All entangled states can generate certified randomness

Xing Chen

1Institute of Physics, Beijing National Laboratory for Condensed Matter Physics, Chinese Academy of Sciences, Beijing 100190, China

Random number has many applications, it plays an important role in quantum information processing. It’s not difficult to generate true random numbers, the main difficulty is how to certify the random numbers generated by untrusted devices. In [Nature(London) 464, 1021 (2010)], the authors provided us a way to generate certified random number by Bell’s theorem. In their scheme, we can use the nonlocal behavior of entangled states to generate certified randomness. But there are entangled states, which admit a local hidden variable model, could not be used in their scheme. We show in our paper that the nonlocal correlations in every entangled state can be used to generate certified randomness, and we use Werner states as an example to show how to quantify the output randomness.

I. INTRODUCTION

A. Background

Random number has many important applications nowadays, such as quantum key distribution and the test of Bell’s theorem. It is believed that we can’t generate true random numbers by classical processes. On the other hand, the random numbers generated by quantum physics are truly random because of the superposition of quantum states. There are three kinds of quantum random number generators(QRNG)[1], the first kind is practical QRNG, which is built on trusted devices; the second kind is self-testing QRNG, which can generate true random numbers without trusting the measurement devices; the last kind of QRNG is called semi-self-testing QRNG, which partially combines the advantages of the first two QRNGs.

It is not difficult to generate true random numbers by tools of quantum physics currently. In the first kind of QRNG, we can actually generate random numbers at a very satisfied speed[2][3][4][5]. But these true random numbers are not easy to be certified, because the adversaries may use memory-stick attack[6]. The so called memory-stick attack is implemented in the following way: the adversaries may generate a very long true random numbers and store them in the devices, when the users use this devices to generate random numbers, the generated random numbers are exactly what the adversaries stored in the devices.

Nonlocality can be used to generate certified random numbers[7][8]. In[7][8] the authors connected Bell’s theorem with randomness, the violation of Bell’s inequality guarantees that the generated random numbers contain true randomness, and this randomness is measurement device independent. Especially in[8], a lower bound of the output randomness was derived by the nonlocality in entangled states. However, not all entangled states can violate Bell’s inequality, and those who admit a local hidden variable model can not be used in their randomness certification system. In order to take advantage of all entangled states, we need a new certification scheme. Inspired by previous work[7][8], with the method provided by[9][10][11], we connect randomness with entanglement. In our paper, we can generate certified private randomness by any entangled state, the output randomness in our protocol is measurement device independent and it only needs some fresh randomness as input.

B. Related work

Similar randomness generation protocol was also mentioned in Chaturvedi and Banik’s paper[12], but there are some major differences between their paper and our paper.

In their paper, Chaturvedi and Banik only gave a very specific entangled state’s output randomness. Also, in their paper, they claimed that the output randomness was safe even local operations and classical communication(LOCC) was allowed between two measurement devices. However, the untrusted measurement devices could share some extra entangled states which are not known by Alice and Bob, and we show in our paper that these extra entangled states have the potential to damage the output randomness without being detected.

C. The result of our paper

In our paper, we give a general lower bound for our randomness generation protocol. The same as[8], the classical communication between different measurement devices is forbidden in our protocol. Moreover, the lower bound derived in our paper takes the secret entangled states shared between untrusted measurement devices into consideration.

Generally, the certified randomness in our scheme is different from the randomness verified by Bell’s theorem. This is because the random numbers in these two...
protocols are not generated in the same way. In Bell’s scenario, the randomness is created by measuring entangled states with optimal positive operator valued measure (POVM) (in order to obtain the maximum Bell value $I$), and the guessing probability of the measurement results is increasing with the decreasing of $I$, only when $I > 2$, the guessing probability is less than $1$, so this protocol needs the violation of Bell’s inequality to guarantee the randomness in the measurement results. While in our protocol, the inputs are nonorthogonal states, the maximum guessing probability has an upper bound which is always less than $1$, and the measurement results in our protocol can be verified by any entangled state, so every entangled state is a useful resource in our protocol.

Our paper is organised in the following way. In section II we give a brief introduction to the randomness generation protocol mentioned in [8]. In section III, the main part of our paper, we show how to construct the protocol in our paper, and we give an example to show how to quantify the output randomness. Section IV is a brief conclusion.

