Quantum and classical noise in practical quantum-cryptography systems based on polarization-entangled photons

S. Castelletto*

Optical Technology Division, National Institute of Standards and Technology, Gaithersburg, Maryland 20899-8441

I. P. Degiovanni[†] and M. L. Rastello

Istituto Elettrotecnico Nazionale G. Ferraris, Strada delle Cacce 91, I-10135 Torino, Italy

Quantum-cryptography key distribution (QCKD) experiments have been recently reported using polarization-entangled photons. However, in any practical realization, quantum systems suffer from either unwanted or induced interactions with the environment and the quantum measurement system, showing up as quantum and, ultimately, statistical noise. In this paper, we investigate how an ideal polarization entanglement in spontaneous parametric down-conversion (SPDC) suffers quantum noise in its practical implementation as a secure quantum system, yielding errors in the transmitted bit sequence. Since all SPDC-based QCKD schemes rely on the measurement of coincidence to assert the bit transmission between the two parties, we bundle up the overall quantum and statistical noise in an exhaustive model to calculate the accidental coincidences. This model predicts the quantum-bit error rate and the sifted key and allows comparisons between different security criteria of the hitherto proposed QCKD protocols, resulting in an objective assessment of performances and advantages of different systems.

I. INTRODUCTION

Quantum-cryptography key distribution (QCKD) is at the moment the most advanced and challenging application of quantum information. QCKD offers the possibility that two remote parties, sender and receiver (conventionally called Alice and Bob), can exchange a secret random key, called sifted key (string of qubits), to implement a secure encryption or decryption algorithm based on a shared secret key, without the need that the two parties meet [1–3].

In a practical QCKD, Alice and Bob use a quantum channel, along which sequences of signals are either sent or measured at random between different bases of orthogonal quantum states. Alice can play the role of either setting randomly the polarization basis of photons and sending them to Bob (faint laser pulses as photon source), or measuring photons randomly in any one of the selected bases (entangled-photon source). Bob, randomly and independently from Alice, measures in one of the bases. The sifted key consists of the subset of measurements performed when bases of Alice and Bob are in an agreed configuration according to the protocol used, obtaining at this point a deterministic outcome whose security relies on the laws of quantum physics, for they previously agreed upon the correspondence between counting a photon in a specific state and the bit values 0 or 1. In contrast, the security of conventional cryptography relies upon the unproven difficulty in factorizing large numbers into prime numbers by a conventional algorithm. We note that there is no guarantee that such an algorithm does not exist.

The underlying feature of QCKD, namely, the reliance of the security of the distributed secret key on the laws of quantum physics [1–3], gives it an advantage over the public key cryptography. In other words, the uncertainty principle prohibits one from gaining information from a quantum channel without disturbing it. Basically, QCKD is based on the principle that when a third party (Eve) performs a measurement on a qubit exchanged, she induces a perturbation, yielding errors in the bit sequence transmitted, revealing her presence. Any attempt by Eve to obtain information about the key leads to a nonzero error rate in the generated sifted key. Nevertheless, this last claim must be somewhat softened because of practical realization of quantum channels [4]. Unfortunately, in practical systems, errors also happen because of experimental leakage, such as losses in optics, detection, electronics, and noise. Also, even when no eavesdropper is disturbing the bit exchange, there will be errors in the transmission and strings of Alice and Bob will not coincide perfectly. Thus, in practice, there is no way to distinguish an eavesdropper attack from experimental imperfections, making it necessary to establish an upper bound on tolerable experimental imperfections in the realization of the quantum channels to implement an error-correction procedure.

Following the first proposal by Bennett and Brassard [1] and later the Ekert protocol invoking entangled states [2], various systems of QCKD have been implemented and tested by groups around the world. Recently, some research groups [5–9] performed the first QCKD experiments based on polarization-entangled photon pairs, and Brassard *et al.* [4] proved theoretically that QCKD schemes based on spontaneous parametric down-conversion (SPDC) offer enhanced performance, mostly in terms of security, compared to QCKD based on weak coherent pulses.

Entangled photons, generated by SPDC in nonlinear crystals, have proved to be largely successful for quantum optical communication [10–13] and quantum radiometry [14–23].

*Electronic address: castelle@ien.it

[†]Electronic address: degio@ien.it

Furthermore, basic experimental tests of the foundation of quantum mechanics had been performed by exploiting the entanglement of this source [24–26]. However, quantum noise in a SPDC quantum state may significantly limit the performance of the proposed quantum optical communication and information technologies.

In this paper, we provide a general model for an *a priori* evaluation of some crucial parameters of a general QCKD scheme based on polarization-entangled photons. We basically adopt the formalism of quantum operations [27] to describe the dynamics of an open quantum system subject either to the interactions with the environment or to a quantum device performing a measurement on it. These unwanted or induced interactions show up as noise in quantum-information processing systems degrading their ideal performance. Exploiting the quantum-operation formalism, we present a model to quantify precisely both quantum and ultimately statistical noise in quantum-information experiments performed using an entangled-photon source.

In Sec. II, we consider quantum noise in a lossless measurement system, where noise is due to the coupling between the polarization mode of the source with the polarizing beam splitter ports. In Sec. III, we discuss the case of a lossy system, where noise is induced by detection deficiencies, such as losses of correlated photons from the presence of optical elements, nonideal detectors, and electronic devices in either channel, and detector dark counts.

The model concludes with the calculation of an overall probability of total coincidence counts, including an imperfect time-correlation measurement, ultimately yielding an estimate of accidental coincidences (Sec. IV).

This result is used in the calculation of the quantum-bit error rate (QBER) for QCKD protocols, i.e., Bennett-Brassard 1984 (BB84) and the two variants of Ekert's protocol, based on Clauser-Horne-Shimony-Holt (CHSH) inequalities and Wigner's inequalities, respectively (Sec. V). Previsions are also presented about the sifted and the corrected key, the QBER before and after a standard error-correction procedure. Finally, we evaluate the performance of security criteria for Ekert's protocols based on both the CHSH inequality and the Wigner inequality (Sec. VI).

II. QUANTUM NOISE IN POLARIZATION SELECTION OF PHOTON PAIRS

In this section, we consider a real either nonmaximally entangled or partially mixed state resulting from both imperfect entangled state generation by SPDC and imperfect polarization state selection by real polarizing beam splitters (PBSs).

In Fig. 1, we depict the typical scheme for quantum-cryptography key distribution as implemented using entangled photons generated by SPDC. Due to nonlinear interaction in a $\chi^{(2)}$ crystal, some pump photons (angular frequency ω_p) spontaneously split into a lower-frequency pair of photons, historically called signal and idler, perfectly correlated in all aspects of their state (direction, energy, polarization, under the constraints of conservation of energy and wave-vector momentum, otherwise known as phase
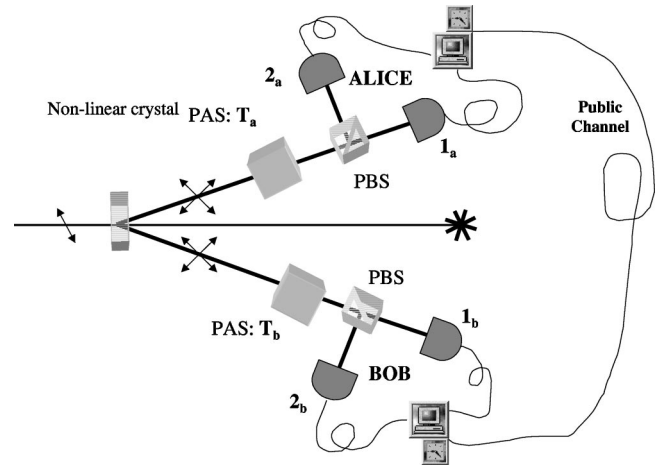

FIG. 1. QCKD setup: polarization-entangled photons generated by SPDC are directed to the two parties (Alice and Bob). The bit sequence of the key is obtained by means of polarization-sensitive synchronized measurements performed by Alice and Bob according to a specific QCKD protocol.

matching). These entangled states show perfect correlation for polarization measured along orthogonal but arbitrary axes.

The QCKD performed by pure entangled states relies on the realization of two quantum correlated optical channels. These channels yield single-photon polarization states, such that whenever Alice performs a polarization measurement on a photon of the pair, automatically the other photon is projected in a defined polarization state, i.e., Alice plays the role of triggering Bob's measurement. In reality, the light field emerging from the output of the nonlinear crystal is a polarization-entangled multimode state. However, it can be described as a polarization entangled two-photon state in only two effective modes (one for channel a and the other for channel b), as signal and idler pairs can be easily emitted noncollinearly with the pump by proper phase-matching rules [28]. This scheme eventually is exploited in quantum-information applications by using one channel as the trigger or reference (a) and the other channel as the probe (b). According to Fig. 1, we denote Alice's detector apparatus to be the trigger and Bob's to be the probe. Detection apparatus of Alice and Bob consists of polarization-analyer systems (PASs) for proper single-beam polarization rotation, PBSs, photon detectors (1_a, 2_a, 1_b, 2_b), data storage systems (computers), and synchronization systems.

