Implementation of a Measurement-Device-Independent Entanglement Witness

Ping Xu,[1,2] Xiao Yuan,[3] Luo-Kan Chen,[1,2] He Lu,[1,2] Xing-Can Yao,[1,2] Xiongfeng Ma,[3,*] Yu-Ao Chen,[1,2,†] and Jian-Wei Pan[1,2,‡]

[1]*Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, China*

[2]*Shanghai Branch, CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai 201315, China*

[3]*Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China*

(Received 23 December 2013; published 10 April 2014)

Entanglement, the essential resource in quantum information processing, should be witnessed in many tasks such as quantum computing and quantum communication. The conventional entanglement witness method, relying on an idealized implementation of measurements, could wrongly conclude a separable state to be entangled due to imperfect detections. Inspired by the idea of a time-shift attack, we construct an attack on the conventional entanglement witness process and demonstrate that a separable state can be falsely identified to be entangled. To close such detection loopholes, based on a recently proposed measurement-device-independent entanglement witness method, we design and experimentally demonstrate a measurement-device-independent entanglement witness for a variety of two-qubit states. By the new scheme, we show that an entanglement witness can be realized without detection loopholes.

DOI: 10.1103/PhysRevLett.112.140506 PACS numbers: 03.67.Mn, 03.67.Dd, 42.50.Dv

Quantum entanglement plays an important role in the nonclassical phenomenons of quantum mechanics. Being the key resource for many tasks in quantum information processing, such as quantum computation [1], quantum teleportation [2], and quantum cryptography [3,4], entanglement needs to be verified in many scenarios. There are several proposals to witness entanglement and we refer to Ref. [5] for a detailed review. A conventional way to detect entanglement, the entanglement witness (EW), gives one of two outcomes: "Yes" or "No," corresponding to the conclusive result that the state is entangled or to failure to draw a conclusion, respectively. Mathematically, for a given entangled quantum state ρ, a Hermitian operator W is called a witness if $\mathrm{tr}[W\rho] < 0$ (output of "Yes") and $\mathrm{tr}[W\sigma] \geq 0$ (output of "No") for any separable state σ. Note that there could also exist an entangled state ρ' such that $\mathrm{tr}[W\rho'] \geq 0$ (output of "No"). In the experimental verification, one can realize the conventional EW with only local measurements by decomposing W into a linear combination of product Hermitian observables [5].

Focusing on the bipartite scenario, a general illustration of the conventional EW is shown in Fig. 1(a), where two parties, Alice and Bob, each receive one component of a bipartite state ρ_{AB} from an untrusted third party Eve. They want to verify whether ρ_{AB} is entangled or not, by performing local operations and measurements on $\rho_A = \mathrm{Tr}_B[\rho_{AB}]$ and $\rho_B = \mathrm{Tr}_A[\rho_{AB}]$. The correctness of such witness relies on implementation details of W. An unfaithful implementation of W, say, due to device imperfections, would render the witness results unreliable. For example, the measurement devices used by Alice and Bob might possibly be manufactured by another untrusted party, who could collaborate with Eve and deliberately fabricate devices to make the real implementation $W' = W + \delta W$ deviate from W, such that W' is not a witness any more,

$$\mathrm{tr}[W'\sigma] < 0 < \mathrm{tr}[W\sigma]. \tag{1}$$

That is, with the deviated witness W', a separable state σ could be identified as an entangled one, which is more likely to happen when $\mathrm{tr}[W\sigma]$ is near zero.

There is a strong similarity between the EW and the quantum key distribution (QKD) where an entanglement-breaking channel would cause insecurity [6]. Roughly

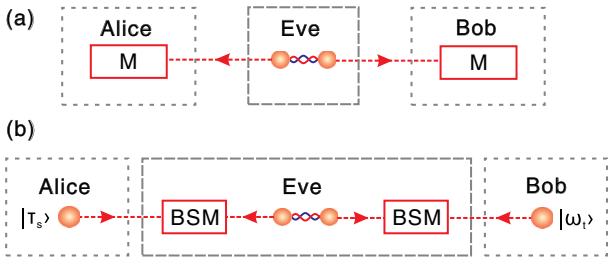

FIG. 1 (color online). (a) Conventional EW setup, where Alice and Bob perform local measurements separately and collect information to decide whether the input state is entangled or not. (b) Measurement-device-independent EW setup, where Alice and Bob each prepare an ancillary state and a third party Eve performs Bell state measurements (BSMs) on the ancillary states and the to-be-witnessed bipartite state. Based on the choices of Alice and Bob's ancillary states and the BSM results, they can judge whether the input state is entangled or not.