II. RANDOMNESS CERTIFIED BY BELL’S THEOREM

Before the illustration of our randomness generation protocol, we first give a brief introduction to the scheme mentioned in [8], the authors used Clauser-Horne-Shimony-Holt (CHSH) [13][14] correlation function

$$ I = \sum_{x,y} (-1)^{xy}[P(a = b|xy) - P(a \neq b|xy)] $$

as an example to show how to generate certified randomness. Where $x$ and $y$ represent certain type of measurement, such as the different polarization directions of polarizers. $a$ and $b$ are the measurement results of Alice and Bob. Choosing certain $x$ and $y$ to measure the entangled state between Alice and Bob could make the Bell value $I > 2$, which means the violation of CHSH inequality, and the violation of CHSH inequality guarantees the randomness in the measurement results $a, b$.

The randomness generation structure is shown in FIG. 1.

In this randomness generation protocol we can use the random seed $x$ and $y$ to generate certified random strings $a$ and $b$ if their correlation violate CHSH inequality, or more generally Bell’s inequality. (One thing we should note here is that the input $x$ and $y$ should both be true random numbers, if they can be predicted by some adversaries, the adversaries may pre-create some correlated random numbers and store them into Alice and Bob’s measurement devices to implement memory-stick attack.) The private randomness in the output strings $a$ and $b$ is quantified by min-entropy, and the details could be find in the supplementary information of [8].

![Randomness certified by Bell nonlocality](image)

**FIG. 1. Randomness certified by Bell nonlocality**

III. RANDOMNESS CERTIFIED BY ANY ENTANGLED STATE

This section is the main part of our paper. It shows how to generate certified randomness by any entangled state, and how to quantify the output randomness.

The randomness generation protocol mentioned in section II takes advantage of the Bell nonlocality in entangled states. However, some entangled states may admit a local hidden variable model, and they do not contain Bell nonlocality [15][16]. In order to make every entangled state useful in certified randomness generation protocol, we must use other property of entangled states instead of Bell nonlocality. In [8], the author proved that with nonorthogonal states as input, the measurement correlation in every entangled state cannot be created by any separate state with local operations and shared randomness (LOSR). The protocol introduced in our paper uses this property of entangled state. For simplicity, we use bipartite scenario to illustrate our protocol.

First, we introduce a Bell-like inequality [10]. In bipartite scenario, Alice and Bob are two separated parties, they share an entangled state $\rho_{AB}$, then they both input some quantum states $\{\tau_s\}$ and $\{\omega_t\}$ into the measurement devices, the measurement devices then output measurement results $a$ and $b$. The correlation between $a$ and $b$ is represented as $P(a, b|\tau_s, \omega_t)$.

$$ P(a, b|\tau_s, \omega_t) = Tr[(P^{A^\prime A}_a \otimes Q^{B^\prime B}_b)(\tau^A_s \otimes \rho_{AB} \otimes \omega^B_t)] $$

where $A, B$ is the Hilbert space of state $\rho_{AB}$, $A^\prime, B^\prime$ is the Hilbert space of nonorthogonal states $\tau_s, \omega_t$, and $P^{A^\prime A}_a, Q^{B^\prime B}_b$ are the POVMs chosen by Alice and Bob. By making suitable joint measurement on their respective part of $\rho_{AB}$ and on the input quantum states $\tau_s, \omega_t$ with $P^{A^\prime A}_a, Q^{B^\prime B}_b$, Alice and Bob can obtain the correlation $P(a, b|\tau_s, \omega_t)$, which cannot be explained without entanglement [9][11]. This allows the existence of the following linear combination of $P(a, b|\tau_s, \omega_t)$:

$$ I_{\rho_{AB}} = \sum_{a, b, s, t} \beta_{s, t, a, b} P(a, b|\tau_s, \omega_t) < 0 $$

where $\beta_{s, t, a, b}$ are some real coefficients. The coefficients
\[ \beta_{s,t,a,b} \] could be obtained from the decomposition of entanglement witness. Because of the completeness of \( \{\tau_s\} \) and \( \{\omega_t\} \), the entanglement witness \( W \) of \( \rho_{AB} \) could be decomposed as

\[ W = \sum_{s,t} \beta_{s,t}\tau_s^\dagger \otimes \omega_t^\dagger \]  

