Photonic quantum simulator for unbiased phase covariant cloning

Laura T. Knoll,[1, 2] Ignacio H. López Grande,[1, 2] and Miguel A. Larotonda[1, 2, 3]

[1]*DEILAP, CITEDEF-CONICET, J.B. de La Salle 4397, 1603 Villa Martelli, Buenos Aires, Argentina*
[2]*Departamento de Física, FCEyN, UBA. Ciudad Universitaria, 1428 Buenos Aires, Argentina*
[3]*CONICET, Argentina*

We present the results of a linear optics photonic implementation of a quantum circuit that simulates a phase covariant cloner. We experimentally simulate the action of two mirrored $1 \to 2$ cloners, each of them biasing the cloned states into opposite regions of the Bloch sphere. We show that by applying a random sequence of these two cloners, an eavesdropper can mitigate the amount of noise added to the original input state and therefore mask its presence in a quantum key distribution protocol. Input polarization qubit states are cloned into path qubit states of the same photon, which is identified as a potential eavesdropper in a quantum key distribution protocol. The device has the flexibility to produce mirrored versions that optimally clone states on either the northern or southern hemispheres of the Bloch sphere, as well as to simulate optimal and non-optimal cloning machines by tuning the asymmetry on each of the cloning machines.

I. INTRODUCTION

The no-cloning theorem of quantum information is the formal statement of the fact that unknown quantum states cannot be perfectly copied [1, 2]. Without this restriction one would be allowed to completely determine the quantum state of a system by measuring copies of it, even leaving the original system untouched! This theorem underlies the security of all Quantum Key Distribution (QKD) protocols, and has consequences at a technological level, imposing limitations on error correction techniques and on other tasks that involve transmission of information [3–5]. Despite this strong restriction, several approximate cloning machines can be constructed. That is, the production of imperfect copies is indeed allowed. In general, this is achieved by coupling the system to be cloned to an auxiliary system and applying a trace-preserving, completely-positive map to the composite system [6–10].

Among the family of Quantum Cloning Machines (QCM), one can make a distinction between *universal* cloning machines (UQCM), which copy all the states with the same fidelity F, regardless of the state $|\psi\rangle$ to be cloned, and *state-dependent* QCM. Optimum UQCM can achieve a cloning fidelity F of $5/6 = 0.833$ [6–8, 11]. State-dependent machines can be designed to perform better for those restricted input states than a UQCM.

One of the most relevant features of quantum cloning is its usefulness for eavesdropping on QKD systems over noisy quantum channels. This quantum channel is controlled by Eve, the eavesdropper, who can perform any operation allowed by quantum mechanics. By exploiting quantum cloning, Eve can keep one of the output states and send another to the legitimate receiver, Bob. Eve's strategy is to try to get as much information as she can while producing as less disturbance in Bob's state. For this task, an *optimal* quantum cloning machine is required, in the sense that for a given fidelity of the original state, the fidelities of the cloned states are maximal. Depending of the specific QKD protocol, different cloning machines can be designed for optimal fidelity. That is, a UQCM may not be optimal for the specific set of states that are involved in a particular QKD protocol, but rather a particular state-dependent QCM may perform optimally the task [12, 13].

The best-known state-dependent QCM is the so-called phase-covariant QCM. It can optimally clone states of the form $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi}|1\rangle)$, that lie on the equator of the Bloch sphere. The Phase-Covariant Cloning (PCC) machine has a remarkable application in quantum cryptography, since it is used in the optimal incoherent strategy for eavesdropping on the BB84 QKD protocol [14–16] that runs with the bases of eigenstates of σ_x and σ_y. The eavesdropper on BB84 needs to gather information only on the four states $\frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ and $\frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)$, however it can be shown that the optimal solution for cloning these four states and for cloning all the states from the equator is the same [17].

