Quantum Cryptography as a Retrodiction Problem

A. H. Werner,[1,*] T. Franz,[1] and R. F. Werner[1]

[1]*Institut für Theoretische Physik, Leibniz Universität Hannover, Appelstraße 2, 30167 Hannover*

(Received 29 September 2009; published 25 November 2009)

We propose a quantum key distribution protocol based on a quantum retrodiction protocol, known as the Mean King problem. The protocol uses a two way quantum channel. We show security against coherent attacks in a transmission-error free scenario, even if Eve is allowed to attack both transmissions. This establishes a connection between retrodiction and key distribution.

DOI: 10.1103/PhysRevLett.103.220504 PACS numbers: 03.67.Dd

Introduction.—Quantum key distribution (QKD) protocols allow two parties, traditionally called Alice and Bob, to generate a secret key which enables them to communicate secretly via onetime pad encryption. There are QKD protocols that guarantee the security of the key against an eavesdropper who is capable of implementing arbitrary quantum operations (coherent attacks) [1–3].

After the execution of a QKD protocol, Alice and Bob should share an identical and random bit string which is unknown to a potential eavesdropper Eve. If one forgets for a moment about the secrecy of the bit string, the goal in a QKD protocol is that one of the communicating partners infers a bit value corresponding to a measurement outcome obtained or a state prepared by the other. In an optimal protocol, one would request that this is possible in every run of the protocol.

A similar problem, the Mean King problem, has been proposed by Vaidman, Aharonov, and Albert in the context of the retrodiction of a measurement result of a spin $\frac{1}{2}$-particle [4]. Alice in this setting has to guess the outcome of a measurement performed by Bob without knowing the measurement basis used. The first proposal to use this setup in a quantum cryptographic context appeared in [5], but a security proof accounting for an arbitrary attack on both quantum channels was not given. In this Letter, we show that there are solutions to the Mean King problem which guarantee the security of these measurement results against an eavesdropper in a stronger scenario thus establishing the connection between retrodiction and security. In addition, the proposed protocol generates a bit of raw key in every single run.

Setting and result.—

The Mean King retrodiction problem.—The retrodiction problem can be stated as a quantum game with two players. One player, Alice, wins the game if she can guess a measurement outcome obtained by the other player, Bob. Both of them agree beforehand on a Hilbert space $\mathcal{H}$ of dimension d and a set of $d+1$ orthonormal bases of this Hilbert space $\{\Phi_b(i); i = 1, \ldots, d, b = 1, \ldots, d+1\}$. Here, $\Phi_b(i)$ denotes the ith basis vector of the bth basis.

Alice starts the game by preparing a maximally entangled state $\Omega \in \mathcal{H} \otimes \mathcal{H}$ and sends the second system to Bob. He performs a projective measurement in a randomly chosen basis $b \in \{1, \ldots, d+1\}$, but keeps this choice and his measurement result i secret. After Bob has returned the resulting eigenstate of his measurement to Alice, she holds the state (conditional on Bob obtaining i)

$$\hat{\Phi}_b(i) = [\mathbb{1} \otimes |\Phi_b(i)\rangle\langle\Phi_b(i)|]\Omega. \tag{1}$$

After Alice has performed a final measurement $\{F_x\}$ on this state, obtaining a classical result x, all quantum information is discarded. In the last step, Bob reveals his choice of basis b and depending on this value and her measurement result x, Alice has to guess Bob's measurement outcome i. Bob can make sure that Alice has not kept an entangled quantum copy, by making her give the answer in the form of a program on his classical computer. We note that the precise form of the result x is not important, and we might think of it as a $(d+1)$-tupel $x = (x(1), \ldots, x(d+1))$ indicating to Alice that she should guess $i = x(b)$ if the basis b was chosen by Bob. We refer to x as a guessing function. As there are d different possible measurement outcomes for each of the $d+1$ measurement bases, the set X of possible guessing functions has d^{d+1} different elements. A successful strategy for Alice consists of a maximally entangled state Ω and a measurement $\{F_x\}$ such that the probability for a wrong guess is zero, which means that $\mathrm{tr}[F_x|\hat{\Phi}_b(i)\rangle\langle\hat{\Phi}_b(i)|] = 0$, unless $x(b) = i$ and that she can make a guess in every round, implying the normalization condition $\sum F_x = \mathbb{1}$.

