Wigner tomography of two-qubit states and quantum cryptography

Thomas Durt,[1,*] Christian Kurtsiefer,[2,†] Antia Lamas-Linares,[2,‡] and Alexander Ling[3,§]
[1]*TENA VUB, Pleinlaan 2, 1050 Brussels, Belgium*
[2]*Centre for Quantum Technologies and Department of Physics, National University of Singapore, 117543 Singapore, Singapore*
[3]*Centre for Quantum Technologies and Temasek Labs, National University of Singapore, 117543 Singapore, Singapore*
(Received 31 August 2007; revised manuscript received 2 June 2008; published 31 October 2008)

Tomography of the two-qubit density matrix shared by Alice and Bob is an essential ingredient for guaranteeing an acceptable margin of confidentiality during the establishment of a secure fresh key through the quantum key distribution scheme. We show how the Singapore protocol for key distribution is optimal from this point of view, due to the fact that it is based on so-called symmetric informationally complete positive-operator-valued measure (SIC POVM) qubit tomography which allows the most accurate full tomographic reconstruction of an unknown density matrix on the basis of a restricted set of experimental data. We illustrate with the help of experimental data the deep connections that exist between SIC POVM tomography and discrete Wigner representations. We also emphasize the special role played by Bell states in this approach and propose a protocol for quantum key distribution during which a third party is able to concede or to deny *a posteriori* to the authorized users the ability to build a fresh cryptographic key.

DOI: 10.1103/PhysRevA.78.042338 PACS number(s): 03.67.Dd, 03.65.Wj, 42.50.−p

I. INTRODUCTION

The goal of quantum cryptographic protocols is to distill a fresh cryptographic key from data encoded in noncommuting bases. In order to guarantee the confidentiality of the key, it is essential that Alice and Bob, the authorized users of the channel, check the correlations between their respective signals in order to estimate the noise present along the transmission line. This procedure imposes severe constraints to a hypothetical eavesdropper (Eve) who cannot manipulate the signal at will and sees her freedom of action seriously limited by the control performed by Alice and Bob. This control procedure is optimal when the correlations tested by Alice and Bob are such that they allow them to carry out a full tomography of the signal [1]. This is the case, for instance, with the so-called six states protocol [2] during which Alice and Bob analyze their qubits in three mutually unbiased bases, which allows them to reconstruct the full density matrix of the signal. Due to the fact that in realistic situations the length of the key is always finite and that it is preferable that Alice and Bob do not sacrifice too many data during their check of the correlations, the optimal tomographic procedure is the one for which Alice and Bob are able to maximize the accuracy of their estimation of the signal, keeping fixed the quantity of data that they sacrifice in order to estimate the correlations. This problem has been studied in the past and it appears that the optimal procedure for performing full tomography (according to this figure of merit) is to measure a symmetric informationally complete positive-operator-valued measure (SIC POVM) [3–5]. This approach is at the core of the so-called Singapore protocol [6] for quantum key distribution where the signal is encrypted in such a way that Alice and Bob directly measure the SIC POVM distribution of their respective bits, and are consequently able to reconstitute the two-qubit density matrix of the full signal.

In the present paper we shall discuss certain advantages of the double qubit SIC POVM scheme from the point of view of tomography (Sec. II). We shall then establish a relation between SIC POVM tomography and the discrete Wigner representation (Sec. III and the Appendix). We shall also show (Sec. IV) that the Bell states constitute the optimal signal for the establishment of a cryptographic key. In the same section, we shall show how it is possible, thanks to slight modifications of the Singapore protocol [6], to provide to a third party who controls the source (Charles) the ability to deny to Alice and Bob the possibility to build a fresh key although they already recorded all the results of their measurements. Charles has nevertheless the possibility to choose *a posteriori* to provide them the possibility to do so, by communicating to them the relevant information on a classical communication line. Besides, even in the case that he allows them to establish a fresh key, Charles remains ignorant of the content of this key.

It is worth noting that, due to the fact that it is impossible to amplify a quantum cryptographic key by classical amplifiers, which prohibits the use of standard communication channels, the installation of a communication line for quantum key distribution (QKD) will remain an expensive investment. It is thus probable that in the case that quantum cryptography gets successfully commercialized, Alice and Bob, the authorized users of a quantum cryptographic channel, will not own it personnally but they will rather rent it to its owner (Charles). In the case that Alice and Bob rent the line to Charles in order to exchange a key, the protocol described in this paper presents obvious advantages regarding the possible commercialization of quantum key distribution.

Finally, we shall present in Sec. V experimental results that show that within an error of a few percent, all the theoretical concepts developed in this paper are concretely realizable.

*thomdurt@vub.ac.be
†christian.kurtsiefer@gmail.com
‡antia@quantumlah.org
§phylej@nus.edu.sg

II. ABOUT TWO-QUBIT TOMOGRAPHY

A. Optimal projection-valued-measure tomography

The estimation of an unknown state is one of the important problems in quantum information and quantum computation [7,8]. Traditionally, the estimation of the d^2-1 parameters that characterize the density matrix of a single qudit consists of realizing $d+1$ independent von Neumann measurements (also called projection-valued-measure measurements or PVM measurements in the literature) on the system.

As it was shown in [9,10], the PVM approach to tomography can be optimized regarding redundancy during the acquisition of the data. Optimality according to this particular figure of merit is achieved when the $d+1$ bases in which the PVM measurements are performed are "maximally independent" or "minimally overlapping" so to say when they are mutually unbiased [two orthonormal bases of a d-dimensional Hilbert space are said to be mutually unbiased bases (MUBs) if whenever we choose one state in the first basis, and a second state in the second basis, the modulus squared of their in product is equal to $1/d$] [9–11]. It is well known that, when the dimension of the Hilbert space is a prime power, there exists a set of $d+1$ mutually unbiased bases [9,10,12]. This is the case, for instance, with the bases that diagonalize the generalized Pauli operators [12,13]. Those unitary operators form a group which is a discrete counterpart of the Heisenberg-Weyl group, the group of displacement operators [14], that present numerous applications in quantum optics and in signal theory [15].

