Continuous Variable Quantum Key Distribution: Finite-Key Analysis of Composable Security against Coherent Attacks

F. Furrer,[1,*] T. Franz,[1] M. Berta,[2] A. Leverrier,[2] V. B. Scholz,[1] M. Tomamichel,[2] and R. F. Werner[1]

[1]*Institut für Theoretische Physik, Leibniz Universität Hannover, Appelstraße 2, 30167 Hannover, Germany*

[2]*Institut für Theoretische Physik, ETH Zürich, 8093 Zürich, Switzerland*

(Received 10 January 2012; revised manuscript received 21 June 2012; published 5 September 2012)

We provide a security analysis for continuous variable quantum key distribution protocols based on the transmission of two-mode squeezed vacuum states measured via homodyne detection. We employ a version of the entropic uncertainty relation for smooth entropies to give a lower bound on the number of secret bits which can be extracted from a finite number of runs of the protocol. This bound is valid under general coherent attacks, and gives rise to keys which are composably secure. For comparison, we also give a lower bound valid under the assumption of collective attacks. For both scenarios, we find positive key rates using experimental parameters reachable today.

DOI: 10.1103/PhysRevLett.109.100502 PACS numbers: 03.67.Dd, 03.67.Hk

Quantum key distribution (QKD) is one of the first ideas from quantum information theory for turning quantum paradoxes into applications, see Ref. [1] and references therein. The task in QKD is to generate a shared key, secret from any eavesdropper (Eve), between two distant parties (Alice and Bob) using communication over a public quantum channel and an authenticated classical channel. Many different implementations of QKD have been proposed, each one with individual strengths and weaknesses. Early proposals were based on exchanging qubits, and are part of the family of discrete variable (DV) QKD protocols. Continuous variable (CV) protocols have later been proposed and offer the possibility to use standard telecom technologies (see Ref. [2] and references therein), in particular, they do not require photon counters.

A generic QKD protocol starts with the distribution of, say, N quantum states between the honest parties which are then measured according to the rules of the protocol. A certain number k of the measurement outcomes is then used to estimate Eve's information about the remaining $n = N - k$ data points from which a key of length ℓ bits is generated by classical postprocessing. The goal of a finite-key security analysis is to prove that the key is secure against any wiretapping strategy of Eve, up to a small failure probability. This is in contrast to the study of asymptotic rates in which perfect security in the limit for N to infinity is considered.

Eve's knowledge can be bounded by the probability that she correctly guesses Alice's measurement outcomes. This is expressed by the conditional smooth min-entropy [3] of the data from which the key is generated given Eve's quantum system. This ensures composable security [4]; i.e., the protocol can securely be combined with other composable secure cryptographic protocols. Since the actual state is not known, the smooth min-entropy has to be bounded for the worst case compatible with the observed measurement data. This is in general a hard task and often simplified by additional assumptions about the power of the eavesdropper. Instead of allowing the most general, *coherent* attack on the quantum communication between Alice and Bob, the eavesdropper is often restricted to *collective* attacks, meaning that every signal is attacked with the same quantum operation. Under this assumption, Alice and Bob can employ state tomography to bound Eve's information and to ensure security. In the case of DV QKD, these security proofs can then often be lifted to security proofs against coherent attacks using the exponential de Finetti theorems [5] or the postselection technique [6].

Most security analyses for CV protocols neglect finite-key effects and consider asymptotic rates by using the Devetak-Winter formula [7] (see Ref. [8] for the infinite-dimensional generalization). We are only aware of [9], where a first finite-key analysis for specific protocols under the assumption of collective Gaussian attacks was provided. Security against coherent attacks was considered in Ref. [10,11] based on entanglement purification protocols, but without a quantitive analysis. The transfer of the exponential de Finetti technique to the infinite-dimensional setting is very subtle. This is because exponential de Finetti theorems in general do not hold in infinite-dimensional systems [12], but only under additional assumptions [13]. It is often argued that, using these results, much of the DV theory can be transferred to CV systems. Unfortunately, this approach provides only pessimistic finite-key rate estimates (c.f. [14]).

