Security of Continuous-Variable Quantum Key Distribution Against General Attacks

Anthony Leverrier,[1,2] Raúl García-Patrón,[3] Renato Renner,[1] and Nicolas J. Cerf[4]
[1]*Institute for Theoretical Physics, ETH Zurich, 8093 Zurich, Switzerland*
[2]*INRIA Paris-Rocquencourt, 78153 Le Chesnay Cedex, France*
[3]*Max-Planck Institut fur Quantenoptik, Hans-Kopfermann Strasse 1, D-85748 Garching, Germany*
[4]*Quantum Information and Communication, Ecole Polytechnique de Bruxelles, CP 165, Université Libre de Bruxelles, 1050 Bruxelles, Belgium*
(Received 24 August 2012; published 18 January 2013)

We prove the security of Gaussian continuous-variable quantum key distribution with coherent states against arbitrary attacks in the finite-size regime. In contrast to previously known proofs of principle (based on the de Finetti theorem), our result is applicable in the practically relevant finite-size regime. This is achieved using a novel proof approach, which exploits phase-space symmetries of the protocols as well as the postselection technique introduced by Christandl, Koenig, and Renner [Phys. Rev. Lett. **102**, 020504 (2009)].

DOI: 10.1103/PhysRevLett.110.030502 PACS numbers: 03.67.Dd, 03.67.Hk, 42.50.−p

Quantum key distribution (QKD), the art of generating 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 analysis [3]. While original proofs were valid in the asymptotic limit where the number of exchanged signals tends to infinity, modern proofs are applicable in the practically relevant finite-size regime [4,5]. A main challenge when proving security of cryptographic protocols is that there is a very large number of possible attack strategies that need to be taken into account. Security proofs generally circumvent this problem by using the natural permutation invariance [6] of most QKD protocols, which allows us to restrict the analysis to the much smaller class of *collective* attacks, where the eavesdropper interacts independently and identically with each individual quantum signal. In an entanglement-based description of QKD, this amounts to assuming that the joint state $\rho_{A^nB^n}$ that the two legitimate parties, Alice and Bob, hold after the initial distribution of entangled signals has an identical and independently distributed (i.i.d.) structure $\rho_{A^nB^n} = \sigma_{AB}^{\otimes n}$ (where n denotes the number of quantum signals exchanged during the protocol).

One usually achieves this reduction from general to collective (i.i.d.) attacks thanks to either de Finetti-type theorems [9] or the postselection technique [10]. Unfortunately, these tools cannot be directly applied to continuous-variable (CV) protocols because they require the dimension of the Hilbert space to be finite (and small compared to n). However, by prepending a suitable energy test to the protocol that gives a bound on the effective dimension, it is still possible to use a specific variant of the de Finetti theorem and prove that CV protocols are secure in principle [11]. However, this approach only works in the limit of very large n. Hence, while providing a proof of principle, it is not applicable to realistic protocols.

The specificity of CV protocols is that the detection consists of (homodyne or heterodyne) measurements of the light-field quadratures (see Ref. [12] for a review). From an experimental point of view, they present many advantages over discrete-variable protocols. Most importantly, they can be implemented with standard telecom components and are compatible with wavelength division multiplexing [13], which is an important advantage when integrating QKD into real-world telecommunication networks. Moreover, quadrature measurements do not require any photon counters and higher repetition rates can be achieved. Distribution of secret keys over long distances (more than 80 km) is currently achievable [14], making CV protocols competitive with respect to their discrete-variable counterparts. However, their security analysis is technically challenging due to the infinite-dimensional nature of the relevant Hilbert space.

