

Probabilistic minimal disturbance measurement of symmetrical qubit states

R. Filip,¹ L. Mišta, Jr.,¹ F. De Martini,² M. Ricci,² and F. Sciarrino^{3,2}

¹*Department of Optics, Palacký University, 17. listopadu 50, Olomouc 772 00, Czech Republic*

²*Dipartimento di Fisica, Università di Roma "La Sapienza," Piazzale Aldo Moro 5, Roma 00185, Italy*

³*Centro Studi e Ricerche "Enrico Fermi," Via Panisperna 89/A Compendio del Viminale, Roma 00184, Italy*

(Received 4 May 2006; published 8 November 2006)

We derive fidelity tradeoffs for probabilistic minimal disturbance measurements for certain discrete sets of symmetrical single qubit states. We propose and experimentally demonstrate a simple linear optical scheme saturating these tradeoffs in which the degree of disturbance is controlled only by measurement of a single ancillary photon.

DOI: [10.1103/PhysRevA.74.052312](https://doi.org/10.1103/PhysRevA.74.052312)

PACS number(s): 03.67.Hk, 03.65.Ta, 42.50.Xa

Extraction of information from operation on a quantum system is inevitably accompanied by disturbance of the state of this system. Moreover, the more information is gained the larger is the disturbance. This at first sight undesirable property of quantum systems has on the contrary a practical application: it allows one to distribute a secret key between authorized communicating parties [1]. To simply demonstrate such the fundamental property of quantum operations it is sufficient to use a suitable finite set of nonorthogonal quantum states. For a single two-level system (qubit) this can be the set of states comprising three mutually unbiased bases [2,3] given, for instance, by eigenvectors of the Pauli matrices σ_x , σ_y , and σ_z . Similarly, for a qubit on the equator of the Bloch sphere (equatorial qubit) this can be the set of states forming two mutually unbiased bases on the equator of the Bloch sphere given by the eigenvectors of the Pauli matrices σ_x and σ_y . Since the two sets represent an alphabet of states into which information is encoded in the six-state [4] and four-state [5] cryptography protocols, respectively, in what follows we speak about six-state and four-state encoding, respectively. These encodings also represent a primitive of a quantum experiment in which a destructive effect of quantum operation on a quantum state can be experimentally observed. This effect was theoretically described using different approaches. Previously, it was discussed for the case of (i) an ensemble of identical states [6] or (ii) a continuous ensemble of completely randomly prepared states [7–9]. The quantities used to quantify the information gain and the state disturbance were in the task (i) distinguishability and fringe visibility [6] while in the task (ii) these were the mean estimation fidelity and the mean output fidelity, respectively [7]. In both the approaches the interplay between the state disturbance and the information gain is then expressed as a certain optimal tradeoff between the two quantities. Particularly interesting are the so-called minimal disturbance measurements (MDMs), i.e., quantum operations which achieve the above-mentioned optimal tradeoffs because they introduce for a given information gain the least possible disturbance. Besides being of fundamental interest MDMs can be used for increase of transmission fidelity of a certain lossy quantum channel [10].

To demonstrate the effect of state disturbance experimentally one has to perform the nondestructive measurements. For this purpose it is necessary to couple the measured system to a probe by a suitable interaction [11]. By controlling probe input state and/or measurement of the probe output

one can increase the information gained from the performed operation at the expense of increase of the degree of disturbance. For task (i) a single-photon experiment demonstrating state disturbance effect caused by a principal possibility to extract information was demonstrated in [12]. In addition, using two photons, one as an additional probe photon controlling the operation, the MDM for the task (i) has been demonstrated experimentally in [13]. Recently, the MDMs for the task (ii) for the six-state as well as four-state encoding were demonstrated experimentally in [14].

There are two aspects of such linear optical experiments. First, they are only probabilistic, since there is not still available a deterministic two qubit operation with a sufficiently large strength of the coupling. Second, they are performed only with a discrete set of input states as it is unfeasible to measure the fidelity averaging over a continuous set. The last problem was resolved for trace-preserving (deterministic) operations in Ref. [15] where it was shown that the average of the fidelity over the continuous set of all pure qubit states can be calculated by averaging the fidelity over only six or even four pure qubit states symmetrically covering the surface of the Bloch sphere. However, here we consider the linear optical implementation of the MDMs which is trace-decreasing (probabilistic) and therefore we cannot simply resort to this known result.

In this paper we investigate in detail the scheme realizing the minimal disturbance measurement of a polarization state of a photon [14]. The scheme requires only linear optics, single photon ancilla, and an electro-optical feed-forward loop. Since the scheme is conditional we prove explicitly that no probabilistic quantum operation can overcome the proposed scheme. We also derive optimal fidelity tradeoff for the six-state encoding and we show that this tradeoff is optimal even only for the set of four pure states represented on the Bloch sphere by the vertices of a regular tetrahedron. We further derive optimal fidelity tradeoff for the four-state encoding and we show that this tradeoff is optimal also for the set of $N > 2$ pure states uniformly distributed on the equator of the Bloch sphere. In addition, it is demonstrated the scheme [14] to realize the MDM not only for six-state and four-state encodings but also for all other above-mentioned sets of states. Finally, we discuss both the operation controls: preparation of ancillary state or detection of ancillary state.

The paper is structured as follows. Section I contains the derivation of optimal fidelity tradeoffs and the corresponding MDMs for certain discrete sets of pure states uniformly dis-

tributed on the whole Bloch sphere and on the equator of the Bloch sphere. In Sec. II we propose a feasible conditional experimental scheme realizing these MDMs. Sec. III deals with the experimental demonstration of this scheme. Section IV contains conclusions.

I. FIDELITY TRADEOFF FOR DISCRETE SETS OF STATES

We assume the discrete set $M = \{|\phi_i\rangle\}_{i=1}^N$ of N input pure states of a d -level system that form an orbit of a discrete group $\mathcal{G} = \{g_i\}_{i=1}^N$, i.e., $|\phi_i\rangle = U_i|\phi_0\rangle$, where $|\phi_0\rangle$ is a reference state and $U_i \equiv U(g_i)$, $g_i \in \mathcal{G}$ is a unitary representation of the group \mathcal{G} on the input Hilbert space \mathcal{H}_{in} . Further, we assume the states to have equal *a priori* probabilities $p_i = 1/N$. Recently, the optimal tradeoff between the mean estimation fidelity and the mean output fidelity was derived for the continuous sets of states given by all pure states of a d -level system [7], finite ensembles of identical pure qubit states [8], and all pure states of a d -level system produced by d independent phase shifts [9] under the assumption of uniform *a priori* probability distribution. Here we mainly concentrate on discrete sets of pure states of a single qubit ($d=2$) formed by six and four states uniformly distributed on the surface of the Bloch sphere and $N > 2$ states uniformly distributed on the equator of the Bloch sphere. We will also prove that for the sets one cannot improve the optimal fidelity tradeoff using probabilistic operations, as can happen in the case of a general discrete set of the input states. For a probabilistic operation the outcome is accepted only if the operation succeeded and otherwise the result is rejected.