Recently, a more direct approach to prove DV QKD secure against coherent attacks was presented in Ref. [15], which is based on an entropic uncertainty relation with quantum side information for smooth entropies [16]. This uncertainty relation gives a bound on Eve's information about Alice's measurement outcomes in terms of the correlation between Alice and Bob. The relation between security in QKD and uncertainty relations has also been employed in Refs. [17,18]. Based on the recent

extension of the smooth entropy formalism to the infinite-dimensional setting [8,19], it is the objective of this Letter to apply the above reasoning to an entanglement based CV protocol using two-mode squeezed vacuum states measured via homodyne detection.

Security definition and key rates.—A generic QKD protocol between two honest parties, Alice (A) and Bob (B) either aborts or outputs a key which consists of strings S_A and S_B on Alice's and Bob's side, respectively. We denote by E the information which is wiretapped during the run of the protocol by an attack on the quantum channel. For CV systems this is modeled on an infinite-dimensional Hilbert space. The state of S_A and E can be described as a classical quantum state

$$\omega_{S_A E} = \sum_s |s\rangle\langle s| \otimes \omega_E^s, \tag{1}$$

where ω_E^s are states on Eve's system. Three requirements have to be fulfilled by an ideal protocol: correctness, secrecy, and robustness. Correctness is achieved when the outputs on Alice's and Bob's side agree, $S_A = S_B$. Secrecy of a key means that S_A is uniformly distributed and independent of E and thus given by $\omega^{\mathrm{id}}_{S_A E} = \tau_{S_A} \otimes \sigma_E$, with τ_{S_A} the uniform mixture of keys, and σ_E an arbitrary state on the E system. A protocol is called secure if it is both correct and secret. Finally, we call an ideal protocol robust if it never aborts when Eve is passive.

In reality, we can only hope to achieve an almost ideal protocol. For small parameters ϵ_c, ϵ_s and an abortion probability p_{abort}, we require that the protocol is ϵ_c-correct, i.e., $\Pr[S_A \neq S_B] \leq \epsilon_c$, and that the protocol is ϵ_s-secret, i.e., $(1 - p_{\mathrm{abort}})\frac{1}{2}\|\omega_{S_A E} - \tau_{S_A} \otimes \omega_E\| \leq \epsilon_s$. Note that a protocol which always aborts is secure. Thus we may impose an additional requirement on the robustness, e.g., $p_{\mathrm{abort}} < 1$. This security definition also ensures that the protocol is secure in the framework of composable security [4], in which different cryptographic protocols can be combined without compromising the overall security. We note that this is not the case for security definitions which are based on a small value of the mutual information between the eavesdropper and the key [20].

The measurement step of a QKD protocol produces a pair of raw keys, X_A and X_B, held by Alice and Bob. If the protocol does not abort, the secret keys S_A and S_B are extracted using classical error correction and privacy amplification schemes. We do not discuss the error correction scheme here and simply assume that it will leak ℓ_{EC} bits of information about the key to the eavesdropper. The correctness is checked using a hash function evaluated on both resulting strings which leads to an additional leakage of order $O(\log\frac{1}{\epsilon_c})$ [15].

In the privacy amplification step, two-universal hash functions are used to compress the raw key to the final length of ℓ bits. Roughly speaking, this reduces Eve's knowledge about Alice's key by $\ell_{\mathrm{raw}} - \ell$ bits if ℓ_{raw} is the length of X_A measured in bits. Hence, choosing sufficiently small ℓ ensures that Eve has no information about the resulting bit strings and the key is independent of E. Formally, Eve's uncertainty (or lack of knowledge) is measured in terms of the probability that she can guess Alice's raw key X_A, i.e., the conditional min-entropy $H_{\min}(X_A|E)$ (see Ref. [21], I for a formal definition). In particular, the resulting key is ϵ_s-secret if [3,8,22]

$$\ell \lesssim H^{\epsilon}_{\min}(X_A|E)_\omega - \ell_{\mathrm{EC}} - O\left(\log\frac{1}{\epsilon_s \epsilon_c}\right), \tag{2}$$

where $\epsilon \propto \epsilon_s / p_{\mathrm{abort}}$. Here, the smooth min-entropy, $H^{\epsilon}_{\min}(X_A|E)$, is the maximization of the min-entropy over states which are ϵ close to $\omega_{X_A E}$, where $\omega_{X_A E}$ denotes the joint state prior to the classical postprocessing conditioned on the event that the protocol does not abort. We derive lower bounds on this entropy for the following protocol.

