




Generation of true quantum random numbers with on-demand probability distributions via single-photon quantum walks

CHAOYING MENG,^{1,2,†} MIAO CAI,^{2,3,†}  YUFANG YANG,^{1,2}
HAODONG WU,^{2,3}  ZHIXIANG LI,^{2,3} YAPING RUAN,^{2,3} 
YONG ZHANG,²  HAN ZHANG,^{1,2,7}  KEYU XIA,^{2,3,4,8}  AND
FRANCO NORI^{5,6} 

¹*School of Physics, Nanjing University, Nanjing 210023, China*

²*National Laboratory of Solid State Microstructures, Nanjing University, Nanjing 210093, China*

³*College of Engineering and Applied Sciences, and National Laboratory of Solid State Microstructures, Nanjing University, Nanjing 210023, China*

⁴*Shishan Laboratory, Suzhou Campus of Nanjing University, Suzhou 215000, China*

⁵*Quantum Computing Center, Cluster for Pioneering Research, RIKEN, Wakoshi, Saitama 351-0198, Japan*

⁶*Physics Department, The University of Michigan, Ann Arbor, Michigan 48109-1040, USA*

⁷*zhanghan@nju.edu.cn*

⁸*keyu.xia@nju.edu.cn*

[†]These two authors contributed equally

Abstract: Random numbers are at the heart of diverse fields, ranging from simulations of stochastic processes to classical and quantum cryptography. The requirement for true randomness in these applications has motivated various proposals for generating random numbers based on the inherent randomness of quantum systems. The generation of true random numbers with arbitrarily defined probability distributions is highly desirable for applications, but it is very challenging. Here we show that single-photon quantum walks can generate multi-bit random numbers with on-demand probability distributions, when the required “coin” parameters are found with the gradient descent (GD) algorithm. Our theoretical and experimental results exhibit high fidelity for various selected distributions. This GD-enhanced single-photon system provides a convenient way for building flexible and reliable quantum random number generators. Multi-bit random numbers are a necessary resource for high-dimensional quantum key distribution.

© 2024 Optica Publishing Group under the terms of the [Optica Open Access Publishing Agreement](#)

1. Introduction

Random numbers are important for science research and engineering applications, such as Monte-Carlo simulations [1,2], cryptography [3,4] and tests of fundamental physics [5,6]. For example, quantum key distribution (QKD) technology highly relies on the availability of true random numbers to protect its communication security [7–10]. Theoretically, pseudo-random number generators, due to their deterministic and predictable nature, cannot satisfy the requirement for building perfectly secure communication systems. Therefore, the inherent randomness of a quantum system makes it a promising platform for generating faithful random numbers. This is known as quantum random number generator (RNG) [11].

Practical quantum RNGs using various sources of randomness have been demonstrated. Discrete generators can use branching paths [12–14], arrival times [15–18], photon counting [19–22], and attenuated pulse [23,24]; whereas continuous approaches exploit quantum vacuum fluctuations [25–27], phase noise of lasers [28–30], amplified spontaneous emission [10,31], and Raman scattering [32]. Among these schemes, quantum RNG based on quantum walks promise a convenient and fast way to generate true random numbers [33].

The applications of a RNG strongly rely on the probability distribution used. Different distributions are indispensable in various fields. Uniformly distributed random numbers are most desirable and particularly useful in practical applications [11] because these avoid inherent bias. A Gaussian distributed RNG is of most significance in the modulation of coherent states in continuous-variable QKD systems [34–36], simulations of communication channels, and stochastic processes (e.g. noise) [37].

It is highly valuable to develop a quantum RNG with an on-demand probability distribution. Based on quantum walks, significant efforts have been made for this task [33,38]. However, it is challenging to find the proper parameter numbers for a complex system to generate true random numbers with a given distribution. In contrast, the gradient descent (GD) algorithm, as a highly adaptive optimization algorithm that has been widely utilized in many fields [39–42], can provide a more general and efficient way to accomplish this challenging task.

In this work, we propose a GD-enhanced quantum walk for realizing quantum RNG with, in principle, an on-demand probability distribution. Our GD-based scheme can be implemented by using a linear optical system without the need of time-bin encoding and dynamical modulation. We further experimentally demonstrate the generation of true random numbers with various selected probability distributions by using quantum walks of heralded single photons.

2. System and model

In quantum walks, the walker is located in the Hilbert space $\mathcal{H} \equiv \mathcal{H}_p \otimes \mathcal{H}_c$, where \mathcal{H}_p is position space and \mathcal{H}_c is the coin space. The coin space contains two basis vectors $\{|L\rangle, |R\rangle\}$, which represent the eigenstate of the coin. Therefore, the definite position and classical coins are both replaced by position states and coin operators in a quantum walk system.

In a one-dimensional (1D) discrete-time quantum walk system, the quantum walker's state can be described by a product state $|\Psi\rangle = |\psi\rangle \otimes |c\rangle$, where $|c\rangle = \alpha_L|L\rangle + \alpha_R|R\rangle$ is the coin state and $|\psi\rangle = \sum_x \alpha_x|x\rangle$ is the position state. Each walking step consists of a unitary operator $\hat{U} = \hat{S}\hat{C}$, where \hat{S} is the conditional shift operator and \hat{C} is the coin operator. The coin operator \hat{C} rotates the coin state and its most general form can be expressed as

$$\hat{C} = \sum_x |x\rangle\langle x| \otimes e^{i\beta} \begin{pmatrix} e^{i\xi} \cos(\theta) & e^{i\xi} \sin(\theta) \\ -e^{i\xi} \sin(\theta) & e^{-i\xi} \cos(\theta) \end{pmatrix}, \quad (1)$$

where $\xi, \zeta \in [0, 2\pi]$ and $\theta \in [0, \pi/2]$ are the parameters of the rotation and β fixes the global phase. The conditional shift operator \hat{S} moves the walker either to the left or right depending on the coin state and has the form

$$\hat{S} = \sum_x |x-1, L\rangle\langle x, R| + |x+1, R\rangle\langle x, L|. \quad (2)$$

