Research Article

ADVANCED PHOTONICS

Realization of a source-device-independent quantum random number generator secured by nonlocal dispersion cancellation

Ji-Ning Zhang,[a,b,c] Ran Yang,[a,b,c] Xinhui Li,[a,b,c,*] Chang-Wei Sun,[a,b,c] Yi-Chen Liu,[a,c,d] Ying Wei,[a,b,c] Jia-Chen Duan,[a,b,c] Zhenda Xie,[a,c,e] Yan-Xiao Gong,[a,b,c,f,*] and Shi-Ning Zhu[a,b,c]

[a]Nanjing University, National Laboratory of Solid State Microstructures, Nanjing, China
[b]Nanjing University, School of Physics, Nanjing, China
[c]Nanjing University, Collaborative Innovation Center of Advanced Microstructures, Nanjing, China
[d]Qingdao University of Technology, School of Science, Qingdao, China
[e]Nanjing University, School of Electronic Science and Engineering, Nanjing, China
[f]Hefei National Laboratory, Hefei, China

Abstract. Quantum random number generators (QRNGs) can provide genuine randomness by exploiting the intrinsic probabilistic nature of quantum mechanics, which play important roles in many applications. However, the true randomness acquisition could be subjected to attacks from untrusted devices involved or their deviations from the theoretical modeling in real-life implementation. We propose and experimentally demonstrate a source-device-independent QRNG, which enables one to access true random bits with an untrusted source device. The random bits are generated by measuring the arrival time of either photon of the time–energy entangled photon pairs produced from spontaneous parametric downconversion, where the entanglement is testified through the observation of nonlocal dispersion cancellation. In experiment, we extract a generation rate of 4 Mbps by a modified entropic uncertainty relation, which can be improved to gigabits per second by using advanced single-photon detectors. Our approach provides a promising candidate for QRNGs with no characterization or error-prone source devices in practice.

Keywords: source device independence; quantum randomness; nonlocal dispersion cancellation; time–energy entanglement.

Received Nov. 21, 2022; revised manuscript received Mar. 6, 2023; accepted for publication Apr. 13, 2023; published online May 5, 2023.

[DOI: 10.1117/1.AP.5.3.036003]

1 Introduction

Random numbers are important resources in scientific and practical applications. Classical random number generators deny the existence of unpredictability, which cannot provide secure randomness. In contrast, quantum random number generators (QRNGs) can generate genuine randomness from the inherent indeterminacy of quantum mechanics,[1,2] which have been applied in various quantum information processing tasks.[3–5]

In the last decades, the generation of quantum random numbers has been extensively studied. Various high-speed and real-time QRNGs have been developed[6–9] and started to become commercial.[10,11] However, these QRNGs can only extract true randomness based on the strong assumption that the source and measurement devices are trusted. The device-independent QRNG (DI QRNG)[4,12,13] is able to access true randomness without any assumptions on the source and measurement devices, but it requires a loophole-free Bell test, resulting in great challenges in implementation and low efficiency. An alternative technique is semi-DI QRNG, where high speed and low-cost information-provable randomness can be generated based on a few justifiable assumptions on the system operation and its critical components, such as trusted sources,[14–17] the characterized measurement settings,[18–24] assumptions on the indistinguishability, or dimension of the input states.[25–28]

*Address all correspondence to Xinhui Li, lixinhui@nju.edu.cn; Yan-Xiao Gong, gongyanxiao@nju.edu.cn

For practical semi-DI QRNGs, security, generation rate, and practicality are highly desirable in applications. Particularly, any deviation of the realistic source from its theoretical modeling may affect the security and generation rate of true randomness. Source-DI QRNGs generating true randomness from an untrusted source provided convenient and characterized measurement devices, offer distinct advantages in semi-DI QRNGs, and have been extensively studied.

One kind of approach is based on measurement of the vacuum noise via homodyne detection.[23,29–31] Benefiting from the fast detection speed, such a technique has achieved a random number generation rate as high as gigabits per second (Gbps); however, the homodyne detection requires a well modeled and calibrated local oscillator. In contrast, the single-photon detection technique, despite the drawback on detection speed, has the merit of easy operation and simple structure. With such a technique, source-DI QRNGs have also been reported[18,20] based on an assumption of the squashing model[32] in the detection devices. In this paper, we propose and experimentally demonstrate a secure and fast source-DI QRNG based on single-photon detection and entangled photons. The random bits are generated via the measurement of photon arrival time that is beneficial for producing high-dimensional QRNGs.[33,34] In our scheme, we use either photon of time–energy entangled photon pairs produced from spontaneous parametric downconversion (SPDC) as the entropy source. The security of our scheme relies on the observation of nonlocal dispersion cancellation (NDC),[35] which has been applied to guarantee the security of quantum key distribution tasks.[36–38] Moreover, we employ a modified entropic uncertainty relation (EUR)[39] to quantify the randomness to improve security. The experiment results show that the genuine quantum randomness can be extracted at a rate of 4 Mbps (megabits per second), which could reach the level of Gbps if using the advanced single-photon detectors with faster detection speed and lower temporal resolution.

2 Source-DI QRNG Protocol

In our protocol, we suppose an untrusted source produces a tripartite state ρ_{ABE} with the reduced state $\rho_{AB} = \mathrm{Tr}_E[\rho_{ABE}]$, where A and B are distributed to two noncommunicating observers named Alice and Bob, respectively, and E is held by the underlying eavesdropper Eve as a quantum memory or considered as the environment. In the ideal case, ρ_{AB} is a pure time–energy entangled photon pair state generated via SPDC. Here we suppose that the SPDC source is pumped by a pulsed laser with a center frequency of ω_p and a coherence time of σ_{coh} and that the generated photon pairs have a correlation time of σ_{cor} determined by phase-matching bandwidth. The ideal state can be written in the time and frequency domains, respectively, as follows:

$$\Psi^t_{AB} = \iint \psi(t_A, t_B) e^{i\omega_p(t_A+t_B)/2} |t_A\rangle_A |t_B\rangle_B \mathrm{d}t_A\, \mathrm{d}t_B, \tag{1}$$

$$\Psi^\omega_{AB} = \iint \phi(\omega_A, \omega_B) |\omega_A\rangle_A |\omega_B\rangle_B \mathrm{d}\omega_A\, \mathrm{d}\omega_B, \tag{2}$$

where the joint time function $\psi(t_A, t_B)$ and joint frequency function $\phi(\omega_A, \omega_B)$ are given by

$$\psi(t_A, t_B) = \frac{1}{\sqrt{2\pi\sigma_{\mathrm{coh}}\sigma_{\mathrm{cor}}}} e^{-(t_A-t_B)^2/4\sigma^2_{\mathrm{cor}} - (t_A+t_B)^2/16\sigma^2_{\mathrm{coh}}}, \tag{3}$$

$$\phi(\omega_A, \omega_B) = \frac{1}{\sqrt{\pi/2\sigma_{\mathrm{coh}}\sigma_{\mathrm{cor}}}} e^{-(\omega_A-\omega_B)^2\sigma^2_{\mathrm{cor}}/4 - (\omega_A+\omega_B)^2\sigma^2_{\mathrm{coh}}}, \tag{4}$$

where $|t_A\rangle_A(|t_B\rangle_B)$ and $|\omega_A\rangle_A(|\omega_B\rangle_B)$ represent photons $A(B)$ at time $t_A(t_B)$ and frequency $\omega_A(\omega_B)$.