(4)

with \( \beta_{s,t,1,1} = \beta_{s,t} \) and \( \beta_{s,t,a,b} = 0, (a,b) \neq (1,1) \), formula 3 becomes:

\[ I_{\rho_{AB}} = \sum_{s,t} \beta_{s,t} P(1,1|\tau_s,\omega_t) < 0 \]  

(5)

It is proved in [11] that this inequality is greater than or equal to zero for any separated state with any possible POVM. For any entangled state, with the following POVMs,

\[ P_{1}^{A} = |\Phi^{+}_{a,s}\rangle \langle \Phi^{+}_{a,s}|, P_{0}^{A} = I - P_{1}^{A} \]

\[ Q_{1}^{B} = |\Phi^{+}_{b,t}\rangle \langle \Phi^{+}_{b,t}|, Q_{0}^{B} = I - Q_{1}^{B} \]  

(6)

where \( |\Phi^{+}_{a,s}\rangle = \sum_{i=0}^{d_{a}-1} |i\rangle \otimes |i\rangle / \sqrt{d_{A}} \), and \( |\Phi^{+}_{b,t}\rangle = \sum_{j=0}^{d_{b}-1} |j\rangle \otimes |j\rangle / \sqrt{d_{B}} \). The Bell-like value \( I_{\rho_{AB}} \) will be:

\[ I_{\rho_{AB}} = \sum_{s,t} \beta_{s,t} P(1,1|\tau_s,\omega_t) = \frac{Tr(W_{\rho_{AB}})}{d_{A}d_{B}} < 0 \]  

(7)

which is less than zero for entangled states, this means the measurement results \( a,b \) must be unpredictable, otherwise there would be contradiction in quantum theory [11].

With the above Bell-like correlation 5 we can design a certified randomness generation protocol, where any entangled state is useful to generate certified randomness. The protocol is shown in FIG 2. In this protocol, Alice and Bob randomly input some nonorthogonal states \( \tau_s,\omega_t \) to the measurement devices, and they measure these nonorthogonal states jointly with their respective part of \( \rho_{AB} \) by the POVM 6. If the linear combination \( I_{\rho_{AB}} \) of the correlation \( P(1,1|\tau_s,\omega_t) \) is less than zero, then the output strings \( a,b \) contain randomness which could not be predicted by the untrusted measurement devices. The certified randomness in \( a,b \) is quantified by min-entropy \( H_{\infty}(AB|ST) \).

We take Werner states as an example to show how to get the lower bound of \( H_{\infty}(AB|ST) \). For Werner states,

\[ \rho_z = \frac{1 - z}{4} I + z |\Phi^{+}\rangle \langle \Phi^{+}| \]  

(8)

where \( |\Phi^{+}\rangle \) is Bell state \( (|00\rangle + |11\rangle) / \sqrt{2} \). The entanglement witness is:

\[ W_{\rho_z} = \frac{1}{2} I - |\Phi^{+}\rangle \langle \Phi^{+}| \]  

(9)

FIG. 2. Randomness certified by any entangled state. In this protocol, the input \( \tau_s,\omega_t \) are nonorthogonal states, and the measurement devices of Alice and Bob are not allowed to communicate with each other. As long as the Bell-like value \( I_{\rho_{AB}} \) is less than zero, Alice and Bob could extract certified randomness from the measurement results \( a,b \).

The input quantum states \( \tau_s,\omega_t \) are nonorthogonal, they could be any nonorthogonal state which forms a complete basis. Without losing generality, they could be:

\[ \tau_s = (I + \vec{v}_s \cdot \vec{\sigma})/2 \]

\[ \omega_t = (I + \vec{v}_t \cdot \vec{\sigma})/2, \]  

(10)

where \( \vec{\sigma} = (\sigma_x,\sigma_y,\sigma_z) \), \( s,t \in \{0,1,2,3\} \), \( \vec{v}_s = (1,1,1)/\sqrt{3}, \vec{v}_t = (1,-1,1)/\sqrt{3} \). \( \vec{v}_1 = (-1,1,1)/\sqrt{3}, \vec{v}_2 = (-1,-1,1)/\sqrt{3} \).