It leads to the conditional shift operation $\hat{S}|x, L\rangle = |x+1, L\rangle$ and $\hat{S}|x, R\rangle = |x-1, R\rangle$. In the following, we fix the parameters $\beta = \pi/2$ and $\xi = \zeta = -\pi/2$, so that we obtain the coin determined by one parameter θ . If $\theta = \pi/4$, the coin then becomes the Hadamard coin :

$$\hat{H} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

After n walking steps, the state of a quantum walk system becomes $|\Psi_n\rangle$. The quantum walker remains in a superposition of many positions until the final measurement is performed. The measured probability for the walker being at x_k after n walking steps can be written as

$$\mathcal{P}(x_k) = |\langle R|\langle x_k|\Psi_n\rangle|^2 + |\langle L|\langle x_k|\Psi_n\rangle|^2. \quad (3)$$

The probability distribution is determined by the choice of the coin parameter set in each walking step. It is difficult to adjust the coin parameters to obtain desired probability distributions

because the number of the coin parameters grows rapidly when increasing the walking steps. In this work, we exploit the gradient descent algorithm to solve this challenging problem.

3. Algorithm

Generally, the training procedure using the GD algorithm consists of the following elements [43]: a differentiable function F , function parameters $\{\theta_i\}$ ($i = 1, 2, \dots, k$) and a loss function \mathcal{L} . The function F defines the input-output relation and is parameterized by the parameters $\{\theta_i\}$ ($i = 1, 2, \dots, k$), and the loss function \mathcal{L} is used to evaluate the difference between the function output $F(x; \{\theta_i\})$ and target T . Here, $F(x; \{\theta_i\})$ represents the function output with a input example x and parameters $\{\theta_i\}$ during each training step. The basic idea of the GD algorithm is to take repeated steps in the opposite direction of the gradient of the loss function to minimize the loss function. Considering the mean square error function as the loss function $\mathcal{L} = \frac{1}{2}(T - F(x; \{\theta_i\}))^2$ in the training, the loss function is then also parameterized by $\{\theta_i\}$ ($i = 1, 2, \dots, k$) and can be written as $\mathcal{L}(\{\theta_i\})$. Essentially, the gradient descent method minimizes the loss function $\mathcal{L}(\{\theta_i\})$ by updating $\{\theta_i\}$ according to $[\theta_i - \eta \cdot \nabla_{\theta_i} \mathcal{L}(\{\theta_i\})] \rightarrow \theta_i$ (the opposite direction of the gradient of the loss function), where $\eta \in (0, 1]$ is the learning rate.

A 1D discrete-time quantum walk process is depicted in Fig. 1(a). The blue circles denote different position states, and the red arrows indicate the directions of the walk starting from different position states in each walking step. Without loss of generality, we assume the splitting ratio can be adjusted for every coin operation at different position states in different walking steps. This assumption can be experimentally realized in a linear optical system [44].

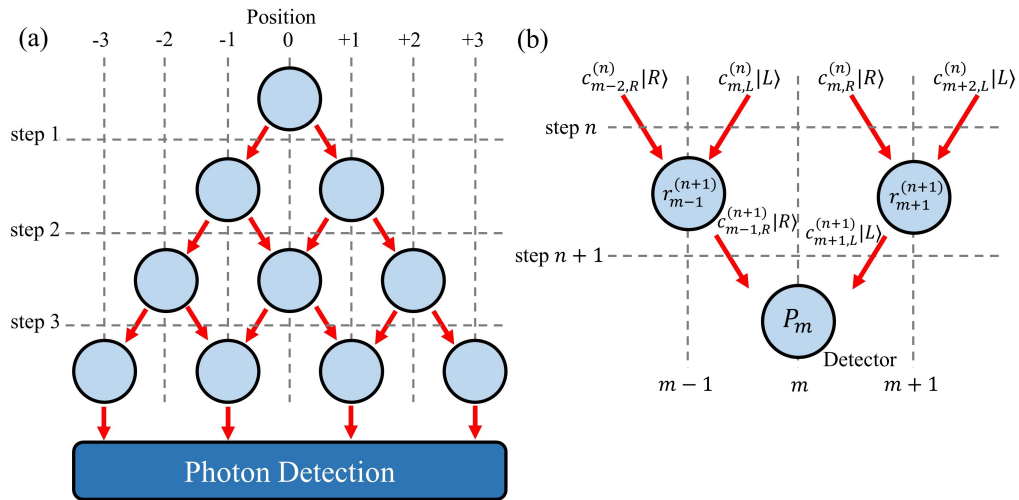


Fig. 1. (a) Schematic of a one-dimensional discrete-time quantum walk process. The red arrows represent the walking directions. The vertical and horizontal gray dashed lines denote the position states and the walking steps, respectively. (b) Details of the quantum state transfer in a quantum walk. The symbols next to the red arrows describe the coin state transfer in each walking step. The symbol $r_m^{(n)}$ represents the splitting ratio of the n -th walking step starting from position m .