For instance, when the system is a spin-$1/2$ particle, three successive Stern-Gerlach measurements performed along orthogonal directions make it possible to infer the values of the three Bloch parameters p_x, p_y, and p_z defined by

$$\langle \sigma_x \rangle = p_x = \gamma \sin\theta \cos\varphi,$$

$$\langle \sigma_y \rangle = p_y = \gamma \sin\theta \sin\varphi,$$

$$\langle \sigma_z \rangle = p_z = \gamma \cos\theta. \tag{1}$$

Once we know the value of these parameters, we are able to determine unambiguously the value of the density matrix, making use of the identity

$$\rho(\gamma,\theta,\varphi) = \frac{1}{2}(I + p_x\sigma_x + p_y\sigma_y + p_z\sigma_z) = \frac{1}{2}(I + \vec{\gamma}\cdot\vec{\sigma}). \tag{2}$$

When the qubit system is not a spin-$1/2$ particle but consists of the polarization of a photon, a similar result can be achieved by measuring its degree of polarization in three independent polarization bases, for instance, with polarizing beam splitters, which leads to the Stokes representation of the state of polarization of the (equally prepared) photons.

Tomography through von Neumann measurements presents an inherent drawback: in order to estimate the d^2-1 independent parameters of the density matrix, $d+1$ measurements must be realized which means that d^2+d histograms of the counting rate are established, one of them being sacrificed after each of the $d+1$ measurements in order to normalize the corresponding probability distribution. From this point of view, the number of counting rates is higher than the number of parameters that characterize the density matrix, which is a form of redundancy, inherent to the tomography through von Neumann measurements.

In the case of tomographic protocols for QKD, Alice and Bob necessarily perform locally and independently a tomographic process on their respective qubits because they are separated in space and are not able in principle to carry out nonlocal measurements [13,16]. Of course by comparing the data gathered during local measurements they can reconstruct the full density matrix but this procedure is highly data consuming in the case of von Neumann (PVM) tomography. For instance, in the case that the carrier of the key is a qubit it requires them to estimate 36 joint probabilities. In the framework of quantum key distribution where the number of available data is *per se* limited and where the protocols of reconciliation and privacy amplification are *per se* highly data consuming it is better to find a tomographic procedure that minimizes the redundancies in the data acquisition. We shall discuss this procedure in the next section.

B. Optimal qubit POVMs for tomography

It is known that a more general class of measurements exists that generalizes the von Neumann (PVM) measurements. This class is represented by the POVM measurements [17], of which only a reduced subset, the PVM measurements correspond to the von Neumann measurements. The most general POVM can be achieved by coupling the system A to an ancilla or assistant B and performing a von Neumann measurement on the full system. When both the system and its assistant are qudit systems, the full system belongs to a d^2-dimensional Hilbert space, which makes it possible to measure d^2 probabilities during a von Neumann measurement performed on the full system. As always, one of the counting rates must be sacrificed in order to normalize the probability distribution so that we are left with d^2-1 parameters. When the coupling to the assistant and the von Neumann measurement are well chosen, we are able, in principle, to infer the value of the density matrix of the initial qudit system from the knowledge of those d^2-1 parameters, in which case the POVM is said to be informationally complete (IC). Obviously, this approach is optimal in the sense that it minimizes the number of counting rates (thus of independent detection processes) that must be realized during the tomographic process. In practice, the implementation of this class of optimal POVMs is simple and has advantages of its own compared to the usual polarization measurements based on von Neumann projections [18].

IC POVMs can also be further optimized regarding the independence of the data collected in different detectors. The so-called covariant symmetric-informationally-complete (SIC) POVMs [3] provide an elegant solution to this optimization constraint. A discrete version of the Heisenberg-Weyl group [19] also plays an essential role in the derivation of such POVMs, which are intimately associated to a set of d^2 minimally overlapping projectors onto pure qudit states (the modulus squared of their in product is now equal to $1/\sqrt{d+1}$).

In the rest of this paper we shall remain exclusively concerned with qubit SIC POVMs. It has been shown in the

past, on the basis of different theoretical arguments [3–5], that the optimal qubit SIC POVM is in one-to-one correspondence with a tetrahedron on the Bloch sphere. Intuitively, such tetrahedrons homogenize and minimize the informational overlap or redundancy between the four histograms collected during the POVM measurement. Some of such tetrahedrons can be shown to be invariant under the action of the Heisenberg-Weyl group which corresponds to so-called covariant SIC POVMs [3]. Concretely, during the measurement of such a SIC POVM, four probabilities of firing $P_{00},P_{01},P_{10},P_{11}$ are measured which are in one-to-one correspondence with the Bloch parameters p_x, p_y, and p_z as shown in the identity