Next, we discuss the guessing probability of the measurement results. It is illustrated in the Appendix that the average guessing probability of the measurement results \( a,b \) can be written as:

\[ p_{guess} = \frac{I_{\rho_{AB}} - I_{\rho_{AB}}^{\infty}}{I_{\rho_{AB}}^{optimal}} + \frac{I_{\rho_{AB}}^{\infty}}{I_{\rho_{AB}}^{optimal}} \times maxP_{\rho}(a,b|\tau_s,\omega_t) \]  

(11)

And the upper bound of this average guessing probability \( p_{guess} \) is

\[ p_{guess} \leq \frac{I_{\rho_{AB}}^{optimal} - I_{\rho_{AB}}}{I_{\rho_{AB}}^{optimal}} + \frac{I_{\rho_{AB}}}{I_{\rho_{AB}}^{optimal}} \times P_{\rho_{max}}(a,b|\tau_s,\omega_t) \]  

For Werner states \( \rho_z \), \( I_{\rho_{AB}} = (1 - 3z)/16 \), \( I_{\rho_{AB}}^{optimal} = I_{\rho_{AB}}^{\infty} = -1/8 \). \( P_{\rho_{max}}(a,b|\tau_s,\omega_t) \) is the maximum guessing probability with input 10 and POVM 6 it is proved in the Appendix that \( P_{\rho_{max}}(a,b|\tau_s,\omega_t) \leq \frac{9 + \sqrt{3}}{16} \). Then the upper bound of the average guessing probability is

\[ p_{guess} \leq \frac{I_{\rho_{AB}}^{\infty} - I_{\rho_{AB}}}{I_{\rho_{AB}}^{optimal}} + \frac{I_{\rho_{AB}}}{I_{\rho_{AB}}^{optimal}} \times \frac{9 + \sqrt{3}}{16} \]

\[ = \frac{-1/8 - (1 - 3z)/16}{-1/8} + \frac{(1 - 3z)/16}{-1/8} \times \frac{9 + \sqrt{3}}{16} \]

\[ = 1 - \frac{7}{16} \times \frac{3z - 1}{2} \]  

(12)
FIG. 3. The lower bound of output randomness for Werner states $\rho_z$. The analytical upper bound of the average guessing probability is $p_{\text{guess}} \leq 1 - \frac{7 - \sqrt{3}}{16} \times \frac{3z - 1}{2}$, and this average guessing probability is the optimal one allowed by quantum theory. Then we can generate at least $-\log_2(1 - \frac{7 - \sqrt{3}}{16} \times \frac{3z - 1}{2})$ bits of certified randomness, and this randomness is the curve a in the figure. Curve b represents the lower bound obtained from semidefinite programs (SDP).

According to the definition of min-entropy, the lower bound of the output randomness for Werner states $\rho_z$ is

$$H_\infty(AB|ST) \geq -\log_2(1 - \frac{7 - \sqrt{3}}{16} \times \frac{3z - 1}{2})$$

(13)

This lower bound is shown in FIG.3.

From FIG.3 we can see that, for any entangled Werner state, the output randomness is greater than zero, which means any entanglement is useful in our randomness generation protocol.

Comparing the lower bound of our randomness generation protocol with the analytical lower bound of the output randomness in [8], our randomness generation protocol could take advantage of all entangled states by introducing nonorthogonal states as input, and in low degree entanglement, our protocol could generate more secured randomness. The compare of the output randomness is shown in FIG.4.

There are some constrains in our randomness generation protocol. Firstly, the corresponding entanglement witness must be decomposable by the nonorthogonal states and the nonorthogonal states cannot be distinguished by the measurement devices. These conditions require that the input quantum states $\tau_s$ and $\omega_t$ must be nonorthogonal states which form a complete basis, and the labels of these nonorthogonal states must not be revealed to the measurement devices. Secondly, it is more reasonable to trust the source devices other than the measurement devices [11], so the generating devices of the nonorthogonal states should be trusted. Thirdly, any classical communication between the measurement devices is forbidden.

FIG. 4. The compare of output certified randomness of $\rho_z$ in our protocol and in Bell protocol [8]. The lower bound of our protocol is given by $H_\infty(AB|ST) \geq -\log_2(1 - \frac{7 - \sqrt{3}}{16} \times \frac{3z - 1}{2})$, and is represented as blue line (curve a) in the figure. The red line (curve c) is the lower bound of output randomness certified by Bell’s theorem, and its formula is $H_\infty(AB|XY) \geq [1 - \log_2(1 + \sqrt{2 - I^2/4})]$, the relationship between $z$ and $I$ is $I = 2\sqrt{2z}$.