The specific description of quantum state transfer in a quantum walk system is shown in Fig. 1(b). The letters c and r represent the complex amplitude and splitting ratio, respectively. The notation $c_{m,R}^{(n)}$ ($c_{m,L}^{(n)}$) represents the complex amplitude of the coin state $|R\rangle$ ($|L\rangle$) at the position m in the n -th walking step; while $r_m^{(n)}$ is the splitting ratio of the n -th walking step starting from position m , and P_m is the measured probability at the detector located at position m . The

splitting ratio r is defined as $r = \cos^2 \theta$. Thus, the state transformation with splitting ratio r can be modeled as $c|L\rangle \rightarrow \sqrt{r} \cdot c|L\rangle + \sqrt{1-r} \cdot c|R\rangle$, and $c|R\rangle \rightarrow \sqrt{1-r} \cdot c|L\rangle - \sqrt{r} \cdot c|R\rangle$. Then the measured probability P_m becomes

$$P_m = \left[\sqrt{1-r_{m-1}^{(n+1)}} a_{m-2,R}^{(n)} - \sqrt{r_{m-1}^{(n+1)}} a_{m,L}^{(n)} \right]^2 + \left[\sqrt{1-r_{m-1}^{(n+1)}} b_{m-2,R}^{(n)} - \sqrt{r_{m-1}^{(n+1)}} b_{m,L}^{(n)} \right]^2 \\ + \left[\sqrt{r_{m+1}^{(n+1)}} a_{m,R}^{(n)} + \sqrt{1-r_{m+1}^{(n+1)}} a_{m+2,L}^{(n)} \right]^2 + \left[\sqrt{r_{m+1}^{(n+1)}} b_{m,R}^{(n)} + \sqrt{1-r_{m+1}^{(n+1)}} b_{m+2,L}^{(n)} \right]^2, \quad (4)$$

where a and b are the real and imaginary components of c , respectively.

According to the GD algorithm, the updated value of $r_m^{(n)}$ with respect to P_j is

$$\Delta r_{m,P_j}^{(n)} = -\eta \frac{\partial \mathcal{L}}{\partial r_m^{(n)}} = -\eta \frac{\partial \mathcal{L}}{\partial P_j} \frac{\partial P_j}{\partial r_m^{(n)}} = \eta (T_j - P_j) \frac{\partial P_j}{\partial r_m^{(n)}}, \quad (5)$$

where here the loss function becomes $\mathcal{L} = \frac{1}{2} \sum_j (T_j - P_j)^2$, and T_j is the target probability at position j . Then the overall updated value of $r_m^{(n)}$ is obtained by summing Eq. (5),

$$\sum_j \Delta r_{m,P_j}^{(n)} = \sum_j \eta (T_j - P_j) \frac{\partial P_j}{\partial r_m^{(n)}}. \quad (6)$$

The details of the derivation are presented in the [Supplement 1](#). Therefore, during each iteration of our algorithm, $r_m^{(n)}$ updates according to the following relation

$$\left[r_m^{(n)} + \sum_j \eta (T_j - P_j) \frac{\partial P_j}{\partial r_m^{(n)}} \right] \rightarrow r_m^{(n)}. \quad (7)$$

The training finishes when the simulated quantum walk probability distribution reaches the target distribution. After the training is completed, the theoretical values of the splitting ratios for generating the desired probability distribution are obtained.

4. Experimental setup

Quantum walks lay the natural foundation for studying plenty of novel quantum phenomena and can be realized in various systems [45–50]. Among these, linear-optics-based quantum walks have advantages in convenience of implementation and compatibility. Therefore, we use this platform for our GD-based quantum RNG scheme.

In linear optical implementations of quantum walks, we use single photons as the quantum walker that moves in both directions in every position. The polarization states $\{|H\rangle, |V\rangle\}$ are introduced to represent two orthogonal coin states $\{|L\rangle, |R\rangle\}$, respectively. We use single-photon spatial modes to represent the position of the walker $|x\rangle$.

The schematic of our experimental setup is shown in Fig. 2(a). Pairs of single photons are created via type-II spontaneous parametric down-conversion in a periodically poled potassium titanyl phosphate (PPKTP) crystal with 20 mm-length. This crystal is pumped by a continuous wave diode laser centered at 397.5 nm and emits orthogonally polarized photon pairs (i.e., horizontal and vertical polarized) with a wavelength of 795 nm and a FWHM bandwidth of 0.3 nm. The photon pairs are separated by a polarized beam splitter. One photon from each pair served as a trigger while the other photon is launched into the quantum walk system.

The position states of the quantum walk are represented by spatial modes of the single photons. The shift operator \hat{S} acting on these modes is implemented by a 37.7 mm long, birefringent calcite beam displacer. The optical axis of each calcite prism is cut so that vertically polarized

