Squeezed Vacuum State Approximation of Discrete Unidimensional Coherent State Constellations

Micael Andrade Dias and Francisco Marcos de Assis

***Abstract*— Recent research on QKD Protocols has focused on discrete modulation schemes for continuous-variable systems, which is a new paradigm in therms of security proof methodologies. Common security proof methodology consists on establishing an equivalent entangled based protocol, which requires the discrete modulated states purification. Here we show how one could approximate the constellation ensemble by a (pure) squeezed vacuum state. We use the quantum fidelity distance measure to calculate the squeezing factor and show that low quadrature modulation variance enables high fidelity between the ensemble and the approximated state.**

***Keywords*— Quantum Fidelity, Squeezed States, DM-CV-QKD.**

I. Introduction

Quantum Key Distribution (QKD) is the first practical application of Quantum Information Theory, one of the most revolutionary research fields of last century [1], aiming to allow two legitimate parties (Alice and Bob) to distribute (or to generate) random and secret cryptographic keys against the efforts of an eavesdropper (Eve) with unlimited computational power. The security of such protocols relies on the very nature of the manipulated quantum systems, whose impossibility of being cloned (no-cloning theorem [2], [3]) and the inherent uncertainty over two non-commuting observables (Heisemberg's uncertainty principle[4], [5]) gives an unconditional security possibility [6], [7], [8], [9].

Since the first proposed QKD protocol, BB84 [10], the field went through different implementations focusing on several aspects as the quantum systems that would be used (discrete or continuous variable systems), quantum detection (single photon detection, homodyne or heterodyne) and the post processing procedures (authentication, information reconciliation and security amplification), as discussed in [11], [12], [13]. Now, recent research on QKD Protocols has focused on discrete modulation schemes for continuous-variable systems, which is a new paradigm in therms of security proof methodologies and aims to simultaneously aggregate the Continuous Variable protocols (CV-QKD) capability of being compatible with common coherent optical communication devices and the Discrete Variable protocols (DV-QKD) easier post-processing procedures implementation.

A prepare and measure protocol (PMP) works as follows. Alice is able to prepare on her laboratory any quantum state from the set $\mathcal{S} = \{|\psi_i\rangle\}_{i=0}^{N-1}$, each one independently and according to a probability distribution that assigns a preparation probability p_i to each state on $\mathcal{S}$. Than, she picks a state $|\psi_i\rangle$, sends it to Bob through a quantum channel, who is going to perform a measurement in order to detect which state was sent, and the process is repeated L times. From Bob's perspective, does not knowing (*a priori*) which state Alice prepared, it is said that he "sees" the classical mixture $\rho = \sum_i p_i \rho_i$, where $\rho_i = |\psi_i\rangle\langle\psi_i|$ is the density operator corresponding to the state $|\psi_i\rangle$. The protocol is then a CV-QKD when the $\mathcal{S}$ is formed by states on continuous variables systems and is discrete modulated when it is finite (also called a constellation). Finally, with above description, a QKD protocol can use discrete secret key values and the shared data can be corrected with classical error correction codes even with a continuous variable state as carrier.

Here is where the security proof problem lies. Shortly, in an asymptotic scenario, that is, in the limit of $L \to \infty$, security is established when the bound on the accessible information to the eavesdropper is no greater than the mutual information shared between the legitimate parties. The task is then, for a given protocol, to find on which conditions (channel parameters, modulation variance, signal to noise ratio level) the protocol remains secure. A common methodology for proving the security is to find an Entangled Base Protocol (EBP) that is equivalent[1] to the PMP, for which the accessible information to the eavesdropper can be bounded from the bipartite state statistical moments.

