Composable Security Proof for Continuous-Variable Quantum Key Distribution with Coherent States

Anthony Leverrier*
Inria, EPI SECRET, B.P. 105, 78153 Le Chesnay Cedex, France
(Received 25 August 2014; revised manuscript received 10 November 2014; published 19 February 2015)

We give the first *composable* security proof for continuous-variable quantum key distribution with coherent states against collective attacks. Crucially, in the limit of large blocks the secret key rate converges to the usual value computed from the Holevo bound. Combining our proof with either the de Finetti theorem or the postselection technique then shows the security of the protocol against general attacks, thereby confirming the long-standing conjecture that Gaussian attacks are optimal asymptotically in the composable security framework. We expect that our parameter estimation procedure, which does not rely on any assumption about the quantum state being measured, will find applications elsewhere, for instance, for the reliable quantification of continuous-variable entanglement in finite-size settings.

DOI: 10.1103/PhysRevLett.114.070501 PACS numbers: 03.67.Dd, 03.67.Hk, 42.50.-p

Quantum key distribution (QKD) is a cryptographic primitive that allows two distant parties, Alice and Bob, who have access to an insecure quantum channel and an authenticated classical channel, to distill a secret key. QKD has spurred a lot of interest in the past decades, because it is arguably the first application of the field of quantum information to reach commercial maturity [1]. Despite a lot of effort invested in the theoretical analysis of QKD protocols, *composable security* [2,3] has been established for only a handful of protocols, for instance, the Bennett-Brassard 1984 protocol (BB84) [4]. This major achievement is the latest step in a series of more and more refined security proofs and improved bounds for the secret key rates. More precisely, composable security proofs have successively used an exponential version of the de Finetti theorem [5], the postselection technique [6], and an entropic uncertainty principle [7].

The situation for continuous-variable (CV) protocols is much less advanced [8]. These protocols [9,10], which do not require single-photon detectors, are particularly appealing in terms of implementation [11], but their security is still far from being completely understood. Recently, a composable security proof for a CV protocol was obtained [12–14] from an entropic uncertainty principle [15], but the protocol requires the generation of squeezed states and is only moderately tolerant to losses. Other approaches to establish the security of a protocol typically consist of two independent steps: first, a composable security proof valid against collective attacks, a restricted type of attacks where the quantum state shared by Alice and Bob's protocol displays a tensor product structure, followed by an additional argument to obtain security against general attacks. These two steps have been partially completed in the case of CV protocols: a reduction from general to collective attacks is obtained via two possible techniques, namely, a de Finetti theorem [16] and the postselection technique [17], the latter technique being more efficient but at the price of adding an unpractical symmetrization step to the protocol [18]. Unfortunately, security against collective attacks has been proved (via a Gaussian optimality argument [20]) only in the asymptotic limit, which does not say anything about composable security [21–23]. Note also that finite-size effects for CV QKD were partly explored in Ref. [24], but under a Gaussian attack assumption.

In this Letter, we give the first composable security proof valid against collective attacks for CV QKD with coherent states [25] and either direct or reverse reconciliation [27]. The postselection technique then implies composable security against general attacks. Remarkably, the secret key rate is asymptotically equal to the one assuming a Gaussian attack, which is not the case for the proof based on the uncertainty principle. This is crucial for the distribution of keys over long distances [11].

To prove this result, we develop a number of techniques including a tool for reliable tomography of the covariance matrix without making any assumption about the quantum state. By performing the parameter estimation (PE) step after error correction (EC), we improve the estimation and are able to use almost all the raw data to distill the secret key. A similar strategy was also considered for BB84 in Ref. [28]. Our only assumptions are that Alice and Bob have access to a classical authenticated channel and that their equipment is trusted: they can prepare coherent states and detect light with heterodyne detection. Our framework can easily incorporate imperfections either in the preparation or in the detection, as long as they are properly modeled. To keep the notations simple, we will, however, assume that the equipment of the legitimate parties is perfect.

Composable security.—An entanglement-based (EB) QKD protocol $\mathcal{E}$ is a completely positive trace-preserving (CPTP) map $\mathcal{E}:\mathcal{H}_A \otimes \mathcal{H}_B \to \mathcal{S}_A \otimes \mathcal{S}_B \otimes \mathcal{C}$ that takes an

arbitrary input state ρ_{AB} shared by Alice and Bob and outputs for each party a classical string S_A or S_B and some public transcript C. For a CV protocol, both $\mathcal{H}_A$ and $\mathcal{H}_B$ correspond to infinite-dimensional Fock spaces, while $\mathcal{S}_A$, $\mathcal{S}_B$, and $\mathcal{C}$ describe classical registers.

