SCIENTIFIC REPORTS

OPEN

Novel pseudo-random number generator based on quantum random walks

Received: 02 February 2015
Accepted: 14 October 2015
Published: 04 February 2016

Yu-Guang Yang[1,2,3,4] & Qian-Qian Zhao[1]

In this paper, we investigate the potential application of quantum computation for constructing pseudo-random number generators (PRNGs) and further construct a novel PRNG based on quantum random walks (QRWs), a famous quantum computation model. The PRNG merely relies on the equations used in the QRWs, and thus the generation algorithm is simple and the computation speed is fast. The proposed PRNG is subjected to statistical tests such as NIST and successfully passed the test. Compared with the representative PRNG based on quantum chaotic maps (QCM), the present QRWs-based PRNG has some advantages such as better statistical complexity and recurrence. For example, the normalized Shannon entropy and the statistical complexity of the QRWs-based PRNG are 0.999699456771172 and 1.799961178212329e-04 respectively given the number of 8 bits-words, say, 16Mbits. By contrast, the corresponding values of the QCM-based PRNG are 0.999448131481064 and 3.701210794388818e-04 respectively. Thus the statistical complexity and the normalized entropy of the QRWs-based PRNG are closer to 0 and 1 respectively than those of the QCM-based PRNG when the number of words of the analyzed sequence increases. It provides a new clue to construct PRNGs and also extends the applications of quantum computation.

Random numbers have an extensive application in various contexts including statistical mechanics, gaming industry, cryptography and communication etc. Two basic types of random number generators exist: true random number generators (TRNGs) and pseudo-random number generators (PRNGs). Generally, the generation of TRNGs depends on certain physical sources such as thermal noise[1], atmospheric noise[2], radioactive decay[3], etc. Although TRNGs are considered to attain a higher security, the implementation of TRNGs generally requires additional devices which make TRNGs inconvenient[4].

By contrast, PRNGs can generate "pseudo-random" numbers deterministically by inputting an initial seed to given algorithms. The main advantages of PRNGs are the rapidity and the repeatability of the pseudo-random sequences and requiring less memory for algorithm storage. In general, PRNGs are based on certain mathematical difficulty assumptions, such as: non-linear congruences[5], linear feedback shift registers (LFSR)[6], discrete logarithm problem[7], quadratic residuosity problem[8], cellular automata[9,10], etc. Unfortunately, such PRNGs are usually slower, due to heavy computational instructions.

Another interesting way to design PRNGs is connected to chaos theory[11]. Chaotic systems are characterized by their high sensitivity to initial conditions and some properties like ergodicity, pseudo-random behavior and high complexity[11] which make chaotic systems very attractive for implementing PRNGs. Several PRNGs have been proposed[12–15]. However, some security loopholes often occur in such chaos-based PRNGs due to the lack of rigorous security analyses[16].

As one of the most important contributions in nonlinear science, classical chaos theory has been studied widely and applied in various contexts such as mathematics, physics, chemistry, computer science, biology and so on. Quantum information theory has achieved a rapid development due to the fascinate quantum effects such as quantum superposition and entanglement. A natural question that arises is how to characterize chaos in the quantum regime, i.e., how to manifest chaos itself at the quantum level. This has led to the development of quantum chaos theory. Signatures of chaos in quantum systems have been explored in the contexts of level statistics

[1]College of Computer Science and Technology, Beijing University of Technology, Beijing, 100124, China. [2]State Key Laboratory of Information Security (Institute of Information Engineering, Chinese Academy of Sciences, Beijing, 100093), China. [3]Beijing Key Laboratory of Trusted Computing, Beijing, 100124, China. [4]National Engineering Laboratory for Critical Technologies of Information Security Classified Protection, Beijing, 100124, China. Correspondence and requests for materials should be addressed to Y.G.Y. (email: yangyang7357@bjut.edu.cn)

of chaotic Hamiltonians[17], the dynamics of open quantum systems undergoing measurement or decoherence[18,19] and hypersensitivity of a system to perturbations[20,21].

Another natural question that arises is how to use the chaotic characteristics of such quantum chaotic systems. In fact, the uses of quantum chaos in constructing PRNGs and other applications have been explored[22–25]. For many years dissipative quantum maps were widely used as informative models of quantum chaos, such as the quantum kicked top, the quantum baker's map, the quantum lazy baker's map, and the quantum sawtooth and cat maps[26,27]. It is natural to ask whether there exist other quantum chaotic systems with more excellent chaotic behaviours.

Quantum computation is a rapidly growing field and lots of breakthroughs have been achieved during the past decades[28]. As a universal quantum computation model, QRWs are the quantum counterparts of classical random walks and have been developed as a useful tool for solving various problems[29–32], such as element distinctness, finding the triangle, and routing, etc. Furthermore, the widespread application of classical random walks in many fields like physics, biology, computer science, finance, etc., infers the possibility that its quantum analog, namely, QRWs, could be used as a tool for many future applications.

Inspired by the above reasons, we are motivated to search for novel quantum chaotic systems. In this paper, we investigate QRWs and propose a novel QRWs-based PRNG. It is found that the QRWs-based PRNG can generate more excellent pseudo-randomness than the QCM-based PRNG[22] by numerical simulations and performance comparisons in terms of quantifiers based on information theory, recurrence plots, non-periodity, and various randomness tests, etc.

Results

The chaotic behavior of quantum random walks.