On DM-CV-QKD protocols, the EBP is obtained through the purification of $\mathcal{S}$. Some protocols have been proposed, with no more than a few quantum states composing the constellation: protocols with two states [14], [15], three states [16], four states [9], [15], [17], [18], [19] and eight states [20], [19][2]. The constellation purification becomes difficult as the size of $\mathcal{S}$ increases, as it requires a diagonal representation in order proceed to purification. For the cases where $\mathcal{S}$ mimics a m-PSK (Phase Shift Key) modulation, the purification is obtained as the the constellation is diagonalized by linear superposition of the coherent states composing it, which approximates a squeezed vacuum or a number state in the continuity limit [21], [22], [23]. Turns out that none of the aforementioned DM-CV-QKD protocols is defined with more than two states distributed along a straight line, that is, a unidimentional protocol (UD-CV-QKD) [24], and it happens probably because there is no

Micael Andrade Dias and Francisco Marcos de Assis, Center of Electrical Engineering and Informatics, Federal University of Campina Grande (UFCG), Campina Grande-PB, Brazil. E-mails: micael.souza@ee.ufcg.edu.br, fmarcos@dee.ufcg.edu.br. This work was partially supported by CAPES.

[1]On the EBP Alice possesses a bipartite entangled state for which she measures the first mode an sends the second one to Bob. The EBP and PMP are equivalent when, outside Alice laboratory, it is impossible to say which one was performed.

[2]We stress that the protocol presented in [19] does not uses amplitude shifted coherent states (unidimensional constellation) but instead applies homodyne measurements to a PSK-like constellation.

diagonal representation for such kind of constellation.

In this paper we show how an ensemble of coherent states distributed one-dimensionaly along one quadrature axis can be approximated by a pure squeezed vacuum state, which has a well definite diagonal form. It will be shown that, as the classical mixture maintains fixed uncertainty on one quadrature and increasing uncertainty on its conjugate, vacuum squeezed states may be statistically close on the second moment, as a function of the squeezing parameter. The closeness between the classical mixture of quantum states and the squeezed state will be measured by quantum fidelity, through its statistical moments.

The paper is structured as follows. We briefly review some topics of quantum optics and quantum distance measures in Section II, and in Section III the discrete unidimentional CV-QKD protocol is presented, formalizing the statistical structure of its state constellations. In Section IV we show how the constellations can be approximated by a vacuum squeezed state using the quantum fidelity. Section V we present the conclusions and future work.

II. Principles on Quantum Optics and Quantum Information

A. Continuous-Variable Systems

A system whose state space is an *infinite dimensional* Hilbert space is called a continuous-variable (or bosonic[3]) quantum system and has as prototype N quantum harmonic oscillators corresponding to N quantized field modes of the electromagnetic wave [13]. This correspondence is due to an equivalence between the canonical momentum and position operators of the quantum harmonic oscillator and the electric and magnetic field operators for the quantized electromagnetic wave [25].

Essentially, each system mode is represented by an infinite dimensional Hilbert Space $\mathcal{H}$ and all modes are associated by the spaces tensor product $\mathcal{H}^{\otimes N} = \otimes_{i=1}^{N}\mathcal{H}_i$, which represents the entire system, and have associated the corresponding N pair of bosonic field operators $\{\hat{a}_1, \hat{a}_1^\dagger\}_{i=1}^N$, also known as annihilation and creation operators, aranged in a vectorial fashion as $\hat{\boldsymbol{b}} = (\hat{a}_1, \hat{a}_1^\dagger, \cdots, \hat{a}_N, \hat{a}_N^\dagger)^T$, which must satisfy the bosonic commutation relation

$$\left[\hat{b_i}, \hat{b_j}\right] = \Omega_{ij} \quad i,j = 1, \cdots 2N, \tag{1}$$

and Ω_{ij} is a generic element of the sympletic form matrix

$$\boldsymbol{\Omega} = \bigoplus_{k=1}^{N} \omega = \begin{pmatrix} \omega & & \\ & \ddots & \\ & & \omega \end{pmatrix}, \quad \omega = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{2}$$

As each mode is spanned by an infinite countable orthonormal basis $\{|n\rangle\}_{i=1}^N$, called Fock (or number-state) basis, the continuous-variable systems are also separable. The number-states are particularly associated with the number operator $\hat{n} := \hat{a}^\dagger\hat{a}$ as they are its eigenstates, $\hat{n}\,|n\rangle = n\,|n\rangle$ and, consequently, related to the bosonic operators as

$$\hat{a}\,|n\rangle = \sqrt{n}\,|n-1\rangle\,, \quad (n \geq 1), \quad \hat{a}\,|0\rangle = 0, \tag{3}$$

$$\hat{a}^\dagger\,|n\rangle = \sqrt{n+1}\,|n+1\rangle\,, \quad (n \geq 0), \tag{4}$$

being $|0\rangle$ the vacuum state, with no photons.

