Information-disturbance tradeoff in sending Direction information via antiparallel quantum spin

ShengLi Zhang¹, XuBo Zou¹, ChuanFeng Li¹, ChenHui Jin² and GuangCan Guo¹
1 Key Laboratory of Quantum Information, University of Science and Technology of China (CAS), Hefei 230026, China.
2 Electronic Technology Institute; Information Engineering University; Zhengzhou; Henan 450004; China

(Dated: July 1, 2011)

For sending unknown direction information, antiparallel spins contains more direction information than parallel spins (Gisin and Popescu, 1999, Phys. Rev. Lett. 83, 432). In this paper, the optimal information-disturbance tradeoff bound for antiparallel spins is derived. The quantum measurements which attain the optimal tradeoff bound are obtained. This result can be of practical relevance for posing some general limits on Eve’s eavesdropping process. Finally, we also present a comparison between the bound for antiparallel spins and the bound for parallel spins.

PACS numbers: 03.67.-a, 03.65.Bz

I. INTRODUCTION

With a preestablished reference frame between two remote users, Alice and Bob, the information of an arbitrary spatial direction \( \vec{n} \) can be conveniently encoded into a series of classical bits which allow them to exchange via quantum or classical channels. However, there are many cases when such a reference frame is not available and all what one can do is to send a natural object, such as gyroscope pointing in a direction, to share and align their reference frames [1]. Quantum spins-1/2 systems, polarized along a direction, to share and align their reference frames [1]. Quantum spins-1/2 systems, polarized along a direction, to share and align their reference frames [1]. The measurement result ±\( m \) provides a fidelity of 2/3 which is the maximal accuracy with which Bob can achieve from the quantum measurement. In Ref. [10], Gisin and Popescu considered this transmission problem using two spins and discovered a surprising effect which is now often coined as “Nolocal without entanglement”. In more details, to transmit the direction \( \vec{n} \) using two spins, there may be two possible strategies. The first one is to encode \( \vec{n} \) in parallel spins \(|\vec{m}\rangle|\vec{m}\rangle\), while the second one is quite similar to the first, except to polarize the second spin in the opposite direction, \(|\vec{m}, -\vec{m}\rangle\) (antiparallel). Although in both cases the two spins are unentangled, it is shown that antiparallel quantum spin provides a definite improvement in the precision and efficiency in the transmission of frame information. Recently, the best strategy for efficient use of \( N \) quantum spins to align the reference frame have also been addressed [11].

All these studies of reference frame transmission is centered around the improvement of the efficiency or the fidelity in our communication. In the real world, particularly in the presence of potential eavesdroppers (Eve), it is also of great importance to keep the security of the shared frame. In Ref. [12], two quantum-cryptographic protocols — BB84-type protocol and Ekert-type protocol have been proposed for secretly communicating a reference frame. However, up till now, a quantitative derivation of the security level (Bell inequalities) above which the BB84-type (Ekert-type) protocol is no longer secure has not been explicitly derived. In this paper, as a first step towards such a goal, we take the antiparallel quantum spins which provides the maximal transmission fidelity for two-qubit encoding as an example and consider the corresponding security bound.

Unintuitively, however, as we will show here, the antiparallel spins may not be the optimal protocol for transmitting the direction information, at least from the aspect of security. Although antiparallel spins provides Alice a convenient tool for improving her fidelity for frame transmission, they improve the fidelity for Eve, too. This allows Eve more freedom to eavesdrop. Thus, a more theoretical and information theory-based analysis is required.

Our result is obtained by a careful derivation of the information disturbance tradeoff problem. In fact, the laws of quantum mechanics imposes a natural restriction on the information processing with the unknown quantum state. There is not a quantum measurement on the quantum system without introducing any disturbance. The more information one gains, the more the quantum state has to be disturbed. There exists a precise tradeoff between the information gain and state disturbance. More importantly, the tradeoff which is inherited by quantum mechanics is applicable to any measurement observer, including Bob and eavesdropper, and imposes a general limit on the information eavesdropping in quantum communications [13–20].