Alice and Bob both have two trusted positive operator-valued measures (POVMs), denoted by $T^j_\delta = \{T^j_k\}$ and $D^j_\delta = \{D^j_k\}$ with $j \in \{A, B\}$ and $k \in \mathbb{N}$. The measurement T^j_δ is the direct photon arrival time detection, expressed as

$$T^j_k = \int_{k\delta}^{(k+1)\delta} |X_t\rangle^j \langle X_t|^j \mathrm{d}t, \tag{5}$$

where $|X_t\rangle^j = \int_{-\infty}^{\infty} \frac{\mathrm{d}\omega}{\sqrt{2\pi}} e^{i\omega t} |\omega\rangle^j$ and δ is the detection precision of the system. The other measurement, D^j_δ, is the arrival time detection after the photons in Alice and Bob, respectively, undergo normal and anomalous dispersion with equal magnitudes, which can be written as

$$D^j_k = \int_{k\delta}^{(k+1)\delta} |Y_t\rangle^j \langle Y_t|^j \mathrm{d}t, \tag{6}$$

where $|Y_t\rangle^j = \int_{-\infty}^{\infty} \frac{\mathrm{d}\omega}{\sqrt{2\pi}} e^{i(\omega t + \beta_j \omega^2/2)} |\omega\rangle^j$ and $\beta_{A(B)}$ is the group-velocity dispersion (GVD) coefficient in Alice (Bob) satisfying $\beta_A = -\beta_B$.

However, in practice, we perform measurements T^j_δ and D^j_δ in a range from $-N_d\delta/2$ to $N_d\delta/2$, where N_d is the frame size (dimensionality); thus the null measurements $T^\varnothing_j$ and $D^\varnothing_j$ can be defined when the photon arrives before or after the range, which limits the characterization of entanglement in high-dimensional quantum systems.[39] The null measurements can be expressed by

$$T^\varnothing_j = \int_{-\infty}^{-N_d\delta/2} |X_t\rangle^j \langle X_t|^j \mathrm{d}t + \int_{N_d\delta/2}^{\infty} |X_t\rangle^j \langle X_t|^j \mathrm{d}t, \tag{7}$$

$$D^\varnothing_j = \int_{-\infty}^{-N_d\delta/2} |Y_t\rangle^j \langle Y_t|^j \mathrm{d}t + \int_{N_d\delta/2}^{\infty} |Y_t\rangle^j \langle Y_t|^j \mathrm{d}t. \tag{8}$$

Then the refined POVMs can be written as $T^j_\delta = \{T^j_k\}^{N_d/2}_{k=-N_d/2} \bigcup T^\varnothing_j$ and $D^j_\delta = \{D^j_k\}^{N_d/2}_{k=-N_d/2} \bigcup D^\varnothing_j$.

Alice and Bob choose two measurements, T_δ and D_δ, separately, which are switched through a classical random signal S with probabilities q and $1-q$, respectively. Before extracting random numbers, Alice and Bob record the joint outcomes of the measurements T_δ to estimate the detection precision δ of the system. Then the outcomes of measurement T_δ in Alice are recorded as the raw random bits, whereas the joint outcomes of the measurements D_δ for Alice and Bob are utilized to certify the entanglement of source and estimate the amount of randomness.

In the process of certification for the source, the NDC[35] is available as a nonlocal test of the time–energy entanglement, where the dispersion effect can be nonlocally canceled when two time–energy entangled photons propagate in two media with equal magnitudes and opposite dispersion signs, respectively. We define the code distance associated with the outcomes of measurement D_δ as a testing value d given by[38]

$$d = \sqrt{\frac{2}{\pi}}\frac{\sigma_{\mathrm{coh},D}}{\delta}, \tag{9}$$

where $\sigma_{\mathrm{coh},D}$ is the correlation time of the photon pairs when Alice and Bob both perform measurement D_δ, and $\sigma_{\mathrm{coh},D} = \sqrt{\sigma_{\mathrm{cor}}^2 + \beta^2/4\sigma_{\mathrm{coh}}^2}$ for the ideal state. The source can be certified to be time–energy entangled if d is less than the classical bound determined by the actual experimental parameters (see Appendix A for details). A preset value d_0 is selected here that is not larger than the classical bound, and the protocol is aborted when $d > d_0$.

Since the source device is untrusted, the input state might be controlled by an eavesdropper, Eve, who can obtain the side information through system E. The amount of genuine randomness that can be extracted from Alice in measurement T_δ is quantified by the conditional quantum min-entropy[40] defined as $H_{\min}(T_\delta^A|E) = -\log_2 P_{\mathrm{guess}}(T_\delta^A|E)$, where $P_{\mathrm{guess}}(T_\delta^A|E)$ is the maximum probability that Eve guesses correctly the outcome of T_δ conditional on her side information. In previous works, the lower bound of conditional quantum min-entropy $H_{\min}(T_\delta^A|E)$ can be given by exploiting the EUR.[41,42]

In practical implementations, the finite measurement range problem will significantly compromise the evaluation of secure min-entropy. To further improve security, we explore the extractable randomness lower bound with the modified EUR[39] based on smooth entropy by taking into account the finite measurement range. The ϵ-smooth conditional min- and max-entropies are defined as

$$H_{\min}^{\epsilon}(A|B)_\rho = \max_{\rho' \in \mathcal{B}^\epsilon(\rho)} H_{\min}(A|B)_{\rho'}, \tag{10}$$

$$H_{\max}^{\epsilon}(A|B)_\rho = \max_{\rho' \in \mathcal{B}^\epsilon(\rho)} H_{\max}(A|B)_{\rho'}, \tag{11}$$

where $\mathcal{B}^\epsilon(\rho) = \{\rho' | \frac{1}{2}\|\rho - \rho'\|_{\mathrm{tr}} \le \epsilon\}$ is the set of operators within an ϵ distance of ρ. Then the modified EUR is written as[39]

$$\begin{aligned} H_{\min}^{\epsilon}(T_\delta^A|E)_\rho &\ge H_{\mathrm{low}}^{\epsilon}(T_\delta^A|E)_\rho \\ &= -2\log_2\Bigg(\sqrt{f_+(p_{T_\delta^A}^{\varnothing}(\rho),\epsilon)} + \sqrt{f_+(p_{D_\delta^A}^{\varnothing}(\rho),\epsilon)} \\ &\quad + \sqrt{1 - f_-(p_{D_\delta^A}^{\varnothing}(\rho),\epsilon)}\sqrt{c^<(T_\delta^A, D_\delta^A)}\left(\sqrt{2^{H_{\max}^{\epsilon}(D_\delta^{A<}|B)_\rho}}\right)\Bigg), \end{aligned} \tag{12}$$

