Security of continuous-variable quantum key distribution: towards a de Finetti theorem for rotation symmetry in phase space

Anthony Leverrier, E. Karpov, Philippe Grangier, Nicolas Cerf

Security of continuous-variable quantum key distribution: towards a de Finetti theorem for rotation symmetry in phase space

2009 New J. Phys. 11 115009

(http://iopscience.iop.org/1367-2630/11/11/115009)

New Journal of Physics
The open-access journal for physics

Security of continuous-variable quantum key distribution: towards a de Finetti theorem for rotation symmetry in phase space

A Leverrier[1,5], E Karpov[2], P Grangier[3] and N J Cerf[2,4]

[1] Institut Telecom/Telecom ParisTech, CNRS LTCI, 46, rue Barrault, 75634 Paris Cedex 13, France

[2] Quantum Information and Communication, Ecole Polytechnique, CP 165/59, Université Libre de Bruxelles, 50 avenue F D Roosevelt, B-1050 Brussels, Belgium

[3] Laboratoire Charles Fabry, Institut d'Optique, CNRS, Université Paris-Sud, Campus Polytechnique, RD 128, 91127 Palaiseau Cedex, France

[4] MIT—Research Laboratory of Electronics, Cambridge, MA 02139, USA

E-mail: anthony.leverrier@enst.fr

New Journal of Physics **11** (2009) 115009 (12pp)
Received 2 March 2009
Published 13 November 2009
Online at http://www.njp.org/
doi:10.1088/1367-2630/11/11/115009

Abstract. Proving the unconditional security of quantum key distribution (QKD) is a highly challenging task as one needs to determine the most efficient attack compatible with experimental data. This task is even more demanding for continuous-variable QKD as the Hilbert space where the protocol is described is infinite dimensional. A possible strategy to address this problem is to make an extensive use of the symmetries of the protocol. In this paper, we investigate a rotation symmetry in phase space that is particularly relevant to continuous-variable QKD, and explore the way towards a new quantum de Finetti theorem that would exploit this symmetry and provide a powerful tool to assess the security of continuous-variable protocols. As a first step, a single-party asymptotic version of this quantum de Finetti theorem in phase space is derived.

[5] Author to whom any correspondence should be addressed.

Contents

1. Introduction and motivation

The greatest novelty brought by quantum key distribution (QKD) is that, for the first time, a secret key agreement scheme can be proven unconditionally secure, that is, without making any assumptions about the power of an adversary.

Even if this claim has been made repeatedly since the proposal of the first QKD protocol in 1984 [1], it is only recently that complete proofs of security have been rigorously established. Proving the security of a scheme without making any simplifying assumptions is indeed quite challenging: the legitimate parties, Alice and Bob, need to infer what is the most efficient attack that an eavesdropper, Eve, could perform. This can be achieved by considering all bipartite states, ρ_{AB}, compatible with Alice and Bob's data, but this quickly becomes almost untractable since the dimension of the Hilbert space, $\mathcal{H}^{\otimes n}$, relevant to describe ρ_{AB} grows exponentially with the number, n, of quantum signals exchanged during the protocol. As a consequence, security proofs were often derived while restricting the adversary to the so-called *collective attacks*. In such attacks, the state ρ_{AB} is supposed to be *independent and identically distributed* (i.i.d.), meaning that there exists a state $\sigma_{\mathrm{AB}} \in \mathcal{H}$ such that $\rho_{\mathrm{AB}} = \sigma_{\mathrm{AB}}^{\otimes n}$. As a consequence, the Hilbert space needed to analyze the protocol becomes $\mathcal{H}$ instead of $\mathcal{H}^{\otimes n}$: no need to emphasize that this 'small' assumption considerably simplifies the analysis!

The question then is to know whether such a hypothesis limits the power of the adversary in a non-trivial way, or, said otherwise, whether this leads to an unreasonably optimistic view of the security of QKD. Fortunately, this is not the case as collective attacks were recently proven asymptotically optimal against protocols described with a finite-dimensional Hilbert space [2]. The main tool used to answer this problem was a quantum de Finetti theorem, which means, roughly speaking, that a certain class of states in $\mathcal{H}^{\otimes n}$, namely *symmetric states*, can be well approximated by mixtures of i.i.d. states. From a cryptographic point of view, this means that general *symmetric* attacks are almost the same as collective attacks. The last step to complete the proof is to show that a symmetric attack is optimal for the eavesdropper, or, equivalently, that the state ρ_{AB} can safely be assumed symmetric, which is indeed the case for most QKD protocols.