$$P_{00}=\frac{1}{4}\left[1+\frac{1}{\sqrt{3}}(p_x+p_y+p_z)\right],$$

$$P_{01}=\frac{1}{4}\left[1+\frac{1}{\sqrt{3}}(-p_x-p_y+p_z)\right],$$

$$P_{10}=\frac{1}{4}\left[1+\frac{1}{\sqrt{3}}(p_x-p_y-p_z)\right],$$

$$P_{11}=\frac{1}{4}\left[1+\frac{1}{\sqrt{3}}(-p_x+p_y-p_z)\right]. \quad (3)$$

$2P_{00}$ is the average value of the operator $(\frac{1}{2})[\sigma_{0,0}+(\frac{1}{\sqrt{3}})(\sigma_{1,0}+\sigma_{0,1}+\sigma_{1,1})]$ (where $\sigma_{i,j}=\sqrt{(-1)^{i\cdot j}}\Sigma_{k=0}^{1}(-1)^{kj}|k+i \bmod 2\rangle\langle k|$; actually, $\sigma_{0,0}=Id$, $\sigma_{0,1}=\sigma_z$, $\sigma_{1,0}=\sigma_x$, $\sigma_{1,1}=\sigma_y$). One can check that this operator is the projector $|\phi\rangle\langle\phi|$ onto the pure state $|\phi\rangle=\alpha|0\rangle+\beta^*|1\rangle$ with $\alpha=\sqrt{1+\frac{1}{\sqrt{3}}}$, $\beta^*=e^{i\pi/4}\sqrt{1-\frac{1}{\sqrt{3}}}$. Under the action of the Pauli group it transforms into a projector onto one of the four pure states $\sigma_{i,j}|\phi\rangle$; i,j: 0,1: $\sigma_{i,j}|\phi\rangle\langle\phi|\sigma_{i,j}=(\frac{1}{2})\{(1-\frac{1}{\sqrt{3}})\sigma_{0,0}+(\frac{1}{\sqrt{3}})[\Sigma_{k,l=0}^{1}(-1)^{i\cdot l-j\cdot k}\sigma_{k,l}]\}$. The signs $(-1)^{il-jk}$ reflect the (anti)commutation properties of the Pauli group. So, the four parameters P_{ij} are the average values of projectors onto four pure states that are "Pauli displaced" of each other. The in product between them is equal, in modulus, to $1/\sqrt{3}=1/\sqrt{d+1}$, with $d=2$ which is the signature of a SIC POVM [3]. One can show [3–5] that such tetrahedrons minimize the informational redundancy between the four collected histograms due to the fact that their angular opening is maximal. The number of counting rates necessary in order to realize a tomographic process by a factorizable POVM measurement is optimal and equal to 16 in the two-qubit case. Moreover, the double qubit SIC POVM tomographic scheme is optimal among the factorizable two-qubit schemes if we consider as a figure of merit [20] the determinant D of the matrix that maps the joint probabilities of firing that are collected during the experiment onto the coefficients of the density matrix [4]. This determinant is optimal (minimal) for the SIC POVM (tetrahedron process) in the single qubit case and factorizes when the tomographic process does, so that the determinant of the double tetrahedron process is extremal among the determinants of all factorisable tomographic processes.

For all these reasons, the SIC POVM approach is at the core of the so-called Singapore protocol [6] for quantum key distribution where the signal is encrypted in such a way that Alice and Bob directly measure the SIC POVM distribution of their respective bits.

III. QUBIT SIC POVMs AND DISCRETE WIGNER DISTRIBUTION

A. Single qubit case

The qubit covariant SIC POVM possesses another very appealing property [21] which is also true in the qutrit case but not in dimensions strictly higher than 3 [22]: the qubit covariant SIC POVM is a direct realization (up to an additive and a global normalisation constants) of the qubit Wigner distribution of the unknown qubit a. Indeed, this distribution W is the symplectic Fourier transform of the Weyl distribution w [23,24] [defined by the relation $w_{i,j}=(1/2)\mathrm{Tr}(\rho.\sigma_{i,j})$] which is, in the qubit case, equivalent (up to a relabeling of the indices) to its double qubit-Hadamard or double qubit-Fourier transform as follows:

$$W_{k,l}=(1/2)\sum_{i,j=0}^{1}(-1)^{il-jk}w_{i,j}$$

$$=\left[(1/\sqrt{2})\sum_{i=0}^{1}(-1)^{il}\right]\left[(1/\sqrt{2})\sum_{j=0}^{1}(-1)^{-jk}\right]w_{i,j}. \quad (4)$$

One can check that $P_{k,l}=(1/\sqrt{3})W_{k,l}+(1-1/\sqrt{3})/4$. The discrete qubit-Wigner distribution directly generalizes its continuous counterpart [25] in the sense that it provides information about the localization of the qubit system in a discrete 2×2 phase space [23,26]. For instance, the Wigner distribution of the first state of the computational basis (spin up along Z) is equal to $W_{k,l}(|0\rangle)=(1/2)\delta_{k,0}$, which corresponds to a state located in the "position" spin up (along Z), and homogeneously spread in "impulsion" (in spin along X), in accordance with uncertainty relations [27]. Similarly, the Wigner distribution of the first state of the complementary basis (spin up along X) is equal to $W_{k,l}[(1/\sqrt{2})(|0\rangle+|1\rangle)]=(1/2)\delta_{l,0}$. For information, the fidelities that were achieved in recent experimental realizations of one qubit SIC POVM tomography were shown to be of the order of 92% in a NMR realization [28] and 99% in a quantum optical realization [18].

B. Double qubit case

Certain Wigner distributions factorize in the sense that in the two-qubit case it is possible to measure a two-qubit or quartit-Wigner distributions [29,30] by measuring simultaneously local qubit SIC POVMs. For instance, a factorizable Wigner distribution derived in Refs. [29,30] in the case $d=4$ is obtained by performing the tetrahedron measurement on the first qubit and the antitetrahedron measurement on the second qubit. The tops of the antitetrahedron are obtained from the tops of the tetrahedron by performing on the Bloch sphere a central symmetry around the origin (Fig. 1). This transformation is not unitary, but one can show (p. 4 of Ref. [31]) that the antitetrahedron is equivalent to the tetrahedron, up to a well-chosen unitary transformation, provided we