The existence of such a strategy has been studied in the case of mutually unbiased bases (MUBs) [4,6]. In [7], it has been shown that weaker conditions are sufficient for constructing a winning strategy. A set of k bases only has to be *nondegenerate*, meaning that the span of the projectors $|\Phi_b(i)\rangle\langle\Phi_b(i)|$ is $k(d-1)+1$ dimensional and has to *admit a classical model*. Here, a set of k bases is said to admit a classical model if there exists a probability distribution of k variables, each taking d values, such that its marginals equal the probability distributions of the joint probabilities $p_{ab}(i,j) = \frac{1}{d}|\langle\Phi_b(i)|\Phi_a(j)\rangle|^2$ for all pairs of bases.

In our scenario with $k = d + 1$, nondegeneracy implies also that the projectors span the space of all Hermitian operators on $\mathcal{H}$. Of course, $d + 1$ mutual unbiased bases (MUBs) are an example of a set of bases exhibiting these properties [7].

The QKD protocol.—We assume a setting for the Mean King problem in which the set of bases is nondegenerate and Alice has a successful strategy that is maximal in the sense of incorporated measurement projectors (see bellow). In each run, there will be n instances of the Mean King problem, and we use a vector arrow to indicate n-tuples of choices, outcomes, etc. It is irrelevant for our analysis whether the steps are carried out sequentially for each instance, or for the full block of n instances simultaneously. Note that only Alice is required to posses a quantum memory.

The protocol is carried out in the following way: (1) Initially, an entangled state ρ_n of n pairs is generated and distributed to Alice and Bob. This process is vulnerable to attack, but they proceed as if $\rho_n = |\Omega^{\otimes n}\rangle\langle\Omega^{\otimes n}|$ consists of n copies of the pure state used for the Mean King problem. (2) Bob chooses at random n measurement bases $\vec{b}$, performs the projective measurement with basis b_k on the kth particle, obtaining the results i_k, and sends back the corresponding eigenstate. Altogether, he returns $\Phi_{\vec{i}}(\vec{b}) = \bigotimes_{k=1}^{n} \Phi_{i_k}(b_k)$, without disclosing $\vec{i}$ or $\vec{b}$. (3) Alice performs her measurement $\{F_x\}$ on each of the returning particles and the corresponding one in her storage, obtaining as a result an n-tuple $\vec{x}$ of guessing functions. (4) After Alice announces that she finished the last of her measurements, Bob publishes his choice of bases $\vec{b}$ from which Alice infers $i'_k = x_k(b_k)$.

Without Eve's interaction, this will produce an identical string $\vec{i}' = \vec{i}$ of d digits because you can regard it as a Mean King game between Alice and Bob. In order to test for the presence of an eavesdropper, Alice and Bob will randomly select some particles k and check for the agreement $i'_k = i_k$ in these instances and accept if they never find a deviation.

Security.—The *transmission-error free scenario* for the security analysis assumes that Alice and Bob find agreement with probability 1, i.e., that a potential attacker does not risk the introduction of any errors at all—also that there are no spontaneous transmission errors. Of course, a full analysis would have to allow for errors, so the proof of security in this scenario is only a proof of principle.

In our setting, Eve can interact at different stages. First, she may provide the initial state, possibly keeping a system of her own entangled with the distributed pairs. Then, she may interact with the states that Bob returns to Alice in a coherent way and finally make a joint measurement on her system. We even allow choices violating time ordering, since we analyze whole blocks simultaneously.

We show in the next section that if Eve's actions do not interfere with the perfect key agreement, which Alice and Bob can test in principle, then her final conclusion will be uncorrelated with the key, i.e., she will have learned nothing about it.

Proof.—A key notion in the Mean King problem is the idea of *safe vectors* [7]. All vectors in the range of a measurement operator F_x must be safe vectors, if Alice does not want to risk a wrong guess. Together with a convenient normalization, we call η_x a safe vector for guessing function x if

$$\langle \eta_x | \hat{\Phi}_b(i) \rangle = \delta_{x(b),i} \quad \forall\ x, i, b \tag{2}$$

with $\hat{\Phi}_b(i)$ from Eq. (1). It is shown in [7] that for a nondegenerate choice of bases, such a vector exists for every guessing function x.

If Alice chooses a measurement $\{F_x\}$ that incorporates all of the projectors $p(x)|\eta_x\rangle\langle\eta_x|$, $p(x) \neq 0$, we call her strategy maximal. We now show that an operator that possesses all the η_x as eigenvectors has to be a multiple of the identity.