speaking, it is crucial for Alice and Bob to prove that entanglement can be preserved in a secure QKD channel. From this point of view, there exists a correlation between the security of the QKD and the success of the EW. For the varieties of attacks in the QKD, such as a time-shift attack [7] and a fake-state attack [8], one may also find similar detection loopholes in the conventional EW process. Originating from this analogy, we construct a time-shift attack that manipulates the efficiency mismatch between detectors used in an EW process. Under this attack, any state could be witnessed to be entangled, even if the input state is separable. By this example, we demonstrate that there do exist loopholes in the conventional EW procedure.

Recently, Lo *et al.* [9] proposed a measurement-device-independent QKD method, which is immune to all hacking strategies on detection. Due to the similarity between the QKD and the EW, one would also expect that there exist EW schemes without detection loopholes. Meanwhile, a nonlocal game is proposed to distinguish any entangled state from all separable states [10]. Inspired by this game, Branciard *et al.* [11] proposed a measurement-device-independent entangelement-witness (MDIEW) method, where they proved that there always exists an MDIEW for any entangled state with untrusted measurement apparatuses.

As shown in Fig. 1(b), Alice and Bob want to identify whether a given bipartite state, prepared by an untrusted party Eve, is entangled or not without trusting measurement devices. To do so, Alice (Bob) prepares an ancillary state τ_s (ω_t) and sends it along with the to-be-witnessed bipartite state to a willing participant, who can be assumed to be Eve again in the worst case scenario. Eve performs two Bell-state measurements (BSMs) on the two ancillary states and the bipartite state. Then, she announces to Alice and Bob the results of the BSMs, based on which they will witness the entanglement of the bipartite state. In the MDIEW, it is guaranteed that a separable state will never be wrongly identified as an entangled one, even if Eve maliciously makes wrong measurements and/or announces unfaithful information [11].

In the experiment, we first show an example of the time-shift attack on the conventional EW process and demonstrate how a separable state can be falsely identified to be entangled when a large efficiency mismatch happens. Then we design and experimentally realize an MDIEW scheme to close such detection loopholes. The MDIEW is used to testify the entanglement of various bipartite states starting from maximally entangled to separable ones. Note that we use heralded single-photon sources to prepare the two ancillary states; thus, our demonstration is realized by a six-photon interferometry.

Time-shift attack.—A time-shift attack, originating from quantum cryptography [7], takes advantage of the efficiency mismatch of the measurement devices. As shown in Fig. 2(a), typically two detectors are used on each side of

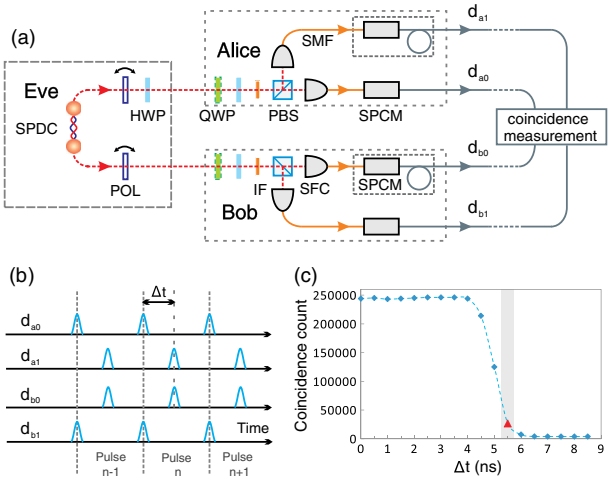

FIG. 2 (color online). Time-shift attack on the conventional EW. (a) Experimental setup of the time-shift attack. Photon pairs are generated by SPDC using a femtosecond pump laser with a central wavelength of 390 nm and a repetition frequency of 80 MHz. POL, polarizer; HWP, half-wave plate; QWP, quarter-wave plate; IF, interference filter with 780 nm central wavelength; PBS, polarizing beam splitter; SFC, single-mode fiber coupler; SMF, single-mode fiber; SPCM, single-photon-counting module. (b) Synchronization between SPCMs. Built-in delay lines enable Eve to shift the output signals d_{a1} and d_{b0} by Δt. (c) Coincidence count versus time delay, where the time window is set to 4 ns. All data points are measured for 2 sec, and the time-shift attack is implemented with $\Delta t = 5.50 \pm 0.24$ ns, which corresponds to the gray area.