where

$$\begin{aligned} f_\pm(p_i^{\varnothing}(\rho),\epsilon) &= 2\epsilon - \epsilon^2 + 2p_i^{\varnothing}(\rho)\epsilon^2 - 4p_i^{\varnothing}(\rho)\epsilon \\ &\quad \pm 2(1-\epsilon)\sqrt{p_i^{\varnothing}(\rho)\epsilon[1 - p_i^{\varnothing}(\rho)](2-\epsilon)} \\ &\quad + p_i^{\varnothing}(\rho), \end{aligned} \tag{13}$$

and $p_{T_\delta^A}^{\varnothing}(\rho) = \mathrm{Tr}[\rho_A T_A^{\varnothing}]$, $p_{D_\delta^A}^{\varnothing}(\rho) = \mathrm{Tr}[\rho_A D_A^{\varnothing}]$ are the null probabilities for measurement $T_A^{\varnothing}$ and $D_A^{\varnothing}$, respectively, which can be written as

$$p_{T_\delta^A}^{\varnothing}(\rho) = 1 - \frac{1}{\sqrt{2\pi}\sigma_{\mathrm{coh}}}\int_{-N_d\delta/2}^{N_d\delta/2} e^{-\frac{t_A^2}{2\sigma_{\mathrm{coh}}^2}} \mathrm{d}t_A, \tag{14}$$

$$p_{D_\delta^A}^{\varnothing}(\rho) = 1 - \frac{1}{\sqrt{2\pi}\sigma_{\mathrm{coh}'}}\int_{-N_d\delta/2}^{N_d\delta/2} e^{-\frac{t_A^2}{2\sigma_{\mathrm{coh}'}^2}} \mathrm{d}t_A, \tag{15}$$

where $\sigma_{\mathrm{coh}'}$ is the standard deviation of arrival-time distribution photon A after propagating through the dispersive medium.

Additionally, $c^<(T_\delta^A, D_\delta^A)$ in Eq. (12) is the maximum overlap for the POVMs T_δ^A and D_δ^A, excluding the null measurement POVM elements, satisfying[39]

$$c^<(T_\delta^A, D_\delta^A) = \max_{T_\delta^A, D_\delta^A \neq \varnothing}\left\|\sqrt{T_\delta^A}\sqrt{D_\delta^A}\right\|_\infty^2, \tag{16}$$

where $\|\cdot\|_\infty$ denotes the maximum singular value. $c^<(T_\delta^A, D_\delta^A)$ can be the upper bound by the $c(T_\delta^A, D_\delta^A) = \max_{T_\delta^A, D_\delta^A}\|\sqrt{T_\delta^A}\sqrt{D_\delta^A}\|^2$ because the sets of POVMs over which the former is maximized are subsets of the sets over which the latter is maximized. Thus we obtain

$$c^<(T_\delta^A, D_\delta^A) \le c(T_\delta^A, D_\delta^A) = \frac{\delta^2}{4\pi^2\beta}, \tag{17}$$

where $\beta = |\beta_A|$ (see Appendix B for details). The smooth conditional max-entropy $H_{\max}^{\epsilon}(D_\delta^{A<}|B)_\rho$ in Eq. (12) represents Bob's lack of knowledge about the measurement results of D_δ^A after Alice discards the null measurements, which can be bounded by[43]

$$H_{\max}^{\epsilon}(D_\delta^{A<}|B)_\rho \le \log_2\gamma(d_0 + \Delta), \tag{18}$$

where function $\gamma(\cdot)$ is formulated as

$$\gamma(x) = \left(x + \sqrt{1+x^2}\right)\left(\frac{x}{\sqrt{1+x^2} - 1}\right)^x, \tag{19}$$

and the statistical fluctuations Δ can be written as

$$\Delta = N_d\sqrt{\frac{1}{q(q-1)N_T^A}\ln\left(\epsilon/4 - 2\sqrt{2\left(1 - (1 - p_{T_\delta^A}^{\varnothing}(\rho))^{N_T^A}\right)}\right)}, \tag{20}$$

where N_T^A is the total number of detections for T_δ^A in a processing unit.

Finally, we extract the secure random bits from the raw random bits by the Toeplitz-hashing extractor and claim that our QRNG scheme successfully generates a string of genuine random bits if all statistical tests are passed.

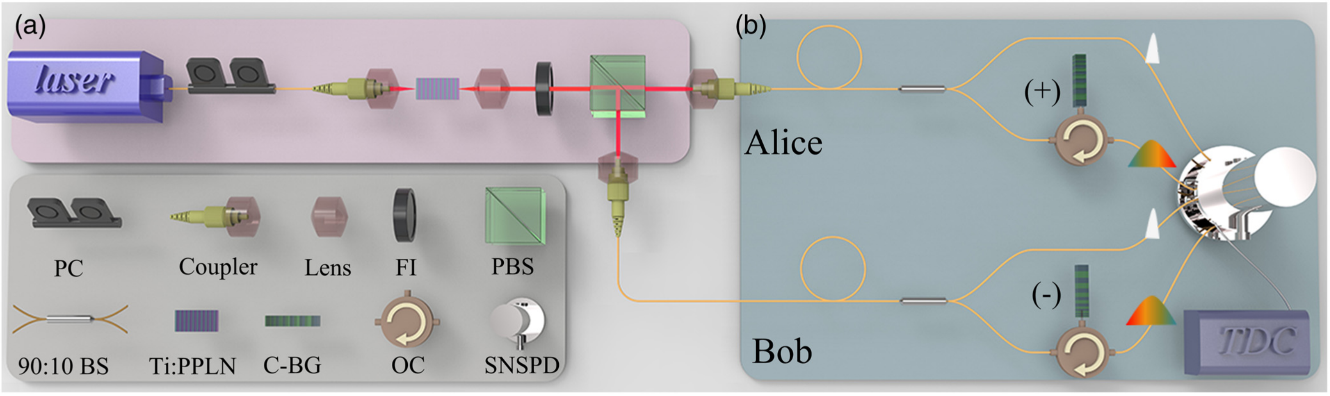

Fig. 1 Experimental setup of the source-DI QRNG. (a) Entanglement source: the time–energy entangled photon pairs are generated from the Ti:PPLN waveguide pumped by a pulsed laser with a duration of 5 ns, which are separated by a PBS. (b) Measurement device: photons are passively selected for measurement T_δ or D_δ by a 90:10 beam splitter (BS) after being coupled to fiber in Alice and Bob sides. PC, polarization controller; FI, filter; C-BG, chirped Bragg grating; OC, optical circulator; SNSPD, superconducting nanowire single-photon detector; and TDC, time-to-digital converter.

