Experimental Eavesdropping Based on Optimal Quantum Cloning

Karol Bartkiewicz,[1,*] Karel Lemr,[1,†] Antonín Černoch,[2] Jan Soubusta,[2] and Adam Miranowicz[3]

[1]*RCPTM, Joint Laboratory of Optics of Palacký University and Institute of Physics of Academy of Sciences of the Czech Republic, Faculty of Science, Palacký University 17. listopadu 12, 771 46 Olomouc, Czech Republic*

[2]*Institute of Physics of Academy of Science of the Czech Republic, Joint Laboratory of Optics of PU and IP AS CR, 17. listopadu 50A, 77207 Olomouc, Czech Republic*

[3]*Faculty of Physics, Adam Mickiewicz University, PL-61-614 Poznań, Poland*

(Received 4 December 2012; revised manuscript received 11 March 2013; published 24 April 2013)

The security of quantum cryptography is guaranteed by the no-cloning theorem, which implies that an eavesdropper copying transmitted qubits in unknown states causes their disturbance. Nevertheless, in real cryptographic systems some level of disturbance has to be allowed to cover, e.g., transmission losses. An eavesdropper can attack such systems by replacing a noisy channel by a better one and by performing approximate cloning of transmitted qubits which disturb them but below the noise level assumed by legitimate users. We experimentally demonstrate such symmetric individual eavesdropping on the quantum key distribution protocols of Bennett and Brassard (BB84) and the trine-state spherical code of Renes (R04) with two-level probes prepared using a recently developed photonic multifunctional quantum cloner [Lemr *et al.*, Phys. Rev. A **85**, 050307(R) (2012)]. We demonstrated that our optimal cloning device with high-success rate makes the eavesdropping possible by hiding it in usual transmission losses. We believe that this experiment can stimulate the quest for other operational applications of quantum cloning.

DOI: 10.1103/PhysRevLett.110.173601 PACS numbers: 42.50.Ex, 03.67.Ac, 03.67.Dd, 03.67.Lx

During the last decades, there has been much interest in secure quantum communication [1,2]. Quantum key distribution (QKD) devices (apart from quantum metrology, random number generators, and adiabatic computers based on quantum annealing) are arguably the only second-generation quantum technologies providing commercially available applications of quantum information and quantum optics up to date [3]. The security of QKD follows from Heisenberg's uncertainty relation or, equivalently, the no-cloning theorem. However, QKD can be secure only below some level of noise that unavoidably occurs in any physical system. Therefore, security bounds of QKDs are expressed in terms of tolerated losses or noise.

For QKD to be secure Alice and Bob must operate on single photons; hence, they need a single-photon source (SPS). SPSs are usually implemented as a weak coherent pulse of light [1]; thus, QKD is prone to photon-number splitting attacks. This attack can be circumvented by, e.g., using decoy states [4] or heralded SPS instead of weak coherent pulses. Since there are no lossless channels, if the eavesdropper (Eve) is equipped with a proper cloning machine mimicking the lossy channel then she can clone (a part of) the state sent by Alice, while hiding her presence in usual transmission losses.

Recent proposals of applications of quantum cloning [5] range from quantum cryptography [6] and quantum metrology [7] to nonclassicality tests in microscopic-macroscopic systems [8] and, even, proposals related to quantum experiments with human eyes [9].

In this Letter, we experimentally demonstrate the usefulness of cloning for quantum cryptoanalysis, i.e., for the eavesdropping of QKD over noisy quantum channels.

There are a number of well-known QKDs including the famous BB84 of Bennett and Brassard [10] based on mutually unbiased bases and the biased-bases R04 of Renes [11]. Attacks on those protocols can be classified as individual (or incoherent) and coherent (including joint and collective) [1]. Every attack can be imagined as follows: Eve sends a photon (probe) prepared in some polarization state which interacts with a photon sent by Alice, then Eve sends a photon to Bob and performs a measurement on her probe (she might wait until the key sifting process is over). Recently, attacks on QKD were proposed exploiting technological loopholes rather than the limits imposed by physics [12,13]. However, in this Letter we analyze the physical bounds on the security of the QKDs.

