Experimental realization of device-independent quantum randomness expansion

Ming-Han Li,1,2 Xingjian Zhang,3 Wen-Zhao Liu,1,2 Si-Ran Zhao,1,2 Bing Bai,1,2 Yang Liu,1,2 Qi Zhao,1,2 Yuxiang Peng,3 Jun Zhang,1,2 Xiongfeng Ma,3 Qiang Zhang,1,2 Jingyun Fan,1,2 and Jian-Wei Pan1,2

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

Randomness is of paramount importance to human activities, from election to drug design and to digital cryptography. The origin of randomness and its applications are under active investigations. The recent realizations of device-independent quantum random number generation provide intrinsically unpredictable random numbers without trusting the inner working of devices, where a great deal of input randomness was used to generate a small output randomness. Randomness expansion—generating a longer sequence of random numbers from a short one, is viable in quantum mechanics but not allowed classically since all classical algorithms are essentially deterministic. Quantum randomness expansion is not only a fundamental question in science but also of practical interest. Here we report the first experimental realization of device-independent quantum randomness expansion by employing the quantum probability estimation framework. We demonstrate to generate output randomness exceeding the input randomness unpredictably by 512 bits at a latency of less than 8 mins, and to achieve an asymptotic rate of \( \approx 0.08 \) bit per trial, the largest for unpredictable random bits generation to date, with a failure probability \( 2^{-64} \approx 5.4 \times 10^{-20} \). Device-independent quantum randomness expansion harvesting quantum advantage not only furthers our understanding of randomness but also is resource-efficient in the generation of quantum-certifiable random bits for practical applications.

Randomness is not only a vital resource for nowadays information processing tasks, but also related to fundamental questions in science and philosophy. Does God play dice? The famous quote contains a question on the existence of randomness which is essential to our understanding of Nature. In general, random number generators can be classified into two categories: classical and quantum mechanical. The classical random number generation is completely predictable given the full knowledge of the random number generator. On the contrary, inherent randomness in quantum theory enables unpredictable quantum random number generation [1–6]. However, the securities of many quantum random number generators are based on the full characterization of devices, which poses significant challenge even to the most skillful experimentalist. Loop-hole free violation of Bell inequality provides us an alternative way to generate genuine randomness without characterizing the inner working of the untrusted devices [4], which is referred as device-independent quantum random number generator (DIQRNG). The security of DIQRNG against both classical and quantum adversaries was proven [6,13], which led to a number of remarkable experimental exhibitions [5,14,16] and the recent loophole free realizations [17,18]. This success directly inspires the device-independent quantum randomness expansion (DIQRE) [4], which takes a short random sequence as input and outputs a long sequence of random bits in a device-independent manner. The scientific merit of DIQRE is bi-fold, aside from being a unique quantum phenomenon that helps to understand the fundamentals about randomness and quantum theory, it is of practical usage in that DIQRE is resource-efficient in the generation of intrinsically unpredictable random numbers which are desired by a number of applications demanding high levels of security and randomness uniformity.

Realization of DIQRE presents a significant challenge to the experimental physics. While experimental realization of loophole free violation of Bell inequality is already a formidable task, experimentally efficient DIQRNG requests a larger violation of Bell inequality, and DIQRE raises the bar even higher. On one hand, entangled atomic systems [19,20] promise large violation of Bell inequality, these systems are currently constrained by low event rates, which makes it hard to accumulate enough statistics for analysis within a reasonable amount of time. On the other hand, entangled photonic systems [21,23] exhibit relatively small violation of Bell inequality but can be operated at high repetition rate, providing an opportunity. We present here a concrete realization of DIQRE based on loophole free violation of Bell inequality with entangled photons taking advantage of two recent advancements. One is the development of cutting-edge single-photon detection with near unity efficiency [24], which significantly improves the violation and output entropy in loophole free Bell test experiments, enabling the realization of DIQRE. The other is the development of randomness analysis techniques in DIQRNG protocols which generate random numbers efficiently. We note that two theoretical DIQRNG protocols attracted recent
outcome sequences by A model Bell test allowed by quantum mechanics. We denote the ical framework a model. In our case, the model is the set of all possible final states ρ.

In each experimental trial, Alice and Bob each determines an individual measurement setting locally and independently upon receiving a random input X, Y ∈ {0, 1} according to some probability distribution \( \{1 - q_1, q_1\} \times \{1 - q_2, q_2\} \) and delivers a random output A, B ∈ {0, 1}, respectively. Here we assume independent and identical distribution (i.i.d.) for input setting choices and fulfillment of measurement independence and locality constraints in the Bell test. For a total number of n experimental trials, we denote respectively the input sequences by X = (X₁, X₂, ..., Xₙ), Y = (Y₁, Y₂, ..., Yₙ), outcome sequences by A = (A₁, A₂, ..., Aₙ), B = (B₁, B₂, ..., Bₙ) for Alice and Bob, and denote Z = XY and C = AB for brevity. Lowercase letters denote the values the variables actually take in an experiment.

Consider that after n experimental trials, the possible final state shared by Alice, Bob and a possible adversary Eve in possession of quantum side information is a classical-quantum state, \( ρ = \sum_{c,z} |cz⟩⟨cz| \otimes ρ_E(cz) \). \( ρ_E(cz) \) is the sub-normalized state of Eve and \( \text{Tr}[ρ_E(CZ)] \) is the probability of a result (C, Z). We call the set of all possible final states ρ under a certain physical framework a model. In our case, the model is the set of all possible classical-quantum final states in the Bell test allowed by quantum mechanics. We denote the model \( C_Q \).

The amount of information-theoretically secure randomness that can be extracted against quantum side information \( I \) is quantified by the smooth min-entropy \( H_{\min}^\epsilon(C|ZE) \), which is lower bounded by α-Rényi entropy \( H_\alpha(C|ZE) \). α-Rényi entropy is closely related with α-Rényi powers \( R_\alpha(CZ|Z) \), which, for all possible states in the model, satisfies an inequality, \( \sum_{c,z} F(cz)R_\alpha(cz|z) ≤ 1 \). In our case we have α > 1. The positive real-valued function \( F(CZ) \), termed as quantum estimation factor (QEF), here is to estimate the lower bound to the smooth min-entropy without relying on any specific Bell inequality. If \( \log_2(F(CZ))/(α - 1) ≥ h_o > 0 \), the smooth min-entropy of the output is lower bounded by

\[
H_{\min}^\epsilon(C|ZE) ≥ h_o - \frac{1}{α - 1} \log_2 \left( \frac{2}{h_o^2} \right),
\]

where \( h_o \) is the amount of entropy witnessed by QEF \( F(CZ) \) and \( \epsilon_o \) is failure probability of randomness generation. Hence central to the protocol is to optimize QEF \( F(CZ) \) to maximize \( h_o \). Note that the model for a single trial in (2,2)-Bell test configuration can be well characterized [30]. Assuming i.i.d. inputs allows us to apply model-chaining over the sequence of experimental trials. We then update QEF by the \( n \)th trial, \( T_n \), as the multiplication of QEFs \( F_j(C_jZ_j) \) of single trials [27], i.e. \( T_n = \prod_{j=1}^{n} F_j(C_jZ_j) \), where we use Z and C to denote the input and output of single trials. The chain-ability of QEFs conveniently enables adaptability. We can vary QEFs for each individual trial in real time as long as they satisfy the defining inequality \( \sum_{c,z} F(cz)R_\alpha(cz|z) ≤ 1 \) for the single-trial model, and if the chained QEF by the \( i \)th trial \( T_i = \prod_{j=1}^{i} F_j(C_jZ_j) \) already witnesses the entropy set prior to the experiment, we stop the experiment with QEFs of subsequent single trials set to 1, which is a valid value satisfying the QEF definition.

