Supplemental Document

Optics EXPRESS

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

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

Supplement DOI: https://doi.org/10.6084/m9.figshare.25737624

Parent Article DOI: https://doi.org/10.1364/OE.509601

Generation of True Quantum Random Numbers with On-Demand Probability Distributions via Single-Photon Quantum Walks: supplemental document

1. DETAILS OF THE THEORETICAL MODEL

Here we present the details of the mathematical expression for our gradient descent (GD) algorithm. The basic idea of our algorithm is iteratively adjusting the splitting ratio of the quantum walk system according to the error between the system output and the target, so that the final single-photon distribution reaches the target distribution. Therefore, the key of our GD-based scheme is deriving the mathematical form of the updated value for the splitting ratio. In the following, we present the mathematical derivation of the updating value in our algorithm.

Without loss of generality, we first consider the splitting ratio at position m in the last walking step of an n-step quantum walk system. The schematic of the last walking step is shown in Fig. S1(a). 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, and $r_m^{(n)}$ is the splitting ratio of the n-th walking step starting from position m. The measured probability and target probability for detecting single photons at position m is denoted by P_m and T_m, respectively. The error e_m between P_m and T_m is defined as $e_m = T_m - P_m$. As we have demonstrated in the main text, the measured probability P_m can be written in terms of the complex amplitude of the coin state. Then P_{m-1} and P_{m+1} in Fig. S1(a) can be written as

$$\begin{aligned} P_{m-1} &= |c_{m,L}^{(n)}|^2 + |c_{m-2,R}^{(n)}|^2 = |a_{m,L}^{(n)} + i \cdot b_{m,L}^{(n)}|^2 + |a_{m-2,R}^{(n)} + i \cdot b_{m-2,R}^{(n)}|^2 \\ P_{m+1} &= |c_{m,R}^{(n)}|^2 + |c_{m+2,L}^{(n)}|^2 = |a_{m,R}^{(n)} + i \cdot b_{m,R}^{(n)}|^2 + |a_{m+2,L}^{(n)} + i \cdot b_{m+2,L}^{(n)}|^2 , \end{aligned} \tag{S1}$$

where a and b are the real and imaginary components of c, respectively. From Fig. S1(a) we can see that the complex amplitudes $c_{m,L}^{(n)}, c_{m,R}^{(n)}$ can be further expressed in terms of $c_{m-1,R}^{(n-1)}, c_{m+1,L}^{(n-1)}$ and the splitting ratio $r_m^{(n)}$ as follows,

$$\begin{aligned} c_{m,L}^{(n)} &= \sqrt{r_m^{(n)}} c_{m+1,L}^{(n-1)} + \sqrt{1 - r_m^{(n)}} c_{m-1,R}^{(n-1)} \\ c_{m,R}^{(n)} &= \sqrt{1 - r_m^{(n)}} c_{m+1,L}^{(n-1)} - \sqrt{r_m^{(n)}} c_{m-1,R}^{(n-1)} , \end{aligned} \tag{S2}$$

so the relation between $\{a_{m,L}^{(n)}, a_{m,R}^{(n)}\}$ ($\{b_{m,L}^{(n)}, b_{m,R}^{(n)}\}$) and $\{a_{m-1,R}^{(n-1)}, a_{m+1,L}^{(n)}\}$ ($\{b_{m-1,R}^{(n-1)}, b_{m+1,L}^{(n)}\}$) becomes

$$\begin{aligned} a_{m,L}^{(n)} &= \sqrt{r_m^{(n)}} a_{m+1,L}^{(n-1)} + \sqrt{1 - r_m^{(n)}} a_{m-1,R}^{(n-1)} \\ a_{m,R}^{(n)} &= \sqrt{1 - r_m^{(n)}} a_{m+1,L}^{(n-1)} - \sqrt{r_m^{(n)}} a_{m-1,R}^{(n-1)} \\ b_{m,L}^{(n)} &= \sqrt{r_m^{(n)}} b_{m+1,L}^{(n-1)} + \sqrt{1 - r_m^{(n)}} b_{m-1,R}^{(n-1)} \\ b_{m,R}^{(n)} &= \sqrt{1 - r_m^{(n)}} b_{m+1,L}^{(n-1)} - \sqrt{r_m^{(n)}} b_{m-1,R}^{(n-1)} . \end{aligned} \tag{S3}$$