Let us consider in the following type-II SPDC entangled states [29], where the output two-photon states are a quantum superposition of orthogonally polarized photons, i.e., the singlet state [30]:

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|H_a\rangle|V_b\rangle - |V_a\rangle|H_b\rangle).$$

Practically, pure entanglement may not be achieved because of imperfect source generation and incomplete entangled-photon collection. According to Refs. [31,32], an uncompensated coherence loss, induced in the state by the

coupling between polarization and frequency modes because of a birefringent environment, may produce a partially mixed or nonmaximally entangled state. Also the collection of the same number of entangled photons on both channels is unlikely, mostly due to the imperfect positioning of the detection systems along the true directions of entangled photons on the SPDC cones. Two complex variables, ζ ($|\zeta| \leq 1$) and ϵ, characterize the imperfect compensation of dephasing and decoherence in the crystal and the misalignment in collecting entangled photons in the optical paths, respectively. The net result is a nonmaximally entangled, or partially mixed state, written as

$$\hat{\rho}^{\psi} = \frac{1}{1+|\epsilon|^2} [|H_a\rangle|V_b\rangle\langle V_b|\langle H_a| + |\epsilon|^2 |V_a\rangle|H_b\rangle\langle H_b|\langle V_a|$$
$$- \epsilon\zeta|V_a\rangle|H_b\rangle\langle V_b|\langle H_a| - (\epsilon\zeta)^*|H_a\rangle|V_b\rangle\langle H_b|\langle V_a|].$$

We analyze now the quantum noise introduced via an imperfect polarization state selection by the PBSs depicted in Fig. 1. Here, the entangled photons are detected according to their polarizations by using imperfect PBSs on both arms and perfect single-photon detectors. The PBSs project photons onto a polarization basis $\{|H_a\rangle|H_b\rangle, |V_a\rangle|V_b\rangle, |H_a\rangle|V_b\rangle, |V_a\rangle|H_b\rangle\}$, while the PASs induce the transformations represented by the unitary operators $\hat{T}_z$ in each arm ($z = a,b$), according to

$$\hat{T}_z|H_z\rangle = c_1|H_z\rangle + c_2|V_z\rangle,$$

$$\hat{T}_z|V_z\rangle = c_2^*|H_z\rangle - c_1^*|V_z\rangle.$$

In the case of ideal PBSs, channel z transmits state $|H_a\rangle$ ($|H_b\rangle$) and reflects state $|V_a\rangle$ ($|V_b\rangle$), i.e., there is a perfect coupling between the output ports of the PBSs and the projections of the photon polarization state. In the approach so far adopted in the literature, a perfect coupling is always assumed because the measurement process is considered as a projection on polarization states $|H_a\rangle$, $|V_a\rangle$, $|H_b\rangle$, $|V_b\rangle$, thus assuming detectors 1_a, 1_b, 2_a, 2_b, are sensitive to polarization. Here we consider a further noise effect induced by the presence of real PBSs, where a small part of the photons projected onto $|V_a\rangle$ ($|V_b\rangle$) are erroneously transmitted, and some photons projected in the state $|H_a\rangle$ ($|H_b\rangle$) are erroneously reflected (generally less than 2% and 5%, respectively), as shown in Fig. 2. For this purpose, we extend the Hilbert space to describe these photon states as

$$|H_z\rangle|O1_z\rangle = t_z|H_z\rangle|I1_z\rangle + r_z|H_z\rangle|I2_z\rangle,$$

$$|H_z\rangle|O2_z\rangle = t_z|H_z\rangle|I2_z\rangle + r_z|H_z\rangle|I1_z\rangle,$$

$$|V_z\rangle|O1_z\rangle = r_z^{\perp}|V_z\rangle|I2_z\rangle + t_z^{\perp}|V_z\rangle|I1_z\rangle,$$

$$|V_z\rangle|O2_z\rangle = r_z^{\perp}|V_z\rangle|I1_z\rangle + t_z^{\perp}|V_z\rangle|I2_z\rangle, \quad (1)$$

where $|Ox_z\rangle$ represents the photon crossing the output port of the PBS towards detector x_z and $|Ix_z\rangle$ represents the photon crossing the input port of the PBS, with $x = 1,2$. $|t_z^{\perp}|^2$ is
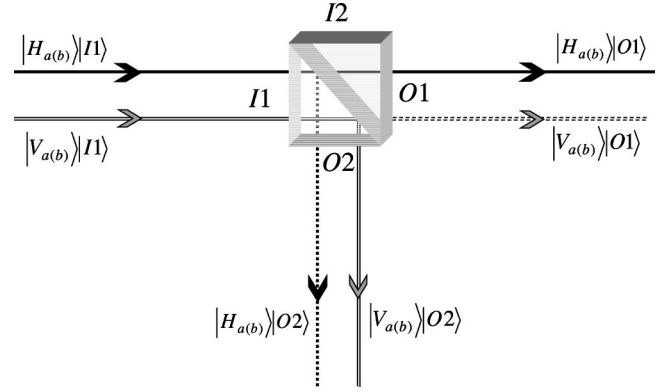

FIG. 2. Real PBS: all photons projected in $|V_{a(b)}\rangle$ polarized state should be reflected, but some of these are wrongly transmitted. Moreover, all photons projected in $|H_{a(b)}\rangle$ polarized state should be transmitted, but some of these are erroneously reflected.

the transmittance of photons in the $|V_z\rangle$ polarization state, and $|r_z^{\perp}|^2 = 1 - |t_z^{\perp}|^2$ is the corresponding reflectance, whose phase relation is $r_z^{\perp}/t_z^{\perp} = i|r_z^{\perp}|/|t_z^{\perp}|$. Analogously, $|t_z|^2$ and $|r_z|^2$ are the transmittance and reflectance of photons in the $|H_z\rangle$ state. So far, we have considered only lossless PBSs. The effect of photon losses due to all optical devices used in the channels are treated in Secs. III and IV.

We define the input density matrix for the PBS ports as

$$\hat{\rho}^{\mathrm{PBS}} = |I1_a\rangle|I1_b\rangle\langle I1_b|\langle I1_a|,$$

and the total input density matrix $\hat{\rho}^{\mathrm{in}}$ of the photon system as

$$\hat{\rho}^{\mathrm{in}} = \hat{\rho}^{\psi} \otimes \hat{\rho}^{\mathrm{PBS}}.$$

The formalism of quantum operation is the most suitable to describe the evolution of a quantum system coupled with another quantum system or with the environment, as well as the evolution of a quantum system subject to measurement [27]. In this context, we consider a set of non-trace-preserving quantum operations $\{\mathcal{E}_{x_a y_b}\}$ defined as

$$\mathcal{E}_{x_a y_b}(\hat{\rho}^{\psi}) = \mathrm{Tr}_{\mathrm{PBS}}(\hat{P}_{x_a y_b}\hat{U}_{\psi\text{-PBS}}\hat{S}_{\psi}\hat{\rho}^{\mathrm{in}}\hat{S}_{\psi}^{\dagger}\hat{U}_{\psi-\mathrm{PBS}}^{\dagger}\hat{P}_{x_a y_b}^{\dagger}),$$

describing the process of detection of the photon pair by the detectors x_a and y_b ($x,y = 1,2$). In this expression, unitary operator $\hat{S}_{\psi}$ describes the action of the PASs and the unitary transformation $\hat{U}_{\psi\text{-PBS}}$ describes the coupling between the photon pair polarization state and the PBS ports. The explicit form of $\hat{U}_{\psi\text{-PBS}}$ is deduced by Eqs. (1), and calculations are reported in Appendix A. Since the operators $\hat{T}_a$ and $\hat{T}_b$ independently act on the corresponding subspaces a and b of the Hilbert space of polarization and induce linear transformation, they are ineffective on the Hilbert space of the PBS ports. Thus, $\hat{\rho}^{\mathrm{in}}$ is subject to a global transformation written as an unitary operator $\hat{S}_{\psi} = \mathbf{1}^{\mathrm{PBS}} \otimes \hat{S}_{a,b}$, where $\hat{S}_{a,b} = \hat{T}_a \otimes \hat{T}_b$.

$\hat{P}_{x_a y_b} = |Ox_a\rangle|Oy_b\rangle\langle Oy_b|\langle Ox_a|$ is the projector representing the detection process by the two detectors x_a and y_b. The probability of detection of the photon pair by the detectors x_a and y_b is

$$p(x_a, y_b) = \text{Tr}_\psi[\mathcal{E}_{x_a y_b}(\hat{\rho}^\psi)]$$

$$= \text{Tr}(\hat{P}_{x_a y_b} \hat{U}_{\psi\text{-PBS}} \hat{S}_\psi \hat{\rho}^{\text{in}} \hat{S}_\psi^\dagger \hat{U}_{\psi\text{-PBS}}^\dagger \hat{P}_{x_a y_b}^\dagger). \quad (2)$$

$\Sigma_{x_a y_b} \mathcal{E}_{x_a y_b}(\hat{\rho}^\psi)$ is trace preserving because the probabilities of distinct outcomes sum to one, i.e., $\text{Tr}_\psi[\Sigma_{x_a y_b} \mathcal{E}_{x_a y_b}(\hat{\rho}^\psi)]$ $= \Sigma_{x_a y_b} p(x_a, y_b) = 1$ for all possible input $\hat{\rho}^\psi$.

III. QUANTUM AND CLASSICAL NOISE IN PHOTON COUNTS

In the following, we consider the noise contribution to the photon counts because of an imperfect collection of photons and a noisy and lossy detection system. For the experimental setup in Fig. 1, we calculate the total probability $p_{\text{tot},x_z}(n)$ of n counts by any detector x_z by separately calculating the probabilities of counts associated with correlated photons $[p_{sp,x_z}(n)]$, with uncorrelated photons $[p_{u,x_z}(n)]$, and with detector dark counts $[p_{d,x_z}(n)]$.

To describe the counting process, we adopt the formalism of quantum operations, where we consider a general density matrix representing photons on a channel ν in term of number of photons, i.e., $\{|n^\nu\rangle\}$, as

$$\hat{\rho}^\nu = \sum_{n,m=0}^\infty \rho_{nm}^\nu |n^\nu\rangle\langle m^\nu|. \quad (3)$$

The evolution of the system $\hat{\rho}^\nu$ is evaluated according to the formalism of quantum operations.