To find optimal fidelity tradeoff for the considered set M of input states we will partially modify the approach developed in the context of continuous sets in [9,16]. Assume that the input state $\rho_i = |\phi_i\rangle\langle\phi_i|$ from the set M enters a general quantum operation having N outcomes. With each outcome k ($k=1, \dots, N$) we can associate a trace decreasing completely positive (CP) map represented by a positive-semidefinite operator χ_k on the tensor product $\mathcal{H}_{\text{in}} \otimes \mathcal{H}_{\text{out}}$ of the input Hilbert space \mathcal{H}_{in} and the output Hilbert space \mathcal{H}_{out} [17]. If the operation gives the outcome k the input state is transformed to $\rho_{k|i} = \text{Tr}_{\text{in}}[\chi_k(\rho_i^T \otimes \mathbb{1}_{\text{out}})]$. The conditional state $\rho_{k|i}$ is normalized such that $\text{Tr}_{\text{out}}(\rho_{k|i}) = P_{k|i}$ is the probability of detecting the outcome k on the state ρ_i . For the input state ρ_i the operation produces on average the output state

$$\rho_{i,\text{out}} = \sum_{k=1}^N \rho_{k|i} = \text{Tr}_{\text{in}} \left[\sum_{k=1}^N \chi_k(\rho_i^T \otimes \mathbb{1}_{\text{out}}) \right]. \quad (1)$$

Since we assume trace decreasing (probabilistic) operation the output state $\rho_{i,\text{out}}$ is unnormalized and its norm $\text{Tr}_{\text{out}}(\rho_{i,\text{out}}) = \sum_{k=1}^N P_{k|i} = P_i$ gives the probability of successful application of the operation to ρ_i . The overall operation is trace decreasing and hence

$$\sum_{k=1}^N \text{Tr}_{\text{out}}(\chi_k) \leq \mathbb{1}_{\text{in}}. \quad (2)$$

Note that the equality sign is achieved if the overall operation is trace preserving (deterministic). The operation also

provides us with classical information on the input state in the form of the outcome k . This information can be converted into the estimate $|\phi_k\rangle$ of the input state. For the input state ρ_i we prepare on average the estimated state of the form

$$\rho_{i,\text{est}} = \sum_{k=1}^N P_{k|i} |\phi_k\rangle\langle\phi_k|. \quad (3)$$

The performance of the considered operation can be quantified by three mean quantities. We define mean probability of success by averaging the probabilities P_i over the *a priori* probability distribution p_i , i.e., $P = (1/N) \sum_{i=1}^N P_i$. The disturbance introduced by the operation into the input state can be quantified by the mean output fidelity

$$F = \frac{1}{NP} \sum_{i=1}^N \langle \phi_i | \rho_{i,\text{out}} | \phi_i \rangle. \quad (4)$$

Similarly, the information gain can be quantified by the mean estimation fidelity

$$G = \frac{1}{NP} \sum_{i=1}^N \langle \phi_i | \rho_{i,\text{est}} | \phi_i \rangle. \quad (5)$$

Since any operation described by the set of CP maps $\{\chi_k\}_{k=1}^N$ can be converted by twirling operation into the covariant operation giving the same mean fidelities F and G as well as the mean probability P [16] we can restrict ourselves without loss of generality to the covariant operations which are described by the *covariant* CP maps. These maps can be generated from a single positive-semidefinite operator χ_0 as follows:

$$\chi_k = (U_k^* \otimes U_k) \chi_0 (U_k^T \otimes U_k^\dagger). \quad (6)$$

For covariant operation the quantities P , F , and G can be expressed using Eqs. (4)–(6) as $P = N \text{Tr}(\chi_0 A)$ and

$$F = \frac{\text{Tr}(\chi_0 R_F)}{\text{Tr}(\chi_0 A)}, \quad G = \frac{\text{Tr}(\chi_0 R_G)}{\text{Tr}(\chi_0 A)}, \quad (7)$$

where

$$A = \frac{1}{N} \sum_{i=1}^N \rho_i^T \otimes \mathbb{1}_{\text{out}},$$

$$R_F = \frac{1}{N} \sum_{i=1}^N \rho_i^T \otimes \rho_i,$$

$$R_G = \frac{1}{N} \sum_{i=1}^N (\rho_i^T \otimes \mathbb{1}_{\text{out}}) \text{Tr}(\rho_i \rho_0). \quad (8)$$

Note that $R_G = \text{Tr}_{\text{out}}[R_F(\mathbb{1}_{\text{in}} \otimes \rho_0)] \otimes \mathbb{1}_{\text{out}}$.

The derivation of the tradeoff between F and G is equivalent to finding the positive-semidefinite operator χ_0 satisfying the constraint (2) that maximizes the convex sum $\Sigma = pF + (1-p)G$, where the parameter $p \in [0, 1]$ controls the ratio between F and G . The sum Σ is upper bounded as [16]

$$\Sigma \leq \lambda_{\max}, \quad (9)$$

where λ_{\max} is the maximum eigenvalue of the matrix $\Lambda = A^{-1/2} \mathcal{R} A^{-1/2}$, where $\mathcal{R} = pR_F + (1-p)R_G$. The operator χ_0 that achieves this bound and satisfies the constraint (2) reads as [16]

$$\chi_0 = e_{\max}^{-1} \tilde{\chi}_0, \quad (10)$$

where $\tilde{\chi}_0 = A^{-1/2} |\lambda_{\max}\rangle \langle \lambda_{\max}| A^{-1/2}$, e_{\max} is the maximum eigenvalue of the matrix

$$\sum_{k=1}^N \text{Tr}_{\text{out}}(\tilde{\chi}_k) = \sum_{k=1}^N U_k^* [\text{Tr}_{\text{out}}(\tilde{\chi}_0)] U_k^T, \quad (11)$$

and $|\lambda_{\max}\rangle$ is the normalized eigenvector of the matrix Λ corresponding to its maximum eigenvalue λ_{\max} . If, in addition, the eigenvalue λ_{\max} is nondegenerate the map (10) is a unique optimal map.