A QKD protocol should be *secure*, meaning that the output keys should be identical and secret [7]. It should also be *robust*, i.e., output nontrivial keys if there is no active attack on the quantum channel. These are actually properties of the output state of the protocol, more precisely, of $\rho_{S_A S_B E}$, which should hold for any input state [29]. The subscript E refers to the quantum register $\mathcal{H}_E$ of the adversary, and the final state is obtained by applying the map $\mathcal{E} \otimes \mathrm{id}_{\mathcal{H}_E}$ to an arbitrary purification Ψ_{ABE} of ρ_{AB}. A QKD protocol is called *correct* if $S_A = S_B$ for any strategy of the adversary, that is, any initial state of the protocol Ψ_{ABE}. A protocol is ϵ_{cor}-correct if $\Pr[S_A \neq S_B] \leq \epsilon_{\mathrm{cor}}$. Denote by $\mathcal{H}_{E'} = \mathcal{H}_E \otimes \mathcal{C}$ the space accessible to the adversary (her quantum system E and the public transcript $\mathcal{C}$). A key is called *δ-secret* if it is δ-close in trace distance to a uniformly distributed key that is uncorrelated with the eavesdropper:

$$\frac{1}{2}\|\rho_{S_A^l E'} - \omega_l \otimes \rho_{E'}\|_1 \leq \delta, \tag{1}$$

where $\rho^l_{S_A E'}$ is the state conditioned on the key length l and ω_l is the fully mixed state on classical strings of length l. If the protocol aborts, it outputs a dummy key of size 0, which is automatically secret. A QKD protocol is called ϵ_{sec}-secret if, for any attack strategy, it outputs δ-secret keys with $(1 - p_{\mathrm{abort}})\delta \leq \epsilon_{\mathrm{sec}}$, where p_{abort} is the abort probability. A QKD protocol is *ϵ-secure* if it is ϵ_{sec}-secret and ϵ_{cor}-correct with $\epsilon_{\mathrm{sec}} + \epsilon_{\mathrm{cor}} \leq \epsilon$. Since a protocol that would always abort is perfectly secure according to this definition, it is important to take into account its *robustness* ϵ_{rob}, which is the probability that the protocol aborts if the eavesdropper is inactive. In the case of a CV QKD protocol, this corresponds to a thermal bosonic channel, which is a good model for the transmission of light in an optical fiber.

Description of the CV QKD protocol $\mathcal{E}_0$.—We focus here on the EB version of the protocol, but the security of its prepare and measure version where Alice sends coherent states and Bob uses heterodyne detection follows immediately. Moreover, we present the reverse reconciliation version, which is the most useful in practice. The direct reconciliation version is easily obtained by interchanging the roles of Alice and Bob in the classical postprocessing part of the protocol. Recall that, in order to obtain security against general attacks, one would need to add another step to the protocol, involving an energy test as well as a potential symmetrization procedure.

The protocol $\mathcal{E}_0$ is sketched in Table 1 (and detailed in Supplemental Material [30]) and depends on a number of parameters: most notably, the number $2n$ of coherent states sent by Alice, the length l of the final key if the protocol did not abort, the discretization parameter d, the size of Bob's communication to Alice, $\mathrm{leak}_{\mathrm{EC}}$, during the error correction procedure, the maximum failure probabilities ϵ_{cor} and ϵ_{PE} for the EC and PE steps, respectively, some bounds on covariance matrix elements, $\Sigma_a^{\max}, \Sigma_b^{\max}, \Sigma_c^{\min}$, for the PE test to pass, and a robustness parameter ϵ_{rob}.

TABLE I. Protocol $\mathcal{E}_0$, with reverse reconciliation and parameters n, l, $\mathrm{leak}_{\mathrm{EC}}$, ϵ_{cor}, n_{PE}, ϵ_{PE}, $\Sigma_a^{\max}$, $\Sigma_b^{\max}$, $\Sigma_c^{\min}$, and d.