3 Experimental Demonstration

The experimental setup comprises an entanglement source and measurement devices, as shown in Fig. 1. The pump light is a pulsed laser with a repetition rate of 10 MHz and a measured coherence time of 2.1 ns, which is extracted from a continuous-wave laser at 774.9 nm through a lithium niobate electro-optic modulator. It is adjusted to horizontal polarization by a polarization controller, then coupled into a 5-cm Ti-diffused periodically poled lithium niobate (Ti:PPLN) waveguide with a poling period of 9.2 μm. The time–energy entangled photon pairs are produced via the type-II SPDC process. After blocking out the pump by a long-pass filter and a 3-nm bandpass filter centered at 1550 nm, the output orthogonally polarized entangled photon pairs are spatially separated by a polarization beam splitter (PBS) and distributed to Alice and Bob, respectively. The wavelength-degenerate photon pairs are centered at 1549.8 nm with 0.7 nm full width at half-maximum (FWHM). The overall detection efficiencies are 20.5% for the photon to Alice and 20% for the photon to Bob, respectively. When the pump power coupled into the waveguide is 1 mW, the single-photon counting rates measured by superconducting nanowire single-photon detectors (SNSPDs) at Alice and Bob are 5 and 4.85 MHz, respectively, with the dark counting rate observed around 500 Hz and thus are ignored. The two-photon coincidence counting rate obtained by the time-to-digital converter (TDC) (PicoHarp-300) is 1 MHz. Thus the proportion of genuine entangled photons in Alice's detection can be estimated to be 97%.

Alice and Bob both randomly perform measurement T_δ or D_δ by a passive 90:10 beam splitter, i.e., $q = 0.9$ in protocol. Explicitly, the measurement T_δ is implemented by directly measuring the arrival time at the SNSPD, while for the measurement D_δ, arrival time detection is performed after the photons to Alice (Bob) propagate through a dispersion module composed of an optical circulator and a chirped (antichirped) Bragg grating with a GVD coefficient of $-1440\ \mathrm{ps}^2$ ($1440\ \mathrm{ps}^2$). The arrival time is detected by the SNSPDs, then recorded by the TDCs with the total time jitters estimated approximately as $\sigma_j \sim 34$ ps (1 standard deviation). The outcome rate of measurement T_δ in Alice is $n_T^A = 4.5$ MHz.

To explore the performance of the source and certify the security of the scheme, we plot the coincidence curves of four combinations for two observers' measurements, as illustrated in Fig. 2. If Alice and Bob both make measurement T_δ, the FWHM of the coincidence peak is $\Delta_T = 120$ ps, as shown in Fig. 2(a), and thus the detection precision is calculated to be $\delta = \Delta_T/\sqrt{2} = 84$ ps based on the assumption that the resolution of all detectors is identical. If the measurements performed by Alice and Bob are different, coincidence peaks are broadened to 750 ps in Fig. 2(b) and 760 ps in Fig. 2(c) due to the dispersion effect. The slight difference between two peaks is caused by the slight difference in magnitude of GVD coefficients in Alice and Bob. If two observers both choose measurement D_δ, as shown in Fig. 2(d), the peak recovers with a narrow FWHM of $\Delta_D = 160$ ps, as shown in Fig. 2(d), corresponding to $\sigma_D = 68$ ps [$\sigma_D = \Delta_D/(2\sqrt{2\ \ln\ 2})$ for Gaussian function] due to the NDC effect. In this case, the testing value d is calculated to be 0.64 according to Eq. (9), which is much smaller than the classical bound $\overline{d}_c = 1.35$ (see Appendix C).

The preset value d_0 is set to be 0.64, since it is the upper bound in the vast majority of the measurement runs in our experiment. If $d \leq d_0$ from the experimentally observed results, the protocol is passed, implying that we can evaluate and extract true randomness from the raw random bits to generate genuine random numbers.

4 Randomness Evaluation and Extraction

From the above results, we could calculate the randomness from the raw random bits according to Eqs. (12)–(20). The null probabilities $p^{\varnothing}_{T^A_\delta}(\rho) = 1 - f_{\mathrm{err}}(0.0140 N_d)$ and $p^{\varnothing}_{D^A_\delta}(\rho) = 1 - f_{\mathrm{err}}(0.0138 N_d)$ can be obtained with $\sigma_{\mathrm{coh}} = 2.1$ and $\sigma_{\mathrm{coh}'} = 2.15$ ns in our experiment, where f_{err} is the error function.[44] The statistical fluctuation Δ defined in Eq. (20) is obtained by setting the smooth entropy parameter $\epsilon = 10^{-10}$,

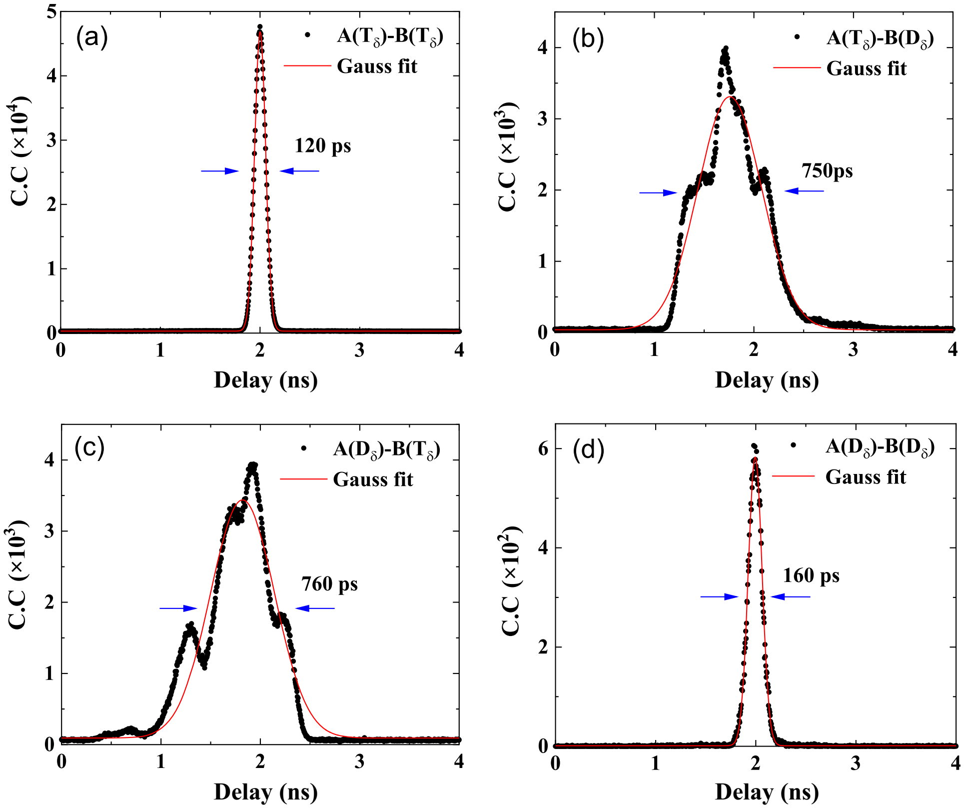

Fig. 2 Photon coincidence counts (CCs) recorded for four measurement combinations of two observers (denoted as A and B) in 10 s.

where the total count N_T^A is deduced by the count rate n_T^A and the cumulative time τ as $N_T^A = n_T^A \tau (1 - p^{\varnothing}_{T_\delta^A}(\rho))$.

We plot the smooth min-entropy $H^{\epsilon}_{\text{low}}(T_\delta^A|E)_\rho$ with respect to N_T^A and N_d, as shown in Fig. 3. It can be seen that $H^{\epsilon}_{\text{low}}(T_\delta^A|E)_\rho$ increases with N_T^A, while for a given N_T^A, with the increasing N_d, $H^{\epsilon}_{\text{low}}(T_\delta^A|E)_\rho$ first keeps growing due to increasing measurement range and then declines for larger statistical fluctuation, where the maximum value can be obtained by optimizing N_d. The maximal entropy values are obtained to be 0.778, 0.877, 0.903, and 0.913 for four processing units with frame size $N_d = 232$, 246, 250, and 256, respectively.

