

## ARTICLE

DOI: 10.1038/s42005-018-0011-x

OPEN

# Three-observer classical dimension witness violation with weak measurement

Hong-Wei Li<sup>1,2,3</sup>, Yong-Sheng Zhang<sup>2,3</sup>, Xue-Bi An<sup>2,3</sup>, Zheng-Fu Han<sup>2,3</sup> & Guang-Can Guo<sup>2,3</sup>

Dimension is an important resource in quantum information theory. Based on weak measurement technology, we propose the three-observer dimension witness protocol in a prepare-and-measure setup. By applying the dimension witness inequality based on the quantum random access code and the nonlinear determinant value, we demonstrate that double classical dimension witness violation is achievable if we choose appropriate weak measurement parameters. Analysis of the results will shed new light on the interplay between the multi-observer quantum dimension witness and the weak measurement technology, which can also be applied in the generation of semi-device-independent quantum random numbers and quantum key distribution protocols.

---

<sup>1</sup>Henan Key Laboratory of Quantum Information and Cryptography, Zhengzhou Information Science and Technology Institute, Henan 450000 Zhengzhou, China. <sup>2</sup>Key Laboratory of Quantum Information, University of Science and Technology of China, 230026 Hefei, China. <sup>3</sup>Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, 230026 Hefei, China. Correspondence and requests for materials should be addressed to H.-W.L. (email: [lihow@ustc.edu.cn](mailto:lihow@ustc.edu.cn))

**D**imension is an important resource in quantum information theory, for instance, a high dimensional quantum system can enhance the performance of the quantum computation<sup>1, 2</sup>, quantum entanglement<sup>3</sup>, quantum communication complexity<sup>4</sup> and others, and it can also reduce the security of certain practical quantum key distribution systems<sup>5</sup>. To estimate the lower bound of the dimensions of a physical system, quantum dimension witness has been proposed and experimentally realized<sup>6-9</sup>, which has important applications in the semi-device-independent quantum key distribution and quantum random number generation<sup>10-15</sup>. Until now, it has been demonstrated that two-observer classical dimension witness violation can be achieved with the Bell inequality test, quantum random access code test, and determinant value test respectively<sup>16-18</sup>, but whether the multi-observer classical dimension witness violation can be obtained or not is still an open question.

Similar to a quantum dimension witness, quantum nonlocality also plays a fundamental role in quantum information theory, which can be used to guarantee the security of device-independent quantum information protocols<sup>19, 20</sup>. In a two-observer system, two observers can perform independent measurements on their subsystem to test the Clauser-Horne-Shimony-Holt (CHSH) inequality<sup>21</sup>, the violation of which certifies quantum nonlocality. Recently, it has been demonstrated that nonlocality sharing among three observers can be established by applying weak measurement technology<sup>22-24</sup>, which demonstrates that subsequent measurements can not be described by using classical probability distributions.

Inspired by the work of sharing nonlocality with weak measurement technology, three-observer classical dimension witness violation will be analyzed in this paper, in which we analyze the dimension witness inequality based on the quantum random access code and the nonlinear determinant value. The analysis result indicate that double classical dimension witness violations can be realized. More interestingly, we demonstrate local and global randomness generation in the three-observer protocol, and the analysis method can also be applied to future multi-observer quantum network studies.

**Results**

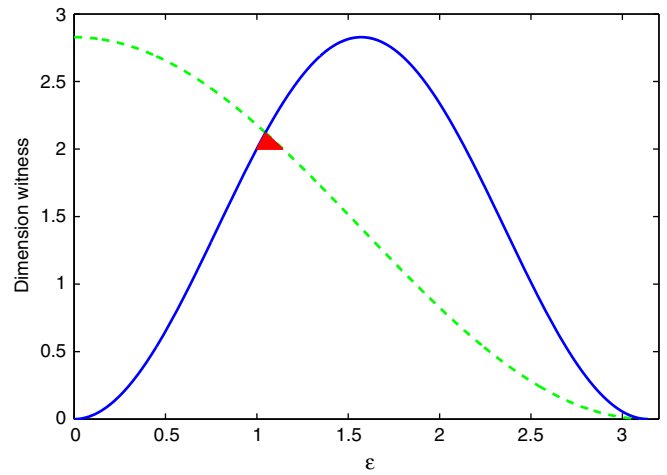
**Quantum dimension witness based on quantum random access code.** The first quantum dimension witness inequality based on the quantum random access code in the two-observer system is given by<sup>10, 11, 18</sup>

$$W_1 = p(1|000) + p(1|001) + p(1|010) - p(1|011) - p(1|100) + p(1|101) - p(1|110) - p(1|111). \tag{1}$$

In the two-dimensional Hilbert space, it has been proved that the upper bound of the classical dimension witness value  $W_1$  is 2, while the upper bound of the quantum dimension witness value  $W_1$  is  $2\sqrt{2}$ . We will apply this dimension witness equation to analyze the dimension witness values between Alice and Bob  $W_{1AB}$  and between Alice and Charlie  $W_{1AC}$ .

Based on the state preparation and measurement model given in the Method section, the dimension witness value between Alice and Bob is given by

$$W_{1AB} = \sqrt{2}(\cos(\epsilon) + 1). \tag{2}$$



**Fig. 1** Three-observer classical dimension witness violation based on the quantum random access code test.  $\epsilon$  is the weak measurement parameter. The dashed green line corresponds to the quantum dimension witness value  $W_{1AB}$ , solid blue line corresponds to the quantum dimension witness value  $W_{1AC}$ , and red area corresponds to the double classical dimension witness violation.

The dimension witness value between Alice and Charlie is given by

$$W_{1AC} = 2\sqrt{2} \sin^2(\epsilon). \tag{3}$$

Note that  $\epsilon = 0$  indicates  $W_{1AB} = 2\sqrt{2}$  and  $W_{1AC} = 0$ , which demonstrates that Charlie’s quantum state has no interaction with Bob’s system. In this case, only  $W_{1AB}$  violates the classical upper bound, which is reduced to a two-observer system (Alice-Bob). Similarly,  $\epsilon = \frac{\pi}{2}$  indicates  $W_{1AB} = 0$  and  $W_{1AC} = 2\sqrt{2}$ , which is reduced to a two-observer system (Alice-Charlie). Thus, our protocol is more general compared with the previous 2-observer protocols, which sheds new light on the dimension witness in the network environment.

