Detection Loophole-free Entanglement Verification

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

[1]Center for Quantum Information, Institute for Interdisciplinary Information Sciences
Tsinghua University, Beijing 100084, China
[2]Hefei National Laboratory for Physical Sciences at Microscale, Department of Modern Physics
University of Science and Technology of China, Hefei, Anhui 230026, China
[3]Shanghai Branch, CAS Center for Excellence and Synergetic Innovation Center in Quantum Information
Quantum Physics University of Science and Technology of China, Shanghai 201315, China

Abstract— Quantum entanglement is an essential resource in quantum information processing, which needs to be verified in many tasks such as quantum cryptography and computation. Due to imperfect detection devices when implementing measurements, the conventional entanglement witness method could wrongly conclude a separable state to be entangled. Inspired by the attacks in quantum key distribution, we construct and experimentally realize a time-shift attack on the conventional entanglement witness process. We demonstrate that any separable state can be falsely identified to be entangled. In order to close detection loopholes, we design and experimentally realize a measurement-device-independent entanglement witness for various two-qubit states. We demonstrate that an entanglement witness can be realized without detection loopholes.

1. INTRODUCTION

It has been widely recognized that quantum entanglement plays an important role in the quantum information processing such as quantum computation [1], quantum teleportation [2] and quantum cryptography [3, 4]. Being the key resource for these tasks, quantum entanglement need to be verified in many circumstances. Entanglement witness (EW) is a conventional way to detect entanglement, which 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 $tr[W\rho] < 0$ (output of 'Yes') and $tr[W\sigma] \geq 0$ (output of 'No') for any separable state σ. It is strictly forbidden when we identify a separable state to be entangled. Note that there could also exist entangled state ρ' such that $tr[W\rho'] \geq 0$ (output of 'No'), thus it is OK to fail identifying an entangled state.

In the experiment, one can realize the conventional EW with only local measurements by decomposing W into a linear combination of product Hermitian operators. Then one can do measurements locally on each part and gather measurement outcomes to decide whether the state is entangled or not. A faithful conclusion of such witness relies on the correctness of the experimental implementation, imperfections of detection devices could wrongly conclude a separable state to be entangled. In the practical case, we can regard such imperfection as possible attacks from an adversary, Eve. For example, if the measurement devices used by the witnessers might possibly be manufactured by some untrusted party, who could collaborate with Eve and deliberately fabricate devices to make the real implementation $W' = W + \delta W$ be deviated from W, such that W' is not a witness any more,

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

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 $tr[W\sigma]$ is near zero.

In quantum key distribution (QKD), the security could be guaranteed by proving the presence of entanglement in a secure QKD channel where an entanglement-breaking channel would cause insecurity [5]. Thus there exist strong correlation between the security of QKD and the success of EW. For the varieties of attacks in QKD, such as time-shift attack [6] and fake-state attack [7], one may also find similar detection loopholes in the conventional EW process. Originated 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. [8] proposed an measurement-device-independent (MDI) QKD method, which closed all possible attacks of detectors. As the aforementioned similarity between QKD and 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 [9]. Inspired by this game, Branciard et al. [10] proposed an MDIEW method, where they proved that there always exists an MDIEW for any entangled state with untrusted measurement apparatuses.

In this paper, we first design a time-shift attack to the conventional EW such that every separable state would be witnessed to be entangled. Then based on the proposal in Ref. [10], we design and experimentally realize an MDIEW scheme to close such detection loopholes. We thus practically show a way to witness entanglement without assuming detectors be perfect.

2. MAIN RESULT

2.1. Time-Shift Attack

In the following, we will focus on the bipartite scenario involving two parties Alice and Bob. Consider a type of bipartite quantum states in the form of

$$\rho_{AB}^{v} = (1-v)\left|\Psi^{-}\right\rangle\left\langle\Psi^{-}\right| + \frac{v}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|), \tag{2}$$

with $v \in [0,1]$ and $|\Psi^{-}\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$. The state is entangled if $v < 1/2$, which can be witnessed by a conventional EW,

$$W = \frac{1}{2}I - |\Psi^{-}\rangle\langle\Psi^{-}|, \tag{3}$$

with result $tr[W\rho_{AB}^{v}] = (2v-1)/2$.