In the following (Sec.III), we will give a detailed description of the information-disturbance model for the security analysis of communication protocol with antiparallel spins. In Sec.III, we derive the optimal tradeoff bound by using group covariant and vector analysis technique. Finally, an exemplary operation satisfying the tradeoff
control of the environmental noise and all the decoherence is assumed to be due to eavesdropping. In Fig. (b), we give a mathematical model for Eve’s eavesdropping process. Without loss of generality, we here suppose Eve performs a POVM measurement to carry out his eavesdropping. This is the most general measurement in quantum mechanics and can be described with a collection of completely positive (CP) maps \( \{ \mathcal{E}_r \} \), where \( r \) denotes the possible measurement results[21, 22]. Moreover, choices of different map \( \mathcal{E}_r \) or of different number of distinct measurement results will constitute different kinds of POVM measurement on condition that the map \( \sum_r \mathcal{E}_r \) satisfies the trace-preserving condition. Namely, there may be infinite many strategies for Eve to choose to maximize his eavesdropping information. In the literature, many different definitions such as Shannon entropy[16], discrimination probability[17] and the quantum fidelity[13,20] have been used to quantify the amount of Eve’s information. For ease, throughout the paper, we will use the fidelity between the state \(|\psi_r\rangle\) (Eve guessed from his measurement result \( r \)) and original state \(|\psi(g)\rangle\) as a figure of merit for Eve’s information \( I \). After the measurement, the state will be extensively disturbed. The disturbed version, say \( \mathcal{E}(\tilde{\rho}(g)) \), will be transmitted to Bob for subsequent processing. The amount of the disturbance \( D \), characterized by the resemblance between the single qubit state and original state \(|\psi(g)\rangle\), i.e., \( \text{Tr} [\mathcal{E}(\tilde{\rho}(g))|\psi(g)\rangle\langle\psi(g)| \otimes I] \), is what we mainly considered. Here, \( I \) denotes the Identity in single-qubit Hilbert Space. In the following, we will search for all kinds of POVM measurements and derive the optimal Information-Disturbance tradeoff.

To give a precise meaning to our problem, we need to investigate some properties of quantum measurement. According to Kraus’ theory[22], each map \( \mathcal{E}_r \) can be written in the form of operator decomposition \( \mathcal{E}_r(\tilde{\rho}(g)) = \sum_r A_{r\mu} \tilde{\rho}(g) A_{r\mu}^\dagger \), and will provide the state \( \rho_r = \sum_r A_{r\mu} \tilde{\rho}(g) A_{r\mu}^\dagger / p_r |g\rangle \langle g| \) (normalized) after the result \( r \) is observed, where, \( p_r |g\rangle = \sum_r A_{r\mu}^\dagger A_{r\mu} |g\rangle \) is the conditional probability of outcome \( r \) occurring given that state \( \tilde{\rho}(g) \) is being input. The trace-Preserving condition for maps \( \mathcal{E}_r \) further requires \( \sum_{r\mu} A_{r\mu}^\dagger A_{r\mu} = I \otimes I \). For a completely unknown direction \( \vec{n} \), one can assume the corresponding group parameter \( g \) is chosen randomly with the uniform probability distribution. Thus, by averaging over all the possible measuring outcome \( r \) and pure state \(|\psi(g)\rangle\), one can identify the average information and average disturbance for the POVM \( \{A_{r\mu}\} \) as follows:

