de Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography

R. Renner
Institute for Theoretical Physics, ETH Zurich, CH-8093 Zurich, Switzerland

J. I. Cirac
Max-Planck-Institut für Quantenoptik, Hans-Kopfermann-Str. 1, D-85748 Garching, Germany
(Received 20 October 2008; published 19 March 2009)

We show that the quantum de Finetti theorem holds for states on infinite-dimensional systems, provided they satisfy certain experimentally verifiable conditions. This result can be applied to prove the security of quantum key distribution based on weak coherent states or other continuous variable states against general attacks.

DOI: 10.1103/PhysRevLett.102.110504 PACS numbers: 03.67.Dd

Composite quantum systems are, in general, very hard to analyze. This is due to the exponential growth of the number of parameters required for their description with N, the number of subsystems. Under certain symmetry assumptions, however, the analysis may be vastly simplified. This occurs, for instance, whenever the state of the whole system, ρ^N, is invariant under permutations of the subsystems. In such a case, the quantum version [1,2] of de Finetti's classical representation theorem [3] enables us to approximate ρ^N by a convex combination of density operators which have an independent and identically distributed (i.i.d.) structure $\sigma^{\otimes N}$ on most subsystems [4]. I.i.d. states can be easily parametrized (they are characterized by the state σ of a single subsystem), and a huge variety of tools are available to handle them.

Quantum key distribution (QKD) [5,6] represents a relevant scenario where permutation symmetry naturally appears and the quantum de Finetti representation is of utmost importance. Roughly speaking, QKD is the art of establishing a secret key between two distant parties, traditionally called *Alice* and *Bob*, connected only by an insecure quantum channel. Most QKD protocols have the property that N signals are exchanged sequentially, but the order in which they are transmitted is irrelevant. One can then assume without loss of generality that the N-partite density operator describing Alice and Bob's information is permutation invariant (even if, upon transmission, the signals are modified arbitrarily by an adversary). Hence, according to the quantum de Finetti representation theorem, the density operator approximately has i.i.d. structure. This, on the other hand, exactly corresponds to the assumption that the adversary's attack is *collective* [7,8], meaning that the adversary manipulates each of the transmitted signals independently and identically. Consequently, for assessing the security of a QKD protocol against general attacks, it is sufficient to consider the (restricted) class of collective attacks. These are well understood for most protocols that have been proposed in the literature, and explicit formulas for the key rate are known (see, e.g., [9] for protocols with one-way communication).

The goal of this Letter is to overcome a main limitation of this argument, namely, that it only applies to discrete variable QKD schemes with low-dimensional signal space. This limitation is due to the fact that the de Finetti representation is generally invalid if the dimension d of the individual subsystems exceeds the number N of subsystems, as shown by an explicit example in [2]. In particular, the argument does not directly extend to continuous variable schemes [10–19], where d may be unbounded; in fact, no security proof against general attacks has been known to date for schemes based on high-dimensional information carriers.

Here, we show that the restriction of the de Finetti representation to low-dimensional systems can be circumvented under certain experimentally verifiable conditions. More precisely, for any permutation invariant state on a (possibly infinite-dimensional) system $\mathcal{H}^{\otimes N}$, the reduced state on $\mathcal{H}^{\otimes n}$, for some $n \approx N$, is approximated by a mixture of density operators with i.i.d. structure, provided that the outcomes of a certain measurement applied to a few subsystems lie within a given range. In particular, we consider measurements with respect to two canonical observables X and Y on $\mathcal{H} = \mathrm{L}^2(\mathbb{R})$, i.e., $[X, Y] = i$. The criterion then is that the outcomes of both the X and the Y measurements have small absolute value. In practical applications, this criterion is often easily verifiable. For example, in continuous variable quantum cryptography, which uses signals in $\mathcal{H} = \mathrm{L}^2(\mathbb{R})$, measurements with respect to two canonical observables X and Y are usually already part of the protocol. Our extended version of de Finetti's theorem then implies that these protocols are secure against the most general attacks, since the security against collective attacks has already been established (see, e.g., [20–22]).