Alice and Bob. By controlling the single-photon-counting modules (SPCMs) and coincidence gate, Eve is able to enlarge the efficiency mismatch and hence manipulate the EW result.

To implement this attack, we choose a conventional witness

$$W = \frac{1}{2} I - |\Psi^-\rangle\langle\Psi^-|$$

for bipartite states in the form of

$$\rho_{AB}^{v} = (1 - v)|\Psi^-\rangle\langle\Psi^-| + \frac{v}{2}(|HH\rangle\langle HH| + |VV\rangle\langle VV|), \tag{2}$$

where H (V) denotes the horizontal (vertical) polarization of the single photons and $|\Psi^-\rangle = (|HV\rangle - |VH\rangle)/\sqrt{2}$ is a Bell state. By decomposing W into a linear combination of product Pauli matrices, the EW can be realized by local measurements,

$$\mathrm{Tr}[W\rho_{AB}] = \frac{1}{4}(1 + \langle\sigma_x\sigma_x\rangle + \langle\sigma_y\sigma_y\rangle + \langle\sigma_z\sigma_z\rangle).$$

That is, to identify the entanglement, Alice and Bob just have to each analyze the qubit state in three bases

separately. When the bipartite state is projected to the positive (negative) eigenstates of $\sigma_x\sigma_x$, $\sigma_y\sigma_y$, and $\sigma_z\sigma_z$, it will contribute positively (negatively) to the witness result $\mathrm{Tr}[W\rho_{AB}]$. For example, when measuring $\sigma_x\sigma_x$, Alice and Bob will both project the input state to the eigenstates of σ_x, σ_x^+, or σ_x^-, with corresponding eigenvalues of $+1$ or -1, respectively, and obtain probabilities $\langle\sigma_x^\pm\sigma_x^\pm\rangle$. Then the value of $\langle\sigma_x\sigma_x\rangle$ is defined as $\langle\sigma_x^+\sigma_x^+\rangle+\langle\sigma_x^-\sigma_x^-\rangle-\langle\sigma_x^+\sigma_x^-\rangle-\langle\sigma_x^-\sigma_x^+\rangle$. From Eve's point of view, she wants to convince Alice and Bob that the bipartite state is entangled, that is, $\mathrm{Tr}[W\rho_{AB}]<0$. Thus, her objective is to suppress the positive contributions of $\mathrm{Tr}[W\rho_{AB}]$, such as $\langle\sigma_x^+\sigma_x^+\rangle$ and $\langle\sigma_x^-\sigma_x^-\rangle$ for the $\sigma_x\sigma_x$ measurement, by manipulating the coincidence rate between SPCMs, equivalently enlarging the detector efficiency mismatch. In this case, from Alice and Bob's point of view, the real implemented witness W' is deviated from the desired one W, and satisfies Eq. (1). More details of the time-shift attack can be found in the Supplemental Material [12].

In our experiment, as shown in Fig. 2(a), by encoding qubits in the polarization of photons, the bipartite state $(|HH\rangle_{ab}+|VV\rangle_{ab})/\sqrt{2}$ is generated via spontaneous parametric down conversion (SPDC). Two adjustable polarizers (POLs) are used to disentangle the initial state and project it to $|HH\rangle_{ab}$ and $|VV\rangle_{ab}$ with equal probabilities, corresponding to the separable state with $v=1$ in Eq. (2). After a 45° half-wave plate (HWP), the to-be-witnessed two-qubit system is prepared in the state of $\rho_{AB}=(|HV\rangle\langle HV|+|VH\rangle\langle VH|)/2$. Then Alice and Bob each perform polarization analysis on a qubit from the bipartite state using wave plates, polarizing beam splitters (PBSs), and SPCMs, and guide the electronic signals from the SPCMs into a coincidence gate.