Lemma 1.—Let $\mathcal{H}$ be a Hilbert space of dimension d and $\{\Phi_b(i)\}$ a set of $d + 1$ nondegenerate ONBs and let Alice have a maximal successful strategy. If an operator E: $\mathcal{H} \otimes \mathcal{H} \to \mathcal{H} \otimes \mathcal{H}$ fulfills $E\eta_x = e_x \eta_x$ for all safe vectors η_x solving (2), then $e_x \equiv e$ is constant and $E = e\mathbb{1}$.

Proof.—At first, from $\sum_x p(x)|\eta_x\rangle\langle\eta_x| = \mathbb{1}$, we can conclude that $\mathrm{span}_{\mathbb{R}}\{\eta_x; x \in X\} = \mathcal{H} \otimes \mathcal{H}$ holds. Since the number d^{d+1} of guessing functions is larger than the maximal dimension, d^2, of $\mathcal{H} \otimes \mathcal{H}$ and there is a safe vector η_x for every guessing function [7], we can ask for a decomposition of a given safe vector η_x in a set of linearly independent safe vectors $\{\eta_y\}$, with $\eta_x \neq \eta_y$ and $\eta_x = \sum_y \alpha_y \eta_y$, such that $\alpha_y \neq 0$, $\forall\ y$. One possibility is to choose the three safe vectors η_u, η_v, η_w, whose guessing functions fulfill for two bases $b', \tilde{b} \in \{1, \ldots, d + 1\}$, $b' \neq \tilde{b}$ with the relations

$$\begin{aligned} x(b') &= v(b') = i' \neq j' = u(b') = w(b') \\ x(\tilde{b}) &= u(\tilde{b}) = \tilde{i} \neq \tilde{j} = v(\tilde{b}) = w(\tilde{b}) \\ x(b) &= u(b) = v(b) = w(b), b \notin \{\tilde{b}, b'\}. \end{aligned}$$

Then, the decomposition is given by $\eta_x = \eta_u + \eta_v - \eta_w$, which can be seen by evaluating the defining Eq. (2) for all cases. If η_x, η_u, η_v, η_w are eigenvectors of the operator E, it follows from the uniqueness of the decomposition in linearly independent vectors and

$$E\eta_x = E(\eta_u + \eta_v - \eta_w) = e_u \eta_u + e_v \eta_v - e_w \eta_w \tag{3}$$

$$E\eta_x = e_x(\eta_u + \eta_v - \eta_w) \tag{4}$$

that η_u, η_v, η_w belong to the same eigenvalue.

Now pick two arbitrary safe vectors, η_x, η_y with $x \neq y$, which by assumption belong to the eigenvalues e_x and e_y. Since $x \neq y$, there exist $1 \leq m \leq d + 1$ bases b_k with $x(b) \neq y(b)$. Now choose a sequence of guessing functions $(z_l)_{l=0}^{m}$ with $z_0(b) = x(b)$ $\forall\ b$ and $z_{l+1}(b) = z_l(b)$ $\forall\ b \neq b_{l+1}$

and $z_{l+1}(b_{l+1}) = y(b_{l+1})$ which accounts for $z_m(b) = y(b)$. With the paragraph above, it follows that $e_{z_l} = e_{z_{l+q}}$ for all l and therefore especially $e_x = e$ for all guessing functions x since x and y were arbitrary.

Using that span $\{\eta_x\} = \mathcal{H} \otimes \mathcal{H}$ holds, we can find for all $\Psi \in \mathcal{H} \otimes \mathcal{H}$ a set of linearly independent $\{\eta_x\}$ such that $\Psi = \sum_x \alpha_x \eta_x$ with $\alpha_x \neq 0 \; \forall \; x$. This shows that every $\Psi \in \mathcal{H} \otimes \mathcal{H}$ is an eigenvector of E and we can conclude that $E = e\mathbb{1}$. ■