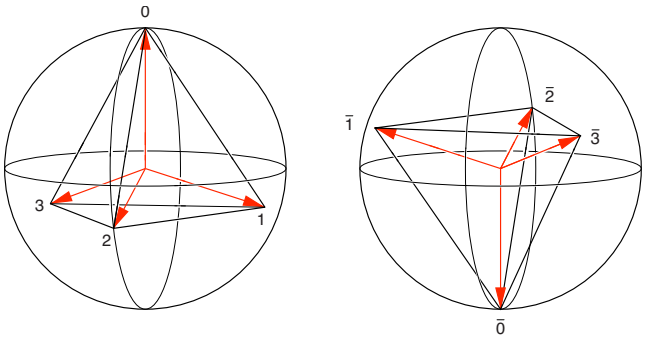

FIG. 1. (Color online) Relative orientation of the tetrahedron (left) and antitetrahedron (right) POVMs on the Bloch sphere. Transforming from the tetrahedron POVM to the antitetrahedron POVM involves both a rotation and a relabeling of the possible outcomes.

modify the order of its branches accordingly. Henceforth we shall most often in the following refer to the simultaneous measurement of local SIC POVMs under the label "double tetrahedron" measurement without noting whether we group the 16 joint probabilities assigned to the 8 (4+4) detectors according to the tetrahedron-tetrahedron (TT) or tetrahedron-antitetrahedron (TA) configuration.

C. Double tetrahedron measurement and tomography

The relation between the statistics of the double tetrahedron measurement and the double Wigner distribution is a straightforward generalization of the corresponding relation in the single qubit case. Let us denote $P_{k,l}$ (where k and l run from 0 to 3) the joint probability of firing of the kth (lth) tetrahedron detector on qubit a (tetrahedron detector on qubit b), and let us define P_k^a (P_l^b) by $P_k^a=\Sigma_{l=0}^3 P_{k,l}^{ab}$ ($P_l^b=\Sigma_{k=0}^3 P_{k,l}^{ab}$), then the double Wigner coefficients $W_{k,l}$ can be derived from the statistics of joint detections via the relation

$$W_{k,l}^{ab}=3P_{k,l}^{ab}+\sqrt{3}(1-\sqrt{3})/4(P_k^a+P_l^b)+[(1-\sqrt{3})/4]^2, \quad (5)$$

where the indices k and l run from 0 to 3.

As the Wigner operators form a basis of the 4×4 linear operators and are orthogonal relatively to the trace norm, we can reconstruct the full density matrix once we know its double Wigner coefficients, and those are in one to one correspondence with the joint probabilities of firing of the detectors associated to branches of the local (a and b) tetrahedrons.

In a following section we shall study the properties of Wigner distributions of Bell states and compare theoretical predictions with data obtained from direct experimental measurement of the correlations.

IV. OPTIMAL ENTANGLED STATES AND CRYPTOGRAPHY

A. Optimal entangled states for cryptography

We learned from the entanglement-based protocol proposed by Ekert [32] that it can be useful to exploit nonlocal correlations between entangled distant quantum systems in order to build a fresh cryptographic key. At this level we did not mention yet explicitly in which bipartite (two-qubit) state the signal was prepared. We shall now show that when the key is established by the double tetrahedron protocol (as in Singapore's protocol [6]), the optimal strategy is to prepare the pairs of qubits sent to Alice and Bob along Bell states (up to local unitaries).

The main argument is a symmetry argument. As we mentioned, qubit SIC POVMs are optimal because they are symmetric, e.g., such POVMs are defined by four pure states that form an equiangular set (tetrahedron) and are treated on the same footing. In order to exploit maximally this symmetry it is natural to try to find entangled states that exhibit either symmetric correlations or symmetric anticorrelations between different branches of the tetrahedrons in the a and b regions. As the tomographic process is full (the Wigner operators form a complete orthonormal basis), once we know the correlation, we also know the state that produces such correlations. We shall show that all states that exhibit symmetric anticorrelations are Bell states up to well-chosen local unitaries (rotations), and that no physically realizable state exhibits symmetric correlations.

In the case that we consider situations during which the experimental configuration of Alice and Bob's devices is fixed there remains a single degree of freedom that consists of varying the labels of the four detectors at each side.

There are then essentially $4!=24$ ways (and not 24^2 ways due to the isotropy of correlations) to group the branches of the tetrahedrons at each side, so that we must now investigate the possibility of perfect correlations (anticorrelations) in each of those cases. The 24 permutations between the four tops of the tetrahedron can be realized either by unitary or by antiunitary transformations so that those permutations can be partitioned according to their order and their parity [we can define the parity of a permutation in the function of the determinant of the 3×3 matrix that represents the action at the level of the Bloch sphere of the orthogonal or "antiorthogonal" transformation that realizes the corresponding permutation at the level of the tetrahedron branches: even transformations correspond to a value +1 (orthogonal transformations), odd ones to −1 (antiorthogonal transformations)] [39].

The identity is even and of order 1, there are three ($4\times3/2\times2$) even permutations of order 2 with no fixed top and 6 ($4\times3/2$) odd permutations of order 2 with two fixed tops, eight (4×2) even permutations of order 3 with one fixed top, and six odd permutations of order 4 with no fixed top. These 12 (identity+11) even permutations can be realized by unitary transformations: the three even permutations of order 2 with no fixed top are associated to the Pauli σ operators (rotations of 180° around X, Y, and Z) while the eight even permutations of order 3 with one fixed top correspond to rotations of +/−120 degrees around the axis of the fixed top.

The 12 remaining (odd) permutations can be decomposed into an odd permutation that fixes two tops and permutes the two remaining ones (described in details in Ref. [31], footnote 38), and an even permutation that can be realized by one among the 12 aforementioned unitary transformations. The reasoning goes as follows: once we impose symmetric

correlations (anticorrelations) the Wigner distribution is fully determined and so is the density matrix of the corresponding state. In principle, we ought to construct case by case 24 candidate states for the symmetric correlations and 24 other ones for the symmetric anticorrelations, and check whether the candidates that we find so are physical states (positive-definite Hermitian operators of trace 1). Due to the unitary equivalence between all even configurations and all odd ones, it is enough to check two candidates in the case of perfect correlations and two candidates in the case of perfect anticorrelations, which we shall do now.