As shown in Fig. 2(b), in the time-shift attack, Eve controls the delay lines in the detection systems and the time window of the coincidence gate, and, hence, manipulates the time-dependent coincidence counting rates between detectors d_{a0} and d_{b0}, d_{a1} and d_{b1}. Hence, she can suppress the positive contributions of measurements $\langle\sigma_x\sigma_x\rangle$, $\langle\sigma_y\sigma_y\rangle$, and $\langle\sigma_z\sigma_z\rangle$. In our demonstration, by setting proper parameters, we let the positive contributions drop to 10.9(1)% of their original values. Since this attack would not affect the negative contributions of $\mathrm{Tr}[W\rho_{AB}]$, the experimental outcomes for $\langle\sigma_x\sigma_x\rangle$, $\langle\sigma_y\sigma_y\rangle$, and $\langle\sigma_z\sigma_z\rangle$ become negative as expected. Finally, Alice and Bob obtain a witness of ρ_{AB} be $\mathrm{tr}[W'\rho_{AB}]=-0.379(4)$, although the input state ρ_{AB} is, in fact, separable. By changing Δt to a larger value, one can even obtain a fake result for that from a maximal entangled state. Thus, a separable bipartite state could be wrongly witnessed to be entangled when Eve is able to manipulate the detection system. It is not hard to see that for any state ρ, Eve can perform a similar attack and trick Alice and Bob into thinking that it is entangled.

Note that in the original time-shift attack in the QKD [7], Eve is only able to partially control the detection efficiency by manipulating the timing of the quantum signals. In that case, Eve cannot arbitrarily enlarge the efficiency mismatch between desired and undesired detection events. In the EW case, there are two quantum signals Eve can manipulate. From our demonstration, we show that by controlling the coincident gates, Eve is able to arbitrarily decrease the coincident detection efficiency (down to 0) for any type of detection events. Thus, Eve can make the EW device output any of her desired results. From this point of view, the efficiency mismatch problem is more serious in the EW.

The MDIEW.—The MDIEW is able to close all loopholes introduced by imperfect measurement devices. In this scheme, to witness entanglement existing in a bipartite state ρ_{AB}, Alice and Bob randomly choose and prepare ancillary states τ_s and ω_t from state sets $\{\tau_s\}$, $\{\omega_t\}$, respectively. By performing two BSMs on the ancillary states and the bipartite state ρ_{AB} as shown in Fig. 1(b), conditional probabilities $p(a,b|\tau_s,\omega_t)=\mathrm{Tr}[(M^a\otimes M^b)(\tau_s\otimes\rho_{AB}\otimes\omega_t)]$ are obtained, where $M^a(M^b)$ denotes the positive operator-valued measure element of Eve's BSM with outcome $a(b)$. The convex combination of the probabilities $p(a,b|\tau_s,\omega_t)$

$$J(\rho_{AB})=\sum_{a,b,s,t}\beta_{s,t}^{a,b}\,p(a,b|\tau_s,\omega_t) \tag{3}$$

define an MDIEW. That is, ρ_{AB} is entangled while $J(\rho_{AB})<0$ and for any separable state σ_{AB}, we have $J(\sigma_{AB})\geq 0$.

For any entangled state ρ_{AB} and its conventional witness W, one can construct an MDIEW in the form of Eq. (3) by decomposing W as a linear combination of product Hermitian operators $\{\tau_s\otimes\omega_t\}$, which are used as the density matrices of the ancillary states [11]. The coefficients β depend on W, the outcome of the BSMs, and ancillary states. We leave the calculation of β to the Supplemental Material [12].