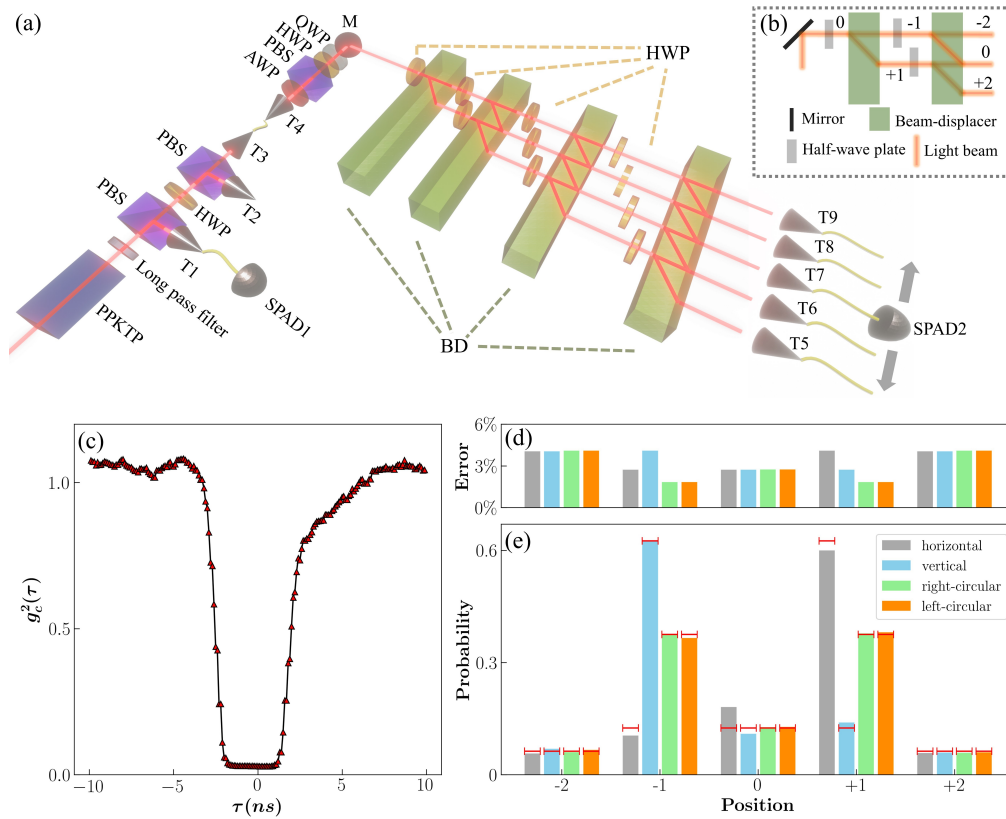


Fig. 2. (a) Schematic of experimental setup. PPKTP: periodically poled potassium titanyl phosphate crystal, PBS: polarized beam splitter, SPAD: single-photon avalanche diode, HWP: half-wave plate, QWP: quarter-wave plate, AWP: adjustable wave plate, M: mirror, BD: beam displacer. Here AWP is designed as a HWP in the middle of two QWPs in order to compensate for the phase shift caused by the fiber twist, and can convert circular polarized light to horizontal polarized light with minimal loss. (b) Details of the first two quantum walk steps in our experiment. (c) The second-order correlation function $g_c^2(\tau)$ versus the delay τ for our heralded single-photon source. The time window length is approximately 3 ns and $g_c^2(0)$ is 0.0286 ± 0.001 . (d) the relative error range of the measurement due to rotation error of HWPs and the stochastic photon number distributions. Different colors represent different polarization states of the initial input single photons, as depicted in (e). (e) measured (color bars) and theoretical (horizontal red segments) probability distribution for a four-step quantum walk.

light was directly transmitted, and horizontal light underwent a 4 mm lateral displacement into a neighboring spatial mode. Here, we place the half wave plates in front of each beam displacer to adjust the splitting ratios in the quantum walk at each step. The aperture diameter of our half-wave plate is small so that each half-wave plate can change the polarization state of one beam of light without affecting adjacent beams. Therefore, we can adjust the splitting ratios at different positions during each walking step.

The details of the first two quantum walk steps are depicted in Fig. 2(b). The spatial modes after step 1 are recombined interferometrically in step 2. Repetition of these steps then forms an interferometric network as in Fig. 2(a). The lattice sites are labeled so that there are odd sites at odd walking steps, and even sites at even steps. After an n -step quantum walk, the photons

output in $(n + 1)$ spatial modes are coupled into an optical fiber and subsequently detected by a single-photon photodiode, in coincidence with the trigger photon. As shown in Fig. 2(a), we connect each single-photon output port and an optical fiber with a fiber coupler. Each fiber coupler is connected to one end of the corresponding fiber, and we manually connect the other end of the fiber to the SPAD2 in order to count the number of single photons output from individual output spatial modes. By adjusting all the fiber couplers, the collection efficiency of each fiber coupler is maximized and ensured to be as consistent as possible. We use one SPAD to count single photons so that the quantum efficiency of each measurement remains the same. By doing so, the measurement error due to the systematic difference between different individual output modes is reduced to a negligible level. We use SPAD1 and SPAD2 to perform coincidence measurements in the experiments. The dark counts during the coincidence measurements are relatively small: in our experiments, the coincidence count of each output spatial mode during each measurement ranges from about 3,000 to 37,000 depending on the specific probability distribution, while the dark count remains between zero and two, which is at a negligible level.

To characterize the single-photon purity in the experiments, we also measure the second-order correlation function $g_c^2(\tau)$ for our heralded single-photon source through the Hanbury-Brown and Twiss (HBT) experiment with coincidence time window of length 3 ns, as depicted in Fig. 2(c). The laser power we used in the HBT experiment is 1 mW, and the photon pairs generation rate is about 16,000/s. The minimal value of $g_c^2(\tau)$ is $g_c^2(0) = 0.0286 \pm 0.001$. We can estimate the probability of our heralded single-photon source generating two-photon states using the equation $g_c^2(0) = 2P_2/P_1^2$ [51], where P_1 and P_2 are probabilities for generating the single- and two-photon states. The estimated two-photon state probability is 1.39%, which is close enough to zero, indicating that our heralded single-photon source has high single-photon purity.

For a four-step quantum walk with an unbiased coin ($\theta = \pi/4$), the measured probability distribution at given sites is shown in Fig. 2(e). Here we choose four initial polarization states to verify our experimental system: horizontal polarization, vertical polarization, right-circular polarization, and left-circular polarization. The experimental data (bars with colors) are in excellent agreement with theoretical simulations (horizontal red segments). The measurement error range is presented in Fig. 2(d), where the ordinate is the relative error level with respect to the corresponding measurement results. There are mainly two sources of error: the systematic error caused by the minimal adjustable angle of our half-wave plate (0.25 degree), and the counting error caused by the two-photon state generated from the heralded single-photon source. The former error range is calculated by introducing a random error within 0.25 deg to each HWP and numerically simulate the quantum walk result 1,000 times, and the latter error range can be obtained from P_2 estimated from $g_c^2(0)$. This error analysis method is used throughout the paper to present the error range of each experimental result.

5. Results

5.1. Uniform distribution

Quantum RNGs with a uniform distribution [20,52] are of importance for applications without inherent bias, such as quantum secure communications [11,53]. Therefore, we first evaluate the performance of our algorithm for generating a uniform distribution in a four-step quantum walk system. Here we use the fidelity \mathcal{F} , defined to evaluate the similarity between the output (simulated or measured output) and the target probability distribution,

$$\mathcal{F} = \frac{\sum_m y(m) \cdot T(m)}{\sum_m \max(y(m), T(m))^2}, \quad (8)$$

where y is the system output, T is the target distribution, and m represents the position.