We focus only on individual attacks on the two QKDs assuming that Eve waits until Alice and Bob complete key sifting and then performs her measurements. This kind of attack requires that Eve has access to quantum memory (QM) in order to store her probes during the key sifting, but does not require Eve to perform a coherent measurement on many photons at a time. Such satisfactory memory has not been invented yet; however, recent encouraging results [14] carry the promise of realizing good QMs in near future. Moreover, in our opinion, coherent multi-qubit readout may require an additional technological leap. For clarity of presentation we focus only on trine-state R04 and BB84. Nevertheless, our approach can be used for

analyzing generalizations of those protocols. By referring hereafter to R04 we mean its trine-state version.

It is known that the acceptable quantum bit error rate (QBER), i.e., the ratio of the number of wrong qubits to the total number of qubits received, is 15% [15] for BB84 and 16.7% [11] for R04 assuming an individual attack with a four-level probe and that Eve does not wait for the key sifting. These QBER bounds could suggest that R04 is more robust to eavesdropping than BB84. However, it was shown that, by assuming one-way communication between Alice and Bob, BB84 is unconditionally secure if QBER $\leq 11\%$ [16], while R04 if QBER $\leq 9.85\%$ [17]. On the other hand, if Eve waits for the key sifting process to finish, BB84 is secure if QBER $\leq 14.6\%$ [18] (or 15% [19] for the two-level probe), while the corresponding QBER bound for R04 is unknown to our knowledge. Nevertheless, in this Letter we show that the QBER bound for R04 and BB84 is 16.7% for the optimal cloning attack with a two-level probe.

The algorithm for the cloning-based eavesdropping investigated in our Letter reads as follows: (i) Eve plugs a cloning machine together with QM into the quantum communication channel between Alice and Bob. (ii) Alice sends one of the states used in BB84 or R04. (iii) Eve intercepts the state and prepares two noisy copies. This cloning introduces losses. (iv) Eve sends one copy to Bob and keeps the other copy in QM. (v) Bob measures the received copy. (vi) Alice and Bob publicly perform key sifting. (vii) Eve performs positive-valued measures on each of the stored qubits to guess the bit value that was obtained by Alice and Bob simultaneously. She assigns corresponding bit values to her measurement outcomes. The steps performed by Eve are discussed below (for additional details see Ref. [20]). Since, in our experiment, we do not have access to QM we simulate it by performing a reconstruction of the two-qubit density matrix shared by Eve and Bob and later by projecting Bob's part of the state onto one of the bases used in QKD. The reduced density matrix describing Eve's qubit is assumed to be stored in QM.

Symmetric attacks on QKD can be performed by using a multifunctional optimal quantum cloner (OQC) [21]. In R04 [11] (explained in Fig. 1) Alice sends one of the three equally separated equatorial qubits $|a_n\rangle = \mathcal{N}[|H\rangle + \exp(i2n\pi/3)|V\rangle]$ and Bob detects $|b_n\rangle = \mathcal{N}[|H\rangle + \exp(i2n\pi/3 + i\pi/3)|V\rangle]$, where $n = 0$, 1, 2 and $\mathcal{N} = 1/\sqrt{2}$. Since all the states used in R04 (and also in BB84) are on the equator of the Bloch sphere (say xy plane), we require that Eve's action causes the Bloch sphere of the qubit received by Bob to shrink uniformly in the xy plane (qubit's purity decreases) so that her presence cannot be easily detected. Thus, the density matrix of Bob's qubit reads as $\rho_B = \frac{1}{2}[\mathbb{1} + (\hat{\eta}_B \vec{r}_B) \cdot \vec{\sigma}_B]$, where the Bloch-sphere shrinking is described by matrix $\hat{\eta}_B = \mathrm{diag}(\eta, \eta, \eta_\perp)$, where η ($\eta_\perp$) is the shrinking factor in the xy plane (z direction), $\vec{r}$ is the Bloch vector of the initial

