ISSN 1674-1056
http://cpb.iphy.ac.cn
http://iopscience.iop.org/cpb
中国物理 B
Chinese Physics
中国物理 Chinese Physics B

# Improved quantum randomness amplification with finite number of untrusted devices based on a novel extractor

Ming-Feng Xu(徐明峰), Wei Pan(潘炜), Lian-Shan Yan(闫连山), Bin Luo(罗斌), Xi-Hua Zou(邹喜华), Peng-Hua Mu(穆鹏华), Li-Yue Zhang(张力月)
**Citation:**Chin. Phys. B . 2018, 27(1): 010305. **doi:** 10.1088/1674-1056/27/1/010305

Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

**What follows is a list of articles you may be interested in**

---

## Decoy-state reference-frame-independent quantum key distribution with both source errors and statistical fluctuations

Kang Liu(刘康), Jian Li(李剑), Jian-Rong Zhu(朱建荣), Chun-Mei Zhang(张春梅), Qin Wang(王琴)
Chin. Phys. B . 2017, 26(12): 120302. **doi:** 10.1088/1674-1056/26/12/120302

## Balancing four-state continuous-variable quantum key distribution with linear optics cloning machine

Xiao-Dong Wu(吴晓东), Qin Liao(廖骎), Duan Huang(黄端), Xiang-Hua Wu(吴湘华), Ying Guo(郭迎)
Chin. Phys. B . 2017, 26(11): 110304. **doi:** 10.1088/1674-1056/26/11/110304

## Performance optimization for quantum key distribution in lossy channel using entangled photons

Yu Yang(杨玉), Luping Xu(许录平), Bo Yan(阎博), Hongyang Zhang(张洪阳), Yanghe Shen(申洋赫)
Chin. Phys. B . 2017, 26(11): 110305. **doi:** 10.1088/1674-1056/26/11/110305

## Improving continuous-variable quantum key distribution under local oscillator intensity attack using entanglement in the middle

Fang-Li Yang(杨芳丽), Ying Guo(郭迎), Jin-Jing Shi(石金晶), Huan-Li Wang(王焕礼), Jin-Jin Pan(潘矜矜)
Chin. Phys. B . 2017, 26(10): 100303. **doi:** 10.1088/1674-1056/26/10/100303

## Time-energy high-dimensional one-side device-independent quantum key distribution

Hai-Ze Bao(包海泽), Wan-Su Bao(鲍皖苏), Yang Wang(汪洋), Rui-Ke Chen(陈瑞柯), Hong-Xin Ma(马鸿鑫), Chun Zhou(周淳), Hong-Wei Li(李宏伟)
Chin. Phys. B . 2017, 26(5): 050302. **doi:** 10.1088/1674-1056/26/5/050302

---

# Improved quantum randomness amplification with finite number of untrusted devices based on a novel extractor*

Ming-Feng Xu(徐明峰)†, Wei Pan(潘炜), Lian-Shan Yan(闫连山), Bin Luo(罗斌), Xi-Hua Zou(邹喜华), Peng-Hua Mu(穆鹏华), and Li-Yue Zhang(张力月)

*Center for Information Photonics and Communications, Southwest Jiaotong University, Chengdu* 611756, *China*

(Received 21 August 2017; revised manuscript received 7 October 2017; published online 28 November 2017)

Quantum randomness amplification protocols have increasingly attracted attention for their fantastic ability to amplify weak randomness to almost ideal randomness by utilizing quantum systems. Recently, a realistic noise-tolerant randomness amplification protocol using a finite number of untrusted devices was proposed. The protocol has the composable security against non-signalling eavesdroppers and could produce a single bit of randomness from weak randomness sources, which is certified by the violation of certain Bell inequalities. However, the protocol has a non-ignorable limitation on the min-entropy of independent sources. In this paper, we further develop the randomness amplification method and present a novel quantum randomness amplification protocol based on an explicit non-malleable two independent-source randomness extractor, which could remarkably reduce the above-mentioned specific limitation. Moreover, the composable security of our improved protocol is also proposed. Our results could significantly expand the application range for practical quantum randomness amplification, and provide a new insight on the practical design method for randomness extraction.