The quantum de Finetti theorem is thus quite powerful as it allows us to derive the security of a QKD scheme against arbitrary attacks as soon as it is proven. Moreover, the full security is obtained almost for free, in the sense that the decrease of key size caused by allowing the adversary to perform any non-collective attack is negligible, at least in an asymptotic regime. In a finite size scenario, however, the impact on the key size could be significant, although it should be compared with other finite-size effects such as the precision of parameter estimation or the efficiency of error correction [3, 4]. In this context, alternatives to the de Finetti theorem might also be worth investigating as they can lead to improved bounds [5].

Unfortunately, the application of the quantum de Finetti theorem, that was presented in [2], is restricted to QKD schemes that are described in a finite-dimensional Hilbert space. Apart from the fact that describing any protocol in the finite-dimensional Hilbert space is nothing less than an approximation (even though quite a reasonable one for protocols involving qubits), it is clear that it does not apply to protocols genuinely described in infinite-dimensional Hilbert spaces, such as protocols explicitly built on the continuous amplitude components of the light field (see [6] and references therein). The reason for this is that the quantum de Finetti theorem fails as soon as the dimension, d, of the Hilbert space $\mathcal{H}$ is not small compared to the number n of subsystems considered, which is obviously the case if d is infinite. Moreover, not only is the present version of the quantum de Finetti theorem limited to low dimensional Hilbert spaces, but counter-examples have been exhibited that demonstrate that a dimension-independent de Finetti theorem cannot exist [7].

Nevertheless, the impossibility of a general dimension-independent theorem does not rule out the possibility of more restricted versions of the theorem, which may still be highly relevant to prove the security of QKD schemes. In particular, the quantum de Finetti theorem of [2] is concerned with (permutation) symmetric states in $\mathcal{H}^{\otimes n}$, that is, states that are invariant under arbitrary permutations of their n subsystems. The only approach that has been pursued to date, in order to extend the range of application of this theorem to the infinite-dimensional Hilbert spaces, has consisted in restricting the set of states in such a way that a finite-dimension theorem can be applied [8]–[10], [12]. In particular reference [10], the quantum de Finetti theorem of [2] has been applied to infinite-dimensional quantum systems conditioned on certain measurement results. The main consequence is to rigorously justify the assumption of a finite-dimension theorem in the context of QKD protocols using attenuated coherent pulses as the support for qubits. The theorem can then be used to derive the security of some continuous-variable schemes [11], as long as the energy of the signal states is not too important. The main drawback is that some experimental conditions need to be checked, which was not the case for finite-dimensional protocols.

In this paper, we explore a radically different approach, which might greatly simplify the security proofs of continuous-variable QKD. The idea is to derive a new quantum de Finetti theorem corresponding to symmetry classes other than permutations of the subsystems. Our main insight is to describe the protocol in a *phase space* instead of Fock representation, and to study a symmetry group that is specific to the phase space. This choice features several advantages. First, the phase space representation is the natural choice for the analysis of continuous-variable QKD, where the information is typically encoded onto the quadratures of the light field (see [6]). Moreover, if collective attacks are indeed asymptotically optimal, as they generally are for discrete-variable QKD, it would be useful to have an interpretation of this result using covariance matrices. It should be pointed out that when restricted to collective attacks, the security of the protocol is completely characterized by the covariance matrix of the

system shared by Alice and Bob [13, 14]. Last but not least, the phase space representation has the remarkable property to be finite dimensional: by trading a discrete description in the infinite-dimensional Hilbert space (the Fock representation) for a *continuous* description in the finite-dimensional real space.

Interestingly, in a classical setting, versions of the de Finetti theorem that apply to orthogonally invariant continuous probability distributions have been known for a long time [15]. Here, we make the first steps towards the generalization of this theorem to a quantum setting. Obviously, since a general dimension-independent quantum de Finetti theorem is impossible, we cannot hope to establish one by switching between an infinite-dimensional state-space representation and a finite-dimensional phase-space representation. The idea is that the symmetry hypotheses, needed for the phase-space de Finetti theorem, are stronger than the ones used in the previous quantum versions of the de Finetti theorem. We will show that these stronger symmetry hypotheses are, however, perfectly compatible with the continuous-variable QKD protocols.

The outline of the paper is as follows. In section 2, we explicitly make the link between symmetry properties and security proofs. In section 3, we present continuous-variable QKD and introduce a new symmetry for such protocols. This symmetry is then presented in more details in section 4, where we make the preliminary steps towards the derivation of a new quantum de Finetti theorem for continuous variables. Finally, the conclusions are drawn in section 5.