By substituting Eq. S3 into Eq. S1, we obtain the mathematical relation between the measured probability and the interested splitting ratio,

$$\begin{aligned}
P_{m-1} &= \left(\sqrt{r_m^{(n)}}a_{m+1,L}^{(n-1)} + \sqrt{1-r_m^{(n)}}a_{m-1,R}^{(n-1)}\right)^2 + \left(\sqrt{r_m^{(n)}}b_{m+1,L}^{(n-1)} + \sqrt{1-r_m^{(n)}}b_{m-1,R}^{(n-1)}\right)^2 \\
&+ \left(\sqrt{1-r_{m-2}^{(n)}}a_{m-1,L}^{(n-1)} - \sqrt{r_{m-2}^{(n)}}a_{m-3,R}^{(n-1)}\right)^2 + \left(\sqrt{1-r_{m-2}^{(n)}}b_{m-1,L}^{(n-1)} - \sqrt{r_{m-2}^{(n)}}b_{m-3,R}^{(n-1)}\right)^2 \\
P_{m+1} &= \left(\sqrt{1-r_m^{(n)}}a_{m+1,L}^{(n-1)} - \sqrt{r_m^{(n)}}a_{m-1,R}^{(n-1)}\right)^2 + \left(\sqrt{1-r_m^{(n)}}b_{m+1,L}^{(n-1)} - \sqrt{r_m^{(n)}}b_{m-1,R}^{(n-1)}\right)^2 \\
&+ \left(\sqrt{r_{m+2}^{(n)}}a_{m+3,L}^{(n-1)} + \sqrt{1-r_{m+2}^{(n)}}a_{m+1,R}^{(n-1)}\right)^2 + \left(\sqrt{r_{m+2}^{(n)}}b_{m+3,L}^{(n-1)} + \sqrt{1-r_{m+2}^{(n)}}b_{m+1,R}^{(n-1)})\right)^2 .
\end{aligned} \tag{S4}$$

As we have demonstrated in the main text, in each iteration of our algorithm, the splitting ratio $r_m^{(n)}$ updates according to $\left[r_m^{(n)} + \sum_j \eta(T_j - P_j)\frac{\partial P_j}{\partial r_m^{(n)}}\right] \to r_m^{(n)}$, where $\eta \in (0,1]$ is the learning rate and the term $(T_j - P_j)$ can be written as e_j. Since $r_m^{(n)}$ only connects to the two photon detector channels P_{m-1} and P_{m+1}, the updating value of $r_m^{(n)}$ can be written as

$$\Delta r_m^{(n)} = \sum_j \eta e_j \frac{\partial P_j}{\partial r_m^{(n)}} = \eta\left(e_{m-1}\frac{\partial P_{m-1}}{\partial r_m^{(n)}} + e_{m+1}\frac{\partial P_{m+1}}{\partial r_m^{(n)}}\right) , \tag{S5}$$

substituting Eq. S4 into Eq. S5, we then obtain the detailed expression for the updated values of the splitting ratio $r_m^{(n)}$ as

$$\begin{aligned}
\Delta r_m^{(n)} =& \eta e_{m-1}\left[\left(\sqrt{r_m^{(n)}}a_{m+1,L}^{(n-1)} + \sqrt{1-r_m^{(n)}}a_{m-1,R}^{(n-1)}\right)\left(\frac{1}{\sqrt{r_m^{(n)}}}a_{m+1,L}^{(n-1)} - \frac{1}{\sqrt{1-r_m^{(n)}}}a_{m-1,R}^{(n-1)}\right)\right] \\
&+ \eta e_{m-1}\left[\left(\sqrt{r_m^{(n)}}b_{m+1,L}^{(n-1)} + \sqrt{1-r_m^{(n)}}b_{m-1,R}^{(n-1)}\right)\left(\frac{1}{\sqrt{r_m^{(n)}}}b_{m+1,L}^{(n-1)} - \frac{1}{\sqrt{1-r_m^{(n)}}}b_{m-1,R}^{(n-1)}\right)\right] \\
&+ \eta e_{m+1}\left[\left(\sqrt{1-r_m^{(n)}}a_{m+1,L}^{(n-1)} - \sqrt{r_m^{(n)}}a_{m-1,R}^{(n-1)}\right)\left(-\frac{1}{\sqrt{1-r_m^{(n)}}}a_{m+1,L}^{(n-1)} - \frac{1}{\sqrt{r_m^{(n)}}}a_{m-1,R}^{(n-1)}\right)\right] \\
&+ \eta e_{m+1}\left[\left(\sqrt{1-r_m^{(n)}}b_{m+1,L}^{(n-1)} - \sqrt{r_m^{(n)}}b_{m-1,R}^{(n-1)}\right)\left(-\frac{1}{\sqrt{1-r_m^{(n)}}}b_{m+1,L}^{(n-1)} - \frac{1}{\sqrt{r_m^{(n)}}}b_{m-1,R}^{(n-1)}\right)\right] .
\end{aligned} \tag{S6}$$