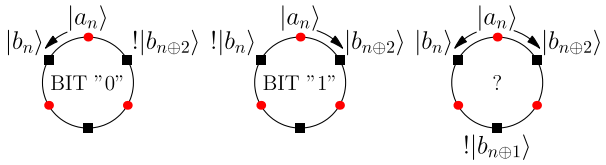

FIG. 1 (color online). Diagram describing R04 [11]. Alice (Bob) publicly agrees beforehand to send (measure) one of the trine states marked by red (black) dots, respectively. Both agree that the clockwise (anticlockwise) sequence of their states corresponds, e.g., to bit 1 (0). Bob publicly informs Alice what he has *not* measured (marked by an exclamation mark). Alice ignores the inconclusive cases (and informs Bob about them). In the other two cases, Alice and Bob obtain the same bit value.

qubit, and $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ is a vector of Pauli's matrices. Our OQC [21] provides the following shrinking factors $\eta = 2\sqrt{p}\Lambda\bar{\Lambda}$ and $\eta_\perp = \Lambda^2 + \bar{\Lambda}^2(p-q)$, where $q + p = 1$ and $\Lambda^2 + \bar{\Lambda}^2 = 1$ assuming that $p, q, \Lambda, \bar{\Lambda} \in [0, 1]$, where p is the asymmetry parameter of the clones and Λ is the cloning "strength" since it affects the purity of the clones (related to the shrinking factors) in the same way. In our experiment we fix values of p and Λ by adjusting polarization sensitive filtering in BDAs (see Fig. 2 and Ref. [20]). Moreover, for Eve's probe we obtain $\hat{\eta}_E(p, \Lambda) = \hat{\eta}_B(q, \Lambda)$. This operation is similar to the one of the mirror phase-covariant cloner [21,22]. The difference depends on p which implies that the states of Eve and Bob have different fidelities with respect to the states sent by Alice. Furthermore, the fidelity of Bob's qubits is $F_B(p, \Lambda) = (1 + 2\sqrt{p}\Lambda\bar{\Lambda})/2$, whereas Eve obtains $F_E(p, \Lambda) = F_B(q, \Lambda)$. The unitary cloning transformation

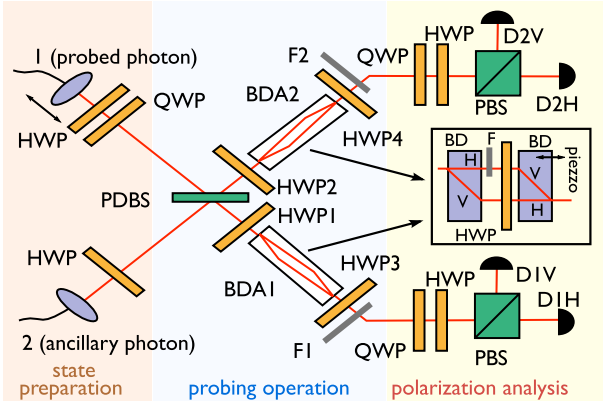

FIG. 2 (color online). Experimental setup as described in the text. States of the probed and ancillary photons are prepared with half-wave (HWP) and quarter-wave (QWP) plates. The photons overlap on the polarization-dependent beam splitter (PDBS) and undergo polarization-sensitive filtering in the beam divider assemblies (BDAs). Each BDA (see figure inset) consists of a pair of beam dividers (BDs), a neutral density filter (F), and a half-wave plate (HWP). The tomography of the two-photon state is accomplished by means of the HWPs, QWPs, polarizing beam splitters (PBDs), and single-photon detectors (D).