The key to showing security for blocks of length n is to consider these n steps as part of a single instance of a Mean King retrodiction game in a larger Hilbert space with more bases. By tensoring, we get $(d+1)^n$ measurement bases $\{\Phi_{\vec{b}}(\vec{i}) = \bigotimes_{l=1}^n \Phi_{b_l}(i_l)\}$ on Bob's side in d^n dimensions. The n entangled states Alice sends to Bob can be considered as an entangled state on $(\mathcal{H} \otimes \mathcal{H})^{\otimes n}$, and an apparently successful strategy is the n times execution of her maximal strategy for the single run $\{F_x\}$ obtaining the guessing functions $\vec{x} = (x_1, \ldots, x_n)$. The resulting vectors of the form $\eta_{\vec{x}} = \bigotimes_{l=1}^n \eta_{x_l}$ we call *safe product vectors* since after rearranging of the tensor factors

$$\langle \eta_{\vec{x}} | \hat{\Phi}_{\vec{b}}(\vec{i}) \rangle = \prod_{l=1}^n \langle \eta_{x_l} | \hat{\Phi}_{b_l}(i_l) \rangle = \prod_{l=1}^n \delta_{x_l(b_l), i_l},$$

they satisfy the constraint (2).

Of course, the set of product measurement bases is no longer nondegenerate, however, because $\dim\{\mathrm{span}_{\mathbb{R}}[|\Phi_{\vec{b}}(\vec{i})\rangle\langle\Phi_{\vec{b}}(\vec{i})|]\} = d^{2n}$ holds they still span the space of all Hermitian operators on $\mathcal{H}^{\otimes n}$, the same is true for the set of all safe product vectors $\{\eta_{\vec{x}}\}$. The safe product vectors $\eta_{\vec{x}}$ inherit the decomposition property from the single safe vectors η_x, by applying the property to one of the tensor factors. So every safe product vector $\eta_{\vec{x}}$ can be decomposed into three linearly independent safe product vectors $\eta_{\vec{u}}$, $\eta_{\vec{v}}$ and $\eta_{\vec{w}}$ with $\eta_{\vec{x}} = \eta_{\vec{u}} + \eta_{\vec{v}} - \eta_{\vec{w}}$. From this point, the argument for the operator E follows along the same line as in the single execution case: First, for every two different safe product vectors $\eta_{\vec{x}}$ and $\eta_{\vec{y}}$, we can find a sequence of guessing functions that via Eq. (4) ensure the eigenvalues to be equal. Second, since the span of all safe product vectors generates again $\mathcal{H} \otimes \mathcal{H}$, which is therefore an eigenspace of the operator E to one single eigenvalue, E is a multiple of the identity. We get

Lemma 2.—Let $\{\eta_{\vec{x}}\}$ be the set of all safe product vectors for the n-times execution of a retrodiction problem with $d+1$ nondegenerate measurement bases $\{\Phi_b(i)\}$ on a Hilbert space $\mathcal{H}$ of dimension d for which Alice has a maximal successful strategy. If E: $(\mathcal{H} \otimes \mathcal{H})^{\otimes n} \to (\mathcal{H} \otimes \mathcal{H})^{\otimes n}$ fulfills $E\eta_{\vec{x}} = e_{\vec{x}}\eta_{\vec{x}}$ for all $\eta_{\vec{x}}$, then $e = e_{\vec{x}}$ for all x and $E = e\mathbb{1}$ holds.

We want to analyze the security of the protocol in a transmission-error free scenario for a full coherent attack on both quantum channels. This means that Eve might eavesdrop on the communication by replacing the transmission line from Alice to Bob by an arbitrary quantum channel, U, and that her operation, V, on the feedback channel might be connected to the outcome of this transformation via an additional quantum channel.

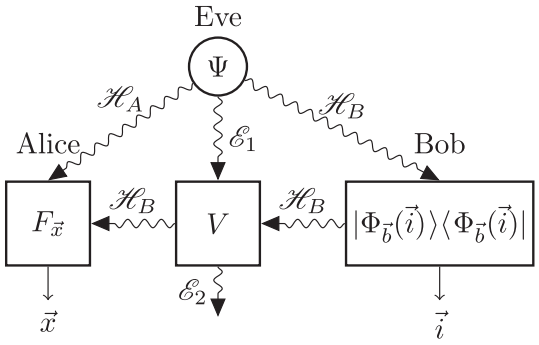

FIG. 1. Full coherent attack on the protocol.

As a further generalization, we even give the control of the source of the maximally entangled state to Eve (see FIG. 1). In this scenario, we prove that if Alice and Bob observe perfect correlations of their data, or more precisely, if Eve chooses an operation that does not cause any errors, the resulting key is perfectly secure.