In what follows we will explicitly derive optimal fidelity tradeoffs and the corresponding MDMs for several discrete sets M . The sets of states to be considered here are formed by pure states of a d -level system satisfying the relation

$$\sum_{i=1}^N \rho_i = \frac{N}{d} \mathbb{1}_{\text{in}}, \quad (12)$$

where $d = \dim \mathcal{H}_{\text{in}}$. Consequently,

$$A = \frac{1}{d} \mathbb{1}_{\text{in}} \otimes \mathbb{1}_{\text{out}}, \quad (13)$$

and we get using Eq. (9) the bound

$$\Sigma \leq d r_{\max}, \quad (14)$$

where r_{\max} is the maximum eigenvalue of the matrix \mathcal{R} . Making use of Eq. (10) the optimal map saturating the bound (14) then reads as

$$\chi_0 = e_{\max}^{-1} d |r_{\max}\rangle \langle r_{\max}|, \quad (15)$$

where $|r_{\max}\rangle$ is the normalized eigenvector of \mathcal{R} corresponding to r_{\max} . Note that the upper bound (14) coincides exactly with the upper bound for continuous sets of input states derived in [9]. However, when deriving the bound (14) we considered discrete sets of input states and more importantly we did not restrict ourselves to the deterministic operations as it was done in [9].

We start by derivation of the optimal fidelity tradeoff for the six-state encoding. In this case, the set M is composed of three pairs of qubit basis states

$$\{|H\rangle, |V\rangle\}, \quad |L_{\pm}\rangle = \frac{|H\rangle \pm |V\rangle}{\sqrt{2}}, \quad |C_{\pm}\rangle = \frac{|H\rangle \pm i|V\rangle}{\sqrt{2}}, \quad (16)$$

where $|H\rangle$ and $|V\rangle$ are eigenvectors of the Pauli matrix $\sigma_z = \text{diag}(1, -1)$ corresponding to the eigenvalues $+1$ and -1 , respectively. Since $|\langle \phi_i | \phi_j \rangle| = 1/\sqrt{2}$ for any two states $|\phi_i\rangle$ and $|\phi_j\rangle$ belonging to different pairs, the states (16) form the so-called mutually unbiased bases [2,3]. The states (16) correspond to the vertices of a regular octahedron in the Bloch sphere and can be obtained as an orbit of a rotation group of

a regular octahedron [18,19]. Strictly speaking, the orbit contains each of the states four times each time with an irrelevant phase factor and therefore we can work only with the six states (16) which means that in the above derived formulas we take $N=6$ for the present case and in the sums we sum over the six states (16). As the set (16) satisfies the Eq. (12) the optimal fidelity tradeoff is reached by a quantum operation which is determined by the properly normalized dominant eigenvector of the operator $\mathcal{R}^{\text{oct}} = pR_F^{\text{oct}} + (1-p)R_G^{\text{oct}}$. Taking the reference state to be $|\phi_0\rangle = |H\rangle$ one obtains using Eq. (8) the operators R_F^{oct} and R_G^{oct} in the form

$$R_F^{\text{oct}} = \frac{1}{6} (\mathbb{1}_{\text{in}} \otimes \mathbb{1}_{\text{out}} + 2|\Phi_+\rangle \langle \Phi_+|),$$

$$R_G^{\text{oct}} = \frac{1}{6} (\mathbb{1}_{\text{in}} + |H\rangle \langle H|) \otimes \mathbb{1}_{\text{out}}, \quad (17)$$

where $|\Phi_+\rangle = (1/\sqrt{2})(|HH\rangle + |VV\rangle)$. The maximum eigenvalue of the operator \mathcal{R}^{oct} is nondegenerate and it reads as

$$r_{\max}^{\text{oct}} = \frac{1}{12} (p + 3 + \sqrt{5p^2 - 2p + 1}). \quad (18)$$

The normalized eigenvector corresponding to this eigenvalue is

$$|r_{\max}^{\text{oct}}\rangle = a|HH\rangle + b|VV\rangle, \quad (19)$$

where a, b are non-negative real parameters satisfying $a^2 + b^2 = 1$. Using Eq. (15) and taking into account that $e_{\max}^{\text{oct}} = 6$ one finds the optimal map to be $\chi_0^{\text{oct}} = (1/3) |r_{\max}^{\text{oct}}\rangle \langle r_{\max}^{\text{oct}}|$. Interestingly, calculation of the left-hand side of the constraint (2) for the operator χ_0^{oct} with the help of Eqs. (6) and (12) reveals that the equality sign holds in the constraint. This means that the optimal fidelity tradeoff for the six-state encoding is saturated by the deterministic quantum operation and no probabilistic operation can give a better tradeoff.

The optimal tradeoff between F and G for the six-state encoding can be calculated substituting χ_0^{oct} , and Eqs. (13) and (17) into Eq. (7) which gives

$$F = \frac{2}{3}(1 + ab), \quad G = \frac{1}{3}(1 + a^2). \quad (20)$$

After elimination of the parameters a and b from Eqs. (20) one finally arrives to the optimal fidelity tradeoff for the six-state encoding in the form:

$$\sqrt{F - \frac{1}{3}} = \sqrt{G - \frac{1}{3}} + \sqrt{\frac{2}{3} - G}. \quad (21)$$

The obtained tradeoff coincides with the optimal trade-off for the continuous set of all pure qubit states derived previously in [7].

The tradeoff (21) is optimal even for a smaller set of states. The set in question is formed by four states ($N=4$)

$$|H\rangle, \frac{1}{\sqrt{3}}(|H\rangle + \sqrt{2}|V\rangle), \quad \frac{1}{\sqrt{3}}(|H\rangle + \sqrt{2}e^{i(2/3)\pi}|V\rangle),$$

$$\frac{1}{\sqrt{3}}(|H\rangle + \sqrt{2}e^{-i(2/3)\pi}|V\rangle), \quad (22)$$

which correspond to the vertices of a regular tetrahedron in the Bloch sphere. The states (22) belong to the orbit of a rotation group of a regular tetrahedron [18,19] which contains each of the states three times each time with a different irrelevant phase factor. Similarly as in the previous case also for the states (22) holds Eq. (12). Starting from the reference state $|\phi_0\rangle=|H\rangle$ one finds that $\mathcal{R}_F^{\text{tet}}=\mathcal{R}_F^{\text{oct}}$ whence $\mathcal{R}_G^{\text{tet}}=\mathcal{R}_G^{\text{oct}}$ and thus $\mathcal{R}^{\text{tet}}=\mathcal{R}^{\text{oct}}$. Consequently, the fidelities F and G are given by the formulas (20) and therefore the optimal fidelity tradeoff for the set (22) is again given by Eq. (21). Further, calculating the matrix (11) for the considered set of states (22) one finds that $e_{\text{max}}^{\text{tet}}=4$ and hence one derives using Eq. (15) the optimal map in the form $\chi_0^{\text{tet}}=(1/2)|r_{\text{max}}^{\text{oct}}\rangle\langle r_{\text{max}}^{\text{oct}}|$. Substitution of the map χ_0^{tet} into the constraint (2) finally reveals that the map is deterministic. Thus we found that the optimal fidelity tradeoff for a single completely unknown qubit state (21) can be demonstrated using only four states (22) which do not comprise the complete set of mutually unbiased bases but yet uniformly cover the surface of the Bloch sphere.

