Security of continuous-variable quantum key distribution against general attacks

Anthony Leverrier[1], Raúl García-Patrón[2], Renato Renner[1], Nicolas J. Cerf[3]
[1]*Institute for Theoretical Physics, ETH Zurich, 8093 Zurich, Switzerland*
[2]*Max-Planck Institut fur Quantenoptik, Hans-Kopfermann Str. 1, D-85748 Garching, Germany and*
[3]*Quantum Information and Communication, Ecole Polytechnique de Bruxelles, CP 165, Université Libre de Bruxelles, 1050 Bruxelles, Belgium*
(Dated: May 20, 2012)

Introduction – Quantum key distribution (QKD), the art of distilling a secret key among distant parties in an untrusted environment, is certainly the most studied quantum cryptographic primitive. Since the seminal papers of Bennett and Brassard [1] and Ekert [2], considerable progress has been made in terms of security proofs [3]. Most well know protocols are today known to be secure against arbitrary attacks even in the realistic finite-size regime. This is a remarkable result, as guaranteeing security against any potential attack is in principle an extremely complex task. Security proofs generally circumvent this problem by using the natural permutation invariance of most QKD protocols to show that it is sufficient to guarantee security against attacks where the eavesdropper interacts independently and identically with every communication signal. In an entanglement-based description of QKD, this will be identical to assume Alice and Bob's joint state $\rho_{A^nB^n}$ having an identical and independently distributed (i.i.d.) structure $\rho_{A^nB^n} = \sigma_{AB}^{\otimes n}$. The reduction of security against general attack to the i.i.d. scenario is usually achieved with the use of either de Finetti like theorems [4] or the postselection technique [5]. Unfortunately, for some protocols these tools cannot be applied. This is the case of discrete-variables protocols such as DPS [6] and COW [7], which are not permutation invariant, as well as device-independent QKD (where Alice and Bob's equipment is not trusted) and continuous-variable (CV) protocols. In the last two cases, the techniques of Refs. [4, 5] can not be applied as the the dimension of the relevant Hilbert space is infinite whereas both results are only valid for (reasonably small) finite dimensions.

In this work, we are interested in continuous-variable QKD protocols, *i.e.* where detection of the quantum states consists of measurement of the light-field quadratures (homodyne or heterodyne) instead of photon counting (see Ref. [8] for a recent review). From an experimental point of view, they present many advantages over discrete-variable protocols. More importantly, they can be implemented with standard telecom components and are compatible with standard wavelength division multiplexed telecommunication components. Secondly, quadrature measurements do not require any photon counters and achieve higher repetition rates than current single-photon detectors. Distribution of secret keys over long distances (more than 80 km) is currently achievable [9], making continuous-variable protocols competitive with respect to their discrete-variable counterparts. Their security analysis, however, is technically challenging due to the infinite-dimensional nature of the Hilbert space with which they are described. Among continuous-variable protocols, the so-called Gaussian ones are the most popular ones, primarily due to the experimental simplicity. Their prepare-and-measure schemes start by Alice sending coherent states or squeezed states with a Gaussian modulation followed by an homodyne or heterodyne measurement at Bob station. Equivalently one can devise an entangled-based scheme where Alice prepares an entangled two-mode squeezed vacuum state (the continuous-variable equivalent of the Bell pair), keeping one mode and sending the other one to Bob through the quantum channel. Then both parties measure their respective state with either an homodyne or heterodyne detection, obtaining two strings of correlated real-valued data. Finally, Alice and Bob extract a secret key through information reconciliation [10] and privacy amplification.

The security of Gaussian protocols in the aymptotic regime is rather well understood. A recent version of the de Finetti theorem compatible with infinite-dimensional Hilbert spaces [11] can be used to reduce the security proof to studying the i.i.d. scenario, which was analyzed in [12, 13] where the optimal attack were shown to be Gaussian attacks . The security of finite-size key exchanges has attracted attention recently, due to their relevance for realistic implementations. A crucial step in that direction is proving the reduction from general attacks to the i.i.d. scenario. Currently, two results in this direction are known. The first one is a version of the de Finetti theorem compatible with infinite-dimensional Hilbert spaces [11]. In that case, the usual protocol is modified by the addition of a test. Conditioned to the success of this test, security against coherent attacks is guaranteed. Unfortunately, this only applies for unrealistic scenarios where the number of signals exchanged between Alice and Bob is way beyond what can be achieved experimentally. Therefore, this result appears as a proof of principle (useful for the asymptotic regime reduction) but needs to be dramatically improved in order to assess the security of experimental implementations. The second result makes use of an entropic uncertainty inequality [14]. The main advantage of this result is that, unlike de Finetti's theorem, it is compatible with realistic finite-size effects. Unfortunately, it is not compatible with realistic experimental parameters. In particular, the tolerated losses correspond to a few hundred meters only.