IV. CONCLUSION

In this article, we construct a protocol to generate certified randomness by any entangled state. Similar protocol was also presented in [12], but the authors didn’t give a general lower bound of their protocol, and the lower bound obtained in [12] is not convincing without considering the secret entanglement shared between untrusted measurement devices. In our article, we take this situation into consideration and we obtain a general lower bound for this kind of randomness generation protocol.

Comparing to the protocol in [8], our protocol can take advantage of any entangled state, and our protocol is based on entanglement theory, the correctness of our protocol is guaranteed by the validity of quantum physics. The randomness generation protocol in our paper shows us the deep connection between entanglement and randomness, and further open questions may arise, such as what’s the relationship between randomness and entanglement, are they equal to each other? How do nonorthogonal states assist entangled states, which admit a local hidden variable model, to generate certified randomness?
Appendix A: The average guessing probability of measurement results

The POVMs in our protocol are:

\[ P_{1}^{A^A} = |\Phi_{d_A}^+\rangle\langle\Phi_{d_A}^+|, P_{0}^{A^A} = I - P_{1}^{A^A} \]

\[ Q_{1}^{B^B} = |\Phi_{d_B}^{+}\rangle\langle\Phi_{d_B}^{+}|, Q_{0}^{B^B} = I - Q_{1}^{B^B} \]

and the input nonorthogonal states are

\[ \tau_s = (I + v_s^x \cdot \vec{\sigma})/2 \]

\[ \omega_t = (I + v_t^z \cdot \vec{\sigma})/2, \]

where \( \vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z) \), \( s, t = 0, 1, 2, 3 \),

\[ v_s^0 = (1, 1, 1)/\sqrt{3}, v_1^0 = (1, -1, -1)/\sqrt{3}, v_2^0 = (-1, 1, -1)/\sqrt{3}. \]

The average guessing probability of the measurement results is:

\[ p_{guess} = \frac{I_{\rho'} - I_{\rho''}}{I_{\rho'}} \times 1 + \frac{I_{\rho''}}{I_{\rho'}} \times \max P_{\rho'}(a, b|\tau_s, \omega_t) \]

\[ \leq \frac{I_{\rho_{optimal}'} - I_{\rho_{optimal}''}}{I_{\rho_{optimal}'} - I_{\rho_{optimal}''}} + \frac{I_{\rho_{optimal}''}}{I_{\rho_{optimal}''}} \times \max P_{\rho_{optimal}'}(a, b|\tau_s, \omega_t) \]

\[ \leq \frac{I_{\rho_{optimal}'} - I_{\rho_{optimal}''}}{I_{\rho_{optimal}'} - I_{\rho_{optimal}''}} + \frac{I_{\rho_{optimal}''}}{I_{\rho_{optimal}''}} \times P_{\rho_{max}}(a, b|\tau_s, \omega_t) \]

where \( I_{\rho'} \) is the Bell-like value of entangled state \( \rho' \), which shares the same given entanglement witness \( W \) of \( \rho_{AB} \). \( P_{\rho'}(a, b|\tau_s, \omega_t) \) is the correlation of the measurement results. We have \( I_{\rho'} \leq I_{\rho_{optimal}'} < 0 \) and \( \max P_{\rho'}(a, b|\tau_s, \omega_t) \geq \max P_{\rho_{optimal}'}(a, b|\tau_s, \omega_t) \), otherwise, it’s meaningless for the measurement devices to forge the measurement results. \( I_{\rho_{optimal}} \) is the minimum Bell-like value for entanglement witness \( W \). \( P_{\rho_{max}}(a, b|\tau_s, \omega_t) \) is the maximum measurement correlation for any two-qubit state with POVM (A1) and with nonorthogonal inputs (A2).