In this way, we define the set of non-trace-preserving quantum operations as $\{\mathcal{E}_m^\mu\}$ as

$$\mathcal{E}_m^\mu(\hat{\rho}^\nu) = \text{Tr}_{\text{E}_\mu}(\hat{P}_m^\mu \hat{U}_{Q_\nu\text{-}E_\mu} \hat{\rho}^\nu \otimes |e_0^\mu\rangle\langle e_0^\mu| \hat{U}_{Q_\nu\text{-}E_\mu}^\dagger \hat{P}_m^{\mu\dagger}), \quad (4)$$

which describes the detection of m photons by the system μ. In this expression, the unitary operator $\hat{U}_{Q_\nu\text{-}E_\mu}$ represents the interaction between the quantum system Q_ν of photons in the channel ν in the initial state $\hat{\rho}^\nu$ and the lossy and noisy environment E_μ in the initial state $|e_0^\mu\rangle$. The action of $\hat{U}_{Q_\nu\text{-}E_\mu}$ on the state "number of photons" is

$$\hat{U}_{Q_\nu\text{-}E_\mu}|n^\nu\rangle|e_0^\mu\rangle = \sum_{m=0}^n d^\mu(m,n)|m^\nu\rangle|e_{m,n}^\mu\rangle, \quad (5)$$

where $|d^\mu(m,n)|^2$ is the probability of measuring m photons out of n present in the channel ν because of losses. $\hat{P}_m^\mu$ $= \Sigma_{n=m}^\infty |e_{m,n}^\mu\rangle\langle e_{m,n}^\mu|$ are the measurement operators.

Thus, the probability of measuring m counts by the detection system μ is

$$p_\mu(m) = \text{Tr}_{Q_\nu}[\mathcal{E}_m^\mu(\hat{\rho}^\nu)] = \sum_{n=m}^\infty \rho_{nn}^\nu |d^\mu(m,n)|^2, \quad (6)$$

where ρ_{nn}^ν is the probability of having n photons on the channel ν.

A. Single counts associated with correlated photons

In the following, we concentrate primarily on the measurement of correlated photons by a lossy detector x_z. We define the density matrix of the number of photon pairs, $\hat{\rho}^p$, as

$$\hat{\rho}^p = \sum_{n,m=0}^\infty \rho_{nm}^p |n^p\rangle\langle m^p|. \quad (7)$$

Analogous to Eq. (7), we write a density matrix of single photons of the pairs (sp) along channel z,

$$\hat{\rho}^{sp,z} = \sum_{n,m=0}^\infty \rho_{nm}^p |n^{sp,z}\rangle\langle m^{sp,z}|. \quad (8)$$

The counting of correlated photons on channel z by the detector x_z is described by mapping $\hat{\rho}^{sp,z}$ on the set of non-trace-preserving quantum operation $\{\mathcal{E}_m^{sp,x_z}\}$. The explicit form of $\mathcal{E}_m^{sp,x_z}(\hat{\rho}^{sp,z})$ is deduced by analogy to Eq. (4), by replacing the interaction unitary operator with $\hat{U}_{Q_{sp,z}\text{-}E_{sp,x_z}}$ and the measurement operator with $\hat{P}_m^{sp,x_z}$, given that $Q_{sp,z}$ is the quantum system of single photons of the pair on the channel z and E_{sp,x_z} is the lossy and noisy environment in the initial state $|e_0^{sp,x_z}\rangle$. The $\hat{U}_{Q_{sp,z}\text{-}E_{sp,x_z}}$ action on the state $|n^{sp,z}\rangle$ is completely described by means of coefficients $d^{sp,x_z}(m,n)$ in complete analogy with Eq. (5), while we have $\hat{P}_m^{sp,x_z} = \Sigma_{n=m}^\infty |e_{m,n}^{sp,x_z}\rangle\langle e_{m,n}^{sp,x_z}|$.

The probability of m counts by the detector x_z corresponding to correlated photons becomes

$$p_{sp,x_z}(m) = \sum_{n=m}^\infty \rho_{nn}^p |d^{sp,x_z}(m,n)|^2. \quad (9)$$

The probability of n pairs is given by $\rho_{nn}^p = (\lambda_p t)^n \exp(-\lambda_p t)/n!$, t being the time of measurement and λ_p the mean rate of photon pairs in the Alice and Bob channels [21,33–35]. The terms

$$|d^{sp,x_a}(m,n)|^2 = \binom{n}{m}\left[\xi_{x_a}\sum_{y_b} p(x_a, y_b)\right]^m$$

$$\times\left[1 - \xi_{x_a}\sum_{y_b} p(x_a, y_b)\right]^{n-m},$$

$$|d^{sp,y_b}(m,n)|^2 = \binom{n}{m}\left[\xi_{y_b}\sum_{x_a} p(x_a,y_b)\right]^m$$
$$\times \left[1-\xi_{y_b}\sum_{x_a} p(x_a,y_b)\right]^{n-m}$$

are the probabilities that only m out of n photons in the channel a (b) are counted by the detector x_a (y_b). Losses due to electronics (π_z), detection efficiencies (η_{x_z}), as well as optical losses (τ_{x_z}) are summed up in the term $\xi_{x_z} = \pi_z \eta_{x_z} \tau_{x_z}$ [22,36]; while we refer to Appendix B for the analysis of dead time in this context. The term τ_{x_z} incorporates all losses in the Alice and Bob optical path, such as from crystals, filters, lenses, PBSs, PASs, and fibers. The terms $\Sigma_{x_a(y_b)}p(x_a,y_b)$ are the probabilities that each photon of the pair may be counted randomly by any arbitrary detector [Eq. (2)]. Probability $p_{sp,x_z}(m)$ is derived according to Eq. (9), giving

$$p_{sp,x_z}(n) = (\lambda_{sp,x_z}t)^n \frac{\exp(-\lambda_{sp,x_z}t)}{n!}, \qquad (10)$$

with mean count rates given by

$$\lambda_{sp,x_a} = \xi_{x_a}\sum_{y_b} p(x_a,y_b)\lambda_p,$$

$$\lambda_{sp,y_b} = \xi_{y_b}\sum_{x_a} p(x_a,y_b)\lambda_p.$$

B. Single counts associated with uncorrelated photons and dark counts

Here, we consider counts from any detector x_z from stray light, uncorrelated photons, and dark counts eventually contributing to noise in the distributed key. The density matrix associated with stray light and uncorrelated photons is

$$\hat{\rho}^{u,x_z} = \sum_{n,m=0}^{\infty} \rho_{nm}^{u,x_z}|n^{u,x_z}\rangle\langle m^{u,x_z}|.$$

By pursuing the same formalism as before, the detection of uncorrelated photons by the detector x_z is described by means of the set of non-trace-preserving quantum operation $\{\mathcal{E}_m^{u,x_z}\}$. The map $\mathcal{E}_m^{u,x_z}(\hat{\rho}^{u,x_z})$ follows in analogy with Eq. (4). The unitary operator $\hat{U}_{Q_{u,x_z}-E_{u,x_z}}$ describes the interaction between the quantum system Q_{u,x_z} of uncorrelated photons on the channel x_z and the lossy environment E_{u,x_z} in the initial state $|e_0^{u,x_z}\rangle$. The measurement operator is $\hat{P}_m^{u,x_z} = \Sigma_{n=m}^{\infty}|e_{m,n}^{u,x_z}\rangle\langle e_{m,n}^{u,x_z}|$. The action of $\hat{U}_{Q_{u,x_z}-E_{u,x_z}}$ on the state $|n^{u,x_z}\rangle$ follows from Eq. (5) with the decomposition coefficients, $d^{u,x_z}(m,n)$.

Thus, the probability of measuring m counts of uncorrelated photons by the detector x_z is

$$p_{u,x_z}(m) = \sum_{n=m}^{\infty} \rho_{nn}^{u,x_z}|d^{u,x_z}(m,n)|^2, \qquad (11)$$

where ρ_{nn}^{u,x_z} is the probability of n uncorrelated photons in the channel x_z. According to Refs. [21,33–35], we assume that we have $\rho_{nn}^{u,x_z}=(\lambda_{u,x_z}t)^n\exp(-\lambda_{u,x_z}t)/n!$, where λ_{u,x_z} is the mean rate of uncorrelated photons. The term

$$|d^{u,x_z}(m,n)|^2 = \binom{n}{m}(\xi_{x_z})^m(1-\xi_{x_z})^{n-m}$$

is the probability of m out of n uncorrelated photons counted by the detector x_z.

The $p_{u,x_z}(n)$ derived accordingly from Eq. (11) is

$$p_{u,x_z}(n) = (\xi_{x_z}\lambda_{u,x_z}t)^n \frac{\exp(-\xi_{x_z}\lambda_{u,x_z}t)}{n!}. \qquad (12)$$

The main source of noise in detectors is due to dark counts, whose distribution is regarded merely from a statistical point of view as the probability of n dark counts

$$p_{d,x_z}(n) = (\lambda_{d,x_z}t)^n \frac{\exp(-\lambda_{d,x_z}t)}{n!},$$

with the mean dark-count rate being λ_{d,x_z}.

