Experimental Extraction of Secure Correlations from a Noisy Private State

K. Dobek,[1,2] M. Karpiński,[3] R. Demkowicz-Dobrzański,[3] K. Banaszek,[1,3] and P. Horodecki[4]

[1]*Institute of Physics, Nicolaus Copernicus University, ul. Grudziadzka 5/7, 87-100 Toruń, Poland*

[2]*Faculty of Physics, Adam Mickiewicz University, ul. Umultowska 85, 61-614 Poznań, Poland*

[3]*Faculty of Physics, University of Warsaw, ul. Hoża 69, 00-681 Warsaw, Poland*

[4]*Faculty of Applied Physics and Mathematics, Technical University of Gdańsk, ul. Narutowicza 11/12, 80-952 Gdańsk, Poland*

(Received 9 November 2010; published 18 January 2011)

We report experimental generation of a noisy entangled four-photon state that exhibits a separation between the secure key contents and distillable entanglement, a hallmark feature of the recently established quantum theory of private states. The privacy analysis, based on the full tomographic reconstruction of the prepared state, is utilized in a proof-of-principle key generation. The inferiority of distillation-based strategies to extract the key is exposed by an implementation of an entanglement distillation protocol for the produced state.

DOI: 10.1103/PhysRevLett.106.030501 PACS numbers: 03.67.Dd, 03.65.Wj, 03.67.Bg, 42.50.Dv

Quantum entanglement can guarantee secure communication as demonstrated by Ekert's protocol [1] for quantum key distribution (QKD) [2], where the random key obtained from a maximally entangled state is known exclusively to legitimate users. A natural way to realize QKD using imperfect noisy entanglement is to attempt its distillation into the maximal form using local operations and classical communication [3]. This strategy, however, may reduce the attainable key length or even preclude its generation altogether, which follows from the recently developed theory of private quantum states [4]. The secure key can be extracted in general at higher rates than that implied by distillable entanglement, and even from certain classes of bound entangled states.

In this Letter we report experimental generation and utilization of a noisy entangled four-photon state that exhibits the separation between secure key contents and distillable entanglement. We perform a full tomographic reconstruction of the produced state using the maximum-likelihood [5] and Bayesian reconstruction methods [6,7], which allows us to obtain credible estimates for the quantities of interest despite their nonlinear character and high sensitivity to statistical noise and experimental imperfections. We present a proof-of-principle extraction of a secure key and implement an entanglement distillation protocol verified to perform suboptimally.

The original example of extracting privacy from quantum entanglement is Ekert's QKD protocol, in which two communicating parties—Alice and Bob—need a sequence of bipartite systems prepared in a maximally entangled two-qubit state such as $|\phi_+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Local projections performed by Alice and Bob in the computational basis $|0\rangle, |1\rangle$ yield perfectly correlated random key bits. The security is checked by measuring the qubits in superposition bases to test coherence between the components $|00\rangle$ and $|11\rangle$. If the state used for QKD is indeed pure, the monogamy of entanglement [8] prevents an eavesdropper Eve from learning measurement outcomes obtained by legitimate users. Of course, a state $|\phi_-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$ would be equally suitable for key generation. But an equiprobable statistical mixture of $|\phi_+\rangle$ and $|\phi_-\rangle$ ensures no security. This is because it can be viewed as a partial trace $\frac{1}{2}(|\phi_-\rangle_{AB}\langle\phi_-| + |\phi_+\rangle_{AB}\langle\phi_+|) = \mathrm{Tr}_E(|\Phi\rangle_{ABE}\langle\Phi|)$ of a tripartite state

$$|\Phi\rangle_{ABE} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} \otimes |0\rangle_E + |11\rangle_{AB} \otimes |1\rangle_E) \qquad (1)$$

involving a qubit E in possession of Eve, who can gain complete information about the results of Alice's and Bob's measurements in the computational basis without introducing any disturbance.