**Keywords:** quantum random number generation, quantum randomness amplification, quantum key distribution

**PACS:** 03.67.–a, 03.67.Hk **DOI:** 10.1088/1674-1056/27/1/010305

## 1. Introduction

Randomness is a kind of particularly special resource that we could benefit from in nature. Nowadays, it is broadly applied in gambling, economics, cryptography, and quantum key distribution.[1–4] Generally, there are two different types of randomness, which could be classified as classical randomness and quantum randomness. The classical randomness, derived from specified algorithms or classical physical phenomenons, such as thermal noise,[5] radioactive decay,[6] or optical chaos,[7] is so-called pseudo randomness as its deterministic nature. However, the quantum randomness is truly "real" randomness, which particularly stems from the uncertainty principle in quantum mechanics.[8]

Recently, as a widely used task, quantum randomness amplification is firstly proposed by Colbeck and Renner in Ref. [9], building on the breakthrough results in Ref. [10]. They constructed a device-independent quantum randomness amplification protocol based on the violation of a Bell inequality, and demonstrated that one can amplify a weak randomness $\varepsilon$-Santha–Vazirani (SV) source[11] to almost ideal randomness bits, which is not possible in classical theory. Subsequently, many protocols have been proposed to further develop the original result.[12–16]

More recently, it has been shown that the quantum randomness amplification protocol could be accomplished with only a finite constant number of devices, even in the presence of a certain noise level.[12] Using a finite number of untrusted devices, this realistic noise-tolerant protocol could produce randomness from an arbitrarily weak SV source and achieve composable security against general no-signaling adversaries, even working with correlations attainable by noisy quantum resources. Compared to most previous quantum randomness amplification protocols, one of the biggest advantages of this protocol is that it needs only a finite number of devices, i.e., 4 or 8 untrusted devices, which therefore makes it directly implementable in practice. Specifically, under certain limitations on the min-entropy sources obtained from the Bell test, the protocol could produce one bit of output randomness in polynomial time with four untrusted devices.

In this paper, we investigate and further develop the realistic noise-tolerant quantum randomness amplification protocol presented in Ref. [12], wherein we focus on the protocol performance from another practical point of view, namely, a randomness extraction method in the practical scenarios. We present an improved quantum randomness amplification protocol with four untrusted devices by introducing a novel non-malleable two independent-source randomness extractor presented in Ref. [17]. Using this novel extractor, we could reduce the limitations on the min-entropy $h_\infty$ of a randomness amplification protocol from $O(\mathrm{poly}\log n)$ to $O(\log n \log\log n)$ with $n$ times of running. This notable improvement could immediately expand the application ranges of quantum randomness amplification protocols for practical scenarios. Moreover, the composable security against general no-signaling adversaries is presented.

*Project supported by the National Natural Science Foundation of China (Grant No. 61775185).

†Corresponding author. E-mail: xmfswjtu@126.com

© 2018 Chinese Physical Society and IOP Publishing Ltd 

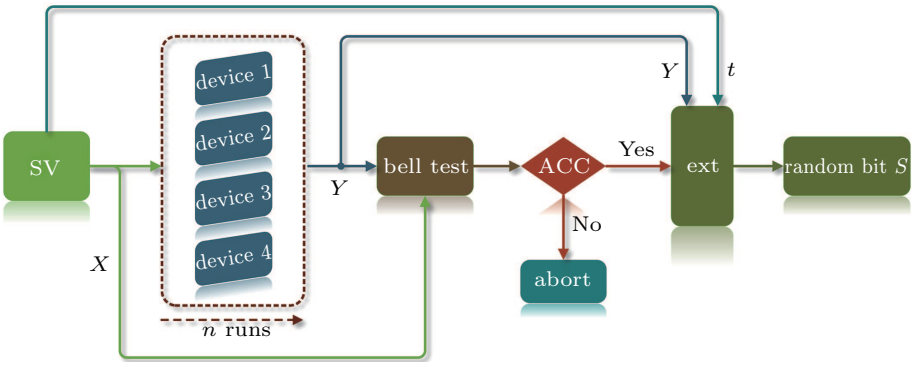



**Fig. 1.** (color online) Schematic diagram of improved quantum randomness amplification protocol with four untrusted devices. The protocol works as follows. First, the bit sequences $X$ from the SV source are delivered to four devices as their measurement inputs, producing output bits $Y$. Then the inputs and outputs of devices $(X,Y)$ are subjected to the Bell tests. When the tests are passed (ACC), the honest parties subsequently apply an extractor to the output strings $Y$ from the devices and further $n$ bits $t$ from the SV source, obtaining the final single random bit $S$ with composable security against most general adversaries. The protocol runs $n$ times, and the colors of the arrows schematically represent their provenances.