\[
\begin{align*}
I &= \int_G dg \sum_r p_r |g\rangle \langle \psi_r | \psi_g \rangle |^2 \\
&= \int_G dg \sum_{r\mu} \text{Tr}[A_{r\mu}^\dagger A_{r\mu} \tilde{\rho}(g)] |\psi_r \langle \psi_g |\langle g| \otimes I|^2 , \\
D &= 1 - F \\
&= 1 - \int_G dg \sum_{r\mu} \text{Tr}[A_{r\mu} \tilde{\rho}(g) A_{r\mu}^\dagger |\psi(g)\rangle \langle \psi(g)| \otimes I].
\end{align*}
\]
To be specific, we shall reuse the notation in Eq. (1) and assign a rotation $r \in SU(2)$ for the guessed state $|\psi_g\rangle$. By rewriting $|\psi_r\rangle = U_r|0\rangle$, we can reduce the expression $I$ to

$$I = \int_{\Omega} dg \sum_{\mu} \text{Tr}[A^\dagger_{\mu}A_\mu \bar{\rho}(g)] |0\rangle U^\dagger_r U_g |0\rangle^2$$

$$= \int_{\Omega} dg \sum_{\mu} \text{Tr} \left[ (U^\dagger_r \otimes U^\dagger_g) A^\dagger_{\mu} A_\mu (U_r \otimes U_g) \bar{\rho}(g) \right] \times \langle \psi_g | 0 \rangle \langle 0 | \psi_g \rangle,$$  \hspace{1cm} (4)

where in the second line we have defined $U_g = U_r^\dagger U_g$ and apply the invariance $dg' = dg$.

Generally, the value of information $I$ varies greatly depending on the intensity of Eve’s eavesdropping attack. However, two extreme cases have already been known: (1) The most informative measurement, with $I_{\text{max}} = \frac{3\sqrt{3}}{6}$, happens when Von Neumann Projection along the four tetrahedral directions is performed[10]. (2) $I_{\text{min}} = 2/3$ regards to the case in which the projective measurement is performed within the Hilbert Space of $|\psi(g)\rangle$ only, leaving the first state $|\psi(0)\rangle$ intact, i.e., $\mathcal{D}(I_{\text{min}}) = 0$ [9]. To escape from being detected, Eve may adjust his strategy, varying his information from $I_{\text{max}}$ to $I_{\text{min}}$. In this case, what is Eve’s minimal disturbance for each intermediate information $I (I_{\text{min}} \leq I \leq I_{\text{max}})$ is what we mainly focused and is in fact the mathematic description of the tradeoff problem.

For this purpose, one needs to perform an exhaustive examination of all the possible $\{A_{\mu}\}$. Fortunately, one can resort to the group covariant technique to strikingly simplify our problems.

### III. COVARIANT MEASUREMENT AND OPTIMAL INFORMATION-DISTURBANCE BOUND

Group covariant quantum measurement is a special kind of measurement which originates from the symmetry of the input state and has already been proven to be optimal in quantum state estimation[21] and the quantum cloning[24] process. It can be easily shown that the optimality also preserves in our problem. In fact, for an arbitrary (or non-covariant) CP map $\mathcal{E}(\rho) = \sum_{\mu} A_{\mu} \rho A^\dagger_{\mu}$, one can construct a covariant CP map $\mathcal{E}'(\rho) = \int G E'_G(\rho) dG$ which yields the same amount of information gain and disturbance, when the $E'_h(\cdot)$ and the guessed state for result $h$ are chosen to be

$$E'_h(\rho) = \sum_{\mu} (U_h U^\dagger_r \otimes U_h U^\dagger_g) A_{\mu} (U_r U^\dagger_h \otimes U_r U^\dagger_h) \rho \times (U_h U^\dagger_r \otimes U_h U^\dagger_g) A^\dagger_{\mu} (U_r U^\dagger_h \otimes U_r U^\dagger_h),$$  \hspace{1cm} (5)

$$|\psi_h\rangle = U_h |0\rangle,$$  \hspace{1cm} (6)