reads as $|H\rangle_A \rightarrow [\Lambda|H,H,0\rangle + \bar{\Lambda}|\psi(p),1\rangle]_{B,E,\mathrm{anc}}$ and $|V\rangle_A \rightarrow [\Lambda|V,V,1\rangle + \bar{\Lambda}|\psi(q),0\rangle]_{B,E,\mathrm{anc}}$, where $|\psi(p)\rangle = \sqrt{p}|H,V\rangle + \sqrt{q}|V,H\rangle$. The resulting state shared by Bob and Eve is obtained by tracing out the ancilla, which in our experiment corresponds to random switching between H- and V-polarized photons used by Eve as probes. For $p = \Lambda^2 = 1/2$ the OQC becomes the symmetric $1 \rightarrow 2$ phase-covariant cloner [23], which for BB84 causes QBER $= 1 - F_B = 14.6\%$. Moreover, for $p = 1/2$ and $\Lambda^2 = 2/3$, the OQC becomes the universal cloner [24]. We assume Eve's probe to be a qubit, while the most general approach requires the probe to be a four-level system. Our restriction is valid if two-photon interactions [21] are only used for the eavesdropping.

Optimal eavesdropping strategy.—Eve knows the initial state of her photon as her OQC performs conditional operations [20,21], where the asymmetry is implemented by introducing additional losses [25]. However, Eve, to optimize her attack on R04, must choose the optimal strategy for distinguishing between Bob's measurement results b_n and $b_{n\oplus 1}$ given that Alice sent a_n and $a_{n\oplus 2}$, respectively, where $\oplus$ stands for sum modulo 3. While restricting Eve's readout to the von Neumann's measurements we found the optimal ones maximizing Eve's information (this follows from the symmetry of the shrinking factors) to be equivalent to Helstrom's measurements [26] discriminating between states $|b_n\rangle$ and $|b_{n\oplus 1}\rangle$ (or $|a_n\rangle$ and $|a_{n\oplus 2}\rangle$) independent of the values Λ, p, and the initial state of the probe. Thus, Eve's measurement is a projection on equatorial qubits of phase $2n\pi/3 + \pi/6 + m\pi$ ($2n\pi/3 + 5\pi/6 + m\pi$) if Bob's message (see Fig. 1) is $!|b_n\rangle$ ($!|b_{n\oplus 2}\rangle$), where $m = 0, 1$ is Eve's bit value. For BB84, Eve uses the measurement as Bob.

For the measurements we calculated [20] the mutual Shannon information $I_{X,Y}$ between the three users, where X, Y stand the initials of the corresponding parties. Next, we calculated the secret-key rate (i.e., the lower bound on the distilled key length per number of the sifted-key bits) $R = I_{A,B} - \min(I_{A,E}, I_{B,E})$ [27] as a function of Λ and p. Finally, we found the optimal cloning attack by maximizing $I_{A,B}$ for $R = 0$. The results of our theoretical analysis, as summarized in Fig. 3, imply that the optimal (cloning restricted) two-level-probe individual attack on R04 yields QBER $= 16.7\%$ for $\Lambda^2 = 4/11$ and $p = 4/7$. Our results for the analogous strategy for BB84 are shown in Fig. 3, where the best attack yields QBER $= 16.7\%$ for $\Lambda^2 = 1/3$ and $p = 1/2$. The QBER depends on the fidelity of cloning [QBER $= 1 - F_B$ for BB84 and QBER $= 4(1 - F_B)/(5 - 2F_B)$ for R04], while the information extracted by Eve depends both on the fidelity (as does $I_{A,E}$) and the entanglement of clones (correlations between Bob's and Eve's qubits). Thus, the optimal attack must balance these two quantities to provide $R = 0$ for a given $I_{A,B}$.