Let us start out by summarizing the main statements of this work. Let ρ^N be a permutation invariant state on an

N-fold product space $\mathcal{H}^{\otimes N}$, that is, $\pi\rho^N\pi^{-1} = \rho^N$ for any permutation π. Our result now consists of two parts. The first (Lemma 2) says that, conditioned on the outcomes of a certain measurement $\mathcal{M}$ applied to k subsystems, for $1 \ll k \ll N$, the joint state ρ^M of the $M = N - k$ remaining subsystems almost certainly lies in the subspace $\mathcal{S}^M_{\bar{\mathcal{H}}^{\otimes M-k}}$ of $\mathcal{H}^{\otimes M}$ spanned by vectors which on all except k subsystems $\mathcal{H}$ are contained in a low-dimensional subspace $\bar{\mathcal{H}} \subset \mathcal{H}$, i.e.,

$$\mathcal{S}^M_{\bar{\mathcal{H}}^{\otimes M-k}} := \mathrm{span}\bigcup_\pi \pi(\bar{\mathcal{H}}^{\otimes M-k} \otimes \mathcal{H}^{\otimes k})\pi^{-1}, \quad (1)$$

where the union is taken over all permutations π. The second part of our result is a de Finetti-type statement (Theorem 4, combined with Lemma 3) that applies to (arbitrary) permutation invariant states in $\mathcal{S}^M_{\bar{\mathcal{H}}^{\otimes M-k}}$. It provides an approximation of these states in terms of a convex combination of states that have i.i.d. structure on almost all subsystems. In the following we will give a precise formulation of these statements and explain the main steps required to prove them. We refer the reader to Ref. [23] for the detailed proofs.

To start the first part of the results, and for the sake of concreteness, we assume that $\mathcal{H} = \mathrm{L}^2(\mathbb{R})$ and that the measurement $\mathcal{M}$ which is applied to the k subsystems of $\mathcal{H}^{\otimes N}$ is with respect to two canonical observables X and Y, each chosen with probability $\frac{1}{2}$. We then consider the condition that the measurement outcomes z satisfy $z^2 < \frac{n_0}{2}$ for some given n_0. In other words, the condition is that measurements with respect to both X^2 and Y^2 result in small values. This, intuitively, implies that also the outcomes of measurements with respect to $X^2 + Y^2$ (i.e., with respect to the number basis) are small.

To make this more precise, let $P^{Z\geq z_0}$ be the projector onto the subspace spanned by the eigenspaces of Z corresponding to (generalized) eigenvalues $z \geq z_0$, for any Hermitian operator Z and $z_0 \in \mathbb{R}$. Furthermore, let $U_1 := \frac{1}{2}P^{X^2\geq n_0/2} + \frac{1}{2}P^{Y^2\geq n_0/2}$ and $V_1 := P^{X^2+Y^2\geq 2n_0+1}$. We then define the quantity

$$\gamma_{U_1\to V_1}(\delta) := \sup\{\mathrm{tr}(V_1\sigma)\colon \sigma \in (\mathcal{H});\ \mathrm{tr}(U_1\sigma) \leq \delta\},$$

which corresponds to the maximum probability that the outcome of a measurement of a state σ with respect to $X^2 + Y^2$ is larger than $2n_0$, for any σ such that measurements with respect to X^2 and Y^2 give values smaller than $\frac{n_0}{2}$ except with probability δ. According to the following lemma, this quantity is small for small values of δ.

Lemma 1.—For any $n_0 \in \mathbb{N}$ and $\delta \geq 0$, $\gamma_{U_1\to V_1}(\delta) \leq 4\delta + \frac{4}{\sqrt{c_0\pi n_0}}e^{-n_0c_0}$, with $c_0 = (1 - 1/\sqrt{2})^2$.

Proof.—We define the operator $W_1 := \frac{1}{\pi}\int d\mu_\alpha |\alpha\rangle\langle\alpha|$, where $|\alpha\rangle$ denotes coherent states and the integral ranges over the complex plane with $|\alpha|^2 \geq n_0$. The claim then follows from the two operator inequalities $V_1 \leq 2W_1$ and $W_1 \leq 2(U_1 + \frac{1}{\sqrt{c_0\pi n_0}}e^{-n_0c_0}\mathbb{1})$, which we prove separately.