with the subscript $h \in SU(2)$ denoting the measurement result of the continuous POVM. Therefore, the optimal trade-off bound for covariant map is also the optimal bound for arbitrary maps. Therefore, in looking for the optimal bound between $I$ and $D$, there will be no loss of generality if we restrict our study in the covariant way. The covariance map in Eq.(3) and (4), along with its good property $\mathcal{E}'_{gh}(\rho) = U_g \mathcal{E}_h(U^\dagger_g \rho U_g) U^\dagger_g$, not only guarantees the measurement achieves its optimal performance for all the possible state $|\psi(g)\rangle$, but also simplifies our following computation considerably. Hereafter, we will consider the covariant instrument

$$A_h = U_h \otimes U_h A_0 U^\dagger_h \otimes U^\dagger_h$$  \hspace{1cm} (7)

with the operator $A_0$ denoting a seed of the whole set of Kraus operators. Notice that the trace-preserving condition now boils down to $\int_h A^\dagger_h A_h = 1 \otimes 1$ which can be further reduced with Schur’s lemma for reducible group representation[20]:

$$\int_{SU(2)} dg U_h \otimes U_h A_0^\dagger U^\dagger_h \otimes U^\dagger_h = \text{Tr}[A_0^\dagger A_0 M_1] M_1 + \text{Tr}[A_0^\dagger A_0 M_2] M_2/3, \hspace{1cm} (8)$$

where $M_1 = |\Psi^\rangle \langle \Psi^| |(01)\rangle (10)/\sqrt{2}$ denotes the uni-dimensional completely asymmetric subspace and $M_2 = 1 \otimes 1 - M_1$ denotes the 3-dimensional symmetric subspace. Now the trace-preserving condition boils down to

$$\text{Tr}[A_0^\dagger A_0 M_1] = 1 \text{ and } \text{Tr}[A_0^\dagger A_0 M_2] = 3. \hspace{1cm} (9)$$

With the covariant map $\{A_h\}$, the integral $dg$ in Eq.(4) and (3) can be easily obtained. For $D$, we have

$$D = 1 - \int \int dG dI \text{Tr} \left[ A_h \bar{\rho}(g) A^\dagger_h |\psi(g)\rangle \langle \psi(g)| \otimes I \right]$$

$$= 1 - \sum_{i=0,1} \int \int dG dI \langle \psi(g)| \langle i | A_0 \bar{\rho}(g) A^\dagger_0 |i\rangle \times \langle i | A_0 \bar{\rho}(g) A^\dagger_0 |i\rangle \rangle$$

$$= 1 - \sum_{i,j,k=0,1} \langle ji | A_0 M_{jk} A^\dagger_0 |ki\rangle,$$  \hspace{1cm} (11)

where the operator

$$M_{jk} = \int_{G} \int dG \langle \psi(g)| j \rangle \cdot \bar{\rho}(g) \cdot \langle k | \psi(g)\rangle, \hspace{1cm} j, k \in \{0, 1\}$$

can be calculated explicitly[22].

The derivation for $I$ can be done in a similar way, which yields

$$I = \int \int dG dI \text{Tr} [ A^\dagger_h A_h \bar{\rho}(g) ] |0\rangle U^\dagger_h U_g |0\rangle^2$$

$$= \int dG dI \text{Tr} \left[ A_0^\dagger A_0 \bar{\rho}(g) \right] \cdot \langle \psi(g)|0\rangle \langle 0 | \psi(g)\rangle$$

$$= \text{Tr} \left[ A_0^\dagger A_0 M_{00} \right]. \hspace{1cm} (12)$$
Now putting all these results together, the tradeoff problem can be formulated with the following semi-definite programming problem:

\[ \text{Min} : \mathcal{D}(\mathcal{I}) = 1 - \mathcal{F} \]

such that

\[ \mathcal{F} = \sum_{i,j,k=0,1} (\langle j | A_0 M_{jk} A_0^\dagger | k \rangle), \]

\[ \mathcal{I} = \text{Tr} \left[ A_0^\dagger M_0 A_0 \right], \quad A_0^\dagger A_0 \geq 0, \]

\[ \text{Tr}[A_0^\dagger A_0 M_1] = 1 \quad \text{and} \quad \text{Tr}[A_0^\dagger A_0 M_2] = 3. \]  

Due to the complication of the minimization above\[^27\], an analytical solution to is not always obvious and available. However, in the rest, one will see that we can rely on the vector analysis technique and derive the optimal tradeoff bound.