QRWs have two models: discrete QRWs and continuous QRWs[28]. The one-dimensional (1D) discrete QRWs on the line includes two quantum systems: a walker whose motion is restricted to the line and a coin. The state of the walker-coin system is denoted by a vector in the Hilbert space $H_t = H_p \otimes H_c$, where the subscripts p and c stand for walker and coin, respectively. The motion of the walk is conditioned by the coin state via a conditional shift operator

$$\hat{S} = \sum_x (|x+1,\, 0\rangle\langle x,\, 0| + |x-1,\, 1\rangle\langle x,\, 1|), \tag{1}$$

where the summation symbol denotes the sum over all possible positions. The evolution of the total quantum system can be implemented by repeating the sequence of the coin flipping operator and the conditional shift operator in equation (1) step by step (so-called discrete time), expressed by

$$\hat{U} = \hat{S}(\hat{I} \otimes \hat{C}), \tag{2}$$

where $\hat{I}$ is the identity operator of the walker and $\hat{C}$ is the flipping operator applied to the coin state, generally expressed by $\hat{C} = \begin{bmatrix} \cos\,\theta & \sin\,\theta \\ \sin\,\theta & -\cos\,\theta \end{bmatrix}$, $\theta \in \{0,\, 2\pi\}$. Hence the final state $|\psi\rangle_t$ after t steps is expressed by

$$|\psi\rangle_t = (\hat{U})^t |\psi\rangle_{initial} = \sum_x \sum_v \lambda_{x,v} |x,\, v\rangle, \tag{3}$$

and the probability of locating the walker at position x after t steps is

$$P(x,\, t) = \sum_{v \in \{0,1\}} \left| \langle x,\, v| (\hat{U})^t |\psi\rangle_{initial} \right|^2, \tag{4}$$

where $|\psi\rangle_{initial}$ is the initial state of the total quantum system.

For n-dimensional discrete QRWs on the line, the final state $|\psi\rangle_t = \hat{U}|\psi\rangle_0$ after t steps is expressed by

$$|\psi\rangle_t = (\hat{U})^t |\psi\rangle_0 = \sum_{x_1}\sum_{v_1}\sum_{x_2}\sum_{v_2}\cdots\sum_{x_n}\sum_{v_n} \lambda_{x_1x_2\cdots x_n, v_1v_2\cdots v_n} |x_1x_2\cdots x_n,\, v_1v_2\cdots v_n\rangle, \tag{5}$$

and the probability of locating the n walkers at position $x_1,\, x_2,\, \cdots,\, x_n$ after t steps is

$$P(x_1x_2\cdots x_n,\, t) = \sum_{v_1,v_2,\cdots,v_n \in \{0,1\}} \left| \left\langle x_1x_2\cdots x_n,\, v_1v_2\cdots v_n \middle| (\hat{U})^t \middle| \psi \right\rangle_0 \right|^2, \tag{6}$$

where $|\psi\rangle_0$ is the initial state of the total n-walker, n-coin quantum system. It can be seen that the resulting probability distribution in equation (6) is the sum of squares of the norms of amplitudes so that there exists a non-linearity map between the initial state $|\psi\rangle_0$ and the resulting probability distribution. And the high sensitivity to initial conditions underlies the proposed PRNG.

Pseudo random number generator based on quantum random walks.

In this section, we discuss how to construct the QRWs-based PRNG by running the one-dimensional discrete QRWs on a circle. In the one-dimensional discrete QRWs on a circle with N nodes, the position state $|x\rangle$ should be altered to $|x\,(\mathrm{mod}\ \ N)\rangle$. The steps of generating pseudo-random numbers are as follows:

(1) Choose the initial parameters (N, (α, β), r, θ) of the one-dimensional discrete QRWs on a circle with N nodes and run it to generate a probability distribution P_1. Here r is the step number of the QRWs whose value belongs to the positive integer domain. N is the node number of the circle whose value also belongs to the positive integer domain. α and β are the amplitude parameters of the coin states which are complex numbers and satisfy the constraint: $|\alpha|^2 + |\beta|^2 = 1$. θ is the parameter of the coin operator $\hat{C}$, where $\theta \in \{0, 2\pi\}$. Here,

$$P_1 = \begin{bmatrix} p_{11} & p_{12} & \cdots & \cdots & p_{1N} \\ p_{21} & p_{22} & \cdots & \cdots & p_{2N} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ p_{N1} & p_{N2} & \cdots & \cdots & p_{NN} \end{bmatrix}_{N\times N}, \tag{7}$$

where $0 \le p_{ij} \le 1$. We transform the probability distribution P_1 into the sequence S_1: $[p_{11}, p_{12}, \cdots p_{1N}, p_{21}, p_{22}, \cdots p_{2N}, \cdots, p_{N1}, p_{N2}, \cdots p_{NN}]$.

(2) Repeat step (1) and group all generated probability distribution sequences $S_i (i = 1, 2, \ldots, m)$ into a random number sequence $k = (S_1, S_2, \cdots, S_m)$.

Note that quantum walks on the line have a property that when a walker takes r steps, where r is an odd number, the probability of standing on a point that labeled even is zero. When r is even, the probabilities on odd points are zero too. But on an odd circle with N nodes, when $r \ge N$, the probabilities on all nodes are nonzero essentially. Therefore, we cannot judge the number of steps, even its parity.

Security analyses of the QRWs-based PRNG.

Experiments are performed on a laptop with Intel(R) Core(TM)2 Duo CPU T5870 2.00 GHz RAM running on Windows 7 professional equipped with the MATLAB R2012a environment. Here we chose the initial key parameters ($N = 6$, ($\alpha = 0$, $\beta = 1$), $r = 10$, $\theta = \pi/3$).

In order to measure the randomness of the QRWs-based PRNG, some quantifiers were proposed. The quantifiers are mainly classified into two classes: (i) quantifiers based on information theory[33–35], (ii) quantifiers based on recurrence plots[36,37].

