $N = 6$, respectively.

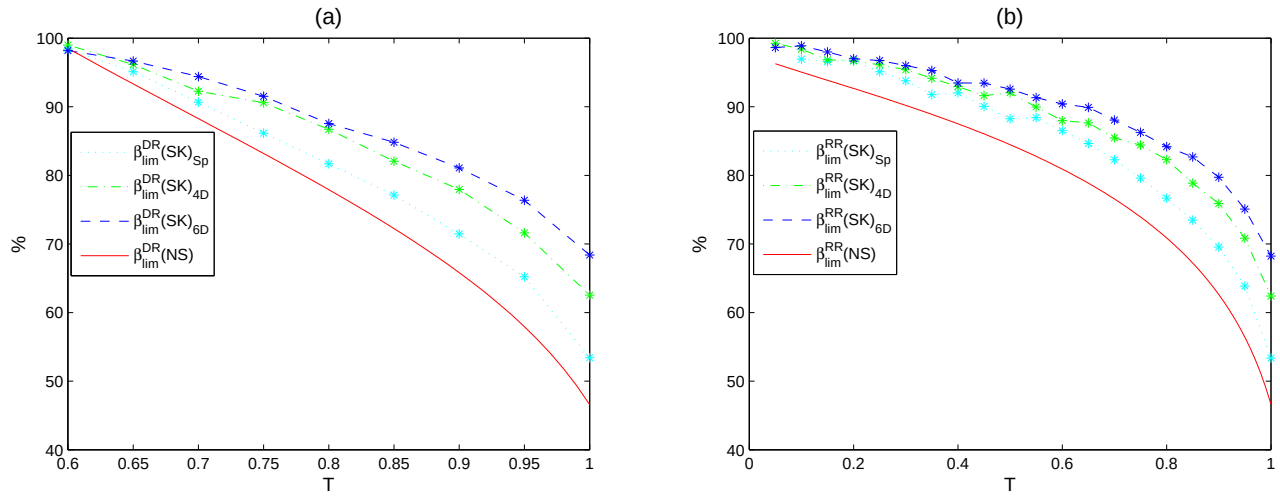


Fig. 11. Minimum necessary reconciliation efficiencies are displayed for DR (**a**) and RR (**b**). Simulated values are compared to the NS protocol (solid red lines). It is possible to note that our protocol requires more efficient reconciliation protocols for a given T. This effect becomes more evident for higher CSNRs.

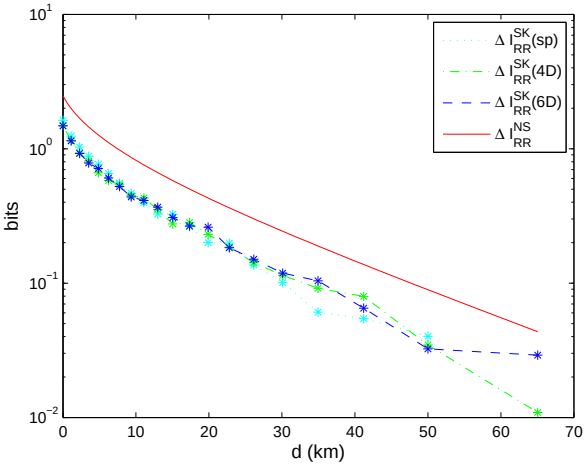


Fig. 12. Simulated values for the secret key rate (RR) are compared to the bound given by Eq. 30 for the NS protocol. Here, *sp* stands for spiral while $4D$ and $6D$ stand for the geodesics dimension. Distances were calculated considering an optical fiber of 0.2 dB/km attenuation.

VI. Conclusion

In this paper, we proposed a CVQKD protocol that uses nonlinear SK maps for the preparation of quantum coherent states. Our idea was to increase the SDR between Alice and Bob by exploiting the error correcting properties of these maps. We assessed the security of our protocol for the feedforward attack optimized for the NS protocol. Simulations have shown that our construction really increases the SDR between Alice and Bob and allows the extraction of a secret key from shared data. The downside of our method is that it also helps Eve to get more information. This fact is inferred from the increase in the minimum necessary reconciliation efficiency when compared to the NS protocol. As suggested in Sect. V, we could lower the required reconciliation efficiency by lowering Alice's variance combined with maps of higher dimension, keeping the geodesics structure.

Some possibilities are envisaged in order to improve our results. One of these would be to include in the design criteria of maps some restriction to confuse Eve. This could prevent Eve of getting the benefits given by maps. The other one would be to conceive a protocol that requires only one quadrature to be measured. This would allow us to get rid of the 3dB penalty of measuring both quadratures.

Acknowledgment

The authors would like to thank Post-Graduate Program in Electrical Engineering (PPgEE-COPELE-UFCG), CAPES, FINEP (QUANTA-RENASIC project) and UNIVASF for their financial support.