## 2. General setup and protocol procedure

We describe the novel explicit non-malleable randomness extraction protocol for improved realistic quantum randomness amplification with four untrusted devices in detail as follows.

Before going into more details, let us introduce some notations and definitions. Let $x$ and $y$ denote the measurement input and output sets of the four honest parties with untrusted devices, respectively. Considering $n$ runs of each untrusted device, we have $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$ and $\boldsymbol{y} = (y_1, y_2, \ldots, y_n)$. For $k \in \{1, 2, \ldots, n\}$, every $x_k$ and $y_k$ is in the form $\boldsymbol{x} = (\boldsymbol{x}^1, \boldsymbol{x}^2, \boldsymbol{x}^3, \boldsymbol{x}^4)$ and $\boldsymbol{y} = (\boldsymbol{y}^1, \boldsymbol{y}^2, \boldsymbol{y}^3, \boldsymbol{y}^4)$, respectively. Let $w$ and $z$ be the inputs and outputs of the adversary and Eve, respectively, and let $e$ denote the side information held by Eve. To specifically describe the protocol, we introduce the so-called probability box, which defines the total probability relation between the input and output in the protocol. Finally, the probability box, held by the four honest parties and Eve is given as $p(y,z \mid x,e,w)$.[12]

As illustrated in Fig. 1, the improved quantum randomness amplification protocol includes the following specific steps:

(i) **Measurement step** First, a portion of bits from classical $\varepsilon$-SV source is delivered to the four honest parties, and used to choose the measurement settings $\boldsymbol{x}_k = (\boldsymbol{x}_k^1, \boldsymbol{x}_k^2, \boldsymbol{x}_k^3, \boldsymbol{x}_k^4)$ for the four no-signalling untrusted devices in the $n$ runs of the protocol. It then produces the output bits $\boldsymbol{y}_k = (\boldsymbol{y}_k^1, \boldsymbol{y}_k^2, \boldsymbol{y}_k^3, \boldsymbol{y}_k^4)$.

(ii) **Estimation step** To check whether a particular Bell inequality is violated to a certain specified level, an estimation test is then performed on the input $x$ and output $y$. The estimation quantity of Bell inequality is given as

$$\hat{B}_{\text{est}} := \frac{1}{n}\sum_{k=1}^{n} B(y_k, x_k), \tag{1}$$

where $B$ is an indictor vector given in the following equation (7), with $16 \times 16$ entries $B(y,x)$ representing the violation amount of the Bell inequality and $\boldsymbol{B} \cdot \{P(\boldsymbol{y}|\boldsymbol{x})\} = 0$ denotes the maximally algebraically violation of Bell inequality. In fact, we can firstly obtain the conditional probability distribution $P(\boldsymbol{y}|\boldsymbol{x})$ from the experimental data of the measurement input $\boldsymbol{x}$ and the measurement output $\boldsymbol{x}$. Then, combining the $P(\boldsymbol{y}|\boldsymbol{x})$ and the Bell indictor vector $\boldsymbol{B}$, we can obtain the Bell inequality to estimate the violation of Bell test. The protocol is aborted unless $\hat{B}_{\text{est}} \leq \delta$ for some fixed constant $\delta > 0$, where $\delta$ is interpreted as the noise level. In particular, we would observe $\hat{B}_{\text{est}} = 0$ in the absence of noise.

(iii) **Randomness extraction step.** Conditioned on the successful test in the above step, the four users then apply an explicit non-malleable independent-source extractor Ext in Ref. [17], to the output strings $y$ from the devices and further a second part of bits $t$ from the SV source. Finally, we could obtain a single perfect random bit $S$ from the extractor Ext, where $S$ is the output of Ext, $S := \text{Ext}(y,t)$.

In fact, to ensure the composable security of the proposed protocol, in the first two steps we adopt similar strategies as those presented in Ref. [12], as well as the Bell inequality. The most important improvement that we develop here is the novel construction method of different randomness amplification extractors, which could significantly improve the practical performance of randomness amplification protocols.

## 3. Composable security proof

In this section, we present some necessary notions and definitions for detailed descriptions at first, and prove the composable security of our protocol in the end.