The task of optimally cloning the equator of the Bloch sphere can be accomplished without ancilla [18]. This situation is usually depicted as a $1 \to 2$ cloning; a single qubit that interacts with another qubit in a blank state (Eve's qubit), which results in a transformation on a two qubit system that makes two imperfect copies of the first qubit. The asymmetric PCC transformation on Bob and Eve's qubit can be expressed as

$$|0\rangle_B|0\rangle_E \to |0\rangle_B|0\rangle_E$$
$$|1\rangle_B|0\rangle_E \to \sqrt{1-q}|1\rangle_B|0\rangle_E + \sqrt{q}|0\rangle_B|1\rangle_E \tag{1}$$

where $0 \le q \le 1$ controls the asymmetry of the cloning operation. Once applied to states on the equator, the reduced density matrices ρ_B and ρ_E can be obtained and the fidelities of the clones can be calculated as $F_B = \langle\psi|\rho_B|\psi\rangle = \frac{1}{2}(1 + \sqrt{1-q})$ and $F_E = \langle\psi|\rho_E|\psi\rangle = \frac{1}{2}(1 + \sqrt{q})$. Both fidelities are independent of the phase ϕ of the input state and for the symmetric case in which $q = 0.5$ we obtain $F_B = F_E = 0.8536$, outperforming a UQCM. Therefore, the PCC machine allows for a higher fidelity than that of the universal cloning machine for all states on the equator of the Bloch sphere.

A relevant issue is that being not universal, a PCC machine comprises an operation that shrinks the Bloch sphere of the copied state non-uniformly towards the north pole (i.e. the $|0\rangle$ state). As a consequence, a bias on the σ_z basis appears when cloning states that lie on the Bloch sphere's equator. Such footprint can be easily detected in a QKD implementation just by adding a single projective measurement in the σ_z basis (for example, detecting $|0\rangle$ states). To overcome this issue, a desirable property of a PCC machine is for it to be able to prepare clones with no bias but with the same individual fidelity. This can be achieved by performing the transformation (1) and also its mirrored version, that is, one that shrinks the bloch sphere towards the $|1\rangle$ state. Several experimental implementations of the PCCM have been performed mainly using photons [19–23] and NMR systems [24, 25]. The use of mirrored PCCM has been introduced in [26–28], in the context of assuming partial knowledge about the input state.

In this work we simulate the mirrored PCC machines using two qubits encoded in the polarization and linear momentum (path) degrees of freedom of a single photon, and the interaction is produced in a linear optics setup, via a series of displaced Sagnac polarizing interferometers. We experimentally observe that by alternating randomly between these two operations, Eve can generate a balanced mixture of cloned states and pass unnoticed the test sketched above. In spite of the fact that the polarization-path dual encoding does not produce a physical clone of the transmitted qubits, with this setup we can access to the full range of the cloning parameter q, which allows us to study optimal and non-optimal cloning conditions. The asymmetry of the clones is easily tunable by means of a waveplate rotation, without the need of custom beam splitters or imposing additional losses that reduce the overall throughput, as required in two photon experiments. Furthermore, the instrinsic stability of the displaced Sagnac interferometers does not require any active stabilization, allowing to study the PCC protocol in different regimes.

Section II of this work presents the experimental setup that implements the phase-covariant cloning machines, and Section III is devoted to the results obtained for different experimental conditions.

II. PHOTONIC QUANTUM SIMULATOR

The experimental arrangement that implements the PCC machine is shown in Figure 1. In this scheme, Alice and Bob share a polarization-entangled photonic state. Photon pairs are generated by spontaneous parametric downconversion (SPDC) in a BBO type-I nonlinear crystal arrangement [29, 30], pumped by a 405nm CW laser diode, polarization entanglement is optimized using temporal and spatial compensating birefringent crystals on the pump beam and on the photon pair paths. Alice's photon is directed into a polarization analysis arrange-

ment where she may perform projective measurements on her photon. Single-photon counting devices detect the incoming photons and send the detections to an FPGA-based coincidence counter.