Let us first consider a TT (even) configuration and let us assume the existence of perfect correlations between equally labeled detectors at Alice and Bob's sides so that the joint probabilities obey $P_{k,l}=(1/4)\delta_{k,l}$; k,l: 0, 1, 2, 3. The expression (5) considerably simplifies in the case of symmetric correlations, when all detectors fire with equal probability one-fourth at each side. Then we have

$$W_{k,l}^{ab}=3P_{k,l}^{ab}-(1/8). \tag{6}$$

Making use of this relation we get that $W_{k,l}=(-1/8)+(3/4)\delta_{k,l}$; k,l: 0, 1, 2, 3. Making use of the identity $\rho=\Sigma_{k_a,k_b,l_a,l_b=0}^{1}(1/4)W_{k_a,l_a}W_{k_b,l_b}$ where the local (qubit) Wigner operators were defined in Eq. (4), we find by a straightforward computation that $\rho=(1/4)[Id^{ab}+3(\sigma_X^a\sigma_X^b+\sigma_Y^a\sigma_Y^b+\sigma_Z^a\sigma_Z^b)]=|00\rangle\langle 00|+|11\rangle\langle 11|-(1/2)|01\rangle\langle 01|-(1/2)|10\rangle\langle 10|+(3/2)|01\rangle\langle 10|+(3/2)|10\rangle\langle 01|$. Such an operator possesses a negative eigenvalue so that it cannot be realized physically.

If now we impose perfect (and isotropically distributed) anticorrelations then the joint probabilities must obey $P_{k,l}=(1/12)-(1/12)\delta_{k,l}$; k,l: 0, 1, 2, 3.

By a similar treatment, we find that

$$W_{k,l}=(1/8)-(1/4)\delta_{k,l};k,l:0,1,2,3. \tag{7}$$

and $\rho=(1/4)(Id^{ab}-\sigma_X^a\sigma_X^b-\sigma_Y^a\sigma_Y^b-\sigma_Z^a\sigma_Z^b)=|\Psi_-\rangle\langle\Psi_-|$ where $|\Psi_-\rangle=\frac{1}{\sqrt{2}}(|1\rangle^a|0\rangle^b-|0\rangle^a|1\rangle^b)$, which is nothing else than the projector onto the singlet state. In the previous treatment we assumed that a TT configuration had been chosen. If instead we impose perfect correlations (anticorrelations) in a TA configuration, that we choose at this level to be such that we can replace W_{k_b,l_b} by a similar operator but with opposite signs in front of the operators σ_x, σ_y, and σ_z (this is a configuration where instead of orienting their tetrahedrons parallely, Alice and Bob choose an experimental setup in which they orient them antiparallely [34]). Imposing now perfect correlations (anticorrelations) between equally labeled detectors in this configuration we find by a direct computation that $\rho=(1/4)[Id^{ab}-3(\sigma_X^a\sigma_X^b+\sigma_Y^a\sigma_Y^b+\sigma_Z^a\sigma_Z^b)]$ in the first case, and $\rho=(1/4)(Id^{ab}+\sigma_X^a\sigma_X^b+\sigma_Y^a\sigma_Y^b+\sigma_Z^a\sigma_Z^b)$ in the second case.

Such operators are easily shown to admit negative eigenvalues so that no physically acceptable state would allow us to obtain symmetric correlations or anticorrelations in this particular configuration. Actually this is not so astonishing for what concerns symmetric anticorrelations because the partial transposition of a singlet state provides a nonphysical state as is well known [35].

As a consequence of the fact that the 12 TT (even) configurations as well as the 12 TA (odd) ones are unitarily equivalent, we have established the following properties:

(A) In each of the 12 TT configurations there exists exactly one state that exhibits symmetric or isotropic anticorrelations, and this state is equivalent to the singlet state up to a well-defined local unitary transformation.

(B) In each of the 12 TA (odd) configurations, it is impossible to find a state that exhibits perfect anticorrelations between Alice and Bob's detectors.

(C) In each of the 12 TA (odd) and 12 TT (even) configurations, it is impossible to find a state that exhibits perfect correlations between Alice and Bob's detectors.

B. Optimal entangled states and generalized cryptographic protocol

It is worth noting that when we locally rotate the singlet state around the axis of one of the tops of the tetrahedron, or around its major axes (X, Y, and Z), we still obtain a state that is equivalent, up to a local unitary transformation, to a singlet state and is thus maximally entangled.

In particular, when we locally rotate the singlet state around one of the major axes (X, Y, and Z) of the tetrahedron, we still obtain a Bell state. Those transformations can be shown to form a group, the Pauli group or discrete displacement (Heisenberg-Weyl) group [36].

As the four Bell states can be obtained from the singlet state by letting act locally one of the Pauli displacement (σ) operators onto the singlet state and that these operators map the tetrahedron onto itself, the four Bell states exhibit symmetric and perfect anticorrelations at the level of Alice and Bob's detectors.

Besides, one can easily check that different Bell states anticorrelate one detector at Alice's side with different detectors at Bob's side and vice versa. This is the main feature that we shall exploit in what follows: when Alice and Bob ignore which Bell state they share, they also ignore which of their detectors are anticorrelated and are unable to establish a key.

Let us now assume that a third party (Charles) controls the source, say a singlet state source (actually a source of an arbitrary Bell state would be equally convenient) and has the possibility to rotate at will Bob's qubit of 180° around one of the three main axes of Bob's tetrahedron (or to do nothing). If Charles decides to carry out one of those four rotations (Pauli displacements) at random with equal probability (25%) without communicating his choices to Alice and Bob, their signal will obviously be totally uncorrelated. If now Charles decides afterwards to inform them about his respective choices they will be able to reconstruct a confidential key (according to the Singapore protocol [6], for instance). Due to the symmetry of the correlations exhibited by the Bell states, Charles will remain totally ignorant of the data measured by Alice and Bob, which guarantees the confidentiality of their key.