Suppose now that in addition to qubits A and B, Alice and Bob possess also qubits A' and B' prepared jointly in a statistical mixture of $|\phi_-\rangle_{AB} \otimes |00\rangle_{A'B'}$ and $|\phi_+\rangle_{AB} \otimes |11\rangle_{A'B'}$. Obviously, a local measurement of A' or B' in the computational basis reveals whether the qubits A and B have been prepared in $|\phi_+\rangle$ or $|\phi_-\rangle$. This enables key generation and entanglement distillation with equal rates. An intriguing case is the privacy of a mixed four-qubit state [4]:

$$\varrho_{\mathrm{priv}} = \tfrac{1}{4}|\phi_-\rangle_{AB}\langle\phi_-| \otimes \varrho_-^{A'B'} + \tfrac{3}{4}|\phi_+\rangle_{AB}\langle\phi_+| \otimes \varrho_+^{A'B'}, \quad (2)$$

where $\varrho_- = |\psi_-\rangle\langle\psi_-|$, $\varrho_+ = \frac{1}{3}(\mathbb{1} - |\psi_-\rangle\langle\psi_-|)$, and we denote $|\psi_\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$. Unlike the preceding example, the two operators $\varrho_\pm^{A'B'}$ cannot be discriminated unambiguously by Alice and Bob using local operations and classical communication, which lowers the value of distillable entanglement E_D [9]. This can be seen from an upper bound

$$E_D \leq \mathcal{L} = \log_2 \mathrm{Tr}|\varrho_{\mathrm{priv}}^{\Gamma}| = \log_2 3 - 1 \approx 0.585, \qquad (3)$$

where $\mathcal{L}$ is the log negativity [10] calculated for the partial transposition Γ with respect to the partition $AA'{:}BB'$. In contrast, the theory of private states [4]—of which

ϱ_{priv} is an example—shows that results of projecting qubits A and B in the computational basis cannot be learned by Eve, thus providing 1 bit of a secure key. This leads to a gap between the key rate and E_D, implying general suboptimality of distillation strategies.

In order to demonstrate experimentally this hallmark feature of private states we generated a noisy entangled four-photon states using a setup shown in Fig. 1. At its center were two 1 mm long type-I down-conversion beta-barium borate crystals with optical axes aligned in perpendicular planes, following the arrangement introduced by Kwiat *et al.* [11]. The crystals were pumped using a Ti: sapphire oscillator (Coherent Chameleon Ultra) emitting a 78 MHz train of 180 fs pulses frequency doubled in a 1 mm long lithium triborate crystal to give a 390 nm wavelength pump of an average power of 200 mW, and focused to a 70 μm diameter waist. The axial symmetry of type-I down-conversion implies that photons emerging along any two opposite ends of the emission cone will be maximally entangled. That way one can collect multiple photon pairs, as shown in the inset of Fig. 1(a), and obtain a four-photon state $|\phi_+\rangle_{AB} \otimes |\phi_+\rangle_{A'B'}$ with $|0\rangle$ and $|1\rangle$ corresponding to horizontal and vertical polarizations. Collimated photons after transmission through 10 nm full width at half maximum bandwidth interference filters were coupled into single-mode fibers wound on manual polarization controllers. Phase relations between two-photon probability amplitudes were controlled by two Soleil-Babinet compensators D placed in the path of the pump beam and photons A.

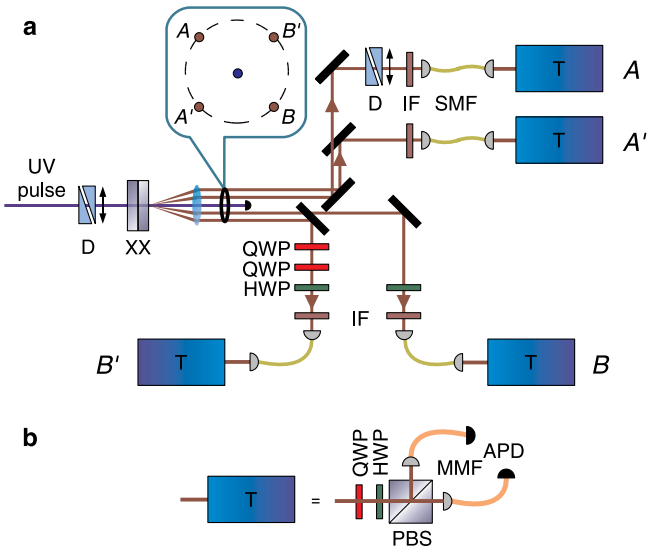

FIG. 1 (color online). Experimental setup. (a) Preparation of noisy private states. Two maximally entangled photon pairs are generated in two nonlinear crystals XX, collected from four directions $AA'BB'$ shown in the inset, and subjected to polarization transformations implemented with quarter wave plates (QWP) and half wave plates (HWP). D, Soleil-Babinet compensators; IF, interference filters; SMF, single-mode fibers. (b) Polarization analyzers. PBS, polarizing beam splitter; MMF, multimode fibers; APD, avalanche photodiodes.