As a trade-off between the entropy bound and practicality, the processing unit is set as $N_T^A = 4.5 \times 10^8$, corresponding to the highest min-conditional entropy of 0.917 bit per count with $N_d = 256$, $p^{\varnothing}_{T_\delta^A}(\rho) = 4 \times 10^{-7}$, $p^{\varnothing}_{D_\delta^A}(\rho) = 6 \times 10^{-7}$, and

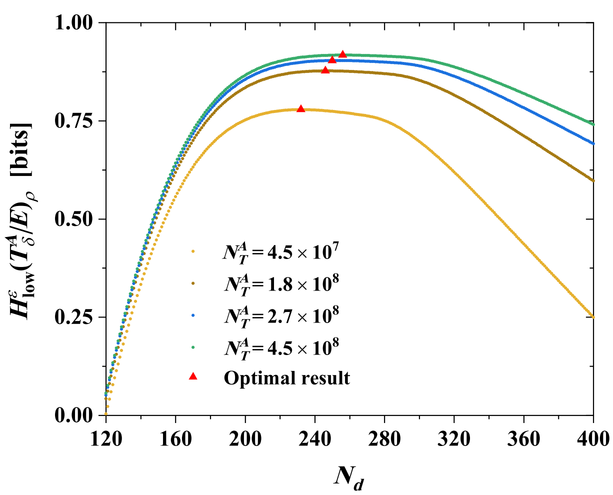

Fig. 3 Smooth entropy $H^{\epsilon}_{\text{low}}(T_\delta^A|E)_\rho$ with respect to the frame size N_d for different processing units N_T^A. The dotted lines represent the entropy evaluated from the experimental data. The red triangles represent optimal results.

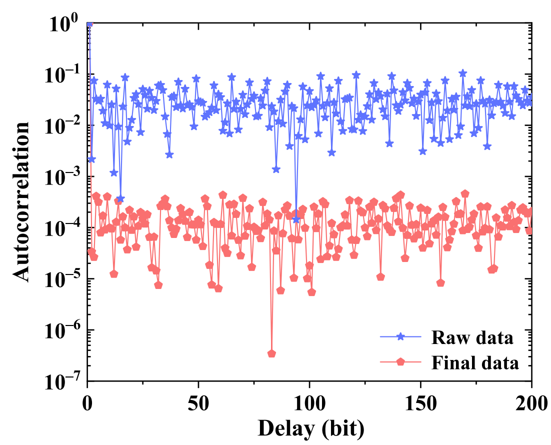

Fig. 4 Autocorrelation coefficients of raw random data and final random data.

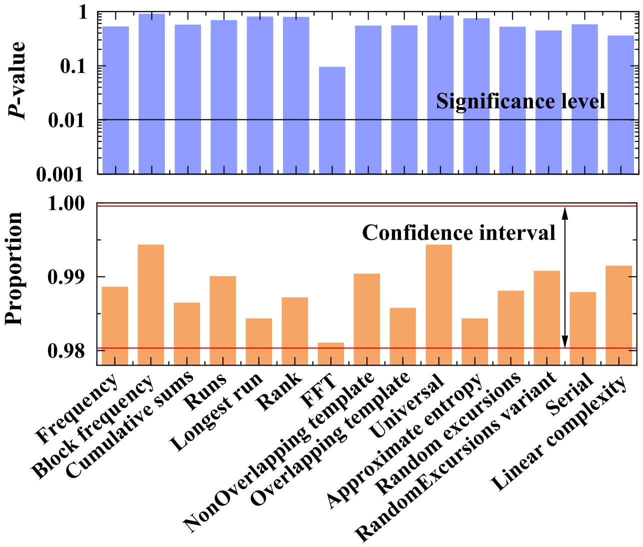

Fig. 5 Results of NIST statistical test suite.

$\tau = 100$ s. Considering the proportion of genuine entangled photons of the SPDC is measured to be 97%, we can extract 0.900-bit genuine randomness per $\log_2(256)$-bit sample. Hence, we generate a Toeplitz matrix with a scale of $80{,}000 \times 9000$ to extract genuine random numbers. As the outcomes rate is $n_T^A = 4.5$ Mcounts/s, the final generation rate of random numbers is 4 Mbps.

To test the quality of random numbers, we perform an autocorrelation coefficient test between the raw and final random data, where the raw data and final random data satisfy the Gaussian distribution and uniform distribution, respectively. As shown in Fig. 4, the final autocorrelation coefficients are below 0.001 within the 200-bit delay, which are significantly lower than the raw data. Furthermore, we perform a standard NIST test suite using 1000 samples of 1 Mb; the significant level is set as $\alpha = 0.01$. The NIST test is passed if P values are higher than 0.01 and the proportion value within the confidence interval of $(1-\alpha) \pm 3\sqrt{(1-\alpha)\alpha/n} = 0.99 \pm 0.00944$ for all tests. As shown in Fig. 5, the random bits in our scheme pass all 15 tests.

5 Conclusions and Discussions

In conclusion, we have proposed and experimentally demonstrated a scheme for a source-DI QRNG, where the random bits are generated by measuring the arrival time of single photons from an untrusted time–energy entangled photon pair source. The NDC effect is employed to testify the entanglement source and thus guarantee the security of true random number acquisition. With a high-quality PPLN waveguide SPDC source, we realized a fast generation of true random numbers with a generation rate of 4 Mbps, which were extracted by utilizing the modified EUR. In Table 1, we list several semi-DI QRNGs as a comparison. It shows that our work achieves a trade-off among security, speed, and practicality.

The generation rate of our protocol can be further increased to Gbps provided we use state-of-the-art single-photon detectors. For instance, the single-photon detector[45] with a temporal resolution of 29 ps could theoretically achieve optimal $H_{\mathrm{low}}^{\epsilon}(T_\delta^A|E)_\rho = 2.66$; combining with its maximum count rate of 2 GHz, the random number generation rate can reach 5.16 Gbps. Moreover, the source-DI QRNG we realized is based on the PPLN waveguide SPDC source, which may be further developed to be an integrated chip-scale device by exploring on-chip photon generation, manipulation, and detection techniques. We hope our approach can stimulate more such investigations.

Furthermore, our scheme provides a secure certification for quantum information and quantum communication tasks with an untrusted source based on dispersion cancellation. Recently, the work on the QKD protocol where the source is trusted but imperfect was proposed.[36] Our approach offers a way to certify the untrusted source via dispersion cancellation for this protocol, which enables us to access the source-DI QKD tasks.

Table 1 Features of our protocol as compared to the features of existing semi-DI QRNG protocols.