Although bosonic operators completely describe the quantum system, they are not hermitian operators ($\hat{a} \neq \hat{a}^\dagger$)) resulting that they aren't system observables. Nevertheless, one is able to obtain hermitian operators derived from the cartesian decomposition of bosonic ones which also describes the quantum system and are known as the quadrature field operators

$$\hat{q}_i := \hat{a}_i + \hat{a}_i^\dagger \qquad \hat{p}_i := i(\hat{a}_i^\dagger - \hat{a}_i), \tag{5}$$

which are the direct analogue of momentum and position operators of an ideal quantum harmonic oscillator, resulting on the respective vector form $\hat{\boldsymbol{x}} = (\hat{q}_1, \hat{p}_1, \cdots, \hat{q}_N, \hat{p}_N)^T$.

Quantum states can also be described by its statistical moments. Particularly, statistical moments of continuous spectra quantum systems are quite useful as they provide simple formulas for quantum information and distance measures. For a given quantum state $\hat{\rho}$, the first moment is called the displacement vector and it is simply the mean value of the vector arranged quadrature operators $\hat{q}$ and $\hat{p}$,

$$\bar{\boldsymbol{x}} := \langle\hat{\boldsymbol{x}}\rangle = \mathrm{tr}(\hat{\boldsymbol{x}}\hat{\rho}); \tag{6}$$

and the second moment is the covariance matrix $\boldsymbol{V}$, with arbitrary element

$$\boldsymbol{V}_{ij} = \frac{1}{2}\left\langle\{\Delta\hat{x}_i, \Delta\hat{x}_j\}\right\rangle, \tag{7}$$

being $\Delta\hat{x}_i = \hat{x}_i - \langle\hat{x}_i\rangle$ and $\{,\}$ the anticomutator.

Some quantum operators are well described as an exponential function of canonical operator. Two of then are quite important for continuous-variable systems describing two fundamental quantum states on quantum optics, the coherent and squeezed states, part of the large class of Gaussian quantum states.

1) The displacement operator and Coherent States: The displacement operator is a quadratic Hamiltonian, defined as

$$\hat{D}(\alpha) = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}, \tag{8}$$

where $\alpha = q + ip$, which acts as a displacement in the phase space picture. This is a fundamental operator on quantum optics, especially when dealing with phase-space methods and quasiprobability distributions, but it isn't in the scope of this work.

Coherent states can be defined in three different ways: the right eigenstates of the annihilation operator $\hat{a}$, the states with equal and minimum quadrature uncertainty product and the displaced vacuum state [26]. For what is worth, all three descriptions are equivalent but we outline the last one, where the coherent state is obtained by the action of the displacement operator on a vacuum state,

[3]Bosons are particles who behaves statistically according to the Bose-Einstein distribuction. One common example of these particles are photons.

$$|\alpha\rangle = \hat{D}(\alpha)\,|0\rangle = e^{-\frac{|\alpha^2|}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}}\,|n\rangle\,, \tag{9}$$

from which the fist and second descriptions can be verified. It is worth remarking that the displaced vacuum state has poissonian photon distribution, first statistical moment $\bar{\boldsymbol{x}}_\alpha = (q,p)^T$, its minimum quadrature uncertainty product means that it reaches the limit on Heisenberg uncertainty principle and its uncertainty equality on both quadratures results on its covariance matrix to be the identity matrix.