In the four-state encoding we work with the last two pairs of states from the set of states (16) ($N=4$). These states correspond to the vertices of a square in the equator of the Bloch sphere and can be generated as an orbit of a rotation group of a square [18,19]. For the reference state $|\phi_0\rangle=|L_+\rangle$ the operators R_F^{sq} and R_G^{sq} read as

$$R_F^{\text{sq}} = \frac{1}{4}(\mathbb{1}_{\text{in}} \otimes \mathbb{1}_{\text{out}} + |VV\rangle\langle HH| + |HH\rangle\langle VV|),$$

$$R_G^{\text{sq}} = \frac{1}{4}\left(\frac{1}{2}\mathbb{1}_{\text{in}} + |L_+\rangle\langle L_+|\right) \otimes \mathbb{1}_{\text{out}}. \quad (23)$$

The operator \mathcal{R}^{sq} has the nondegenerate maximum eigenvalue

$$r_{\text{max}}^{\text{sq}} = \frac{1}{8}(p + 2 + \sqrt{2p^2 - 2p + 1}), \quad (24)$$

and the corresponding eigenvector has then the following structure:

$$|r_{\text{max}}^{\text{sq}}\rangle = a|\Phi_+\rangle + b|\Psi_+\rangle, \quad (25)$$

where a, b are non-negative real parameters satisfying $a^2 + b^2 = 1$ and $|\Psi_+\rangle = (1/\sqrt{2})(|HV\rangle + |VH\rangle)$. Since the maximum eigenvalue of the matrix (11) is in this case $e_{\text{max}}^{\text{sq}}=4$, Eq. (15) gives the optimal map of the form $\chi_0^{\text{sq}}=(1/2)|r_{\text{max}}^{\text{sq}}\rangle\langle r_{\text{max}}^{\text{sq}}|$. Moreover, analogically as in the former cases the map χ_0^{sq} can be shown to be deterministic. From the above it then follows using Eqs. (7), (13), (23), and (25) that the fidelities F and G are

$$F = \frac{1}{2}(1 + a^2), \quad G = \frac{1}{2}(1 + ab). \quad (26)$$

Eliminating the parameters a, b one can finally derive the optimal relation between F and G

$$\sqrt{4G - 1} = \sqrt{2(1 - F)} + \sqrt{2F - 1}, \quad (27)$$

which is the same as for the continuous set of all pure states of an equatorial qubit [9].

In fact, the tradeoff (27) is optimal even for the whole class of discrete sets of equatorial states. The sets in question are composed of $N > 2$ pure qubit states distributed uniformly on the equator of the Bloch sphere and having uniform *a priori* distribution, i.e., the states of the form:

$$\frac{1}{\sqrt{2}}(|H\rangle + e^{i(2\pi/N)k}|V\rangle), \quad k = 0, 1, \dots, N-1 \quad (28)$$

and $p_k = 1/N$ for all k . This set of states can be generated as an orbit of a rotation group of a regular N -sided polygon in two dimensions [18,19]. As Eq. (12) is satisfied also for the states (28) as follows from the formula $\sum_{k=0}^{N-1} e^{i2\pi k/N} = 0$ valid for $N > 1$ the optimal map is given by Eq. (15). Starting from the reference state $|\phi_0\rangle=|L_+\rangle$ one finds the matrix $\mathcal{R}_F^{(N)}$ for the set (28) to be $\mathcal{R}_F^{(N)}=\mathcal{R}_F^{\text{sq}}$ which implies $\mathcal{R}_G^{(N)}=\mathcal{R}_G^{\text{sq}}$ and therefore $\mathcal{R}^{(N)}=\mathcal{R}^{\text{sq}}$. Hence the normalized eigenvector of the matrix $\mathcal{R}^{(N)}$ is given by Eq. (25). Taking into account the fact that the matrix (11) is equal to $N\mathbb{1}_{\text{in}}$ we have $e_{\text{max}}^{(N)}=N$ and the optimal map $\chi_0^{(N)}=(2/N)|r_{\text{max}}^{\text{sq}}\rangle\langle r_{\text{max}}^{\text{sq}}|$ is deterministic. The obtained result reveals that the tradeoff (27) is optimal also for N qubit states uniformly distributed on the equator of the Bloch sphere with uniform *a priori* distribution. This result shows in particular that the tradeoff (27) can be demonstrated in a most simple way using only the so-called trine states [20], i.e., the set of states (28) with $N=3$. In what follows we propose a single scheme realizing MDM for all the above-mentioned sets of states and we demonstrate it experimentally for six-state and four-state encodings.

II. EXPERIMENTAL SCHEME

The scheme of the MDM is depicted in Fig. 1. It is optimal both for a previously discussed discrete set of qubit states as well as for the continuous sets of qubit states discussed in [7,9]. The scheme is reminiscent of the recent experiment on quantum parity check [21]. But there is an interesting difference in the preparation of the probe state or probe measurement that opens a way to build quantum operation with minimal disturbance.

First, we will discuss the operation controlled (“programmed”) by the state of the ancilla A . We assume input photon S has been prepared in an unknown polarization state $|\phi\rangle = \alpha|H\rangle + \beta|V\rangle$ chosen randomly with a uniform distribution from some set of pure states of a single qubit. At a polarization beam splitter PBS this photon is mixed with the ancillary photon A which is randomly prepared (in a preparation device P) in one of the following nonorthogonal states:

$$p_h = \frac{1}{2}: \quad |h\rangle = \cos \theta|H\rangle - \sin \theta|V\rangle \cdots H \text{ is detected,}$$

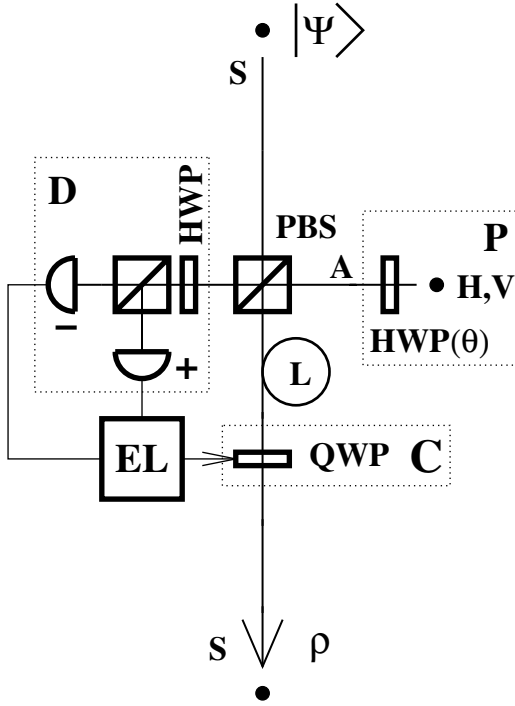


FIG. 1. Experimental setup for optimal conditional operation with a minimal disturbance: PBS—polarizing beam splitter, HWP—half-wave plate, EL—electronical logic, and L—delay fiber loop.