The protocol.—The analysis of coherent and collective attacks can widely be treated in parallel. We consider a trusted source located in Alice's lab that produces an entangled state by mixing two squeezed vacuum states on a balanced beam splitter. We assume that each beam consists of only one bosonic mode. Alice sends one beam to Bob whereupon both perform a homodyne measurement. They choose uniformly at random between two canonically conjugated quadrature observables, amplitude and phase, such that Alice's and Bob's outcomes are maximally correlated whenever their choices agree. In the case of collective attacks they additionally perform measurements to estimate the covariance matrix. We further assume that the states generated by the source have tensor product form and that the probability that Alice measures an amplitude or phase quadrature is larger than α ($\hbar = 1$) is bounded by p_α. This is possible since the source is trusted and located in Alice's lab.

After all measurements are performed, the two parties reveal their measurement choices. In the case of coherent attacks, they discard the data in which they have measured different quadratures ending up with a string of N measurement results. Then, they divide the continuous outcome range of the quadrature measurements into intervals $(-\infty, -\alpha + \delta], (-\alpha + \delta, -\alpha + 2\delta], \ldots, (\alpha - \delta, \infty)$ where we assume for simplicity that $2\alpha/\delta \in \mathbb{N}$. We denote the outcome alphabet by $\mathcal{X} = \{1, 2, ..., 2\alpha/\delta\}$. A random sample X_A^{pe}, $X_B^{\mathrm{pe}} \in \mathcal{X}^k$ of length k is used for parameter estimation, in which they check the quality of their correlation by computing the average distance $d(X_A^{\mathrm{pe}}, X_B^{\mathrm{pe}}) = \frac{1}{k}\sum_{i=1}^k |X_{A,i}^{\mathrm{pe}} - X_{B,i}^{\mathrm{pe}}|$ where $X_A^{\mathrm{pe}} = (X_{A,i}^{\mathrm{pe}})_{i=1}^k$ and $X_B^{\mathrm{pe}} = (X_{B,i}^{\mathrm{pe}})_{i=1}^k$. If $d(X_A^{\mathrm{pe}}, X_B^{\mathrm{pe}})$ is smaller than d_0 they proceed and otherwise they abort the protocol. In case the test is passed, they use the remaining data X_A, $X_B \in \mathcal{X}^n$ ($n = N - k$) as the raw key and execute the error correction and privacy amplification protocol as discussed in the paragraph before. For collective attacks, the strings $X_A \in \mathcal{X}^n$ and $X_B \in \mathcal{X}^n$ are generated as for coherent attacks but

the remaining data (before the binning) is used to estimate the covariance matrix. This also includes the one in which Alice and Bob measured different quadratures.

Analysis for coherent attacks.—The goal is to bound the smooth min-entropy conditioned on the event that the protocol does not abort. For that we use an infinite-dimensional version of the entropic uncertainty relation for smooth entropies with side information [8], combining the uncertainty principle for complementary measurements with monogamy of entanglement. It states that Eve's information about the measurement outcomes X_A can be bounded by using the complementary of the measurements and the correlation between X_A and X_B. In particular, if Alice and Bob are highly correlated after measuring, e.g., the phase quadrature, then Eve's knowledge about the outcome of the amplitude measurement is nearly zero, since the observables are maximally complementary. We measure this correlation strength by the smooth max-entropy $H^{\epsilon}_{\max}(X_A|X_B)$, which characterizes the amount of information Alice has to send Bob to retrieve X_A. This leads to the bound ([21], II)

$$H^{\epsilon}_{\min}(X_A|E)_{\omega} \geq n \log \frac{1}{c(\delta)} - H^{\epsilon'}_{\max}(X_A|X_B)_{\omega}, \qquad (3)$$

where $c(\delta)$ is the overlap of the two conjugated quadrature measurements on an interval of length δ which is well approximated by $c(\delta) \approx \delta^2/(2\pi)$ for small δ. By log we denote the binary logarithm. Equation (3) assumes a uniformly random choice of measurement settings. Since projectors onto intervals $(-\infty, -\alpha]$ and $[\alpha, \infty)$ would lead to a trivial state-independent uncertainty relation, the probability of this event has to be estimated using p_{α}. In Eq. (3) this is included in the change of the smoothing parameter from ϵ to ϵ' ([21], II).