Refs.	Uncharacterized Source	Uncharacterized Measurement	Finite-size Analysis	Finite Measurement Ranges Considered[a]	Generation Rate
15	×	√	×	—	5.7 kbps
17	×	√	√	×	47.8 Mbps
20	√	×	√	—	1 Mbps
21	√	×	√	×	8.05 Gbps
24	√	×[b]	√	—	1 Mbps
25	√[c]	√	√	—	23 bps
27	√[d]	√	√	—	1.25 Mbps
31	√	×	√	×	17 Gbps
This work	√	×	√	√	4 Mbps

[a]The measurements are discrete systems.
[b]Without a detailed characterization.
[c]With additional assumption on the dimension of input states.
[d]With additional assumption on the input energy.

6 Appendix A: The Definition of Testing Value

In this section, we provide the proof that the testing value d defined in Eq. (9) as the code distance for systems A and B in D_δ basis can be used to certify the time–energy entanglement for the ideal state in Eq. (1).

Let us consider the case that systems A and B are two separable photons or classical pulses. The spectrum and temporal functions of the photon A can be written as, respectively,

$$\phi_A^c(\omega) \propto e^{-\frac{\omega^2}{4\sigma_\nu^2}}, \tag{21}$$

$$\psi_A^c(t) \propto e^{-\frac{t^2}{4\sigma_t^2}}, \tag{22}$$

where σ_ν is the spectrum bandwidth (1 standard deviation) of the photon, and σ_t is the temporal bandwidth. Meanwhile, $\phi_B^c(\omega)$ and $\psi_B^c(t)$ for photon B are defined similarly with photon A. After two photons propagate through the dispersive medium, the intensity detected at Alice and Bob can be written as

$$\begin{aligned} I_A(t_A) &= \left| \int \frac{\mathrm{d}\omega_A}{\sqrt{2\pi}} \phi_A^c(\omega_A) e^{i(\omega_A t_A + \beta\omega_A^2/2)} \right|^2, \\ I_B(t_B) &= \left| \int \frac{\mathrm{d}\omega_B}{\sqrt{2\pi}} \phi_B^c(\omega_B) e^{i(\omega_B t_B + \beta\omega_B^2/2)} \right|^2. \end{aligned} \tag{23}$$

The joint detection probability that Alice's detector clicks at time t_A and Bob's clicks at time t_B simultaneously is $P(t_A, t_B) = I_A(t_A) I_B(t_B)$, and the overall probability $P(\Gamma)$ of detecting two photons at a time lag $\Gamma = t_A - t_B$ can be calculated as

$$P(\Gamma) = \int I_A(t_A) I_B(t_B) \mathrm{d}t_A \propto e^{-\frac{\Gamma^2}{2\sigma_{\mathrm{cor,c}}^2}}, \tag{24}$$

where the correlation time thus given by

$$\sigma_{\mathrm{cor,c}}^2 = \sigma_{\mathrm{cor}}^2 + 2\beta^2\sigma_\nu^2, \tag{25}$$

and $\sigma_{\mathrm{cor}} = \sqrt{2}\sigma_t$ is the origin correlation time.

It has been proved that the origin correlation time σ_{cor} and standard deviation in the spectrum intensity of the sum of frequency $\Delta(\omega_A + \omega_B)$ for two separable photons satisfy the following inequality:[46,47]

$$\sigma_{\mathrm{cor}} \Delta(\omega_A + \omega_B) \geq 1, \tag{26}$$

where $\Delta(\omega_A + \omega_B)$ can be calculated to be $\sqrt{2}\sigma_\nu$. Hence, substituting this inequality into Eq. (25), we can obtain

$$\sigma_{\mathrm{cor,c}}^2 \geq \sigma_{\mathrm{cor}}^2 + \frac{\beta^2}{\sigma_{\mathrm{cor}}^2}, \tag{27}$$

which defines the minimum broadening of temporal correlations between two separable photons after they propagate through two dispersive media with equal and opposite dispersion. By normalizing the correlation time $\sigma_{\mathrm{cor},c}$ into the detection precision δ, the testing value d for a pair of separable photons can be written as

$$d \geq \sqrt{\frac{2\sigma_{\mathrm{cor}}^2}{\pi\delta^2} + \frac{2\beta^2}{\pi\delta^2\sigma_{\mathrm{cor}}^2}}. \tag{28}$$

A violation of this inequality implies the presence of entanglement, which is able to be used as a witness for the certification of time–energy entanglement. We denote the right-hand side of Eq. (28) as the classical bound d_c.

Let us now consider the case that the source device distributes the entangled photon pairs with the state given by Eq. (1) to Alice and Bob, and they both choose measurement D_δ, i.e., the arrival time after two photons traveled through the dispersive elements. The joint detection rate between two detectors is proportional to the Glauber second-order correlation function,

$$G^{(2)}(t_A; t_B) = |\langle Y_t^A(t_A) Y_t^B(t_B) | \Psi_{AB}^\omega \rangle|^2 = |\psi_D(t_A, t_B)|^2, \tag{29}$$

where the joint time function becomes

$$\psi_D(t_A, t_B) = \frac{1}{2\pi} \iint \phi_{AB}(\omega_A, \omega_B) e^{i\frac{\beta}{2}(\omega_A^2 - \omega_B^2) - i(\omega_A t_A + \omega_B t_B)} \mathrm{d}\omega_A \, \mathrm{d}\omega_B. \tag{30}$$

Then the correlation time of outcomes in measurement D_δ can be calculated as

$$\begin{aligned} \sigma_{\mathrm{cor},D}^2 &= \iint (t_A - t_B)^2 |\psi_D(t_A, t_B)|^2 \mathrm{d}t_A \, \mathrm{d}t_B \\ &= \iint (t_A - t_B)^2 |\psi_{AB}(t_A, t_B)|^2 \mathrm{d}t_A \, \mathrm{d}t_B \\ &\quad + \beta^2 \iint (\omega_A + \omega_B)^2 |\phi_{AB}(\omega_A, \omega_B)|^2 \mathrm{d}\omega_A \, \mathrm{d}\omega_B \\ &= \sigma_{\mathrm{cor}}^2 + \beta^2\sigma_\omega^2, \end{aligned} \tag{31}$$

and $\sigma_\omega = 1/(2\sigma_{\mathrm{coh}})$ is the pump spectrum bandwidth. Thus the theoretical d for the ideal state given by Eq. (1) is achieved by

$$d = \sqrt{\frac{2\sigma_{\mathrm{cor}}^2}{\pi\delta^2} + \frac{\beta^2}{2\pi\sigma_{\mathrm{coh}}^2\delta^2}}. \tag{32}$$

In the limit of large coherence time σ_{coh}, the testing value d reduces to

$$d = \sqrt{\frac{2\sigma_{\mathrm{cor}}^2}{\pi\delta^2}}, \tag{33}$$

which is obviously smaller than the classical bound d_c.