The detailed quantum dimension witness values  $W_{1AB}$  and  $W_{1AC}$  with different weak measurement parameter  $\epsilon$  values are given in Fig. 1. The analysis results indicate that double classical dimension witness violations ( $\min\{W_{1AB}, W_{1AC}\} > 2$ ) can be obtained if the weak measurement parameter  $\epsilon$  satisfies  $\arcsin\left(\sqrt{\frac{1}{2}}\right) < \epsilon < \arccos(\sqrt{2} - 1)$ .

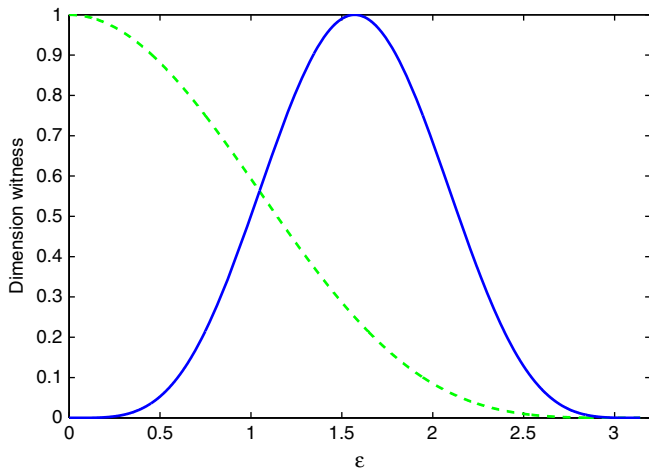
**Quantum dimension witness based on the determinant value.**

The second quantum dimension witness inequality based on the nonlinear determinant value test in the two-observer system is given by<sup>13, 14</sup>

$$W_2 = \begin{vmatrix} p(1|000) - p(1|010) & p(1|100) - p(1|110) \\ p(1|001) - p(1|011) & p(1|101) - p(1|111) \end{vmatrix}. \tag{4}$$

Assuming that the state preparation and measurement devices are independent, it has been proved that this nonlinear dimension witness can tolerate an arbitrarily low detection efficiency. In the two-dimensional Hilbert space, the upper bound of the quantum dimension witness value is 1, while the classical dimension witness value is 0. Similar to the previous subsection, the dimension witness values between Alice and Bob  $W_{2AB}$  and between Alice and Charlie  $W_{2AC}$  can be analyzed.

Based on the state preparation and measurement model given in the Method section, the dimension witness value between Alice



**Fig. 2** Three-observer classical dimension witness violation based on the determinant value. The dashed green line corresponds to the quantum dimension witness value  $W_{2AB}$ , and solid blue line corresponds to the quantum dimension witness value  $W_{2AC}$ .

and Bob is given by

$$W_{2AB} = \left(\frac{1}{2} \cos(\epsilon) + \frac{1}{2}\right)^2. \tag{5}$$

The dimension witness value between Alice and Charlie is given by

$$W_{2AC} = \sin^4(\epsilon). \tag{6}$$

Note that  $\epsilon=0$  indicates  $W_{2AB}=1$  and  $W_{2AC}=0$ , which demonstrates that Charlie’s quantum state has no interaction with Bob’s system. In this case, only  $W_{2AB}$  violates the classical upper bound, which is reduced to a two-observer system (Alice-Bob).

The detailed quantum dimension witness values  $W_{2AB}$  and  $W_{2AC}$  with different weak measurement parameters  $\epsilon$  are given in Fig. 2.

The analysis result demonstrates that double classical dimension witness violations ( $W_{2AB} > 0$ ,  $W_{2AC} > 0$ ) can be obtained if  $0 < \epsilon < \pi$ . However, since Bob’s system may be influenced by Alice and Charlie’s system, the security of the measurement outcome  $b$  should be guaranteed by considering the double classical dimension witness violation  $W_{2AB} > 0$  and  $W_{2AC} > 0$ .

**Semi-device-independent random number generator.** The classical dimension witness violation can generate semi-device-independent quantum random numbers, for which we can only assume knowledge of the dimension of the underlying physical system, but otherwise nothing about the quantum devices. The generated random numbers in our protocol are the measurement outcomes  $b$  and  $c$ , and the eavesdropper can not guess the measurement outcomes even if the state preparation and measurement devices are imperfect.

Randomness generation can be divided into global randomness and the local randomness, where global randomness must analyze the global conditional probability distribution  $p(b,c|x,y,z)$ , while local randomness must analyze the local conditional probability distribution  $p(b|x,y)$ . With the given conditional probability distributions, the random number generation efficiency can be

estimated by following min-entropy functions<sup>25</sup>

$$H_{\min 1} = -\log_2 \left[ \frac{1}{16} \sum_{x,y,z} \max_{b,c} (p(b,c|x,y,z)) \right], \tag{7}$$

$$H_{\min 2} = -\log_2 \left[ \frac{1}{8} \sum_{x,y} \max_b (p(b|x,y)) \right].$$

To analyze the global randomness generation efficiency  $H_{\min 1}$ , the maximal guessing probability  $\frac{1}{16} \sum_{x,y,z} \max_{b,c} (p(b,c|x,y,z))$  can be estimated by

$$\begin{aligned} & \frac{1}{16} \sum_{x,y,z} \max_{b,c} p(b,c|x,y,z) \\ &= \frac{1}{16} \sum_{x,y,z} \max_{b,c} p(b|x,y,z) p(c|x,y,z,b) \\ &= \frac{1}{16} \sum_{x,y,z} \max_{b,c} (p(b|x,y,z) p(c|x,z)) \\ &\leq \left[ \frac{1}{8} \sum_{x,z} \max_c p(c|x,z) \right] \times \max_{b,x,y,z} (p(b|x,y,z)), \end{aligned} \tag{8}$$

where the second line is based on the condition for which Charlie’s measurement outcome  $c$  can not be effected by Bob, and the corresponding randomness generation efficiency  $H_{\min 1}$  is given by

$$H_{\min 1} \geq -\log_2 \left[ \frac{1}{8} \sum_{x,z} \max_c p(c|x,z) \right] - \log_2 [\max_{b,x,y,z} (p(b|x,y,z))], \tag{9}$$

where the first part is the randomness generation in Charlie’s side, and the second part is the randomness generation in Bob’s side.