We see thus that Charles possesses the capacity to deny at will to Alice and Bob the authorization to establish a fresh key, even after they measured all the necessary data. This possibility could lead to interesting applications in realistic

quantum cryptographic schemes, for instance in the case that Alice and Bob would rent the cryptographic quantum transmission line to Charles, its legitimate owner, who would be supposed to be able to control the source and to produce at will one among the four Bell states.

Before finishing this section it is worth comparing the POVM-based QKD protocols of the type considered in the present paper with PVM-based protocols. One could imagine, for instance, that even in the (Ekert version of the) Bennett-Brassard 1984 (BB84) protocol, which is a PVM-based protocol, the owner of the line Charles controls the source and encodes the signal at random in the Bell states Ψ^- and Φ^+. In such a case Alice and Bob's signal is an incoherent sum with equal weights of perfectly correlated and anticorrelated signals (in the X and Z bases). Such a signal is totally useless for establishing a key before Charles accepts to reveal to Alice and Bob what his prepared states were. The feasibility of a modified BB84 protocol based on entangled photons has been proven experimentally [37]. Besides, an apparent advantage of the POVM scheme is that it is not necessary to change constantly and randomly the measurement basis so that we avoid the losses due to basis reconciliation (sifting) but one should note that the effective gain in bit transfer rate is negligible in comparison to, say, the BB84 protocol because the POVM-based protocol requires a posttreatment of the correlated data [6] that is equally data consuming.

Moreover the number of copies needed for state estimation can be made arbitrarily smaller than the number of copies needed for the key and it is only when considering finite number effects in a practical implementation that it is advantageous to use a POVM measurement instead of a conventional, PVM, one.

Considered so, the POVM approach is not superior to the PVM approach. Nevertheless it is worth noting that beside advantages regarding tomography, POVM measurements also present effective advantages regarding calibration and stability and remain a promising candidate for quantum key distribution.

In the next section, we represent experimental confirmations of our theoretical predictions concerning anticorrelations exhibited by Bell states.

V. EXPERIMENTAL TOMOGRAPHY OF BELL STATES

The aforementioned Singapore protocol for QKD, in which Alice and Bob share a single state and establish a secret key on the basis of the anticorrelations exhibited by this singlet state when they both realize an optimal SIC POVM onto their respective qubit has been implemented experimentally (see Fig. 2). Among others this implementation requires a simple polarimetric setup in order to realize the qubit covariant SIC POVM. This setup was shown in the past to perform tomographic reconstruction of any arbitrary qubit state with high fidelity (differing from unity by less than 1%) [18].

We used a pair of such setups in order to implement a double tetrahedron measurement on arbitrary Bell states. To prepare the Bell states, we used a spontaneous parametric down-conversion (SPDC) source of entangled photon pairs [38]. The pairs of photons are identified by coincidence timing and the probabilities derived from the raw count rates via normalization to the total number of coincidences (Fig. 3).

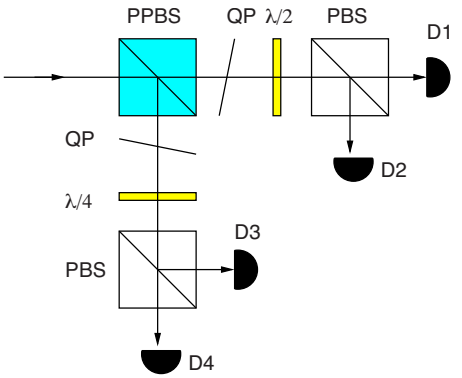

FIG. 2. (Color online) Experimental implementation of a single tetrahedron measurement. The incoming photon is incident upon a partially polarizing beam splitter (PPBS) and each of the output arms is modified by the combination of a quartz plate (QP) to modify the phase between H and V polarizarions, and either a quarter wave plate ($\lambda/4$) or a half wave plate ($\lambda/2$) to rotate into the right measurement basis. The final projection is performed by polarizing beam splitters (PBS). The individual photons are detected by Si avalanche photodiodes. Changing from a tetrahedron to an antitetrahedron measurement involves only a change in orientation of the wave plates and a relabeling of the detector outputs.

We first prepared the singlet Bell state $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|1\rangle^a|0\rangle^b - |0\rangle^a|1\rangle^b)$, which we measured in the TT configuration and also in the TA configuration. The second time, we prepared the Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle^a|0\rangle^b + |1\rangle^a|1\rangle^b)$ that we measured in the TT configuration. In each case we measured the correlation matrices that represent the relative frequency of coincidental signals between the detectors of Alice and Bob.

On the basis of those matrices we obtain, making use of the relation (5), their respective Wigner distributions. The ideal, theoretical counterpart of the Wigner matrice $W^{TT}(\Psi^-)$ is expressed by Eq. (7):

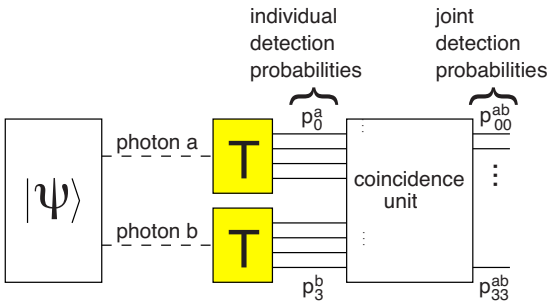

FIG. 3. (Color online) Tetrahedron-based measurements. Each member of a photon pair is sent to a measurement device implementing either the tetrahedron (T) or antitetrahedron (A) POVM (see also Fig. 2). Coincidence timings between a pair of tetrahedron measurements are translated into probabilities by normalizing each joint detection between a particular detector pair to the total number of joint detections.