Statistical complexity measure. Complexity is a measure of off-equilibrium 'order'. Statistical complexity measures (SCM) were proposed as quantifiers of the degree of physical structure in a signal[33,38,39]. They are null for total random processes. In this section, based on the method of ref. 40, we analyzed the statistical complexity of the QRWs-based PRNG. The intensive SCM ($C_J[P]$) can be considered as a quantity that characterizes the probability distribution P associated with the time series generated by the dynamical system[40]. It quantifies not only randomness but also the presence of correlational structures[39,40] and can be used to study the intricate structures hidden in the dynamics. The measure of statistical complexity $C_J[P]$ is defined as[40]:

$$C_J[P] = Q_J[P, P_e] \cdot H_S[P], \tag{8}$$

where the normalized entropic measure $H_S[P] = S[P]/S_{\max}$ is associated with the probability distribution P, with $S_{\max} = S[P_e](0 \le H_S \le 1)$ for the equilibrium distribution P_e and S is the Shannon entropy. The disequilibrium Q_J is defined in terms of the Jensen-Shannon divergence[40] by

$$Q_J[P, P_e] = Q_0\{S[(P + P_e)/2] - S[P]/2 - S[P_e]/2\}, \tag{9}$$

with Q_0 being the normalization constant $(0 \le Q_J \le 1)$. Thus, the disequilibrium Q_J is an intensive quantity. Following the methodology proposed by Bandt and Pompe[41], the comparisons between our proposal and the QCM-based scheme[22] in terms of the normalized entropy H_S and the intensive statistical complexity C_J as functions of the number of 8 bits-words are shown in Figs 1 and 2 respectively. As can be seen from the figures, when the number of words of the analyzed sequence increases, the statistical complexity and the normalized entropy tend to 0 and 1 respectively. It is shown that given the same words, our scheme has better statistical complexity and normalized Shannon entropy than the PRNG scheme based on QCM[22]. For example, the normalized Shannon entropy and the statistical complexity of the QRWs-based PRNG are 0.999699456771172 and 1.799961178212329e-04 respectively given the number of 8 bits-words, say, 16Mbits. By contrast, the corresponding values of the QCM-based PRNG are 0.999448131481064 and 3.701210794388818e-04 respectively. Thus the statistical complexity and the normalized entropy of the QRWs-based PRNG are closer to 0 and 1 respectively than those of the QCM-based PRNG when the number of words of the analyzed sequence increases. It can be concluded that, the randomness of the proposed QRWs-based PRNG is successfully verified by the statistical complexity and the normalized Shannon entropy.

Recurrence plots. Recurrence is a fundamental property of dynamical systems, which can be exploited to characterize the system's behaviour in phase space. In 1987, Eckmann *et al.* introduced a powerful tool for visualization and analysis of recurrences called recurrence plot (*RP*)[36]. *RP* is a two-dimensional representation in which both axes are time ones. The recurrence of a state appearing at two given times t_i, t_j is pictured in the two-dimensional graph by means of either black or white dots, where a black dot denotes a recurrence.

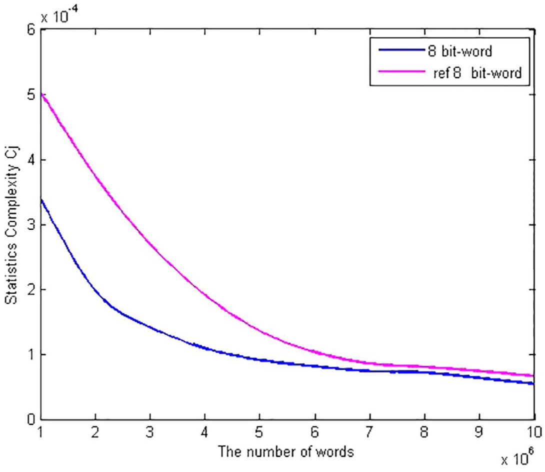

Figure 1. Comparisons in terms of Normalized Shannon entropy H_S. The red curve denotes the Normalized Shannon entropy in the QCM-based scheme[22] as functions of the number of 8 bits-words, while the blue curve represents the Normalized Shannon entropy of our proposal. (see text in the section entitled Results).

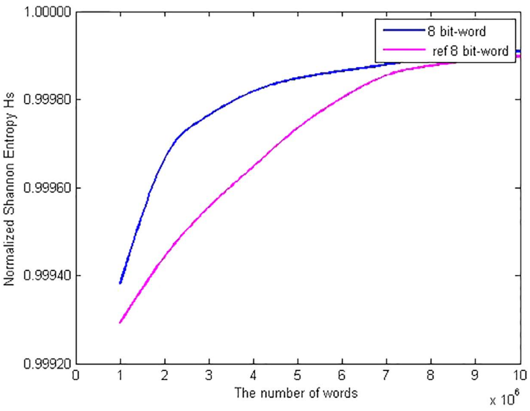

Figure 2. Comparisons in terms of intensive statistical complexity measure C_J. The red curve denotes the intensive statistical complexity in the QCM-based scheme[22] as functions of the number of 8 bits-words, while the blue curve represents the intensive statistical complexity of our proposal. (see text in the section entitled Results).

To visualize the recurrences of states of a dynamical system, the *RP* of a trajectory $\vec{x}_i \in \Re^d$ can be formally expressed by the matrix

$$R_{i,j}(\varepsilon) = \Theta\left(\varepsilon - \left\|\vec{x}_i - \vec{x}_j\right\|\right),\ i, j = 1, \cdots, N, \tag{10}$$

where N is the number of measured points $\vec{x}_i$, ε is a threshold distance, $\Theta(\cdot)$ is the Heaviside function (i.e. $\Theta(x) = 0$, if $x < 0$, and $\Theta(x) = 1$ otherwise) and $\| \cdot \|$ is a norm.

Because the visual impact produced by the *RP* is insufficient to demonstrate the quality of the QRWs-based PRNG because of the 'small-scale' structures[37], several measures of complexity which quantify the small scale structures in *RP*s, have been proposed[42–44] and are known as recurrence quantification analysis (*RQA*). In this paper, these measures based on the diagonal and vertical line structures are considered.