2. Role of symmetry in the security proofs

The goal of this section is to explain how symmetry considerations can simplify the theoretical analysis of quantum cryptography. In particular, we would like to provide a theoretical justification to the common attitude of considering the state ρ_{AB} shared by Alice and Bob as being symmetric. Note that a more mathematical argument can be found in [5].

As we mentioned previously, applying the de Finetti theorem to prove the security of QKD protocols works if one can first assume, without loss of generality, that the state ρ_{AB} is symmetric, that is invariant under any permutation of its n subsystems. Here, we show that this assumption is justified, but that one is actually not limited to considering the action of this particular symmetry group $\mathcal{S}_n$ (one can also consider larger symmetry groups). Basically, the idea is that by assuming any symmetry, Alice and Bob will always underestimate the secret key rate they can extract from their data.

The secret key rate for a particular instance of a QKD protocol is a function of the state ρ_{AB} shared by the legitimate parties, Alice and Bob. The eavesdropper, Eve, is assumed to have the maximal information compatible with ρ_{AB} meaning that her state ρ_{E} is such that $\rho_{\mathrm{E}} = \mathrm{tr}_{\mathrm{AB}}(|\Psi_{\mathrm{ABE}}\rangle)$ where $|\Psi_{\mathrm{ABE}}\rangle$ is any purification of ρ_{AB}. Note that all purifications are equivalent up to an unitary operation applied on system E. More precisely, ρ_{AB} represents the *knowledge* that Alice and Bob have about the quantum state they share. For this reason, ρ_{AB} is subjective and inevitably depends on the assumptions made by Alice and Bob. It must be emphasized that this cannot be avoided by performing a quantum tomography of the state, since the latter is also subject to hypotheses, namely that one has access to an arbitrary large number of independent and identical copies of a single state. The exponential version of the quantum de Finetti theorem as derived in [2] gives a partial answer to this problem: if ρ_{AB} is invariant under permutations of its subsystems, then it can be well approximated by a mixture of i.i.d. states, so quantum tomography is therefore justified.

A crucial observation is that Alice and Bob would like to ignore or forget the properties of ρ_{AB} they are not interested in, typically possible correlations between the n subsystems of their state, hence obtaining $\rho_{AB} = \sigma_{AB}^{\otimes n}$ for some prototype state $\sigma_{AB} \in \mathcal{H}$. Unfortunately, this action of forgetting comes at a price, namely erasing some potentially useful information. The first idea to make the argument more rigorous is that Alice and Bob can actually *enforce* the symmetry they want. Let us, for instance, consider symmetry under permutations of the subsystems of ρ_{AB} which is the symmetry commonly used in various QKD security proofs (with the notable exception of protocols such as the differential phase shift (DPS) [16] or the coherent one-way (COW) [17]). This symmetry can be enforced in the following way: Alice and Bob can perform the same random permutation π over their respective state, with π being chosen uniformly over the symmetric group $\mathcal{S}_n$. This operation transforms ρ_{AB} into

$$\frac{1}{n!}\sum_{\pi\in\mathcal{S}_n} \pi\rho_{AB}\pi^\dagger \otimes |\pi\rangle\langle\pi|_C,$$

where π is the unitary operator implementing the permutation π to both systems A and B, $\{|\pi\rangle\}_\pi$ is an orthogonal family of vectors and C is a classical auxiliary space whose sole purpose is to store the information concerning the permutation π that was applied. Then, tracing over system C (or equivalently giving this system to Eve), Alice and Bob obtain the state $\bar{\rho}_{AB}$, which is symmetric by construction. Obviously, for any practical purpose, applying such a procedure is out of the question as it would at least involve a quantum memory in order to store each subsystem while Alice and Bob wait for the total state ρ_{AB}. One may object, however, that applying such a permutation π to ρ_{AB} is equivalent to merely relabeling the indices of Alice and Bob's data, which is much simpler to implement. The key is that both procedures are indistinguishable, which is a clear consequence of the fact that the permutation of subsystems commutes with the measurement procedure and classical post-processing. This is true for most protocols, such as BB84 or continuous-variable protocols, but not for DPS or COW as explained below. In order for the two procedures to be completely equivalent, Alice and Bob should completely forget which particular permutation was performed. A second crucial point is that, in reality, Alice and Bob do not even need to permute the labels of their data. What is really necessary is that they should never use any information related to the order of their data (the labeling of their data) when they extract the key.