A. Linear optics PCC implementation

In this quantum simulator, the eavesdropper is encoded on the path qubit of Bob's photon using a displaced Sagnac interferometer based on a polarizing beam splitter (PBS) [31]. An equivalent optical setup has been implemented using calcite beam displacers in [32] to study the dynamics of multipartite entanglement. By associating the horizontal polarization component H with the state $|0\rangle$ and the vertical polarization V with state $|1\rangle$, and the eavesdropper is represented by the two path modes of the photon (0 and 1), the PCC transformation is implemented as follows: an incoming photon in mode 0 is split into its H and V components by the PBS. The vertically polarized photons are reflected and propagate inside the interferometer in the clockwise direction, passing through a half-wave plate (H1) which transforms the vertical polarization state into $\cos(2\alpha)|V\rangle + \sin(2\alpha)|H\rangle$, where α is the physical angle of the half-wave plate. The horizontal component of this rotated state exits the interferometer, transmitted into mode 1 (dashed-line in Fig.1) with probability $q = \sin^2(2\alpha)$, while the vertical component is reflected into mode 0 with probability $1 - q = \cos^2(2\alpha)$.

On the other hand, the horizontally polarized photons of the input state propagate through the interferometer in the counter-clockwise direction and exit through the PBS into mode 0, with their polarization state unchanged. In this way, we obtain the following transformation

$$
\begin{aligned}
|H\rangle|0\rangle &\rightarrow |H\rangle|0\rangle \\
|V\rangle|0\rangle &\rightarrow \sqrt{1-q}|V\rangle|0\rangle + \sqrt{q}|H\rangle|1\rangle,
\end{aligned}
\tag{2}
$$

which is a PCC transformation (1) with $q = \sin^2(2\alpha)$. A HWP oriented at $0°$ (H2) is placed on the H photons path to compensate for the optical path difference. The relative path length of the interferometer is adjusted so that when H1 is oriented at $0°$ the polarization of the input state remains unaltered.

Bob performs standard quantum state tomography (QST) of his polarization state, in coincidence with Alice's detections, using quarter-wave plates on each path, a half-wave plate, and a third passage through the polarizing beam splitter. H polarized photons on mode 1 are rotated by a HWP oriented at $45°$ (H3) just before passing through the PBS. This operation recombines mode 1 into mode 0 coherently so that both modes exit the interferometer through the same path. Eve's qubit encoded on Bob's path photon is mapped into a polarization qubit by this operation, since photons propagating through mode 0 are horizontally polarized at the output of the PBS and photons propagating through mode 1 are vertically po-

larized. Therefore, Eve can also perform standard QST on her qubit using a QWP, a HWP and a PBS.
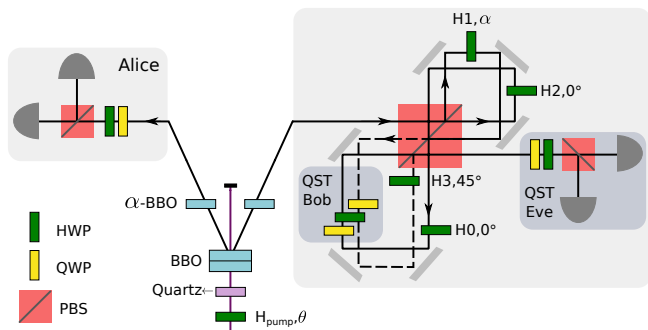

FIG. 1: (Color online) Experimental setup for the implementation of the phase covariant cloning machine. The PCC machine is implemented using a displaced Sagnac polarization interferometer: photons enter the interferometer through a PBS, where the H and V polarization components are routed in different directions. If $\alpha = 0°$ ($H1$) both polarization components are coherently recombined in the PBS and exit the interferometer in the same path. For every other angle of α the V component is transformed into an H polarized photon with probability $q = \sin^2(2\alpha)$ and exits the interferometer through path mode 1, in dashed-lines. Bob may perform quantum state tomography on his polarization qubit before it exits the interferometer using a combination of QWPs and a HWP. Both paths are later coherently recombined using a HWP oriented at $45°$ (H3) on path 1 and pass one more time through the polarizing beam splitter. In this way, Eve's qubit is ultimately mapped into a polarization qubit and standard quantum state tomography can be performed using another set of QWP, HWP and a PBS.