(1) *State preparation.*—Alice prepares $2n$ two-mode squeezed vacuum states, keeps the first half of each state, and transmits the second half to Bob through an insecure quantum channel. Alice and Bob then share a global quantum state $\rho_{\mathrm{AB}}^{\otimes(2n)}$.
(2) *Measurement.*—Alice and Bob measure their respective modes with heterodyne detection and obtain two strings $X, Y \in \mathbb{R}^{4n}$. Bob discretizes his $4n$-vector Y to obtain the m-bit string U, where $m = 4dn$; i.e., each symbol is encoded with d bits of precision.
(3) *Error correction.*—Bob sends some side information of size $\mathrm{leak}_{\mathrm{EC}}$ to Alice (syndrome of U for a linear error correcting code C agreed on in advance), and Alice outputs a guess $\hat{U}$ for the string of Bob. Bob computes a hash of U of length $\lceil \log_2(1/\epsilon_{\mathrm{cor}}) \rceil$ and sends it to Alice, who compares it with her own hash. If both hashes differ, the protocol aborts.
(4) *Parameter estimation.*—Bob sends $n_{\mathrm{PE}} = O(\log(1/\epsilon_{\mathrm{PE}}))$ bits of information to Alice that allow her to compute $\|X\|^2, \|Y\|^2$ and $\langle X, Y \rangle$, as well as γ_a, γ_b, and γ_c defined in Eqs. (3)–(5). The PE test passes if $[\gamma_a \leq \Sigma_a^{\max}] \wedge [\gamma_b \leq \Sigma_b^{\max}] \wedge [\gamma_c \geq \Sigma_c^{\min}]$; otherwise, the protocol aborts.
(5) *Privacy amplification.*—Alice and Bob apply a random universal$_2$ hash function to their respective strings, obtaining two strings S_A and S_B of size l.

Our main result quantifies the security of the protocol $\mathcal{E}_0$ in the composable security framework.

Theorem 1: The protocol $\mathcal{E}_0$ is ϵ-secure against collective attacks if $\epsilon = \sqrt{\epsilon_{\mathrm{PE}} + \epsilon_{\mathrm{cor}} + \epsilon_{\mathrm{ent}}} + 2\epsilon_{\mathrm{sm}} + \bar{\epsilon}$ and if the key length l is chosen such that

$$l \leq 2n[2\hat{H}_{\mathrm{MLE}}(U) - f(\Sigma_a^{\max}, \Sigma_b^{\max}, \Sigma_c^{\min})] - \mathrm{leak}_{\mathrm{EC}} - \Delta_{\mathrm{AEP}} - \Delta_{\mathrm{ent}} - 2\log\frac{1}{2\bar{\epsilon}}, \tag{2}$$

where $\hat{H}_{\mathrm{MLE}}(U)$ is the empirical entropy of U, $\Delta_{\mathrm{AEP}} := \sqrt{2n}[(d+1)^2 + 4(d+1)\log_2(2/\epsilon_{\mathrm{sm}}^2) + 2\log_2(2/\epsilon^2\epsilon_{\mathrm{sm}})] + 4\epsilon_{\mathrm{sm}} d/\epsilon$, $\Delta_{\mathrm{ent}} := \log_2(1/\epsilon) + \sqrt{8n\log_2^2(4n)\log(2/\epsilon_{\mathrm{sm}})}$, and f is the Holevo information between Eve and Bob's measurement result for a Gaussian state with covariance matrix parametrized by $\Sigma_a^{\max}, \Sigma_b^{\max}, \Sigma_c^{\min}$.

This secret key size should be compared to the asymptotic secret key rate assuming collective, Gaussian attacks. This can be done by assuming a passive quantum channel corresponding to a Gaussian channel with transmittance T and excess noise ξ. One needs to factor in the robustness of the protocol, that is, the probability that the PE test will not