2) Squeezing Operator and the Squeezed Vacuum State: The non-linear crystal effect of emitting an even number of photons when a pumped by a bright laser is modeled by the one-mode squeezing operator [13]

$$\hat{S}(\xi) := e^{(\xi^*\hat{a}^2 - \xi\hat{a}^{\dagger 2})/2}, \tag{10}$$

with $\xi = re^{i\phi}$, $r < \infty$ and $0 \leq \phi < 2\pi$. Clearly, the quadratic canonical operators are required by the $2n$ photon numbers. The application of $S(\xi)$ on the vacuum state produces the one mode squeezed vacuum state (SVS)

$$\begin{aligned} |\xi\rangle &= \hat{S}(\xi)\,|0\rangle \\ &= \frac{1}{\sqrt{\cosh r}} \sum_{n=0}^{\infty} \frac{\sqrt{(2n)!}}{2^n n!} \big(-e^{i\phi}\tanh r\big)^n\,|2n\rangle\,. \end{aligned} \tag{11}$$

This quantum state presents certain peculiarities. One is that they are also minimum uncertainty product states and thus reaches equality on Heisenberg uncertainty principle. Differently from coherent states, its quadrature uncertainty aren't equal. So, while one quadrature uncertainty is squeezed the other is dilated and uncertainty principle is preserved. It can be shown that its firs moment equals $\bar{\boldsymbol{x}}_\xi = (0,0)^T$ and, as r and ϕ parameters controls the squeezinfg effect, the covariance matrix $\boldsymbol{V}$ for a SVS with $\xi = -r$ is

$$\boldsymbol{V}_\xi = \begin{pmatrix} e^{-2r} & 0 \\ 0 & e^{2r} \end{pmatrix}. \tag{12}$$

B. Quantum Fidelity

The fidelity measure informs how close two *information objects* are, either on a classical information theoretical scope with probability distribution functions or with quantum states, in the quantum case. Even the fidelity not being a metric itself, there are some ways to construct metrics from it. Then, the quantum fidelity acts as a *static measure* from which a *dynamic measure* can be built, measuring how much a process preserves information [3]. For two given quantum states $\hat{\rho}$ and $\hat{\sigma}$ the fidelity is given by

$$F(\hat{\rho},\hat{\sigma}) = \mathrm{Tr}\Big\{\sqrt{\hat{\rho}^{1/2}\hat{\sigma}\hat{\rho}^{1/2}}\Big\}. \tag{13}$$

From the definition, some properties come immediately.

1) $0 \leq F(\hat{\rho},\hat{\sigma}) \leq 1$, with the left equality if $\hat{\rho}$ and $\hat{\sigma}$ have orthogonal supports and the right equality is attended if the states commute.
2) If $\hat{\rho}$ is a pure state $|\psi\rangle\langle\psi|$ and $\hat{\sigma}$ is an arbitrary state, the fidelity is the square root of the overlap between $|\psi\rangle$ and $\hat{\sigma}$:
$$F(|\psi\rangle, \hat{\sigma}) = \sqrt{\langle\psi|\hat{\sigma}|\psi\rangle}. \tag{14}$$
3) The fidelity is invariant under unitary transformations.

When dealing with continuous variable systems, $\hat{\rho}$ and $\hat{\sigma}$ will lie on infinite dimensional Hilbert spaces. Fortunately, Gaussian states can be described by its statistical moments and the quantum fidelity can be given as a function of the states fist and second statistical moments:

$$F(\rho,\sigma) = \sqrt{\frac{2}{\sqrt{\Delta+\delta}-\sqrt{\delta}}\exp\Big\{-\frac{1}{2}\boldsymbol{d}^T(\boldsymbol{V}_\rho+\boldsymbol{V}_\sigma)^{-1}\boldsymbol{d}\Big\}}, \tag{15}$$

where $\Delta = \det(\boldsymbol{V}_\rho + \boldsymbol{V}_\sigma)$, $\delta = (\det \boldsymbol{V}_\rho - 1)(\det \boldsymbol{V}_\sigma - 1)$ and $d = \hat{\boldsymbol{x}}_\sigma - \hat{\boldsymbol{x}}_\rho$.