References

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, pp. 145–195, Mar 2002. doi: 10.1103/RevModPhys.74.145

[2] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information," *Rev. Mod. Phys.*, vol. 84, pp. 621–669, May 2012. doi: 10.1103/RevModPhys.84.621

[3] S. L. Braunstein and P. van Loock, "Quantum information with continuous variables," *Rev. Mod. Phys.*, vol. 77, pp. 513–577, Jun 2005. doi: 10.1103/RevModPhys.77.513

[4] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Phys. Rev. Lett.*, vol. 88, p. 057902, Jan 2002. doi: 10.1103/PhysRevLett.88.057902

[5] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using gaussian-modulated coherent states," *Nature*, vol. 421, pp. 238–241, Jan. 2003. doi: 10.1038/nature01289

[6] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, "Quantum cryptography without switching," *Phys. Rev. Lett.*, vol. 93, p. 170504, Oct 2004. doi: 10.1103/PhysRevLett.93.170504

[7] ——, "Coherent-state quantum key distribution without random basis switching," *Phys. Rev. A*, vol. 73, p. 022316, Feb 2006. doi: 10.1103/PhysRevA.73.022316

[8] R. Renner and J. I. Cirac, "de finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography," *Physical Review Letters*, vol. 102, p. 110504, Mar 2009. doi: 10.1103/PhysRevLett.102.110504

[9] M. Bloch, A. Thangaraj, S. McLaughlin, and J.-M. Merolla, "Ldpc-based gaussian key reconciliation," in *Information Theory Workshop, 2006. ITW '06 Punta del Este. IEEE*, March 2006. doi: 10.1109/ITW.2006.1633793 pp. 116–120.

[10] G. Van Assche, J. Cardinal, and N. J. Cerf, "Reconciliation of a quantum-distributed gaussian key," *Information Theory, IEEE Transactions on*, vol. 50, no. 2, pp. 394–400, Feb 2004. doi: 10.1109/TIT.2003.822618

[11] Y.-B. Zhao, Y.-Z. Gui, J.-J. Chen, Z.-F. Han, and G.-C. Guo, "Computational complexity of continuous variable quantum key distribution," *Information Theory, IEEE Transactions on*, vol. 54, no. 6, pp. 2803–2807, June 2008. doi: 10.1109/TIT.2008.921889

[12] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, "Quantum key distribution over 25 km with an all-fiber continuous-variable system," *Phys. Rev. A*, vol. 76, p. 042305, Oct 2007. doi: 10.1103/PhysRevA.76.042305

[13] Z. Bai, X. Wang, S. Yang, and Y. Li, "High-efficiency gaussian key reconciliation in continuous variable quantum key distribution," *Science China Physics, Mechanics & Astronomy*, vol. 59, no. 1, pp. 1–5, 2016. doi: 10.1007/s11433-015-5702-7

[14] P. Jouguet, D. Elkouss, and S. Kunz-Jacques, "High-bit-rate continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 90, p. 042329, Oct 2014. doi: 10.1103/PhysRevA.90.042329

[15] A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, "Multidimensional reconciliation for a continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 77, p. 042325, Apr 2008. doi: 10.1103/PhysRevA.77.042325

[16] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, "Long-distance continuous-variable quantum key distribution with a gaussian modulation," *Phys. Rev. A*, vol. 84, p. 062317, Dec 2011. doi: 10.1103/PhysRevA.84.062317

[17] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution," *Nat Photon*, vol. 7, no. 5, pp. 378–381, May 2013.

[18] T. C. Ralph and A. P. Lund, "Nondeterministic noiseless linear amplification of quantum systems," *AIP Conference Proceedings*, vol. 1110, no. 1, pp. 155–160, 2009. doi: http://dx.doi.org/10.1063/1.3131295

[19] R. Blandino, A. Leverrier, M. Barbieri, J. Etesse, P. Grangier, and R. Tualle-Brouri, "Improving the maximum transmission distance of continuous-variable quantum key distribution using a noiseless amplifier," *Phys. Rev. A*, vol. 86, p. 012327, Jul 2012. doi: 10.1103/PhysRevA.86.012327

[20] Y. Zhang, S. Yu, and H. Guo, "Application of practical noiseless linear amplifier in no-switching continuous-variable quantum cryptography," *Quantum Information Processing*, vol. 14, no. 11, pp. 4339–4349, 2015. doi: 10.1007/s11128-015-1095-9

[21] J. Fiurášek and N. J. Cerf, "Gaussian postselection and virtual noiseless amplification in continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 86, p. 060302, Dec 2012. doi: 10.1103/PhysRevA.86.060302

[22] N. Walk, T. C. Ralph, T. Symul, and P. K. Lam, "Security of continuous-variable quantum cryptography with gaussian postselection," *Phys. Rev. A*, vol. 87, p. 020303, Feb 2013. doi: 10.1103/PhysRevA.87.020303

[23] J. M. Wozencraft and I. M. Jacobs, *Principles of Communication Engineering*. John Wiley and Sons, Inc., 1965.