To continue our discussion, we need to introduce a few vectors \( \{ \tilde{v}_i = (v_{i1}, v_{i2})^T, v_{ij} \in \mathbb{C} \}, (i = 1, 2, \cdots, 8, j = 1, 2) \) such that

\[ A_0 = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix} = \begin{pmatrix} \tilde{v}_1 & \tilde{v}_2 & \tilde{v}_3 & \tilde{v}_4 \\ \tilde{v}_5 & \tilde{v}_6 & \tilde{v}_7 & \tilde{v}_8 \end{pmatrix}. \]

This helps to give much simpler expressions to our problem. First of all, the trace-preserving equation \( \mathcal{I} \) can be reduced to

\[ \sum_i |\tilde{v}_i|^2 = 4, \]

\[ |\tilde{v}_2 - \tilde{v}_3|^2 + |\tilde{v}_7 - \tilde{v}_6|^2 = 2. \]

Then, it can be easily obtained that

\[ \mathcal{F} = \frac{1}{2} + \frac{1}{12} f, \quad \mathcal{I} = \frac{1}{2} + \frac{1}{12} g, \]

with \( f \) and \( g \) defined by

\[ f = |\tilde{v}_2|^2 - |\tilde{v}_3|^2 + |\tilde{v}_7|^2 - |\tilde{v}_6|^2 - |\tilde{v}_1|^2 - |\tilde{v}_8|^2 + |\tilde{v}_7 - \tilde{v}_6 + \tilde{v}_4|^2 + |\tilde{v}_8 + \tilde{v}_2 - \tilde{v}_3|^2 - 2, \]

\[ g = |\tilde{v}_2|^2 - |\tilde{v}_3|^2 + |\tilde{v}_6|^2 - |\tilde{v}_7|^2. \]

The optimization in Eq. \( \mathcal{I} \) can now be equivalently reduced to looking for a set of vectors \( \tilde{v}_i \) that satisfy the constraints Eq. \( \mathcal{I} \) and \( \mathcal{I} \) and maximize \( f \) for a given value \( g \).

After some lengthy but not very interesting algebra, one can checked that the relation between \( f \) and \( g \) actually follows

\[ f \leq f_{\text{max}}(g) = g + \sqrt{24 - 2g^2}. \]

This means that for any quantum measurement, the amount of the disturbance \( \mathcal{D} \) caused on the quantum states must follow

\[ \mathcal{D} \geq \mathcal{D}_{\text{min}} = 1 - \mathcal{I} - \sqrt{\frac{1}{3} + 2\mathcal{I} - 2\mathcal{I}^2}. \]

In the literature, the quantum measurement whose disturbance equals \( \mathcal{D}_{\text{min}} \) is named as “Minimal Disturbance Measurement (MDM)”. This is the best strategy for Eve, as it maximizes his information gain for a given average disturbance.

The MDM quantum operation for antiparallel spins can be deduced from the derivation of Eq.\( \mathcal{I} \). Here we omit the complicated process and list the main result. In fact, the operators \( A_0 \) with

\[ \frac{\tilde{v}_2}{|\tilde{v}_2|} = \frac{\tilde{v}_3}{|\tilde{v}_3|} = \frac{\tilde{v}_8}{|\tilde{v}_8|}, \quad \tilde{v}_1 = \tilde{v}_4 = \tilde{v}_5 = \tilde{v}_6 = \tilde{v}_7 = 0 \]

is one example at hand. Particularly, to see the interpolation between the two extreme cases mentioned in Sec. II, we can introduce a control parameter \( \theta \):

\[ A_0 = |00\rangle\langle \Psi^-| + \frac{\sqrt{6} \cos \theta}{2} |00\rangle\langle \Psi^+| + \sqrt{3} \sin \theta |10\rangle\langle 11|, \]

with \( \theta \in \left[ 0, \arccos(1/\sqrt{3}) \right] \). \( \mathcal{I} \)