III. Discrete modulated UD-CV-QKD Protocols

Now we turn our attention to the QKD protocol that drives this work. The unidimensional protocol presented in [24] by Usenko and Grosshans happens to be a modification of the most general Gaussian modulated protocol GG02 [27], for which both quadratures are modulated according to independent and identically distributed Gaussian random variables. On Usenko's protocol, only one quadrature is modulated, resulting on a simplified implementation with only an intensity modulator and dispensing the phase modulator. The security proof for this protocol starts from a typical two-mode squeezed vacuum state and, by squeezing the second mode (Bob's mode), the EBP is than obtained.

For a discrete modulated UD-CV-QKD, the coherent state constellation will be analogous to a classical PAM signaling, where the states will be distributed along one quadrature axis (q-quadrature, for now) with K pairs of coherent states $\{|\alpha_i\rangle, |-\alpha_i\rangle\}_{i=1}^K$, as in Figure 1. Each state will be prepared with a probability $Pr[state = |\alpha_i\rangle] = Pr[state = |-\alpha_i\rangle] = p_i/2$, satisfying $\sum_i p_i = 1$, and the amplitudes can be parameterized with $\alpha_0 \in \mathbb{R}$, $\alpha_i = \lambda\alpha_{i-1}$ where λ is a real parameter to be defined. Said that, the constellation ensemble for the discrete modulated protocol is the classical mixture given by

$$\rho_m = \frac{1}{2}\sum_{i=0}^{K-1} p_i(|\alpha_i\rangle\langle\alpha_i| + |-\alpha_i\rangle\langle-\alpha_i|), \tag{16}$$

which must be purified in order to establish security. As mentioned before, there is no intuitive diagonalization procedure for ρ_m that allows for purification but, for the squeezing state approximation, the constellation statistical moments can be computed.

We begin with the expectations

$$\langle\hat{a}\rangle = \langle\hat{a}^\dagger\rangle = \mathrm{tr}(\rho_m\hat{a}) = 0, \tag{17}$$

$$\langle\hat{a}^2\rangle = \langle\hat{a}^{\dagger 2}\rangle = \langle\hat{a}^\dagger\hat{a}\rangle = \mathrm{tr}\big(\rho_m\hat{a}^2\big) = \sum_{i=0}^{K-1} p_i\alpha_i^2, \tag{18}$$

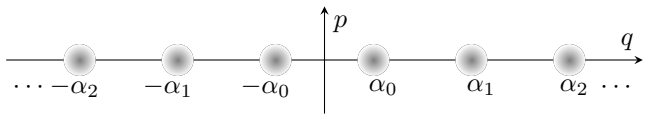

Fig. 1. General constellation for a symmetric unidimensional discrete modulated CVQKD protocol.

and, by Equation (5), one has that $\hat{\boldsymbol{x}} = (\hat{q}, \hat{p})^T$ and the first statistical moment is $\bar{\boldsymbol{x}}_{\rho_m} = (0,0)^T$. For the second moment we note that $\Delta\hat{x}_i = \hat{x}_i$ and the covariance matrix will have the form

$$\boldsymbol{V}_{\rho_m} = \begin{pmatrix} \langle \hat{q}^2 \rangle & \frac{1}{2}\langle \hat{q}\hat{p} + \hat{p}\hat{q} \rangle \\ \frac{1}{2}\langle \hat{p}\hat{q} + \hat{q}\hat{p} \rangle & \langle \hat{p}^2 \rangle \end{pmatrix} = \begin{pmatrix} V_q & 0 \\ 0 & 1 \end{pmatrix}. \quad (19)$$

where we called $\langle \hat{q}^2 \rangle = V_q = 4\sum_{i=0}^{K-1} p_i \alpha_i^2 + 1$ as the quadrature variance. It is worth mentioning that the modulation variance V_m refers to the states amplitudes variance, according to associated probability distribution (which is an inherent parameter to the constellation shape), while the quadrature modulation variance V_q is the quadrature operator $\hat{q}^2$ expectation. We can then relate V_m to V_q as

$$V_m = \sum_{i=0}^{K-1} p_i \alpha_i^2 = \frac{V_q - 1}{4}. \quad (20)$$

IV. Approximation via Squeezed Vacuum States

As mentioned before, constellations shaped like Figure 1 resulting on ensembles according to Equation (16) have no intuitive purification and our aim is to propose an approximation via a squeezed vacuum state. On Section III we developed the covariance matrix $\boldsymbol{V}_{\rho_m}$ expression for the ensemble, which has fixed minimum variance on p-quadrature and V_q increases proportionally to the modulation variance. Our aim is to find how close a SVS, as presented in Section II-A.2, can be to the discrete modulated UD-CV-QKD constellation using the quantum fidelity as a similarity measure, which can be computed using the statistical moments shown in previous sections.