In the two-observer system, with a given random access code based dimension witness value  $W_1$ , the relationship between  $W_1$  and the randomness generation efficiency  $H_{\min 2}(W_1)$ <sup>26</sup> is given by

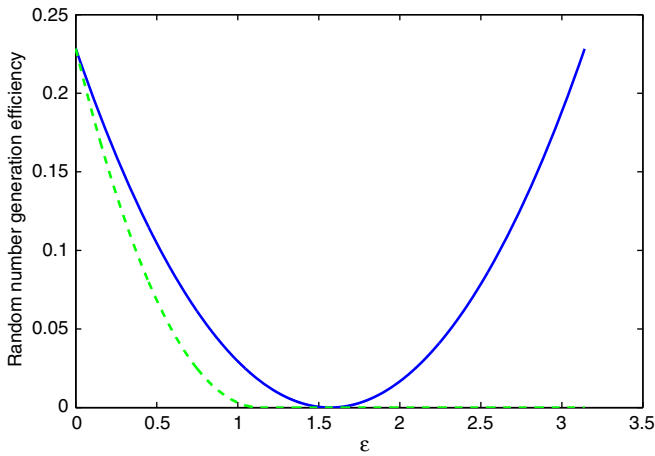
$$H_{\min 2}(W_1) = -\log_2 \left( \frac{1}{2} + \frac{1}{2} \sqrt{\frac{1 + \sqrt{1 - \left(\frac{W_1^2 - 4}{4}\right)^2}}{2}} \right). \tag{10}$$

However, the eavesdropper can apply Charlie’s input parameter  $z$  to guess Bob’s measurement outcome  $b$ , thus the previous method can not be directly applied in our protocol. To estimate the local randomness generation in Bob’s side, we will estimate the dimension witness value between Alice and Bob  $W_{1AB(z)}$  with different input random number  $z \in \{0,1\}$  as follows

$$W_{1AB(z=0)} = W_{1AB(z=1)} = \sqrt{2} \cos(\epsilon) + \sqrt{2}, \tag{11}$$

with the detailed calculation is given in the Method section, and the corresponding local randomness generation efficiency in Bob’s side is  $H_{\min 2}(W_1 = \sqrt{2} \cos(\epsilon) + \sqrt{2})$ .

With the given determinate value based on dimension witness  $W_2$  in the two-observer system, the relationship between the quantum dimension witness value  $W_2$  and the randomness



**Fig. 3** Local random number generation efficiency with different weak measurement parameters  $\epsilon$ . The dashed green line corresponds to  $H''_{\min 2}(W_1 = \sqrt{2} \cos(\epsilon) + \sqrt{2})$ , and solid blue line corresponds to  $H''_{\min 2}(W_2 = \cos(\epsilon))$ .

generation efficiency  $H''_{\min 2}(W_2)^{13}$  is given by

$$H''_{\min 2}(W_2) = -\log_2 \left( \frac{1}{2} + \frac{1}{2} \sqrt{\frac{1 + \sqrt{1 - W_2^2}}{2}} \right). \quad (12)$$

Similar to the previous calculation, the dimension witness value between Alice and Bob  $W_{2AB(z)}$  with different input random number  $z$  can be given by

$$W_{2AB(z=0)} = W_{2AB(z=1)} = \cos(\epsilon), \quad (13)$$

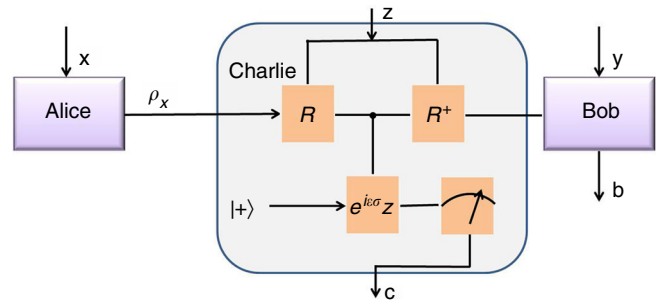
with the detailed calculation is given in the Method section, and the corresponding local randomness generation efficiency in Bob's side is  $H''_{\min 2}(W_2 = \cos(\epsilon))$ .

Based on the previous analysis result, the detailed local randomness generation efficiency with different weak measurement parameter  $\epsilon$  values are given in Fig. 3. Note that the local random number generation in Charlie's side can be directly estimated by the two-observer protocol. Thus double local randomness generation can be realized if we choose an appropriate weak measurement parameter.

Comparing with the random access code based protocol, the determinant value based protocol can provide the double classical dimension witness violation except the special case ( $\epsilon = k\pi, k = 0, 1, 2, \dots$ ), thus it has the advantage in the experimental realization. However, the disadvantage is that this protocol has a strong assumption that the state preparation and measurement devices are independent.

**Discussion**

We proposed a three-observer dimension witness protocol, where the weak measurement technology was applied to analyze the double classical dimension witness violations. The results of our analysis shed new light on understanding the quantum dimension witness in the network environment. The three-observer dimension witness protocol can be assumed to be a sequential measurement protocol, and it will be interesting to analyze a higher dimensional multi-observer quantum system with sequential measurement<sup>27</sup> technology. We demonstrated the randomness generation in the three-observer protocol, and the analysis results demonstrate that weak measurement may have significant applications in multi-observer semi-device-independent quantum



**Fig. 4** Analysis model of three-observer classical dimension witness violation. Alice prepares the two-dimensional quantum state  $\rho_x$ , and Bob and Charlie apply the two-dimensional strong measurement and weak measurement respectively

information theory. This study also provides tremendous motivation for further experimental research.