**$\varepsilon$-SV source.** In the most general case, an $\varepsilon$-SV source is described as the probability distribution $P(X_i \mid X_{i-1}, \ldots, X_1)$, such that

$$\frac{1}{2} - \varepsilon \leq P(X_i \mid X_{i-1}, \ldots, X_1) \leq \frac{1}{2} + \varepsilon \tag{2}$$

for all $i$, where $0 \leq \varepsilon < \frac{1}{2}$.

**Bell inequality** As demonstrated in Ref. [10], the violation of Bell inequalities could be used to generate certified randomness with device-independent certification. The Bell inequality we use here is four-parties Bell inequality as presented in Ref. [12]. It contains four spatially separated parties with measurement settings $\boldsymbol{x}=(\boldsymbol{x}^1,\boldsymbol{x}^2,\boldsymbol{x}^3,\boldsymbol{x}^4)$ and respective outcomes $\boldsymbol{y}=(\boldsymbol{y}^1,\boldsymbol{y}^2,\boldsymbol{y}^3,\boldsymbol{y}^4)$. We have two possible measurement settings and two possible output settings, namely, $\boldsymbol{x}^i\in\{0,1\}$ and $\boldsymbol{y}^i\in\{0,1\}$ for $i\in\{1,2,3,4\}$, where the measurement settings could be divided into two sets such that

$$\boldsymbol{X}_0=\{\{0001\},\{0010\},\{0100\},\{1000\}\}, \tag{3}$$

$$\boldsymbol{X}_1=\{\{0111\},\{1011\},\{1101\},\{1110\}\}. \tag{4}$$

The Bell inequality is given in Ref. [18] as

$$\sum_{\boldsymbol{y},\boldsymbol{x}}(\boldsymbol{I}_{\oplus_{i=1}^4\boldsymbol{y}^i=0}\cdot\boldsymbol{I}_{\boldsymbol{x}\in X_0}+\boldsymbol{I}_{\oplus_{i=1}^4\boldsymbol{y}^i=1}\cdot\boldsymbol{I}_{\boldsymbol{x}\in X_1})\cdot P(\boldsymbol{y}|\boldsymbol{x})\geq 2, \tag{5}$$

where the indicator function $\boldsymbol{I}_{\boldsymbol{x}\in X_0}=1$ if $\boldsymbol{x}\in X_0$ and 0 otherwise. Hence, the Bell inequality can be written as

$$\boldsymbol{B}\cdot\{P(\boldsymbol{y}|\boldsymbol{x})\}=\sum_{\boldsymbol{y},\boldsymbol{x}}B(\boldsymbol{y},\boldsymbol{x})P(\boldsymbol{y}|\boldsymbol{x})\geq 2, \tag{6}$$

where $\boldsymbol{B}$ is an indicator vector for Bell inequality with $16\times 16$ entries

$$B(\boldsymbol{y},\boldsymbol{x})=\boldsymbol{I}_{\oplus_{i=1}^4\boldsymbol{y}^i=0}\cdot\boldsymbol{I}_{\boldsymbol{x}\in X_0}+\boldsymbol{I}_{\oplus_{i=1}^4\boldsymbol{y}^i=1}\cdot\boldsymbol{I}_{\boldsymbol{x}\in X_1}. \tag{7}$$

Next, we show that there exists the maximally algebraic violation of the given Bell inequality. First, we suggest the quantum state

$$|\Psi\rangle=\frac{1}{\sqrt{2}}\Big(|\phi_-\rangle|\widetilde{\phi}_+\rangle+|\psi_+\rangle|\widetilde{\psi}_-\rangle\Big), \tag{8}$$

where

$$|\phi_-\rangle=\frac{1}{\sqrt{2}}(|0\rangle|0\rangle-|1\rangle|1\rangle), \tag{9}$$

$$|\widetilde{\phi}_+\rangle=\frac{1}{\sqrt{2}}(|0\rangle|+\rangle+|1\rangle|-\rangle), \tag{10}$$

$$|\psi_+\rangle=\frac{1}{\sqrt{2}}(|0\rangle|1\rangle+|1\rangle|0\rangle), \tag{11}$$

$$|\widetilde{\psi}_-\rangle=\frac{1}{\sqrt{2}}(|0\rangle|-\rangle-|1\rangle|+\rangle). \tag{12}$$