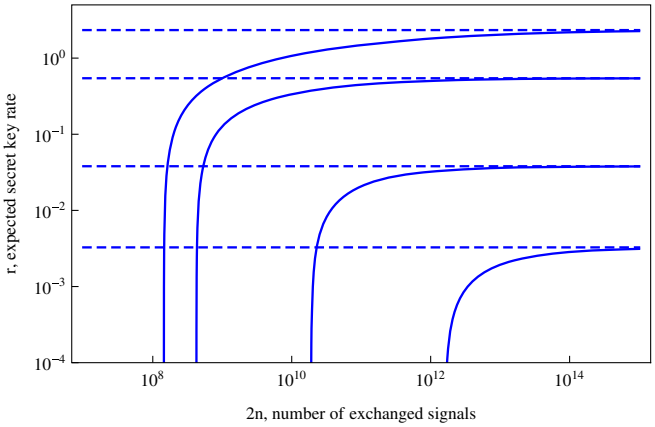

FIG. 1 (color online). Expected secret key rate $r = (1-\epsilon_{\mathrm{rob}})I/2n$ secure against collective attacks, as a function of $2n$, the number of exchanged signals. From top to bottom, the transmittance of the quantum channel corresponds to distances of 1, 10, 50, and 100 km for assumed losses of 0.2 dB per kilometer. For each distance, the expected secret key rate reaches the asymptotic value for large enough n. The modulation variance is optimized; the reconciliation efficiency is set to $\beta = 0.95$, the discretization parameter to $d = 5$ (the value of d should be optimized depending on the error correcting codes used in the reconciliation; see, e.g., [46]), the excess noise to $\xi = 0.01$, the robustness parameter to $\epsilon_{\mathrm{rob}} \leq 10^{-2}$, and the security parameter to $\epsilon = 10^{-20}$. Dashed lines correspond to the respective asymptotic expected secret key rates. Refer to the Supplemental Material for a detailed derivation of the value of the expected secret key rate.

pass in the case of a passive channel. We plot the secret key rate as a function of n for $\epsilon = 10^{-20}$ in Fig. 1. The asymptotic key rate is typically reached for n between 10^8 and 10^{11} for distances up to 50 km.

Parameter estimation.—We defer the detailed description of the protocol $\mathcal{E}_0$ and its full security proof to the Supplemental Material [30] and focus more specifically on the PE step here. A novelty of the protocol is that PE is performed *after* EC. This can be done quite efficiently, since a rough estimate of the signal-to-noise ratio of the data is in general sufficient to choose an appropriate error correcting code and proceed with the reconciliation. At the end of the EC step, Alice therefore knows the strings X and U, and it is not hard to show that, if Bob sends her a few additional bits, she can learn the values of $\|X\|^2$, $\|Y\|^2$, and $\langle X, Y\rangle$ arbitrarily well.

The goal of the PE step is to obtain a confidence region for the covariance matrix of the state $\rho_{\mathrm{AB}}^{\otimes(2n)}$. Here, one needs to be careful, because, by the time PE is performed, the state has already been measured and it does not make real sense to talk about its covariance matrix anymore. We will follow the paradigm for tomography introduced in Ref. [47] and define a quantum tomography process as a CPTP map that takes an input state $\rho^{n+k} \in \mathcal{H}^{\otimes(n+k)}$, symmetrizes it, and outputs a state $\rho^n \in \mathcal{H}^{\otimes n}$ as well as a confidence region R of $\mathcal{P}_{=}(\mathcal{H}^{\otimes n})$, the set of normalized density operators on $\mathcal{H}^{\otimes n}$ [48]. In words, it consists in measuring a subsystem of the initial state and making a prediction for the remaining state. The quality of the quantum tomography is assessed by two parameters: the probability that the prediction is false and the size of the region. A larger region means a smaller error probability but also a more pessimistic secret key rate.

An important issue concerning the tomography of a CV system is that the covariance matrix is *a priori* unbounded. Consider, for instance, the state $\sigma^{\otimes(n+k)}$ with $\sigma = (1-\epsilon)|0\rangle\langle 0| + \epsilon|N\rangle\langle N|$. The covariance matrix of σ is $\mathrm{diag}(1 + N\epsilon/2, 1 + N\epsilon/2)$, but any tomographic procedure that examines only $k \ll 1/\epsilon$ modes will conclude that the covariance matrix is close to that of the vacuum, which is clearly incorrect if $N\epsilon \gg 1$. The solution to this problem consists in first appropriately symmetrizing the state ρ^{n+k} before measuring k subsystems and inferring properties for the remaining n modes.

Ideally, the tomography of the input state ρ_{AB}^{2n} of the QKD protocol $\mathcal{E}_0$ should consist of the following steps, which involve additional parties A_1 and A_2 on Alice's side and B_1 and B_2 on Bob's side:

(1) *State symmetrization.*—Alice's $2n$ modes are processed with a random network of beam splitters and phase shifts, and Bob's modes with the conjugate network, giving a new state $\tilde{\rho}^{2n}$.