Therefore, during the training process of our algorithm, we iteratively update the values of $r_m^{(n)}$ according to Eq. S6 to minimize the loss function. For a splitting ratio in the walking step other than the last step, the derivation of its updating value in our algorithm is similar to the above process. Here we consider the splitting ratio at position m in the $(n-1)$ walking step of an n-step quantum walk, as depicted in Fig. S1. From Fig. S1 we can see that the value of $r_m^{(n-1)}$ affects three photon detection probabilities: P_{m-2}, P_m, P_{m+2}. Therefore, the updating value of $r_m^{(n-1)}$ during the algorithm training process can be written as

$$\begin{aligned}
\Delta r_m^{(n-1)} &= \sum_j \eta e_j \frac{\partial P_j}{\partial r_m^{(n-1)}} = \eta\left(e_{m-2}\frac{\partial P_{m-2}}{\partial r_m^{(n-1)}} + e_m\frac{\partial P_m}{\partial r_m^{(n-1)}} + e_{m+2}\frac{\partial P_{m+2}}{\partial r_m^{(n-1)}}\right) . \\
&= \eta e_{m-1}\left(\frac{\partial P_{m-2}}{\partial a_{m-1,L}^{(n)}}\frac{\partial a_{m-1,L}^{(n)}}{\partial a_{m,L}^{(n-1)}}\frac{\partial a_{m,L}^{(n-1)}}{\partial r_m^{(n-1)}} + \frac{\partial P_{m-2}}{\partial b_{m-1,L}^{(n)}}\frac{\partial b_{m-1,L}^{(n)}}{\partial b_{m,L}^{(n-1)}}\frac{\partial b_{m,L}^{(n-1)}}{\partial r_m^{(n-1)}}\right) .
\end{aligned} \tag{S7}$$

The terms in brackets in Eq. S7 are the sum of the partial derivatives of $\{P_{m-2}, P_m, P_{m+2}\}$ with respect to $r_m^{(n-1)}$, which can be split into four partial derivation paths as marked in Fig. S1(b).

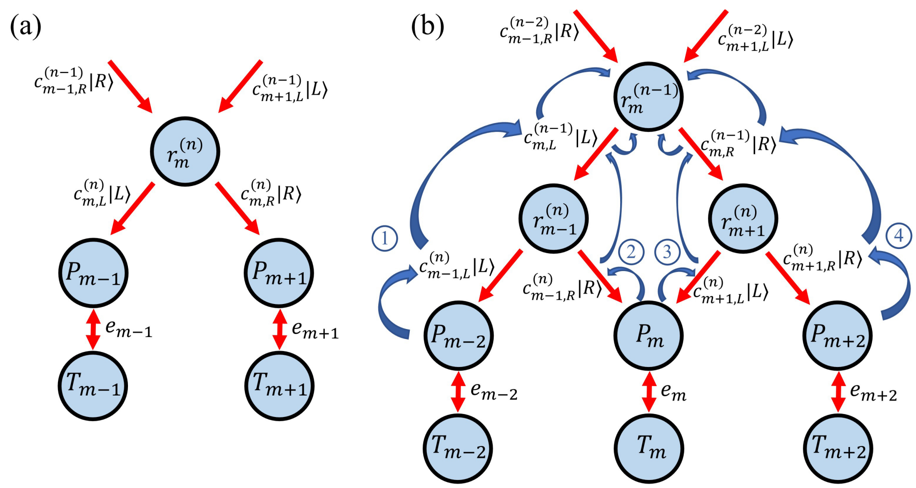

Fig. S1. Detailed description of quantum state transfer in a quantum walk system. (a) Detailed quantum state transfer in the last quantum walking step. (b) Detailed quantum state transfer in the second-to-last quantum walking step. Blue arrows and circled numbers represent the different partial derivation paths of detection probabilities $\{P_{m-2}, P_m, P_{m+2}\}$ with respect to $r_m^{(n-1)}$.