It is straightforward to verify that, from equations \( \mathcal{I} \) \( \mathcal{I} \), that the performance of the covariant measurement Eq.\( \mathcal{I} \) follows

\[ \mathcal{I} = \frac{1}{2} + \frac{\sqrt{6} \cos \theta}{6}, \]

\[ \mathcal{D} = \frac{1}{2} - \frac{\sqrt{3} \cos \theta}{6} - \frac{\sqrt{6} \sin \theta}{6}, \]

and the equality sign in Eq. \( \mathcal{I} \) actually can be satisfied.

**IV. DISCUSSIONS AND CONCLUDING REMARKS**

Before concluding this work, we have two problems to remark.
The normalization condition enables the implementation of the covariance using only discrete POVMs. From the covariance operators above, we can construct an POVM with only four outcomes. Other operator can be obtained by $A_i = \frac{1}{2} U_i \otimes U_i A_i U_i^\dagger \otimes U_i^\dagger$, $(i = 0, 1, \ldots, 3)$, with $U_i$:

\begin{align}
U_0 &= I, U_1 = \frac{\sqrt{3}}{3} I - i\sigma_y,
U_2 &= \frac{\sqrt{3}}{3} I + i\frac{\sqrt{6}}{\sqrt{3}} \sigma_y + i\frac{\sqrt{2}}{\sqrt{3}} \sigma_x,
U_3 &= \frac{\sqrt{3}}{3} I + i\frac{\sqrt{6}}{\sqrt{3}} \sigma_y - i\frac{\sqrt{2}}{\sqrt{3}} \sigma_x.
\end{align}

One can easily checked that all these operator satisfies the normalization condition $\sum_i A_i A_i = I \otimes I$ and the optimal tradeoff for measuring antiparallel states follows Eq. (22). This indicates the relation in Eq. (21) is exactly a tight one and cannot be further improved any more.

The second one is the physical meaning of the tradeoff bound in Eq. (22). We remark that it sheds some light on the secure transmission of frame information on the parallel and antiparallel spins, along with the optimal POVM measurement as shown in this paper. This means that there exists a much better eavesdropping strategy for Eve. For example, by choosing $A_0 = |00\rangle \langle \sqrt{2} + \sqrt{3}|01\rangle|10\rangle$, it is not difficult to show that the minimum disturbance $D = (3 - \sqrt{3})/6$ can be reached. This is far from a piece of good news for transmission via the antiparallel spins. With the antiparallel state, Alice gains a definitely improvement in the precision or fidelity in her transmission of frame information to Bob. But the precision or fidelity is improved for Eve, too. what is worse, compared with the parallel quantum state, Eve could obtain the same amount of information with a less disturbance. To see this, in Fig. 2 we give a comparative plot of the information-disturbance tradeoff between the case of antiparallel spin and of the parallel spin. The tradeoff bound for Parallel spins marked with Dashing line is borrowed from Ref. [29]. It can be obviously observed that antiparallel spins provides an unexceptional improvement in the information gain ($I$ up to $3 + \sqrt{3})/6$). However, for the values $I \leq 3/4$ a pronounced decrease in the disturbance will be spotted. In order to see the degree of decrease in a better way, we also plots the dependence of decrease $\Delta D = D_{\text{anti}} - D_{\text{para}}$ on the information gain. Numerical analysis reveals that the amount of reduction in $D$ increases monotonically with the gain, with the maximum $\Delta D/D = \sqrt{2}/3 = 81.65\%$ attained at $I = 3/4$.