Measures based on diagonal lines. The measures are related to the histogram $P(\varepsilon, l)$ of the diagonal line lengths l, given by

$$P(\varepsilon, l) = \sum_{i,j=1}^{N} (1 - R_{i-1,j-1}(\varepsilon))(1 - R_{i+l,j+l}(\varepsilon)) \prod_{k=0}^{l-1} R_{i+k,j+k}(\varepsilon). \tag{11}$$

The ratio of recurrence points that form diagonal structures (of at least length $l_{\min}$) to all recurrence points is defined by

$$DET = \frac{\sum_{l=l_{\min}}^{N} lP(\varepsilon, l)}{\sum_{l=1}^{N} lP(\varepsilon, l)}, \tag{12}$$

as a measure for determinism (or predictability) of the system. The threshold $l_{\min}$ excludes the diagonal lines which are formed by the tangential motion of the phase space trajectory.

A diagonal line of length l means that a segment of the trajectory is rather close during l time steps to another segment of the trajectory at a different time; thus these lines are related to the divergence of the trajectory segments. The average diagonal line length

$$L = \frac{\sum_{l=l_{\min}}^{N} lP(\varepsilon, l)}{\sum_{l=l_{\min}}^{N} P(\varepsilon, l)}, \tag{13}$$

is the average time that two segments of the trajectory are close to each other, and can be interpreted as the mean prediction time.

Measures based on vertical lines. The total number of the vertical lines of the length v in the RP is then given by the histogram

$$P(v) = \sum_{i,j=1}^{N} (1 - R_{i,j}(\varepsilon))(1 - R_{i,j+v}(\varepsilon)) \prod_{k=0}^{v-1} R_{i,j+k}(\varepsilon). \tag{14}$$

Analogous to the definition of the determinism in equation (12), the ratio between the recurrence points forming the vertical structures and the entire set of recurrence points can be computed,

$$LAM = \frac{\sum_{v=v_{\min}}^{N} vP(v)}{\sum_{v=1}^{N} vP(v)}. \tag{15}$$

The computation of LAM is realized for those v that exceed a minimal length $v_{\min}$ in order to decrease the influence of the tangential motion. LAM will decrease if the RP consists of more single recurrence points than vertical structures.

The average length of vertical structures is given by

$$TT = \frac{\sum_{v=v_{\min}}^{N} vP(v)}{\sum_{v=v_{\min}}^{N} P(v)}, \tag{16}$$

and is called trapping time. TT estimates the mean time that the system will abide at a specific state or how long the state will be trapped.

Figure 3 gives some selected RQA measures for different values of the parameter r and demonstrates the good statistical properties of the QRWs-based PRNG. Figure 4 gives the corresponding selected RQA measures for different values of the dissipation parameter β based on QCM[25] with the initial parameters (x,y,z,r) = (0.62352345,0.0152345,0.0352345,3.99). Generally, processes with uncorrelated or weakly correlated and stochastic or chaotic behaviours cause none or very short diagonals, whereas deterministic processes cause longer diagonals (verticals) and less single, isolated recurrence points. Therefore, the measure DET or LAM should be small given an appropriate threshold $l_{\min}$ ($v_{\min}$), with a typical value of 0.3 or so as shown in Fig. 3. The measure L or TT is the average time that two segments of the trajectory are close to each other, and can be interpreted as the mean prediction time, with a typical value of 3 or so given the parameters at hand. By contrast, the corresponding values of the QCM-based PRNG, i.e., DET, LAM, L and TT average 0.8, 0.6, 60 and 100, respectively. It can be concluded that, the randomness of the proposed QRWs-based PRNG is successfully verified.

Degree of non-periodicity. In this section, we use the scale index to study the non-periodicity in the QRWs-based PRNG, which is introduced by Benìtez *et al.*[45]. The scale index technique is based on the continuous wavelet transform (CWT) and the wavelet multi-resolution analysis[46]. To study non-periodicity of the QRWs-based PRNG[47], we assumed that the key sequence f is compactly supported and defined over a finite time interval I = [a, b]. In order to avoid boundary problems, the wavelet function is compactly supported and the interval I is big enough.

The CWT of f at time u and scale s is defined as follows[46]:

$$Wf(u, s) := \langle f, \psi_{u,s} \rangle = \int_{-\infty}^{+\infty} f(t) \psi_{u,s}^{*}(t) dt, \tag{17}$$

and it provides the frequency component (or details) of f corresponding to the scale s and time location t.

The scalogram of f is defined as follows:

$$\zeta(s) := \| Wf(u, s) \| = \left(\int_{-\infty}^{+\infty} |Wf(u, s)|^2 du \right)^2, \tag{18}$$