**Methods**

**Weak measurement protocol.** Weak measurement is a powerful method to extract less information about a system with smaller disturbance<sup>28</sup>, which has proven to be useful for signal amplification, state tomography, solving quantum paradoxes and others<sup>29-33</sup>. In this work, we use the weak measurement definition given in refs. 22-24, and the corresponding analysis model is given in Fig. 4.

There are three observers Alice, Bob and Charlie in the analysis model, and the purpose of our protocol is to establish double classical dimension witness violations under the two-dimensional Hilbert space restriction. More precisely, Alice prepares the two-dimensional quantum state  $\rho_x \in C^2$  and sends it through the quantum channel with a different classical input random number  $x \in \{00,01,10,11\}$ . Then, Charlie receives the quantum state and applies the following operation with the input random number  $z \in \{0,1\}$

$$R_z^+ |0\rangle = |\omega_z\rangle, R_z^+ |1\rangle = |\omega_z^\perp\rangle, \quad (14)$$

where the above operation illustrates that the rotation maps the initial Hilbert space basis of  $\{|0\rangle, |1\rangle\}$  to a new basis of  $\{|\omega_z\rangle, |\omega_z^\perp\rangle\}$  depending on the given  $z$  value. Charlie also has an two-dimensional ancillary quantum state  $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$  in the quantum channel, and then, the following control operation is applied when Charlie receives the quantum state  $|1\rangle$

$$e^{i\epsilon\sigma_z} = \begin{pmatrix} e^{i\epsilon} & 0 \\ 0 & e^{-i\epsilon} \end{pmatrix}. \quad (15)$$

where  $\epsilon$  is the weak measurement parameter. If Charlie receives the quantum state  $|0\rangle$ , he will apply the identity operation  $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ , thus the total unitary operation in Charlie's side can be given by

$$\begin{aligned} U &= R_z^+ |0\rangle\langle 0| R_z \otimes I + R_z^+ |1\rangle\langle 1| R_z \otimes e^{i\epsilon\sigma_z} \\ &= |\omega_z\rangle\langle \omega_z| \otimes I + |\omega_z^\perp\rangle\langle \omega_z^\perp| \otimes e^{i\epsilon\sigma_z} \\ &= W_B^{+\perp z} \otimes I + W_B^{-z} \otimes e^{i\epsilon\sigma_z}, \end{aligned} \quad (16)$$

where we define  $W_B^{+\perp z} = |\omega_z\rangle\langle \omega_z|$ ,  $W_B^{-z} = |\omega_z^\perp\rangle\langle \omega_z^\perp|$ . Note that Charlie will apply the identity operation  $I$  if the weak measurement parameter  $\epsilon$  is 0, which can be simply proved since  $W_B^{+\perp z} \otimes I + W_B^{-z} \otimes I = I$ . In this case, Charlie will only obtain the initial ancillary quantum state  $|+\rangle$  after the control operation, which demonstrates that Charlie can not gain any information about Alice's state  $\rho_x$ , and there is no interaction introduced by Charlie correspondingly.

To prove the dimension witness in the three-observer system, we should analyze the density matrix to illustrate Bob and Charlie's system. The initial quantum state can be given by

$$\rho_{BCx} = \rho_x \otimes |+\rangle\langle +|. \quad (17)$$

By applying the previous unitary transformation  $U$ , the quantum state  $\rho_{BCx}$  will be transformed into

$$\begin{aligned} \rho'_{BCx} &= U\rho_{BCx}U^\dagger \\ &= W_B^{+z} \otimes I\rho_{BCx}W_B^{+z} \otimes I \\ &\quad + W_B^{+z} \otimes I\rho_{BCx}W_B^{-z} \otimes e^{-ie\sigma_z} \\ &\quad + W_B^{-z} \otimes e^{ie\sigma_z}\rho_{BCx}W_B^{+z} \otimes I \\ &\quad + W_B^{-z} \otimes e^{ie\sigma_z}\rho_{BCx}W_B^{-z} \otimes e^{-ie\sigma_z}. \end{aligned} \quad (18)$$

The quantum state  $\rho'_{Bx} = \text{Tr}_C\rho'_{BCx}$  will be transmitted to Bob, as follows

$$\begin{aligned} \rho'_{Bx} &= \text{Tr}_C\rho'_{BCx} \\ &= W_B^{+z}\rho_x W_B^{+z} + W_B^{-z}\rho_x W_B^{-z} \\ &\quad + \cos\epsilon(W_B^{+z}\rho_x W_B^{-z} + W_B^{-z}\rho_x W_B^{+z}) \\ &= (1 - \cos\epsilon)(W_B^{+z}\rho_x W_B^{+z} + W_B^{-z}\rho_x W_B^{-z}) \\ &\quad + \cos\epsilon\rho_x. \end{aligned} \quad (19)$$

Similarly, the quantum state  $\rho'_{Cx} = \text{Tr}_B\rho'_{BCx}$  will be transmitted to Charlie, as follows

$$\begin{aligned} \rho'_{Cx} &= \text{Tr}_B\rho'_{BCx} \\ &= \text{Tr}_B(W_B^{+z}\rho_x)|+\rangle\langle+| \\ &\quad + \text{Tr}_B(W_B^{-z}\rho_x)e^{ie\sigma_z}|+\rangle\langle+|e^{-ie\sigma_z}. \end{aligned} \quad (20)$$

After receiving the quantum state  $\rho'_{Bx}$ , Bob will apply the two-dimensional projective measurement depending on the input random number  $y \in \{0,1\}$ . If Bob's input random number is 0, the corresponding measurement basis in Bob's side is given by

$$\{|\nu_0\rangle\langle\nu_0|, |\nu_0^\perp\rangle\langle\nu_0^\perp|\}. \quad (21)$$

If Bob's input is 1, Bob's measurement basis is

$$\{|\nu_1\rangle\langle\nu_1|, |\nu_1^\perp\rangle\langle\nu_1^\perp|\}, \quad (22)$$

where the measurement outcomes  $|\nu_0\rangle\langle\nu_0|$  and  $|\nu_1\rangle\langle\nu_1|$  indicate classical bit 1, and the measurement outcomes  $|\nu_0^\perp\rangle\langle\nu_0^\perp|$  and  $|\nu_1^\perp\rangle\langle\nu_1^\perp|$  indicate classical bit  $-1$ .