Currently, two different proofs of security for CV protocols against general attacks are known. The first is based on the aforementioned de Finetti theorem [11], which shows that collective attacks are asymptotically optimal. In addition, one uses that Gaussian attacks are optimal among collective attacks [15,16]. It then suffices to prove security against Gaussian collective attacks, which is relatively straightforward. As explained above, however, this proof method only works in an asymptotic regime where the number of exchanged signals n tends to infinity. The second approach uses an entropic uncertainty relation [17] and works for more reasonable values of n but is only applicable to a protocol where both Alice and Bob perform homodyne measurements, corresponding to a prepare-and-measure protocol where Alice sends squeezed states through the quantum channel [18]. Here, we wish to address the security of the more practical protocols where

Alice sends coherent states [19], or equivalently performs a heterodyne detection on her modes (in an entanglement-based variant [20]).

In the remainder of this Letter, we first explain on a general level how one can obtain a protocol secure against general attacks by prepending an initial energy test to a protocol that is secure against collective attacks. This result is quite generic and can be applied to various CV protocols provided that they display a rather natural invariance in phase space. Then, in order to explain the proof (sketch) on a more concrete level, we study the specific case of a Gaussian protocol where Alice sends coherent states and Bob performs heterodyne measurements.

Main result.—Our main result is a proof in the finite-size regime that if a protocol is secure against collective attacks, then it is secure against coherent attacks. As in Refs. [11,17], this is achieved by prepending an initial test to a protocol already proven secure against collective attacks. The purpose of the test is to verify that the quantum state shared by Alice and Bob is well approximated by a state living in a reasonably low-dimensional Hilbert space. This allows us to use the postselection technique [10] which shows roughly that if a (permutation-invariant) protocol with n signals is ϵ-secure against collective attacks, then it is $\tilde{\epsilon}$-secure against general attacks with $\tilde{\epsilon} = \epsilon \times \mathrm{poly}(n)$.

Our result is based on two central ideas, which allow us to go beyond the analysis of Ref. [11]. The first is the use of the postselection technique. It is well known that the postselection technique guarantees much better bounds than the approach based on a de Finetti theorem when reducing general to collective attacks [21]. Moreover, and this is in fact the main technical contribution of the present work, we exploit specific symmetries of the CV QKD protocol in phase space instead of the usual permutation symmetry in state space, which is not sufficient to apply the postselection technique to our case. More precisely, the QKD protocol is invariant if Alice and Bob process their respective modes with global conjugate passive linear transformations of their n modes before performing their measurements. This rotational invariance in phase space is better suited to analyze CV protocols [22], allowing us to precisely bound the effective number of photons per mode from the results of random quadrature measurements.

QKD protocols and their security.—A QKD protocol is a CP map from the infinite-dimensional Hilbert space $(\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes n}$, corresponding to the initially distributed entanglement, to the set of pairs (S_A, S_B) of l-bit strings (Alice's 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 $\mathcal{E}$ in a composable framework, one compares it with an ideal protocol [23]. The action of an ideal protocol $\mathcal{F}$ is defined by concatenating the protocol $\mathcal{E}$ 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; that is, $\mathcal{F} = \mathcal{S} \circ \mathcal{E}$. Then, a protocol will be called *ϵ-secure* if the advantage in distinguishing it from an ideal version is not larger than ϵ. This advantage is quantified by (one half of) the diamond norm defined by

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

where the supremum is taken over density operators on $(\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes n} \otimes \mathcal{K}$ for any auxiliary system $\mathcal{K}$.

General approach: Protocols with prepended test.—Our main technical result is a reduction of the security against general attacks to that against collective attacks, for which security has already been proved in earlier work. Let us therefore suppose that our CV QKD protocol of interest, $\mathcal{E}_0$, is secure against collective attacks. We will slightly modify it by prepending 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 randomly chosen modes (identical for Alice and Bob) and comparing the measurement outcome to a threshold fixed in advance. The test succeeds if the measurement outcome (related to the energy) is small, meaning that the global state is compatible with a state containing only a low number of photons per mode. Such a state is well described in a low-dimensional Hilbert space, which leads to better bounds when using the postselection technique. Depending on the outcome of the test, either the protocol aborts or one applies the original protocol $\mathcal{E}_0$ on the n remaining modes. A more precise description is provided below when we consider the specific case of the "heterodyne protocol."