Photons B were sent through a half wave plate whose two selected orientations introduced a transformation $\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$ or $\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$. The set of two quarter wave plates and a half wave plate placed in the path of photons B' realized one of four operations $\mathbb{1}$, σ_x, σ_z, or $\sigma_y = i\sigma_x\sigma_z$. Applying combinations $\sigma_z^B \otimes \sigma_y^{B'}$, $\sigma_x^B \otimes \mathbb{1}^{B'}$, $\sigma_x^B \otimes \sigma_x^{B'}$, and $\sigma_x^B \otimes \sigma_z^{B'}$ randomly with equal probabilities produced ideally the state

$$\varrho_{\text{id}} = \tfrac{1}{4}|\phi_-\rangle_{AB}\langle\phi_-| \otimes \varrho_-^{A'B'} + \tfrac{3}{4}|\psi_+\rangle_{AB}\langle\psi_+| \otimes \varrho_+^{A'B'}, \quad (4)$$

equivalent up to a local unitary to ϱ_{priv}. The secure key can be obtained by measuring qubits A and B in the eigenbasis of σ_y given by $|\bar{v}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i(-1)^v|1\rangle)$, $v = 0, 1$.

The photons were detected using free space polarization analyzers constructed from a quarter wave plate, a half wave plate, and a Wollaston polarizer with two output ports coupled into multimode fibers, connected to avalanche photodiode (APD) modules (Perkin-Elmer SPCM-AQRH), as shown in Fig. 1(b). Detection efficiencies within each polarization analyzer, determined from an independent macroscopic measurement, were equalized in the postprocessing by binomial resampling. Electric signals from APDs were registered with a field programmable gate array circuit using a coincidence window of 6 ns. Typical count rates were 10^5 s^{-1} for single counts, 6×10^3 s^{-1} for two-photon, and 2 s^{-1} for fourfold coincidences.

Assuming that only four-photon events are available to Alice and Bob, we reconstructed a density matrix of a private state and performed a proof-of-principle secure key generation. A complete measurement consisted of a sequence of 33 637 intervals, each 10 s long. Before a single interval, settings of individual polarization analyzers were selected randomly and independently on Alice's and Bob's side to project polarization in the eigenbasis of σ_x, σ_y, or σ_z. The density matrix of the generated state was reconstructed from fourfold coincidences using two independent techniques: the Kalman filter (KF) method [7] based on Gaussian approximation and Bayesian inference which provides an *a posteriori* probability distribution on the set of density matrices, and the maximum-likelihood (ML) method with physical constraints [5]. In the KF approach the resulting *a posteriori* distribution served to generate a sample of 10^4 physical density matrices with the help of the slice-sampling technique [12]. This sample was used to calculate mean values and standard deviations of individual elements of the density matrix depicted in Fig. 2, as well as the information-theoretic quantities reported in Eq. (7). Uncertainties of ML estimates were obtained by generating 2000 reconstructions using perturbed experimental data as an input. The uncertainties calculated account for both the Poissonian photon counting noise and 0.25° uncertainty of the wave plate orientation in polarization analyzers. Calculation of the KF *a posteriori* distribution took 20 s on a standard PC, a significant advantage compared with 20 min for the ML method.