After receiving the quantum state  $\rho'_{Cx}$ , Charlie will apply the two-dimensional projective measurement

$$\{|t\rangle\langle t|, |t^\perp\rangle\langle t^\perp|\}, \quad (23)$$

where the measurement outcomes  $|t\rangle\langle t|$  and  $|t^\perp\rangle\langle t^\perp|$  respectively indicate the classical bit 1 and  $-1$ . Before the state measurement, Charlie randomly chooses rotation  $\{R_z, R_z^\perp\}$  with respect to the input random number  $z \in \{0,1\}$ .

In the case where the weak measurement parameter  $\epsilon$  is 0, there is no interaction on Charlie's side, and then, Charlie's density matrix will be transformed into  $\rho'_{Cx} = \text{Tr}_B(W_B^{+z}\rho_x + W_B^{-z}\rho_x)|+\rangle\langle+| = |+\rangle\langle+|$ , and Bob's density matrix will be transformed into  $\rho_{Bx} = \rho_x$ . In the following section, we will focus on the situation  $0 \leq \epsilon \leq \pi$ , and analyze the interaction introduced by the weak measurement, which can be used to obtain the information gain in Charlie's side.

The general representation of a qubit can be illustrated by using the density matrix formalism  $\frac{I + \vec{r}\cdot\vec{\sigma}}{2}$ , where  $\vec{\sigma}$  is the Pauli matrix vector  $(\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix})$ , and  $\vec{r} = (r_x, r_y, r_z)$  is a real three-dimensional vector such that  $\|\vec{r}\| \leq 1$ , thus the conditional probability

distribution to illustrate Alice and Bob's system can be given by

$$\begin{aligned} p(b|xy) &= \sum_z p(z)\text{Tr}(B_y^b \rho'_{Bx}(z)) \\ &= \frac{1}{2}(1 - \cos\epsilon) \sum_z p(z)b\omega_z \cdot \nu_y \times \omega_z \cdot \rho_x \\ &\quad + \frac{1}{2}\cos\epsilon(1 + b\nu_y \cdot \rho_x) + \frac{1}{2}(1 - \cos\epsilon), \end{aligned} \quad (24)$$

where  $B_y^b$  is the measurement operator acting on the two-dimensional Hilbert space with input parameter  $y$  and output parameter  $b$  by considering the prepared quantum state  $\rho'_{Bx}(z)$ . The conditional probability distribution to illustrate Alice and Charlie's system is given by

$$\begin{aligned} p(c|xz) &= \text{Tr}(C^c \rho'_{Cx}(z)) \\ &= \frac{1}{2}(1 + \omega_z \cdot \rho_x)(1 + c - c \sin^2\epsilon), \end{aligned} \quad (25)$$

where  $C^c$  is the measurement operator acting on the two-dimensional Hilbert space to obtain the measurement outcome  $c$  with the state  $\rho'_{Cx}(z)$ .

Based on the previous observed statistics  $p(b|xy)$  and  $p(c|xz)$ , we can calculate the dimension witness value between Alice and Bob and between Alice and Charlie respectively.

### Three-observer dimension witness based on quantum random access code.

The general representation of a qubit can be illustrated by using the density matrix formalism  $\frac{I + \vec{r}\cdot\vec{\sigma}}{2}$ , where  $\vec{\sigma}$  is the Pauli matrix vector

$(\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix})$ , and  $\vec{r} = (r_x, r_y, r_z)$  is a real three-dimensional vector such that  $\|\vec{r}\| \leq 1$ . In the following section, we apply  $\vec{r} = (r_x, r_y, r_z)$  to demonstrate the quantum state  $\rho_x (x \in \{00,01,10,11\})$ ,  $|\nu_y\rangle\langle\nu_y| (y \in \{0,1\})$ ,  $|\omega_z\rangle\langle\omega_z| (z \in \{0,1\})$  and  $|t\rangle\langle t|$ .

To prove the double classical dimension witness violation under Eq. (1), we propose the following density matrix prepared in Alice's side

$$\begin{aligned} \rho_{00} &= \left(\frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}}\right), \\ \rho_{01} &= \left(-\frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}}\right), \\ \rho_{10} &= \left(\frac{1}{\sqrt{2}}, 0, -\frac{1}{\sqrt{2}}\right), \\ \rho_{11} &= \left(-\frac{1}{\sqrt{2}}, 0, -\frac{1}{\sqrt{2}}\right). \end{aligned} \quad (26)$$

The measurement operator in Bob's side is given by

$$\begin{aligned} \nu_0 &= (0, 0, 1), \\ \nu_1 &= (1, 0, 0). \end{aligned} \quad (27)$$

The measurement operator in Charlie's side is given by

$$t = (1, 0, 0). \quad (28)$$

The rotation operator in Charlie's side is given by

$$\begin{aligned} \omega_0 &= (0, 0, 1), \\ \omega_1 &= (1, 0, 0). \end{aligned} \quad (29)$$

Based on the previous state preparation and measurement operator, we can calculate the corresponding conditional probability distribution  $p(b = 1|x,y)_{AB}$  with

different classical input random numbers  $x \in \{00,01,10,11\}$  and  $y \in \{0,1\}$ .