It must be realized that enforcing such a symmetry can only decrease the secret key rate, since Alice and Bob give additional information to Eve, or, equivalently, forget some *a priori* available information. On the other hand, while they are only throwing information that they do not use in practice (the labeling of their data), the impact of this symmetrization step to the key rate is actually negligible. Note that nothing forbids one to use such a technique in the study of the DPS and COW protocols. However, correlations between different subsystems are essential for these protocols to work and no key could be extracted if one was forgetting them. In principle, any symmetrization is applicable to any QKD protocol, but some symmetrization procedures essentially erase all the relevant information and are consequently useless for the study of such protocols. Other symmetries have been investigated in the literature, for instance random bit-flip or phase-flip applied simultaneously by Alice and Bob, and have led to simplifications in the analysis of some protocols [18].

The above reasoning can easily be generalized to other symmetries. Let $\mathcal{G}$ be a symmetry group in $\mathcal{H}^{\otimes n}$. Alice and Bob can perform a random g drawn from $\mathcal{G}$ and later forget about g,

thus transforming ρ_{AB} into

$$\bar{\rho}_{AB}^{\mathcal{G}} = \mathrm{tr}_C \left(\frac{1}{\#\mathcal{G}} \sum_{g \in \mathcal{G}} g \ \rho_{AB} \ g^{\dagger} \otimes |g\rangle\langle g|_C \right),$$

where $\#\mathcal{G}$ is the cardinal of $\mathcal{G}$. The group $\mathcal{G}$ can even be continuous (albeit compact), in which case the discrete sum should simply be replaced by an integral over the Haar distribution of $\mathcal{G}$. This is actually what we will do for continuous-variable protocols.

3. Phase-space symmetry for continuous-variable QKD

3.1. Brief summary of the theoretical analysis of continuous-variable QKD

We rapidly describe continuous-variable protocols, as a more detailed presentation can be found in [6]. Continuous-variable QKD comes with two flavors depending on whether the quantum state shared by Alice and Bob is characterized by a quantum bit error rate (QBER) or by a covariance matrix. In the first category lie protocols where the quadratures of the light field are just the support for encoding bits. Such protocols usually use postselection to improve their QBER [19]. Then, the analysis is somewhat similar to that of discrete-variable protocols. In the second category of protocols, such as [20], with which we are only concerned here, the quantum state shared by Alice and Bob is characterized by its covariance matrix. This means that the continuous-variable approach is used even for the description of the state, and not only as a means to carry information over quantum channels. On the positive side, these protocols, and in particular their security, are easier to study. However, this approach suffers an important drawback, namely that postselection is *a priori* impossible: one must keep all data. This is particularly damaging during the classical post-processing of the protocol where one now has to deal with real random variables instead of binary random variables. The main implication is that the reconciliation step, which roughly corresponds to correcting discrepancies between Alice and Bob's classical data, becomes a task that is much more involved than correcting errors between two binary strings. The error rate may indeed be much higher as the protocols with continuous variables may tolerate very low signal-to-noise ratio. The classical problem of reconciliation was until recently limiting the range of continuous-variable QKD protocols [21]. However, simpler discrete modulation schemes can help dealing with the reconciliation problem [11].

3.2. Rotation symmetries for continuous-variable QKD

One of the nice features of continuous-variable QKD is that the security against collective attacks is entirely characterized by the covariance matrix of ρ_{AB} [13, 14]. As we restrict our analysis to collective attacks, one has $\rho_{AB} = \sigma_{AB}^{\otimes n}$, and the covariance matrix Γ of σ_{AB} is usually assumed to be of the form:

$$\Gamma_{\mathrm{sym}} = \begin{pmatrix} X\mathbb{1}_2 & Z\sigma_z \\ Z\sigma_z & Y\mathbb{1}_2 \end{pmatrix}, \tag{1}$$

where $\sigma_z = \mathrm{diag}(1, -1)$, and X, Y and Z are real numbers referring to Alice's variance, Bob's variance, and the covariance between Alice and Bob, respectively. Note that this form can easily be understood from an experimental point of view since the quantum channel is not supposed to

induce correlations between different quadratures, for instance, but no theoretical justification has been given so far. Here, we use the ideas explained in the previous section to prove that Γ can indeed take this simple form.