This reduces the problem to upper bounding the smooth max-entropy between X_A and X_B, which can be done by $n \log \gamma(d(X_A, X_B))$, where γ is a function arising from a large deviation consideration ([21], III). Using sampling theory, the quantity $d(X_A, X_B)$ can then, with high probability, be estimated by $d(X_A^{\mathrm{pe}}, X_B^{\mathrm{pe}})$ plus a correction μ, which quantifies its statistical deviation to $d(X_A, X_B)$ and depends on p_{α}, k, and n. Since the protocol aborts if $d(X_A^{\mathrm{pe}}, X_B^{\mathrm{pe}}) > d_0$, we obtain the following formula for the key length ([21], IV): *For parameters* k, p_{α}, δ, d_0, an ϵ_s-secret key of length

$$\ell = n\left[\log \frac{1}{c(\delta)} - \log \gamma(d_0 + \mu)\right] - \ell_{\mathrm{EC}} - O\left(\log \frac{1}{\epsilon_s \epsilon_c}\right).$$

can be extracted.

We assume that the source in Alice's lab is trusted and that her measurement device is described by projections onto two canonical variables. Note that the measurement device on Bob's side need not to be trusted, except that measurements on different signals commute. Hence, the additional reference signal (local oscillator) used by Bob for homodyne detection is covered by our security analysis. Placing the trusted source in Alice's lab also implies that the analysis is not compatible with reverse reconciliation.

We calculate the correlation between X_A and X_B under the assumption of an identically and independently distributed source producing states with an input squeezing of 11 dB and antisqueezing of 16 dB. Squeezing at this level has been realized in an experiment at 1550 nm [23]. Our noise model consists of loss and excess noise, where the latter is set to be 1% as it is mainly due to the classical data acquisition ([21], V). The leakage term is estimated assuming an error correction efficiency of 0.95 [24] (see Ref. [21], IV for details). In Fig. 1 the resulting key rates ℓ/N (number of extractable secure bits per signal) are plotted for different symmetric losses. We have set security parameters $\epsilon_s = \epsilon_c = 10^{-6}$ such that the leakage per bit is $\epsilon/\ell \lesssim 10^{-11}$ for the relevant values of N [15]. The optimization over the other free parameters is done numerically for each N. Typical values for $N = 10^9$ are $k = 10^8$, $\alpha = 52$ and $\delta = 0.01$.

Analysis for collective attacks.—Under the assumption of collective attacks, the state between Alice, Bob, and Eve has tensor product structure, $\omega_{ABE}^{\otimes N}$, enabling statistical estimations of the covariance matrix of ω_{AB}. However, we do not cover the statistical details here and simply introduce confidence sets $\mathcal{C}_{\epsilon_{\mathrm{pe}}}$, which ensure that whenever the protocol does not abort the covariance matrix Γ_{AB} of ω_{AB} lies in $\mathcal{C}_{\epsilon_{\mathrm{pe}}}$ with probability at least $1 - \epsilon_{\mathrm{pe}}$. Hence, we have to give a lower bound on the smooth min-entropy $H^{\epsilon}_{\min}(X_A|E)_{\omega^{\otimes n}}$ over all states with a covariance matrix $\Gamma_{AB} \in \mathcal{C}_{\epsilon_{\mathrm{pe}}}$. The smooth min-entropy is evaluated on the classical quantum state $\omega_{X_A E}$ which is obtained from ω_{AB} by taking a purification ω_{ABE} and applying the discretized quadrature measurement on the A system.

We employ the quantum equipartition property of the smooth min-entropy [25] for infinite-dimensional systems [19], stating that for large n, $H^{\epsilon}_{\min}(X_A|E)_{\omega^{\otimes n}}$ approaches the conditional von Neumann entropy $H(X_A|E)_{\omega}$. More precisely, we have

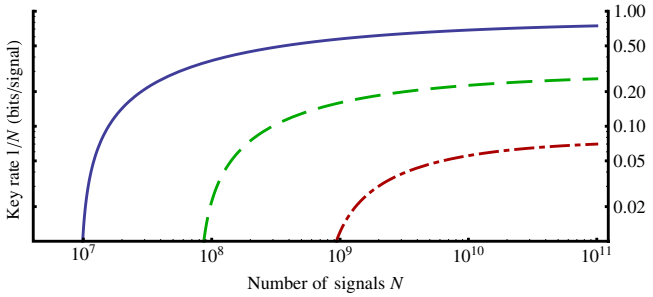

FIG. 1 (color online). Key rate ℓ/N in bits per signal against coherent attacks for an input squeezing of 11 dB , antisqueezing of 16 dB and additional symmetric losses of 0% (solid line), 4% (dashed line) and 6% (dash-dotted line). We assumed an error correction efficiency of 0.95 and set $\epsilon_s = \epsilon_c = 10^{-6}$.