With model chaining, the objective of QEF optimization is to maximize an expected output entropy rate with respect to a probability distribution \( ν(CZ) \), with \( ν(Z) = \sum_{c,z} ν(cz) \). If the experiment goes as expected, then the average entropy rate (without considering the failure probability) witnessed by F(CZ) is \( ξ_o(F;α) = \sum_{c,z} ν(cz) \log_2(F(cz))/ (α - 1) \). However, there is not a systematic way solving the QEF optimization efficiently in practice. Instead, a suggested method [27] is to first solve a counterpart optimization problem against classical side information, or the probability estimation factor (PEF) optimization [31], where the side information \( ρ_E(CZ) \) is restricted to be one-dimensional. The argument is that the expected entropy rate witnessed by PEF \( F(CZ) \) is nearly identical to QEF \( F(CZ) \), which was adopted with success in a recent experiment [18], and same here. The intuition is that quantum side information does not benefit an adversary more than classical side information significantly. Consequently, the optimized PEF can be validly used as a QEF with a scaling factor very close to unity (Appendix A.3).

Prior to the execution of randomness expansion, we first obtain the probability distribution \( ν(CZ) \) with a set of “training data” generated from a sequence of Bell test experiments to assist the optimization of QEF [18]. According to the protocol, we must appoint the target entropy of randomness expansion k (bits) and total failure probability \( \epsilon \) which encompasses \( \epsilon_o \) for randomness generation via a sequence of Bell test experiments and \( \epsilon_x \) for randomness extraction. We also need to appoint the largest allowed number of experimental trials \( N \) learning from the “training”. The expected number of trials to fulfill the assignment is determined by

\[
n_{\text{exp}} = \frac{k + \log_2(2/c_x^2)/(α - 1)}{ξ_o(F;α) - \epsilon_{\text{in}}},
\]
where $e_{in}$ is the input entropy rate. Considering statistical fluctuation we conservatively set $N = 2n_{exp}$ for all DIQRE tasks studied in this paper. With these set, we start the experiment on randomness expansion, update QEF $T_n$ with real-time data. If by the $n^{th}$ trial with $n \leq N$, $T_n$ witnesses that

$$\log_2(T_n)/(\alpha - 1) \geq k + n e_{in} + \log_2(2/e^2)/(\alpha - 1),$$  \hspace{1cm} (3)$$

we can certify that after taking a failure probability into consideration, the output randomness exceeds the input by an amount of $k$. The experiment succeeds and is stopped. We then apply a strong quantum-proof extractor to the sequence of output data. Denoting $n_{act} \equiv n$ the actual number of trials completing the task, $R_{exp} = k/n_{exp}$ the expected randomness expansion rate, and $R_{act} = k/n_{act}$ the actual randomness expansion rate, we expect $R_{act} \approx R_{exp}$ if the experiment behaves well (see Fig. (2)). If we do not witness a randomness expansion of $k$ by the end of $N$ trials, the experiment fails and we start over again.

Our experimental realization of DIQRE requires a few assumptions: (1) The devices and adversary observe quantum mechanics. (2) The outputs of the experiment are not leaked. (3) Alice and Bob's inputs are from independent and trusted sources, and are i.i.d. (4) Alice and Bob each has a trusted classical post-processing unit for randomness extraction. The second assumption can be guaranteed via the so-called secure labs. While in our DIQRE realization, we allow for the announcement of inputs after the experiment. We use a quantum-proof strong extractor, here the Toeplitz-matrix hashing extractor [32], which takes the experimental output sequence C in the Bell test, together with a uniform bit string S, or the seed, as the input, and delivers a string of near-uniform random bits. We do not consider the seed as entropy consumed in the experiment, because by definition the seed of a strong extractor can be reused albeit at the cost of a security parameter increased by $\epsilon_\pi$. [32]. Security is not compromised even if the seed is known by Eve, as long as it is independent of the raw data and the classical post-processing process is authenticated, as witnessed by the second and the fourth assumptions, respectively.

Our experimental realization of DIQRE is based on an upgraded entangled photonic platform which was used in a previous demonstration of DIQRNG against quantum adversaries [17] (Appendix B.1). In each experimental trial, a photon at the wavelength of 780 nm is injected into a periodically poled potassium titanyl phosphate (PPKTP) crystal enclosed in a Sagnac interferometer to probabilistically generate a pair of photons at the wavelength of 1560 nm in the polarization-entangled quantum state, which are sent via optical fibre to two remote stations, Alice and Bob, where they are projected into one of two measurement bases randomly before destructive detection by superconducting nanowire single-photon detectors (SNSPD). Non-signaling condition is enforced by keeping spacelike separation between events of emission of entangled photons in the source and measurements at the two stations and between events of Alice’s measurement and Bob’s measurement, as shown in Fig. 1.

We obtain an efficiency from creation in the source to measurement of photons at stations A and B; upper: corresponding spacetime analysis exhibiting spacelike separation between relevant events, drawn to the scale. (See Appendix B.4 for details.) The time segments correspond to time elapsed for: $T_R$—generation of a pair of entangled photons at the source; $T_{QRNG1,2}$—generation of random bits as input setting choice (1,2—station A,B); $T_{Delay1,2}$—delay between quantum random number generator (QRNG) and Pockels cell; $T_{PC1,2}$—Pockels cell gets ready for state measurement after receiving a random bit; $T_{M1,2}$—photon detector outputs an electronic signal.