For generating a uniform probability distribution, the fidelity curve during the training of our GD algorithm is shown in Fig. 3(a). The "iterations" represent the accumulating time step

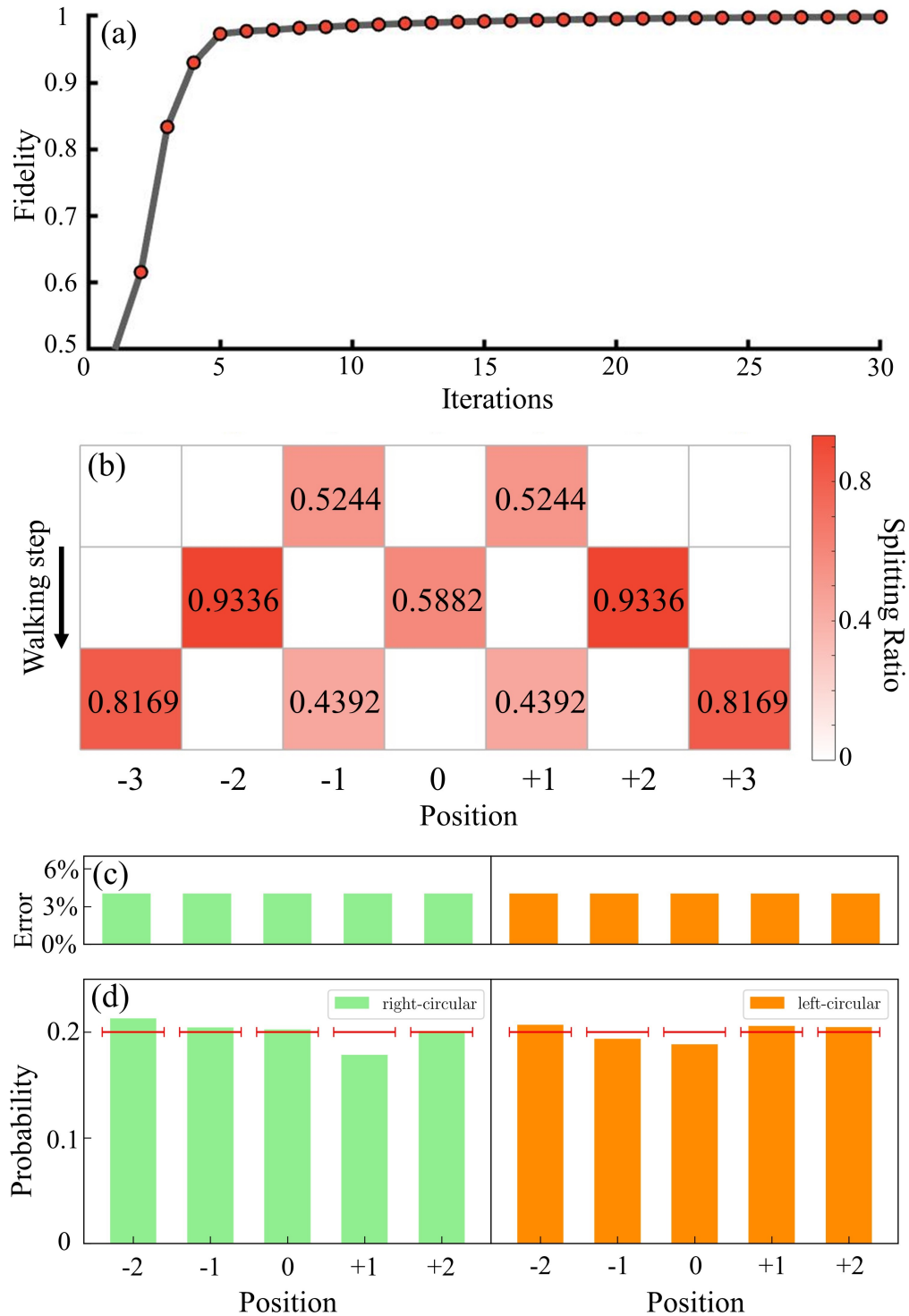


Fig. 3. Uniform probability distribution generation in a four-step quantum walk system. (a) Fidelity as the iteration increases. (b) Values of the splitting ratio of each position and walking step, obtained with our GD algorithm. The black arrow points out the direction of the quantum walking process. The number displayed on the cell is the value of the corresponding splitting ratio r . (c) The relative error range of the measurement. (d) Measured probability distribution of the quantum walk with right-circular (green) and left-polarized (orange) single photons at the input. The horizontal red segments represent the values of the target probability distribution.