C. Total counts

As real counters cannot distinguish among counts due to correlated photons, counts due to uncorrelated photons, and dark counts, the total probability of measuring k counts by detector x_z is calculated according to Refs. [21,33,35],

$$p_{\text{tot},x_z}(k) = \sum_{l,m,n=0}^{\infty} \delta_{k,l+m+n} P_{sp,x_z}(l)\, p_{u,x_z}(m)\, p_{d,x_z}(n),$$

giving

$$p_{\text{tot},x_z}(n) = (\lambda_{\text{tot},x_z}t)^n \frac{\exp(-\lambda_{\text{tot},x_z}t)}{n!},$$

where the mean rate of total counts measured by the detector x_z is $\lambda_{\text{tot},x_z} = \lambda_{sp,x_z} + \xi_{x_z}\lambda_{u,x_z} + \lambda_{d,x_z}$.

IV. COINCIDENCE COUNTS

We build up a model for the probability $p_{c,x_ay_b}(n)$ of measuring n coincidences by a pair of detectors x_a and y_b in order to estimate crucial quantities of a typical QCKD experiment, such as the sifted key and the QBER before and after the error-correction procedure, whenever different protocols are applied. We distinguish between the probability distribution of true coincidences [$p_{p,x_ay_b}(n)$ due to correlated photons] and the probability distribution of accidental coincidences [$p_{Acc,x_ay_b}(n)$ because of imperfections in the detection electronics].

We consider the density matrix in terms of counted pair states [Eq. (7)], and we describe its evolution exploiting the formalism of quantum operations as described in Sec. IV by defining another set of non-trace-preserving quantum operations $\{\mathcal{E}_m^{p,x_a y_b}\}$.

$\mathcal{E}_m^{p,x_a y_b}(\hat{\rho}^p)$ describes the measurement of m coincidences originated by the detection of the two photons of a pair by the detectors x_a, y_b. Its explicit expression is found from Eq. (4), except for the interaction between the quantum system Q_p of photon pairs in the initial state $\hat{\rho}^p$ and the lossy and noisy environment $E_{p,x_a y_b}$ in the initial state $|e_0^{p,x_a y_b}\rangle$ represented by the unitary operator $\hat{U}_{Q_p\text{-}E_{p,x_a y_b}}$ and the measurement operator $\hat{P}_m^{p,x_a y_b} = \sum_{n=m}^{\infty} |e_{m,n}^{p,x_a y_b}\rangle\langle e_{m,n}^{p,x_a y_b}|$.

The action of $\hat{U}_{Q_p\text{-}E_{p,x_a y_b}}$ on the state number of photon pairs is

$$\hat{U}_{Q_p\text{-}E_{p,x_a y_b}}|n^p\rangle|e_0^{p,x_a y_b}\rangle = \sum_{m=0}^{n} d^{p,x_a y_b}(m,n)|m^p\rangle|e_{m,n}^{p,x_a y_b}\rangle.$$

Thus, the probability of measuring m true coincidences corresponding to photon pairs by the pair of detectors x_a, y_b is

$$p_{p,x_a y_b}(m) = \sum_{n=m}^{\infty} \rho_{nn}^p |d^{p,x_a y_b}(m,n)|^2. \quad (13)$$

Realizing that a true coincidence may occur only if both photons of the pair are not lost, we emphasize that the terms $|d^{p,x_a y_b}(m,n)|^2$ are the probabilities that only m pairs are detected as coincidences by the pair of detectors x_a, y_b when n photons are present in the channels of Alice and Bob. It is straightforward to deduce the explicit form of $|d^{p,x_a y_b}(m,n)|^2$ as

$$|d^{p,x_a y_b}(m,n)|^2 = \binom{n}{m}[\xi_{x_a}\xi_{y_b}p(x_a,y_b)]^m$$
$$\times [1 - \xi_{x_a}\xi_{y_b}p(x_a,y_b)]^{n-m}.$$

Probability $p_{p,x_a y_b}(n)$ is derived according to Eq. (13), obtaining

$$p_{p,x_a y_b}(n) = (\lambda_{p,x_a y_b}t)^n \frac{\exp(-\lambda_{p,x_a y_b}t)}{n!},$$

where $\lambda_{p,x_a y_b} = \xi_{x_a}\xi_{y_b}p(x_a,y_b)\lambda_p$ is the mean rate of true coincidences seen by the pair of detectors x_a and y_b.

A. Accidental coincidences

The presence of the temporal coincidence window w, during which coincidences are measured, modifies the mean total coincidence counts, thus forcing one to distinguish between true and accidental coincidence statistics. We assume that true coincidences occur in the middle of the coincidence temporal window. Then we deduce the probability distribu-

tion of accidental coincidences and finally the probability distribution of total coincidences, accounting for true and accidental coincidences, assuming $w < D_z$, where D_z is the dead time in the z channel according to Appendix B.

We regard $p_{N,x_z}(n)$ as the probability distribution of photons counted by the detector x_z that may contribute to accidental coincidences in the time interval Δt. By observing that the probability distributions $p_{\text{tot},x_z}(n)$ and $p_{p,x_a y_b}(n)$ are Poisson, it is simple to demonstrate that we have

$$p_{N,x_z}(n) = (\lambda_{N,x_z}\Delta t)^n \frac{\exp(-\lambda_{N,x_z}\Delta t)}{n!},$$

where $\lambda_{N,x_a} = \lambda_{\text{tot},x_a} - \lambda_{p,x_a y_b}$ and $\lambda_{N,y_b} = \lambda_{\text{tot},y_b} - \lambda_{p,x_a y_b}$ are the mean count rates possibly contributing to accidental coincidences from the detectors x_a and y_b, respectively.

Let us denote by q_{y_b} the probability that at least one photon in y_b is counted in the coincidence window $\Delta t = w$,

$$q_{y_b} = \sum_{n=1}^{\infty} p_{N,x_z}^{\Delta t = w}(n) = 1 - \exp(-\lambda_{N,x_z}w), \quad (14)$$

because detectors x_a are here considered as triggers.

The term in Eq. (14) is intended to account for the contribution of single detectors y_b. Since detectors y_b are statistically independent, the probability that both detectors count a photon producing an accidental coincidence is $q_{1_b}q_{2_b}$. The final probability of accidental counts from detector y_b is obtained by subtracting half the probability that both detectors in Bob's channel count an accidental photon, in formula

$$q_{1_b}^* = q_{1_b}\left(1 - \frac{1}{2}q_{2_b}\right), \quad (15)$$

$$q_{2_b}^* = q_{2_b}\left(1 - \frac{1}{2}q_{1_b}\right). \quad (16)$$

According to Refs. [21,33–35], we calculate the probability distribution of accidental coincidences in the time measurement t by applying the discrete convolution between the Poisson distribution of "triggering" counts and the binomial distribution with parameter $q_{y_b}^*$,

$$p_{Acc,x_a y_b}(m) = \sum_{n=m}^{\infty} p_{N,x_a}(n)B_{y_b}(m,n),$$

with $B_{y_b}(m,n) = \binom{n}{m}(q_{y_b}^*)^m(1-q_{y_b}^*)^{n-m}$, giving

$$p_{Acc,x_a y_b}(n) = (\lambda_{Acc,x_a y_b}t)^n \frac{\exp(-\lambda_{Acc,x_a y_b}t)}{n!}$$

with $\lambda_{Acc,x_a y_b} = q_{y_b}^*\lambda_{N,x_a}$.

Lastly, the probability distribution of total coincidence counts $p_{c,x_a y_b}(n)$ is obtained by

$$p_{c,x_a y_b}(k) = \sum_{m,n=0}^{\infty} \delta_{k,m+n} p_{p,x_a y_b}(m) p_{Acc,x_a y_b}(n)$$

$$= (\lambda_{c,x_a y_b} t)^k \frac{\exp(-\lambda_{c,x_a y_b} t)}{k!},$$

where the mean rate of total coincidence measured by an arbitrary pair of x_a and y_b detectors is

$$\lambda_{c,x_a y_b} = \lambda_{p,x_a y_b} + \lambda_{Acc,x_a y_b}. \tag{17}$$

To characterize a particular QCKD procedure, we embody the effect of transformations $\hat{T}_a$ and $\hat{T}_b$ on photon polarization by the rotation matrices

$$\hat{T}_z = \begin{pmatrix} \cos\theta_z & \sin\theta_z \\ \sin\theta_z & -\cos\theta_z \end{pmatrix}. \tag{18}$$

We rewrite Eq. (17) in terms of the rotation angles θ_a and θ_b, induced by transformations $\hat{T}_a$ and $\hat{T}_b$ on the polarization state of photons, by replacing $p(x_a, y_b)$ with $p_{\theta_a,\theta_b}(x_a, y_b)$, whose complete expression is in Appendix A. More specifically, the calculated mean coincident counts are made explicit in terms of angular settings θ_a and θ_b as $\lambda_{c,x_a y_b}(\theta_a, \theta_b)t$.

V. EVALUATION OF THE QBER

To characterize a particular QCKD procedure and to assess its advantages, we evaluate particular quantities such as the QBER and the sifted key for different types of QCKD protocols so far experimentally implemented, i.e., the BB84 protocol and Ekert's protocols based on the CHSH and Wigner inequalities, respectively.

The QBER is a parameter for describing the signal quality in the transmission of the sifted key, defined as the relative frequency of errors induced by accidental coincidences, i.e., the number of errors divided by the total size of the cryptographic sifted key (K) [35].

In other words, the QBER is given by total coincidence provided by those detectors "wrongly" firing in coincidence according to the chosen protocol. In fact, the protocol establishes which pair of detectors should fire to contribute to the key.