B. Mirrored Device

We now describe how to obtain the action of a mirrored PCC operation, so that the fidelity for cloning states on the southern hemisphere is now enhanced. This transformation is implemented in the following way: for the input states $\{|1\rangle_B|0\rangle_E, |0\rangle_B|0\rangle_E\}$ we first apply a bit-flip operation on the first qubit, followed by the PCC (1), and finally another bit-flip on the first qubit, resulting in the following transformation

$$
\begin{aligned}
|1\rangle_B|0\rangle_E &\to |1\rangle_B|0\rangle_E \\
|0\rangle_B|0\rangle_E &\to \sqrt{1-q}|0\rangle_B|0\rangle_E + \sqrt{q}|1\rangle_B|1\rangle_E
\end{aligned}
\tag{3}
$$

where again $0 \leq q \leq 1$ controls the asymmetry of the cloning operation. It is easy to see that for states on the equator the fidelities of the clones are once again $F_B = \langle\psi|\rho_B|\psi\rangle = \frac{1}{2}(1 + \sqrt{1-q})$ and $F_E = \langle\psi|\rho_E|\psi\rangle = \frac{1}{2}(1 + \sqrt{q})$, independent of the phase ϕ of the input state. This operation shrinks the Bloch sphere of the copied state towards the state $|1\rangle$. By applying randomly these two mirrored operations, Eve can clone the equatorial

states with optimized fidelity, while adding no bias on σ_z.

Interestingly, the mirrored operation can be easily implemented with the same setup by simply rotating half-wave plate H2 instead of H1, which in turn remains fixed at $0°$. In this case, the horizontally polarized photons passing through half-wave plate H2 are transformed into $\cos(2\alpha')|H\rangle + \sin(2\alpha')|V\rangle$, where α' is the physical angle of the half-wave plate and we obtain

$$
\begin{aligned}
|V\rangle|0\rangle &\to |V\rangle|0\rangle \\
|H\rangle|0\rangle &\to \sqrt{1-q}|H\rangle|0\rangle + \sqrt{q}|V\rangle|1\rangle,
\end{aligned}
\tag{4}
$$

which is equivalent to the mirrored-PCC operation (3) with $q = \sin^2(2\alpha')$. Throughout the rest of the text we will refer to the machines described in (2) and (4) as PCC(+) and PCC(−) respectively.

The action of these mirrored PCC machines can indeed be implemented in two photon experiments, where typically both qubits are encoded on the polarization degree of freedom of two different photons by simply adding half-wave plates before and after the cloning operation, on the signal's qubit path. When rotated at $45°$, these HWPs essentially perform a bit-flip operation on the signal qubit, which allows for the mirrored PCC to be implemented as described above. Nevertheless, these experimental implementations require more complicated setups, have low throughput due to multiple coincidence requirements [20, 33], and they are less suited to serve as testbeds for different conditions of the cloning protocol.

III. RESULTS

With this experimental setup we can prepare and measure an arbitrary qubit state, and control the asymmetry of the cloning operation by simply rotating half-wave plate H1 (or H2). We tested the action of the PCC machines for different experimental conditions: we projected different polarization states on Alice's qubit and performed quantum state tomography on Bob and Eve's qubits. In this way, we obtained the density matrix of both clones and calculated the fidelities for different states and cloning parameters.

A. Equatorial States

Figure 2 shows the theoretical curves and the experimentally measured fidelities for both Bob and Eve's qubits while Alice's qubit is projected onto state $|D\rangle\langle D|$, for different values of the cloning parameter q and for both PCC(+) and PCC(−). The shaded areas represent the experimental error. As the cloning parameter increases, Bob's fidelity decays to its minimum value $F=0.5$, while Eve's fidelity achieves its maximum when $q=1$. The experimental data shows a good agreement with the theoretical predictions. The fidelity of both

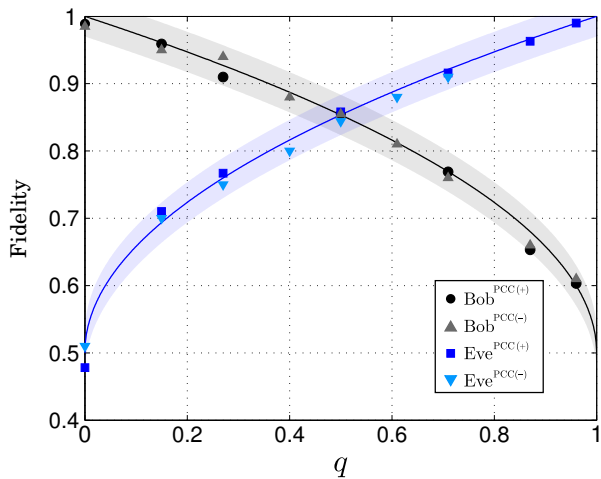cloning machines show the same behavior as a function of the cloning parameter.