7 Appendix B: The Maximum Overlap of T_δ^A and D_δ^A

We recall the measurements $T_\delta^A = \{T_k^A\}$ and $D_\delta^A = \{D_k^A\}$, which can be expressed as

$$T_k^A = \int_{k\delta}^{(k+1)\delta} |X_t\rangle^A \langle X_t|^A \mathrm{d}t, D_k^A = \int_{k\delta}^{(k+1)\delta} |Y_t\rangle^A \langle Y_t|^A \mathrm{d}t, \tag{34}$$

where $|X_t\rangle^A = a^\dagger(t)|0\rangle$ satisfies the orthonormality condition $\langle X_{t_1}|X_{t_2}\rangle = \delta(t_1 - t_2)$. Note that the measurements D_δ^A and T_δ^A can be transformed by the dispersion operator U[36] as

$$D_\delta^A = U T_\delta^A U^\dagger, \tag{35}$$

where

$$U = \frac{1}{\sqrt{2\pi\beta}} \int_{-\infty}^{+\infty} \mathrm{d}t_1 \int_{-\infty}^{+\infty} \mathrm{d}t_2 e^{-i(t_1-t_2)^2/2\beta} |X_{t_1}\rangle^A \langle X_{t_2}|^A. \tag{36}$$

The associated observables of T_δ^A and D_δ^A can be, respectively, written as

$$\begin{aligned} O_T^A &= \int_{-\infty}^{+\infty} \mathrm{d}t t |X_t\rangle^A \langle X_t|^A, \\ O_D^A &= \frac{1}{2\pi\beta} \int_{-\infty}^{+\infty} \mathrm{d}t \int_{-\infty}^{+\infty} \mathrm{d}t_1 \int_{-\infty}^{+\infty} \\ &\quad \times \mathrm{d}t_2 t e^{-i(t_1^2 - t_2^2)/2\beta + i(t_1 - t_2)t/\beta} |X_{t_1}\rangle^A \langle X_{t_2}|^A. \end{aligned} \tag{37}$$

Based on the derivation in Ref. 38, the observable O_D^A can be further simplified as

$$\begin{aligned} O_D^A &= \int_{-\infty}^{+\infty} \mathrm{d}t t |X_t\rangle^A \langle X_t|^A + \frac{\beta}{i} \int_{-\infty}^{+\infty} \mathrm{d}t |X_t\rangle^A \frac{\partial}{\partial t} \langle X_t|^A, \\ &= O_T^A + 2\pi\beta O_\omega^A, \end{aligned} \tag{38}$$

where $O_\omega^A = \int_{-\infty}^{+\infty} \frac{\mathrm{d}\omega}{2\pi} \omega |\omega\rangle^A \langle \omega|^A$ is the observable of frequency. According to the commutation relation $[O_T^A, O_\omega^A] = i$,[48] we can derive the commutation relation of O_T^A and O_D^A as follows:

$$[O_T^A, O_D^A] = i2\pi\beta. \tag{39}$$

Using the overlap result for maximally incompatible observables,[38,49] we can obtain

$$c(T_\delta^A, D_\delta^A) = \frac{\delta^2}{4\pi^2\beta}. \tag{40}$$

8 Appendix C: The Classical Bound of Experimental Testing Value

In our source-DI QRNG framework, the security of the scheme relies on the observation of d in experiment. To certify the entanglement, we need to calculate the classical bound of testing value in our experiment.

Taking into account the time jitter of our detection systems in practice, the correlation time in Eq. (27) can be rewritten in a modified form,

$$\overline{\sigma}_{\mathrm{cor,c}}^2 \geq 2\sigma_j^2 + \sigma_{\mathrm{cor}}^2 + \frac{\beta^2}{\sigma_{\mathrm{cor}}^2}. \tag{41}$$

Recall that we measured the coincidence distribution and obtained $\sigma_0 = \Delta_T/(2\sqrt{2\ln 2})$ with $\beta = 0$ in Fig. 2(a), i.e., $\sigma_0^2 = 2\sigma_j^2 + \sigma_{\mathrm{cor}}^2$. Then combining the GVD coefficient β in our system, we can calculate the modified correlation time $\overline{\sigma}_{\mathrm{cor,c}} \geq 100$ ps and the corresponding classical bound $\overline{d}_c = 1.35$.

Acknowledgments

We acknowledge insightful discussions with F.-H Xu. This work was supported by the National Key Research and Development Program of China (Grant No. 2019YFA0705000), the Innovation Program for Quantum Science and Technology (Grant No. 2021ZD0301500), the Leading-edge Technology Program of Jiangsu Natural Science Foundation (Grant No. BK20192001), and the National Natural Science Foundation of China (Grant Nos. 51890861 and 11974178). The authors declare no conflicts of interest.

Data Availability

Data underlying the results presented in this paper are not publicly available at this time but may be obtained from the authors upon reasonable request.

References

1. X. Ma et al., "Quantum random number generation," *NPJ Quantum Inf.* **2**(1), 16021 (2016).
2. M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," *Rev. Mod. Phys.* **89**(1), 015004 (2017).
3. B. G. Christensen et al., "Detection-loophole-free test of quantum nonlocality, and applications," *Phys. Rev. Lett.* **111**(13), 130406 (2013).
4. Y. Liu et al., "Device-independent quantum random-number generation," *Nature* **562**(7728), 548–551 (2018).
5. T. Paraïso et al., "A photonic integrated quantum secure communication system," *Nat. Photonics* **15**(11), 850–856 (2021).
6. F. Xu et al., "Ultrafast quantum random number generation based on quantum phase fluctuations," *Opt. Express* **20**(11), 12366–12377 (2012).
7. B. Bai et al., "18.8 Gbps real-time quantum random number generator with a photonic integrated chip," *Appl. Phys. Lett.* **118**(26), 264001 (2021).
8. Y. Guo et al., "40 Gb/s quantum random number generation based on optically sampled amplified spontaneous emission," *APL Photonics* **6**(6), 066105 (2021).
9. T. Gehring et al., "Homodyne-based quantum random number generator at 2.9 Gbps secure against quantum side-information," *Nat. Commun.* **12**(1), 605 (2021).
10. PicoQuant, "Quantum random number generator-picoquant," https://www.idquantique.com/random-number-generation/products/quantis-random-number-generator/ (2023).
11. CTek, "Quantum random number source QuantumCTek-quantum secures every bit," http://www.quantum-info.com/product/coredevice/112.html (2023).
12. S. Pironio et al., "Random numbers certified by Bell's theorem," *Nature* **464**(7291), 1021–1024 (2010).
13. W. Z. Liu et al., "Device-independent randomness expansion against quantum side information," *Nat. Phys.* **17**(4), 448–451 (2021).
14. Z. Cao, H. Zhou, and X. Ma, "Loss-tolerant measurement-device-independent quantum random number generation," *New J. Phys.* **17**(12), 125011 (2015).
15. Y.-Q. Nie et al., "Experimental measurement-device-independent quantum random-number generation," *Phys. Rev. A* **94**(6), 060301 (2016).
16. P. Mironowicz et al., "Quantum randomness protected against detection loophole attacks," *Quantum Inf. Process.* **20**(1), 39 (2021).