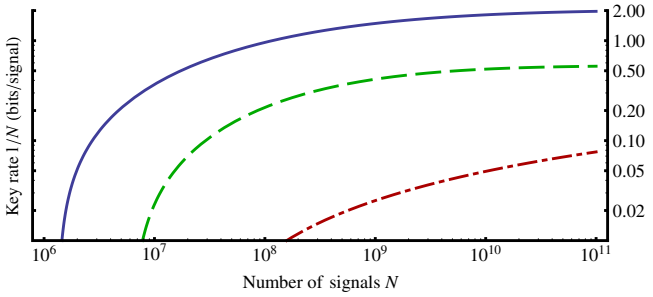

FIG. 2 (color online). Key rate ℓ/N in bits per signal against collective Gaussian attacks for losses of 0% (solid line), 15% (dashed line), 25% (dash-dotted line). Squeezing strength, error correction efficiency, and security parameters are chosen as in the case of coherent attacks.

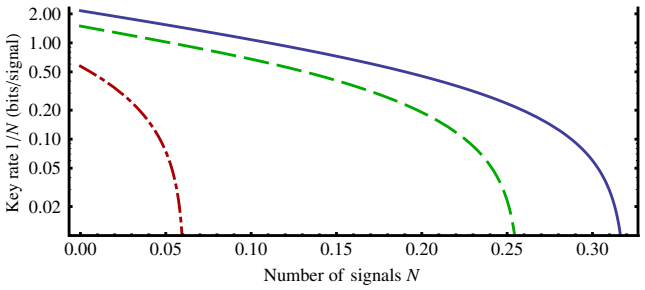

FIG. 3 (color online). Key rate ℓ/N versus losses secure against coherent attacks at $N = 10^9$ (dash-dotted line), collective Gaussian attacks at $N = 10^9$ (dashed line), and the Devetak-Winter rate [7] for perfect information reconciliation (solid line). Squeezing strength, error correction efficiency, and security parameters are chosen as in the case of coherent attacks.

$$H_{\min}^{\epsilon}(X_A|E)_{\omega^{\otimes n}} \geq nH(X_A|E)_{\omega} - \sqrt{n}\Delta, \tag{4}$$

where Δ is a function of ϵ, δ and α ([21], VI). Using that the minimum of $H(X_A|E)_{\omega}$ over all states with a fixed covariance matrix Γ_{AB} is attained for the corresponding Gaussian state $\omega^{\Gamma_{AB}}$ ([21], VII and [26]), we get the following formula for the key length.

For *parameters* k, α, δ, an $(\epsilon_s + \epsilon_{\text{pe}})$-secret key of length

$$n \inf_{\Gamma \in \mathcal{C}_{\epsilon_{\text{pe}}}} H(X_A|E)_{\omega^{\Gamma}} - \sqrt{n}\Delta - \ell_{\text{EC}} - O\left(\log \frac{1}{\epsilon_s \epsilon_c}\right)$$

can be extracted assuming collective attacks.

To evaluate this finite-key bound numerically, we need explicit expressions for the confidence sets. For this, we use results from [9], which assumes collective Gaussian attacks. We computed the key rates ℓ/N in Fig. 2 for the same squeezing strength and loss model as in the case of coherent attacks. Note that since the key rate is in bits per signal, it can be larger than 1. The detailed calculation of $H(X_A|E)_{\omega^{\Gamma}}$ can be found in ([21], VIII). For simplicity, we assumed a constant binning of δ over the entire outcome range ($\alpha = \infty$). In contrast to the case of coherent attacks, reverse reconciliation is possible and can increase the key rate essentially if asymmetric losses are assumed (which we do not discuss here). In Fig. 3, we plotted the key rate for coherent and collective Gaussian attacks in dependence of the losses, and compare them with the Devetak-Winter rate [7,8] for perfect error correction.