To compute the fidelity from Equation (15), it is clear that $\bar{\boldsymbol{x}}_\xi = \bar{\boldsymbol{x}}_{\rho_m} = (0,0)^T$ and, from the covariance matrices expressions of Equations (12) and (19), $\delta = 0$ as $\det V_\xi = 1$. Then, the quantum fidelity between $\rho_\xi = |\xi\rangle\langle\xi|$ and ρ_m reduces to

$$\begin{aligned} F(\rho_m, \rho_\xi) &= \sqrt{\frac{2}{\sqrt{\Delta}}}, \\ &= \sqrt{\frac{2}{\sqrt{(V_q + e^{-2r})(1 + e^{2r})}}}, \end{aligned} \quad (21)$$

which is plotted in Figure 2 as a function of the constellation modulation variance V_m and the SVS squeezing parameter r.

From Equation (21) and Figure 2 it is clear that the only possibility for the fidelity to reach its maximum value, that is, the states ρ_m and ρ_ξ to be indistinguishable, is when $V_m = 0$ and $r = 0$, which is the fidelity between two vacuum states. Otherwise, the fidelity will be strictly less than one.

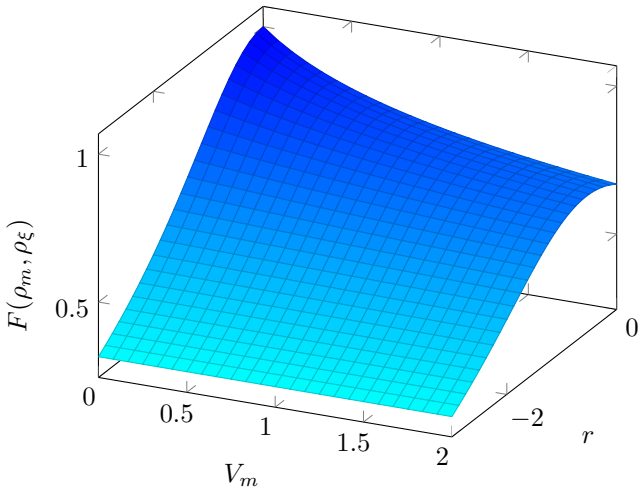

Fig. 2. Fidelity for the constellation ensemble with modulation variance V_m and the squeezed vacuum state with squeezing parameter r.

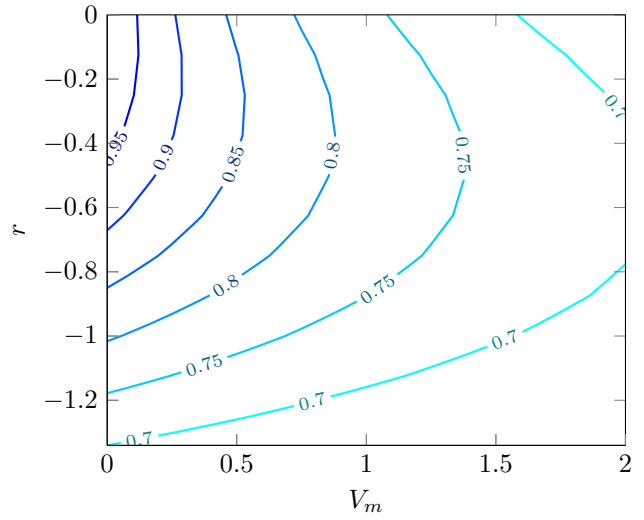

Fig. 3. (color line) Contour line for several fidelity values for the constellation ensemble with modulation variance V_m and the squeezed vacuum state with squeezing parameter r.