![Fig. 1. Schematics of experimental configuration. Bottom: creation of a pair of entangled photons at the source and measurement of photons at stations A and B; upper: corresponding spacetime analysis exhibiting spacelike separation between relevant events, drawn to the scale. (See Appendix B.4 for details.) The time segments correspond to time elapsed for: $T_R$—generation of a pair of entangled photons at the source; $T_{QRNG1,2}$—generation of random bits as input setting choice (1,2—station A,B); $T_{Delay1,2}$—delay between quantum random number generator (QRNG) and Pockels cell; $T_{PC1,2}$—Pockels cell gets ready for state measurement after receiving a random bit; $T_{M1,2}$—photon detector outputs an electronic signal.](image-url)
TABLE I. Expected entropy rates with different bias ratios (without considering the failure probability).

| $r$  | $e_{in}$ | $\xi'_i(F;\alpha)$ | Expansion |
|------|----------|----------------------|-----------|
| 1    | 2        | 0.166456138          | No        |
| 600  | 0.035516523 | 0.113596013        | Yes       |

in the experiment, indicating a substantial improvement in the violation of Bell inequality and output randomness over our previous results [15, 17, 23]. This is critical to the realization of DIQRE. Besides, we use a biased probability distribution $\{1 - q_1, q_1\} \times \{1 - q_2, q_2\}$ for input setting choices. We set $q_1 = q_2 = q$, and define $(1 - q)/q$ as the bias ratio $r$. $r$ needs to be large such that the expected entropy rate $\sum x \nu(cz) \log_2(F(cz)) / (\alpha - 1) > e_{in}$, where $e_{in} = -2(q \log_2(q) + (1 - q) \log_2(q))$ is the input entropy per trial. We repeat the Bell test experiment at a repetition rate of 2 MHz.

Our first DIQRE assignment is to produce $k = 512$ random bits with a total failure probability $\epsilon = 2^{-64}$, which is a standardized request in many applications [18]. We perform some pre-experiments with different $r$ and optimize $F'(CZ)$ to derive expected entropy rates as described above (Appendix A), which predicts randomness expansion against classical side information, i.e., $\xi'_i(F';\alpha) = E_x \log_2(F'(CZ)) / (\alpha - 1)$ exceeds $e_{in}$ for $r = 600$, as shown in Table I. In comparison to DIQRNG which inputs 2 bits of randomness to generate 0.166456138 bit of randomness per trial, DIQRE expands an input randomness of 0.035516523 bit to 0.113596013 bit per trial and hence is more resource-efficient in random number generation. With the extraction failure probability set to $\epsilon_x = 2^{-100}$, the total failure probability is $\epsilon \approx \epsilon_x = 2^{-64}$. We find QEF using PEF with the scaling factor ranging in $[1, 1 + 1.71 \times 10^{-10}]$. The expected entropy rate witnessed by QEF is $\xi'_i(F;\alpha) = 0.113596013$ with $\alpha = 1 + 2.001001 \times 10^{-6}$. In this case $n_{exp} = 8.26 \times 10^4, N = 1.65 \times 10^4$.

We carry out the experiment in such a way that we update $\log_2 T_n$ with every 5 seconds of data as a block. Each block is composed of $n_b = 5 \times 2 \times 10^8$ trials. After $n = jn_b$ trials we have $\log_2 T_n = \log_2 T_{(\leq j)} = \log_2(\prod_{i=1}^{j} T_{(i)})$, where $T_{(i)}$ is the QEF of the $i$th block and $T_{(\leq j)}$ represents the accumulated QEF by the end of $j$th block. The accumulated expected output entropy (smooth line) exceeds the accumulated input entropy together with the failure probability term (dashed line) and the experimental results (dotted line) are consistent with the expectation (Fig. 2). We complete the task at a latency of less than 8 minutes (red open dot) and derive 512 random bits after applying the Toeplitz extractor (Appendix A). Here we count the latency starting from the 1st trial of randomness expansion, without including the time for “training” and extraction. We purposely take data longer than the required to test system stability. We estimate that it takes more than $10^{12}$ trials ($> 10^4$ minutes) to accomplish the same task with the latest development of EAT [25], suggesting that there is more room for improvement there.

We then perform a series of DIQRE tasks with $k = 2^\zeta$, $\zeta \in [9, 33]$ and $\zeta \in \mathbb{Z}$, all with a fixed failure probability $\epsilon_s = 2^{-64}$ in randomness generation. For each task, once we test the loophole free Bell inequality with $J \geq 0.751$, we begin to execute randomness expansion with the same set of parameters optimized for the task of $k = 512$ bits only with $N$ adjusted accordingly. Note that the QEF in the previous task is valid in this series of tasks with $\zeta \geq 9$, while may not support the tasks with $k < 512$ (see Appendix A). All tasks (including Toeplitz extraction) are accomplished as shown in Fig.3. This study allows us to examine the asymptotic behaviour of QEF under a constant failure probability. We show in this case the randomness expansion rate asymptotically approaches 0.08 bit per trial, the highest for intrinsically unpredictable random bit generation known to date.

In conclusion, we present an experimental realization of DIQRE, a quantum phenomenon without classical counterpart. This is a substantial progress towards the ultimate understanding of randomness. In particular, this may further inspire the research of other interesting directions of randomness, for example, randomness amplification [35], which, instead of requiring input ran-
domness to be independent of the devices, could amplify
the imperfect random bits into perfect ones. For these
tasks, possible candidates for input randomness source
could be cosmic randomness [26] and human randomness
[37]. DIQRE, which expands a very small random seed to
rather long sequence of random bits without compromis-
ing the security, possesses a great potential for realistic
applications demanding high level secure randomness.

ACKNOWLEDGMENTS

The authors would like to thank X. Yuan for enlighten-
ing discussions. This work has been supported by the Na-
tional Key R&D Program of China (2017YFA0304000),
the National Fundamental Research Program (under
Grant No. 2013CB336800), the National Natural Sci-
ence Foundation of China, and the Chinese Academy of
Science.

Appendix A: Theory of Device-Independent Quantum Randomness Expansion

In our experiment, we adopt a CHSH-type Bell test, i.e. (2,2,2)-Bell test configuration. The configuration involves
two stations, commonly referred to as ‘Alice’ and ‘Bob’. In each trial, Alice and Bob make independent local
measurements, where Alice’s setting choices form a random variable $X$ and Bob’s form $Y$, $X,Y \in \{0,1\}$. Their
outcomes form another two random variables $A,B$ ranging in the set $\{0,1\}$. We use subscripts to label the trial
number, and letters without subscripts represent variables in a general single trial. Quantum random number generator
involves one device in the final analysis, while the introduction of two parties (parts of the device) is the implication
of a non-signaling constraint between them. When we refer to the device as a whole, we denote the input to the device
as $Z = (X,Y)$ and output as $C = (A,B)$. $(C_i,Z_i)$ is called the result of the $i^{th}$ trial. For a sequence of trials, we use
letters in bold, that is, $\mathbf{Z} = (Z_1,Z_2,\cdots) = (XY)$ and similar for other letters. Following convention, lowercase letters
represent specific values the variables take in an experiment.

Ever since Colbeck first proposed the idea of quantum randomness expansion via Bell test in his PhD thesis [4] and
some pioneer works [5,6,8,9,12], much progress has been made on the security analysis of device-independent quan-
tum random number generation (DIQRNG). So far there are two major protocols promising information-theoretically
secure randomness generation in the presence of quantum side information and in a non-i.i.d condition with current
technology. One is based on entropy accumulation theorem (EAT), which requires a “min-tradeoff function” [13]. A
modified protocol further utilises NPA hierarchy method [25]. The other protocol is based on quantum estimation
factor (QEF) [27], which directly estimates the output entropy from the observed statistics. The two protocols each
has its own pros and cons: EAT has optimal asymptotic behaviour, while methods developed so far require a long
latency; QEF’s asymptotic behaviour has not been well characterised, yet it can be much more efficient for a small-size
randomness generation and experiments with a small Bell violation. Considering the characteristics of our optical
platform and task target, we employ the QEF method in our device-independent quantum randomness expansion
(DIQRE) experiment.