FIG. 2: (Color online) Fidelity of the clones with respect to the original state $|D\rangle$, for different cloning parameters q, for both PCC (+) and its mirrored operation (−). Filled lines represent the theoretical prediction and the different symbols the experimental data. The shaded area around the theoretical curve accounts for the experimental error.

A PCC machine clones equally well all states from the equator of the Bloch sphere: by projecting different states on the equator on Alice's side for a particular cloning parameter (q=0.4), we obtained the results shown on figure 3. The theoretical curves are obtained calculating the fidelity between the ideal equatorial states and the states resulting from projection and cloning processes, applied to the experimentally available input state. Both fidelities for Bob and Eve remain almost constant within the experimental error (represented by the shaded region), as expected. That is, for states of the form $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi}|1\rangle)$ the fidelity of the clones is independent of the phase ϕ, excluding experimental limitations. This particular election of the cloning parameter produces unbalanced fidelities for the two clones.

B. Non-Equatorial States

Finally, we projected different states of the form $|\psi\rangle = \cos(2\theta)|H\rangle + \sin(2\theta)|V\rangle$ on Alice's qubit and reconstructed the density matrix for both Bob and Eve's qubits, for q=0.5. Figure 4 shows the calculated fidelities for both clones, performing the traditional PCC (black line) and its mirrored operation (blue line). The different symbols represent the experimental data for both operations. Once again, there is a good agreement between the experimental data and the theoretical predictions: PCC(+) clones the state $|H\rangle$ with maximum fidelity (F=1) and state $|V\rangle$ with the minimum possible fidelity (F=0.5), while the PCC(−) operates in the
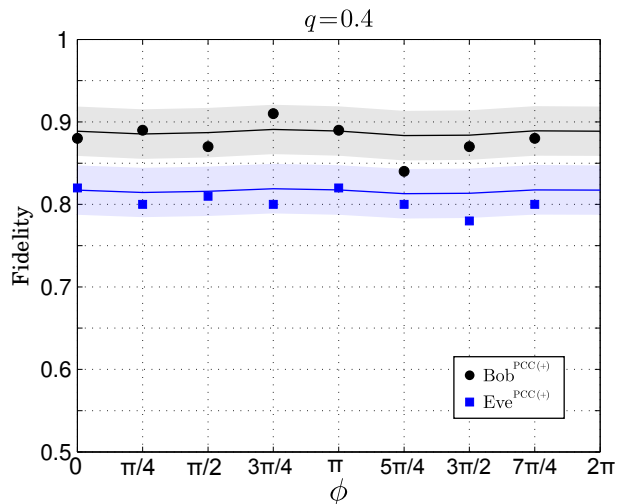

FIG. 3: (Color online) Fidelity of the clones for different states on the equator, characterized by the phase ϕ, for q=0.4. The theoretical predictions were calculated numerically based on the entangled input state. The experimental fidelity is shown in black circles for Bob's qubit and blue squares for Eve's. The shaded area represents the experimental error.

exact opposite way. Both pairs of curves cross at the balanced superposition state, $\theta = \pi/8$, recovering the symmetric cloning condition with a measured fidelity of 0.852 ± 0.005.
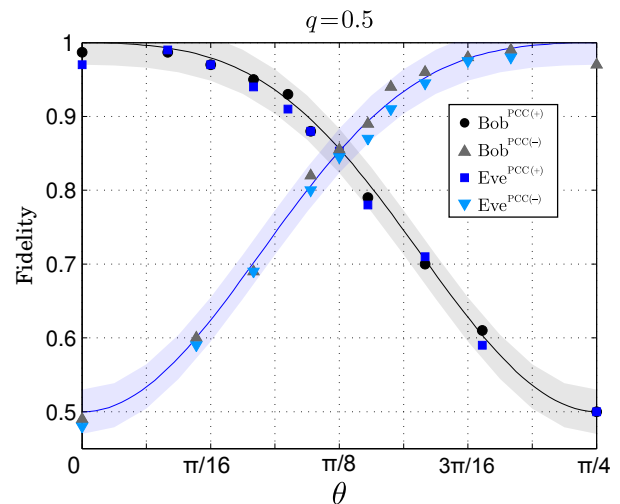