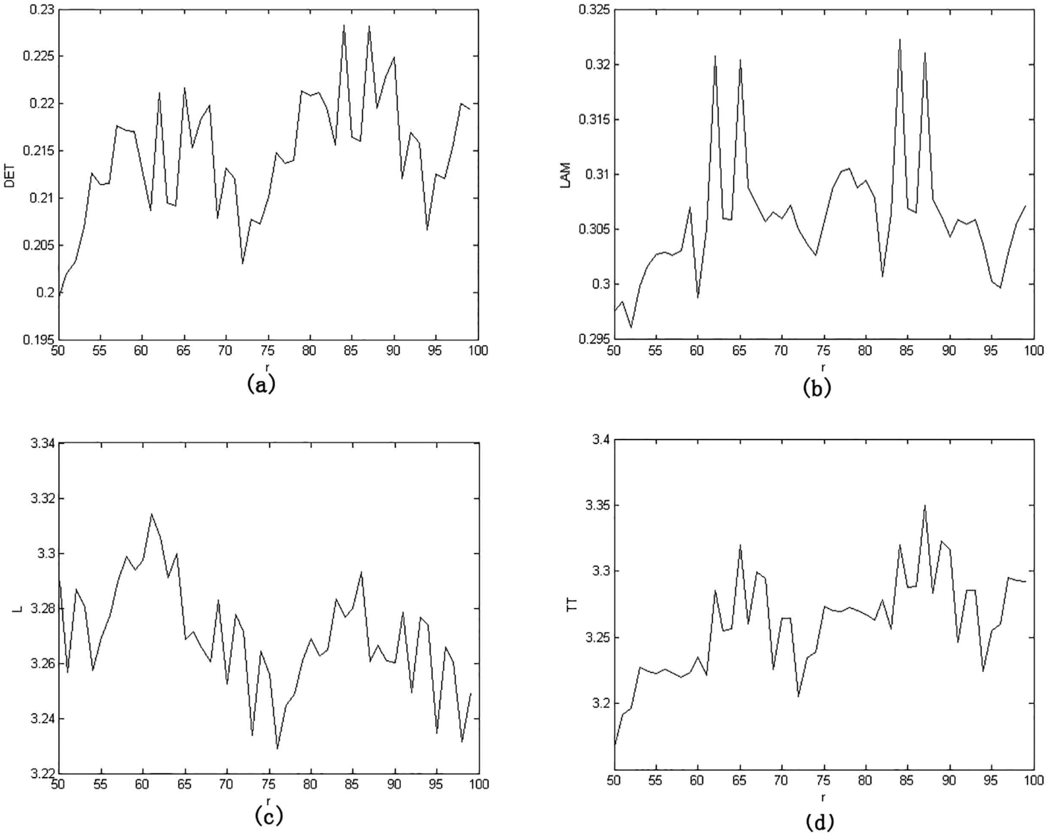

Figure 3. Selected *RQA* measures for the QRWs-based PRNG. (**a**) *DET*, (**b**) *LAM*, (**c**) *L*, (**d**) *TT*. (see text in the section entitled Results).

where $\zeta(s)$ is the energy of the CWT of f at scale s. The scalogram is a useful tool for studying a signal, since it allows the detection of its most representative scales or frequencies[45,47]. Also, the inner scalogram of f at a scale s can be defined by:

$$\zeta^{inner}(s) := \|Wf(u, s)\|_{J(s)} = \left(\int_{c(s)}^{d(s)} |Wf(u, s)|^2 du\right)^2, \tag{19}$$

where $J(s) = [c(s), d(s)] \subseteq I$ is the maximal subinterval in I for which the support of $\psi_{u,s}$ is included in I for all $u \in J(s)$. As the length of $J(s)$ depends on the scale s, the values of the inner scalogram at different scales cannot be compared. Therefore, the inner scalogram should be normalized as follows[45]:

$$\overline{\zeta}^{inner}(s) = \frac{\zeta^{inner}(s)}{(d(s) - c(s))^{\frac{1}{2}}}. \tag{20}$$

Supplementary Figure S1 online shows that the normalized inner scalogram can be a valuable tool for detecting the non-periodicity of the signal, where a signal with details at every scale is non-periodic. Here the selection of the scale interval $[s_0, s_1]$ is very important in the scalogram analysis. Since the non-periodic character of a signal is given by its behavior at large scales, there is no need for s_0 to be very small. In general, we can choose s_0 such that $s_{\max} = s_0 + \varepsilon$ where ε is positive and close to zero. On the other hand, s_1 should be large enough for detecting periodicities. Here, we considered the integer scales between $s_0 = 1$ and $s_1 = 20$.

The scale index of f in the scale interval $[s_0, s_1]$ can be defined by:

$$i_{scale} := \frac{\zeta(s_{\min})}{\zeta(s_{\max})}, \tag{21}$$

where $s_{\max}$ is the smallest scale such that $\zeta(s) \leq \zeta(s_{\max})$ for all $s \in [s_0, s_1]$, and $s_{\min}$ is the smallest scale such that $\zeta(s_{\min}) \leq \zeta(s)$ for all $s \in [s_{\max}, s_1]$. Note that for compactly supported signals only the normalized inner scalogram will be considered[45]. From its definition, the scale index i_{scale} meets $0 \leq i_{scale} \leq 1$ and it can be interpreted as a measure of the degree of non-periodicity of the signal: the scale index will be zero or close to zero for periodic sequences and close to one for highly non-periodic sequences[45].