Note that test $\mathcal{T}$ has essentially no impact on the practical feasibility since it only requires $k \ll n$ additional homodyne (or heterodyne) measurements.

In order to establish that the protocol $\mathcal{E} := \mathcal{E}_0 \circ \mathcal{T}$ is ϵ-secure against arbitrary attacks, one needs to bound $\|\mathcal{E} - \mathcal{F}\|_\diamond$. The postselection theorem [10] allows us to bound the diamond norm between such maps by simply considering i.i.d. states (i.e., the equivalent of collective attacks), but only when the maps act on finite-dimensional spaces. We address this issue by introducing another 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 $\bar{\mathcal{H}}_A := \mathrm{Span}(|0\rangle, |1\rangle, \ldots, |d_A - 1\rangle)$ and $\bar{\mathcal{H}}_B := \mathrm{Span}(|0\rangle, |1\rangle, \ldots, |d_B - 1\rangle)$ are, respectively, a d_A- and a d_B-dimensional subspace of the Fock spaces $\mathcal{H}_A$ and $\mathcal{H}_B$. We define (virtual) protocols $\tilde{\mathcal{E}} := \mathcal{E}_0 \circ \mathcal{P} \circ \mathcal{T}$ and $\tilde{\mathcal{F}} := \mathcal{S} \circ \tilde{\mathcal{E}}$. The security of the protocol $\mathcal{E}$ is then a consequence of the following derivation:

$$\begin{aligned}\|\mathcal{E} - \mathcal{F}\|_\diamond &\le \|\tilde{\mathcal{E}} - \tilde{\mathcal{F}}\|_\diamond + \|\mathcal{E} - \tilde{\mathcal{E}}\|_\diamond + \|\mathcal{F} - \tilde{\mathcal{F}}\|_\diamond \\ &\le \|\tilde{\mathcal{E}} - \tilde{\mathcal{F}}\|_\diamond + \|\mathcal{E}_0 \circ (\mathrm{id} - \mathcal{P}) \circ \mathcal{T}\|_\diamond \\ &\quad + \|\mathcal{F}_0 \circ (\mathrm{id} - \mathcal{P}) \circ \mathcal{T}\|_\diamond \\ &\le \|\tilde{\mathcal{E}} - \tilde{\mathcal{F}}\|_\diamond + 2\|(\mathrm{id} - \mathcal{P}) \circ \mathcal{T}\|_\diamond, \qquad (2)\end{aligned}$$

where we used the triangle inequality and the fact that the CP maps $\mathcal{E}_0$ and $\mathcal{F}_0 := \mathcal{S} \circ \mathcal{E}_0$ cannot increase the diamond norm. The first term can be bounded thanks to the postselection theorem because $\tilde{\mathcal{E}}$ and $\tilde{\mathcal{F}}$ are finite dimensional, and it can be made arbitrary small at the price of reducing slightly the key rate. The second term can be bounded by a function of the threshold in the test $\mathcal{T}$ thanks to the following theorem, of which we give a proof sketch for the heterodyne protocol below (and a full proof in the Supplemental Material [24]).

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

$$\|(\mathrm{id}_{\mathcal{H}^{\otimes n}} - \mathcal{P}) \circ \mathcal{T} \otimes \mathrm{id}_{\mathcal{K}}(\rho_{ABE})\|_1 \leq \epsilon, \qquad (3)$$

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

Specific analysis for the protocol with heterodyne detection.—Consider the heterodyne protocol of Ref. [25] as our protocol $\mathcal{E}_0$. In its entangled version, Alice prepares n two-mode squeezed vacuum states, measures one mode of each state with a heterodyne detection (meaning that she measures both quadratures q and p for each mode), and sends the other one through the quantum channel. Bob then also performs a heterodyne measurement of the states he receives. At the end of this process, Alice and Bob have access to two correlated vectors in $\mathbb{R}^{2n}$, $\vec{x}_A$ for Alice and $\vec{x}_B$ for Bob. Then, they perform the reconciliation procedure [26,27] in order to extract a common string, and finally privacy amplification [28] to distill their final secret keys, S_A and S_B, respectively.