FIG. 4: (Color online) Fidelity of the clones for different states of the form $\cos(2\theta)|H\rangle + \sin(2\theta)|V\rangle$, for $q = 0.5$. Theoretical curves for the PCC(+) (black line) and PCC(−) operation (blue line) are shown. The different symbols plot the experimental data for both operations and the shaded area represents the experimental error.

C. Eavesdropping with PCC

The security limit for the BB84 protocol against incoherent attacks arises on an eavesdropping scenario where Eve uses a PCC machine. This kind of attack can be easily identified if Bob performs measurements on σ_z (or at least he can project the qubits in one of the two states of the basis), because a side effect of this attack is a bias in the value of σ_z of the ensemble of received states with respect to the original emitted states ($\sigma_z = 0$). For a PCC attack the bias in terms of the cloning parameter q is: $\langle \sigma_z \rangle = q$.

Detecting this kind of attack can be used by Alice and Bob to reduce the information gained by Eve, for example by moving to a six-states BB84 protocol [34] every time that a significant bias value is detected.

The track left by Eve can be erased if she uses a slightly different strategy, that consists on alternating randomly between PCC(+) and PCC(−). Thus sending Bob ensembles of cloned states with no bias in σ_z but with the same individual fidelity. Figure 5 shows the effect on the σ_z mean value for different cloning parameters q under the action of PPC(+) and the strategy proposed above: while the first protocol adds an increasing bias on the computational basis measurement for increasing values of q, the second strategy leaves the z component unbiased, for any strength of the cloning parameter. It can be seen that the experimental implementation of these eavesdropping strategies clearly show the described behaviors.
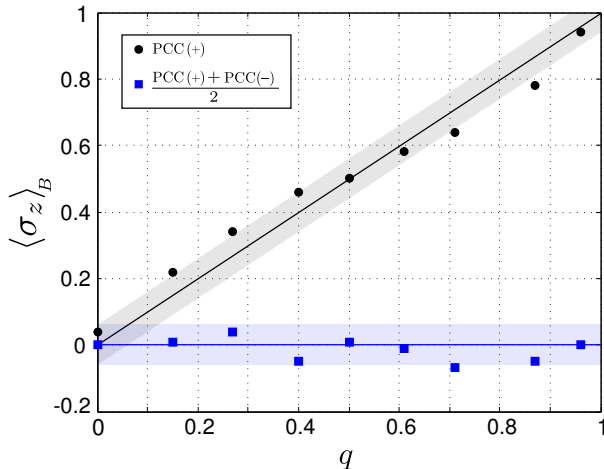
IV. CONCLUSIONS

We have presented the results of a photonic realization of a protocol that fully simulates a phase-covariant cloning machine, where Alice and Bob share a polarization entangled state, while the eavesdropper is encoded on Bob's path qubit. The cloning algorithm is implemented by means of a displaced Sagnac interferometer and retardation waveplates. The versatility of the experimental setup allows us to prepare and measure an arbitrary qubit state, and easily control the asymmetry of the cloning operation in its two mirrored designs. We tested the action of the PCCM and its mirrored version for different experimental conditions, by projecting different polarization states on Alice's qubit, and performing quantum state tomography on Bob and Eve's qubits.

On an eavesdropping scenario where Eve uses a PCC machine, output states are left unbalanced in the σ_z basis after the cloning procedure and could therefore be detected by Bob just by adding a single projective measurement in the σ_z basis. We showed that by alternating between both cloning operations PCC(+) and PCC(−), Eve can mask her presence by sending Bob cloned states with no bias in σ_z but with the same individual fidelity.

FIG. 5: (Color online) Mean value of the σ_z component of Bob's reconstructed density matrix for different cloning parameters q. The black line and circles correspond to PCC (+) while the blue line and squares represent the averaged values of σ_z for an unbiased sequence of PCC (+) and PCC (−) implementations. The shaded area around the theoretical curves accounts for the experimental error.