17. C. Wang et al., "Provably-secure quantum randomness expansion with uncharacterised homodyne detection," *Nat. Commun.* **14**(1), 316 (2023).
18. Z. Cao et al., "Source-independent quantum random number generation," *Phys. Rev. X* **6**, 011020 (2016).
19. D. G. Marangon, G. Vallone, and P. Villoresi, "Source-device-independent ultrafast quantum random number generation," *Phys. Rev. Lett.* **118**(6), 060503 (2017).
20. Y.-H. Li et al., "Quantum random number generation with uncharacterized laser and sunlight," *NPJ Quantum Inf.* **5**(1), 97 (2019).
21. D. Drahi et al., "Certified quantum random numbers from untrusted light," *Phys. Rev. X* **10**, 041048 (2020).
22. X. Lin et al., "Security analysis and improvement of source independent quantum random number generators with imperfect devices," *NPJ Quantum Inf.* **6**(1), 100 (2020).
23. J. Cheng et al., "Mutually testing source-device-independent quantum random number generator," *Photonics Res.* **10**(3), 646–652 (2022).
24. X. Lin et al., "Certified randomness from untrusted sources and uncharacterized measurements," *Phys. Rev. Lett.* **129**(5), 050506 (2022).
25. T. Lunghi et al., "Self-testing quantum random number generator," *Phys. Rev. Lett.* **114**(15), 150501 (2015).
26. T. Van Himbeeck et al., "Semi-device-independent framework based on natural physical assumptions," *Quantum* **1**, 33 (2017).
27. D. Rusca et al., "Self-testing quantum random-number generator based on an energy bound," *Phys. Rev. A* **100**(6), 062338 (2019).
28. H. Tebyanian et al., "Semi-device independent randomness generation based on quantum state's indistinguishability," *Quantum Sci. Technol.* **6**(4), 045026 (2021).
29. P. R. Smith et al., "Simple source device-independent continuous-variable quantum random number generator," *Phys. Rev. A* **99**(6), 062326 (2019).
30. T. Michel et al., "Real-time source-independent quantum random-number generator with squeezed states," *Phys. Rev. Appl.* **12**(3), 034017 (2019).
31. M. Avesani et al., "Source-device-independent heterodyne-based quantum random number generator at 17 Gbps," *Nat. Commun.* **9**(1), 5365 (2018).
32. N. J. Beaudry, T. Moroder, and N. Lütkenhaus, "Squashing models for optical measurements in quantum communication," *Phys. Rev. Lett.* **101**(9), 093601 (2008).
33. Y.-Q. Nie et al., "Practical and fast quantum random number generation based on photon arrival time relative to external reference," *Appl. Phys. Lett.* **104**(5), 051110 (2014).
34. F. Xu, J. H. Shapiro, and F. N. C. Wong, "Experimental fast quantum random number generation using high-dimensional entanglement with entropy monitoring," *Optica* **3**(11), 1266–1269 (2016).
35. J. D. Franson, "Nonlocal cancellation of dispersion," *Phys. Rev. A* **45**(5), 3126–3132 (1992).
36. J. Mower et al., "High-dimensional quantum key distribution using dispersive optics," *Phys. Rev. A* **87**(6), 062322 (2013).
37. C. Lee et al., "Entanglement-based quantum communication secured by nonlocal dispersion cancellation," *Phys. Rev. A* **90**(6), 062331 (2014).
38. M. Y. Niu et al., "Finite-key analysis for time-energy high-dimensional quantum key distribution," *Phys. Rev. A* **94**(5), 052323 (2016).
39. J. E. Bourassa and H.-K. Lo, "Entropic uncertainty relations and the measurement range problem, with consequences for high-dimensional quantum key distribution," *J. Opt. Soc. Am. B* **36**(3), 65–76 (2019).
40. R. Konig, R. Renner, and C. Schaffner, "The operational meaning of min- and max-entropy," *IEEE Trans. Inf. Theory* **55**(9), 4337–4347 (2009).
41. G. Vallone et al., "Quantum randomness certified by the uncertainty principle," *Phys. Rev. A* **90**(5), 052327 (2014).
42. P. J. Coles et al., "Entropic uncertainty relations and their applications," *Rev. Mod. Phys.* **89**(1), 015002 (2017).
43. F. Furrer et al., "Continuous variable quantum key distribution: finite-key analysis of composable security against coherent attacks," *Phys. Rev. Lett.* **109**(10), 100502 (2012).
44. Wolfram Research, "Erf," https://reference.wolfram.com/language/ref/Erf.html (2022).
45. J. Münzberg et al., "Superconducting nanowire single-photon detector implemented in a 2D photonic crystal cavity," *Optica* **5**(5), 658–665 (2018).
46. S. Mancini et al., "Entangling macroscopic oscillators exploiting radiation pressure," *Phys. Rev. Lett.* **88**(12), 120401 (2002).
47. L. K. Shalm et al., "Three-photon energy–time entanglement," *Nat. Phys.* **9**(1), 19–22 (2013).
48. Z. Zhang et al., "Unconditional security of time-energy entanglement quantum key distribution using dual-basis interferometry," *Phys. Rev. Lett.* **112**(12), 120506 (2014).
49. T. Gehring et al., "Implementation of continuous-variable quantum key distribution with composable and one-sided-device-independent security against coherent attacks," *Nat. Commun.* **6**(1), 8795 (2015).

Ji-Ning Zhang is now a PhD student at the School of Physics of Nanjing University. Her current research interests include quantum optics and quantum information.

Ran Yang is now a PhD student at the School of Physics of Nanjing University. His current research interests include quantum optics and quantum tomography.

Xinhui Li obtained her PhD in cryptography from Beijing University of Posts and Telecommunications in 2020. She was awarded a scholarship from the State Scholarship Fund which was selected through a rigid academic evaluation process organized by the China Scholarship Council to pursue her studies at the National University of Singapore from August 2017 to August 2018. She is now a postdoctoral fellow at the School of Physics of Nanjing University. She is currently working on the security of quantum information processing and the foundations of quantum correlations.

Chang-Wei Sun obtained his PhD from the School of Physics at Nanjing University in 2021. He works on nonlinear optics and quantum optics.

Yi-Chen Liu received his PhD from the School of Physics at Nanjing University in 2021. In 2021, he joined as a senior researcher at Qingdao University of Technology. His current research interests include nonlinear optics and quantum optics.

Ying Wei is now a PhD student at the School of Physics of Nanjing University. His current research interests include quantum simulation and quantum tomography.

Jia-Chen Duan is now a PhD student at the School of Physics of Nanjing University. His current research interests include nonlinear optics and integrated optical quantum technologies.

Zhenda Xie obtained his PhD from Nanjing University in 2011. From 2011 to 2016, he joined as a postdoctoral fellow at Columbia University in the City of New York and a research fellow at University of California, Los Angeles, respectively. He is now a professor at the School of Electronic Science and Engineering of Nanjing University. He is currently working on solid-state laser technology, nonlinear optics, and quantum optics.

Yan-Xiao Gong obtained his PhD in optics from the University of Science and Technology of China in 2009. In 2009, he joined as a postdoctoral fellow at Nanjing University. From 2011 to 2017, he worked in the Department of Physics of the Southeast University. He is now a professor at the School of Physics of Nanjing University. He is currently working on nonlinear optics, quantum optics and integrated optical quantum technologies, and quantum information.

Shi-Ning Zhu obtained his PhD from Nanjing University in 1996 and is the group leader of Dielectric Superlattice Laboratory at Nanjing University. His research interests include condensed matter optics, quasiphase matching physics and nonlinear optics, optoelectronic functional materials, quantum optics, and metamaterials.