$$p_v = \frac{1}{2}: \quad |v\rangle = \sin \theta |H\rangle - \cos \theta |V\rangle \cdots V \text{ is detected,} \quad (29)$$

where θ is the angle of the rotation of the half-wave plate (HWP). This ancillary photon A probes the state $|\phi\rangle$ and the operation is successful if both the photons leave PBS separately, one to the detection device D and the second as the output of the operation. If the operation was successful for the ancillary state $|h\rangle$ ($|v\rangle$) then the polarization H (V) has been measured on the input state. Assuming the detection D measures the basis $|L_{\pm}\rangle$ this will occur with probabilities

$$p_H = |\alpha|^2 \cos^2 \theta + |\beta|^2 \sin^2 \theta, \quad (30)$$

$$p_V = |\alpha|^2 \sin^2 \theta + |\beta|^2 \cos^2 \theta,$$

where $p_H + p_V = 1$ and the total probability of success of this procedure is $1/2$. According to the result \mp of the detection device D the following un-normalized states are prepared at the output

$$|H, \mp\rangle = \alpha \cos \theta |H\rangle \pm \beta \sin \theta |V\rangle,$$

$$|V, \mp\rangle = \alpha \sin \theta |H\rangle \pm \beta \cos \theta |V\rangle. \quad (31)$$

Thus performing unitary correction $|H\rangle \rightarrow |H\rangle$ and $|V\rangle \rightarrow -|V\rangle$ in the case when the result $+$ is obtained the same states are at the output independently on the result \pm . At the output of the operation we have on average the state

$$\rho_S = |\alpha|^2 |H\rangle\langle H| + |\beta|^2 |V\rangle\langle V| + \sin(2\theta)(\alpha\beta^* |H\rangle\langle V| + \text{H.c.}) \quad (32)$$

with the state-dependent output fidelity

$$f(|\phi\rangle) = 1 - 2|\alpha|^2 |\beta|^2 [1 - \sin(2\theta)]. \quad (33)$$

According to the results of the successful state probing, one prepares on average the estimated state

$$\rho_E = p_H |H\rangle\langle H| + p_V |V\rangle\langle V| \quad (34)$$

having the state-dependent estimation fidelity

$$g(|\phi\rangle) = \cos^2 \theta - 2|\alpha|^2 |\beta|^2 \cos(2\theta). \quad (35)$$

For the six-state encoding discussed in the first part of this paper, according to Eqs. (33) and (35) the output and estimation fidelities in the correct basis are $f=1$ and $g=\cos^2 \theta$. In the rest of the complementary bases, they are $f'=1-(1/2)[1-\sin(2\theta)]$ and $g'=\cos^2 \theta - (1/2)\cos(2\theta)$. Calculating mean output and estimation fidelities

$$F = \frac{1}{6}(2f + 4f'), \quad G = \frac{1}{6}(2g + 4g') \quad (36)$$

we obtain

$$F = \frac{2 + \sin(2\theta)}{3}, \quad G = \frac{3 + \cos(2\theta)}{6}, \quad (37)$$

which saturate the tradeoff (21). In the first part of this paper we proved that this tradeoff is optimal for the considered set of input states and it cannot be overcome using any other probabilistic quantum operation. Therefore our conditional operation is sufficient for a fair demonstration of the MDM for the six-state encoding.

The proposed scheme also realizes the MDM for the set of states (22). This follows from the fact that in this case Eqs. (33) and (35) give for the reference state $|H\rangle$ the fidelities $f=1$ and $g=\cos^2 \theta$ while for the rest of these states they give $f'=1-(4/9)[1-\sin(2\theta)]$ and $g'=\cos^2 \theta - (4/9)\cos(2\theta)$. Substitution of these fidelities into the formulas $F=(1/4)(f+3f')$ and $G=(1/4)(g+3g')$ for mean output and estimation fidelities, respectively, finally leads to F and G equal to those in Eq. (37).

It is worth noting that for the continuous set of all pure qubit states with uniform *a priori* distribution, which was discussed in [7], averaging of fidelities (33) and (35) over all possible input states also gives mean output and estimation fidelities (37) which satisfy Banaszek's tradeoff for a single qubit [7] given by Eq. (21).

The proposed scheme can be also used for the MDM for the so-called equatorial qubits, i.e., pure qubit states lying on the equator of the Bloch sphere. They can be, for example, of the form

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|L_+\rangle + e^{i\psi}|L_-\rangle). \quad (38)$$

For these states we have

$$|\alpha|^2 = \frac{1}{4}|1 + e^{i\psi}|^2, \quad |\beta|^2 = \frac{1}{4}|1 - e^{i\psi}|^2. \quad (39)$$

First, let us consider the four-state encoding with the alphabet of states $|V\rangle$, $|H\rangle$, $|L_+\rangle$, and $|L_-\rangle$. If the measurement is performed in the correct basis Eqs. (33) and (35) yield $f=1$ and $g=\cos^2\theta$ while in the complementary basis they give $f'=1-(1/2)[1-\sin(2\theta)]$ and $g'=\cos^2\theta-(1/2)\cos(2\theta)$. Calculating mean output and estimation fidelities

$$F = \frac{1}{4}(2f + 2f'), \quad G = \frac{1}{4}(2g + 2g') \quad (40)$$

one obtains

$$F = \frac{3 + \sin(2\theta)}{4}, \quad G = \frac{2 + \cos(2\theta)}{4}, \quad (41)$$

which satisfy the relation (27).

In the case of $N > 2$ equatorial states of the form

$$|\phi_k\rangle = \frac{1}{\sqrt{2}}(|L_+\rangle + e^{i(2\pi/N)k}|L_-\rangle), \quad k = 0, 1, \dots, N-1, \quad (42)$$

we obtain using Eqs. (33), (35), and (39)

$$f(|\phi_k\rangle) = 1 - \frac{1}{4} \left[1 - \cos\left(\frac{4\pi}{N}k\right) \right] [1 - \sin(2\theta)],$$

$$g(|\phi_k\rangle) = \cos^2\theta - \frac{1}{4} \left[1 - \cos\left(\frac{4\pi}{N}k\right) \right] \cos(2\theta). \quad (43)$$

Hence calculating the mean fidelities F and G using the formulas $F = (1/N)\sum_{k=0}^{N-1} f(|\phi_k\rangle)$ and $G = (1/N)\sum_{k=0}^{N-1} g(|\phi_k\rangle)$ we arrive at the same F and G as in Eq. (41). Therefore the scheme in Fig. 1 realizes MDM also for the states (42).

For the continuous set of all pure equatorial states substitution to Eqs. (33) and (35) and integration over the parameter ψ gives the same mean fidelities as in Eq. (41) that saturate the optimal fidelity tradeoff for the equatorial qubits (27) derived in [9].