To derive the first operator inequality, we expand W_1 in the Fock basis, $\{|n\rangle_f\}_{n=0}^\infty$, which gives $W_1 = \sum q_n|n\rangle_f\langle n|$ with $q_n = \Gamma(n+1, n_0)/\Gamma(n+1, 0)$, where Γ is the incomplete Gamma function [24]. Since $q_{n+1} \geq q_n > 0$, we can write $V_1 \leq q_{n_0}^{-1}W_1$, where $q_{n_0}^{-1} = \Gamma(n_0+1, 0)/\Gamma(n_0+1, n_0) < 2$.

For the second operator inequality, we first extend our Hilbert space to $\mathcal{H}_1 \otimes \mathcal{H}_2$ and show that

$$W_1 = \int dxdy\, {}_f\langle 0|U(|x\rangle_X\langle x| \otimes |y\rangle_Y\langle y|)U^\dagger|0\rangle_f, \quad (2)$$

where the integral is defined for $x, y \in \mathbb{R}$ with the restriction $x^2 + y^2 \geq n_0$. Here $|0\rangle_f \in \mathcal{H}_2$, and $|x\rangle_{X,Y}$ denote generalized eigenstates of X and Y, respectively. Furthermore, $U = e^{(\pi/4)(a_1\otimes a_2^\dagger - a_1^\dagger\otimes a_2)}$ is the so-called beam splitter operator [25], where $a_{1,2} := (X_{1,2} + iY_{1,2})/\sqrt{2}$ are the annihilation operators acting on the first and second system, respectively. This expression for W_1 can be derived by showing that ${}_f\langle 0|U|x\rangle_X \otimes |y\rangle_Y = \pi^{-1/2}|\alpha\rangle$, with $\alpha = x + iy$. By looking at the integration domain in (2) it is clear that $W_1 \leq A + B$, where

$$A = \int dxdx'\, {}_f\langle 0|U(|x\rangle_X\langle x| \otimes |x'\rangle_X\langle x'|)U^\dagger|0\rangle_f,$$

$$B = \int dxdx'\, {}_f\langle 0|U(|x'\rangle_Y\langle x'| \otimes |x\rangle_Y\langle x|)U^\dagger|0\rangle_f,$$

where the integral is restricted to $|x|^2 \geq n_0/2$, and where we have used that the integral of $|x'\rangle_X\langle x'|$ is equal to that of $|x'\rangle_Y\langle x'|$. It is straightforward to verify that

$$A = \frac{1}{\sqrt{\pi}}\int_{|z|^2\geq n_0} dz e^{-(z-X)^2} =: F(X)$$

and that $F(X) \leq P^{X^2\geq a^2} + F(a)$ for all $a > 0$, and, similarly, for B. Noting that $F(a) \leq (1/\sqrt{\pi})e^{-(\sqrt{n_0}-a)^2}/(\sqrt{n_0} - a)$, for $a \in [0, \sqrt{n_0}]$, and choosing $a = \sqrt{n_0/2}$ we conclude the proof. □

We now combine Lemma 1 with a result from [26]. The latter allows to infer the statistics of measurements on the subsystems of a permutation invariant state ρ^N with respect to a positive operator valued measure (POVM) $\mathcal{V}$, given the statistics obtained by measuring a (small) sample of subsystems with respect to a (possibly different) POVM $\mathcal{U}$. For our purpose, we let $\mathcal{U} = \{U_0 = \mathbb{1} - U_1, U_1\}$ be the binary POVM that describes a measurement according to X or Y followed by a test which outputs 0 whenever the outcome z is bounded by $z^2 < \frac{n_0}{2}$ and 1 otherwise. Likewise, $\mathcal{V} = \{V_0 = \mathbb{1} - V_1, V_1\}$ outputs 1 whenever a measurement with respect to $X^2 + Y^2$ gives an output larger than $2n_0$.

Given a permutation invariant state ρ^N, let $f_{\mathbf{u}}$ and $f_{\mathbf{v}}$ be the relative frequencies of outcomes 1 obtained from measurement $\mathcal{U}$ applied to the first k subsystems and measurement $\mathcal{V}$ applied to the remaining $M = N - k$ subsystems, respectively. Then, according to [26] (see also Lemma III.1 of [23]), the frequency $f_{\mathbf{v}}$ is essentially upper bounded by

$\gamma_{U_1 \to V_1}(f_{\mathbf{u}})$ except with probability exponentially small in k. The crucial observation now is that a small value of $f_{\mathbf{v}}$ is equivalent to a successful projection onto the subspace $\mathcal{S}^M_{\bar{\mathcal{H}}^{\otimes M-k}}$ of $\mathcal{H}^{\otimes M}$, for $\bar{\mathcal{H}}$ defined as the support of $P^{X^2+Y^2 \leq 2n_0}$. Using this and Lemma 1, we arrive at the following statement.