Since we make the assumption of a collective attack, the covariance matrix Γ is well defined and can be estimated by Alice and Bob. The most general form for Γ is

$$\Gamma = \begin{pmatrix} X_{11} & X_{12} & Z_{11} & Z_{12} \\ X_{12} & X_{22} & Z_{21} & Z_{22} \\ Z_{11} & Z_{21} & Y_{11} & Y_{12} \\ Z_{12} & Z_{22} & Y_{12} & Y_{22} \end{pmatrix}. \tag{2}$$

The idea is that Alice and Bob can perform some symmetrization operation, which transforms Γ into Γ_{sym}. First, note that their classical data are two strings $x, y \in \mathbb{R}^n$, which correspond to the results of homodyne measurements of the various quadratures of ρ_{AB}. The reconciliation is always optimized for a Gaussian channel, meaning that the random variable y is modeled as $y = tx + z$ [21], where t is a transmission factor and z is a random variable modeling the added noise and characterized by its variance σ^2. Therefore, the reconciliation procedure would not be affected if Alice and Bob both performed the same random orthogonal transformation $R \in O(n)$ to their respective data, since one would then have $Ry = tRx + z'$, where z' is a rotated noise with the same variance σ^2. If Alice and Bob apply such a random orthogonal transformation and forget which one has been performed, their data becomes 'symmetric' in the sense that the matrix Γ takes the form of Γ_{sym}, where $X = (X_{11} + X_{22})/2$, $Y = (Y_{11} + Y_{22})/2$ and $Z = (Z_{11} - Z_{22})/2$. The fact that the covariance matrix Γ_{sym} features $Z\sigma_z$ instead of $Z\mathbb{1}_2$ simply reflects the fact that Γ_{sym} is not the covariance matrix of the classical data of Alice and Bob in the *prepare-and-measure* scenario, but the covariance matrix of ρ_{AB} in the equivalent *entanglement-based* scenario. In the latter case, Alice and Bob would actually apply *conjugate* orthogonal transformations to their respective share of the state instead of the same transformation. By conjugate transformation, we mean the transformation whose corresponding $2n \times 2n$ matrix in phase space is obtained from the original one by flipping the sign of all rows whose label corresponds to a p quadrature and then flipping the sign of all columns whose label corresponds to a p quadrature. This can be understood by considering a two-mode squeezed vacuum, which is the state characterizing the inherent symmetry of continuous-variable QKD: this state has a covariance matrix Γ_{sym} where $Y = X$ and $Z = \sqrt{X^2 - 1}$, and is invariant under conjugate orthogonal transformations performed by Alice and Bob.

As we will see, this new symmetrization (based on orthogonal transformations in phase space instead of permutations in state space) has several crucial consequences. First, it allows us to rigorously prove that Alice and Bob can safely assume their covariance matrix to have a simple structure, characterized by only three parameters which are easily estimated experimentally (this was done until now with no firm theoretical justification). The second consequence, which we will study in the next section, is that it gives a simple structure to the state ρ_{AB} which enables us to investigate the unconditional security using a de Finetti approach.

4. Invariant states under orthogonal transformations in phase space

The goal of this section is to give some insights on the structure of the states which are invariant under orthogonal transformations in phase space. More precisely, if Alice and Bob perform n homodyne measurements on ρ_{AB} (Alice and Bob are assumed to measure the same quadrature

since they discard the data corresponding to measurements of incompatible quadratures), they obtain two random vectors $x, y \in \mathbb{R}^n$. We are interested in unitary transformations whose effect on ρ_{AB} is described by an orthogonal transformation on the probability distributions of x and y. As these probability distributions are completely characterized by the Wigner function of ρ_{AB}, the states of interest are simply those whose Wigner function is invariant under such transformations.

Before describing the bipartite case, it is useful to consider first the single-party case, where the state of Bob is traced out.

4.1. Single party case

Here, we are interested in generalizing the concept of *orthogonally invariant* probability distributions to the quantum setting, that is, to Wigner functions. A n-mode state $\rho^{(n)}$ is termed *orthogonally invariant* in phase space if it is invariant under the action of any n-mode Gaussian unitary operator corresponding to an orthogonal transformation in the $2n$-dimensional phase space of $\rho^{(n)}$. Physically, this means that $\rho^{(n)}$ remains unchanged after being processed via any n-mode passive linear interferometer (the orthogonal transformations that are not in the special orthogonal subgroup are irrelevant in the single-party case). The set of such orthogonally invariant states is convex and is, therefore, characterized by its extremal points, namely the states

$$\sigma_k^{(n)} = \frac{1}{a_k^n} \sum_{\substack{k_1 \ldots k_n \\ \text{s.t.} \sum_i k_i = k}} |k_1 \ldots k_n\rangle\langle k_1 \ldots k_n|,$$

where $|k_1 \ldots k_n\rangle$ is the n-mode Fock state with k_i photons in mode i and $a_k^n = \binom{n+k-1}{n-1}$.