There is an alternative possibility how to control the ratio between the output and the estimation fidelities in which the state of ancilla is fixed while the measurement on the ancilla is continuously varied. The setup is the same as in the previous case but now we prepare the ancilla in the fixed input state $|L_+\rangle$. After mixing it with the photon S in PBS, both photons are in the entangled state

$$\alpha|HH\rangle + \beta|VV\rangle \quad (44)$$

if the photons leave the PBS separately. Then it is sufficient to implement the projective measurement on the ancilla consisting of projectors $|\tilde{v}\rangle\langle\tilde{v}|$ and $|\tilde{h}\rangle\langle\tilde{h}|$, where

$$|\tilde{h}\rangle = \cos\theta|H\rangle - \sin\theta|V\rangle \cdots H \text{ is detected,}$$

$$|\tilde{v}\rangle = \cos\theta|V\rangle + \sin\theta|H\rangle \cdots V \text{ is detected,} \quad (45)$$

and if we detect state $|\tilde{h}\rangle$ we consequently perform the transformation $|H\rangle \rightarrow |H\rangle$ and $|V\rangle \rightarrow -|V\rangle$ on the signal photon

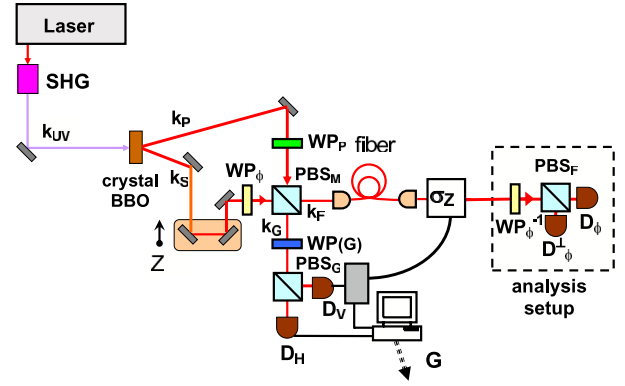


FIG. 2. (Color online) Optical setup implementing the MDM. The output qubit is characterized adopting the analysis setup illustrated in the dashed box.

state. Since the same detection probabilities (30) as well as the same output state (32) are reproduced we get the same fidelities as in Eqs. (33) and (35). Consequently, the measurement strategy also saturates the fidelity tradeoffs (21) and (27) for the above-mentioned discrete and continuous sets of input states. Here, rather than programming the device by a state of ancillary photon, the control is performed by optimal erasing of information extracted by the coupling with the ancillary photon in a fixed state. This method is used in the experiment to test the tradeoffs for the six-state and four-state encodings.

III. EXPERIMENT

The present section reports the experimental realization of a MDM device based on the second approach presented above. In the present experiment two photons with equal wavelength (WL) $\lambda=795$ nm were generated in the initial polarization product state $|H\rangle_S|H\rangle_P$ on the modes k_S and k_P by spontaneous parametric down conversion (SPDC) in a type I BBO crystal [22] (see Fig. 2). The main source of the experimental apparatus was a Ti:Sa mode-locked pulsed laser (Coherent: MIRA) with WL λ and repetition rate 76 MHz providing by second-harmonic generation (SHG) the UV pump field (WL: $\lambda_{UV}=397.5$ nm) for the SPDC process associated with the spatial mode k_{UV} . The input qubit was codified into the polarization state $|\phi\rangle_S = \alpha|H\rangle_S + \beta|V\rangle_S$ of the single photon belonging on the mode k_S by means of a half and a quarter wave plates (WP_ϕ), whereas the ancillary qubit was polarization encoded in the state $|L_+\rangle_P$ of the single photon over the mode k_P adopting the half-wave plate WP_P . The “parity check” operation is then applied to the input and probe qubits by letting them interfere with the respective single photons wave packets at the polarizing beam splitter PBS_M layer. This process is accomplished by injecting the photons S and P on the two input modes of PBS_M with an adjustable mutual temporal delay $\Delta t = 2Z/c$, with Z being the position of an optical trombone. The condition $\Delta t=0$, corresponding to the maximal interference, has been experimentally identified by verifying the entangling feature of the “parity check” device when excited by the overall input state $(1/2)|L_+\rangle_S|L_+\rangle_P$ and postselecting only the events in which a

TABLE I. Experimental data of the quantum fidelity $F(\theta)$ for different input qubits and different angular positions of wave plate WP_G .

$\vartheta = \theta/2$	$ H\rangle$	$ V\rangle$	$ L_+\rangle$	$ L_-\rangle$	$ C_+\rangle$	$ C_-\rangle$	F_{univ}	F_{cov}
22.5°	0.976	0.991	0.919	0.893	0.920	0.875	0.929	0.945
20°	0.965	0.983	0.912	0.866	0.906	0.826	0.909	0.931
17°	0.985	0.990	0.888	0.817	0.907	0.779	0.894	0.920
14°	0.990	0.980	0.856	0.765	0.865	0.712	0.861	0.898
11°	0.982	0.974	0.816	0.706	0.825	0.660	0.827	0.870
8°	0.987	0.992	0.735	0.600	0.753	0.565	0.772	0.828
5°	0.982	0.967	0.648	0.551	0.710	0.487	0.724	0.787
2°	0.986	0.980	0.600	0.473	0.630	0.387	0.676	0.760
0°	0.988	0.973	0.565	0.415	0.598	0.385	0.654	0.735

single photon emerges in each one of the output modes k_F and k_G . For $\Delta t \gg \tau$, τ being the coherence time of the biphoton wave packet, the overall output state is an incoherent superposition of the two states $|HH\rangle_{FG}$ and $|VV\rangle_{FG}$: $\rho_{FG}(\Delta t \gg \tau) = (|HH\rangle_{FG}\langle HH| + |VV\rangle_{FG}\langle VV|)/2$, whereas for $\Delta t = 0$ the entangled output state $\rho_{FG}(\Delta t = 0) = |\Phi_{\pm}\rangle_{FG}\langle\Phi_{\pm}|$ is obtained. By switching on the interference, that is by varying Z from the condition $\Delta t \gg \tau$ to $\Delta t = 0$, an enhancement of a factor $R=2$ of the $|L_+\rangle_F|L_+\rangle_G$ component of the overall output state is expected. An experimental enhancement $R=1.90 \pm 0.01$ has been observed. After the implementation of the ‘‘parity check’’ operation, the mode k_F corresponds to the output quantum channel of the MDM device, while the photon belonging on mode k_G enters the classical measurement apparatus adopted to infer the classical guess G . This estimation task is realized by means of a tunable half-wave plate $WP(G)$, a polarizing beam splitter PBS_G , and two detectors D_H, D_V . All adopted photodetectors (D) were equal SPCM-AQR14 Si-avalanche nonlinear single photon units. One interference filter with bandwidth $\Delta\lambda = 3$ nm was placed in front of each detector D . The angular position of $WP(G)$, $\vartheta_G = \theta/2$, determines the strength of the measurement. The complete protocol implies a classical feed-forward on the polarization state of the photon belonging to the mode k_S depending on which detector of the guessing apparatus is fired: precisely if the detector D_V clicks, a σ_Z Pauli operation is applied on the qubit belonging on the mode k_F , in the other case no transformation is implemented on the quantum chan-