The idea of time-shift attack is originated from quantum cryptography [6] and takes advantage of efficiency mismatches existing in measurement devices. Inspired by this idea, we construct a time-shift attack for the conventional witness defined in Eq. (3). Define $\sigma_0 = I$ and σ_1, σ_2, σ_3 be the Pauli matrices σ_x, σ_y, and σ_z, correspondingly. Then we can decompose W to

$$W = \frac{1}{4}\left(\sum_{i=0}^{3}\sigma_i \otimes \sigma_i\right), \tag{4}$$

and the EW can be realized by local measurements,

$$Tr\left[W\rho_{AB}\right] = \frac{1}{4}\left(1 + \langle\sigma_x\sigma_x\rangle + \langle\sigma_y\sigma_y\rangle + \langle\sigma_z\sigma_z\rangle\right). \tag{5}$$

As shown in Fig. 1, we exploit the time mismatch of the two single-photon-detectors such that one detector is more efficient than the other. In this case, the real implementation (W') is deviated from the original design witness W. In the attack Eve can suppress the positive contributes of the witness result $Tr[W\rho_{AB}]$ to let the witness result $Tr[W'\rho_{AB}]$ be negative by adjusting the time mismatch. For example, when measuring $\sigma_x\sigma_x$, Alice and Bob will project the input state to the

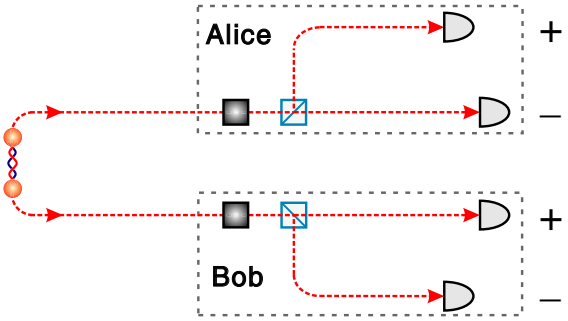

Figure 1: Time-shift attack on the conventional EW. Built-in delay lines enable Eve to control the efficiency of coincidence detection between Alice's and Bob's outcomes.

eigenstates of σ_x, that is σ_x^+ and σ_x^-, corresponding to positive and negative eigenvalue 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

$$\langle\sigma_x\sigma_x\rangle = \langle\sigma_x^+\sigma_x^+\rangle + \langle\sigma_x^-\sigma_x^-\rangle - \langle\sigma_x^+\sigma_x^-\rangle - \langle\sigma_x^-\sigma_x^+\rangle. \tag{6}$$

The probabilities $\langle\sigma_x^\pm\sigma_x^\pm\rangle$ is measured from coincidence counts $N_A^\pm N_B^\pm$ of detectors, that is

$$\langle\sigma_x^\pm\sigma_x^\pm\rangle = \frac{N_A^\pm N_B^\pm}{\sum N_A^\pm N_B^\pm}. \tag{7}$$

If the positive coincidence counts are all suppressed, that is $N_A^+N_B^+ = N_A^-N_B^- = 0$, then the outcome of $\langle\sigma_x\sigma_x\rangle$ is

$$\langle\sigma_x\sigma_x\rangle = -\langle\sigma_x^+\sigma_x^-\rangle - \langle\sigma_x^-\sigma_x^+\rangle = -\frac{N_A^+N_B^-}{\sum N_A^\pm N_B^\pm} - \frac{N_A^-N_B^+}{\sum N_A^\pm N_B^\pm} = -1. \tag{8}$$

Similarly, the all the other local measurements $\langle\sigma_y\sigma_y\rangle$ and $\langle\sigma_z\sigma_z\rangle$ become -1 by suppressing positive coincidence counts, which gives a witness result of

$$Tr[W'\rho_{AB}] = -\frac{1}{2} \tag{9}$$

for any state ρ_{AB}.