Lemma 2.—Let $(z_1, \ldots, z_k)$ be the outcomes of measurements with respect to X and Y (both chosen with probability $\frac{1}{2}$) applied to k subsystems of a permutation invariant state ρ^N, and let Ω be the event that a projection on $\mathcal{S}^M_{\bar{\mathcal{H}}^{\otimes M-k}}$ applied to the remaining $M = N - k$ systems fails. Then

$$\Pr\left[\Omega \wedge \max_{i=1}^{k} z_i^2 < \frac{n_0}{2}\right] \leq 8k^{3/2} e^{-(k^3/25N^2)}$$

for any $n_0 \geq 12 \ln(5N/k)$ and $N/k \gg 1$.

The lemma implies that, with almost certainty, the joint state of the remaining M subsystems is contained in the space $\mathcal{S}^M_{\bar{\mathcal{H}}^{\otimes M-k}}$, under the (experimentally verifiable) condition that $\max_{i=1}^{k} z_i^2 < \frac{n_0}{2}$. This concludes the first part of our argument.

The second part of our result is about the structure of general permutation invariant states ρ^M on the subspace $\mathcal{S}^M_{\bar{\mathcal{H}}^{\otimes M-k}}$ of $\mathcal{H}^{\otimes M}$, and can be seen as a generalization of the de Finetti-type representation theorem proved in [2] (where the Hilbert space $\mathcal{H}$ has been assumed to be low dimensional). The main idea is to consider purifications of ρ^M on the *symmetric subspace* $\mathrm{Sym}^M(\mathcal{K}) = \{\psi \in \mathcal{K}^{\otimes M} : \pi\psi = \psi (\forall\ \pi)\}$ of $\mathcal{K}^{\otimes M}$, for $\mathcal{K} = \mathcal{H} \otimes \mathcal{H}$. The following lemma, which is a generalization of Lemma 4.2.2 of [1], states that such a purification always exists and that the property of lying in $\bar{\mathcal{H}} \subset \mathcal{H}$ in most subsystems is conserved.

Lemma 3.—For any permutation invariant state ρ^M on $\mathcal{S}^M_{\bar{\mathcal{H}}^{\otimes M-k}} \subseteq \mathcal{H}^{\otimes M}$ there exists a purification which lies both in $\mathrm{Sym}^M(\mathcal{K})$ and $\mathcal{S}^M_{\bar{\mathcal{K}}^{\otimes M-2k}} \subseteq \mathcal{K}^{\otimes M}$, where $\mathcal{K} = \mathcal{H} \otimes \mathcal{H}$ and $\bar{\mathcal{K}} = \bar{\mathcal{H}} \otimes \bar{\mathcal{H}}$.

The proof of the lemma is analogous to Lemma III.1 of [27]. We refer to [23] for a full proof.

Lemma 3 allows us to restrict our attention to states on $\mathrm{Sym}^M(\mathcal{K}) \cap \mathcal{S}^M_{\bar{\mathcal{K}}^{\otimes M-2k}}$. Theorem 4 below gives an approximation of such states in terms of convex combinations of states that have almost i.i.d. structure $\nu^{\otimes M}$, except on a few subsystems. More precisely, for some $n \geq n'$, we consider the space $\mathcal{S}^n_{\nu^{\otimes n'}} := \mathcal{S}^n_{(\mathrm{span}\,\nu)^{\otimes n'}}$, i.e., the span of all vectors $\Psi \in \mathcal{K}^{\otimes n}$ that are, up to reorderings, of the form $\nu^{\otimes n'} \otimes \Psi'$ for some arbitrary $\Psi' \in \mathcal{K}^{\otimes n-n'}$. The quality of the approximation is measured by the fidelity F.