A. BB84 protocol

Here, we examine the BB84 protocol variant proposed for entangled states in Ref. [3]. Recall that Alice and Bob measure photons randomly and independently between two bases of orthogonal quantum states. One basis corresponds to horizontal and vertical linear polarization ($\oplus$), while the other to linear polarizations rotated by 45° ($\otimes$). Only half of the photon pairs can contribute to the sifted key, as only the subset of measurements performed with the two analyzers in the same basis contributes.
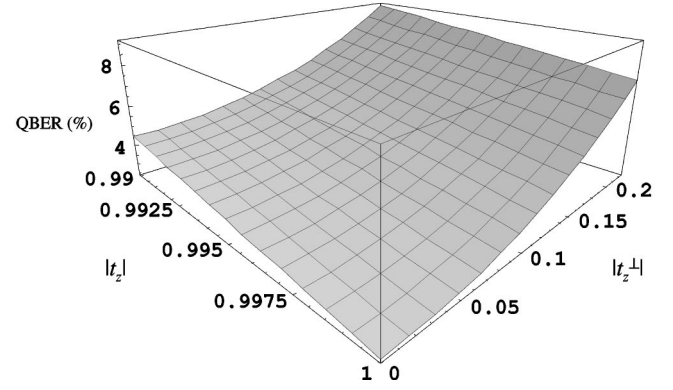
The sifted key is given by

FIG. 3. The QBER for the BB84 protocol versus the PBS coefficients $|t_z|$ and $|t_z^\perp|$.

$$K_{BB84}(\theta_a) = f_{basis} f_{setting} \sum_{x_a y_b} [\lambda_{c,x_a y_b}(\theta_a, \theta_a)$$

$$+ \lambda_{c,x_a y_b}(\theta_a + \pi/4, \theta_a + \pi/4)]t, \tag{19}$$

where $f_{basis} = 1/2$ is the probability to measure in the right basis [(θ_a, θ_a) and $(\theta_a + \pi/4, \theta_a + \pi/4)$], while $f_{setting} = 1/2$ is the probability to measure in a particular analyzer setting [(θ_a, θ_a) or $(\theta_a + \pi/4, \theta_a + \pi/4)$].

All detectors contribute to the sifted key K, but only coincidences between $1_a 2_b$ and $2_a 1_b$ correspond to the expected anticorrelation when measurements are performed in the same basis ($\theta_a = \theta_b$), while QBER contributions come from the coincidences between detectors $1_a 1_b$ and $2_a 2_b$ [as it is clear from Eqs. (A1) in Appendix A]. Therefore, the BB84 QBER $\mathcal{R}_{BB84}$ explicit formula is

$$\mathcal{R}_{BB84}(\theta_a)$$

$$= \frac{\sum_{x=1,2} [\lambda_{c,x_a x_b}(\theta_a, \theta_a) + \lambda_{c,x_a x_b}(\theta_a + \pi/4, \theta_a + \pi/4)]t}{4K_{BB84}(\theta_a)}.$$

$$\tag{20}$$

To test the behavior of QBER, we simulate a realistic experiment with parameters $\eta_{x_a} = \eta_{y_b} = 0.5$ (quantum efficiency of the four detectors), $\tau_{x_a} = \tau_{y_b} = 0.1$ (transmittance of the four channels), $\lambda_{d,x_a} = \lambda_{d,y_b} = 50$ s^{-1} (dark-count rate of the four detectors), $D_a = D_b = 100$ ns (total dead time of the detection systems of Alice and Bob), $\theta_a = 0$ and $w = 4$ ns. The entanglement parameters are $\epsilon = 0.95$ and $\zeta = 1$, the correlation level in the Alice channel is $\alpha_a = 0.25$ [$\alpha_a = \lambda_p/(\lambda_p + \Sigma_{x_a} \lambda_{u,x_a})$], and the correlated photon rate is $\lambda_p = 700$ KHz.

In Fig. 3, we show the dependence of QBER versus the optical properties of real PBS, i.e., the transmittance $|t_z|$ and $|t_z^\perp|$ ($z = a, b$) for the states $|H_z\rangle$ and $|V_z\rangle$, respectively. Results show how strongly the QBER can be affected by the optical properties of PBSs, whose influence has been neglected so far.
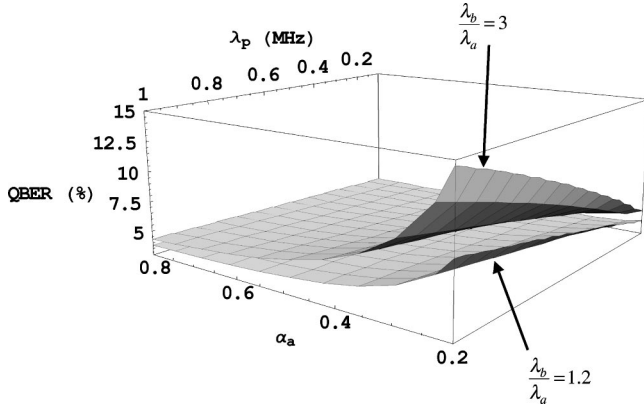
In Fig. 4, the behavior of the QBER is presented versus

FIG. 4. The QBER for the BB84 protocol versus the correlation level in the Alice channel $\alpha_a = \lambda_p/(\lambda_p + \Sigma_{x_a} \lambda_{u,x_a})$ and the correlated photon rate λ_p for two noise levels in the channels ($\lambda_b/\lambda_a = 1.2$ and 3, where $\lambda_a = \lambda_p + \Sigma_{x_a} \lambda_{u,x_a}$ and $\lambda_b = \lambda_p + \Sigma_{y_b} \lambda_{u,y_b}$).

the level of correlation, α_a, in the Alice channel and the rate λ_p of the correlated photon pairs for two different noise levels, i.e., the ratio between the mean rate of photons in the two channels. Far from ideal conditions, the presence of uncorrelated events in the two channels induces a nonlinear increase of the QBER. The other parameters are set as in Fig. 3 for realistic PBSs parameters, $|t_z|^2 = 0.99$ and $|t_z^\perp|^2 = 0.025$.

B. Ekert's protocol

Ekert's protocol has the peculiarity of relying on the completeness of quantum mechanics for security. Therefore, the possible combined choices between Alice and Bob for analyzer settings split into three groups: the first for key distribution, the second containing the security proof, and the third garnering the discarded measurements.

Here, we consider two possible variants of Ekert's protocol: the variant based on the Clauser-Horne-Shimony-Holt inequality (CHSH), similar to the one proposed in Ref. [8], and the variant based on Wigner's inequality [7].

1. Ekert's protocol based on CHSH inequalities

To increase the number of measurements devoted to the key distribution, we consider the case where Alice and Bob measure randomly among four analyzer settings and use the CHSH inequality to test eavesdropping. In this scheme, Alice's choices for the analyzer settings are $\theta_a = (\theta_a, \theta_a + \pi/8, \theta_a + \pi/4, \theta_a + 3\pi/8)$ and Bob's are $\theta_b = (\theta_a + \pi/8, \theta_a + \pi/4, \theta_a + 3\pi/8, \theta_a + \pi/2)$.

The key distribution is performed when settings for Alice and Bob are the same or orthogonal, so that the sifted key is

$$K_{\text{CHSH}}(\theta_a) = f_{setting} \sum_{x_a y_b} [\lambda_{c,x_a y_b}(\theta_a, \theta_a + \pi/2) + \lambda_{c,x_a y_b}(\theta_a + \pi/8, \theta_a + \pi/8) + \lambda_{c,x_a y_b}(\theta_a + \pi/4, \theta_a + \pi/4) + \lambda_{c,x_a y_b}(\theta_a + 3\pi/8, \theta_a + 3\pi/8)]t,$$

where $[(\theta_a, \theta_a + \pi/2), (\theta_a + \pi/8, \theta_a + \pi/8), (\theta_a + \pi/4, \theta_a + \pi/4), (\theta_a + 3\pi/8, \theta_a + 3\pi/8)]$ are angular settings generating the key and $f_{setting} = 1/16$.

In a maximally entangled state configuration, the detectors contributing to the key should be $1_a 1_b$ and $2_a 2_b$ for the orthogonal analyzer settings and $1_a 2_b$ and $2_a 1_b$ for the parallel settings. Thus, the QBER is calculated according to

$$\mathcal{R}_{\text{CHSH}}(\theta_a) = \frac{1}{4K_{\text{CHSH}}(\theta_a)} \left\{ \sum_{x_a, y_b(x \neq y)} \lambda_{c,x_a y_b}(\theta_a, \theta_a + \pi/2)t \right.$$
$$+ \sum_{x_a, y_b(x=y)} [\lambda_{c,x_a y_b}(\theta_a + \pi/8, \theta_a + \pi/8)$$
$$+ \lambda_{c,x_a y_b}(\theta_a + \pi/4, \theta_a + \pi/4)$$
$$\left. + \lambda_{c,x_a y_b}(\theta_a + 3\pi/8, \theta_a + 3\pi/8)]t \right\},$$

where the intuitive notation $\Sigma_{x_a, y_b(x \neq y)}$ indicates the sum over $1_a 2_b$ and $2_a 1_b$ detectors and $\Sigma_{x_a, y_b(x=y)}$ indicates the sum over $1_a 1_b$ and $2_a 2_b$.

2. Ekert's protocol based on Wigner's inequality

As in Ref. [7], we consider the case of the Ekert's variant where the security of the quantum channels follows from Wigner's inequality. In this case, Alice and Bob measure randomly among four analyzers settings, whose choices are $\theta_a = (\theta_a - \pi/6, \theta_a)$ for Alice and $\theta_b = (\theta_a, \theta_a + \pi/6)$ for Bob. The key distribution is performed when settings for Alice and Bob are the same so that the sifted key is

$$K_{\text{WI}}(\theta_a) = f_{setting} \sum_{x_a y_b} \lambda_{c,x_a y_b}(\theta_a, \theta_a)t,$$

with $f_{setting} = 1/4$.