1. Models in Quantum Estimation Factor Framework

In QEF framework, the essence is a characterization of the set of possible final states in the experiment. After the
experiment, the joint state of the device and quantum side information is a classical-quantum state

$$
\rho = \sum_{cz} |cz\rangle \langle cz| \otimes \rho_E(cz).
$$

(A1)
\( \rho_E(\mathbf{cz}) \) is the quantum side information and \( \text{Tr}[\rho_E(\mathbf{cz})] \) is the probability of the result \((\mathbf{c}, \mathbf{z})\). For an adversary Eve in possession of the quantum side information, however, after the experiment with inputs announced, she can only be certain that the sub-normalized state in her possession is \( \rho_E(\mathbf{z}) = \sum_{\mathbf{c}} \rho_E(\mathbf{cz}) \). In our DIQRE experiment, the final state \( \rho \) comes from local quantum measurements on a joint quantum state. Suppose the initial state shared by Alice, Bob and Eve is \( \rho_{ABE} \), and the result observed by Alice and Bob is \( \mathbf{Z} = (X, Y), \mathbf{C} = (A, B) \). The positive-operator valued measurement (POVM) element can be expressed as \( P_{\mathbf{C}|\mathbf{Z}} = Q_{A|X} \otimes Q_{B|Y} \), with \( Q_{A|X}, Q_{B|Y} \geq 0, \sum_{\mathbf{a}} Q_{a|X} = \sum_{\mathbf{b}} Q_{b|Y} = 1 \). If the input \( \mathbf{Z} \) is drawn with a probability \( \mu(\mathbf{Z}) \), the final state is

\[
\rho = \sum_{\mathbf{cz}} |\mathbf{cz}\rangle \langle \mathbf{cz}| \otimes \left( \mu(\mathbf{z}) \text{Tr}_{AB}[\rho_{ABE}(P_{\mathbf{c}|\mathbf{z}} \otimes 1_E)] \right).
\] (A2)

In our DIQRE experiment, we denote the model as \( C_Q \).

It is difficult to deal with \( C_Q \) for many trials as a bulk directly, though. While as proved by Lemma 3.8 in [27], as long as future inputs are independent of past outputs given the quantum side information and input, i.e. the input of the \( i \)th trial \( z_i \), the inputs previous to the \( i \)th trial \( \mathbf{Z}_{<i} \) together with quantum side information \( E \) and the past outputs \( \mathbf{C}_{<i} \) form a quantum Markov chain

\[
Z_i \leftrightarrow \mathbf{Z}_{<i} E \leftrightarrow \mathbf{C}_{<i}, \tag{A3}
\]

we can construct the final model by chaining the model for trials previous to the \( i \)th trial \( C_{Q:<i} \) and the model of the \( i \)th trial \( C_{Q:i} \), and each model can be analysed individually. In our DIQRE experiment, we have assumed i.i.d. inputs, thus satisfying the quantum Markov condition between all adjacent single trials. Therefore we only need to focus on the model of a single trial.

The model for a single trial of \((2,2,2)\)-Bell test has been well investigated [30]. Here we use the results of Theorem 8.1 in [27] for subsequent analysis. For a single trial, the model can be expressed as the convex combination of states in the form

\[
\rho = \mu(Z)U^{1/2}P_{\mathbf{C}|\mathbf{Z}}T^{1/2}U^†, \tag{A4}
\]

where \( \tau \geq 0, U \) is an isometry: \((\mathbb{C}^2)^{\otimes 2} \to \mathcal{H}(E)\). With a discussion on the dimension, it is known that \( \mathcal{H}(E) \) can be restricted to \( \mathbb{C}^4 \) [38]. The measurement operator \( P_{\mathbf{C}|\mathbf{Z},\theta} = Q_{A|X;\theta_1} \otimes Q_{B|Y;\theta_2} \). Here we introduce the parameter \( \theta = (\theta_1, \theta_2) \) to characterize the measurement operators, where

\[
Q_{a|0;\theta_1} = \frac{I + (-1)^a\sigma_z}{2},
\]

\[
Q_{a|1;\theta_1} = \frac{I + (-1)^a[\cos(\theta_1)\sigma_z + \sin(\theta_1)\sigma_x]}{2}, \quad \theta_1 \in (-\pi, \pi],
\] (A5)

and a similar representation holds for Bob’s measurement operators.

2. Quantum Estimation Factor

For a concrete model, we can define quantum estimation factors (QEF).

**Definition 1.** (Rényi powers) Let \( \rho \geq 0 \), and the support of \( \rho \) lies in \( \sigma \geq 0 \), \( \beta = \alpha - 1 > 0 \). The Rényi power of order \( \alpha \) of \( \rho \) conditional on \( \sigma \) is

\[
\mathcal{R}_\alpha(\rho|\sigma) = \text{Tr}\left[ (\sigma^{-\beta/(2\alpha)} \rho \sigma^{-\beta/(2\alpha)})^\alpha \right]. \tag{A6}
\]

**Definition 2.** (Quantum estimation factor) The positive real-valued function \( F(\mathbf{CZ}) \) is a quantum estimation factor (QEF) with power \( \beta > 0 \) for the model \( C_Q \), if \( F(\mathbf{CZ}) \) satisfies the following inequality with power \( \beta \) for \( \forall \rho \in C_Q \)

\[
\sum_{\mathbf{cz}} F(\mathbf{cz}) \mathcal{R}_\alpha(\rho_E(\mathbf{cz})|\rho_E(\mathbf{z})) \leq 1. \tag{A7}
\]

In the following we write \( \mathcal{R}_\alpha(\mathbf{CZ}|\mathbf{Z}) := \mathcal{R}_\alpha(\rho_E(\mathbf{cz})|\rho_E(\mathbf{z})) \) for brevity and in accordance with the main text. By definition the QEF can be naturally interpreted as an estimator of the Rényi power Via Markov’s inequality. It can be proved then that the QEF provides a valid lower bound to the smooth min-entropy (Theorem 4.18 in [27]).
Theorem 1. Suppose $F(CZ)$ is a valid QEF with power $\beta$ for the model $C_Q$. For an arbitrary state $\rho \in C_Q$, fix $1 \geq p > 0$ and $\epsilon > 0$, such that $\min_{cz} F(cz) = 2/(p^2 \cdot \epsilon^2)$. Then the $\epsilon$-smooth min-entropy of the state $\rho$ can be lower bounded by

$$H_{\min}^\epsilon(CZE) \geq -\log_2(p) = \log_2(\min(F(cz)))/\beta + \log_2 \left( \frac{\epsilon^2}{2} \right) / \beta.$$  

(A8)