Then choose the measurements in the $X$ basis as

$$\Big\{|+\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle),\ \ |-\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\Big\} \tag{13}$$

corresponding to $\boldsymbol{x}^i=0$ and the measurements in the $Z$ basis as

$$\Big\{|0\rangle,\ \ |1\rangle\Big\}, \tag{14}$$

corresponding to $\boldsymbol{x}^i=1$ for each of the four parties $i\in\{1,2,3,4\}$.[12] Finally, we perform the above measurements on the quantum state $|\Psi\rangle$ and could achieve the maximally algebraic violation of Bell inequality, i.e., $\boldsymbol{B}\cdot\{P(\boldsymbol{y}|\boldsymbol{x})\}=\sum_{\boldsymbol{y},\boldsymbol{x}}B(\boldsymbol{y},\boldsymbol{x})P(\boldsymbol{y}|\boldsymbol{x})=0$.

**Min-entropy sources** For a given random variable $S$, the min-entropy is defined as

$$H_\infty(S)=\min_{s\in\mathrm{supp}(S)}\log\frac{1}{P(S=s)}. \tag{15}$$

As an example, the min-entropy of the SV source is no smaller than $\log(\frac{1}{2}+\varepsilon)$. We notice that, one can realize the randomness amplification task by using two independent-source extractors for multiple weak sources of randomness. Here, we use the following result on a two-source extractor.

**Explicit non-malleable two-source extractor** The explicit non-malleable extractor that we use in the randomness extraction step is described as the following lemma.

**Lemma 1** (Theorem 1.9 in Ref. [17]).

For every constant $\sigma>0$, there exists a constant $c'>1$ and an explicit two-source extractor $\mathrm{Ext}:\{0,1\}^n\times\{0,1\}^n\mapsto\{0,1\}$ for min-entropy $h_\infty\geq c'\log n\log\log n$, with error $\sigma$.

Actually, as described above, this non-malleable extractor is a two min-entropy source randomness extractor. In fact, once we have two random sources that both satisfy the restrictions on min-entropy, then using this novel extractor, we could extract one single bit of randomness from two min-entropy sources, which is termed as $y$ and $t$ in our protocol. Moreover, as explained detailedly in Ref. [17], the non-malleable extractor has an explicit construction way, leading to an important significance for practical applications.

**Proof of composable security** In this subsection, we briefly proof the composable security of our protocol as follows.

**Theorem 1** For a general $\varepsilon$-SV source with $\varepsilon>0$ and the specific parameters described in Ref. [12], then for any probability distribution $p_w(y,z,x,t,e)$ satisfying the Bell violation, the proposed protocol could produce on single perfect random bit $s$ using an explicit non-malleable independent-source extractor Ext: $\mathrm{Ext}(y,t)=s$ with constant error $\sigma$, such that

$$d_{\mathrm{c}}p(\mathrm{ACC})\leq 2^{-\Omega(n\log\log n)}, \tag{16}$$

where $s$ is the finally obtained one single random bit, ACC means the acceptance of the estimation step and $d_{\mathrm{c}}$ is the composable security criterion which is defined in terms of the standard variational distance of the actual box $p(s,z,e\mid w,\mathrm{ACC})$ and an ideal box, given by

$$d_{\mathrm{c}}:=\sum_{s,e}\max_w\sum_z\Big|p(s,z,e\mid w,\mathrm{ACC})-\frac{1}{2}p(z,e\mid w,\mathrm{ACC})\Big|. \tag{17}$$

We briefly proof the above theorem as follows. From the security proof in Ref. [12], it is shown that with high probability, either we can get a min-entropy from the outputs of

the devices when conditioned on the successful acceptance of ACC, or else the probability of acceptance is small. As claimed in Ref. [12], the crux of the proof is to show that the outputs of untrusted devices constitute a min-entropy, which is certified by the violation of Bell inequality. Then we can apply a randomness extractor to the two independent sources. Here, using the similar building method of two independent min-entropy sources $y$ and $t$, we could then produce one single random bit with the explicit non-malleable extractor presented in Lemma 1. Thanks to the cascaded structure, we could adopt the explicit non-malleable extractor proposed in Ref. [17] instead of that in Ref. [12], which immediately reduces the limitation on the min-entropy. Namely, we could change the $h_\infty \geq \log^c(n)$ with $h_\infty \geq c' \log n \log\log n$ ($c$ is a large enough constant, see Ref. [12]). As a result, similar to the security proof in Ref. [12], one can easily get the inequality (16) with the setting $|S| = 2$. That completes the proof.