Next, we give an example to show the meaning of the average guessing probability. Suppose the entangled state shared between Alice and Bob is

\[ \rho_z = \frac{1 - z}{4} I + z|\Phi^{+}\rangle\langle\Phi^{+}| \]

The corresponding entanglement witness will be

\[ W_{\rho_z} = \frac{1}{2} I - |\Phi^{+}\rangle\langle\Phi^{+}| \]
With the POVM [A1] and with nonorthogonal inputs [A2] the correlations of measurement results are
\[ P_{\rho_z}(a, b | \tau_z, \omega_z) = z P_{\Phi^+}(a, b | \tau_z, \omega_z) + (1 - z) P_k(a, b | \tau_z, \omega_z) \]
\[ = \frac{7 - 5a - 5b + 4ab}{12} + \frac{(1 - z)(3 - 2a)(3 - 2b)}{16} \]
\[ = \frac{(3 - 2a)(3 - 2b)}{16} + \frac{z(1 - 2a)(1 - 2b)}{48} \]
and the maximum \( P_{\rho_z}(a, b | \tau_z, \omega_z) \) is
\[ \max_{a, b} P_{\rho_z}(a, b | \tau_z, \omega_z) = P_{\rho_{\tau_0}}(0, 0 | \tau_z, \omega_z) \]
\[ = \frac{9}{16} + \frac{z}{48} \]
\[ = \frac{27 + z}{48} \] (A5)

This equation shows that the guessing probability is becoming larger with the increasing of \( z \). It seems without entanglement, the output randomness is better. Actually, this is not the case. From formula [A5], the guessing probability is maximum when the shared entangled state is Bell state, so the optimal cheating strategy for the measurement devices is to fake the measurement results with built-in state \( |\Phi^+\rangle \). Here is the detail, suppose \( z = 0.34 \), then
\[ \rho_{\tau_0} = 0.66 \times \frac{I}{4} + 0.34 \times |\Phi^+\rangle \langle \Phi^+| \] (A6)

If the measurement devices do the corresponding measurement honestly, the maximum guessing probability of the measurement results will be
\[ \max_{a, b} P_{\rho_{\tau_0}}(a, b | \tau_z, \omega_z) = P_{\rho_{\tau_0}}(0, 0 | \tau_z, \omega_z) \]
\[ = \frac{27 + 0.34}{48} \] (A7)

the output randomness is \(-\log_2(\frac{27 + 0.34}{48}) = 0.812\), it’s quite large for a low degree entangled state like [A6]. However, most part of the output randomness cannot be certified, the untrusted measurement devices could use the following trick to jeopardize the security in the measurement results:

When Alice and Bob used entangled state [A6] to generate certified random number, the expected Bell-like value \( I_{\rho_{\tau_0}} \) is
\[ I_{\rho_{\tau_0}} = \frac{Tr(W_{\rho_{\tau_0}})}{4} \]
\[ = \frac{1 - 3 \times 0.34}{16} \]
\[ = -\frac{1}{800} \] (A8)

Without being detected, the measurement devices could take advantage of their built-in Bell state \( |\Phi^+\rangle \) to deceive Alice and Bob. The entanglement witness of \( |\Phi^+\rangle \) and \( \rho_{\tau_0} \) could both be \( W_{\rho_{\tau_0}} \), the corresponding Bell-like value of \( |\Phi^+\rangle \) is \(-1/8\), it’s much less than that of \( \rho_{\tau_0} \).

As long as the Bell-like value of the measurement results are equal to \( I_{\rho_{\tau_0}} \), Alice and Bob will not detect any insecurity in the measurement results. By using this fact, the measurement devices can fake about 99% of the measurement results. These fake measurement results can be stored in the measurement devices without being known by Alice and Bob, and the Bell-like value of this fake part can be as less as zero. For the rest 1%, the measurement devices choose to jointly measure \( |\Phi^+\rangle \) with the built-in state \( |\Phi^+\rangle \), the Bell-like value of these measurement results is \( I_{\rho^+} = -1/8 \). From the view of Alice and Bob, the average Bell-like value of the whole measurement results would be
\[ I_{\text{average}} = 0 \times 99\% + \frac{1}{8} \times 1\% = -\frac{1}{800} \]

which is the same as \( I_{\rho_{\tau_0}} \). The fake part of the measurement results is known by the measurement devices, the guessing probability could be 1. For the measurement results of the built-in state \( |\Phi^+\rangle \), the maximum guessing probability is \( 7/12 \). Then the average guessing probability of the whole measurement results for the measurement devices should be \( 0.99 \times 1 + 0.01 \times 7/12 = 0.9958 \), and the corresponding lower bound of the output randomness is \(-\log_2(0.9958) = 0.006\).

One thing we should note here is that, the untrusted measurement devices could not force all the measurement results, there must be some truly random measurement results from the shared entanglement between measurement devices to make sure the average Bell-like value is less than zero. Otherwise, without sharing entanglement, the measurement devices could make \( I_{\rho_z} < 0 \), which is contradict with quantum physics [11].