Despite the impossibility of an approximation via SVS with maximum fidelity in practical constellations ($V_m > 0$), it is possible to achieve any given fidelity value for certain values of V_m and r grater than zero, as presented in Figure 3 with the contour lines for several fidelity values. It can be seen that the higher the fidelity gets the lower the modulation variance and the squeezing parameter must be.

Of course, the modulation variance can be attained by shaping it geometrically and probabilistically. As an example, consider the ensemble with four states $\mathcal{S}_4 = \{|\alpha_0\rangle, |-\alpha_0\rangle, |\alpha_1\rangle, |-\alpha_1\rangle\}$ prepared equiprobably and with $\alpha_1 = \lambda_1\alpha_0$, and another ensemble $\mathcal{S}'_4 = \{|\alpha_0\rangle, |-\alpha_0\rangle, |\alpha_1\rangle, |-\alpha_1\rangle\}$ prepared with probabilities $\{2/6, 2/6, 1/6, 1/6\}$ and $\alpha_1 = \lambda_2\alpha_0$. Both ensembles will have the same modulation variance if $\lambda_2 = \sqrt{(3\lambda_1^2 - 1)/2}$, where the probabilistic shaping is compensated by the geo-

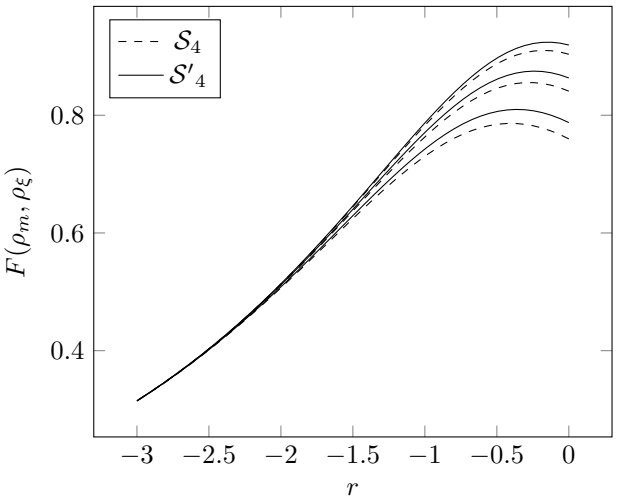

Fig. 4. Fidelity between ρ_ξ and the ensembles $\mathcal{S}_4$ and $\mathcal{S}'_4$ for $V_m = [0.25, 0.5, 1]$ from top to bottom.

metrical shaping. On the other hand, if $\lambda_1 = \lambda_2 = 2$, we have that $V'_m = 4V_m/5$, where V_m is the modulation variance for $\mathcal{S}_4$ and V'_m for $\mathcal{S}'_4$. This means that the same SVS will be closer to $\mathcal{S}'_4$, as it is shown on Figure 4 for several values of V_m.

V. Conclusions

In this work, we presented how a discrete ensemble of coherent states describing a discrete modulated UD-CV-QKD can be approximated by a squeezed vacuum state. As the one-dimensional ensemble has no intuitive diagonalization, which allows for a purification and therefore a security proof, the approximation through a squeezed state is a solution to have an ensemble representation that is already diagonalized and the security proof can be made. We used the quantum fidelity to analyze how good the approximation was and, for low modulation variance, it is possible to find a squeezed vacuum state for which the fidelity is higher then 0.9. Future works may focus on what is the approximation effect on security proofs for discrete modulated UD-CV-QKD protocols.

References

[1] M. M. Wilde, *Quantum Information Theory*, 2nd ed. Cambridge University Press, 2017.

[2] N. J. Cerf, A. Ipe, and X. Rottenberg, "Cloning of Continuous Quantum Variables," *Phys. Rev. Lett.*, vol. 85, no. 8, pp. 1754–1757, 2000.

[3] M. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.

[4] W. Heisenberg, "Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik," *Zeitschrift für Physik*, vol. 43, no. 3-4, pp. 172–198, Mar. 1927.