This protocol is invariant under the action of conjugate passive linear operations (beam splitters and phase shifts) because these correspond to some orthogonal transformation $R \in O(2n)$ of the quadratures in phase space. Specifically, if such an operation is applied, then Alice's and Bob's vectors become $R\vec{x}_A$ and $R^T\vec{x}_B$ [24], meaning that the effect of the beam splitters and phase shifts can be undone by simply applying the inverse rotation on the classical data. More generally, for a QKD protocol to be invariant in phase space, it is sufficient to check that passive linear operations commute with the measurements.

We assume in the following that the protocol $\mathcal{E}_0$ is secure against collective attacks, in the sense that for any pure state $\rho_{ABE} \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ where $\mathcal{H}_E \cong \mathcal{H}_A \otimes \mathcal{H}_B$, the quantity $\|(\mathcal{E}_0 - \mathcal{F}_0) \otimes \mathrm{id}_{\mathcal{K}}(\rho_{ABE}^{\otimes n})\|_1$ can be made exponentially small in n, say $2^{-c\delta^2 n}$, at the price of reducing the secret key rate by an arbitrary small fraction δ compared to the asymptotic optimal rate, for some constant $c > 0$. We note that despite being proven secure against collective attacks in the asymptotic limit [15,16,29], the security of $\mathcal{E}_0$ for finite size attacks is not yet completely understood in the sense that the precise relation between the values of c and δ is not currently known: this is due to the difficulty of estimating a covariance matrix in the finite-size regime (see Ref. [30]).

As mentioned above, we will prove the security of a slightly modified protocol, denoted $\mathcal{E}$ which starts with $n + k$ modes (instead of n in the case of $\mathcal{E}_0$), k of which are being used to conduct a test $\mathcal{T}$. If the test passes, corresponding roughly to a scenario where the state does not contain too many photons, then Alice and Bob proceed with the protocol $\mathcal{E}_0$, otherwise they abort. For simplicity we define here a protocol with a test $\mathcal{T}$ that depends only on Bob's classical data. This implies the assumption that Alice prepares her state in a trusted environment, meaning that her reduced state is an $(n + k)$-modal thermal state. Note that one could easily remove this assumption by applying the test $\mathcal{T}$ at Alice's and Bob's stations simultaneously.

The test consists in first choosing a random rotation R in $\mathbb{R}^{2(n+k)}$ (with the appropriate measure) and applying it to the $2(n + k)$-dimensional vector corresponding to Bob's measurement outcomes (and apply the transpose rotation to Alice's vector). Let us denote by $q_1, p_1, q_2, p_2, \ldots, q_k, p_k$ the first $2k$ coordinates of Bob's rotated vector and define the variable $Y_k := 1/(2k) \sum_{i=1}^{k} (q_i^2 + p_i^2)$. The coordinates correspond to heterodyne measurements of k modes of ρ_B^{n+k} after being processed through an appropriate network of beam splitters and phase shifts [24]. The test $\mathcal{T}$ is characterized by two parameters: a threshold Y_{test} and k. It passes if $Y_k \leq Y_{\mathrm{test}}$ and fails otherwise. We note that the test does not break the invariance in phase space of the protocol: the invariance is enforced by the random rotation R. Because the test commutes with the measurement, it can equivalently be seen as a map from $(\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes(n+k)}$ to $(\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes n}$ (plus an additional bit encoding whether the test passed or not) that returns the n remaining modes when it passes and an "abort" state when it fails.