Experimental aspects of the eavesdropping.—In order to implement the cloning attack, we employed the

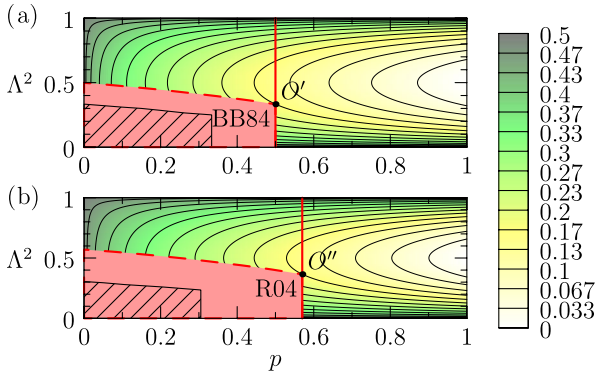

FIG. 3 (color online). Cloning parameters, QBER and the cloning-attack security of the (a) BB84 and (b) R04 as a function of the cloning asymmetry parameter p and cloning "strength" Λ. Dashed red lines show the QBER bound corresponding to the zero-length distilled key, i.e., $R = I_{A,B} - \min(I_{A,E}, I_{B,E}) = 0$. Thus, cloning enables successful eavesdropping in the regions marked by names of the QKDs. The optimal cloning attacks cause QBER $= 16.7\%$ if $p = 0.57$ and $\Lambda^2 = 0.36$ (point O'') for R04 and $p = 0.5$ and $\Lambda^2 = 0.33$ (point O') for BB84. The vertical solid red lines show the QBER bounds on the privacy of directly transmitted information corresponding to $I_{A,B} = I_{A,E}$, which are equal to 15.0% for R04 and 14.6% for BB84. The area of $\Lambda^2 \geq 1/2$ ($\Lambda^2 = 1/2$) corresponds to the mirror phase-covariant OQC [22] (the asymmetric phase-covariant OQC [5,25]). Hatched areas indicate the range of the cloning attacks without using quantum memory.

experimental setup (see Fig. 2), which consists of three main parts: the source of photon pairs, the cloner, and the two-photon polarization analyzer. Spatially separated photon pairs of $\lambda = 826$ nm wavelength are created in noncolinear type I degenerate spontaneous parametric down-conversion process in $LiIO_3$ crystal (1 cm thick) pumped by a cw Kr^+ laser beam (TEM_{00} mode, 250 mW of optical power). Our source approximates two synchronized SPSs with the accuracy adequate for our demonstration, since the probability of having more than one photon in a mode for the 1 ns detection window is much lower than the probability of single-photon detection (approximately 10^{-5} [20]). The emitted photons are in a separable polarization state; hence, Alice's state encoded as the signal does not change the polarization of the probe. Random choice of the states sent by Alice ensures that the polarization of the two photons is uncorrelated. This corresponds to having two independent but synchronized SPSs. However, in a real attack Eve would have to use a separate SPS. The photons propagate from the source to the OQC input via single-mode fibers. The photons are coherently superposed on the polarization-dependent beam splitter (PDBS). Next, the photons are subjected to polarization-sensitive filtering in both output modes (see BDA in Fig. 2). Finally, we postselect on coincidences—one photon in each of the two output modes of the cloner—and carry out polarization analysis of the two-photon

TABLE I. Performance of the OQC for BB84 and R04. The experimental values (subscript E) of the QBER and the secret-key rate R calculated from the measured density matrices are compared with theoretical predictions (subscript T). The success probability p_s of the OQC was estimated as in Ref. [21]. The OQC parameters p and Λ determine the shrinking of the Bloch sphere due to the cloning.

QKD	R	QBER	p_s	p	Λ^2
$BB84_T$	0.00	16.7%	13.7%	1/2	1/3
$BB84_E$	0.03 ± 0.03	$18.5\% \pm 1.5\%$	$15.1\% \pm 1.1\%$	1/2	1/3
$R04_T$	0.00	16.7%	12.7%	4/7	4/11
$R04_E$	0.01 ± 0.08	$18.0\% \pm 3.5\%$	$7.4\% \pm 0.1\%$	4/7	4/11

state [28]. Using our tomographical data, we estimated the two-photon density matrix applying the maximum likelihood method [29]. We used the tomography results to numerically simulate Eve's attack assuming that she probes Alice's photon, keeps the probe until key sifting, and passes the probed photon to Bob (for details see Ref. [20]). We calculated the QBER and secret-key rate and compared them with theoretical predictions in Table I.