Our experimental setup for MDIEW is shown in Fig. 3, where a six-photon interferometry is utilized. The to-be-witnessed bipartite state ρ_{34}^v, defined in Eq. (2), is encoded in the photon pair 3 and 4. Photon pairs 1, 2 and 5, 6 are used to prepare the ancillary input states $|\tau_s\rangle_2$ and $|\omega_t\rangle_5$, respectively. In our work, various bipartite states $\{\rho_{34}^v\}$, from maximally entangled to separable, are prepared and tested with the MDIEW. The bipartite state ρ_{34}^v is first prepared in the Bell state $|\Phi^-\rangle_{34}=(|HH\rangle-|VV\rangle)/\sqrt{2}$ via a Bell-state synthesizer [13]. As the coherence length of photons is limited by the interference filtering, two 2-mm β-barium-borate (BBO) crystals in each arm result in a relative phase delay between horizontal and vertical polarization components and cause polarization decoherence. Different v can be selected by the "state selector" [14]. They satisfy the relation

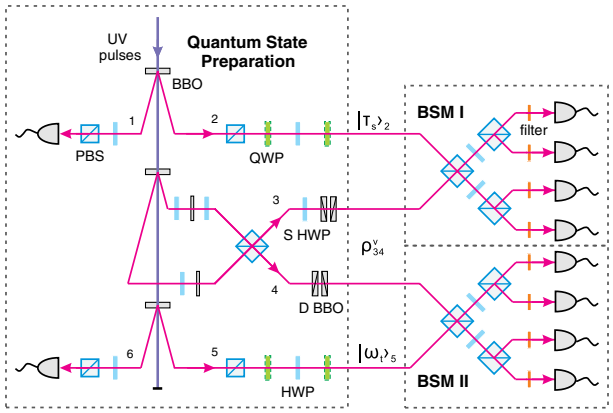

FIG. 3 (color online). Experimental setup for the MDIEW. The photon pairs are generated by type-II SPDC in 2-mm β-barium-borate (BBO) crystals. The pulsed pump laser has a central wavelength of 390 nm and a repetition rate of 76 MHz. To prepare the desired state (3), two 2-mm decoherer BBOs (D BBO) are placed side by side with fast axis setting at 0° (up) and 180° (down) to reduce the spatial walk-off effect. By changing the angle θ of the selector HWP (S HWP), the desired state (2) is prepared with $v = \cos^2(2\theta)$. Heralded photons 2 and 5 are triggered by the detections of photon 1 and 6, respectively. Wave plates are used to rotate the polarizations to encode photons 2 and 5 to the desired states $|\tau_s\rangle_2$ and $|\omega_t\rangle_5$. The BSM module is composed of three PBSs and two HWPs at 22.5°. All photons are filtered by narrow-band filters (with $\lambda_{\mathrm{FWHM}} = 2.8$ nm for BSM I and $\lambda_{\mathrm{FWHM}} = 8.0$ nm for BSM II) and then coupled into single-mode fibers, which connect to SPCMs.

$$v = \cos^2(2\theta), \tag{4}$$

where θ is the angle of the fast axis of the selector HWP.

In the experiment, eight ancillary state pairs $\{\tau_s, \omega_t\}$ are prepared. The states are encoded by tunable wave plates (one HWP sandwiched by two quarter-wave plates (QWPs), which can realize arbitrary single-qubit unitary transformation. Instead of measuring the polarization directly as used in the conventional EW, the analysis of MDIEW is completed by BSMs on $\rho_3^v \otimes |\tau_s\rangle\langle\tau_s|_2$ and $\rho_4^v \otimes |\omega_t\rangle\langle\omega_t|_5$, with two, $|\Phi^{\pm}\rangle = (|HH\rangle \pm |VV\rangle)/\sqrt{2}$, out of four outcomes being collected.

As defined in Eq. (3), we obtain the experimental results J_{exp}^v as shown in Fig. 4. In comparison, we also plot $J_{\mathrm{th}}(\rho_{AB}^v)$ for all values of v. Recall that in the aforementioned time-shift attack demonstration, the conclusion from the conventional witness is entanglement for $v = 1$, whereas here we show that our MDIEW result is 0.107 ± 0.019 and does not conclude that there is an entangled state. One can see that our MDIEW is immune to this attack. The BSM results only provide as information whether or not the entanglement is successfully swapped. It is the ancillary states that determine whether the detection event contributes positively or negatively to the witness value defined in Eq. (3). Thus, by knowing and/or manipulating the BSM results, Eve cannot suppress the positive components of the witness, nor can she cause the MDIEW to render false conclusions.