Physically, these extremal states are (proportional to) the projectors onto the different eigenspaces of the total number operator $\hat{n} = \hat{n}_1 + \cdots \hat{n}_n$ labeled with the integer parameter k, corresponding to the total number of photons distributed over the n modes. The normalization constant a_k^n simply counts the number of ways of distributing k photons into n modes. These extremal states $\sigma_k^{(n)}$ form a discrete infinite set of mixed states. Importantly, any pure eigenstate chosen in the eigenspace corresponding to a given total photon number k is generally not orthogonally invariant; only the uniform mixture of them fulfils this invariance (Schur's lemma), which is why the extremal states $\sigma_k^{(n)}$ are mixed for $n > 1$. Finally, any state $\rho^{(n)}$ that is invariant under orthogonal transformations in phase space can be written as

$$\rho^{(n)} = \sum_{k=0}^{\infty} c_k \sigma_k^{(n)},$$

where the weights c_k satisfy $0 \leqslant c_k \leqslant 1$ and $\sum_k c_k = 1$.

4.2. An asymptotic quantum de Finetti theorem for orthogonally invariant states

Let us now introduce a classical de Finetti theorem for continuous variables. An infinite sequence of real-valued random variables $X_1, \ldots, X_n, \ldots$ is called *orthogonally invariant* if, for every n, the probability distribution of $X_1, \ldots, X_n$ is invariant under all orthogonal transformations of $\mathbb{R}^n$. It was proven in [22, 23] that orthogonally invariant distributions are exactly mixtures of i.i.d. normal distributions.

This result holds only approximately for finite sequences: if the probability distribution of $X_1, \ldots, X_n$ is invariant under orthogonal transformations of $\mathbb{R}^n$, then there exists a mixture of i.i.d. normals such that its variation distance to the marginal law of the first k coordinates of $X_1, \ldots, X_n$ is bounded by $O(k/n)$ for $k \ll n$ [15]. This cannot be directly applied to quantum systems, however, since Wigner functions are not necessary legitimate probability distributions (they can be negative). Here, we prove that this generalization is nevertheless correct in the asymptotic regime. In particular, we prove that an orthogonally invariant state tends to a mixture of multimode thermal states, which are products of n thermal states with the same mean photon number.

Let us consider an n-mode state $\rho^{(n)}$ which is orthogonally invariant in phase space. For any $N > n$, $\rho^{(n)}$ is the partial trace over $(N-n)$ modes of an N-mode orthogonally invariant state $\rho^{(N)}$. As stated above, $\rho^{(N)}$ is a convex mixture of the states $\sigma_k^{(N)}$. Therefore, it is enough to prove that the trace over $(N-n)$ modes of $\sigma_k^{(N)}$ becomes asymptotically close (for the trace distance) to a multimode thermal state as N tends to infinity. Since the state of interest $\mathrm{tr}_{N-n}\, \sigma_k^{(N)}$ as well as the 'target' n-mode thermal state $\rho_{\mathrm{th}}^{(n)}$ with k/n photons per mode are orthogonally invariant, they can both be written as mixtures of $\sigma_l^{(n)'}$s

$$\mathrm{tr}_{N-n}\ \sigma_k^{(N)} = \sum_{l=0}^{k} f(l)\sigma_l^{(n)}, \qquad \rho_{\mathrm{th}}^{(n)} = \sum_{l=0}^{\infty} g(l)\sigma_l^{(n)}$$

with

$$f(l) = \frac{a_l^n\, a_{k-l}^{N-n}}{a_k^N}, \qquad g(l) = a_l^n \frac{(k/N)^l}{(1+(k/N))^{n+l}}.$$

Note that f and g also depend on k, n and N, but we do not mention these parameters explicitly in order to simplify the notations. The trace distance between the two states is given by the variation distance between the two classical probability distributions f and g

$$\|\ \mathrm{tr}_{N-n}\ \sigma_k^{(N)} - \rho_{\mathrm{th}}^{(n)}\ \|_1 = \sum_{l=0}^{\infty} |f(l) - g(l)|.$$