With model chaining, we just need to analyze a single trial. The QEF for the entire experimental sequence can be obtained by QEF chaining, that is, the overall QEF $T_n(CZ)$ for a sequence of $n$ trials is the multiplication of single trial QEFs $F_i(C_iZ_i)$

$$T_n(CZ) = \prod_{i \leq n} F_i(C_iZ_i).$$  

(A9)

3. Optimization of Quantum Estimation Factor

In a DIQRE experiment, we need to optimize the QEF used for witnessing quantum randomness. If the experiment has a stable behaviour, we may expect the existence of some probability distribution $\nu(CZ)$ behind the result. We can use a same single trial QEF for all trials, and optimize it to maximize the right-hand side of Eq. (A8) for a total of $n$ trials

$$\max \frac{1}{\beta} \left\{ n \sum_{cz} \nu(cz) \log_2(F(cz)) + \log_2 \left( \frac{\epsilon^2}{2} \right) \right\},$$

s.t. $\sum_{cz} F(cz) R_\alpha(cz|z) \leq 1.$  

(A10)

The quantity $\xi_{\nu}^\epsilon = (\sum_{cz} \nu(cz) \log_2(F(cz)) + \log_2(\epsilon^2/2)/n) / \beta$ can be regarded as the expected entropy rate, taking consideration of a failure probability of $\epsilon$. No efficient direct optimization of Eq. (A10) has been developed, though. While a sub-optimal solution can be accepted, as long as it does not compromise security, i.e. the solution satisfies the constraint in Eq. (A10). A heuristic solution is to first solve a similar optimization, however, wherein the adversary is constrained to be a classical one, and rescale that solution with some coefficient to derive a valid QEF. The first step of the optimization is the so-called optimization of probability estimation factor (PEF), proposed in [31]. We write the PEF as $F'(CZ)$. In this case Eve’s system is restricted to be one-dimensional. Therefore the original $p_E(CZ)$ defined above degenerates to a probability distribution. We write the corresponding model as $C_C$, which becomes a set of joint probability distributions $\rho'$. And in the case of classical side information, the error term becomes $\log_2(\epsilon)$. If we take $\epsilon$ in the form of $\epsilon = 2^{-\frac{1}{2} \alpha \kappa}$, with $\alpha = E_{\nu} \log_2(F'(CZ))/\beta$, the optimization problem can be taken as

$$\max_{F'(CZ), \beta} (1 - \kappa/\beta) E_{\nu} \left( \log_2(F'(CZ))/\beta \right),$$

s.t. $F'(CZ) \geq 0$, $\forall cz$,

$$\sum_{cz} F'(cz) \rho'(cz|z) \beta \rho'(cz) \leq 1$, $\forall \rho' \in C_C,$

(A11)

This optimization problem is a concave maximization problem over a convex set, to which a global optimal solution can be found in principle. Directly solving this optimization problem is still difficult, though. The probability distributions come from measuring quantum states. Possible probability distributions form a convex set, yet not a polytope, hence going over the solving domain determined by the constraints is no easy task. While approximate solutions to this method can be derived with appropriate expansion of the solving domain into a polytope. This does not lead to security problems in the context of an adversary in hold of classical side information, as the PEFs determined in the modified optimization is $\epsilon$-sound against the worst conditional probability (Eve’s optimal guessing probability) possible in this enlarged set, which is absolutely at least $\epsilon$-sound against all conditional probability distributions possible from quantum measurements. Besides, the solution to the PEF optimization needs further rescaling to satisfy the QEF definition. In our experiment, we optimize the PEF over a domain determined by 8 PR-boxes [39] and the corresponding Tsirelson’s bounds [38]. In all, the modified optimization problem is defined over a polytope with 80 extreme points, and they can be constructed by PR-boxes and local deterministic points [40].
Then the optimization becomes
\[
\begin{align*}
\max_{F'(CZ), \beta} & \quad (1 - \kappa/\beta) E_\nu \left( \log_2(F'(CZ))/\beta \right), \\
\text{s.t.} & \quad F'(CZ) \geq 0, \forall \varepsilon_z, \\
& \quad \sum_{\varepsilon_z} F'(cz) \rho_k(z) \rho_k'(cz) \leq 1, k = 1, 2, \ldots, K, \\
& \quad \beta > 0. 
\end{align*}
\] (A12)

\( \rho_k'(CZ) \) are the extremal points of this convex polytope model.

After obtaining the optimal PEF \( F'(CZ) \), we rescale it to obtain a QEF. We first normalize \( F'(CZ) \) such that \( \sum_{\varepsilon_z} F'(cz) = 1 \). Then we introduce a parameter \( f_{\max} \) and solve the optimization problem
\[
\begin{align*}
f_{\max} &= \max \sum_{\varepsilon_z} \mu(z) F'(cz) (\text{Tr}[P_{cz;\theta}^{1/\alpha} P_{cz;\theta}])^\alpha, \\
\text{s.t.} & \quad \theta = (\theta_1, \theta_2) \in [0, \pi] \times [0, \pi], \tau \geq 0 \text{ with } \text{Tr}[\tau] = 1. 
\end{align*}
\] (A13)

The value \( F'(CZ)/f_{\max} \) delivers a valid QEF. For fixed \( \theta \), \( f_{\max} \) is concave with respect to \( \tau \), and we apply a Frank-Wolfe type optimization \( 41 \). Optimization over \( \theta \) is cumbersome, though. While it suffices to derive an upper bound of \( f_{\max} \), and we have the following result (Lemma 8.3 in \( 27 \)):

**Lemma 1.** Denote \( f_{\max}(\theta) = \max \sum_{\varepsilon_z} \mu(z) F'(cz) (\text{Tr}[\tau^{1/\alpha} P_{cz;\theta}])^\alpha \) for fixed \( \theta = (\theta_1, \theta_2) \). Consider \( \theta, \theta' \) such that \( \theta - \theta' = e_i \phi_i \) where \( \phi_i \in (0, \pi/2] \) and \( e_i \) is a two-dimensional vector with its \( i \)-th element equal to unity and the other zero. Let \( f = f_{\max}(\theta) \) and \( f' = f_{\max}(\theta') \), then for the point in between \( \theta \) and \( \theta' \) in the parameter space, i.e. \( \forall \phi \in [0, \phi], \theta'' = \theta + \phi e_i, \) we have
\[
f_{\max}(\theta'') \leq u(\varphi) := \frac{(\sin(\varphi - \phi) + \sin(\varphi))^2 (\sin(\phi - \varphi) f + \sin(\varphi) f')}{\sin(\phi)^2} \leq \left( \frac{\phi}{\sin(\phi)} \right)^\alpha \max(f, f').
\] (A14)

We first divide the parameter space determined by \( \theta_1, \theta_2 \) and calculate the values \( f(\theta) \) on the mesh grid. This gives us a lower bound to the upper bound to \( f_{\max} \). Applying the lemma gives us an upper bound to \( f_{\max} \). By iteratively using this lemma and refining the mesh, we can tighten the gap between these two values.