(2) *Distribution to additional players.*—Alice and Bob distribute $\tilde{\rho}_1^n$ corresponding to the first n modes of $\tilde{\rho}^{2n}$ to A_1 and B_1. Similarly, they give $\tilde{\rho}_2^n$ to A_2 and B_2.

(3) *Measurement.*—A_1 and B_1 measure $\tilde{\rho}_1^n$ with heterodyne detection and obtain two vectors $X_1, Y_1 \in \mathbb{R}^{2n}$. Similarly, A_2 and B_2 obtain $X_2, Y_2 \in \mathbb{R}^{2n}$.

(4) *Parameter estimation.*—B_1 sends some information to A_1 so that she can learn the values of $\|X_1\|^2$, $\|Y_1\|^2$, and $\langle X_1, Y_1\rangle$ and then compute a confidence region for the (averaged) covariance matrix of $\tilde{\rho}_2^n$. Similarly, A_2 computes a confidence region for that of $\tilde{\rho}_1^n$.

By averaged covariance matrix, we mean the three real values Σ_a, Σ_b, and Σ_c defined by $\Sigma_{a/b} := (1/2n)\sum_{i=1}^{n}(\langle q_{A/B_i}^2\rangle + \langle p_{A/B,i}^2\rangle)$ and $\Sigma_c := (1/2n)\sum_{i=1}^{n}(\langle q_{A,i}q_{B,i}\rangle - \langle p_{A,i}p_{B,i}\rangle)$, where $q_{A,i}$ is the quadrature operator $(1/\sqrt{2})(\hat{a}_i + \hat{a}_i^{\dagger})$ for the ith mode of Alice, for instance.

An interesting feature of this PE procedure is that A_1 and A_2 can, respectively, estimate the covariance matrices of $\tilde{\rho}_2^n$ and $\tilde{\rho}_1^n$, meaning that a secret key can be distilled from both halves of the state. In other words, no raw key is wasted because of parameter estimation. While it is clear that this scheme is rather impractical, one can show that it can nevertheless be efficiently simulated by Alice, without any need for symmetrization or for additional parties.

In fact, if Alice learns the values of $\|X\|^2$, $\|Y\|^2$, and $\langle X, Y\rangle$, she can compute $\gamma_a, \gamma_b, \gamma_c$ as follows:

$$\gamma_a := \frac{1}{2n}\left[1 + 2\sqrt{\frac{\log(36/\epsilon_{\mathrm{PE}})}{n}}\right]\|X\|^2 - 1, \tag{3}$$

$$\gamma_b := \frac{1}{2n}\left[1 + 2\sqrt{\frac{\log(36/\epsilon_{\mathrm{PE}})}{n}}\right]\|Y\|^2 - 1, \tag{4}$$

$$\gamma_c := \frac{1}{2n}\langle X, Y\rangle - 5\sqrt{\frac{\log(8/\epsilon_{\mathrm{PE}})}{n^3}}(\|X\|^2 + \|Y\|^2). \tag{5}$$

We are now in a position to define the parameter estimation test and bound its failure probability (proven in the Supplemental Material [30]).

Theorem 2: The probability that the parameter estimation test passes, that is, $[\gamma_a \le \Sigma_a^{\max}] \wedge [\gamma_b \le \Sigma_b^{\max}] \wedge [\gamma_c \ge \Sigma_c^{\min}]$ and that Eve's information $\chi(U;E)$ computed for the Gaussian state with the covariance matrix characterized by $\Sigma_a^{\max}$, $\Sigma_b^{\max}$, and $\Sigma_c^{\min}$ is underestimated, is upper bounded by ϵ_{PE}.

Here the Holevo information $\chi(U;E)$ is upper bounded by $f(\Sigma_a^{\max}, \Sigma_b^{\max}, \Sigma_c^{\min}) := g[(\nu_1 - 1)/2] + g[(\nu_2 - 1)/2] - g[(\nu_3 - 1)/2]$, where ν_1 and ν_2 are the symplectic eigenvalues of the covariance matrix

$$\begin{bmatrix} \Sigma_a^{\max}\mathbb{1}_2 & \Sigma_c^{\min}\sigma_z \\ \Sigma_c^{\min}\sigma_z & \Sigma_b^{\max}\mathbb{1}_2 \end{bmatrix}, \tag{6}$$

$\nu_3 = \Sigma_a^{\max} - (\Sigma_c^{\min})^2/(1 + \Sigma_b^{\max})$, $\sigma_z = \mathrm{diag}(1, -1)$, and $g(x) := (x+1)\log_2(x+1) - x\log_2(x)$.