The results indicate that our attack would be possible if QM was available. However, to deploy this device in a real QKD network, one has to consider several technological aspects of this attack. First, because of its probabilistic nature, the OQC introduces losses. The success probability of 10%–20% corresponds to 7–10 dB losses. Observing such losses might indicate that the line is insecure. Thus, Eve must mask these losses as usual channel losses. Supposing typical fibers losses of 3.5 dB/km (as for the fibers in our experiment and in [1]), Eve would need to replace 2–3 km of the line with a fiber of negligible losses. Using photons at telecom wavelengths would be more practical than 826 nm light for communicating over large distances since, for the telecom-window wavelengths, the loses are ~0.2 dB/km [1,2], which makes the distances about ten times larger and Eve's task more difficult. Typical detectors, designed for the telecom regime, provide low efficiency of about 0.25 (approximately 6 dB of losses) and high dark-count rate, i.e., noise. Much larger losses, which could enable eavesdropping, appear for long-range free-space transmission reaching, e.g., 157 dB for photons reflected from the Ajisai satellite [30]).

Eve should also control the unsuccessful cases when the signal and the probe propagate to Bob, who can detect them and raise alarm. Eve can achieve this by using quantum nondemolition (QND) measurement [31]. If she does not find a photon in her output mode, she will close the line towards Bob. Finally, Eve's attack relies on the perfect overlap between the signal and the probe photons (Hong-Ou-Mandel's interference). Typical full width at half maximum (FWHM) of photons generated via spontaneous parametric down-conversion corresponds to tens of μm. Thus, the requirement on the two-photon overlap is of the order of μm. This corresponds to a few fs. Any jitter caused by Alice leads to the reduced two-photon overlap, lower purity, and fidelity of the output states. Eve can however overcome this by performing the QND detection at her OQC input, which triggers the cloning process but requires photon generation on demand. In a real cloning attack Eve has to prepare photons of the same spectral properties as the photons sent by Alice. In our experiment we use photons at 826 nm with spectral width FWHM = 8.9 nm (160 fs coherence time). These are typical values reached by Alice using a femtosecond laser as a photon source. Let us note that the photon peaks need to overlap as perfectly as possible making the acceptable time difference corresponding to a fraction of coherence time which changes as the wavelength squared over FWHM. Hence, overlapping is easier for longer wavelengths (e.g., in the telecom window) and narrow FWHM. Both the parameters should be tuned by Alice to maximize the security of the QKD.

Conclusions.—We investigated the feasibility of symmetric individual attacks on BB84 [10] and R04 [11] assuming that Eve tracks the key sifting and uses a multifunctional OQC [21]. We optimized quantum cloning such that the minimum mutual information between an eavesdropper and a legitimate user was equal to the mutual information between the legitimate users at the lowest QBER. Thus, legitimate users cannot distil a secret key from their raw key bits. Consequently we found tolerable QBER for this kind of attack to be 16.7% for BB84 and R04. We performed the proof-of-principle experiment in which $R \approx 0$ was attained for QBER $= 18.5\% \pm 1.5\%$ for BB84 and QBER $= 18.0\% \pm 3.5\%$ for R04. Our experiment together with the reported progress in development of QM (see, e.g., [14]) suggest that, even in the presence of SPSs and perfect detectors, the QKD could be successfully attacked with a probe similar to ours if Alice and Bob tolerate too high QBER (see Table I) or losses (approximately 7 dB for our device). Our experiment shows that the OQCs are interesting both from the fundamental and practical points of view as tools of quantum cryptanalysis as they establish the security bound for an important class of QKDs.

We thank Ravindra Chhajlany, Anirban Pathak, and Radim Filip for discussions. K. B. and A. M. were supported by Grants No. DEC-2011/03/B/ST2/01903 and

No. DEC-2011/02/A/ST2/00305 of the Polish National Science Centre. K. B. and K. L. were supported by Grants No. CZ.1.05/2.1.00/03.0058, No. CZ.1.07/2.3.00/20.0017, No. CZ.1.07/2.3.00/20.0058, No. CZ.1.07/2.3.00/30.0004, and No. CZ.1.07/2.3.00/30.0041. A. Č. and J. S. acknowledge support by the GAČR Grant No. P205/ 12/0382.