Main result – In this paper, we give the first security proof of CV QKD against general attacks, which guarantees a secret key rate for realistic experimental regimes, in terms of losses and noise, and taking into account finite-size effects. We prove that any Gaussian protocol that is ϵ-secure in an i.i.d. scenario becomes $\tilde{\epsilon}$-secure against general attacks, where $\tilde{\epsilon} = \epsilon \times 2^{\mathrm{poly}(\log n)}$. This is sufficient in general since ϵ can be made exponentially small in n at the price of reducing the asymptotic key-rate by a arbitrarily small fraction. Our proof exploits the specific symmetries of CV QKD in phase-space [15] showing that the protocols can be well-approximated by a finite-dimensional protocol with a reasonably small dimension, which allows us to use the postselection technique [5].

Sketch of the proof – Our result is a reduction of the security against coherent attacks to that against collective attacks. Let us suppose that our CV QKD protocol of interest, let us note it $\mathcal{E}_0$, is secure against collective attacks. Here, $\mathcal{E}_0$ is a CP map from the infinite-dimensional Hilbert space $(\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes n}$ to the set of pairs (S_A, S_B) of l-bit strings (Alice and Bob's final keys, respectively) and C, a transcript of the classical communication. In order to assess the security of a given QKD protocol, it is useful to compare it with an ideal protocol. Such an ideal protocol can be constructed (at least in principle) by concatenating the protocol with a map $\mathcal{S}$ taking (S_A, S_B, C) as input and outputting the triplet (S, S, C) where the string S is a perfect secret key (uniformly distributed and unknown to Eve) with the same length as S_A. By construction, the protocol $\mathcal{F}_0 := \mathcal{S} \circ \mathcal{E}_0$ is secure since it always outputs a secret key.

We need to slightly modify the protocol $\mathcal{E}_0$ in order to establish its security against general attacks. This is done by appending to it an initial test $\mathcal{T}$. More precisely, $\mathcal{T}$ is a CP map taking a state in a slightly larger Hilbert space, $(\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes(n+k)}$, measuring k suitably chosen modes (identical for Alice and Bob) and comparing a function of the measurement outcomes to a value fixed in advance. Crucially, the test $\mathcal{T}$ commutes with the measurements and can be performed on Bob's classical measurement results. After measuring his $n+k$ modes, Bob holds a $(n+k)$-dimensional real-valued vector $\vec{x}_B$ (for a protocol with homodyne detection). He then chooses a random subspace T of $\mathbb{R}^{n+k}$ of dimension k (this can be done with complexity $O(kn)$) and compares the square norm Y_k of the projection of $\vec{x}_B$ onto T to a threshold value $Y_{\mathcal{T}}$ fixed in advance. The test succeeds if the norm is smaller than $Y_{\mathcal{T}}$, in which case Bob describes T to Alice and and they both apply the usual protocol $\mathcal{E}_0$ to their respective n-dimensional vectors orthogonal to T. Otherwise the test fails and the protocol is aborted. When the test passes, it means that the global state is compatible with a state containing only a low number of photons, that is a state well-described in a low dimensional Hilbert space.

In the following, we are interested in proving the security of the modified protocol $\mathcal{E} := \mathcal{E}_0 \circ \mathcal{T}$ against coherent attacks. This is done by deriving an upper bound on the diamond norm $||\mathcal{E} - \mathcal{F}||_\diamond$ between the true protocol $\mathcal{E}$ and its ideal counterpart $\mathcal{F} := \mathcal{S} \circ \mathcal{E}$, where the diamond norm is defined as

$$||\mathcal{E} - \mathcal{F}||_\diamond := \sup_{\rho_{ABE}} \|(\mathcal{E} - \mathcal{F}) \otimes \mathrm{id}_{\mathcal{K}}(\rho_{ABE})\|_1 \,, \tag{1}$$

where the supremum is taken over $(\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes(n+k)} \otimes \mathcal{K}$ for any auxiliary system $\mathcal{K}$. Remark that if diamond norm is bounded by ϵ, it means that Alice, Bob and Eve together cannot distinguish the true protocol $\mathcal{E}$ from the ideal one, $\mathcal{F}$, with a probability of success larger than $1/2 + \epsilon$. The protocol $\mathcal{E}$ will be ϵ-secure against arbitrary attacks when $||\mathcal{E} - \mathcal{F}||_\diamond \leq \epsilon$.

All the subtlety of our result resides in proving that when the test succeeds (*i.e.*, $Y_k \leq Y_{\mathcal{T}}$), the global state shared between Alice and Bob is compatible with a low number of photons per mode, that is, a state well-described in a low dimensional Hilbert space. To prove that, we introduce the (virtual) CP map $\mathcal{P}$ which projects a state in $(\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes n}$ onto a low-dimensional Hilbert space $(\bar{\mathcal{H}}_A \otimes \bar{\mathcal{H}}_B)^{\otimes n}$ where $\bar{\mathcal{H}}_A := \mathrm{Span}(|0\rangle, |1\rangle, \cdots, |d_A - 1\rangle)$ and $\bar{\mathcal{H}}_B := \mathrm{Span}(|0\rangle, |1\rangle, \cdots, |d_B - 1\rangle)$ are respectively a d_A and a d_B-dimensional subspace of the Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$. Remark that the CP map $\mathcal{P}$ is only a theoretical artifact of our proof but do not need to be implemented in the real protocol, contrary to $\mathcal{T}$. We then define the (virtual) protocols $\tilde{\mathcal{E}} = \mathcal{E}_0 \circ \mathcal{P} \circ \mathcal{T}$ and $\tilde{\mathcal{F}} = \mathcal{S} \circ \tilde{\mathcal{E}}$ which are intrinsically finite dimensional, due to the presence of $\mathcal{P}$. This means that one can analyze the security of $\tilde{\mathcal{E}}$ with the help of the postselection theorem [5]. The remaining element is a proof that the protocol $\tilde{\mathcal{E}}$ is close (for the diamond distance) to the true experimental protocol $\mathcal{E}$. For this, we use the following theorem, proven in the long version of the paper,