Then Eq. S7 can be written as

$$
\begin{aligned}
\Delta r_m^{(n-1)} &= \eta e_{m-2}\text{①} + \eta e_m\text{②} + \eta e_m\text{③} + \eta e_{m+2}\text{④} \\
&= \eta e_{m-2}\left(\frac{\partial P_{m-2}}{\partial a^{(n)}_{m-1,L}}\frac{\partial a^{(n)}_{m-1,L}}{\partial a^{(n-1)}_{m,L}}\frac{\partial a^{(n-1)}_{m,L}}{\partial r^{(n-1)}_m} + \frac{\partial P_{m-2}}{\partial b^{(n)}_{m-1,L}}\frac{\partial b^{(n)}_{m-1,L}}{\partial b^{(n-1)}_{m,L}}\frac{\partial b^{(n-1)}_{m,L}}{\partial r^{(n-1)}_m}\right) \\
&\quad + \eta e_m\left(\frac{\partial P_m}{\partial a^{(n)}_{m-1,R}}\frac{\partial a^{(n)}_{m-1,R}}{\partial a^{(n-1)}_{m,L}}\frac{\partial a^{(n-1)}_{m,L}}{\partial r^{(n-1)}_m} + \frac{\partial P_m}{\partial b^{(n)}_{m-1,R}}\frac{\partial b^{(n)}_{m-1,R}}{\partial b^{(n-1)}_{m,L}}\frac{\partial b^{(n-1)}_{m,L}}{\partial r^{(n-1)}_m}\right) \\
&\quad + \eta e_m\left(\frac{\partial P_m}{\partial a^{(n)}_{m+1,L}}\frac{\partial a^{(n)}_{m+1,L}}{\partial a^{(n-1)}_{m,R}}\frac{\partial a^{(n-1)}_{m,R}}{\partial r^{(n-1)}_m} + \frac{\partial P_m}{\partial b^{(n)}_{m+1,L}}\frac{\partial b^{(n)}_{m+1,L}}{\partial b^{(n-1)}_{m,R}}\frac{\partial b^{(n-1)}_{m,R}}{\partial r^{(n-1)}_m}\right) \\
&\quad + \eta e_{m+2}\left(\frac{\partial P_{m+2}}{\partial a^{(n)}_{m+1,R}}\frac{\partial a^{(n)}_{m+1,R}}{\partial a^{(n-1)}_{m,R}}\frac{\partial a^{(n-1)}_{m,R}}{\partial r^{(n-1)}_m} + \frac{\partial P_m}{\partial b^{(n)}_{m+1,R}}\frac{\partial b^{(n)}_{m+1,R}}{\partial b^{(n-1)}_{m,R}}\frac{\partial b^{(n-1)}_{m,R}}{\partial r^{(n-1)}_m}\right).
\end{aligned}
\tag{S8}
$$

According to Eq. S8 we can obtain the updating value for $r_m^{(n-1)}$ during the training. The mathematical expression of the updating value for the splitting ratio seems complex, but it is convenient to be programmed because the partial derivatives have highly similar mathematical forms.

2. SYSTEM ROBUSTNESS ANALYSIS

Our GD algorithm can be used to obtain precise splitting ratio values for generating arbitrarily distributed single photons. However, the actual splitting ratio values in the experiment may have a slight deviation from theoretical values. In the following, we will show that the influence caused by these deviations can be neglected. We introduce a random deviation Δr_{err} into each splitting ratio value in our quantum walk system and numerically simulated its final probability distribution, and compare the probability distribution with the deviation-free simulated result. By doing so, we can quantify the robustness of our quantum walk system.

Here we introduce random deviation at $\sim 1\%$ level into each splitting ratio value in a 10-step quantum walk system, and numerically simulated its probability distributions. The results are shown in Fig. S2, where the left and right panel present the results for the generation of a Gaussian (a) and a uniform probability (b) distribution, respectively. The red dots are the ideal probability

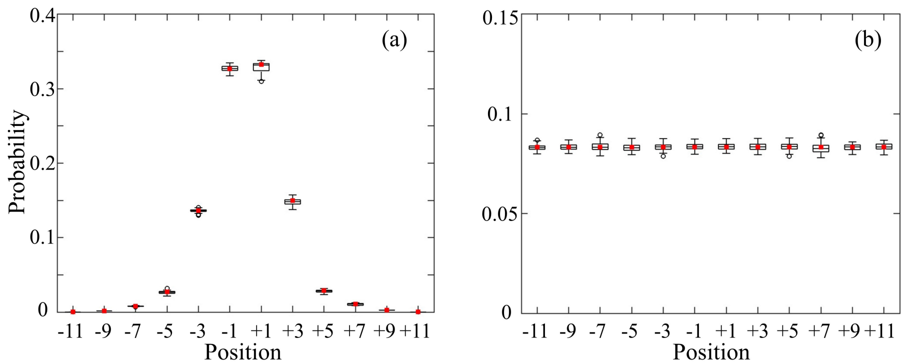

Fig. S2. Numerical simulations of a Gaussian (a) and a uniform (b) probability distributions of a quantum walk system with 1% deviation in the splitting ratio. Box-plot is counted from 100 numerical simulation results. Red markers indicate the ideal probabilities of the target distributions.

distributions. The box-plots are drawn by characterizing 100 numerical simulation results. From Fig. S2 we can see that the influence caused by the splitting ratio deviation are tolerable. The fidelities of the simulated probability distributions with deviation are also above 95%, which further proves the strong robustness of our quantum walk system.