Theorem 4.—Let $\bar{\mathcal{K}}$ be a d-dimensional subspace of a Hilbert space $\mathcal{K}$ and let ρ^M be a density operator on $\mathrm{Sym}^M(\mathcal{K}) \cap \mathcal{S}^M_{\bar{\mathcal{K}}^{\otimes M-2k}}$. Then there exists a probability distribution p_ν on a finite set $\mathcal{V}$ of unit vectors $\nu \in \bar{\mathcal{K}}$ and a family $\{\hat{\rho}_\nu^{M-4k}\}_{\nu \in \mathcal{V}}$ of density operators on $\mathcal{S}^{M-4k}_{\nu^{\otimes M-8k}}$ such that, for $\rho^{M-4k} = \mathrm{tr}_{4k}(\rho^M)$,

$$F\left(\rho^{M-4k}, \sum_{\nu \in \mathcal{V}} p_\nu \hat{\rho}_\nu^{M-4k}\right) > 1 - k^d e^{-(4k(k+1)/M)}. \quad (3)$$

The proof relies on a generalization of ideas developed in [2] (see [23]).

Application to QKD.—The results outlined above can be used to assess the security of QKD protocols against general attacks. The following analysis applies to a large class of QKD schemes, which includes almost all protocols proposed in the literature [28]. More concretely, the following conditions must hold.

Property 1.—The protocol is invariant under permutations of the N particle pairs held by Alice and Bob after the distribution phase. (This requirement is usually satisfied because each of the N signals is prepared, sent, and received independently of the other signals.)

Property 2.—In a final privacy amplification step [31,32], the key is computed by two-universal hashing [33]. (This criterion is not restrictive because two-universal hashing is optimal with respect to the extractable key length [1].)

Property 3.—The protocol employs measurements to check that the dimension of the relevant subspace $\bar{\mathcal{H}}$ of the signal space $\mathcal{H}$ is small compared to N. (Note that this step is unnecessary if the signal space already has small dimension.) For example, if the signal space is $\mathcal{H} = \mathrm{L}^2(\mathbb{R})$, the measurement may be with respect to two canonical observables X and Y, each of them chosen with probability $\frac{1}{2}$. The protocol then only continues if all outcomes z satisfy $z^2 < \frac{n_0}{2}$, for some appropriately chosen $n_0 = \dim(\bar{\mathcal{H}})$ (see Lemma 1 and Lemma 2).

According to Property 1, if a key distilled from N signals in state ρ^N is secure then the same is true for the key distilled from a permuted state $\pi\rho^N\pi^\dagger$, for any permutation $\pi \in S_N$. We can thus assume without loss of generality that the N signals are permuted at random and, hence, their state ρ^N is permutation invariant [34]. Now, according to our de Finetti representation theorem and using Property 3, we conclude that the reduced state ρ^n, for some $n \approx N$, is approximated by a mixture of almost i.i.d. states $\hat{\rho}_\nu^n$. Finally, we use Property 2, which implies that the only relevant quantity is the smooth min-entropy of the raw key conditioned on the adversary's information (the smooth min-entropy is a measure for the number of bits that can be extracted by two-universal hashing [32]). The smooth min-entropy of almost i.i.d. states $\hat{\rho}_\nu^n$ is approximated by the entropy of i.i.d. states $\nu^{\otimes n}$, as shown in [1]. Hence, we can without loss of generality assume that ρ^n is a mixture of i.i.d. states, which could equivalently be the result of a collective attack. Summarizing, we have thus proved that any QKD protocol satisfying the properties above is secure against general attacks whenever it is secure against collective attacks [35].

Conclusions.—We have shown that permutation invariant states on large N-partite systems are approximated by a convex combination of almost i.i.d. states, provided mea-

surements on a few subsystems with respect to certain observables only give bounded values. In particular, under this condition, a permutation invariant state can be considered equal to an unknown i.i.d. state, except on an arbitrarily small fraction of the subsystems. This has various implications. Of particular interest to experimental physics is that state tomography can be employed without the need for i.i.d. assumptions, as discussed in [2]. An important difference of our result compared to previously known de Finetti-type theorems is that it does not rely on nontestable assumptions such as that the dimension of systems is small (as, e.g., in [2]) or that the states lie in certain subspaces (as in [36]).

Applied to quantum cryptography, our result enables full security proofs for QKD schemes in the (practically relevant) case where the dimension of the signal space may be unbounded. This is an intrinsic property of continuous variable protocols, but the necessity of taking into account infinite-dimensional systems may also arise in the analysis of discrete variable schemes, for instance when they are implemented using weak coherent pulses (see, e.g., [37]) and if alternative techniques such as the *squashing method* [38] cannot be applied. The security of these schemes has been investigated intensively, but existing proofs are only valid under the assumption of collective attacks (see the introductory part for references). The de Finetti representation theorem derived here allows us to drop this assumption, implying that security holds against all possible attacks.