Lemma 2 shows that the n-time execution of a retrodiction game can be viewed as a one-time execution of retrodiction game on a larger Hilbert space. Because of this, we can prove the security of the n times execution of the single qudit protocol by proving the security of a protocol where Alice and Bob use a d^n-dimensional maximally entangled state initially and the product bases and measurements defined in Lemma 2.

Now suppose Eve prepares the state $\Psi \in \mathcal{H} \otimes \mathcal{H} \otimes \mathcal{E}$. Using $U_{m,l} = X_d^m Z_d^l$ the elements of the generalized Pauli-group of a d-dimensional Hilbert space [8], we can decompose this state in the maximally entangled basis on the first two tensor factors and write it as

$$\begin{aligned}\Psi^{ABE} &= \sum_{m,l,\beta} p_{m,l\beta} (\mathbb{1}_A \otimes U_{m,l} \otimes \mathbb{1}_E) |\Omega^{\otimes n}\rangle \otimes |e_\beta\rangle \\ &= \sum_\beta (\mathbb{1}_A \otimes \hat{U}_\beta \otimes \mathbb{1}_E) |\Omega^{\otimes n}\rangle \otimes |e_\beta\rangle,\end{aligned}$$

where the operators $U_{m,l}$ have the property of generating all basis states of the maximally entangled basis if they are applied in turn to the second tensor factor of $|\Omega^{\otimes n}\rangle$ [9]. For the purpose of clarity, the $U_{m,l}$ and the $p_{m,l,\beta}$ are absorbed into the $\hat{U}_\beta$. By measuring this state in the product bases $\vec{b}$ and obtaining the result $\vec{i}$, Bob projects onto the state

$$|\Psi_{\vec{b},\vec{i}}\rangle = \sum_\beta (\hat{U}_\beta^T \otimes \mathbb{1}_B \otimes \mathbb{1}_E) |\hat{\Phi}_{\vec{b}}(\vec{i})\rangle \otimes |e_\beta\rangle.$$

Here, we used that $(\mathbb{1} \otimes \hat{U})|\Omega\rangle = (\hat{U}^T \otimes \mathbb{1})|\Omega\rangle$ holds for an operator $\hat{U} \in \mathcal{B}(\mathcal{H})$ and the maximally entangled state $|\Omega\rangle \in \mathcal{H} \otimes \mathcal{H}$. Eve might implement an arbitrary quantum channel, V, acting on her subsystem and the eigenstate

of the measurement Bob is sending back to Alice. We now analyze the result of this operation:

$$V[|\Psi_{\vec{b},\vec{i}}\rangle\langle\Psi_{\vec{b},\vec{i}}|] = \sum_{\beta,\beta',l} (\hat{U}_\beta^T \otimes V_l)|\hat{\Phi}_{\vec{b}}(\vec{i})\rangle|e_\beta\rangle\langle\hat{\Phi}_{\vec{b}}(\vec{i})|\langle e_{\beta'}|(\hat{U}_{\beta'}^T \otimes V_l)^\star \otimes |e_l\rangle\langle e_l|. \quad (5)$$

In order to avoid detection, Eve must restrict her attack to quantum channels that do not disturb the measurement statistics observed by Alice and Bob. Even after Eve has interfered with the quantum systems, Alice should guess the right measurement outcome if no transmission errors are taken into account. This means that the states received by Alice still respond to the same safe vectors $\eta_{\vec{x}}$ as before so the condition

$$\mathrm{tr}\{|\eta_{\vec{x}}\rangle\langle\eta_{\vec{x}}|\mathrm{tr}_E(V[|\Psi_{\vec{b},\vec{i}}\rangle\langle\Psi_{\vec{b},\vec{i}}|])\} = \prod_{l=1}^{n} \delta_{x_l(b_l),i_l}$$

must be respected for all guessing functions $\vec{x}$, bases $\vec{b}$ and measurement results $\vec{i}$. Expanding the Kraus operators V_l in a standard basis

$$V_l = \sum_{\gamma,\delta,\mu,\nu} v_{l_{\gamma\delta\nu\mu}}|\gamma\delta\rangle\langle\nu\mu|,$$

inserting this expression in Eq. (5) and tracing out Eve's system we obtain the state controlled by Alice before her final measurement

$$\rho_{\vec{b},\vec{i}}^A = \sum_{l,k} E_{lk}|\hat{\Phi}_{\vec{b}}(\vec{i})\rangle\langle\hat{\Phi}_{\vec{b}}(\vec{i})|E_{lk}^\star \quad (6)$$

where we defined the operators E_{lk} as

$$E_{lk} = \sum_\beta \left[\hat{U}_\beta^T \otimes \left(\sum_{\gamma\nu} v_{l_{\gamma k\nu e_\beta}}|\gamma\rangle\langle\nu|\right)\right].$$