$$\begin{aligned}
 p(1|000)_{AB} &= \frac{\sqrt{2}}{8} \cos(\epsilon) + \frac{4+\sqrt{2}}{8}, \\
 p(1|001)_{AB} &= \frac{\sqrt{2}}{8} \cos(\epsilon) + \frac{4+\sqrt{2}}{8}, \\
 p(1|010)_{AB} &= \frac{\sqrt{2}}{8} \cos(\epsilon) + \frac{4+\sqrt{2}}{8}, \\
 p(1|011)_{AB} &= -\frac{\sqrt{2}}{8} \cos(\epsilon) + \frac{4-\sqrt{2}}{8}, \\
 p(1|100)_{AB} &= -\frac{\sqrt{2}}{8} \cos(\epsilon) + \frac{4-\sqrt{2}}{8}, \\
 p(1|101)_{AB} &= \frac{\sqrt{2}}{8} \cos(\epsilon) + \frac{4+\sqrt{2}}{8}, \\
 p(1|110)_{AB} &= -\frac{\sqrt{2}}{8} \cos(\epsilon) + \frac{4-\sqrt{2}}{8}, \\
 p(1|111)_{AB} &= -\frac{\sqrt{2}}{8} \cos(\epsilon) + \frac{4-\sqrt{2}}{8}.
 \end{aligned} \tag{30}$$

By applying the previous conditional probability distributions  $p(b=1|x,y)_{AB}$ , the dimension witness value<sup>10, 11, 18</sup> between Alice and Bob is given by

$$\begin{aligned}
 W_{1AB} &= p(1|000)_{AB} + p(1|001)_{AB} + p(1|010)_{AB} \\
 &\quad - p(1|011)_{AB} - p(1|100)_{AB} + p(1|101)_{AB} \\
 &\quad - p(1|110)_{AB} - p(1|111)_{AB} \\
 &= \sqrt{2}(\cos(\epsilon) + 1).
 \end{aligned} \tag{31}$$

Based on the previous state preparation and measurement operator, we can calculate the corresponding conditional probability distribution  $p(b=1|x,z)_{AC}$  as follows

$$\begin{aligned}
 p(1|000)_{AC} &= \frac{2+\sqrt{2}}{4} \sin^2(\epsilon), \\
 p(1|001)_{AC} &= \frac{2+\sqrt{2}}{4} \sin^2(\epsilon), \\
 p(1|010)_{AC} &= \frac{2+\sqrt{2}}{4} \sin^2(\epsilon), \\
 p(1|011)_{AC} &= \frac{2-\sqrt{2}}{4} \sin^2(\epsilon), \\
 p(1|100)_{AC} &= \frac{2-\sqrt{2}}{4} \sin^2(\epsilon), \\
 p(1|101)_{AC} &= \frac{2+\sqrt{2}}{4} \sin^2(\epsilon), \\
 p(1|110)_{AC} &= \frac{2-\sqrt{2}}{4} \sin^2(\epsilon), \\
 p(1|111)_{AC} &= \frac{2+\sqrt{2}}{4} \sin^2(\epsilon).
 \end{aligned} \tag{32}$$

By applying the previous conditional probability distributions  $p(b=1|x,y)_{AC}$ , the dimension witness value between Alice and Charlie is given by

$$W_{1AC} = 2\sqrt{2} \sin^2(\epsilon). \tag{33}$$

To prove local randomness generation in Bob's side, we analyze the dimension witness value  $W_{1ABz}$  with different input weak measurement parameters  $z \in \{0,1\}$ .

In the case of  $z=0$ , we can obtain the corresponding conditional probability distributions  $p(b=1|x,y)_{AB,z=0}$  as follows

$$\begin{aligned}
 p(1|000)_{AB,z=0} &= \frac{2+\sqrt{2}}{4}, \\
 p(1|001)_{AB,z=0} &= \frac{2+\sqrt{2}\cos(\epsilon)}{4}, \\
 p(1|010)_{AB,z=0} &= \frac{2+\sqrt{2}}{4}, \\
 p(1|011)_{AB,z=0} &= \frac{2-\sqrt{2}\cos(\epsilon)}{4}, \\
 p(1|100)_{AB,z=0} &= \frac{2-\sqrt{2}}{4}, \\
 p(1|101)_{AB,z=0} &= \frac{2+\sqrt{2}\cos(\epsilon)}{4}, \\
 p(1|110)_{AB,z=0} &= \frac{2-\sqrt{2}}{4}, \\
 p(1|111)_{AB,z=0} &= \frac{2-\sqrt{2}\cos(\epsilon)}{4}.
 \end{aligned} \tag{34}$$

By applying the previous conditional probability distributions  $p(b=1|x,y)_{AB,z=0}$ , the dimension witness value between Alice and Bob is given by

$$W_{1AB,z=0} = \sqrt{2} \cos(\epsilon) + \sqrt{2}. \tag{35}$$

In the case of  $z=1$ , we obtain the corresponding conditional probability distribution  $p(b=1|x,y)_{AB,z=1}$  as follows

$$\begin{aligned}
 p(1|000)_{AB,z=1} &= \frac{2+\sqrt{2}\cos(\epsilon)}{4}, \\
 p(1|001)_{AB,z=1} &= \frac{2+\sqrt{2}}{4}, \\
 p(1|010)_{AB,z=1} &= \frac{2+\sqrt{2}\cos(\epsilon)}{4}, \\
 p(1|011)_{AB,z=1} &= \frac{2-\sqrt{2}}{4}, \\
 p(1|100)_{AB,z=1} &= \frac{2-\sqrt{2}\cos(\epsilon)}{4}, \\
 p(1|101)_{AB,z=1} &= \frac{2+\sqrt{2}}{4}, \\
 p(1|110)_{AB,z=1} &= \frac{2-\sqrt{2}\cos(\epsilon)}{4}, \\
 p(1|111)_{AB,z=1} &= \frac{2-\sqrt{2}}{4}.
 \end{aligned} \tag{36}$$