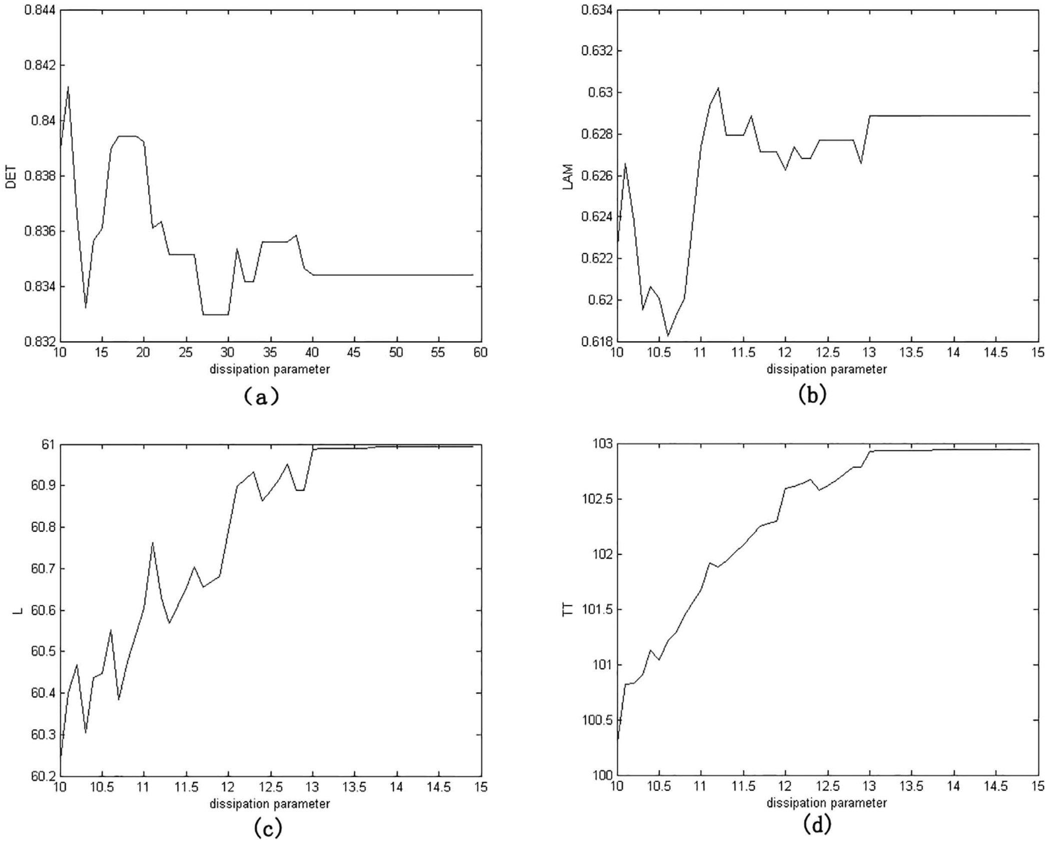

Figure 4. Selected *RQA* measures for the QCM-based scheme[22]. (**a**) *DET*, (**b**) *LAM*, (**c**) *L*, (**d**) *TT*. (see text in the section entitled Results).

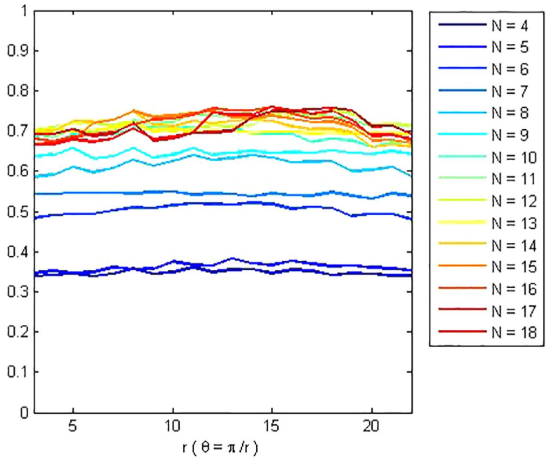

Figure 5. The scale index of the QRWs-based PRNG for different values of the parameter θ.

Since the scale index gives a measure of the degree of non-periodicity of the signal, this can be used to specify which values of the QRWs parameters are best for the generation of pseudo-random number sequences. In Fig. 5, the scale index analysis of the QRWs-based key sequence is presented. It can be concluded that, the best value of the scale index is $i_{scale} \approx 0.7$ for all $N \geq 15$ and θ, which is just the upper bound of that of the scheme in ref. 22. Thus, the sequence in this state is highly non-periodic and it can be used for any PRNG purpose.

Key space analysis. A desirable image encryption scheme should have a sufficiently large key space to resist brute-force attacks. The encryption key of our algorithm can be represented by (n, (α, β), r, θ). Although there is an infinite key space theoretically, because of finite precision of digital computers, the key space actually turns out

Test name	P-value	Result
Approximate entropy test (block = 10)	0.565844	SUCCESS
Block frequency test (block = 128)	0.932368	SUCCESS
Cumulative sums (forward) test	0.438435	SUCCESS
Cumulative sums (reverse) test	0.051895	SUCCESS
Spectral DFT test	0.180314	SUCCESS
Frequency test	0.222465	SUCCESS
Linear complexity (block = 500)	0.826735	SUCCESS
Longest runs of ones test	0.388167	SUCCESS
Non-Overlapping templates test		
(m = 9, template = 000111101)	0.962460	SUCCESS
Overlapping template of all ones test (m = 9)	0.577368	SUCCESS
Random excursions test (x = −1)	0.506488	SUCCESS
Random excursions variant test (x = +1)	0.527057	SUCCESS
Rank test	0.436267	SUCCESS
Runs test	0.436267	SUCCESS
Serial test1 (block = 16)	0.719705	SUCCESS
Serial test2 (block = 16)	0.580439	SUCCESS
Universal statistical test (block = 7)	0.596355	SUCCESS

Table 1. Randomness test by NIST SP800-22 for the QRWs-based PRNG.

to be finite. Considering that the calculation precision is 10^{-16}, the size of key space for initial conditions and control parameters would be roughly $10^{80} \approx 2^{266}$, which is large enough for any encryption purposes and is also large enough to resist all kinds of brute-force attacks.

Random tests for the pseudo-random sequences. To verify the randomness property of our QRWs-based PRNG sequence, we used NIST SP800-22 to test the randomness of the sequences generated by QRWs (see Table 1). Each test produces a *P-value* in [0, 1]. If the *P-value* is higher than the preset threshold α, it means that the sequences pass the test. In our tests, we set $\alpha = 0.01$ and generate a large of number to meet the requirements of the software NIST for the magnitude 1000000. $\alpha = 0.01$ implies that the pseudo-random sequence can be inferred to be random with 99% probability if it passes the test. From Table 1, the results of different number sequences generated by QRWs are all "success". Hence, we can judge that our QRWs-based generator passes the NIST SP800-22 tests.

Speed performance analysis. Speed is an important factor for evaluating the performance of a PRNG. For the proposed PRNG algorithm, we measured the time cost in the running environment: Windows 7, Matlab R2012a, Intel(R) Core(TM) i3-2370M CPU 2.00GHz 2GB RAM and the mean time cost of generating random sequences is 0.001361s or so. Therefore, our algorithm is fast enough for practical application.

Discussion

As a kind of TRNGs, quantum random number generators (QRNGs) can significantly improve the security of cryptographic protocols by means of quantum effects. QRNGs have typically been based on specialized physical hardware, such as single-photon sources and detectors[48] or homodyne detection[49], photon-number resolving detectors[50], parametric oscillators[51], or Raman scattering[52]. However, the cost, size, and power requirements of current QRNGs have prevented them from becoming widespread. Fortunately, Sanguinetti *et al.*[53] proposed a novel method for quantum random number generation by means of cameras which can be integrated in many common devices such as cell photons, tablets, and laptops. They exploited the quantum effect called "quantum noise" or "shot noise" to realize a QRNG by using a detector capable of resolving this distribution. In experiment, Sanguinetti *et al.* exploited the image sensors in cameras and smartphones to resolve quantum noise. In contrast to Sanguinetti *et al.*'s QRNG, our QRWs-based PRNG exploits the properties of QRWs, i.e., the high sensitivity of the walker's position probability distribution to initial conditions. Without any physical device, the PRNG merely relies on the equations used in the QRWs, and thus the random number generation algorithm is simple and the computation speed is fast.