Using (6), we find that the probability of measuring one of the safe product vectors $\eta_{\vec{x}}$ for a given tuple of measurement results $\vec{i}$ in a certain product bases $\vec{b}$ is given by

$$p(\eta_{\vec{x}}, \vec{b}, \vec{i}) = \mathrm{tr}(|\eta_{\vec{x}}\rangle\langle\eta_{\vec{x}}|\rho_{\vec{b},\vec{i}}^A) = \sum_{l,k} |\langle\eta_{\vec{x}}|E_{lk}|\hat{\Phi}_{\vec{b}}(\vec{i})\rangle|^2.$$

From the constraint $p(\eta_{\vec{x}}, \vec{b}, \vec{i}) = \delta_{\vec{x}(\vec{b}),\vec{i}}$, we can conclude that $\langle\eta_{\vec{x}}|E_{lk}|\hat{\Phi}_{\vec{b}}(\vec{i})\rangle$ has to be valid for every l, k, $\vec{b}$, $\vec{i}$, and $\vec{x}$. The safe product vectors $\eta_{\vec{x}}$ are unique one-dimensional projectors and E_{kl} cannot have all the $|\hat{\Phi}_{\vec{b}}(\vec{i})\rangle$ as eigenvectors if $E_{ik} \neq \gamma_{kl}\mathbb{1}$ holds. This leads to the constraint that in order to avoid detection, the operators E_{lk} corresponding to Eve's attack have to fulfill the eigenvalue equations

$$E^\star \eta_{\vec{x}} = \bar{\gamma}_{lkx}\eta_{\vec{x}}$$

for all $\eta_{\vec{x}}$. With Lemma 2, we can conclude that the operators are of the form $E_{kl} = \gamma_{kl}\mathbb{1}$ independent of the measurement result $\vec{x}$ that Alice obtains.

The state under Eve's control after the transmissions is given by

$$\begin{aligned}\rho_{\mathrm{final}}^E &= \mathrm{tr}_{AB}(V[|\Psi_{\vec{b},\vec{i}}\rangle\langle\Psi_{\vec{b},\vec{i}}|]) \\ &= \sum_{l,k,k'} \mathrm{tr}_{AB}[E_{l,k}|\hat{\Phi}_{\vec{b}}(\vec{i})\rangle\langle\Phi_{\vec{b}}(\vec{i})|E_{l,k'}^\star \otimes |k\rangle\langle k'| \otimes |e_l\rangle\langle e_l|] \\ &= \sum_{l,k,k'} \gamma_{k,l}\bar{\gamma}_{k',l}|k\rangle\langle k'| \otimes |e_l\rangle\langle e_l|.\end{aligned}$$

Hence, ρ_{final}^E is independent of Bob's choice of bases $\vec{b}$, his measurement result $\vec{i}$, and Alice's guessing function $\vec{x}$. Subsequently, Eve cannot infer any information about the exchanged key if she wants to stay undetected. This shows the security of the proposed protocol in a transmission-error free scenario.

T. F. and A. W. acknowledge funding from the DFG. T. F. acknowledges support from Braunschweig IGSM.

*albert.werner@itp.uni-hannover.de

[1] C. H. Bennett and G. Brassard, *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175-179.
[2] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[3] R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A **72**, 012332 (2005).
[4] L. Vaidman, Y. Aharonov, and D. Z. Albert, Phys. Rev. Lett. **58**, 1385 (1987).
[5] J. Bub, Phys. Rev. A **63**, 032309 (2001).
[6] G. Kimura, H. Tanaka, and M. Ozawa, Phys. Rev. A **73**, 050301(R) (2006).
[7] M. Reimpell and R. F. Werner, Phys. Rev. A **75**, 062334 (2007).
[8] V. Karimipour, S. Bagherinezhad, and A. Bahraminasab, Phys. Rev. A **65**, 052331 (2002).
[9] S. D. Bartlett, H. de Guise, and B. C. Sanders, Phys. Rev. A **65**, 052316 (2002).