In our experiment demonstration, we only suppress the positive coincidence counts to 10.9(1)% instead of neglecting all of them. 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.

2.2. Counter-Measure: MDIEW

The MDIEW method in Ref. [10] is capable to close all detection loopholes, such as the time shift attack we showed in the last paragraph. As shown in Fig. 2, MDIEW requires Alice (Bob) to prepare another ancillary state τ_s (ω_t) and perform Bell-state measurements (BSMs) on the to be witnessed state and the ancillary state.

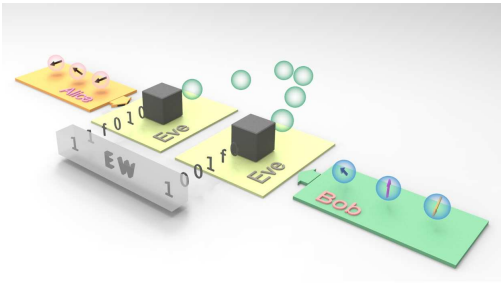

Figure 2: Measurement device independent entanglement witness.

Conditioned on the measurement outcomes, a and b, MDIEW is defined as

$$J(\rho_{AB}) = \sum_{s,t} \beta_{s,t}^{a,b} p(a,b|\tau_s,\omega_t), \tag{10}$$

where the choice of the ancillary states are labeled by s and t. That is, ρ_{AB} is entangled while $J(\rho_{AB}) < 0$ and for any separable state σ_{AB}, we have $J(\sigma_{AB}) \geq 0$. Here the probabilities $p(a,b|\tau_s,\omega_t)$ are obtained from performing two BSMs on the to be witnessed state ρ_{AB} and the ancillary states τ_s and ω_t. That is,

$$p(a,b|\tau_s,\omega_t) = Tr[(M_a \otimes M_b)(\tau_s \otimes \rho_{AB} \otimes \omega_s)], \tag{11}$$

where M_a and M_b represent BSMs performed by Alice and Bob with outcome a and b, respectively.

The MDIEW is capable to witness any entangled state, because it can be constructed from the conventional EW such that $J = tr[W\rho]/4$. Here the coefficient $\beta_{s,t}^{a,b}$ is determined by the choice

of ancillary states, measurement outcomes and the conventional witness W. In the experiment, as only two $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ and $|\Phi^-\rangle = (|00\rangle - |11\rangle)/\sqrt{2}$ out of four BSM outcomes are recorded, we consider the outcomes of a and b to be $+$ and $-$, which refer to $|\Phi^+\rangle$ and $|\Phi^-\rangle$, respectively. Thus, there are four kinds of $\beta_{s,t}^{a,b}$, depending on different values of a and b. By doing this, we improve the efficiency of experiments by four times comparing to the original proposal [10].

$$J = \frac{1}{4}\sum_{s,t}\left(\beta_{s,t}^{++}p(+,+|\tau_s,\omega_t) + \beta_{s,t}^{+-}p(+,-|\tau_s,\omega_t) + \beta_{s,t}^{-+}p(-,+|\tau_s,\omega_t) + \beta_{s,t}^{--}p(-,-|\tau_s,\omega_t)\right) \quad (12)$$

To witness entanglement for the bipartite states defined in Eq. (2) with MDIEW defined in Eq. (12), in total eight different ancillary state pairs should be prepared, and the results are summarized in Table 1.

Table 1: Our MDIEW in the form of Eq. (12) for the bipartite states defined in Eq. (2).