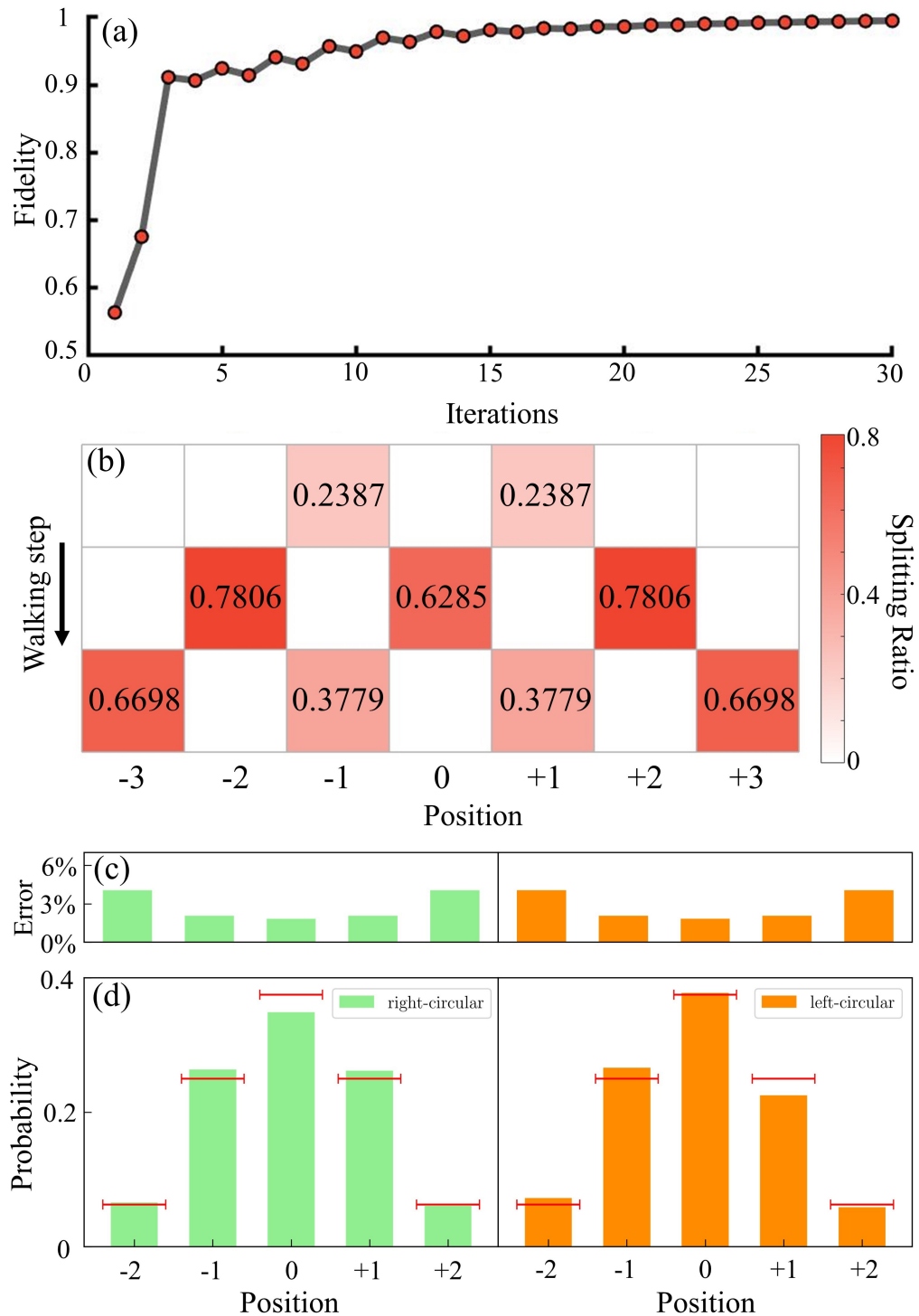


Fig. 4. Gaussian probability distribution generation in a four-step quantum walk system. (a) Fidelity as the iteration increases. (b) Values of the splitting ratio for each walking step and position, obtained with our GD algorithm. (c) The relative error range of the measurement. (d) Measured probability distribution of the quantum walk with right-circular (green) and left-polarized (orange) single photons at the input.

when the training progresses. From Fig. 3(a) we can see that the fidelity increases rapidly as the training process goes on. It exceeds 0.95 after 5 iterations and finally approaches unity within 20 iterations. The learning rate of the training process is set as 0.1. The convergence rate of the training can be further improved by appropriately choosing the learning rate η .

When the training is completed, we obtain the values of the splitting ratio for generating a uniform probability distribution in the quantum walk. The values are shown in Fig. 3(b). Obviously, these values are unlikely to be found manually, while our algorithm can find proper values to obtain a high fidelity. According to these values, we adjust $\{r\}$ in the quantum walk experimental setup by rotating the half-wave plates in front of the BDs. The rotation accuracy of our half-wave plate and the existence of two-photon states leads to a slight deviation between the actual splitting ratios in the experiment and the theoretical values. The error range is depicted in Fig. 3(c). But this does not affect the performance of our experiment because our system is very robust (See Supplement 1 for details of the experimental system robustness analysis). We perform experiments with right-circular and left-circular polarized single photons at the input, respectively. The measured probability distributions for detecting the photon at given positions are shown in Fig. 3(d). It is clear that the measured probability distributions are in good agreement with the target distribution. The fidelities of the experimental results are 96.5% for right-circular polarized input photons and 95.8% for left-circular polarized input photons.

5.2. Gaussian distribution

Gaussian RNGs, as another important RNG, also have diverse applications, including Monte Carlo simulation of Gaussian noises. Specific to quantum information, this type of RNGs provide Gaussian distributed randomness for coherent states modulation in continuous-variable quantum key distribution systems [34–36]. In the following, we show that our GD algorithm can find the parameter set for the quantum walk based RNG to generate Gaussian distributed single-photon outputs.

We set the Gaussian distribution as the target probability distribution for the GD algorithm. The fidelity change during the training process is shown in Fig. 4(a). It can be seen that the fidelity rapidly increases to 95% at the 10th iteration. The splitting ratios can be found in Fig. 4(b).

Figure 4(d) presents the measured probability distribution of single photons in a quantum walk with GD-optimized splitting ratios. Right- and left-circularly polarized photons are chosen as input photons to perform the quantum walk experiment. The experimentally measured probability distribution is again in good agreement with the target distribution. The fidelities of the experiment results are 94.1% and 95.8% for the right- and left-circular polarized input photons, respectively. These results show that our algorithm can be utilized to adjust a quantum walk system to generate single photons with desired distributions. This allows one to build an effective quantum RNG that conforms to arbitrary probability distributions.

6. Conclusion

We have reported a GD-enhanced quantum RNG based on quantum walks of single photons in a linear optical system. Our multi-bit quantum RNG can generate true random numbers with an arbitrarily defined probability distribution with nearly unitary fidelity. The promised faithful randomness of our quantum RNG can determine the random measurement basis in high-dimensional quantum communications [54–57]. We note that quantum walks with a uniform distribution can be used to generate quantum random numbers [58]. In comparison with this method, our GD-enhanced quantum walk can generate quantum random numbers with flexible probability distribution.