It is also useful to describe the CP map $\mathcal{P}$ characterized by three numbers, n, and the local dimensions d_A and d_B. This map corresponds to the binary outcome measurement in $(\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes n}$ described by the operators $\{P_A^{\otimes n} \otimes P_B^{\otimes n}, \mathbb{1} - P_A^{\otimes n} \otimes P_B^{\otimes n}\}$, where P_A and P_B are the single-mode projectors on $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively, defined as $P_{A/B} = |0\rangle\langle 0| + |1\rangle\langle 1| + \cdots + |d_{A/B} - 1\rangle\langle d_{A/B} - 1|$.

In order to establish Theorem 1, we will bound the probability p_{bad} of the following bad event: "the state passes the test but the projection onto $P_A^{\otimes n} \otimes P_B^{\otimes n}$ fails" for some initial state $\rho_{AB}^n \in (\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes n}$, meaning, roughly speaking, that the test did not detect that the state exceeds the desired low-dimensional Hilbert space. Let us note $\tilde{\rho}_{AB}^n$ the unnormalized state after the test when it passed; the probability of passing the test is simply $p_{\mathrm{test}} = \mathrm{tr}\tilde{\rho}_{AB}^n$ and $p_{\mathrm{bad}} = \mathrm{tr}[(1 - \mathcal{P})\tilde{\rho}_{AB}^n]$. One can bound p_{bad} in the following way:

$$\begin{aligned} p_{\mathrm{bad}} &= \mathrm{tr}(\mathrm{id}_{AB} - P_A^{\otimes n} \otimes P_B^{\otimes n})\tilde{\rho}_{AB}^n \\ &\leq \mathrm{tr}[(\mathrm{id}_A - P_A^{\otimes n})\tilde{\rho}_A^n] + \mathrm{tr}[(\mathrm{id}_B - P_B^{\otimes n})\tilde{\rho}_B^n] \\ &\leq \mathrm{tr}[(\mathrm{id}_A - P_A^{\otimes n})\rho_A^n] + \mathrm{tr}[(\mathrm{id}_B - P_B^{\otimes n})\tilde{\rho}_B^n], \end{aligned} \qquad (4)$$

where we used the union bound and the fact that Alice does not apply the test. The first term is easy to compute because the state of Alice, a multimode thermal state, is well known: $\rho_A^n = \rho_{\text{thermal}}^{\otimes n}$ with $\rho_{\text{thermal}} = \sum_{k=0}^{\infty} \frac{\lambda^k}{(1+\lambda)^{k+1}} |k\rangle\langle k|$ for a state with λ photons per mode. The value of λ is a parameter of the protocol and should be optimized given the expected characteristics of the quantum channel. The union bound gives

$$1 - \text{tr}(P_A^{\otimes n} \rho_A^n) \leq n[1 - \text{tr}(P_A \rho_{\text{thermal}})] = n\left(\frac{\lambda}{1+\lambda}\right)^{d_A}.$$

In particular, choosing $d_A = \frac{\log(n/\epsilon_A)}{\log(1+1/\lambda)}$ for the dimension of Alice's Hilbert space leads to $1 - \text{tr}(P_A^{\otimes n} \rho_A^n) \leq \epsilon_A$.

Bounding the second term in Eq. (4) is much trickier because one cannot assume that Bob's state ρ_B^n is Gaussian or that it even has an i.i.d. structure. This is because it corresponds to the output of the unknown quantum channel controlled by Eve. Here, we will make use of the specific symmetries of the QKD protocol in phase space in order to greatly simplify the problem. In general, most protocols are invariant under permutations of the subsystems of Alice and Bob. This means that the state ρ_{AB}^n (and therefore also ρ_B^n) can be assumed to display this invariance. However, CVQKD protocols such as the one considered here respect a much stronger symmetry: they are invariant when Alice and Bob apply to their respective $(n + k)$ modes conjugate passive linear transformations, implemented by any network of beam splitters and phase shifts [22,29] (see Supplemental Material [24]). Here, it is crucial that the test $\mathcal{T}$ respects the symmetry, and this can be enforced at the level of classical data by the choice of the random rotation in $\mathbb{R}^{2(n+k)}$.