nel. To carry out the σ_Z transformation we adopted a fast LiNbO₃ Pockels cell (PC) electronically driven by a transistor array activated by a click of detector D_V . The problem of realizing a fast electronic circuit transforming the output signal of a single photon detector (TTL signal) into a calibrated fast pulse in the kV range was solved by a single chain of fast avalanche transistors (Zetex ZXT413 [23]). The σ_Z transformation was then achieved by applying to the PC a $\lambda/2$ voltage, i.e., leading to a $\lambda/2$ induced phase shift of the $|V\rangle$ polarization component at the end of the propagation inside the LiNbO₃ crystal. In order to synchronize the operating time window of the Pockels cell with the output qubit, the photon over the mode k_F was delayed through propagation over a 30 m long single mode optical fiber. This assures a flying time of ≈ 150 ns long enough to allow the activation of the PC electronically driven circuit. Since once triggered, the PC remains excited for a few microseconds, the counting rates of D_V and D_H were kept lower than 15 000 counts/s in order to prevent unwanted σ_Z operations. The fixed polarization transformation induced by the propagation inside the fiber was counterbalanced by a Babinet compensator and a $\lambda/2$ wave plate. The polarization state on the mode k_F after the propagation through the system fiber+PC was analyzed by the combination of the wave plate WP_{ϕ}^{-1} and of the polarization beam splitter PBS_F . For each input polarization state $|\phi\rangle_S$, WP_{ϕ}^{-1} was set in order to make PBS_F transmit $|\phi\rangle$ and reflect $|\phi^{\perp}\rangle$.

The device has been characterized either for a universal set or for a covariant set of input qubits. To demonstrate the

TABLE II. Experimental data of the classical guess $G(\theta)$ for different input qubits and different angular positions of wave plate WP_G .

$\vartheta = \theta/2$	$ H\rangle$	$ V\rangle$	$ L_+\rangle$	$ L_-\rangle$	$ C_+\rangle$	$ C_-\rangle$	G_{univ}	G_{cov}
22.5°	0.533	0.510	0.500	0.500	0.500	0.500	0.507	0.511
20°	0.637	0.626	0.500	0.500	0.500	0.500	0.544	0.566
17°	0.768	0.732	0.500	0.500	0.500	0.500	0.583	0.625
14°	0.839	0.802	0.500	0.500	0.500	0.500	0.607	0.660
11°	0.891	0.900	0.500	0.500	0.500	0.500	0.632	0.698
8°	0.956	0.951	0.500	0.500	0.500	0.500	0.651	0.727
5°	0.985	1.000	0.500	0.500	0.500	0.500	0.664	0.746
2°	1.000	1.000	0.500	0.500	0.500	0.500	0.666	0.750
0°	1.000	1.000	0.500	0.500	0.500	0.500	0.666	0.750

realization of the MDM apparatus it is sufficient to use a finite set of nonorthogonal quantum states from mutually unbiased bases, as shown in Sec. I. For the universal MDM, we have adopted the three mutually unbiased bases $|H\rangle$, $|V\rangle$, $|L_{\pm}\rangle$, and $|C_{\pm}\rangle$ whereas for the phase covariant MDM we employed the $|H\rangle$, $|V\rangle$, and $|L_{\pm}\rangle$ bases only. Such sets of states are adopted in the conventional quantum cryptographic protocols [4,5]. For each state $|\phi\rangle_S$, the corresponding values of F_{ϕ} and G_{ϕ} were measured for different ϑ_G settings. This task was achieved by collecting the two-fold coincidences between the two sets of detectors $\{D_H, D_V\}$ and $\{D_{\phi}, D_{\phi}^{\perp}\}$ and then extracting the joint probabilities of the two-photon states $p_{H\phi}$, $p_{V\phi}$, $p_{H\phi^{\perp}}$, and $p_{V\phi^{\perp}}$ where p_{ij} is the relative frequency of the coincidence count $D_i - D_j$. The fidelity of the output state ρ_{out} can be evaluated as $F_{\phi} = \langle \phi | \rho_{out} | \phi \rangle = p_{H\phi} + p_{V\phi}$. To extract the value G_{ϕ} , we first calculate the occurrence probability P_i $\{i=H, V\}$ of the measurement $|i\rangle\langle i|$, as $P_i = p_{i\phi} + p_{i\phi^{\perp}}$. In this case the input state is guessed to be in the quantum state $|i\rangle$ leading to a fidelity $|\langle \phi | i \rangle|^2$. Hence for each state $|\phi\rangle$ the resulting estimation fidelity is obtained as $G_{\phi} = \sum_i P_i |\langle \phi | i \rangle|^2$. This implies that for the states $|L_{\pm}\rangle$ and $|C_{\pm}\rangle$ and more generally for all the states $|\Gamma\rangle = (1/\sqrt{2})(|H\rangle + e^{i\varphi}|V\rangle)$ equally spaced with respect to $|H\rangle$ and $|V\rangle$, $G(\theta)$ is constant and equal to $\frac{1}{2}$. The experimental data for different input states are reported in Tables I and II. The mean quantum fidelities and classical guesses were averaged over all the input states. The measurement of each experimental point lasted 60 s.

For the universal MDM the extreme experimental points are $(G_{univ}^{expt} = 0.666 \pm 0.001; F_{univ}^{expt} = 0.654 \pm 0.004)$ and $(0.507 \pm 0.004; 0.929 \pm 0.002)$, corresponding to the settings $\vartheta_G = 0^\circ$ and $\vartheta_G = 22.5^\circ$ (see Fig. 3). These figures are to be compared with the theoretical limits: $(G_{univ}^{th} = 0.666; F_{univ}^{th} = 0.666)$ and $(0.5; 1)$. Likewise, for the phase covariant MDM the extremal experimental points are $(G_{cov}^{expt} = 0.750 \pm 0.001; F_{cov}^{expt} = 0.735 \pm 0.004)$ and $(0.511 \pm 0.006; 0.945 \pm 0.003)$ to be compared with the theoretical: $(G_{univ}^{th} = 0.75; F_{univ}^{th} = 0.75)$ and $(G_{univ}^{th} = 0.5; F_{univ}^{th} = 1)$. The discrepancies between the theoretical and experimental curves are mainly due to not perfect interference visibility at the PBS, which partially spoil the ‘‘parity check’’ operation. The deviation equal to $\sim 7\%$ between the theoretical value $F_{univ}^{th} = 1$ and the experimental one 0.93 can be attributed to the PBS (3% due to a nonvanishing reflectivity for the H polarization), decoherence in optical fiber propagation and classical feed-forward (2%), and spatial matching of the overlapping modes (2%). A simple analysis leads to the consideration that the value of $(F^{th} - F^{expt})$ decreases for lower value of F^{th} .