[1] W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).

[2] D. Dieks, Physics Letters A **92**, 271 (1982).

[3] R. F. Werner, in *Quantum information* (Springer, 2001), pp. 14–57.

[4] P. H. Eberhard and R. R. Ross, Foundations of Physics Letters **2**, 127 (1989).

[5] A. Peres and D. R. Terno, Reviews of Modern Physics **76**, 93 (2004).

[6] V. Bužek and M. Hillery, Physical Review A **54**, 1844 (1996).

[7] D. Bruß, D. P. DiVincenzo, A. Ekert, C. A. Fuchs, C. Macchiavello, and J. A. Smolin, Physical Review A **57**, 2368 (1998).

[8] N. Gisin and S. Massar, Physical review letters **79**, 2153 (1997).

[9] J. Fiurášek, R. Filip, and N. J. Cerf, Quantum Information & Computation **5**, 583 (2005).

[10] S. Iblisdir, A. Acin, and N. Gisin, arXiv preprint quant-ph/0505152 (2005).

[11] N. Gisin, Physics Letters A **242**, 1 (1998).

[12] G. M. DAriano and P. L. Presti, Physical Review A **64**, 042308 (2001).

[13] G. M. DAriano and C. Macchiavello, Physical Review A **67**, 042306 (2003).

[14] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, Physical Review A **56**, 1163 (1997).

[15] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Physical Review Letters **88**, 127902 (2002).

[16] D. Bruß, M. Cinchetti, G. M. DAriano, and C. Macchiavello, Physical Review A **62**, 012302 (2000).

[17] V. Scarani, S. Iblisdir, N. Gisin, and A. Acin, Reviews of Modern Physics **77**, 1225 (2005).

[18] C.-S. Niu and R. B. Griffiths, Physical Review A **60**, 2764 (1999).

[19] F. Sciarrino and F. De Martini, Physical Review A **72**, 062313 (2005).

[20] J. Soubusta, L. Bartůšková, A. Černoch, M. Dušek, and J. Fiurášek, Physical Review A **78**, 052323 (2008).

[21] L. Bartůšková, M. Dušek, A. Černoch, J. Soubusta, and J. Fiurášek, Physical review letters **99**, 120505 (2007).

[22] J.-S. Xu, C.-F. Li, L. Chen, X.-B. Zou, and G.-C. Guo, Physical Review A **78**, 032322 (2008).

[23] Z. Zhao, A.-N. Zhang, X.-Q. Zhou, Y.-A. Chen, C.-Y. Lu, A. Karlsson, and J.-W. Pan, Physical review letters **95**, 030502 (2005).

[24] H. Chen, X. Zhou, D. Suter, and J. Du, Physical Review A **75**, 012317 (2007).

[25] J. Du, T. Durt, P. Zou, H. Li, L. C. Kwek, C. Lai, C. H. Oh, and A. Ekert, Physical review letters **94**, 040505 (2005).

[26] J. Fiurášek, Physical Review A **67**, 052314 (2003).

[27] V. Karimipour and A. Rezakhani, Physical Review A **66**, 052111 (2002).

[28] K. Lemr, K. Bartkiewicz, A. Černoch, J. Soubusta, and A. Miranowicz, Physical Review A **85**, 050307 (2012).

[29] P. G. Kwiat, E. Waks, A. G. White, I. Appelbaum, and P. H. Eberhard, Physical Review A **60**, R773 (1999).

[30] L. T. Knoll, C. T. Schmiegelow, and M. A. Larotonda, Applied Physics B **115**, 541 (2014).

[31] M. Almeida, F. de Melo, M. Hor-Meyll, A. Salles, S. Walborn, P. S. Ribeiro, and L. Davidovich, Science **316**, 579 (2007).

[32] O. J. Farías, G. H. Aguilar, A. Valdés-Hernández, P. S. Ribeiro, L. Davidovich, and S. P. Walborn, Physical review letters **109**, 150403 (2012).

[33] J. Soubusta, L. Bartůšková, A. Černoch, J. Fiurášek, and M. Dušek, Physical Review A **76**, 042318 (2007).

[34] D. Bruß, Physical Review Letters **81**, 3018 (1998).