Once we are able to analyze the PE test, the rest of the security proof follows in a rather straightforward fashion: see the Supplemental Material for all the details [30]. It should be noted that the assumption of collective attacks was not used in the PE step: this is because the symmetrization breaks the tensor product of the state. However, we crucially rely on the collective attack assumption when exploiting the asymptotic equipartition property of the smooth min-entropy, which is the quantity of interest to analyze the success of the privacy amplification step.

A security proof against general attacks.—So far, we have restricted the analysis to collective attacks. For CV QKD, there are two known techniques to obtain a full security proof from one holding against collective attacks: an exponential version of the de Finetti theorem [16] and the postselection technique [17]. The former technique directly applies here and can be used to upgrade the protocol $\mathcal{E}_0$ to a slightly more complicated one (including an energy test and a random permutation) that is provably $\tilde{\epsilon}$-secure against general attacks, but with $\tilde{\epsilon} \gg \epsilon$, provided the key length is adequately shortened. However, while this provides composable security CV QKD with coherent states against general attacks, it does not give very good finite-key estimates. The postselection technique is better but still falls short on providing useful finite-size key estimates. Indeed, in order to apply it, one needs to add an energy test which depends on a small parameter ϵ_{test}, and if the protocol $\mathcal{E}_0$ was ϵ-secure against collective attacks, the new protocol is $\tilde{\epsilon}$-secure against general attacks where $\tilde{\epsilon} = \epsilon 2^{O(\log^4(n/\epsilon_{\mathrm{test}}))} + 2\epsilon_{\mathrm{test}}$, which is prohibitive in practice. Moreover, in the case of reverse reconciliation, it seems that the current postselection technique requires an additional symmetrization step for the classical data, which have complexity $\Theta(n^2)$. Whether or not this symmetrization can be simulated, as was the case in the PE step, is left as an interesting open question.

Conclusion.—We have provided a composable security proof of a CV QKD protocol using coherent states valid against collective attacks. This was the missing step to establish the security of such protocols against general attacks in the composable security framework. The bounds we obtained are compatible with state-of-the-art experiments. For protocols with direct reconciliation, this directly gives a composable security proof against general attacks. For reverse reconciliation, which is required to achieve long distances, an additional symmetrization step provides the same level of security. Further work will be needed to improve the current reductions from general to collective attacks, which should be possible since the current techniques do not exploit all the symmetries of the protocols.

We expect our parameter estimation procedure to find applications in the field of continuous-variable entanglement. Indeed, most criteria for detecting CV entanglement are based on the covariance matrix [49], and, to our knowledge, our procedure gives the first robust estimation of the covariance matrix of an unknown quantum state without relying on any assumption such as the Gaussian nature of the state.

I thank Fabian Furrer and Philipe Grangier, who provided very useful comments on a preliminary version of this manuscript. I am especially grateful to Marco Tomamichel for enlightening discussions about smooth entropies and the asymptotic equipartition property.

*anthony.leverrier@inria.fr

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[2] R. Canetti, in *Proceedings of the 42nd IEEE Symposium on Foundations of Computer Science* (IEEE, New York, 2001), pp. 136–145.

[3] J. Müller-Quade and R. Renner, New J. Phys. **11**, 085006 (2009).

[4] C. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), Vol. 175.