It can be bounded from above as

$$\sum_{l=0}^{\infty} |f(l) - g(l)| = \sum_{l=0}^{\infty} \left| \frac{f(l)}{g(l)} - 1 \right| g(l) = 2 \sum_{l=0}^{\infty} \left(\frac{f(l)}{g(l)} - 1 \right)^+ g(l),$$
$$\leqslant 2 \left(\sup_l \frac{f(l)}{g(l)} - 1 \right)$$

where the last inequality follows from the triangle inequality, and $(x)^+$ stands for x if $x \geq 0$ and 0 if $x < 0$. Let us introduce the notation

$$h(l) \equiv \frac{f(l)}{g(l)} = \frac{a_{k-l}^{N-n}}{a_k^N} \times \frac{(1+(k/N))^{n+l}}{(k/N)^l}.$$

The rest of the proof consists in approximating $\sup h$ in the asymptotic regime. This is done by using the asymptotic approximation of a_{xn}^{yn} with $n \to \infty$ resulting from Stirling's formula, namely

$$a_{xn}^{yn} \sim \sqrt{\frac{1+y/x}{nx}}\, 2^{y\, n\, G(x/y)},$$

where $G(z) = (z+1)\log_2(z+1) - z\log_2(z)$ is the von Neumann entropy of a thermal state with z photons. Let us introduce the reduced variables $x = k/N$, $y = n/N$, $z = l/N$ and $t = (1-y)/(x-z)$. We can approximate the function of interest $h(l)$ as

$$h(zN) = \frac{a_{N(x-z)}^{Nt(x-z)}}{a_{xN}^{N}} \frac{(1+x)^{N(y+z)}}{x^{Nz}} \sim A2^{NB},$$

where

$$A = \sqrt{\frac{x(1+t)}{(x-z)(1+1/x)}} = \sqrt{\frac{tx(1+t)}{(1-y)(1+1/x)}}$$

and

$$B = (1-y)G(1/t) - G(x) + (y+z)\log(1+x) - z\log(x).$$

Deriving B with respect to z, one has

$$\frac{\partial B}{\partial z} = -\log(1+t) + \log(1+1/x).$$

Therefore, B is extremal for $t = 1/x$, that is $z = xy$, giving $B \leqslant 0$. As a result, one has

$$\sup_l h(l) = \sup_z h(zN) \sim \frac{1}{\sqrt{1-y}} \sim 1 + \frac{n}{2N} \quad \text{for} \quad n \ll N.$$

Hence, $\|\mathrm{tr}_{N-n}\,\sigma_k^{(N)} - \rho_{\mathrm{th}}^{(n)}\|_1 \to 0$ for $N \to \infty$, which proves the quantum continuous-variable version of the de Finetti theorem for orthogonally invariant states in the asymptotic regime. Note that the technique of this proof is very similar to that used to establish a de Finetti theorem for Werner states in [7] (theorem III.7).

4.3. Bipartite case

So far, we only discussed single-partite orthogonally invariant states. Obviously, in order to use this approach to the study of QKD security, one needs a bipartite generalization. Let us consider the case of a $2n$-mode bipartite state ρ_{AB}, meaning that Alice and Bob each have n modes. Such a state ρ_{AB} is termed *invariant under conjugate orthogonal transformations* in phase space if, for any Gaussian unitary operation U corresponding to an orthogonal transformation in Alice's $2n$-dimensional phase space, it satisfies

$$U \otimes U^* \, \rho_{\mathrm{AB}} \, U^\dagger \otimes U^T = \rho_{\mathrm{AB}},$$

where U^* is the Gaussian unitary operation corresponding to the conjugate orthogonal transformation in Bob's phase space. Physically, this invariance means that ρ_{AB} remains unchanged when Alice processes her n modes into any passive linear interferometer while Bob processes his n modes into the passive linear interferometer effecting the conjugate orthogonal transformation in phase space (the orthogonal transformations that are not in the special orthogonal subgroup should be applied at the measurement outcomes, not at the level of quantum states).

Ideally, one should have a quantum de Finetti theorem for bipartite orthogonally invariant states since this is the case which is directly relevant for proving the security of continuous-variable QKD. The reason is that, following the arguments in section 2, Alice and Bob can indeed assume their bipartite state ρ_{AB} to be invariant under conjugate orthogonal transformations. Thus, a bipartite quantum de Finetti theorem would rigorously prove that ρ_{AB} is 'close to' a product of Gaussian states. Note, however, that an *exponential* version of the theorem would actually be required to address the security of continuous-variable QKD, meaning that it is enough to trace over only a negligible number of modes in order to get an exponentially good approximation by a Gaussian state. Then, such a Gaussian state would actually be the product of n i.i.d. Gaussian states, and the security against collective attacks would, therefore, imply the security against arbitrary attacks.