By applying the previous conditional probability distributions  $p(b=1|x,y)_{AB,z=1}$ , the dimension witness value between Alice and Bob is given by

$$W_{1AB,z=1} = \sqrt{2} \cos(\epsilon) + \sqrt{2}. \tag{37}$$

**Three-observer dimension witness based on determinant value.** To prove the double classical dimension witness violation under Eq. (4), we propose the following density matrix preparation in Alice's side

$$\begin{aligned}
 \rho_{00} &= (0, 0, 1), \\
 \rho_{01} &= (0, 0, -1), \\
 \rho_{10} &= (1, 0, 0), \\
 \rho_{11} &= (-1, 0, 0).
 \end{aligned} \tag{38}$$

The measurement operator in Bob's side is given by

$$\begin{aligned}
 \nu_0 &= (0, 0, 1), \\
 \nu_1 &= (1, 0, 0).
 \end{aligned} \tag{39}$$

The measurement operator in Charlie's side is given by

$$t = (1, 0, 0). \tag{40}$$

The rotation operator in Charlie's side is given by

$$\begin{aligned}
 \omega_0 &= (0, 0, 1), \\
 \omega_1 &= (1, 0, 0).
 \end{aligned} \tag{41}$$

Note that the state preparation and measurement operator are the same as the Bennett and Brassard 1984 (BB84) quantum key distribution protocol<sup>34</sup>, but the weak measurement model may disturb Alice's quantum state with the different weak measurement parameter  $\epsilon$ , and this disturbance can be detected by the quantum bit error rate.

Based on the previous state preparation and measurement, we can calculate the corresponding conditional probability distribution  $p(b=1|x,y)_{AB}$  as follows

$$\begin{aligned}
 p(1|000)_{AB} &= \frac{1}{4} \cos(\epsilon) + \frac{3}{4}, \\
 p(1|001)_{AB} &= \frac{1}{2}, \\
 p(1|010)_{AB} &= -\frac{1}{4} \cos(\epsilon) + \frac{1}{4}, \\
 p(1|011)_{AB} &= \frac{1}{2}, \\
 p(1|100)_{AB} &= \frac{1}{2}, \\
 p(1|101)_{AB} &= \frac{1}{4} \cos(\epsilon) + \frac{3}{4}, \\
 p(1|110)_{AB} &= \frac{1}{2}, \\
 p(1|111)_{AB} &= -\frac{1}{4} \cos(\epsilon) + \frac{1}{4}.
 \end{aligned} \tag{42}$$

By applying the previous conditional probability distributions  $p(b=1|x,y)_{AB}$ , the dimension witness value<sup>13, 14</sup> between Alice and Bob is given by

$$\begin{aligned}
 W_{2AB} &= \left| \begin{array}{cc} p(1|000)_{AB} - p(1|010)_{AB} & p(1|100)_{AB} - p(1|110)_{AB} \\ p(1|001)_{AB} - p(1|011)_{AB} & p(1|101)_{AB} - p(1|111)_{AB} \end{array} \right| \\
 &= \left( \frac{1}{2} \cos(\epsilon) + \frac{1}{2} \right)^2.
 \end{aligned} \tag{43}$$

Based on the previous state preparation and measurement, we can also calculate the corresponding conditional probability distribution  $p(b=1|x,z)_{AC}$  as follows

$$\begin{aligned} p(1|000)_{AC} &= \sin^2(\epsilon), \\ p(1|001)_{AC} &= \frac{1}{2}\sin^2(\epsilon), \\ p(1|010)_{AC} &= 0, \\ p(1|011)_{AC} &= \frac{1}{2}\sin^2(\epsilon), \\ p(1|100)_{AC} &= \frac{1}{2}\sin^2(\epsilon), \\ p(1|101)_{AC} &= \sin^2(\epsilon), \\ p(1|110)_{AC} &= \frac{1}{2}\sin^2(\epsilon), \\ p(1|111)_{AC} &= 0. \end{aligned} \quad (44)$$

By applying the previous conditional probability distributions  $p(b=1|x,y)_{AC}$ , the dimension witness value between Alice and Charlie is given by

$$W_{2AC} = \sin^4(\epsilon). \quad (45)$$

To prove local randomness generation in Bob's side, we will analyze the dimension witness value  $W_{2ABz}$  with different input weak measurement parameters  $z \in \{0,1\}$ .

In the case of  $z=0$ , we can obtain the corresponding conditional probability distribution  $p(b=1|x,y)_{AB,z=0}$  as follows

$$\begin{aligned} p(1|000)_{AB,z=0} &= 1, \\ p(1|001)_{AB,z=0} &= \frac{1}{2}, \\ p(1|010)_{AB,z=0} &= 0, \\ p(1|011)_{AB,z=0} &= \frac{1}{2}, \\ p(1|100)_{AB,z=0} &= \frac{1}{2}, \\ p(1|101)_{AB,z=0} &= \frac{1+\cos(\epsilon)}{2}, \\ p(1|110)_{AB,z=0} &= \frac{1}{2}, \\ p(1|111)_{AB,z=0} &= \frac{1-\cos(\epsilon)}{2}. \end{aligned} \quad (46)$$

Based on the previous conditional probability distributions  $p(b=1|x,y)_{AB,z=0}$ , the dimension witness value between Alice and Bob is given by

$$W_{2AB,z=0} = \cos(\epsilon). \quad (47)$$

In the case of  $z=1$ , we can obtain the corresponding conditional probability distribution  $p(b=1|x,y)_{AB,z=1}$  as follows

$$\begin{aligned} p(1|000)_{AB,z=1} &= \frac{1+\cos(\epsilon)}{2}, \\ p(1|001)_{AB,z=1} &= \frac{1}{2}, \\ p(1|010)_{AB,z=1} &= \frac{1-\cos(\epsilon)}{2}, \\ p(1|011)_{AB,z=1} &= \frac{1}{2}, \\ p(1|100)_{AB,z=1} &= \frac{1}{2}, \\ p(1|101)_{AB,z=1} &= 1, \\ p(1|110)_{AB,z=1} &= \frac{1}{2}, \\ p(1|111)_{AB,z=1} &= 0. \end{aligned} \quad (48)$$

By applying the previous conditional probability distributions  $p(b=1|x,y)_{AB,z=1}$ , the dimension witness value between Alice and Bob is given by

$$W_{2AB,z=1} = \cos(\epsilon). \quad (49)$$

**Code availability.** Source codes of the plots are available from the corresponding authors on request.

**Data availability.** The data that support the findings of this study are available from the corresponding authors on request.