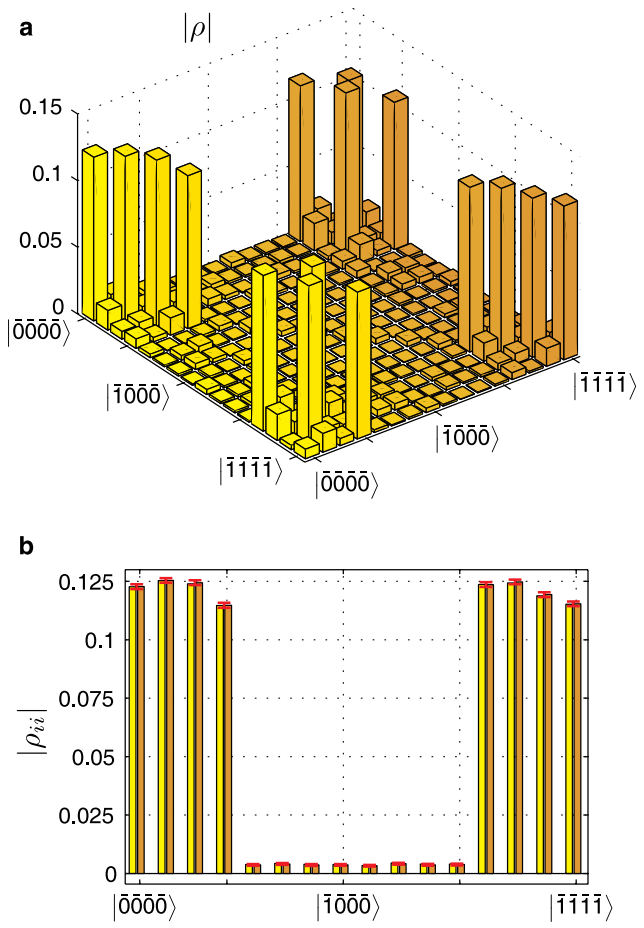

FIG. 2 (color online). Reconstructed private state. (a) Absolute values of density matrix elements in the σ_y basis reconstructed using KF method. (b) Diagonal KF values [dark gray (orange), with error bars] compared with the ML results [light gray (yellow)].

A more time-consuming stage, however, was generation of statistical samples of physical density matrices, which took 2 s per matrix using the KF distribution and required repetition each time of the full reconstruction in the ML case.

Figure 2 depicts the state ϱ_{exp} obtained using the KF method. The fidelity $\mathcal{F} = \mathrm{Tr}(\sqrt{\sqrt{\varrho_{\mathrm{id}}}\varrho_{\mathrm{exp}}\sqrt{\varrho_{\mathrm{id}}}})$ of this state is $\mathcal{F}_{\mathrm{KF}} = 0.9724(7)$, and the ML value $\mathcal{F}_{\mathrm{ML}} = 0.9715(7)$ lies within the confidence interval. The figure shows that the qubits A and B are indeed strongly correlated in the basis $|\bar{0}\rangle, |\bar{1}\rangle$. To characterize the privacy of these correlations, we consider a purification $|\Psi\rangle_{AA'BB'E}$ of the complete system $AA'BB'E$ in the worst-case scenario when Eve controls all environmental degrees of freedom E. Thus, $\varrho_{\mathrm{exp}} = \mathrm{Tr}_E(|\Psi\rangle_{AA'BB'E}\langle\Psi|)$, which generalizes Eq. (1). After Alice projects the qubit A onto a state $|a\rangle$, the state of Bob's qubit reduces to $\varrho_B^{(a)} = \frac{1}{p_a}\mathrm{Tr}_{A'B'E}({}_A\langle a|\Psi\rangle_{AA'BB'E}\langle\Psi|a\rangle_A)$, while Eve is in possession of a system in a state $\varrho_E^{(a)} = \frac{1}{p_a}\mathrm{Tr}_{A'BB'}({}_A\langle a|\Psi\rangle_{AA'BB'E}\langle\Psi|a\rangle_A)$, where $p_a = \mathrm{Tr}_{A'BB'E}({}_A\langle a|\Psi\rangle_{AA'BB'E}\langle\Psi|a\rangle_A)$ is the probability of obtaining the projection onto $|a\rangle$ by Alice. An attempt to gain information about Alice's outcome by either Bob or Eve can be viewed as a classical to quantum communication channel $A \to B$ or $A \to E$ [13]. In such a scenario—denoted as cqq—Alice and Bob can establish a secret key at a rate at least

$$\mathcal{X}^{\mathrm{cqq}} = \chi_B - \chi_E, \tag{5}$$

where $\chi_{B(E)}$ is the Holevo quantity [14] for the respective channel $A \to B(E)$, defined as

$$\chi_{B(E)} = S\Big(\sum_a p_a \rho_{B(E)}^{(a)}\Big) - \sum_a p_a S(\rho_{B(E)}^{(a)}), \tag{6}$$

$S(\cdot)$ denotes the von Neumann entropy, and the summations are carried out over an orthonormal basis of states $|a\rangle$, in our case $|\bar{0}\rangle$ and $|\bar{1}\rangle$.