**Appendix B: System characterization**

1. **Entangled photon pairs: creation, delivery and measurement**

Fig. 4 is the experimental schematics for creation, delivery and detection of entangled photon pairs. We create entangled photon pairs at 1560 nm based on type-II spontaneous parametric downconversion (SPDC), which has negligible loss propagating through 100 meter optical fibre. We enclose a periodically poled potassium titanyl phosphate (PPKTP) crystal with poling period 46.5 \( \mu \)m in a Sagnac loop. With the injection of a pump pulse at wavelength of 780 nm and pulse width of 10 ns, the loop emits a pair of polarization-entangled photons at 1560 nm. We set the beam waist to be 180 \( \mu \)m for the pump beam (780 nm) and 85 \( \mu \)m for the collection beam (1560 nm) to optimize the efficiency to couple the generated photons at 1560 nm into optical fibre \( 42 \). The free space distance between Alice’s (Bob’s) measurement station and the source is 93 (90) m and the fibre length is 130 (118) m. We assign it a trial beginning with the emission of a pump pulse at 780 nm through measurement completion by Alice and Bob. We repeat such a trial at a rate of 2 MHz. In each trial, Alice and Bob each receives a random bit “0” or “1” from a quantum random number generator (QRNG) \( 15, 17 \) to set Pockels cell at zero or half-wave voltage, following probability distribution \( (q_1, 1 - q_1) \times (q_2, 1 - q_2) \). We set \( q_1 = q_2 = q \) and \( q/(1 - q) = 600 : 1 \) in this experiment to realize randomness expansion. We use a polarization controller and a half-wave plate to compensate polarization drift in the experiment. The photons are detected by superconducting nanowire single-photon detectors (SNSPDs) \( 24 \). All detection results are recorded with a time-to-digital converter (TDC).

2. **Determination of single photon efficiency**

We define the single photon heralding efficiency as \( \eta_A = C/N_B \) and \( \eta_B = C/N_A \) for Alice and Bob, in which two-photon coincidence events \( C \) and single photon detection events for Alice \( N_A \) and Bob \( N_B \) are measured in the experiment. The heralding efficiency is given by
\[
\eta = \eta_A^{sc} \times \eta_A^{ao} \times \eta_B^{fibrc} \times \eta_m \times \eta_{det},
\] (B1)
FIG. 4. Schematics of the experiment. a) Creation of pairs of entangled photons: Light pulses of 10 ns, 2 MHz from a 1560 nm seed laser (LD) are amplified by an erbium-doped fibre amplifier (EDFA), and frequency-doubled in an in-line periodically poled lithium niobate (PPLN) waveguide. With the residual 1560 nm light removed by a wavelength-division multiplexer (WDM) and spectral filters, the 780 nm light pulses are focused into a periodically poled potassium titanyl phosphate (PPKTP) crystal in a Sagnac loop to generate polarization-entangled photon pairs. A set of quarter-wave plate (QWP) and half-wave plate (HWP) are used in the creation of non-maximally polarization-entangled two-photon state. The residual 780 nm pump light is removed by dichroic mirrors (DMs). The two photons of an entangled pair at 1560 nm travel in opposite directions to two remote measurement stations Alice and Bob, where they are subject to polarization state measurements. b) Single photon polarization measurement: In the measurement station, Alice (Bob) uses Pockels Cell to project the single photon into one of two pre-assigned measurement bases, upon receiving an input from a random number generator and then detect single photon by superconducting nanowire single-photon detectors (SNSPD). A time-digital convertor (TDC, not shown) is used to time-tag the events for random number generation and single-photon detection.

where $\eta^{sc}$ is the efficiency to couple entangled photons into single mode optical fibre, $\eta^{so}$ the efficiency for photons passing through the optical elements in the source, $\eta^{fibre}$ the transmittance of fibre connecting source to measurement station, $\eta^{m}$ the efficiency for light passing through the measurement station, and $\eta^{det}$ the single photon detector efficiency. $\eta^{so}$, $\eta^{fibre}$, $\eta^{m}$, $\eta^{det}$ can be measured with classical light beams and NIST-traceable power meters. The coupling efficiency $\eta^{sc}$ is derived as

$$\eta^{sc} = \frac{\eta}{\eta^{so} \times \eta^{fibre} \times \eta^{m} \times \eta^{det}}, \quad (B2)$$

| Parties | Heralding, $\eta$ | $\eta^{sc}$ | $\eta^{so}$ | $\eta^{fibre}$ | $\eta^{m}$ | $\eta^{det}$ |
|---------|-----------------|--------------|--------------|----------------|--------------|--------------|
| Alice   | 80.87%          | 92.7%        | 95.9%        | 99%            | 95.1%        | 96.6%        |
| Bob     | 81.98%          | 93.1%        | 95.9%        | 99%            | 95.3%        | 97.3%        |

The transmittance of optical elements used in our experiment are listed in Table III, with which we obtain the efficiency $\eta^{so}$:

$$\eta^{so} = \eta^{AS} \times \eta^{S} \times (\eta^{DM})^4 \times \eta^{780/1560HWP} \times \eta^{780/1560PBS} \times \eta^{PPKTP} = 95.9\%,$$  

(B3)
where we use four dichroic mirrors.

The transmittance of the 130 meter fibre connecting source and detection is 99%. The transmittance of the measurement station including Pockels cell is 95.1% for Alice and 95.3% for Bob. The efficiency of SNSPD [24] (from company: PhotonSpot) is measured to be 96.6% for Alice and 97.3% for Bob, which is significantly higher than that of our previous experimental realization of device-independent quantum random number generation [17]. The single photon heralding efficiency of the system is determined to be \(\eta_A = (80.87 \pm 1.9\%)\) for Alice and \(\eta_B = (81.98 \pm 1.5\%)\) for Bob with photon-counting statistic in the experiment.

### TABLE III. The efficiencies of optical elements.

| Symbol | Optical element | Efficiency |
|--------|-----------------|------------|
| \(\eta^{AS}\) | Aspherical lens | 99.27\% ± 0.03\% |
| \(\eta^S\) | Spherical lens | 99.6\% ± 1.0\% |
| \(\eta^{780/1560HWP}\) | Half wave plate (780nm/1560nm) | 99.93\% ± 0.02\% |
| \(\eta^{1560HWP}\) | Half wave plate (1560nm) | 99.92\% ± 0.04\% |
| \(\eta^{1560QWP}\) | Quarter wave plate (1560nm) | 99.99\% ± 0.08\% |
| \(\eta^{780/1560PBS}\) | Polarizing beam splitter (780nm/1560nm) | 99.6\% ± 0.1\% |
| \(\eta^{1560PBS}\) | Polarizing beam splitter (1560nm) | 99.6\% ± 0.2\% |
| \(\eta^{DM}\) | Dichroic mirror | 99.46\% ± 0.03\% |
| \(\eta^{PPKTP}\) | PPKTP | 99.6\% ± 0.2\% |
| \(\eta^P\) | Pockels cell | 98.7\% ± 0.5\% |

3. Quantum state and measurement bases

To maximally violate the Bell inequality in experiment, we create non-maximally entangled two-photon state \[\cos(24.3^\circ) |HV\rangle + \sin(24.3^\circ) |VH\rangle\] and set measurement bases to be \(A_1 = -83.08^\circ\) and \(A_2 = -118.59^\circ\) for Alice, and \(B_1 = 6.92^\circ\) and \(B_2 = -28.59^\circ\) for Bob, respectively.