The QBER is calculated according to

$$\mathcal{R}_{\text{WI}}(\theta_a) = f_{setting} \frac{[\lambda_{c,1_a 1_b}(\theta_a, \theta_a) + \lambda_{c,2_a 2_b}(\theta_a, \theta_a)]t}{K_{\text{WI}}(\theta_a)},$$

by taking the detectors contributing to the wrong bits as $1_a 1_b$ and $2_a 2_b$.

In Fig. 5, we present a comparison of QBER levels for the BB84 protocol and the Ekert protocols considering both the inequalities of CHSH and Wigner versus the analyzers angular setting θ_a and the entanglement parameter ϵ. Experimental conditions are the same (low noise) as for Figs. 3 and 4. Results highlight that the QBER is sensitive to the angle θ_a when the ideal entanglement is not achieved for both the variants of Ekert's protocols. In the Wigner's case, the sensitivity is so remarkable that this protocol has to be considered less robust than the BB84- and the CHSH-inequality-based Ekert's protocols.

VI. SECURITY AND ERROR CORRECTION

The security of the BB84 variant protocol is based on a public comparison between measurements of Alice and Bob
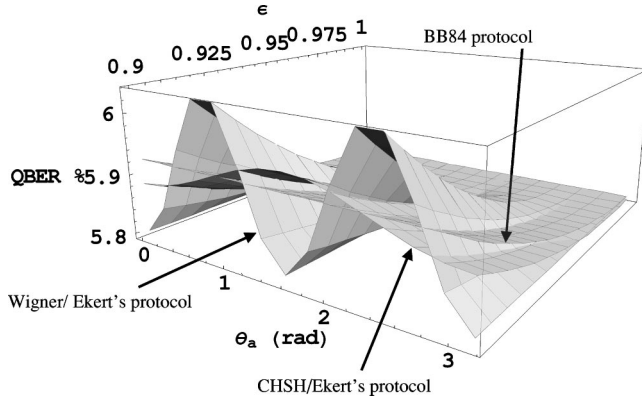
FIG. 5. The QBER in case of the CHSH- and Wigner-inequality-based Ekert's protocols, together with the BB84 protocol versus the angular analyzers settings θ_a, and the entanglement parameter ϵ. The parameters settings are $\lambda_a = 2.8 \times 10^6$ s^{-1}, $\alpha_a = 0.25$, $\lambda_b/\lambda_a = 1.2$, $\eta_{x_a} = \eta_{y_b} = 0.5$, $\tau_{x_a} = \tau_{y_b} = 0.1$, $\lambda_{d,x_a} = \lambda_{d,y_b} = 50$ s^{-1}, $D_a = D_b = 100$ ns, $w = 4$ ns, and $\zeta = 1$, taken from typical and experimental realistic values so far implemented. PBSs are considered real with $|t_z|^2 = 0.99$ and $|t_z^\perp|^2 = 0.025$ ($z = a, b$).

on a sufficiently large random subset of the sifted key, e.g., more than half is recommended in Ref. [3].

The security proof for the CHSH-inequality-based Ekert's protocol is evaluated with the specific choices of settings by the CHSH inequality,

$$S(\theta_a) = E(\theta_a, \theta_a + \pi/8) - E(\theta_a, \theta_a + 3\pi/8) + E(\theta_a + \pi/4, \theta_a + \pi/8) + E(\theta_a + \pi/4, \theta_a + 3\pi/8),$$

$$S'(\theta_a) = E(\theta_a + \pi/8, \theta_a + \pi/4) - E(\theta_a + \pi/8, \theta_a + \pi/2) + E(\theta_a + 3\pi/8, \theta_a + \pi/4) + E(\theta_a + 3\pi/8, \theta_a + \pi/2),$$

where we have

$$E(\theta_a, \theta_b) = M_{1_a 1_b}(\theta_a, \theta_b) - M_{1_a 2_b}(\theta_a, \theta_b) + M_{2_a 2_b}(\theta_a, \theta_b) - M_{2_a 1_b}(\theta_a, \theta_b).$$

Here,

$$M_{x_a y_b}(\theta_a, \theta_b) = \frac{\lambda_{c,x_a y_b}(\theta_a, \theta_b)}{\sum_{x_a y_b} \lambda_{c,x_a y_b}(\theta_a, \theta_b)}$$

is the normalized coincidence rate as a function of the analyzer settings and detector choices. The terms $M_{x_a y_b}(\theta_a, \theta_b)$ are commonly stored when experiments are performed.

For maximally entangled states, we have $|S_{ql}| = |S'_{ql}| = 2\sqrt{2}$, while for any realistic local theory, we have $|S, S'| \leq 2$. It is expected that the presence of an eavesdropper will reduce the observed value of $|S, S'|$, giving $|S_{Eve}, S'_{Eve}| \leq \sqrt{2}$, when the eavesdropper measures photons over either one or both (total eavesdropping) the channels of Alice and Bob [2].

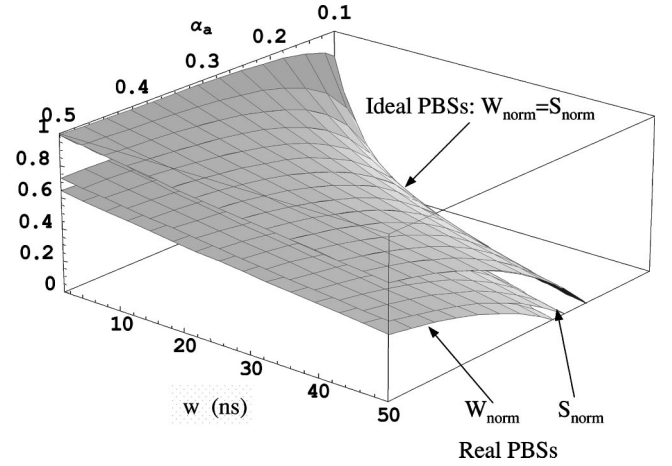FIG. 6. The CHSH and Wigner inequalities parameters S_{norm} and W_{norm} versus the coincidence window w and the correlation level in the Alice channel α_a. In the case of maximally entangled states we have $W_{norm} = S_{norm} = 1$, while the lower cut is defined by the eavesdropping limit $W_{norm} \leq 0$ and $S_{norm} \leq 0$. The choice of parameter values are the same of Fig. 4 except for $\theta_a = 0$ and $\epsilon = 0.95$. The lower two surfaces represented correspond to W_{norm} and S_{norm} in the case of real PBSs, with parameters $|t_z|^2 = 0.98$ and $|t_z^\perp|^2 = 0.05$. The higher surface represents $S_{norm} = W_{norm}$ in the case of ideal PBSs.

In the case of Wigner's-inequality-based Ekert's protocol, the Wigner inequality result has

$$W(\theta_a) = M_{1_a 1_b}(\theta_a - \pi/6, \theta_a) + M_{1_a 1_b}(\theta_a, \theta_a + \pi/6) - M_{1_a 1_b}(\theta_a - \pi/6, \theta_a + \pi/6),$$

giving for the maximally entangled states, $W_{ql} = -1/8$ and $W \geq 0$ for any local realistic theory. As for the CHSH inequality, it can be proved that the limit becomes $W_{Eve} \geq 1/16$ for Eve detecting only one photon of the pair, while in the case of total eavesdropping, there is no boundary condition [37].

In Fig. 6, we compare the behaviors of the CHSH- and Wigner-inequality parameters, $S_{norm} = (|S| - |S_{Eve}|)/(|S_{ql}| - |S_{Eve}|)$ and $W_{norm} = (W - W_{Eve})/(W_{ql} - W_{Eve})$, versus the coincidence window w and the correlation level in Alice's channel α_a. The lower surfaces represent the case of real PBSs, where $W_{norm} < S_{norm}$, while the upper surface corresponds to ideal PBSs, where $W_{norm} = S_{norm}$. We observe that, given the same noise level in the system and real PBSs, Wigner's parameter reaches the eavesdropping limit faster than the CHSH one does, revealing the intrinsic weakness of Wigner's test against experimental parameters.

Furthermore, Wigner's security test guarantees against eavesdropping strategies only for the detection of one photon of the pair, while the CHSH security is independent on the adopted strategy (see Refs. [2,37]).

A satisfactory protocol must be able to recover from noise as well as from partial leakage, allowing Alice and Bob to reconcile the two strings of bits measured and distill from the sifted key to a corrected key. A strong need for the application of any error-correction method is an *a priori* knowledge
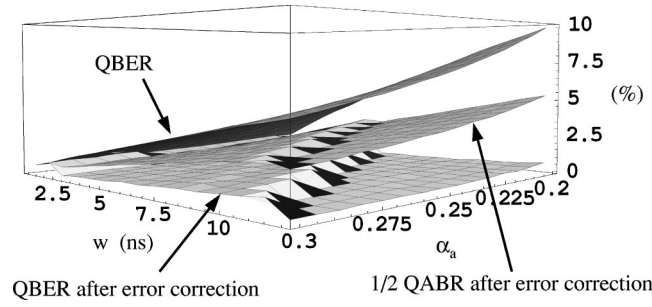
FIG. 7. The QBER in the case of the BB84 protocol versus the coincidence window w and the correlation parameter in the Alice channel α_a: the sawtooth shape is due to the application of the error correction procedure. The parameters are set as in Fig. 6 except that, in this case, ideal PBSs are considered.

of the QBER, which provides information regarding how many times the error-correction procedure must be applied to reduce the QBER to a certain agreed level, commonly 1%. Here, we show an example of error correction on an *a priori* evaluated QBER according to a common approach reported in Ref. [7], to show that our model allows for prediction of the corrected key length.