Thanks to this symmetry, one can assume that the state ρ_B^{n+k} of Bob (before applying the test $\mathcal{T}$) is rotationally invariant. Such states satisfy a de Finetti theorem [31]: if sufficiently many modes of ρ_B^{n+k} are traced out, then the remaining state is close to a mixture of thermal states. Intuitively, one then expects that the second term of Eq. (4) behaves like the first one, and this is what we prove rigorously. Before we explain how to bound $\text{tr}(P_B^{\otimes n} \tilde{\rho}_B^n)$, we recall two useful properties of states, such as ρ_B^{n+k}, which are rotationally invariant [31]. First, these states are mixtures of generalized $(n + k)$-mode Fock states $\sigma_p^{n+k} := 1/\binom{n+k+p-1}{p} \sum_{p_1+\cdots+p_m=p} |p_1, p_2, \ldots, p_m\rangle\langle p_1, p_2, \ldots, p_m|$, where $|p_1, \ldots, p_m\rangle$ is the product of Fock states with p_1 photons in the first mode, p_2 photons in the second mode, etc., and the sum is taken over all states with a total number of p photons in $n + k$ modes. Second, the Wigner function $W(q_1, p_1, \ldots, q_{n+k}, p_{n+k})$ of ρ_B^{n+k} is isotropic, that is only depending on the norm of the vector $(q_1, p_1, \ldots, q_{n+k}, p_{n+k})$. This also holds for the Q-function of the state, that is the probability distribution of the outcomes of the heterodyne measurements.

Let us introduce another random variable $Z_n := 1/(2n) \sum_{i=1}^n q_{k+i}^2 + p_{k+i}^2$, corresponding to the norm of Bob's heterodyne measurements for the n modes of ρ_B^{n+k} not measured during the test $\mathcal{T}$. We show in Ref. [24] that the probability ϵ_{test} of passing the test with Z_n being much larger than Y_{test}, is exponentially small in k when the value of Y_{test} is chosen slightly larger than the expected variance of Bob's measurement results. In turn, this implies that the *total* number of photons in the state ρ_B^n is bounded by $O(nY_{\text{test}})$. Finally, we show that the projection over the space $\bar{\mathcal{H}}_B^{\otimes n}$ succeeds with high probability if $d_B = \dim \bar{\mathcal{H}}_B = O(\log \frac{2n}{\epsilon})$. This finally provides a bound on $\|(\text{id}_{\mathcal{H}^{\otimes n}} - \mathcal{P}) \circ \mathcal{T}\|_\diamond$ and proves Theorem 1.

We now put things together and establish that protocol $\mathcal{E}$ is secure against general attacks. First, choosing d_A and d_B on the order of $O(\log(n/\epsilon_{\text{test}}))$, one obtains $\|(\text{id}_{\mathcal{H}^{\otimes n}} - \mathcal{P}) \circ \mathcal{T}\|_\diamond \leq \epsilon_{\text{test}}$. Second, assuming that the original protocol $\mathcal{E}_0$ is secure against collective attacks, the diamond norm $\|\tilde{\mathcal{E}} - \tilde{\mathcal{F}}\|_\diamond$ can be bounded by $2^{-c\delta^2 n + O[\log^4(n/\epsilon_{\text{test}})]}$ using the postselection technique where the dimension of the relevant Hilbert space $\bar{\mathcal{H}}_A \otimes \bar{\mathcal{H}}_B$ is $d_A d_B = O[\log^2(n/\epsilon_{\text{test}})]$ (see Ref. [10] for details). This shows that protocol $\mathcal{E}$ is ϵ-secure against general attacks with

$$\epsilon = 2^{-c\delta^2 n + O[\log^4(n/\epsilon_{\text{test}})]} + 2\epsilon_{\text{test}}. \tag{5}$$