In conclusion, we give a heuristic security analysis of transmitting reference reframes, with the model of information-disturbance tradeoff. A strict bound for antiparallel spins, along with the optimal POVM measurement which attains the bound is obtained. Finally, we give a comparison between the tradeoff in antiparallel and parallel cases, which reveals that the improvement in information gain doesn’t always mean a good matter, at least in the cases when information is being measured with fidelities. We believe more thorough analysis using the information theory-based methods should be required.

Acknowledgments

This work was supported by National Fundamental Research Program, also by National Natural Science Foundation of China (Grant No. 10674128 and 60121503) and the Innovation Funds and “Hundreds of Talents” program of Chinese Academy of Sciences and Doctor Foundation of Education Ministry of China (Grant No. 20060358043).

[1] S. D. Bartlett, T. Rudolph, R. W. Spekkens, Rev. Mod. Phys. 79, 555 (2007).
[2] A. Peres and Petra F. Scudo, Arxiv: quant-ph/0201017.
[3] A. Peres and W. K. Wootters, Phys. Rev. Letts 66, 1119 (1991).
[4] E. Bagan, M. Baig, and R. Muñoz-Tapia, Phys. Rev. Lett. 87, 257903 (2001); ibid, 89, 277904 (2002); Phys. Rev. A 70, 030301 (2004).
[5] E. Bagan, M. Baig, A. Brey, and R. Muñoz-Tapia, R. Tarrach, Phys. Rev. Lett. 85, 5230 (2000).
[6] G. Chiribella, G. M. D’Ariano, P. Perinotti, and M. F. Sacchi, Phys. Rev. Lett. 93, 180503 (2004).
[7] A. Peres and Petra F. Scudo, Phys. Rev. Lett. 87, 167901 (2001).
[8] A. Peres and Petra F. Scudo, Phys. Rev. Lett. 86 4160(2001).
[9] S. Massar and S. Popescu, Phys. Rev. Lett. 95, 1259 (1995).
[10] N. Gisin, S. Popescu, Phys. Rev. Lett. 83, 432 (1999).
[11] Piotr Kolenderski and Rafal Demkowicz-Dobrzenski, Phys. Rev. A 78, 052333 (2008).
[12] Giulio Chiribella, Lorenzo Maccone, and Paolo Perinotti, Phys. Rev. Lett. 98, 120501 (2007).
[13] C. A. Fuchs and A. Peres, Phys. Rev. A 53, 2038 (1996).
[14] C. A. Fuchs and K. Jacobs, Phys. Rev. A 63, 062305 (2001).
[15] L. Místa Jr., J. Fiurášek, and R. Filip, Phys. Rev A 72, 012311 (2005).
[16] L. Maccone, Phys. Rev. A 73, 042307 (2006).
[17] Francesco Buscemi and Massimiliano F. Sacchi, Phys. Rev. A 74 052320 (2006).
[18] K. Banaszek, Phys. Rev. Lett 86, 1366 (2001).
[19] K. Banaszek, Phys. Rev. A 62, 024301 (2001).
[20] M. F. Sacchi, Phys. Rev. Lett 96, 220502 (2006).
there seems to be no simpler formula for $\mathcal{F}$

$$
\mathcal{F} = I + \frac{1}{6} \left[ \sum_i |\langle 1_i | A_0^\dagger | 10 \rangle|^2 - \sum_i |\langle 1_i | A_0 | 01 \rangle|^2 \right] 
+ \frac{1}{6\sqrt{2}} \left( \text{Tr}[A_0^\dagger | \Psi^- \rangle \langle 11 | A_0 | 0 \otimes 1 ] - \right. 
\left. \text{Tr}[A_0 | 00 \rangle \langle \Psi^- | A_0^\dagger | 1 \otimes 1 ] + \text{c.c.} \right),
$$

in which c.c. denotes Complex Conjugate.