According to the analysis above, the average guessing probability of the measurement results for Werner states [A3] should be:
\[ p_{\text{guess}} = \frac{I_{|\Phi^+\rangle} - I_{\rho_z}}{I_{|\Phi^+\rangle}} \times 1 + \frac{I_{\rho_{\tau_0}}}{I_{|\Phi^+\rangle}} \times \max_{a, b} P_{|\Phi^+\rangle}(a, b | \tau_z, \omega_z) \]

The measurement correlation \( \max_{a, b} P_{|\Phi^+\rangle}(a, b | \tau_z, \omega_z) \) may not be the optimal one, as there are some entangled states’ measurement correlation larger than Bell state. We use \( P_{\rho_{\max}}(a, b | \tau_z, \omega_z) \) to represent the maximum correlation allowed by quantum physics, then the upper bound of the average guessing probability is
\[ p_{\text{guess}} = \frac{I_{|\Phi^+\rangle} - I_{\rho_z}}{I_{|\Phi^+\rangle}} \times 1 + \frac{I_{\rho_{\tau_0}}}{I_{|\Phi^+\rangle}} \times \max_{a, b} P_{|\Phi^+\rangle}(a, b | \tau_z, \omega_z) \]
\[ \leq \frac{I_{|\Phi^+\rangle} - I_{\rho_z}}{I_{|\Phi^+\rangle}} + \frac{I_{\rho_{\tau_0}}}{I_{|\Phi^+\rangle}} \times P_{\rho_{\max}}(a, b | \tau_z, \omega_z) \] (A9)
Appendix B: The maximum measurement correlation $P_{\rho_{\max}}(a, b|\tau_s, \omega_t)$

In this appendix, we calculate $P_{\rho_{\max}}(a, b|\tau_s, \omega_t)$. It is said in [17] that any two-qubit density matrix $\rho_{AB}$ is an element in the linear space expanded by $\{\sigma_i \otimes \sigma_j, i, j \in \{0, 1, 2, 3\}\}$ ($\sigma_0 = I_{2 \times 2}$). $Tr(\rho_{AB}) = 1$, so the coefficient of $\sigma_0 \otimes \sigma_0$ is $1$.

Thus all the two-qubit density matrices have 15 different coefficients, they are $c_{3i+j}$, $i, j \in \{0, 1, 2, 3\}$, $(i, j) \neq (0, 0)$. $\rho_{AB}$ could be written as:

$$\rho_{AB} = \frac{1}{4} \sigma_0 \otimes \sigma_0 + \sum_{i,j=0,1,2,3 \atop (i,j)\neq(0,0)} c_{3i+j} \sigma_i \otimes \sigma_j \quad (B1)$$

$\rho_{AB}$ is a quantum state, which means the minimum eigenvalue $\lambda_{\min,AB} \geq 0$. From the property of eigenvalue, the eigenvalue of $\rho_{AB}$ is less than the eigenvalue sum of its each part [18]:

$$\lambda_{AB} \leq \sum_{i,j=0,1,2,3} c_{3i+j} \lambda_{3i+j}$$

The eigenvalues of $\sigma_0 \otimes \sigma_0$ are $\{1, 1, 1, 1\}$, the eigenvalues of $\sigma_i \otimes \sigma_j$ $(i, j) \neq (0, 0)$ are $\{-1, -1, 1, 1\}$. We already know the coefficient of $\sigma_0 \otimes \sigma_0$ is $\frac{1}{4}$, then the range of $\rho_{AB}$’s eigenvalues could be represented as

$$\lambda_{AB1} \leq \frac{1}{4} - \sum_{i,j=0,1,2,3 \atop (i,j)\neq(0,0)} c_{3i+j},$$
$$\lambda_{AB2} \leq \frac{1}{4} - \sum_{i,j=0,1,2,3 \atop (i,j)\neq(0,0)} c_{3i+j},$$
$$\lambda_{AB3} \leq \frac{1}{4} + \sum_{i,j=0,1,2,3 \atop (i,j)\neq(0,0)} c_{3i+j},$$
$$\lambda_{AB4} \leq \frac{1}{4} + \sum_{i,j=0,1,2,3 \atop (i,j)\neq(0,0)} c_{3i+j} \quad (B2)$$