Conclusion.—We have proved that Gaussian continuous-variable QKD protocols, using a Gaussian distribution of coherent states and homodyne or heterodyne measurements, are secure against arbitrary attacks in the practically relevant finite-size regime. Our proof exploits the specific symmetries in phase space of Gaussian QKD protocols and uses a simple test to ensure that the global state shared between Alice and Bob is well described by assigning a low-dimensional Hilbert space to each mode. This allows one to employ the postselection technique, which was introduced in Ref. [10] for discrete-variable protocols. On a more general level, our result illustrates the use of symmetries for the analysis of cryptographic protocols. While in the present case of Gaussian protocols we have exploited a rotational invariance in phase space (instead of the usual permutation symmetry), it is conceivable to extend our technique to take advantage of other symmetries. One may even go one step further and design protocols that naturally exhibit additional symmetries.

This work was supported by the Swiss National Science Foundation (SNF) through the National Centre of Competence in Research "Quantum Science and Technology" and through Grant No. 200020-135048, the European Research Council (Grant No. 258932), the Humboldt foundation, and the F.R.S.-FNRS under project HIPERCOM.

[1] C. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), Vol. 175.
[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[4] V. Scarani and R. Renner, Phys. Rev. Lett. **100**, 200501 (2008).
[5] M. Tomamichel, C. Lim, N. Gisin, and R. Renner, Nat. Commun. **3**, 634 (2012).
[6] A protocol is said to be *permutation invariant* if it commutes with any permutation of the order in which the quantum signals are exchanged between the legitimate parties. There are only very few protocols that do not have this symmetry property, for instance, distributed-phase-reference protocols [7,8].
[7] K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002).
[8] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, Appl. Phys. Lett. **87**, 194108 (2005).
[9] R. Renner, Nat. Phys. **3**, 645 (2007).
[10] M. Christandl, R. König, and R. Renner, Phys. Rev. Lett. **102**, 020504 (2009).
[11] R. Renner and J. I. Cirac, Phys. Rev. Lett. **102**, 110504 (2009).
[12] 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).
[13] B. Qi, W. Zhu, L. Qian, and H. K. Lo, New J. Phys. **12**, 103042 (2010).
[14] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, arXiv:1210.6216.
[15] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).
[16] M. Navascués, F. Grosshans, and A. Acín, Phys. Rev. Lett. **97**, 190502 (2006).
[17] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, Phys. Rev. Lett. **109**, 100502 (2012).
[18] N. J. Cerf, M. Lévy, and G. Van Assche, Phys. Rev. A **63**, 052311 (2001).
[19] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[20] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and Ph. Grangier, Quantum Inf. Comput. **3**, 535 (2003).
[21] L. Sheridan, T. Le, and V. Scarani, New J. Phys. **12**, 123019 (2010).
[22] A. Leverrier, E. Karpov, P. Grangier, and N. J. Cerf, New J. Phys. **11**, 115009 (2009).
[23] J. Müller-Quade and R. Renner, New J. Phys. **11**, 085006 (2009).
[24] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.110.030502 for details.
[25] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **93**, 170504 (2004).
[26] G. Van Assche, J. Cardinal, and N. J. Cerf, IEEE Trans. Inf. Theory **50**, 394 (2004).
[27] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, Phys. Rev. A **84**, 062317 (2011).
[28] R. Renner, Ph.D. thesis, ETH Zurich, 2005, arXiv:quant-ph/0512258.
[29] A. Leverrier and P. Grangier, Phys. Rev. A **81**, 062314 (2010).
[30] A. Leverrier, F. Grosshans, and P. Grangier, Phys. Rev. A **81**, 062343 (2010).
[31] A. Leverrier and N. J. Cerf, Phys. Rev. A **80**, 010102 (2009).