We measure diagonal/anti-diagonal visibility in the bases set \(\{45^\circ, -24.3^\circ\}\), \(\{114.3^\circ, 45^\circ\}\) for minimum coincidence, and in the bases set \(\{(45^\circ, 65.7^\circ), (24.3^\circ, 45^\circ)\}\) for maximum coincidence, where the angles represent measurement basis \(\cos(\theta) |H\rangle + \sin(\theta) |V\rangle\) for Alice and Bob. By setting the mean photon number to \(\mu = 0.0025\) to suppress the multi-photon effect, we measure the visibility to be 99.5\% and 98.4\% in horizontal/vertical basis and diagonal/anti-diagonal basis.

We perform quantum state tomography measurement of the non-maximally entangled state, with result shown in Fig. 5. The state fidelity is 99.16\%. We attribute the imperfection to multi-photon components, imperfect optical elements, and imperfect spatial/spectral mode matching.

4. Spacetime configuration of the experiment

To close the locality loophole, space-like separation must be satisfied between relevant events at Alice and Bob’s measurement stations: the state measurement events by Alice and Bob, measurement event at one station and the setting choice event at the other station (Fig. 6). We then obtain

\[
\begin{cases} 
\frac{|SA| + |SB|}{c} > T_E - (L_{SA} - L_{SB})/c + T_{QRNG1} + T_{Delay1} + T_{PC1} + T_{M2}, \\
\frac{|SA| + |SB|}{c} > T_E - (L_{SA} - L_{SB})/c + T_{QRNG2} + T_{Delay2} + T_{PC2} + T_{M1}, 
\end{cases}
\]

(B4)

where \(|SA| = 93\ m\) (\(|SB| = 90\ m\)) is the free space distance between entanglement source and Alice’s (Bob’s) measurement station, \(T_E = 10\ ns\) is the generation time for entangled photon pairs, which is mainly contributed by the 10 ns pump pulse duration, \(L_{SA} = 191\ m\) (\(L_{SB} = 173.5\ m\)) is the effective optical path which is mainly contributed by the long fibre (130 m, 118 m) between source and Alice/Bob’s measurement station, \(T_{QRNG1} = T_{QRNG2} = 96\ ns\) is the time elapse for QRNG to generate a random bit, \(T_{Delay1} = 270\ ns\) (\(T_{Delay2} = 230\ ns\)) is the delay between QRNG and Pockels cells, \(T_{PC1} = 112\ ns\) (\(T_{PC2} = 100\ ns\)) including the internal delay of the Pockels Cells (62 ns, 50 ns) and the time for Pockels cell to stabilize before performing single photon polarization state projection after
switching which is 50 ns, $T_{M1} = 55$ ns ($T_{M2} = 100$ ns) is the time elapse for SNSPD to output an electronic signal, including the delay due to fibre and cable length.

Measurement independence requirement is satisfied by space-like separation between entangled-pair creation event and setting choice events, so we can have

\[
\begin{aligned}
|SA|/c > L_{SA}/c - T_{Delay1} - T_{PC1} \\
|SB|/c > L_{SB}/c - T_{Delay2} - T_{PC2}
\end{aligned}
\] (B5)

As shown in Fig. 6, Alice’s and Bob’s random bit generation events for input setting choices are outside the future light cone (green shade) of entanglement creation event at the source.

Appendix C: Experimental Results

1. Randomness expansion task: 512 bits

Our first device-independent quantum randomness expansion (DIQRE) task is set to produce 512 bits in randomness expansion. We examine four such experiment instances. In each instance, before the randomness expansion process is formally executed, we first optimize the single trial QEF with respect to a set of “training data”, which is generated from a sequence of loophole free Bell test experiments, with a local setting bias ratio $r = 600$. The input entropy rate is $e_{in} = 0.035516523$. As stated in Sect. A, we first optimize a PEF under the PR-boxes and Tsirelson’s bounds. We set $\kappa = 1 \times 10^{-6}$ in Eq. (A11). The power $\beta$ of the optimized PEF is $\beta = 2.001001001 \times 10^{-6}$. After obtaining the PEF, we normalize it and solve the optimization of $f_{\text{max}}$ in Eq. (A13). Such an optimization problem is tackled via the parallel computation toolbox in Matlab. The overall QEF rescaling factor is the multiplication of the sum of the 16 PEF values and $f_{\text{max}}$. We derived an upper bound of $1 + 1.71 \times 10^{-10}$ to the rescaling factor, indicating that the PEF can be used as a QEF. The expected output entropy rate witnessed by the QEF is $\xi_{F}(n;\alpha) = 0.113596013$, and the expected number of trials to reach our target is $n_{\exp} = 8.26 \times 10^8$. We conservatively set the largest allowed number of trials $N = 2n_{\exp} = 1.65 \times 10^9$. For the optimization of $f_{\text{max}}$, we used 24 workers for parallel computation and it costs about 17.5 hours. The average time to actually accomplish the expansion task is less than 8 minutes, see Table IV.

In Table IV, we list the time for experiment and extraction for a few selected expansion tasks.

2. Randomness extraction

We use Toeplitz extractor in the experiment, which takes the experimental output as input and delivers a sequence of near uniform random bits [17, 32, 33, 44].
FIG. 6. Spacetime analysis of the experiment. \( T_E = 10 \) ns is the time elapse to generate a pair of entangled photons. \( T_{QRNG1,2} \) is the time elapse to generate random bits to switch the Pockels cell. \( T_{Delay1,2} \) is the delay between QRNG and the Pockels cell. \( T_{PC1,2} \) is the time elapse for the Pockels cell to be ready to perform state measurements after receiving the random bits from the QRNG. \( T_{M1,2} \) is the time elapse for the SNSPD to output an electronic signal. For \( T_{QRNG1} = T_{QRNG2} = 96 \) ns, \( T_{Delay1} = 270 \) ns and \( T_{Delay2} = 230 \) ns, \( T_{PC1} = 112 \) ns and \( T_{PC2} = 100 \) ns, \( T_{M1} = 55 \) ns and \( T_{M2} = 100 \) ns, we place Alice’s measurement station and Bob’s measurement station on the opposite side of the source and 93 ± 1 (90 ± 1) meter from the source, and set the effective optical length between Alice’s (Bob’s) station and the source to be 130 m (118 m). This arrangement ensures spacelike separation between measurement event and distant base setting event and between base setting event and photon pair emission event.