In general, Alice and Bob cannot distinguish between errors caused either by an eavesdropper or by the environment. Thus, they must assume that all errors are due to an eavesdropper and evaluate the leaked information from the QBER. Also, even though by the error-correction procedure one can disregard incorrect bits by simply dropping them off in building the distilled key, the residual knowledge of an eavesdropper may still not be faithfully quantified by the reduced QBER obtained after the correction. The effects of Eve's strategy is, in fact, equivalent to quantum noise yielding eventually accidental coincidences, these last contributing to both incorrect and correct bits transmitted, as it is clear from Eqs. (19) and (20). Hence the error-correction procedure is not sufficient to cancel a potential Eve's knowledge of part of the key due to accidental coincidence.

To prove this last assertion, we introduce the quantum accidental bit rate (QABR), a quantity related to accidental coincidences and, in this sense, analogous to the QBER. However, the error-correction procedure cannot reduce the QABR at the QBER level. As an example, we give the QABR in the case of Ekert's protocol based on Wigner's inequality,

$$\mathcal{B}_{\mathrm{WI}}(\theta_a) = f_{setting} \frac{\sum_{x_a y_b} \lambda_{Acc, x_a y_b}(\theta_a, \theta_a) t}{K_{\mathrm{WI}}(\theta_a)}.$$

Figure 7 shows the QBER with and without the application of the error-correction procedure together with the $1/2\ \mathcal{B}$ vs the coincidence window and the correlation parameter in Alice's channel. The error-correction procedure is very ineffective at reducing the QABR and consequently the possible effect of Eve's knowledge on the corrected key.

VII. CONCLUSIONS

This paper is concerned with an *a priori* evaluation of QCKD crucial parameters when entangled photons produced by SPDC are exploited. The basic experimental feature consists of the detection of coincident photons. Toward this aim, we developed a statistical model to calculate the probability of accidental coincidences contributing to errors in the sifted key, not completely accounted for by simple experimental means.

We investigated the noise contribution due to imperfect source generation and selection, imperfect polarizing beam splitters performing polarization state analysis, and noisy and lossy measurement system for photon-number detection. We emphasized some basic system imperfections such as uncorrelated photons collection, detection system deficiencies, detection system noise due to detector dark counts, and electronic system imperfections associated with non-ideal-time-correlation measurements.

We discussed how this model can be adopted for the evaluation of the QBER and the sifted key for different well-known protocols, i.e., the BB84 and the Ekert protocols based on both CHSH and Wigner inequalities, and compared them to expected results.

Given that this model predicts precisely the QBER and the sifted key, it ultimately guarantees a method to compare different security criteria of the hitherto proposed QCKD protocols and provides an objective assessment of performances and advantages of different systems. Thus, it yields a method for an *a priori* evaluation of the tolerable experimental imperfections in a practically implemented quantum system to establish the degree of security and competitiveness of QCKD systems.

Finally, we used the model in a standard error-correction procedure, observing that this does not completely cancel the possible residual eavesdropping knowledge on the corrected key. We emphasize that this model yields also the degree of security of the corrected key, if a precise modeling of system imperfections is provided.

APPENDIX A: INTERACTION MATRIX $\hat{U}_{\psi-\mathrm{PBS}}$

We explicitly calculate the unitary transformation $\hat{U}_{\psi\text{-PBS}}$ according to Eqs. (1) obtaining a 16×16 matrix

$$\hat{U}_{\psi\text{-PBS}} = \begin{pmatrix} U_1 & U_2 & U_3 & U_4 \\ U_2 & U_1 & U_4 & U_3 \\ U_3 & U_4 & U_1 & U_2 \\ U_4 & U_3 & U_2 & U_1 \end{pmatrix},$$

where we indicate

$$U_1 = \begin{bmatrix} \mathcal{T}_a\mathcal{T}_b & 0 & 0 & 0 \\ 0 & \mathcal{T}_a\mathcal{T}_b^\perp & 0 & 0 \\ 0 & 0 & \mathcal{T}_a^\perp\mathcal{T}_b & 0 \\ 0 & 0 & 0 & \mathcal{T}_a^\perp\mathcal{T}_b^\perp \end{bmatrix};$$

$$U_2 = \begin{bmatrix} \mathcal{T}_a\mathcal{R}_b & 0 & 0 & 0 \\ 0 & \mathcal{T}_a\mathcal{R}_b^\perp & 0 & 0 \\ 0 & 0 & \mathcal{T}_a^\perp\mathcal{R}_b & 0 \\ 0 & 0 & 0 & \mathcal{T}_a^\perp\mathcal{R}_b^\perp \end{bmatrix};$$

$$U_3 = \begin{bmatrix} \mathcal{R}_a\mathcal{T}_b & 0 & 0 & 0 \\ 0 & \mathcal{R}_a\mathcal{T}_b^\perp & 0 & 0 \\ 0 & 0 & \mathcal{R}_a^\perp\mathcal{T}_b & 0 \\ 0 & 0 & 0 & \mathcal{R}_a^\perp\mathcal{T}_b^\perp \end{bmatrix};$$

$$U_4 = \begin{bmatrix} \mathcal{R}_a\mathcal{R}_b & 0 & 0 & 0 \\ 0 & \mathcal{R}_a\mathcal{R}_b^\perp & 0 & 0 \\ 0 & 0 & \mathcal{R}_a^\perp\mathcal{R}_b & 0 \\ 0 & 0 & 0 & \mathcal{R}_a^\perp\mathcal{R}_b^\perp \end{bmatrix};$$

and $\mathcal{T}_z = t_z/(t_z^2 - r_z^2)$, and $\mathcal{R}_z = r_z/(t_z^2 - r_z^2)$ $(z = a,b)$, analogously for $\mathcal{T}_z^\perp$ and $\mathcal{R}_z^\perp$.

According to Eqs. (2) and (18), we obtain for $p_{\theta_a,\theta_b}(x_a,y_b)$ the following:

$$p_{\theta_a,\theta_b}(1_a,1_b) = \frac{1}{1+|\epsilon|^2}\{\cos^2(\theta_b)[\cos^2(\theta_a)(|\mathcal{T}_a\mathcal{T}_b^\perp|^2$$

$$+|\mathcal{T}_a^\perp\mathcal{T}_b\epsilon|^2) + \sin^2(\theta_a)(|\mathcal{T}_a^\perp\mathcal{T}_b^\perp|^2$$

$$+|\mathcal{T}_a\mathcal{T}_b\epsilon|^2)] + \sin^2(\theta_b)[\cos^2(\theta_a)(|\mathcal{T}_a\mathcal{T}_b|^2$$

$$+|\mathcal{T}_a^\perp\mathcal{T}_b^\perp\epsilon|^2) + \sin^2(\theta_a)(|\mathcal{T}_a^\perp\mathcal{T}_b|^2$$

$$+|\mathcal{T}_a\mathcal{T}_b^\perp\epsilon|^2)] + \sin(2\theta_a)\cos(2\theta_b)\mathrm{Re}(\epsilon\zeta/2)$$

$$\times(-|\mathcal{T}_a\mathcal{T}_b|^2 + |\mathcal{T}_a^\perp\mathcal{T}_b|^2 + |\mathcal{T}_a\mathcal{T}_b^\perp|^2$$

$$-|\mathcal{T}_a^\perp\mathcal{T}_b^\perp|^2)\},$$

$$p_{\theta_a,\theta_b}(1_a,2_b) = \frac{1}{1+|\epsilon|^2}\{\cos^2(\theta_b)[\cos^2(\theta_a)(|\mathcal{T}_a\mathcal{R}_b^\perp|^2$$

$$+|\mathcal{T}_a^\perp\mathcal{R}_b\epsilon|^2) + \sin^2(\theta_a)(|\mathcal{T}_a^\perp\mathcal{R}_b^\perp|^2$$

$$+|\mathcal{T}_a\mathcal{R}_b\epsilon|^2)] + \sin^2(\theta_b)[\cos^2(\theta_a)(|\mathcal{T}_a\mathcal{R}_b|^2$$

$$+|\mathcal{T}_a^\perp\mathcal{R}_b^\perp\epsilon|^2) + \sin^2(\theta_a)(|\mathcal{T}_a^\perp\mathcal{R}_b|^2$$

$$+|\mathcal{T}_a\mathcal{R}_b^\perp\epsilon|^2)] + \sin(2\theta_a)\cos(2\theta_b)\mathrm{Re}(\epsilon\zeta/2)$$

$$\times(-|\mathcal{T}_a\mathcal{R}_b|^2 + |\mathcal{T}_a^\perp\mathcal{R}_b|^2 + |\mathcal{T}_a\mathcal{R}_b^\perp|^2$$

$$-|\mathcal{T}_a^\perp\mathcal{R}_b^\perp|^2)\},$$

$$p_{\theta_a,\theta_b}(2_a,1_b) = \frac{1}{1+|\epsilon|^2}\{\cos^2(\theta_b)[\cos^2(\theta_a)(|\mathcal{R}_a\mathcal{T}_b^\perp|^2$$

$$+|\mathcal{R}_a^\perp\mathcal{T}_b\epsilon|^2) + \sin^2(\theta_a)(|\mathcal{R}_a^\perp\mathcal{T}_b^\perp|^2$$

$$+|\mathcal{R}_a\mathcal{T}_b\epsilon|^2)] + \sin^2(\theta_b)[\cos^2(\theta_a)(|\mathcal{R}_a\mathcal{T}_b|^2$$