IV. CONCLUSIONS

In summary, we proposed and experimentally demonstrated a conditional scheme for the minimal disturbance measurement for six pure qubit states uniformly distributed on the Bloch sphere and for four pure qubit states uniformly distributed on the equator of the Bloch sphere. The scheme utilizes only two photons, linear optical elements and electro-optical feed-forward control. It has been also shown the scheme to realize the minimal disturbance measurement

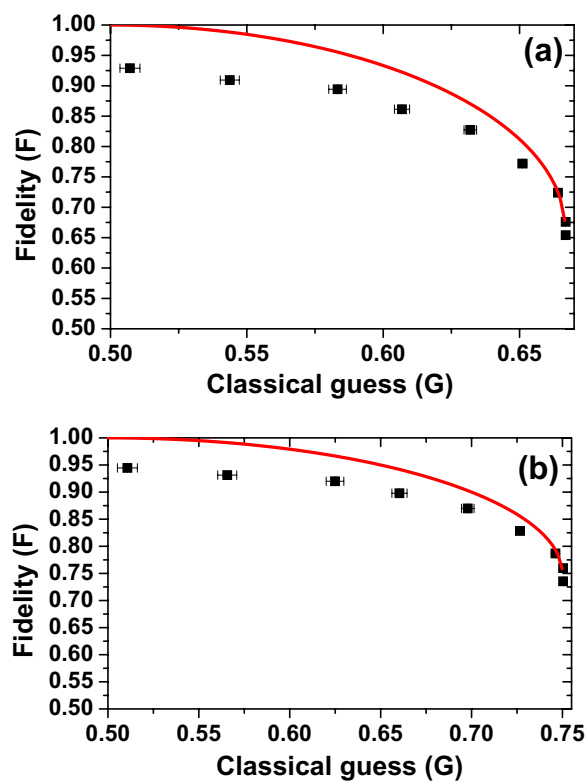


FIG. 3. (Color online) (a) Experimental data of the quantum fidelity F vs the classical guess G for an arbitrary input qubit. The fidelities have been averaged over the six states $\{|H\rangle, |V\rangle, |L_{\pm}\rangle, |C_{\pm}\rangle\}$; solid line: optimal tradeoff between F_{univ} and G_{univ} given by Eq. (21). (b) Experimental data of the quantum fidelity F vs the classical guess G for an equatorial input qubit. The fidelities have been averaged over the four states $\{|H\rangle, |V\rangle, |L_{\pm}\rangle\}$; solid line: optimal tradeoff between F_{cov} and G_{cov} given by Eq. (27).

for four pure qubit states represented by the vertices of a regular tetrahedron in the Bloch sphere as well as for $N > 2$ pure qubit states uniformly distributed on the equator of the Bloch sphere. Further, it has been proved that for the sets of states the fidelity tradeoff cannot be improved using any other probabilistic operation. The optimal interplay between mean output and estimation fidelities can be controlled by alternating nonorthogonal states of ancilla or by changing the measurement on ancilla. An experiment realizing the MDM device both for universal and phase-covariant qubits has been carefully described.

ACKNOWLEDGMENTS

We thank J. Fiurášek for fruitful discussions. The research has been supported by Research project ‘‘Measurement and Information in Optics’’ (MSM 6198959213) and Centre of Modern Optics (LC06007) of Czech Ministry of Education, project OCP11.003 in framework of the EU grant COST P11, and by the EU under project SECOQC (IST-2002-506813). R. F. thanks the support by Project 202/03/D239 of the Grant Agency of Czech Republic. F. D. M., M. R., and F. S. acknowledge financial support from MIUR (PRIN 2005).

- [1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Rev. Mod. Phys.* **74**, 145 (2002).
- [2] I. D. Ivanovic, *J. Phys. A* **14**, 3241 (1981).
- [3] W. K. Wootters and B. D. Fields, *Ann. Phys. (N.Y.)* **191**, 363 (1989).
- [4] D. Bruss, *Phys. Rev. Lett.* **81**, 3018 (1998).
- [5] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.
- [6] B.-G. Englert, *Phys. Rev. Lett.* **77**, 2154 (1996).
- [7] K. Banaszek, *Phys. Rev. Lett.* **86**, 1366 (2001).
- [8] K. Banaszek and I. Devetak, *Phys. Rev. A* **64**, 052307 (2001).
- [9] L. Mišta, J. Fiurášek, and R. Filip, *Phys. Rev. A* **72**, 012311 (2005).
- [10] M. Ricci, F. Sciarrino, N. J. Cerf, R. Filip, J. Fiurášek, and F. De Martini, *Phys. Rev. Lett.* **95**, 090504 (2005).
- [11] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000), p. 91.
- [12] P. D. D. Schwindt, P. G. Kwiat, and B.-G. Englert, *Phys. Rev. A* **60**, 4285 (1999).
- [13] G. J. Pryde, J. L. O'Brien, A. G. White, S. D. Bartlett, and T. C. Ralph, *Phys. Rev. Lett.* **92**, 190402 (2004).
- [14] F. Sciarrino, M. Ricci, F. De Martini, R. Filip, and L. Mišta, Jr., *Phys. Rev. Lett.* **96**, 020408 (2006).
- [15] M. D. Bowdrey, D. K. L. Oi, A. J. Short, K. Banaszek, and J. A. Jones, *Phys. Lett. A* **294**, 258 (2002); M. A. Nielsen, *ibid.* **303**, 249 (2002); E. Bagan, M. Baig, and R. Muñoz-Tapia, *Phys. Rev. A* **67**, 014303 (2003); K. Zyczkowski and H.-J. Sommers, *ibid.* **71**, 032313 (2005).
- [16] J. Fiurášek, *Phys. Rev. A* **70**, 032308 (2004).
- [17] A. Jamiolkowski, *Rep. Math. Phys.* **3**, 275 (1972); M.-D. Choi, *Linear Algebr. Appl.* **10**, 285 (1975).
- [18] M. Hamermesh, *Group Theory and Its Application to Physical Problems* (Addison-Wesley, Reading, London, 1964).
- [19] T. Decker, D. Janzing, and T. Beth, *Int. J. Quantum Inf.* **2**, 353 (2004).
- [20] A. Peres and W. K. Wootters, *Phys. Rev. Lett.* **66**, 1119 (1991).
- [21] T. B. Pittman, B. C. Jacobs, and J. D. Franson, *Phys. Rev. A* **66**, 052305 (2002).
- [22] F. De Martini and F. Sciarrino, *Prog. Quantum Electron.* **29**, 165 (2005).
- [23] S. Giacomini, F. Sciarrino, E. Lombardi, and F. De Martini, *Phys. Rev. A* **66**, 030302(R) (2002).