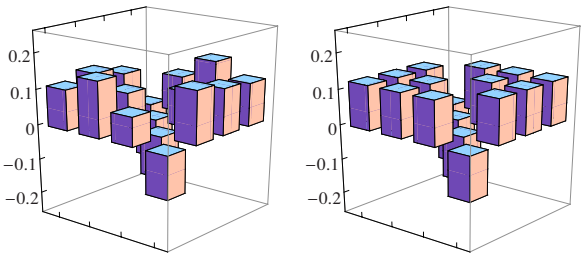

FIG. 4. (Color online) Experimental (left) versus theoretical [right, Eq. (8)] histograms of the Wigner distribution of the singlet state in the TT configuration.

$$W^{TT}(\Psi^-) = (1/8)\begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}. \tag{8}$$

The counterpart of $W^{TA}_{theor}(\Psi^-)$ can be shown [39] to be equal to

$$W^{TA}_{theor}(\Psi^-) = (1/4)\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{9}$$

Similarly, one gets that

$$W^{TT}(\Phi^+) = (1/8)\begin{pmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 \end{pmatrix}. \tag{10}$$

We controlled that, up to experimental discrepancies and *ad hoc* reorderings of the coefficients, the experimental Wigner distributions corresponded to their theoretical counterpart. Those results are plotted in Figs. 4–6.

We could estimate by a straightforward computation the fidelity of the experimental tomographic procedure, making use of the orthonormalization of the Wigner operators regarding the trace norm. The fidelity is equal to four times the sum of the products of the experimentally obtained Wigner coefficients with their theoretical counterparts. We obtain so fidelities equal to 0.960 and 0.956 for the singlet (Ψ^-) state in the TT and TA configurations, and a bit less for the Φ^+

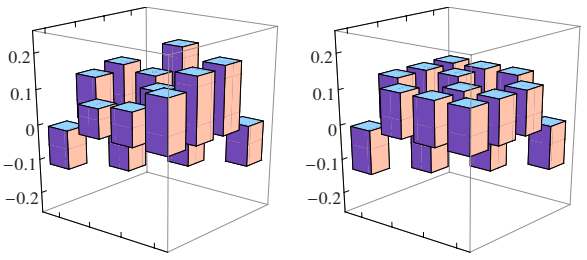

FIG. 5. (Color online) Experimental (left) versus theoretical [right, Eq. (8)] histograms of the Wigner distribution of the state Φ^+ in the TT configuration.

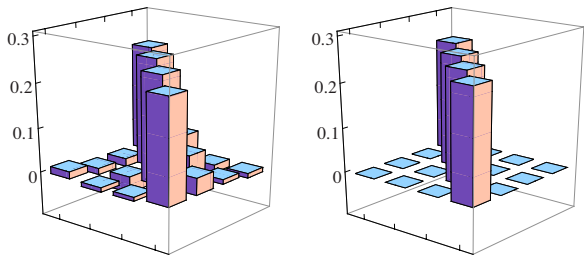

FIG. 6. (Color online) Experimental (left) versus theoretical [right, Eq. (9)] histograms of the Wigner distribution of the singlet state in the TA configuration.

state. The fidelities are less high than for the single qubit tomographic process [18], which is not astonishing because in the present case, additive experimental errors are likely to occur at the level of the source of entangled states, and also at both sides during the local one-qubit SIC POVM processes. Moreover, supplementary errors could also be due to a misalignment between the local tetrahedrons and to finite-size statistical effects (the sample sizes were of the order of 4×10^4).

This topic is out of the scope of the present paper but we inform the reader that in the Appendix of Ref. [31] the question of the factorizability of two-qubit Wigner distributions [23,29] is discussed in detail in relation with the two possible choices of configurations (TT and TA).

VI. CONCLUSION

Protocols for quantum key distribution that allow Alice and Bob to perform full tomography of the signal are optimal for what concerns security against eavesdropping. Due to the fact that in such protocols the amount of data is *per se* limited, full tomographic protocols based on SIC POVM tomography are also optimal for what concerns the authentification protocol. We showed that the natural entangled states that respect the symmetry of SIC POVMs are the Bell states (up to local unitaries). We also showed how their properties make it possible to conceive a protocol during which a third party (Charles) controls the source and is free to concede the authorization to Alice and Bob to establish a key *after* they measured all the physical data necessary therefore. This possibility opens the way to interesting applications in the case of realistic commercial developments of quantum cryptography; for instance it opens the possibility of delayed on-line payment by the users who rent the cryptographic line.

ACKNOWLEDGMENTS

T.D. acknowledges support from the ICT Impulse Program of the Brussels Capital Region (Project Cryptasc), the IUAP programme of the Belgian government, the Grant V-18, the Solvay Institutes for Physics and Chemistry, the Fonds voor Wetenschappelijke Onderzoek, Vlaanderen, and last but not least, support from the Quantum Lah at N.U.S. A.L., A.L.-L., and C.K. acknowledge support from ASTAR under SERC Grant No. 052 101 0043. The authors thank the referees and Michel Planat for their helpful comments.