[5] P. J. Coles, M. Berta, M. Tomamichel, and S. Wehner, "Entropic uncertainty relations and their applications," *Reviews of Modern Physics*, vol. 89, no. 1, 2017.

[6] H.-K. Lo and H. F. Chau, "Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances," *Science*, vol. 283, no. 5410, pp. 2050–2056, Mar. 1999.

[7] P. W. Shor and J. Preskill, "Simple Proof of Security of the {BB}84 Quantum Key Distribution Protocol," *Phys. Rev. Lett.*, vol. 85, no. 2, pp. 441–444, Jul. 2000.

[8] D. Mayers, "Unconditional security in quantum cryptography," *Journal of the {ACM}*, vol. 48, no. 3, pp. 351–406, 2001.

[9] A. Leverrier and P. Grangier, "Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation," *Phys. Rev. Lett.*, vol. 102, no. 18, 2009.

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

[11] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in Quantum Cryptography," *arXiv:1906.01645 [math-ph, physics:physics, physics:quant-ph]*, Jun. 2019.

[12] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *npj Quantum Information*, vol. 2, no. 1, p. 16025, Nov. 2016.

[13] 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, no. 2, pp. 621–669, 2012.

[14] Y. B. Zhao, M. Heid, J. Rigas, and N. Lütkenhaus, "Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks," *Phys. Rev. A*, vol. 79, no. 1, pp. 1–14, 2009.

[15] A. Leverrier and P. Grangier, "Continuous-variable Quantum Key Distribution protocols with a discrete modulation," *ArXiv*, Feb. 2010.

[16] K. Brádler and C. Weedbrook, "Security proof of continuous-variable quantum key distribution using three coherent states," *Phys. Rev. A*, vol. 97, no. 2, pp. 1–16, 2018.

[17] J. Lin, T. Upadhyaya, and N. Lütkenhaus, "Asymptotic Security Analysis of Discrete-Modulated Continuous-Variable Quantum Key Distribution," *Physical Review X*, vol. 9, no. 4, p. 041064, Dec. 2019.

[18] S. Ghorai, P. Grangier, E. Diamanti, and A. Leverrier, "Asymptotic Security of Continuous-Variable Quantum Key Distribution with a Discrete Modulation," *Physical Review X*, vol. 9, no. 2, p. 021059, Jun. 2019.

[19] W. Zhao, R. Shi, Y. Feng, and D. Huang, "Unidimensional continuous-variable quantum key distribution with discrete modulation," *Physics Letters A*, vol. 384, no. 2, p. 126061, Jan. 2020.

[20] I. B. Djordjevic, "Optimized-Eight-State CV-QKD Protocol Outperforming Gaussian Modulation Based Protocols," *IEEE Photonics Journal*, vol. 11, no. 4, pp. 1–10, Aug. 2019.

[21] J. Janszky and A. V. Vinogradov, "Squeezing via one-dimensional distribution of coherent states," *Physical Review Letters*, vol. 64, no. 23, pp. 2771–2774, Jun. 1990.

[22] V. Bužek and P. Knight, "The origin of squeezing in a superposition of coherent states," *Optics Communications*, vol. 81, no. 5, pp. 331–336, Mar. 1991.

[23] V. Bužek, A. Vidiella-Barranco, and P. L. Knight, "Superpositions of coherent states: Squeezing and dissipation," *Physical Review A*, vol. 45, no. 9, pp. 6570–6585, May 1992.

[24] V. C. Usenko and F. Grosshans, "Unidimensional continuous-variable quantum key distribution," *Physical Review A*, vol. 92, no. 6, p. 062337, Dec. 2015.

[25] M. O. Scully and M. S. Zubairy, *Quantum Optics*. Cambridge University Press, 1997.

[26] C. Gerry and P. Knight, *Introductory Quantum Optics*. Cambridge University Press, 2004.

[27] F. Grosshans and P. Grangier, "Continuous Variable Quantum Cryptography Using Coherent States," *Phys. Rev. Lett.*, vol. 88, no. 5, p. 57902, Jan. 2002.