Discussion and outlook.—We provided a finite-key security analysis for a CV QKD protocol and obtain a composable secure positive key rate against coherent attacks for experimentally feasible parameters. We compare it with key rates computed under the assumption of collective Gaussian attacks and find that they are significantly higher. This is because the applied entropic uncertainty relation, Eq. (3), is not tight for the considered state, which might be improved by a state dependent version thereof. Our results for collective attacks suggest that an extension of the postselection technique to infinite-dimensional systems (see Ref. [27] for a proposal) is desirable. In order to relax the assumptions in the security proof against coherent attacks, it would be interesting to study the overlap for more realistic models of the quadrature measurements, which may include a continuum of modes. Moreover, our arguments might also be applicable to other CV QKD schemes [28,29].

We thank R. Renner for suggesting this work, and R. García-Patrón and I. Cirac for helpful discussions. F. F. acknowledges support from the LUH GRK 1463. T. F., V. B. S., and R. F. W. acknowledge support from the DFG (Grant No. WE-1240/12-1), BMBF project QuORep, EU project Q-ESSENCE, and the research cluster QUEST. M. B. is supported by the SNF (Grant No. PP00P2-128455), and the DFG (Grants No. CH 843/1-1 and No. CH 843/2-1). A. L., M. B., V. B. S., and M. T. are supported by the SNF through the National Centre of Competence in Research "Quantum Science and Technology."

*fabian.furrer@itp.uni-hannover.de

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[2] 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).
[3] R. Renner, Security of Quantum Key Distribution, Ph.D. thesis, ETH Zurich, 2005.
[4] R. Canetti, in *Proc. IEEE Int. Conf. on Cluster Comput.* (IEEE, New York, 2001), pp. 136–145.
[5] R. Renner, Nature Phys. **3**, 645 (2007).
[6] M. Christandl, R. König, and R. Renner, Phys. Rev. Lett. **102**, 020504 (2009).
[7] I. Devetak and A. Winter, Proc. R. Soc. A **461**, 207 (2005).
[8] M. Berta, F. Furrer, and V. B. Scholz, arXiv:1107.5460v1.
[9] A. Leverrier, F. Grosshans, and P. Grangier, Phys. Rev. A **81**, 062343 (2010).

[10] D. Gottesman and J. Preskill, Phys. Rev. A **63**, 022309 (2001).
[11] G. Van Assche, S. Iblisdir, and N. J. Cerf, Phys. Rev. A **71**, 052304 (2005).
[12] M. Christandl, R. König, G. Mitchison, and R. Renner, Commun. Math. Phys. **273**, 473 (2007).
[13] R. Renner and J. I. Cirac, Phys. Rev. Lett. **102**, 110504 (2009).
[14] F. Pedrocchi, Master's thesis, ETH Zurich, 2008.
[15] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Nature Commun. **3**, 634 (2012).
[16] M. Tomamichel and R. Renner, Phys. Rev. Lett. **106**, 110506 (2011).
[17] F. Grosshans and N. J. Cerf, Phys. Rev. Lett. **92**, 047905 (2004).
[18] M. Koashi, J. Phys. Conf. Ser. **36**, 98 (2006).
[19] F. Furrer, J. Aberg, and R. Renner, Commun. Math. Phys. **306**, 165 (2011).
[20] R. Renner and R. König, in *Proc. of TCC, LNCS* (Springer, New York, 2005), Vol. 3378, pp. 407–425.
[21] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.109.100502 for details.
[22] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, IEEE Trans. Inf. Theory **57**, 5524 (2011).
[23] T. Eberle, V. Händchen, J. Duhme, T. Franz, R. F. Werner, and R. Schnabel, Phys. Rev. A **83**, 052329 (2011).
[24] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, Phys. Rev. A **84**, 062317 (2011).
[25] M. Tomamichel, R. Colbeck, and R. Renner, IEEE Trans. Inf. Theory**55**, 5840 (2009).
[26] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).
[27] A. Leverrier, E. Karpov, P. Grangier, and N. J. Cerf, New J. Phys. **11**, 115009 (2009).
[28] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[29] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **93**, 170504 (2004).