I. C. acknowledges support from the EU project COMPAS and Caixa Manresa. R. R. received support from the EU project SECOQC and from the Swiss National Science Foundation. He also would like to thank Johan Åberg and Fabio Pedrocchi for very helpful comments.

[1] R. Renner, Ph.D. thesis, Swiss Federal Institute of Technology (ETH) Zurich, 2005, arXiv:quant-ph/0512258.
[2] R. Renner, Nature Phys. **3**, 645 (2007).
[3] B. de Finetti, Ann. Inst. Henri Poincaré **7**, 1 (1937).
[4] I.i.d. is for independent and identically distributed.
[5] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.
[6] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[7] E. Biham and T. Mor, Phys. Rev. Lett. **78**, 2256 (1997).
[8] E. Biham and T. Mor, Phys. Rev. Lett. **79**, 4034 (1997).
[9] I. Devetak and A. Winter, Proc. R. Soc. A **461**, 207 (2005).
[10] T. C. Ralph, Phys. Rev. A **61**, 010303 (1999).
[11] M. Hillery, Phys. Rev. A **61**, 022309 (2000).
[12] M. D. Reid, Phys. Rev. A **62**, 062308 (2000).
[13] D. Gottesman and J. Preskill, Phys. Rev. A **63**, 022309 (2001).
[14] N. J. Cerf, M. Lévy, and G. V. Assche, Phys. Rev. A **63**, 052311 (2001).
[15] C. Silberhorn, N. Korolkova, and G. Leuchs, Phys. Rev. Lett. **88**, 167902 (2002).
[16] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[17] F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature (London) **421**, 238 (2003).
[18] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **93**, 170504 (2004).
[19] S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, Nature Phys. **4**, 726 (2008).
[20] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).
[21] M. Navascués, F. Grosshans, and A. Acín, Phys. Rev. Lett. **97**, 190502 (2006).
[22] Y. Zhao, M. Heid, J. Rigas, and N. Lütkenhaus, Phys. Rev. A **79**, 012307 (2009).
[23] R. Renner and J. I. Cirac, arXiv:0809.2243.
[24] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products* (Academic Press, San Diego, 2000).
[25] R. A. Campos, B. E. A. Saleh, and M. C. Teich, Phys. Rev. A **40**, 1371 (1989).
[26] M. Christandl, R. Renner, and A. Ekert, arXiv:quant-ph/0402131.
[27] M. Christandl, R. König, G. Mitchison, and R. Renner, Commun. Math. Phys. **273**, 473 (2007).
[28] Among the few exceptions are the differential phase shift (DPS) [29] and the coherent one-way (COW) protocol [30]. Both rely on measurements involving two subsequent signals at the same time, so that the order in which the signals are received is relevant.
[29] K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002).
[30] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, Appl. Phys. Lett. **87**, 194108 (2005).
[31] C. H. Bennett, G. Brassard, and J.-M. Robert, SIAM J. Comput. **17**, 210 (1988).
[32] R. Renner and R. König, *Second Theory of Cryptography Conference TCC*, Lecture Notes in Computer Science Vol. 3378 (Springer, New York, 2005), pp. 407–425.
[33] M. N. Wegman and J. L. Carter, J. Comput. Syst. Sci. **22**, 265 (1981).
[34] V. Scarani and R. Renner, in *Theory of Quantum Computation, Communication, and Cryptography*, Lecture Notes in Computer Science Vol. 5106, edited by Y. Kawano and M. Mosca, (Springer, Berlin/Heidelberg, 2008).
[35] In particular, known bounds on the secret key rate calculated for the special case of collective attacks (such as [9]) directly apply to the general case.
[36] C. D'Cruz, T. J. Osborne, and R. Schack, Phys. Rev. Lett. **98**, 160406 (2007).
[37] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, *Advances in Cryptology-EUROCRYPT 2000*, LNCS Vol. 1807 (Springer, Berlin/Heidelberg, 2000), pp. 289–299.
[38] N. J. Beaudry, T. Moroder, and N. Lütkenhaus, Phys. Rev. Lett. **101**, 093601 (2008).