[5] R. Renner, Nat. Phys. **3**, 645 (2007).
[6] M. Christandl, R. König, and R. Renner, Phys. Rev. Lett. **102**, 020504 (2009).
[7] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Nat. Commun. **3**, 634 (2012).
[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).
[9] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[10] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **93**, 170504 (2004).
[11] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Nat. Photonics **7**, 378 (2013).
[12] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, Phys. Rev. Lett. **109**, 100502 (2012).
[13] F. Furrer, Phys. Rev. A **90**, 042325 (2014).
[14] T. Gehring, V. Händchen, J. Duhme, F. Furrer, T. Franz, C. Pacher, R. F. Werner, and R. Schnabel, arXiv:1406.6174.
[15] M. Berta, M. Christandl, F. Furrer, V. B. Scholz, and M. Tomamichel, J. Math. Phys. (N.Y.) **55**, 122205 (2014).
[16] R. Renner and J. I. Cirac, Phys. Rev. Lett. **102**, 110504 (2009).
[17] A. Leverrier, R. García-Patrón, R. Renner, and N. J. Cerf, Phys. Rev. Lett. **110**, 030502 (2013).
[18] The postselection technique should not be mistaken with the postselection of data in certain protocols [19].
[19] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, Phys. Rev. Lett. **89**, 167901 (2002).
[20] M. M. Wolf, G. Giedke, and J. I. Cirac, Phys. Rev. Lett. **96**, 080502 (2006).
[21] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).
[22] M. Navascués, F. Grosshans, and A. Acín, Phys. Rev. Lett. **97**, 190502 (2006).
[23] S. Pirandola, S. L. Braunstein, and S. Lloyd, Phys. Rev. Lett. **101**, 200504 (2008).
[24] A. Leverrier, F. Grosshans, and P. Grangier, Phys. Rev. A **81**, 062343 (2010).
[25] We note that coherent states can also be used in BB84 implementations, for instance, in decoy-state protocols, and that composable security has been proved in Ref. [26].
[26] M. Hayashi and R. Nakayama, New J. Phys. **16**, 063009 (2014).
[27] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. Cerf, and P. Grangier, Nature (London) **421**, 238 (2003).
[28] C.-H. Fung, X. Ma, and H. Chau, Phys. Rev. A **81**, 012318 (2010).
[29] In this Letter, we denote by $\rho_{\mathcal{H}}$ the marginal of the state ρ restricted to subspace $\mathcal{H}$.
[30] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.114.070501 for the basic definitions related to the composable security of QKD, the complete description of the QKD protocol E0, the details on how to compute the expected secret key rate, the tools needed for the security proof, the ideas behind the Parameter Estimation procedure and details on how to upgrade E0 to a protocol provably secure against general attacks, which includes Refs. [31–45].
[31] J. Lodewyck *et al.*, Phys. Rev. A **76**, 042305 (2007).
[32] A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, Phys. Rev. A **77**, 042325 (2008).
[33] G. Van Assche, J. Cardinal, and N. J. Cerf, IEEE Trans. Inf. Theory **50**, 394 (2004).
[34] I. Kremer, N. Nisan, and D. Ron, in *Proceedings of the 27th Annual ACM Symposium on Theory of Computing, Las Vegas, 1995* (ACM, New York, 1995), pp. 596–605.
[35] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).
[36] R. Renner and R. König, in *Theory of Cryptography* (Springer, New York, 2005), pp. 407–425.
[37] R. Renner, Int. J. Quantum. Inform. **06**, 1 (2008).
[38] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, IEEE Trans. Inf. Theory **57**, 5524 (2011).
[39] R. König, R. Renner, and C. Schaffner, IEEE Trans. Inf. Theory **55**, 4337 (2009).
[40] M. Tomamichel, R. Colbeck, and R. Renner, IEEE Trans. Inf. Theory **55**, 5840 (2009).
[41] M. Berta, F. Furrer, and V. B. Scholz, arXiv:1107.5460.
[42] M. Tomamichel, Ph. D. thesis, Department of Physics, ETH Zurich, 2012.
[43] L. Paninski, Neural Comput. **15**, 1191 (2003).
[44] A. Antos and I. Kontoyiannis, Random Struct. Algorithms **19**, 163 (2001).
[45] B. Laurent and P. Massart, Ann. Stat. **28**, 1302 (2000).
[46] P. Jouguet, D. Elkouss, and S. Kunz-Jacques, Phys. Rev. A **90**, 042329 (2014).
[47] M. Christandl and R. Renner, Phys. Rev. Lett. **109**, 120403 (2012).
[48] The superscript n for ρ^n should not be interpreted as saying that the state has an independent and identically distributed structure nor that ρ^n corresponds to a marginal state of ρ^{n+k}; it is merely a remainder of the size of Hilbert space it lives in.
[49] L.-M. Duan, G. Giedke, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **84**, 2722 (2000).