$$+|\mathcal{R}_a^\perp\mathcal{T}_b^\perp\epsilon|^2) + \sin^2(\theta_a)(|\mathcal{R}_a^\perp\mathcal{T}_b|^2$$

$$+|\mathcal{R}_a\mathcal{T}_b^\perp\epsilon|^2)] + \sin(2\theta_a)\cos(2\theta_b)\mathrm{Re}(\epsilon\zeta/2)$$

$$\times(-|\mathcal{R}_a\mathcal{T}_b|^2 + |\mathcal{R}_a^\perp\mathcal{T}_b|^2 + |\mathcal{R}_a\mathcal{T}_b^\perp|^2$$

$$-|\mathcal{R}_a^\perp\mathcal{T}_b^\perp|^2)\},$$

$$p_{\theta_a,\theta_b}(2_a,2_b) = \frac{1}{1+|\epsilon|^2}\{\cos^2(\theta_b)[\cos^2(\theta_a)(|\mathcal{R}_a\mathcal{R}_b^\perp|^2$$

$$+|\mathcal{R}_a^\perp\mathcal{R}_b\epsilon|^2) + \sin^2(\theta_a)(|\mathcal{R}_a^\perp\mathcal{R}_b^\perp|^2$$

$$+|\mathcal{R}_a\mathcal{R}_b\epsilon|^2)] + \sin^2(\theta_b)[\cos^2(\theta_a)$$

$$\times(|\mathcal{R}_a\mathcal{R}_b|^2 + |\mathcal{R}_a^\perp\mathcal{R}_b^\perp\epsilon|^2) + \sin^2(\theta_a)$$

$$\times(|\mathcal{R}_a^\perp\mathcal{R}_b|^2 + |\mathcal{R}_a\mathcal{R}_b^\perp\epsilon|^2)]$$

$$+ \sin(2\theta_a)\cos(2\theta_b)\mathrm{Re}(\epsilon\zeta/2)(-|\mathcal{R}_a\mathcal{R}_b|^2$$

$$+|\mathcal{R}_a^\perp\mathcal{R}_b|^2 + |\mathcal{R}_a\mathcal{R}_b^\perp|^2 - |\mathcal{R}_a^\perp\mathcal{R}_b^\perp|^2)\}.$$

In the case of maximally entangled states, i.e., $\epsilon = 1$ and $\zeta = 1$, and ideal PBSs, i.e., $|\mathcal{R}_z| = |\mathcal{T}_z^\perp| = 0$ and $|\mathcal{R}_z^\perp| = |\mathcal{T}_z| = 1$, the $\hat{U}_{\psi\text{-PBS}}$ is simply given by

$$U_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}; \quad U_2 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix};$$

$$U_3 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & i & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}; \quad U_4 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix};$$

and

$$p_{\theta_a,\theta_b}(1_a,1_b) = p_{\theta_a,\theta_b}(2_a,2_b) = \sin^2(\theta_a - \theta_b)/2, \quad \text{(A1)}$$

$$p_{\theta_a,\theta_b}(1_a,2_b) = p_{\theta_a,\theta_b}(2_a,1_b) = \cos^2(\theta_a - \theta_b)/2.$$

APPENDIX B: DEAD-TIME CORRECTION DETERMINATION

According to Refs. [36,38], in the case of nonextending dead time, the correction is $\pi_z = 1/(1 + \bar{n}_z D_z/t)$, where $\bar{n}_z$

are the mean number of photons counted in the z channel, i.e., $\bar{n}_z = \Sigma_{x_z=1_z,2_z} \Sigma_k k p_{\text{tot},x_z}(k)$ with $p_{\text{tot},x_z}(k)$ calculated in the absence of dead time D_z, and $\xi_{x_z} = \eta_{x_z} \tau_{x_z}$. We can, therefore, write down the dead-time correction in this case as

$$\pi_a = \left\{ 1 + \sum_{x_a} \left[\sum_{y_b} p(x_a, y_b) \eta_{x_a} \tau_{x_a} \lambda_p + \eta_{x_a} \tau_{x_a} \lambda_{u,x_a} \right. \right.$$
$$\left. \left. + \lambda_{d,x_a} \right] D_a \right\}^{-1}$$

and

$$\pi_b = \left\{ 1 + \sum_{y_b} \left[\sum_{x_a} p(x_a, y_b) \eta_{y_b} \tau_{y_b} \lambda_p + \eta_{y_b} \tau_{Y_b} \lambda_{u,y_b} \right. \right.$$
$$\left. \left. + \lambda_{d,y_b} \right] D_b \right\}^{-1}$$

by noting that, when several devices are used in series, a good approximation considers the whole apparatus to be a black box, with a nonextending dead time equal to the largest of dead times of the single component [36]. We showed in Ref. [38] that π_z provides a satisfactory approximation for $t \gg D_z$.

[1] C. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore* (IEEE, New York, 1984), p. 175.

[2] A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[3] C.H. Bennett, G. Brassard, and N.D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

[4] G. Brassard, N. Lutkenhaus, T. Mor, and B.C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).

[5] A.K. Ekert, J.G. Rarity, P.R. Tapster, and G.M. Palma, Phys. Rev. Lett. **69**, 1293 (1992).

[6] A.V. Sergienko, M. Atature, Z. Walton, G. Jaeger, B.E.A. Saleh, and M.C. Teich, Phys. Rev. A **60**, R2622 (1999).

[7] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **84**, 4729 (2000).

[8] D.S. Naik, C.G. Peterson, A.G. White, A.J. Berglund, and P.G. Kwiat, Phys. Rev. Lett. **84**, 4733 (2000).

[9] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **84**, 4737 (2000).

[10] L. Mandel, J. Opt. Soc. Am. B **1**, 108 (1984).

[11] E. Jakeman and J.G. Rarity, Opt. Commun. **59**, 219 (1986).

[12] J.G. Rarity, P.R. Tapster, and E. Jakeman, Opt. Commun. **62**, 201 (1987).

[13] J.G. Rarity and P.R. Tapster, Appl. Phys. B: Photophys. Laser Chem. **55**, 298 (1992).

[14] D.C. Burnham and D.L. Weinberg, Phys. Rev. Lett. **25**, 84 (1970).

[15] D.N. Klyshko, *Photons and Nonlinear Optics* (Gordon and Breach Science, New York, 1988).

[16] J.G. Rarity, K.D. Ridley, and P.R. Tapster, Appl. Opt. **26**, 4616 (1987).

[17] A.N. Penin and A.V. Sergienko, Appl. Opt. **30**, 3582 (1991).

[18] P.G. Kwiat, A.M. Steinberg, R.Y. Chiao, P.H. Eberhard, and M.D. Petroff, Appl. Opt. **33**, 1844 (1994).

[19] A.L. Migdall, R.U. Datla, A.V. Sergienko, J.S. Orszak, and Y.H. Shih, Metrologia **32**, 479 (1996).

[20] S. Castelletto, A. Godone, C. Novero, and M.L. Rastello, Metrologia **32**, 501 (1996).

[21] M.M. Hayat, A. Joobeur, and B.E.A. Saleh, J. Opt. Soc. Am. A **16**, 348 (1999).

[22] G. Brida, S. Castelletto, C. Novero, and M.L. Rastello, J. Opt. Soc. Am. B **16**, 1623 (1999).

[23] G. Brida, S. Castelletto, I.P. Degiovanni, C. Novero, and M.L. Rastello, Metrologia **37**, 625 (2000).

[24] P.R. Tapster, J.G. Rarity, and P.C.M. Owens, Phys. Rev. Lett. **73**, 1923 (1994).

[25] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **81**, 3563 (1998).

[26] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **81**, 5039 (1998).

[27] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, NY, 2000).

[28] N. Boeuf, D. Branning, I. Chaperot, E. Dauler, S. Guerin, G. Jaeger, A. Muller, and A. Migdall, Opt. Eng. **39**, 1016 (2000).

[29] P.G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A.V. Sergienko, and Y. Shih, Phys. Rev. Lett. **75**, 4337 (1995).

[30] Entangled states may be successfully generated for this purpose by two type-I nonlinear crystals, according to P.G. Kwiat, E. Waks, A.G. White, I. Appelbaum, and P.H. Eberhard, Phys. Rev. A **60**, R773 (1999), so that the general state is $|\psi\rangle = |H_a\rangle |H_b\rangle - \exp[i\phi] |V_a\rangle |V_b\rangle$.

[31] P.G. Kwiat, A.J. Berglund, J.B. Altepeter, and A.G. White, Science **290**, 498 (2000).

[32] A.J. Berglund, e-print quant-ph/0010001.

[33] S. Castelletto, I.P. Degiovanni, and M.L. Rastello, in *Proceedings of the Fifth International Conference on Quantum Communication, Measurement and Computing, Capri, Italy*, edited by P. Tombesi and O. Hirota (Kluwer Academic, New York, 2001), p. 131.

[34] J. Perina, Jr., O. Haderka, and J. Soubusta, Phys. Rev. A **64**, 052305 (2001).

[35] S. Castelletto, I.P. Degiovanni, and M.L. Rastello, J. Opt. Soc. Am. B **19**, 1247 (2002).

[36] S. Castelletto, I.P. Degiovanni, and M.L. Rastello, Metrologia **37**, 613 (2000).

[37] S. Castelletto and I.P. Degiovanni private communication.

[38] S. Castelletto, I.P. Degiovanni, and M.L. Rastello, in *Advanced Mathematical and Computational tools in Metrology V,* edited by P. Ciarlini, M. Cox, E. Filipe, F. Pavese, and D. Richter (World Scientific, Singapore, 2001), p. 41.