Funding. National Natural Science Foundation of China (92365107, 11890704); Office of Naval Research Global (N62909-23-1-2074); Foundational Questions Institute Fund (FQXi-IAF19-06); Asian Office of Aerospace Research and Development (FA2386-20-1-4069); Nippon Telegraph and Telephone Corporation (NTT) Research, the Japan Science

and Technology Agency (JST) via the Quantum Leap Flagship Program (Q-LEAP), and the Moonshot Research and Development Program (JPMJMS2061); Program for Innovative Talents and Teams in 213 Jiangsu (JSSCTD202138); National Key Research and Development Program of China (2019YFA0308700).

Acknowledgements. The authors thank Lijian Zhang and Ben Wang for helpful discussions. We thank the High Performance Computing Center of Nanjing University for allowing the numerical calculations on its blade cluster system.

Disclosures. The authors declare that there are no conflicts of interest related to this article.

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.

Supplemental document. See [Supplement 1](#) for supporting content.

References

1. N. Metropolis and S. Ulam, "The Monte Carlo method," *J. Am. Stat. Assoc.* **44**(247), 335–341 (1949).
2. H. Niederreiter, "Quasi-Monte Carlo methods and pseudo-random numbers," *Bull. Amer. Math. Soc.* **84**(6), 957–1041 (1978).
3. C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.* **28**(4), 656–715 (1949).
4. R. Gennaro, "Randomness in cryptography," *IEEE Secur. Priv.* **4**(2), 64–67 (2006).
5. J. S. Bell, "On the Einstein-Podolsky-Rosen paradox," *Physica* **1**, 195 (1964).
6. P. Shadbolt, J. C. F. Mathews, A. Laing, *et al.*, "Testing foundations of quantum mechanics with photons," *Nat. Phys.* **10**(4), 278–286 (2014).
7. N. Gisin, G. Ribordy, W. Tittel, *et al.*, "Quantum cryptography," *Rev. Mod. Phys.* **74**(1), 145–195 (2002).
8. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, *et al.*, "The security of practical quantum key distribution," *Rev. Mod. Phys.* **81**(3), 1301–1350 (2009).
9. H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nat. Photonics* **8**(8), 595–604 (2014).
10. A. Martin, B. Sanguinetti, C. C. W. Lim, *et al.*, "Quantum random number generation for 1.25-GHz quantum key distribution systems," *J. Lightwave Technol.* **33**(13), 2855–2859 (2015).
11. M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," *Rev. Mod. Phys.* **89**(1), 015004 (2017).
12. J. G. Rarity, P. C. M. Owens, and P. R. Tapster, "Quantum random-number generation and key sharing," *J. Mod. Opt.* **41**(12), 2435–2444 (1994).
13. T. Jennewein, U. Achleitner, G. Weihs, *et al.*, "A fast and compact quantum random number generator," *Rev. Sci. Instrum.* **71**(4), 1675–1680 (2000).
14. A. Stefanov, N. Gisin, O. Guinnard, *et al.*, "Optical quantum random number generator," *J. Mod. Opt.* **47**(4), 595–598 (2000).
15. H.-Q. Ma, Y. Xie, and L.-A. Wu, "Random number generation based on the time of arrival of single photons," *Appl. Opt.* **44**(36), 7760–7763 (2005).
16. M. Stipčević and B. M. Rogina, "Quantum random number generator based on photonic emission in semiconductors," *Rev. Sci. Instrum.* **78**(4), 045104 (2007).
17. J. F. Dynes, Z. L. Yuan, A. W. Sharpe, *et al.*, "A high speed, postprocessing free, quantum random number generator," *Appl. Phys. Lett.* **93**(3), 031109 (2008).
18. M. A. Wayne, E. R. Jeffrey, G. M. Akselrod, *et al.*, "Photon arrival time quantum random number generation," *J. Mod. Opt.* **56**(4), 516–522 (2009).
19. H. Fürst, H. Weier, S. Nauerth, *et al.*, "High speed optical quantum random number generation," *Opt. Express* **18**(12), 13029–13037 (2010).
20. M. Ren, E. Wu, Y. Liang, *et al.*, "Quantum random-number generator based on a photon-number-resolving detector," *Phys. Rev. A* **83**(2), 023820 (2011).
21. Y. Jian, M. Ren, E. Wu, *et al.*, "Two-bit quantum random number generator based on photon-number-resolving detection," *Rev. Sci. Instrum.* **82**(7), 073109 (2011).
22. S. Tisa, F. Villa, A. Giudice, *et al.*, "High-speed quantum random number generation using CMOS photon counting detectors," *IEEE J. Sel. Top. Quantum Electron.* **21**(3), 23–29 (2015).
23. W. Wei and H. Guo, "Bias-free true random-number generator," *Opt. Lett.* **34**(12), 1876–1878 (2009).
24. Z. Bisadi, A. Meneghetti, G. Fontana, *et al.*, "Quantum random number generator based on silicon nanocrystals LED," in *Integrated Photonics: Materials, Devices, and Applications III*, vol. 9520 J.-M. Fédéli, ed. (2015), p. 952004.
25. Y. Shen, L. Tian, and H. Zou, "Practical quantum random number generator based on measuring the shot noise of vacuum states," *Phys. Rev. A* **81**(6), 063814 (2010).
26. C. Gabriel, C. Wittmann, D. Sych, *et al.*, "A generator for unique quantum random numbers based on vacuum states," *Nat. Photonics* **4**(10), 711–715 (2010).
27. Y. Zhu, G. He, and G. Zeng, "Unbiased quantum random number generation based on squeezed vacuum state," *Int. J. Quantum Inf.* **10**(01), 1250012 (2012).
28. H. Guo, W. Tang, Y. Liu, *et al.*, "Truly random number generation based on measurement of phase noise of a laser," *Phys. Rev. E* **81**(5), 051137 (2010).