Theorem 1. *(Informal.) For any state in $\rho_{ABE} \in (\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes(n+k)} \otimes \mathcal{K}$,*

$$||\left(\mathrm{id}_{\mathcal{H}^{\otimes n}} - \mathcal{P}\right) \circ \mathcal{T} \otimes \mathrm{id}_{\mathcal{K}}(\rho_{ABE})||_1 \leq \epsilon, \tag{2}$$

where ϵ is a function of k, n, the dimensions d_A and d_B of the projection $\mathcal{P}$ and the threshold $Y_{\mathcal{T}}$ in the test $\mathcal{T}$.

The security of the protocol $\mathcal{E}$ is then a consequence of the following derivation

$$\begin{aligned} ||\mathcal{E}-\mathcal{F}||_\diamond &\leq ||\tilde{\mathcal{E}}-\tilde{\mathcal{F}}||_\diamond + ||\mathcal{E}-\tilde{\mathcal{E}}||_\diamond + ||\mathcal{F}-\tilde{\mathcal{F}}||_\diamond & (3)\\ &= ||\tilde{\mathcal{E}}-\tilde{\mathcal{F}}||_\diamond + ||\mathcal{E}_0\circ(\mathrm{id}-\mathcal{P})\circ\mathcal{T}||_\diamond + ||\mathcal{F}_0\circ(\mathrm{id}-\mathcal{P})\circ\mathcal{T}||_\diamond & (4)\\ &\leq ||\tilde{\mathcal{E}}-\tilde{\mathcal{F}}||_\diamond + 2||(\mathrm{id}-\mathcal{P})\circ\mathcal{T}||_\diamond, & (5)\end{aligned}$$

where we used the triangle inequality in Eq.(3) and the fact that the CP maps $\mathcal{E}_0$ and $\mathcal{F}_0$ cannot increase the diamond norm in Eq.(5). Finally, we bound the first term of Eq.(5) using the postselection theorem [5] and the second term using the Theorem 1 above.

Conclusion– We have proved that Gaussian continuous-variable QKD protocols, using a Gaussian distribution of coherent or squeezed states and homodyne or heterodyne measurement, are secure against arbitrary attacks. Our proof exploits the specific symmetries in phase-space of Gaussian QKD protocols to prove that once a simple test over the measurement outcomes succeeds ($Y_k \leq Y_\mathcal{T}$), the global state shared between Alice and Bob is well decribed by assigning a low dimensional Hilbert space to each mode. Then one can use the postselection technique introduced in Ref. [5] for discrete-variable protocols to conclude. Our result greatly improves over previous ones using either a de Finetti theorem or an entropic uncertainty principle which could not be applied to prove the security of protocols in realistic experimental implementations. Finally, our result seems to indicate that in order to prove the security of any QKD protocol one should exploit all the available symmetries of the protocol, beyond the traditional permutation.

[1] C. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (1984), vol. 175.
[2] A. Ekert, Physical review letters **67**, 661 (1991).
[3] V. Scarani, H. Bechmann-Pasquinucci, N. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[4] R. Renner, Nature Physics **3**, 645 (2007).
[5] M. Christandl, R. König, and R. Renner, Phys. Rev. Lett. **102**, 020504 (2009).
[6] K. Inoue, E. Waks, and Y. Yamamoto, Physical review letters **89**, 37902 (2002).
[7] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, Appl. Phys. Lett. **87**, 194108 (2005).
[8] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012), URL `http://link.aps.org/doi/10.1103/RevModPhys.84.621`.
[9] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, submitted to QCRYPT 2012 (2012).
[10] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, Phys. Rev. A **84**, 062317 (2011).
[11] R. Renner and J. I. Cirac, Phys. Rev. Lett. **102**, 110504 (2009).
[12] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).
[13] M. Navascués, F. Grosshans, and A. Acín, Phys. Rev. Lett. **97**, 190502 (2006).
[14] F. Furrer, T. Franz, M. Berta, V. Scholz, M. Tomamichel, and R. Werner, Arxiv preprint ArXiv:1112.2179 (2011).
[15] A. Leverrier, E. Karpov, P. Grangier, and N. J. Cerf, New J. Phys. **11**, 115009 (2009).