Finding a bipartite version of this quantum de Finetti theorem is the subject of further work. Although we do not have a rigorous proof yet, the fact that a bipartite version of the theorem holds is very likely. In particular, both partial traces $\rho_A = \mathrm{tr}_B\, \rho_{AB}$ and $\rho_B = \mathrm{tr}_A\, \rho_{AB}$ are single-partite orthogonally invariant states, for which the theorem applies. Hence, locally, we already know that a state ρ_{AB} that is invariant under conjugate orthogonal transformations in phase space becomes asymptotically Gaussian. One only needs to prove that the correlations between Alice and Bob also behave according to the bipartite version of the theorem.

5. Conclusion and perspectives

We have discussed the role of symmetries in the security analysis of QKD, and introduced a new symmetry that is especially suited to continuous-variables schemes. This rotation symmetry, which can be spelled out in the phase space representation, encompasses the usual symmetry under permutations in state space that have been considered so far in the context of discrete-variable QKD. We then derived an asymptotic quantum de Finetti theorem for orthogonally invariant states in phase space, and showed that Gaussian states play a role similar to that of i.i.d. states in the usual de Finetti theorem. More precisely, any orthogonally invariant state can be shown to be asymptotically close to a mixture of product Gaussian (thermal) states. This first application of a symmetry in phase space to the QKD security analysis seems very promising as Gaussian states have been known to play a fundamental role in the analysis of continuous-variable QKD.

The perspectives of this work towards proving the unconditional security of continuous-variable QKD are twofold. A first approach would be to study the generalization of our (asymptotic) continuous-variable quantum de Finetti theorem in phase space to the bipartite scenario, and then investigate whether an exponential version can be derived. The second option would be to see if the techniques recently introduced in [5] can be generalized to continuous-variable QKD.

Acknowledgments

AL thanks Renato Renner and Johan Åberg for fruitful discussions. We acknowledge financial support of the European Union under project QAP (FP7-ICT-015848), of Agence Nationale de la Recherche under projects PROSPIQ (ANR-06-NANO-041-05) and SEQURE (ANR-07-SESU-011-01), and of the Brussels-Capital Region under the project CRYPTASC and the programme Prospective Research for Brussels.

References

[1] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing* 175
[2] Renner R 2007 *Nat. Phys.* **3** 645
[3] Hayashi M 2006 *Phys. Rev.* A **74** 022307
[4] Scarani V and Renner R 2008 *Phys. Rev. Lett.* **100** 200501
[5] Christandl M, König R and Renner R 2009 *Phys. Rev. Lett.* **102** 020504
[6] Cerf N J and Grangier P 2007 *J. Opt. Soc. Am.* B **24** 324
[7] Christandl M, König R, Mitchison G and Renner R 2007 *Commun. Math. Phy.* **273** 473
[8] König R and Mitchison G 2009 *J. Math. Phys.* **50** 012105
[9] D´Cruz C, Osborne T J and Schack R 2007 *Phys. Rev. Lett.* **98** 160406
[10] Renner R and Cirac J I 2008 2009 *Phys. Rev. Lett.* **102** 110504
[11] Leverrier A and Grangier P 2009 *Phys. Rev. Lett.* **102** 180504
[12] König R and Wolf M M 2009 *J. Math. Phys.* **50** 012102
[13] García-Patrón R and Cerf N J 2006 *Phys. Rev. Lett.* **97** 190503
[14] Navascués M, Grosshans F and Acín A 2006 *Phys. Rev. Lett.* **97** 190502
[15] Diaconis P and Freedman D A 1987 *Ann. Inst. Henri Poincaré,* **23** 397
[16] Inoue K, Waks E and Yamamoto Y 2002 *Phys. Rev. Lett.* **89** 37902
[17] Stucki D, Thew R, Scarani V, Brunner N, Gisin N, Gautier J D and Barreiro C 2005 *Appl. Phys. Lett.* **87** 194108
[18] Kraus B, Gisin N and Renner R 2005 *Phys. Rev. Lett.* **95** 80501
[19] Silberhorn C, Ralph T C, Lütkenhaus N and Leuchs G 2002 *Phys. Rev. Lett.* **89** 167901
[20] Grosshans F and Grangier P 2002 *Phys. Rev. Lett.* **88** 57902
[21] Leverrier A, Alléaume R, Boutros J, Zémor G and Grangier P 2008 *Phys. Rev.* A **77** 42325
[22] Schoenberg I J 1938 *Trans. Amer. Math. Soc.* **44** 522
[23] Freedman D A 1962 *Ann. Math. Stat.* **33** 916