*Electronic address.
bartkiewicz@jointlab.upol.cz
†Electronic address.
k.lemr@upol.cz

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[2] T.-Y Chen *et al.*, Opt. Express **18**, 27217 (2010).
[3] I. Georgescu and F. Nori, Phys. World **25**, 16 (2012).
[4] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[5] N. J. Cerf and J. Fiurášek, *Progress in Optics*, edited by E. Wolf (Elsevier, Amsterdam, 2006), Vol. 49, p. 455.
[6] N. Gisin, S. Pironio, and N. Sangouard, Phys. Rev. Lett. **105**, 070501 (2010).
[7] R. T. Glasser, H. Cable, J. P. Dowling, F. De Martini, F. Sciarrino, and C. Vitelli, Phys. Rev. A **78**, 012339 (2008); N. Spagnolo, C. Vitelli, V. G. Lucivero, V. Giovannetti, L. Maccone, and F. Sciarrino, Phys. Rev. Lett. **108**, 233602 (2012); C. Vitelli, N. Spagnolo, L. Toffoli, F. Sciarrino, and F. De Martini, Phys. Rev. Lett. **105**, 113602 (2010).
[8] F. De Martini, F. Sciarrino, and C. Vitelli, Phys. Rev. Lett. **100**, 253601 (2008).
[9] P. Sekatski, N. Brunner, C. Branciard, N. Gisin, and C. Simon, Phys. Rev. Lett. **103**, 113601 (2009).
[10] C. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), p. 175.
[11] J. M. Renes, Phys. Rev. A **70**, 052314 (2004).
[12] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010).
[13] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Nat. Commun. **2**, 349 (2011).
[14] H. Specht, C. Nölleke, A. Reiserer, M. Uphoff, E. Figueroa, S. Ritter, and G. Rempe, Nature (London) **473**, 190 (2011).
[15] N. Lütkenhaus, Phys. Rev. A **54**, 97 (1996).
[16] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[17] J.-C. Boileau, K. Tamaki, J. Batuwantudawe, R. Laflamme, and J. M. Renes, Phys. Rev. Lett. **94**, 040503 (2005).
[18] C. A. Fuchs, N. Gisin, R. B. Griffiths, C. S. Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997).
[19] N. Gisin and B. Huttner, Phys. Lett. A **228**, 13 (1997).
[20] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.110.173601 for technical details and extra figures.
[21] K. Lemr, K. Bartkiewicz, A. Černoch, J. Soubusta, and A. Miranowicz, Phys. Rev. A **85**, 050307(R) (2012).
[22] K. Bartkiewicz, A. Miranowicz, and Ş. K. Özdemir, Phys. Rev. A **80**, 032306 (2009).
[23] D. Bruß, M. Cinchetti, G. M. D'Ariano, and C. Macchiavello, Phys. Rev. A **62**, 012302 (2000).
[24] V. Bužek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).
[25] L. Bartůšková, M. Dušek, A. Černoch, J. Soubusta, and J. Fiurášek, Phys. Rev. Lett. **99**, 120505 (2007).
[26] A. Chefles, Contemp. Phys. **41**, 401 (2000).
[27] I. Csiszár and J. Körner, IEEE Trans. Inf. Theory **24**, 339 (1978).
[28] E. Halenková, A. Černoch, K. Lemr, J. Soubusta, and S. Drusová, Appl. Opt. **51**, 474 (2012).
[29] M. Ježek, J. Fiurášek, and Z. Hradil, Phys. Rev. A **68**, 012305 (2003).
[30] P. Villoresi *et al.*, New J. Phys. **10**, 033038 (2008).
[31] M. Bula, K. Bartkiewicz, A. Černoch, and K. Lemr, Phys. Rev. A **87**, 033826 (2013).