Based on measured data, the Bayesian *a posteriori* distribution for density matrices yields the following estimates for the attainable key rate and the log negativity:

$$\mathcal{X}^{\mathrm{cqq}}_{\mathrm{KF}} = 0.690(7), \qquad \mathcal{L}_{\mathrm{KF}} = 0.581(4). \tag{7}$$

These results show a clear separation, exceeding 10 standard deviations, between distillable entanglement and the key rate, exposing a fundamental feature of general private states. The ML method yields consistent results $\mathcal{X}^{\mathrm{cqq}}_{\mathrm{ML}} = 0.704(7)$ and $\mathcal{L}_{\mathrm{ML}} = 0.578(4)$. The slightly higher value of $\mathcal{X}^{\mathrm{cqq}}_{\mathrm{ML}}$ may be attributed to the fact that the ML method returns a lower-rank density matrix with weaker entanglement between the system $AA'BB'$ and the environment E.

The consistency of KF and ML results was verified by calculating the Mahalanobis distance [7] between the density matrices produced by both the methods with the KF covariance matrix used as a metric. The obtained distance 16.8 is below the value 17.1 corresponding to a 95% confidence interval. The KF method allows one to check for the presence of systematic errors: since the mean of the *a posteriori* distribution is not forced to be positive definite, its Mahalanobis distance from the mean of the distribution with imposed positivity constraints is an indicator of possible systematic errors in the measurement process [7]. For our data this distance is 17.7, implying that systematic errors are not significant.

In order to extract a secure key from the four-photon state we selected randomly one event from each interval when both the qubits A and B were measured in the σ_y bases obtaining $N = 3716$ raw key bits. We simulated a binary interactive error-correction procedure [15] exchanging 990 parity bits, which corrected all errors, and performed privacy amplification using two-universal hashing functions. Using the KF estimate of Eve's knowledge in the asymptotic limit given by χ_E, conservatively enhanced by 5 standard deviations, and adding a security margin [16] to guarantee that the probability of Eve learning at least 1 bit of the key is below 10^{-6}, yields 2164 bits of a secure key.

The subsystems A' and B' play the role of a shield protecting the private key contained in subsystems A and B from an eavesdropping attempt. Given ϱ_{id}, tracing out

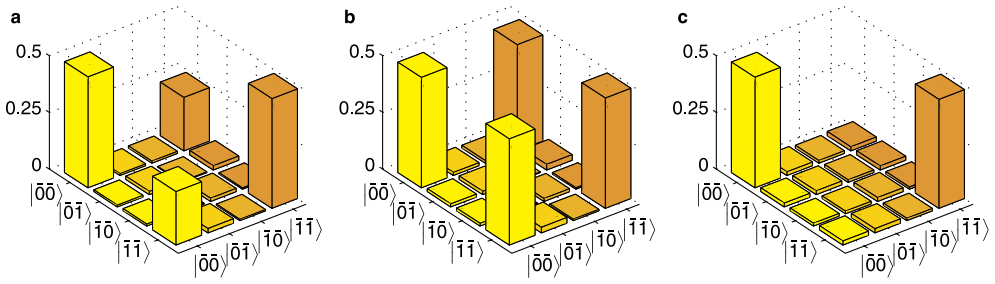

FIG. 3 (color online). Two-qubit AB state. (a) Absolute values of the elements of the reduced density matrix obtained by tracing out qubits A' and B'. (b),(c) Absolute values of the elements of density matrices conditioned upon finding qubits A' and B' in identical (b) or orthogonal (c) states when measured in the same basis.

A' and B' reduces the qubits A and B to a mixed state $\varrho_{AB} = \frac{1}{4}|\phi_-\rangle_{AB}\langle\phi_-| + \frac{3}{4}|\psi_+\rangle_{AB}\langle\psi_+|$. The corresponding experimental state, shown in Fig. 3(a), has $\mathcal{X}_{\mathrm{KF}}^{\mathrm{cqq}} = -0.009(4)$, which demonstrates that the shield is critical to ensure security. The shield qubits can be used to implement a simple entanglement distillation protocol for ϱ_{id}: if A' and B' are projected in the same basis, identical outcomes collapse the state of qubits A and B to a maximally entangled state $|\psi_+\rangle_{AB}$, while opposite results produce a separable state $\frac{1}{2}(|\phi_-\rangle_{AB}\langle\phi_-| + |\psi_+\rangle_{AB}\langle\psi_+|) = \frac{1}{2}(|\bar{0}\,\bar{0}\rangle_{AB}\langle\bar{0}\,\bar{0}| + |\bar{1}\,\bar{1}\rangle_{AB}\langle\bar{1}\,\bar{1}|)$ useless for key generation. Figures 3(b) and 3(c) depict experimental conditional density matrices reconstructed for these two cases using the KF method. The key rate is positive only for identical outcomes and equals 0.693(9), which multiplied by the relative frequency of these events 0.511 yields the average value $\mathcal{X}_{\mathrm{KF}}^{\mathrm{cqq}} = 0.354(5)$, falling significantly behind the result reported in Eq. (7). Using the resulting subset of qubit pairs to generate a key under the same security assumptions as before yields below 650 bits after error correction and privacy amplification of 1859 raw bits obtained from intervals when the qubits A and B were measured in the same bases. Note that the 50% reduction in the raw key length compared to the four-photon key extraction corresponds exactly to the success rate of the distillation protocol which halves the raw bit rate if only compatible measurements yielding perfectly correlated outcomes are applied.