29. B. Qi, Y.-M. Chi, H.-K. Lo, *et al.*, “High-speed quantum random number generation by measuring phase noise of a single-mode laser,” *Opt. Lett.* **35**(3), 312–314 (2010).
30. Y.-Q. Nie, L. Huang, Y. Liu, *et al.*, “The generation of 68 Gbps quantum random number by measuring laser phase fluctuations,” *Rev. Sci. Instrum.* **86**(6), 063105 (2015).
31. C. R. S. Williams, J. C. Salevan, X. Li, *et al.*, “Fast physical random number generator using amplified spontaneous emission,” *Opt. Express* **18**(23), 23584–23597 (2010).
32. P. J. Bustard, D. Moffatt, R. Lausten, *et al.*, “Quantum random bit generation using stimulated Raman scattering,” *Opt. Express* **19**(25), 25173–25180 (2011).
33. A. Sarkar and C. M. Chandrashekar, “Multi-bit quantum random number generation from a single qubit quantum walk,” *Sci. Rep.* **9**(1), 12323 (2019).
34. Y. Zhang, Z. Li, Z. Chen, *et al.*, “Continuous-variable QKD over 50 km commercial fiber,” *Quantum Sci. Technol.* **4**(3), 035006 (2019).
35. Y. Zhang, Z. Chen, S. Pirandola, *et al.*, “Long-distance continuous-variable quantum key distribution over 202.81 km of fiber,” *Phys. Rev. Lett.* **125**(1), 010502 (2020).
36. M. Huang, Z. Chen, Y. Zhang, *et al.*, “A Gaussian-distributed quantum random number generator using vacuum shot noise,” *Entropy* **22**(6), 618 (2020).
37. D. B. Thomas, W. Luk, P. H. Leong, *et al.*, “Gaussian random number generators,” *ACM Comput. Surv.* **39**(4), 11–49 (2007).
38. R. Zhang, R. Yang, J. Guo, *et al.*, “Arbitrary coherent distributions in a programmable quantum walk,” *Phys. Rev. Res.* **4**(2), 023042 (2022).
39. J. Biamonte, P. Wittek, N. Pancotti, *et al.*, “Quantum machine learning,” *Nature* **549**(7671), 195–202 (2017).
40. P. Palittapongarnpim, P. Wittek, E. Zahedinejad, *et al.*, “Learning in quantum control: High-dimensional global optimization for noisy quantum dynamics,” *Neurocomputing* **268**, 116–126 (2017).
41. I. Kerenidis and A. Prakash, “Quantum gradient descent for linear systems and least squares,” *Phys. Rev. A* **101**(2), 022316 (2020).
42. M. Cai, Y. Lu, M. Xiao, *et al.*, “Optimizing single-photon generation and storage with machine learning,” *Phys. Rev. A* **104**(5), 053707 (2021).
43. S. Ruder, “An overview of gradient descent optimization algorithms,” *arXiv*, arXiv:1609.04747, (2016).
44. H. Jeong, M. Paternostro, and M. S. Kim, “Simulation of quantum random walks using the interference of a classical field,” *Phys. Rev. A* **69**(1), 012310 (2004).
45. H. B. Perets, Y. Lahini, F. Pozzi, *et al.*, “Realization of quantum walks with negligible decoherence in waveguide lattices,” *Phys. Rev. Lett.* **100**(17), 170506 (2008).
46. A. Peruzzo, M. Lobino, J. C. F. Matthews, *et al.*, “Quantum walks of correlated photons,” *Science* **329**(5998), 1500–1503 (2010).
47. H. Tang, C. Di Franco, Z.-Y. Shi, *et al.*, “Experimental quantum fast hitting on hexagonal graphs,” *Nat. Photonics* **12**(12), 754–758 (2018).
48. Q.-P. Su, Y. Zhang, L. Yu, *et al.*, “Experimental demonstration of quantum walks with initial superposition states,” *npj Quantum Inf.* **5**(1), 40 (2019).
49. Z. Yan, Y.-R. Zhang, M. Gong, *et al.*, “Strongly correlated quantum walks with a 12-qubit superconducting processor,” *Science* **364**(6442), 753–756 (2019).
50. Q.-P. Su, S.-C. Wang, Y. Chi, *et al.*, “Implementing quantum walks with a single qubit,” *arXiv*, arXiv:2206.03642 (2022).
51. M. Chen, J. Tang, L. Tang, *et al.*, “Photon blockade and single-photon generation with multiple quantum emitters,” *Phys. Rev. Res.* **4**(3), 033083 (2022).
52. M. Eaton, A. Hossameldin, R. J. Birrittella, *et al.*, “Resolution of 100 photons and quantum generation of unbiased random numbers,” *Nat. Photonics* **17**(1), 106–111 (2022).
53. Z. Tang, Z. Liao, F. Xu, *et al.*, “Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution,” *Phys. Rev. Lett.* **112**(19), 190503 (2014).
54. A. Vaziri, J.-W. Pan, T. Jennewein, *et al.*, “Concentration of higher dimensional entanglement: Qutrits of photon orbital angular momentum,” *Phys. Rev. Lett.* **91**(22), 227902 (2003).
55. X.-L. Wang, Y.-H. Luo, H.-L. Huang, *et al.*, “18-qubit entanglement with six photons’ three degrees of freedom,” *Phys. Rev. Lett.* **120**(26), 260502 (2018).
56. Z.-F. Liu, C. Chen, J.-M. Xu, *et al.*, “Hong-Ou-Mandel interference between two hyperentangled photons enables observation of symmetric and antisymmetric particle exchange phases,” *Phys. Rev. Lett.* **129**(26), 263602 (2022).
57. Z.-X. Li, D. Zhu, P.-C. Lin, *et al.*, “High-dimensional entanglement generation based on a Pancharatnam-Berry phase metasurface,” *Photonics Res.* **10**(12), 2702–2707 (2022).
58. M. Grafe, R. Heilmann, A. Perez-Leija, *et al.*, “On-chip generation of high-order single-photon W-states,” *Nat. Photonics* **8**(10), 791–795 (2014).