As a quantum analog of simulated annealing, quantum annealing (QA) has also attracted lots of attention[54,55]. It can be exploited for solving optimization problems by using quantum tunneling. In QA, the optimization problem is encoded in a Hamiltonian H_P. The algorithm starts by introducing strong quantum fluctuations by adding a disordering Hamiltonian H' that does not commute with H_P. An example case is

$$H = H_P + \Gamma H', \tag{22}$$

where Γ changes from a large value to zero during the evolution. The disorder is slowly removed by removing H' (reducing Γ). Generally, it is rather difficult to solve the Schrödinger equation in equation (22) and thus the random-process-based methods are used, such as quantum Monte Carlo method. If the process is slow enough, the system will settle in a local minimum close to the exact solution. Theoretically the slower the evolution, the better the solution will be achieved at the cost of consuming longer computation time. To reduce the computation time, on the one hand, QRWs can be introduced into the moving strategies for performing Metropolis Monte Carlo sampling so as to decrease the times of finding global optimum efficiently using the properties of quantum parallel computation. On the other hand, the QRWs-based PRNG can also be used for quantum annealers as an efficient random number generator needed during iteration.

Conclusion

In a summary, we have proposed a new QRWs-based PRNG. Numerical simulations demonstrate that the proposed PRNG exhibits excellent pseudo-randomness in terms of quantifiers based on information theory, recurrence plots, non-periodity, and NIST tests. It can be concluded that the new QRWs-based PRNG can generate a high percentage of usable pseudo-random numbers for various applications and it also extends the application scope of quantum computation.

Future work will also concentrate on how to design QRWs with better cryptographic properties. To obtain more complicated non-linear dynamic behaviors of QRWs, it is necessary to research the construction of multi-walker, multi-coin QRWs on a circle, tree, graph or other graph structures.

Methods

To generate the probability distribution P_1, we assume the initial state of the total quantum system of the one-dimensional discrete QRWs on a circle with N nodes

$$\left|\psi\right\rangle_0 = \left|x\right\rangle \otimes \left|\upsilon\right\rangle. \tag{23}$$

Here

$$|\upsilon\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{24}$$

where $|\alpha|^2 + |\beta|^2 = 1$.

The difference between a line and a circle is that the circle has N nodes and is cyclical. The difference of walks on the line and on circles is that the conditional shift operator on circles becomes $\hat{S}$, i.e.,

$$\hat{S} = \begin{cases} |2,\, 0\rangle\langle 1,\, 0| + |N,\, 1\rangle\langle 1,\, 1|, & for \quad x = 1; \\ |1,\, 0\rangle\langle N,\, 0| + |N - 1,\, 1\rangle\langle N,\, 1|, & for \quad x = N; \\ |x + 1,\, 0\rangle\langle x,\, 0| + |x - 1,\, 1\rangle\langle x,\, 1|, & for \quad x \neq 1,\, N. \end{cases} \tag{25}$$

Here we let the coin operator $\hat{C}$

$$\hat{C} = \begin{bmatrix} \cos\ \theta & \sin\ \theta \\ \sin\ \theta & -\cos\ \theta \end{bmatrix}.\quad \theta \in \left\{0,\, 2\pi\right\}. \tag{26}$$

Choose the initial parameters $(N, (\alpha,\ \beta), r, \theta)$ of the one-dimensional discrete QRWs on a circle with N nodes and run it to generate a probability distribution P_1, given by

$$P_1 = \sum_{v \in \{0,1\}} \left|\langle x,\, v|\,(\hat{S}(\hat{I} \otimes \hat{C}))^r\,|\psi\rangle_0\right|^2. \tag{27}$$

References

1. Bucci, M., Germani, L., Luzzi, R., Trifiletti, A. & Varanonuovo, M. A high speed random number source for cryptographic applications on a Smart card. *IEEE Trans. Comput*. **52,** 403–409 (2003).
2. Holman, W. T., Connelly, J. A. & Downlatabadi, A. B. An integrated analog/digital random noise source. *IEEE Trans. Circuits System I* **44,** 521–528 (1997).
3. Walker, J. HotBits: genuine random numbers generated by radioactive decay. (2001). Available at: http://www.fourmilab.ch/hotbits, (Accessed: 20th November 2014).
4. Lunghi, T. *et al.* Self-testing quantum random number generator. *Phys. Rev. Lett*. **114,** 150501 (2015).
5. Eichenauer, J. & Lehn, J. A non-linear congruential pseudo random number generator. *Statistische Hefte* **27,** 315–326 (1986).
6. Peinado, A. & Fuster-Sabater, A. Generation of pseudorandom binary sequences by means of linear feedback shift registers (LFSRs) with dynamic feedback. *Math. Comput. Model.* **57,** 2596–2604 (2013).
7. Blum, M. & Micali, S. How to generate cryptographically strong sequences of pseudorandom bits. *SIAM J. Comput*. **13,** 850–864 (1984).
8. Blum, L., Blum, M. & Shub, M. A simple unpredictable pseudo-random number generator. *SIAM J. Comput*. **15,** 364–383 (1986).
9. Tomassini, M., Sipper, M., Zolla, M. & Perrenoud, M. Generating high-quality random numbers in parallel by cellular automata. *Future Gener. Comput. Syst*. **16,** 291–305 (1999).
10. Vlassopoulos, N. & Girau, B. A metric for evolving 2-D cellular automata as pseudo-random number generators. *J. Cell. Auto.* **9,** 139–152 (2014).
11. Álvarez, G. & Li, S. Some basic cryptographic requirements for chaos-based cryptosystems. *Int. J. Bifurcat. Chaos* **16,** 2129–2151 (2006).
12. Lui, O. Y., Yuen, C. H. & Wong, K. W. A pseudo-random number generator employing multiple Renyi maps. *Int. J. Mod. Phys. C* **24,** 1350079 (2013).