A \( m \times n \) Toeplitz matrix takes the form,

\[
T_{m \times n} = \begin{pmatrix}
a_0 & a_1 & \cdots & a_{-(n-2)} & a_{-(n-1)} \\
a_1 & a_0 & \cdots & a_{-(n-3)} & a_{-(n-2)} \\
a_2 & a_1 & \cdots & a_{-(n-4)} & a_{-(n-3)} \\
\vdots & \vdots & \ddots & \ddots & \vdots \\
a_{m-1} & a_{m-2} & \cdots & a_{-(n+1)} & a_{-(n+2)} \\
a_{m} & a_{m-1} & \cdots & a_{-(n)} & a_{-(n+1)}
\end{pmatrix},
\]

(C1)
TABLE IV. Characteristics of four instances for randomness expansion task of 512 bits. \( \epsilon_s = 2^{-64} \approx 5.42 \times 10^{-20} \). \( N = 2^n_{exp} \), where \( n_{exp} \) is the number of trials determined empirically from “training” [18]. \( n_{act} \) is the actual number of trials executed in an instance to achieve the set goal of 512 bits. The expansion rate is estimated by \( 512/n_{act} \). We update the accumulated output entropy every 5 seconds with a data block containing the latest \( 5 \times 2 \times 10^6 = 10^7 \) trials.

\begin{tabular}{cccccc}
Instance & Number of Training blocks & \( N \times 10^6 \) & \( n_{act} \times 10^6 \) & Number of blocks & Expansion rate \( \times 10^{-7} \) \\
1 & 1440 & 14.51 & 8.90 & 89 & 5.75 \\
2 & 2160 & 16.28 & 8.50 & 85 & 6.02 \\
3 & 2880 & 16.21 & 7.40 & 74 & 6.92 \\
4 & 3600 & 15.98 & 8.80 & 88 & 5.82 \\
\end{tabular}

The experimental output is written in the form of a \( n \)-dimensional vector,

\[ V_n = \begin{pmatrix} v_0 \\ v_1 \\ v_2 \\ \vdots \\ v_{n-1} \end{pmatrix}. \]  

(C2)

The output of the Toeplitz extractor is a sequence of nearly uniform random bits \( R_m \), with

\[ R_m = \begin{pmatrix} r_0 \\ r_1 \\ r_2 \\ \vdots \\ r_{m-1} \end{pmatrix}. \]  

(C3)

We use the fast Fourier transform (FFT) to speed up the multiplication,

\[ T_{m \times n} \times V_n = IFFT(FFT(T_{m+n-1} \cdot FFT(V_m))). \]  

(C4)

Here FFT is the fast Fourier transform on the vector, \( T_{m+n-1} \) is the elements \((a_{-(n-1)}, ..., a_{-1}, a_0, a_1, ..., a_{m-1})\) in the Toeplitz matrix. IFFT is the inverse fast Fourier transform of the product of the vectors. The vector dimension should be expand to \( m+n-1 \) by adding zeros at the end.

In our experiment, we divide the matrix into \( k = n/l \) blocks each with dimension \( m \times l \),

\[ T_{m \times n} = \begin{pmatrix} T_{m \times l}^0 & T_{m \times l}^1 & \cdots & T_{m \times l}^{k-1} \end{pmatrix}, \]  

(C5)

with block \( T_{m \times l}^i \) given by

\[ T_{m \times l}^i = \begin{pmatrix} a_{-i-l} & a_{-(i+l+1)} & \cdots & a_{-(i+l+1-1)} \\ a_{-i-l+1} & a_{-i-l} & \cdots & a_{-(i+l+1)+1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{-i-l+m-1} & a_{-i-l+m-2} & \cdots & a_{-(i+l+1)+m-1} \end{pmatrix}. \]  

(C6)

Similarly, we divide the vector into \( k \) blocks,

\[ V_n = \begin{pmatrix} V_{l}^0 \\ V_{l}^1 \\ \vdots \\ V_{l}^{k-1} \end{pmatrix}. \]  

(C7)
with each block given by

$$V_i^j = \begin{pmatrix} v_{i,0} \\
v_{i,1} \\
\vdots \\
v_{i,t-1} \end{pmatrix}.$$  \hspace{1cm} (C8)

We then apply FFT to each block. The results are given by

$$R'_m = \begin{pmatrix} R_i^0 \\
R_i^1 \\
\vdots \\
R_i^{k-1} \end{pmatrix},$$  \hspace{1cm} (C9)

where $R_i^j = T_{i \times t} \cdot V_i^j$, which is given by

$$R_i^j = \begin{pmatrix} r_i^0 \\
r_i^1 \\
\vdots \\
r_i^{m-1} \end{pmatrix}.$$  \hspace{1cm} (C10)

The final result is given by

$$R_m = \begin{pmatrix} \Sigma_i r_i^0 \\
\Sigma_i r_i^1 \\
\vdots \\
\Sigma_i r_i^{m-1} \end{pmatrix}.$$  \hspace{1cm} (C11)

The blocked algorithm is slower than the full FFT algorithm, but it saves memory.

TABLE V. Time consumed for different expansion tasks (with parameters optimized for the task of achieving 512 bits in randomness expansion). We perform the extraction calculation on a personal computer with 16 Gbytes memory. The extraction time includes data loading and computation.

| Expansion tasks (bits) | Expected expansion experiment time (s) | Actual expansion experiment time (s) | Extraction time (s) | Blocks in extraction |
|------------------------|----------------------------------------|--------------------------------------|---------------------|----------------------|
| $2^9$                  | 412.84                                 | 445                                  | 2286.42             | 30                   |
| $2^{15}$               | 413.04                                 | 445                                  | 2302.11             | 30                   |
| $2^{21}$               | 426.26                                 | 450                                  | 2884.16             | 40                   |
| $2^{24}$               | 520.27                                 | 570                                  | 3121.85             | 50                   |

[1] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, npj Quantum Inform. 2, 16021 (2016).
[2] A. Acín and L. Masanes, Nature 540, 213 (2016).
[3] M. Herrero-Collantes and J. C. Garcia-Escartin, Rev. Mod. Phys. 89, 015004 (2017).
[4] R. Colbeck, Ph.D. thesis, Trinity College, University of Cambridge (2006).
[5] S. Pironio, A. Acín, S. Massar, A. B. de La Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, et al., Nature 464, 1021 (2010).
[6] S. Fehr, R. Gelles, and C. Schaffner, Phys. Rev. A 87, 012335 (2013).
[7] S. Pironio and S. Massar, Phys. Rev. A 87, 012336 (2013).
[8] U. Vazirani and T. Vidick, in Proceedings of the Forty-fourth Annual ACM Symposium on Theory of Computing, STOC ‘12 (ACM, New York, NY, USA, 2012) pp. 61–76.
[9] C. A. Miller and Y. Shi, in Proceedings of the 46th Annual ACM Symposium on Theory of Computing, STOC ’14 (ACM, New York, NY, USA, 2014) pp. 417–426.
[10] K.-M. Chung, Y. Shi, and X. Wu, arXiv:1402.4797 (2014).
[11] M. Coudron and H. Yuen, in Proceedings of the 46th Annual ACM Symposium on Theory of Computing (ACM, 2014) pp. 427–436.