[24] D. J. Sakrison, *Communication Theory: Transmission of Waveforms and Digital Information*. John Wiley and Sons, Inc., 1968.

[25] E. J. Nascimento and F. M. de Assis, "Improving continuous-variable quantum key distribution with shannon-kotel'nikov maps," in *2016 IEEE Globecom Workshops (GC Wkshps)*, Dec 2016. doi: 10.1109/GLOCOMW.2016.7848931 pp. 1–6. [Online]. Available: http://dx.doi.org/10.1109/GLOCOMW.2016.7848931

[26] E. Hodgson, G. Brante, R. D. Souza, and J. L. Rebelatto, "On the physical layer security of analog joint source channel coding schemes," in *2015 IEEE 16th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, June 2015. doi: 10.1109/SPAWC.2015.7227105. ISSN 1948-3244 pp. 585–589.

[27] F. Hekland, P. A. Floor, and T. A. Ramstad, "Shannon-kotel-nikov mappings in joint source-channel coding," *IEEE Transactions on Communications*, vol. 57, no. 1, pp. 94–105, January 2009. doi: 10.1109/TCOMM.2009.0901.070075

[28] J. Ziv, "The behavior of analog communication systems," *IEEE Transactions on Information Theory*, vol. 16, no. 5, pp. 587–594, Sep 1970. doi: 10.1109/TIT.1970.1054509

[29] T. Goblick, "Theoretical limitations on the transmission of data from analog sources," *IEEE Transactions on Information Theory*, vol. 11, no. 4, pp. 558–567, Oct 1965. doi: 10.1109/TIT.1965.1053821

[30] S. I. R. Costa, "On closed twisted curves," *Proceedings of the American Mathematical Society*, vol. 109, no. 1, pp. 205–214, May 1990. doi: 10.1090/S0002-9939-1990-0993746-1

[31] V. A. Vaishampayan and S. I. R. Costa, "Curves on a sphere, shift-map dynamics, and error control for continuous alphabet sources," *IEEE Transactions on Information Theory*, vol. 49, no. 7, pp. 1658–1672, July 2003. doi: 10.1109/TIT.2003.813561

[32] R. M. Taylor, L. Mili, and A. Zaghloul, "Packing tubes on tori: An efficient method for low snr analog error correction," in *Information Theory Workshop (ITW), 2013 IEEE*, Sept 2013. doi: 10.1109/ITW.2013.6691263 pp. 1–5.

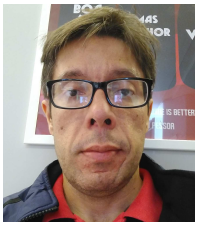
[33] O. Gonzalez and J. H. Maddocks, "Global curvature, thickness, and the ideal shapes of knots," *Proceedings of the National Academy of Sciences*, vol. 96, no. 9, pp. 4769–4773, 1999. doi: 10.1073/pnas.96.9.4769

[34] J. Sudjana, L. Magnin, R. García-Patrón, and N. J. Cerf, "Tight bounds on the eavesdropping of a continuous-variable quantum cryptographic protocol with no basis switching," *Phys. Rev. A*, vol. 76, p. 052301, Nov 2007. doi: 10.1103/PhysRevA.76.052301

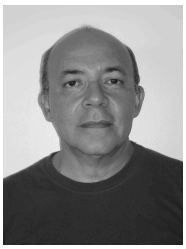
[35] J. Lodewyck and P. Grangier, "Tight bound on the coherent-state quantum key distribution with heterodyne detection," *Phys. Rev. A*, vol. 76, p. 022332, Aug 2007. doi: 10.1103/PhysRevA.76.022332

[36] U. Leonhardt, *Essential Quantum Optics: From Quantum Measurements to Black Holes*. Cambridge University Press, 2010.

[37] A. Kraskov, H. Stögbauer, and P. Grassberger, "Estimating mutual information," *Phys. Rev. E*, vol. 69, p. 066138, Jun 2004. doi: 10.1103/PhysRevE.69.066138



Edmar José do Nascimento was born in Santa Cruz do Capibaribe, Pernambuco, Brazil, in 1978. He received the bachelor's degree in 2002, the master's degree in 2004 and the doctorate's degree in 2017, all in electrical engineering from the Federal University of Campina Grande, Paraíba, Brazil. Since 2009, he has been with the Department of Electrical Engineering at the Federal University of Vale do São Francisco (Univasf), where he is currently an adjunct professor. His research interests include digital communications, information theory, quantum communications, cryptography and error correcting coding.



Francisco Marcos de Assis was born in João Pessoa, Paraíba, Brazil, in 1954. He received the B.Sc. and M.Sc. degrees in electrical engineering from the Military Institute of Engineering, Rio de Janeiro, Brazil, in 1984 and 1992, respectively, and the Ph.D. degree in electrical engineering from Pontifical Catholic University of Rio de Janeiro, Rio de Janeiro, in 1994. He is currently a Professor with the Federal University of Campina Grande, Paraíba, Brazil. His research interests include coding and information theory.