Received: 18 October 2017 Accepted: 5 February 2018  
Published online: 22 March 2018

## References

- Shor, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comp.* **26**, 1484–1509 (1997).
- Grover, L. K. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.* **79**, 325 (1997).
- Collins, D. et al. Bell inequalities for arbitrarily high-dimensional systems. *Phys. Rev. Lett.* **88**, 040404 (2002).
- Tavakoli, A. et al. Dimensional discontinuity in quantum communication complexity at dimension seven. *Phys. Rev. A* **95**, 020302 (2017).
- Scarani, V. et al. The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301 (2009).
- Hendrych, M. et al. Experimental estimation of the dimension of classical and quantum systems. *Nat. Phys.* **8**, 588–591 (2012).
- Navascues, M. & Vertesi, T. Bounding the set of finite dimensional quantum correlations. *Phys. Rev. Lett.* **115**, 020501 (2015).
- Ahrens, J. et al. Experimental device-independent tests of classical and quantum dimensions. *Nat. Phys.* **8**, 592–595 (2012).
- Brunner, N., Navascues, M. & Vertesi, T. Dimension witnesses and quantum state discrimination. *Phys. Rev. Lett.* **110**, 150501 (2013).
- Li, H.-W. et al. Semi-device-independent random-number expansion without entanglement. *Phys. Rev. A* **84**, 034301 (2011).
- Li, H.-W. et al. Semi-device-independent randomness certification using  $n$  to 1 quantum random access codes. *Phys. Rev. A* **85**, 052308 (2012).
- Pawlowski, M. & Brunner, N. Semi-device-independent security of one-way quantum key distribution. *Phys. Rev. A* **84**, 010302 (2011).
- Bowles, J., Quintino, M. T. & Brunner, N. Certifying the dimension of classical and quantum systems in a prepare-and-measure scenario with independent devices. *Phys. Rev. Lett.* **112**, 140407 (2014).
- Lunghi, T. et al. Self-testing quantum random number generator. *Phys. Rev. Lett.* **114**, 150501 (2015).
- Ahrens, J. et al. Experimental tests of classical and quantum dimensionality. *Phys. Rev. Lett.* **112**, 140401 (2014).
- Brunner, N. et al. Testing the dimension of Hilbert spaces. *Phys. Rev. Lett.* **100**, 210503 (2008).
- Moroder, T. et al. Device-independent entanglement quantification and related applications. *Phys. Rev. Lett.* **111**, 030501 (2013).
- Gallego, R. et al. Device-independent tests of classical and quantum dimensions. *Phys. Rev. Lett.* **105**, 230501 (2010).
- Pironio, S. et al. Random numbers certified by Bell's theorem. *Nature* **464**, 1021 (2010).
- Acín, A. et al. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.* **98**, 230501 (2007).
- Clauser, J. F. et al. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.* **23**, 880 (1969).
- Hu, M.-J. et al. Experimental sharing of nonlocality among multiple observers with one entangled pair via optimal weak measurements. Preprint at <http://arxiv.org/abs/1609.01863> (2016).
- Schiavon, M. et al. Three-observer Bell inequality violation on a two-qubit entangled state. *Quantum Sci. Technol.* **2**, 015010 (2017).
- Silva, R. et al. Multiple observers can share the nonlocality of half of an entangled pair by using optimal weak measurements. *Phys. Rev. Lett.* **114**, 250401 (2015).
- Koenig, R., Renner, R. & Schaffner, C. The operational meaning of min- and max-entropy. *IEEE Trans. Inf. Theory* **55**, 4337 (2009).
- Li, H.-W. et al. Detection efficiency and noise in a semi-device-independent randomness-extraction protocol. *Phys. Rev. A* **91**, 032305 (2015).
- Curchod, F. J. et al. Unbounded randomness certification using sequences of measurements. *Phys. Rev. A* **95**, 020102 (2017).
- Hosten, O. & Kwiat, P. Observation of the spin Hall effect of light via weak measurements. *Science* **319**, 787 (2008).
- Dixon, P. B. et al. Ultrasensitive beam deflection measurement via interferometric weak value amplification. *Phys. Rev. Lett.* **102**, 173601 (2009).
- Xu, X. Y. et al. Phase estimation with weak measurement using a white light source. *Phys. Rev. Lett.* **111**, 033604 (2013).
- Lundeen, J. S. et al. Direct measurement of the quantum wavefunction. *Nature* **474**, 188 (2011).
- Lundeen, J. S. & Bamber, C. Procedure for direct measurement of general quantum states using weak measurement. *Phys. Rev. Lett.* **108**, 070402 (2012).
- Aharonov, Y. et al. Revisiting Hardy's paradox: counterfactual statements, real measurements, entanglement and weak values. *Phys. Lett. A* **301**, 130 (2002).
- Bennett, C. H. & Brassard, G. *Proc. IEEE International Conference on Computer System and Signal Processing* 175–179 (IEEE Press, New York, 1984).

## Acknowledgements

We thank Marcin Pawłowski for helpful discussions. This work are supported by the National Natural Science Foundation of China (Grant Nos. 61675235, 11304397, 11674306), National key research and development program of China (Grant No.

2016YFA0302600), and China Postdoctoral Science Foundation (Grant No. 2013M540514).

### Author contributions

H.-W.L., Y.-S.Z., and G.-C.G. conceived the project. H.-W.L., X.-Bi.A., and Z.-F.H. performed the optimization calculation and analysis. H.-W.L. wrote the paper.

### Additional information

**Competing interests:** The authors declare no competing interests.

**Reprints and permission** information is available online at <http://npg.nature.com/reprintsandpermissions/>

**Publisher's note:** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this license, visit <http://creativecommons.org/licenses/by/4.0/>.

© The Author(s) 2018