In conclusion, we demonstrated experimentally a fundamental feature of private states, namely, the separation between distillable entanglement and the secret key contents, using a noisy entangled state of photon quadruplets. The results confirmed the suboptimality of distillation-based strategies to extract private correlations. This highlights the complex nature of mixed entanglement in higher dimensions similarly to that exhibited in multiparty scenarios [17] and paves the way to develop QKD protocols that make optimal use of realistic imperfect resources.

We wish to acknowledge insightful discussions with Koenraad Audenaert and Jan Tuziemski. This work was supported by FP7 FET projects CORNER and Q-ESSENCE, the Foundation for Polish Science TEAM project, and Polish Ministry for Scientific Research (Grant No. N202 231937).

[1] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991); T. Jennewein *et al.*, *ibid.* **84**, 4729 (2000); D. S. Naik *et al.*, *ibid.* **84**, 4733 (2000); W. Tittel *et al.*, *ibid.* **84**, 4737 (2000).
[2] N. Gisin *et al.*, Rev. Mod. Phys. **74**, 145 (2002); V. Scarani *et al.*, *ibid.* **81**, 1301 (2009).
[3] C. H. Bennett *et al.*, Phys. Rev. Lett. **76**, 722 (1996); D. Deutsch *et al.*, *ibid.* **77**, 2818 (1996).
[4] K. Horodecki *et al.*, Phys. Rev. Lett. **94**, 160502 (2005); IEEE Trans. Inf. Theory **55**, 1898 (2009); J. M. Renes and G. Smith, Phys. Rev. Lett. **98**, 020502 (2007).
[5] K. Banaszek *et al.*, Phys. Rev. A **61**, 010304 (1999); D. F. V. James *et al.*, *ibid.* **64**, 052312 (2001); Z. Hradil, D. Mogilevtsev, and J. Řeháček, Phys. Rev. Lett. **96**, 230401 (2006).
[6] V. Bužek *et al.*, Ann. Phys. (N.Y.) **266**, 454 (1998).
[7] K. M. R. Audenaert and S. Scheel, New J. Phys. **11**, 023028 (2009).
[8] V. Coffman, J. Kundu, and W. K. Wootters, Phys. Rev. A **61**, 052306 (2000).
[9] C. H. Bennett *et al.*, Phys. Rev. A **54**, 3824 (1996).
[10] G. Vidal and R. F. Werner, Phys. Rev. A **65**, 032314 (2002).
[11] P. G. Kwiat *et al.*, Phys. Rev. A **60**, R773 (1999).
[12] D. J. C. MacKay, *Information Theory, Inference, and Learning Algorithms* (Cambridge University Press, Cambridge, England, 2003).
[13] I. Devetak and A. Winter, Phys. Rev. Lett. **93**, 080501 (2004); Proc. R. Soc. A **461**, 207 (2005).
[14] A. S. Holevo, Probl. Inf. Transm. **9**, 177 (1973).
[15] C. H. Bennett *et al.*, J. Cryptol. **5**, 3 (1992).
[16] G. V. Assche, *Quantum Cryptography and Secret Key Distillation* (Cambridge University Press, Cambridge, England, 2006).
[17] E. Amselem and M. Bourennane, Nature Phys. **5**, 748 (2009); H. Kampermann *et al.*, Phys. Rev. A **81**, 040304 (2010); J. Lavoie *et al.*, arXiv:1005.1258; J. T. Barreiro *et al.*, arXiv:1005.1965.