Because the minimum element of $\lambda_{AB}$ is greater than or equal to zero, we have

$$-\frac{1}{4} \leq \sum_{i,j=0,1,2,3 \atop (i,j)\neq(0,0)} c_{3i+j} \leq \frac{1}{4} \quad (B3)$$

The correlation $P(a, b|\tau_s, \omega_t)$ is the correlation sum of each basis:

$$P(a, b|\tau_s, \omega_t) = Tr[(P_{\sigma}^A \otimes Q_{\rho}^B)(\tau_s \otimes \rho_{AB} \otimes \omega_t)]$$

$$= Tr[(P_{\sigma}^A \otimes Q_{\rho}^B)(\tau_s \otimes (\sum_{i,j=0,1,2,3} c_{3i+j} \sigma_i \otimes \sigma_j) \otimes \omega_t)]$$

$$= \frac{9}{16} + \left( \sum_{i,j=0,1,2,3 \atop (i,j)\neq(0,0)} c_{3i+j} P(\sigma_i \otimes \sigma_j) \right)$$

$$\leq \frac{9}{16} + \sum_{i,j=0,1,2,3 \atop (i,j)\neq(0,0)} c_{3i+j} \max P(\sigma_i \otimes \sigma_j)$$

$$\leq \frac{9}{16} + \frac{\max P(\sigma_i \otimes \sigma_j)}{4}$$

where $P(\sigma_i \otimes \sigma_j) = Tr[(P_{\sigma}^A \otimes Q_{\sigma}^B)(\tau_s \otimes (\sigma_i \otimes \sigma_j) \otimes \omega_t)]$.

With the given POVM $\{A_{1/2}\}$ and with nonorthogonal states $\{A_{1/2}\}$, we can get $\max P(\sigma_i \otimes \sigma_j) = \sqrt{\frac{3}{4}}$, and the maximum measurement correlation is $P_{\rho_{\max}}(a, b|\tau_s, \omega_t) = \frac{9 + \sqrt{3}}{16}$. Then the upper bound of the average guessing probability (A9) is

$$p_{\text{guess}} \leq \frac{I_{\rho(\Phi^+) - I_{\rho z}}}{I_{\rho(\Phi^+)}} + \frac{I_{\rho z}}{I_{\rho(\Phi^+)}} \times \frac{9 + \sqrt{3}}{16}$$

The similar analysis could be applied to any entangled state $\rho_{AB}$ shared between Alice and Bob, thus the upper bound of the average guessing probability in our randomness generation protocol is:

$$p_{\text{guess}} \leq \frac{I_{\rho_{\text{optimal}}(\Phi^+) - I_{\rho_{\text{optimal}} z}}}{I_{\rho_{\text{optimal}}(\Phi^+)}} + \frac{I_{\rho_{\text{optimal}} z}}{I_{\rho_{\text{optimal}}(\Phi^+)}} \times \frac{9 + \sqrt{3}}{16}$$

where $I_{\rho_{\text{optimal}}}$ is the minimum Bell-like value for the given entanglement witness of entangled state $\rho_{AB}$.

Appendix C: SDP output randomness

From the perspective of the measurement devices, searching for the optimal guessing probability $p_{\text{guess}}$ is equal to solve the next optimization problem:

$$\max p_{\text{guess}}$$

subject to

$$p_{\text{guess}} = \frac{I_{\rho^A}}{I_{\rho' \rho^A}} + \frac{I_{\rho_{\text{AB}}}}{I_{\rho' \rho_{\text{AB}}}} \times \max P_{\rho^A}(a, b|\tau_s, \omega_t)$$

$$I_{\rho_{\text{AB}}} = \sum_{s,t} \beta_{s,t} P_{\rho_{AB}}(1, 1|\tau_s, \omega_t)$$

$$I_{\rho'} = \sum_{s,t} \beta_{s,t} P_{\rho'}(1, 1|\tau_s, \omega_t)$$

$$I_{\rho'} < 0$$

$$\max p_{\rho^A}(a, b|\tau_s, \omega_t) \geq \max P_{\rho_{\text{AB}}}(a, b|\tau_s, \omega_t)$$

This problem can be formulating as semidefinite programs (SDP) [19][20][21]. the lower bound of the output randomness obtained from SPD is shown as curve $b$ in FIG 3.