τ_s	ω_t	β_{st}^{++}	$p(+,+\|\tau_s,\omega_t)$	β_{st}^{+-}	$p(+,-\|\tau_s,\omega_t)$
$I/2$	$I/2$	$2\sqrt{3}-2$	$1/16$	$2\sqrt{3}+2$	$1/16$
$\frac{I+\sigma_x}{2}$	$\frac{I+\sigma_x}{2}$	1	$(1-v)/16$	-1	$(1+v)/16$
$\frac{I+\sigma_y}{2}$	$\frac{I+\sigma_y}{2}$	1	$(1-v)/16$	-1	$(1+v)/16$
$\frac{I+\sigma_z}{2}$	$\frac{I+\sigma_z}{2}$	1	$(1-v)/8$	1	$(1-v)/8$
$I/2$	$\frac{I+(\sigma_x+\sigma_y+\sigma_z)/\sqrt{3}}{2}$	$-\sqrt{3}$	$1/16$	0	-
$\frac{I+(\sigma_x+\sigma_y+\sigma_z)/\sqrt{3}}{2}$	$I/2$	$-\sqrt{3}$	$1/16$	0	-
$I/2$	$\frac{I+(-\sigma_x-\sigma_y+\sigma_z)/\sqrt{3}}{2}$	0	-	$-\sqrt{3}$	$1/16$
$\frac{I+(-\sigma_x-\sigma_y+\sigma_z)/\sqrt{3}}{2}$	$I/2$	0	-	$-\sqrt{3}$	$1/16$

Based on this proposal, we design and implement the MDIEW for the bipartite scenario, which is immune to all detection loopholes [11].

2.3. Experiment Results

In the experiment, eight ancillary state pairs $\{\tau_s, \omega_t\}$ are prepared. The states are encoded by tunable waveplates (one HWP sandwiched by two QWPs), which can realize arbitrary single-qubit unitary transformation. Different from directly polarization measurement 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 been collected, where ρ_3^v (ρ_4^v) is the experimentally to-be-witnessed state sent to Alice (Bob).

3. CONCLUSION

In this work, by proposing and realizing the time shift attack to the conventional EW methods, we claim that there do exist severe loopholes in the conventional EW procedure. Meanwhile, as a counter-measure, we design and realize the recently proposed MDIEW methods with six photon entanglement. The experimental results show that the MDIEW is practical for real-life implementation. We further expect that such MDI strategy can be applied to other fields, such as quantum key distribution and quantum secret sharing.

ACKNOWLEDGMENT

This work has been supported by the National Basic Research Program of China Grants No. 2011CB A00300, No. 2011CBA00301, No. 2011CB921300, and No. 2013CB336800, the National Natural Science Foundation of China Grants, and the Chinese Academy of Sciences.

REFERENCES

1. Bennett, C. H. and S. J. Wiesner, "Communication via one-and two-particle operators on Einstein-Podolsky-Rosen states," *Phys. Rev. Lett.*, Vol. 69, No. 20, 2881, 1992.
2. Bennett, C. H., et al., "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Phys. Rev. Lett.*, Vol. 70, No. 13, 1895, 1993.

3. Bennett, C. H. and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Vol. 175, No. 150, 1984.
4. Ekert, A. K., "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, Vol. 67, No. 6, 661–663, 1991.
5. Curty, M., M. Lewenstein, and N. Ltkenhaus, "Entanglement as a precondition for secure quantum key distribution," *Phys. Rev. Lett.*, Vol. 92, No. 21, 217903, 2004.
6. Qi, B., C. H. F. Fung, H. K. Lo, et al., "Time-shift attack in practical quantum cryptosystems," *Quantum Inf. Comput.*, Vol. 7, No. 073, 2007.
7. Makarov, V., A. Anisimov, and J. Skaar, "Effects of detector efficiency mismatch on security of quantum cryptosystems," *Phys. Rev. A*, Vol. 74, No. 2, 022313, 2006.
8. Lo, H. K., M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, Vol. 108, No. 13, 130503, 2012.
9. Buscemi, F., "All entangled quantum states are nonlocal," *Phys. Rev. Lett.*, Vol. 108, No. 20, 200401, 2012.
10. Branciard, C., D. Rosset, Y. C. Liang, et al., "Measurement-device-independent entanglement witnesses for all entangled quantum states," *Phys. Rev. Lett.*, Vol. 110, No. 6, 060405, 2013.
11. Xu, P., X. Yuan, L. K. Chen, et al., "Implementation of a measurement-device-independent entanglement witness," *Phys. Rev. Lett.*, Vol. 112, No. 14, 140506, 2014.