[1] Y. C. Liang, D. Kaszlikowski, B.-G. Englert, L.-C. Kwek, and C. H. Oh, Phys. Rev. A **68**, 022324 (2003).
[2] D. Bruss, Phys. Rev. Lett. **81**, 3018 (1998).
[3] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, J. Math. Phys. **45**, 2171 (2004).
[4] A. E. Allahverdyan, R. Balian, and Th. M. Nieuwenhuizen, Phys. Rev. Lett. **92**, 120402 (2004).
[5] J. Rehacek, B.-G. Englert, and D. Kaszlikowski, Phys. Rev. A **70**, 052321 (2004).
[6] B.-G. Englert, D. Kaszlikowski, J. Rehacek, H.-K. Ng, W.-K. Chua, and J. Anders, e-print arXiv:quant-ph/0412075.
[7] Isaac L. Chuang *et al.*, Nature (London) **393**, 143 (1998).
[8] C. H. Bennett and D. P. Divincenzo, Nature (London) **404**, 247 (2000).
[9] I. D. Ivonovic, J. Phys. A **14**, 3241 (1981).
[10] W. K. Wootters and B. D. Fields, Ann. Phys. (N.Y.) **191**, 363 (1989).
[11] J. Schwinger, Proc. Natl. Acad. Sci. U.S.A. **46**, 570 (1960).
[12] S. Bandyopadhyay, P. Boykin, V. Roychowdhury, and F. Vatan, Algorithmica **34**, 512 (2002).
[13] T. Durt, J. Phys. A **38**, 5267 (2005).
[14] D. F. Walls and Gerard J. Milburn, *Quantum Optics* (Springer, Berlin, 1994).
[15] A. Vourdas, J. Phys. A **29**, 4275 (1996).
[16] G. Bjork, J. L. Romero, A. B. Klimov, and L. L. Sanchez-Soto, J. Opt. Soc. Am. B **24**, 371 (2007).
[17] Michael A. Nielsen and Isaac L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
[18] A. Ling, K. P. Soh, A. Lamas-Linares, and C. Kurtsiefer, Phys. Rev. A **74**, 022309 (2006).
[19] H. Weyl, Z. Phys. **46**, 1 (1927); *Gruppenthorie und Quantenmechanik* (1928); english translation by H. P. Robertson and E. P. Dutton (NY, 1932).
[20] Let us consider as an illustrating example that conventional, PVM, qubit tomography is realized in three nearly linearly dependent bases, very close to each other. This is obviously a bad tomographic process regarding the redundancy of the collected data. In such a situation, certain coefficients of the density matrix must be estimated on the basis of the differences between frequencies collected in the different bases. Those differences are very small parameters when those bases are strongly overlapping, which corresponds to a high value of the determinant D of the matrix that maps the average probabilities of firing that are measured during the experiment onto the coefficients of the density matrix. In such a case the small experimental discrepancies that affect the measured mean frequencies are strongly amplified during the estimation process of the density matrix and a precise tomography requires, in accordance with the law of large numbers, a high number of data. As we see, a "good" tomographic process corresponds to a small value of the determinant D.
[21] W. K. Wootters, Found. Phys. **36**, 112 (2006).
[22] S. Colin, J. Corbett, T. Durt, and D. Gross, J. Opt. B: Quantum Semiclassical Opt. **7**, S778 (2005).
[23] W.-K. Wootters, Ann. Phys. (N.Y.) **176**, 1 (1987).
[24] T. Durt, Int. J. Mod. Phys. B **20**, 1742 (2006).
[25] E. P. Wigner, Phys. Rev. **40**, 749 (1932); M. Hillery, R. F. O'Connell, M. O. Scully, and E. P. Wigner, Phys. Rep. **106**, 121 (1984).
[26] K. S. Gibbons, M. J. Hoffman, and W. K. Wootters, Phys. Rev. A **70**, 062101 (2004).
[27] A. O. Pittenger and M. H. Rubin, J. Phys. A **38**, 6005 (2005).
[28] J. F. Du, M. Sun, X. Peng, and T. Durt, Phys. Rev. A **74**, 042341 (2006).
[29] W. K. Wootters, IBM J. Res. Dev. **48**, 99 (2004).
[30] T. Durt, e-print arXiv:quant-ph/0604117; Open Syst. Inf. Dyn. **13**, 1 (2006); Laser Phys. **16**, 1557 (2006).
[31] T. Durt, A. Lamas-Linares, C. Ling, and C. Kurtsiefer, e-print arXiv:quant-ph/0806.0272.
[32] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[33] We could as well have defined the parity of permutations following the mathematical tradition in which the parity of a permutation is defined to be equal to the parity of the number of elementary (two by two) permutations necessary for realizing this permutation.
[34] In a following section we shall present experimental results that were collected in this configuration. As we show in the long version of our paper that can be found on the arXives (Ref. [30]) such a configuration is equivalent to the TT configuration, up to a well-chosen rotation and a well-chosen (odd) permutation of a pair of local detectors.
[35] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).
[36] The Pauli group is a normal subgroup of the Clifford group that also counts 24 elements. Clifford unitaries are a class of group operations that stabilize Pauli operations [40,41]. Michel Planat (private communication) drew our attention to the fact that there exists an isomorphism between the central quotient of the single qubit Clifford group, the group of quaternions automorphisms, and the group of permutations of the tetrahedron tops (the symmetric group S4 with 24 elements) considered in the present paper.
[37] I. Marcikic, A. Lamas-Linares, and C. Kurtsiefer, Appl. Phys. Lett. **89**, 101122 (2006); A. Poppe, A. Fedrizzi, T. Loruenser, O. Maurhardt, R. Ursin, H. R. Boehm, M. Peev, M. Suda, C. Kurtsiefer, H. Weinfurter, T. Jennewein, and A. Zeilinger, Opt. Express **12**, 3865 (2004).
[38] C. Kurtsiefer, M. Oberparleiter, and H. Weinfurter, Phys. Rev. A **64**, 023802 (2001).
[39] Actually it is shown in Ref. [42] with the help of very general arguments that the two matrices (8) and (9) do cover all possible phase space representations of Bell states (up to trivial reorderings associated to translations generated by the local displacement operators). This question is also discussed in the Appendix of Ref. [30].
[40] M. Appleby, J. Math. Phys. **46**, 052107 (2005).
[41] M. Planat and M. Kibler, e-print arXiv:0807.3650.
[42] J. P. Paz, A. J. Roncaglia, and M. Saraceno, Phys. Rev. A **72**, 012309 (2005).