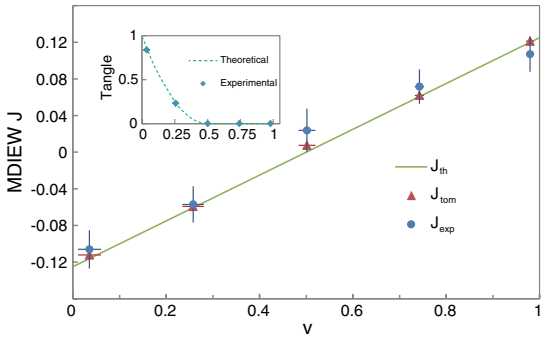

FIG. 4 (color online). MDIEW values are compared for three cases. The theoretical results (J_{th}, solid line) are calculated for the states ρ_{AB}^v with different values of v in Eq. (2). The tomography results (J_{tom}, triangle points) are evaluated for the states ρ_{34}^v after performing tomography on the to-be-witnessed bipartite state. Each point of the experimental results (J_{exp}, circular points) is measured from a 16-h experiment. Vertical error bars indicate 1 standard deviation and horizontal error bars of the fitting values v from state tomography are described in the Supplemental Material [12]. The inset shows theoretical and experimental values of tangle for input states ρ_{34}^v.

Furthermore, we perform tomography on the to-be-witnessed bipartite states $\{\rho_{34}^v\}$. The results of the density matrices are shown in the Supplemental Material [12]. The values of v are also fitted according to Eq. (4) in the Supplemental Material [12], which are consistent with tomography results. We evaluate the MDIEW results, Eq. (3), from the results of the state tomography J_{tom} as shown in Fig. 4. Meanwhile, to quantify the entanglement of the bipartite states $\{\rho_{34}^v\}$, we adopt the measure of tangle [15], which can be directly calculated from tomography results. When the tangle goes to zero, the bipartite state becomes a separable state. As shown in the insert of Fig. 4, no entanglement exists when v grows beyond $1/2$. Such a phenomenon is related to the "sudden death of entanglement" [16].

In summary, we show that the conventional EW method is not reliable due to the loopholes on detections. Meanwhile, as a countermeasure, we design and implement the MDIEW for the bipartite scenario, which is immune to all detection loopholes. The experimental results show that the MDIEW is practical for real-life implementation. Our method can be extended to other multipartite quantum tasks, such as quantum secret sharing.

We acknowledge insightful discussions with K. Chen, Y.-J. Deng, and Z. Zhang. This work has been supported by the National Basic Research Program of China Grants No. 2011CB921300, No. 2013CB336800, No. 2011CBA00300, and No. 2011CBA00301, the National Natural Science Foundation of China Grants, and the Chinese Academy of Sciences. P. X. and X. Y. contributed equally to this work.

*xma@tsinghua.edu.cn
†yuaochen@ustc.edu.cn
‡pan@ustc.edu.cn

[1] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[2] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[3] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE Press, New York, 1984), pp. 175–179.
[4] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[5] O. Gühne and G. Tóth, Phys. Rep. **474**, 1 (2009).
[6] M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004).
[7] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Quantum Inf. Comput. **7**, 073 (2007).
[8] V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74**, 022313 (2006).
[9] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[10] F. Buscemi, Phys. Rev. Lett. **108**, 200401 (2012).
[11] C. Branciard, D. Rosset, Y.-C. Liang, and N. Gisin, Phys. Rev. Lett. **110**, 060405 (2013).
[12] See Supplemental Material athttp://link.aps.org/supplemental/10.1103/PhysRevLett.112.140506 for details of calculations and data postprocessing.
[13] X.-C. Yao, T.-X. Wang, P. Xu, H. Lu, G.-S. Pan, X.-H. Bao, C.-Z. Peng, C.-Y. Lu, Y.-A. Chen, and J.-W. Pan, Nat. Photonics **6**, 225 (2012).
[14] A. G. White, D. F. V. James, W. J. Munro, and P. G. Kwiat, Phys. Rev. A **65**, 012301 (2001).
[15] W. K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).
[16] T. Yu and J. H. Eberly, Phys. Rev. Lett. **93**, 140404 (2004).