It is clear from the above analysis that, the improved randomness amplification protocol we present here requires only four untrusted devices, and holds composable security against the most general adversaries by introducing an explicit non-malleable extractor, which enables a true random bit to be generated from two min-entropies. Compared to the original results presented in Ref. [12], our protocol could significantly reduce min-entropy $h_\infty$ requirement from $O(\text{poly}\log n)$ to $O(\log n \log\log n)$.

In fact, due to the cascaded structure, our approach could be easily extended to the alternative randomness amplification protocol with the eight devices in Ref. [12] and other randomness amplification protocols. Moreover, our extractor has an explicit construction method as described in Ref. [17]. This added benefit makes our protocol more useful for applications in practical scenarios.

## 4. Conclusions

In this work, we demonstrated a novel randomness amplification protocol with four untrusted devices using an explicit non-malleable extractor. We characterized the composable security of the proposed protocol and proved that it could produce a single random bit from two min-entropy sources. Improvements in the randomness extraction method could obviously reduce the demand for min-entropy sources. Moreover, the cascaded nature of the protocol makes it compatible with a variety of practical random number generations, such as source-independent[19] and source-device-independent[20] quantum random number generation schemes.

Future work into the more advanced randomness extraction method would enable general practical random number generations in a range of applications. As such, our results may provide new insights into common randomness extraction techniques for practical quantum randomness amplification and quantum random number generations.

## References


[1] Herrero-Collantes M and Garcia-Escartin J C 2017 *Rev. Mod. Phys.* **89** 015004
[2] Quan D X, Zhu C H, Liu S Q and Pei C X 2015 *Chin. Phys. B* **24** 050309
[3] Ma H Q, Zhu W, Wei K J, Li R X and Liu H W 2016 *Chin. Phys. B* **25** 050304
[4] Li Y M, Wang X Y, Bai Z L, Liu W Y, Yang S S and Peng K C 2017 *Chin. Phys. B* **26** 040303
[5] Bucci M, Germani L, Luzzi R, Trifiletti and Varanonuovo M 2003 *IEEE Tran. Comput.* **52** 403
[6] Schmidt H 1970 *J. Appl. Phys.* **41** 462
[7] Uchida A, Amano K, Inoue M, Hirano K, Naito S, Someya H, Oowada I, Kurashige T, Shiki M, Yoshimori S, Yoshimura K and Davis P 2016 *Nat. Photon.* **2** 728
[8] Acin A and Masanes L 2016 *Nature* **540** 213
[9] Colbeck R and Renner R 2012 *Nat. Phys.* **8** 450
[10] Pironio S, Acin A, Massar S, Boyer de la Giroday A, Matsukevich D N, Maunz P, Olmschenk S, Hayes D, Luo L, Manning T A and Monroe C 2010 *Nature* **464** 1021
[11] Santha M and Vazirani U V 1984 *IEEE 25th Annual Symposium on Foundations of Computer Science* 434
[12] Brandao F G S L, Ramanathan R, Grudka A, Horodecki K, Horodecki M, Horodecki P, Szarek T and Wojewodka H 2016 *Nat. Commun.* **7** 11345
[13] Gallego R, Masanes L, de la Torre G, Dhara C, Aolita L and Acin A 2013 *Nat. Commun.* **4** 2654
[14] Grudka A, Horodecki K, Horodecki M, Horodecki P, Pawlowski M and Ramanathan R 2014 *Phys. Rev. A* **90** 032322
[15] Mironowicz P, Gallego R and Pawlowski M 2015 *Phys. Rev. A* **91** 032317
[16] Ramanathan R, Brandao F G S L, Horodecki K, Horodecki M, Horodecki P and Wojewodka H 2016 *Phys. Rev. Lett.* **117** 230501
[17] Li X 2016 arXiv:1608.00127
[18] Ghne O, Tth G, Hyllus P and Briegel H 2005 *Phys. Rev. Lett.* **95** 120405
[19] Cao Z, Zhou H Y, Yuan X and Ma X F 2016 *Phys. Rev. X* **6** 011020
[20] Marangon D G, Vallone G and Villoresi P 2017 *Phys. Rev. Lett.* **118** 060503