13. François, M., Grosges, T., Barchiesi, D. & Erra, R. A new pseudo-random number generator based on two chaotic maps. *Informatica* **24,** 181–197 (2013).
14. Hu, H., Liu, L. & Ding, N. Pseudorandom sequence generator based on Chen chaotic system. *Comput. Phys. Commun*. **184,** 765–768 (2013).
15. François, M., Grosges, T., Barchiesi, D. & Erra, R. Pseudo-random number generator based on mixing of three chaotic maps. *Commun. Nonlinear Sci. Numer. Simulat*. **19,** 887–895 (2014).
16. Özkaynak, F. & Yavuz, S. Security problems for a pseudorandom sequence generator based on the Chen chaotic system. *Comput. Phys. Commun*. **184,** 2178–2181 (2013).
17. Bohigas, O., Giannoni, M. J. & Schmit, C. Characterization of chaotic quantum spectra and universality of level fluctuation. *Phys. Rev. Lett*. **52,** 1–4 (1984).
18. Bhattacharya, T., Habib, S. & Jacobs, K. Continuous quantum measurement and the emergence of classical chaos. *Phys. Rev. Lett*. **85,** 4852–4855 (2000).
19. Zurek, W. H. & Paz, J. P. Decoherence, Chaos, and the 2nd law. *Phys. Rev. Lett*. **72,** 2508–2511 (1994).
20. Peres, A. Stability of quantum motion in chaotic and regular systems. *Phys. Rev. A* **30,** 1610–1615 (1984).
21. Schack, R. & Caves, C. Information-theoretic characterization of quantum chaos. *Phys. Rev. E* **53,** 3257–3270 (1996).
22. Akhshani, A., Akhavan, A., Mobaraki, A., Lim, S. C. & Hassan, Z. Pseudo random number generator based on quantum chaotic map. *Commun. Nonlinear Sci. Numer. Simulat*. **19,** 101–111 (2014).
23. Turgut, O. E., Turgut, M. S. & Coban, M. T. Chaotic quantum behaved particle swarm optimization algorithm for solving nonlinear system of equations. *Computers Math. Appl*. **68,** 508–530 (2014).
24. Abd El-Latif, A. A., Li, L.,Wang, N., Han, Q. & Niu, X. M. A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces. *Sig. Process*. **93,** 2986–3000 (2013).
25. Akhshani, A., Akhavan, A., Lim, S. C. & Hassan, Z. An image encryption scheme based on quantum logistic map. *Commun. Nonlinear Sci. Numer. Simulat*. **17,** 4653–4661 (2012).
26. Berry, M. V., Balazs, N. L., Tabor, M. & Voros, A. Quantum maps. *Ann. Phys*. **122,** 26–63 (1979).
27. Soltan, P. M. On quantum maps into quantum semigroups. *Houston J. Math*. **40,** 779–790 (2014)
28. Elías, S. & Andraca, V. Quantum walks: a comprehensive review. *Quantum Inf. Process*. **11,** 1015–1106 (2012).
29. Ambainis, A. Quantum walk algorithm for element distinctness. *SIAM J. Comput*. **37,** 210–239 (2007).
30. Magniez, F., Santha, M. & Szegedy, M. Quantum algorithms for the triangle problem. *SIAM J. Comput*. **37,** 413–424 (2007).
31. Zhan, X., Qin, H., Bian, Z. H., Li, J. & Xue, P. Perfect state transfer and efficient quantum routing: A discrete-time quantum-walk approach. *Phys. Rev. A* **90,** 012331 (2014).
32. Babatunde, A. M., Cresser, J. & Twamley, J. Using a biased quantum random walk as a quantum lumped element router. *Phys. Rev. A* **90,** 012339 (2014).
33. López-Ruiz, R., Mancini, H. L. & Calbet, X. A statistical measure of complexity. *Phys. Lett. A* **209,** 321–326 (1995).
34. Lamberti, P. W., Martin, M. T., Piastino, A. & Rosso, O. A. Intensive entropy non-triviality measure. *Physica A* **334,** 119–131 (2004).
35. Rosso, O. A., Larrondo, H. A., Martin, M. T., Plastino, A. & Fuentes, M. A. Distinguishing noise from chaos. *Phys. Rev. Lett.* **99,** 154102 (2007).
36. Eckmann, J. P., Oliffson Kamphorst, S. & Ruelle, D. Recurrence plots of dynamical systems. *Europhys. Lett*. **4,** 973–977 (1987).
37. Marwan, N., Romano, M. C., Thiel, M. & Kurths, J. Recurrence plots for the analysis of complex systems. *Phys. Rep*. **438,** 237–329 (2007).
38. Shiner, J. S., Davison, M. & Landsberg, P. T. Simple measure for complexity. *Phys. Rev. E* **59,** 1459–1464 (1999).
39. Martin, M. T., Plastino, A. & Rosso, O. A. Statistical complexity and disequilibrium. *Phys. Lett. A* **311,** 126–132 (2003).
40. Larrondo, H. A., González, C. M., Martin, M. T., Plastino, A. & Rosso, O. A. Intensive statistical complexity measure of pseudorandom number generators. *Physica A* **356,** 133–138 (2005).
41. Bandt, C. & Pompe, B. Permutation entropy: A natural complexity measure for time series. *Phys. Rev. Lett*. **88,** 174102 (2002).
42. Marwan, N., Wessel, N., Meyerfeldt, U., Schirdewan, A. & Kurths, J. Recurrence-plot-based measures of complexity and its application to heart-rate-variability data. *Phys. Rev. E* **66,** 026702 (2002).
43. Zbilut, J. P. & Webber, C. L. Embeddings and delays as derived from quantification of recurrence plots. *Phys. Lett. A* **171,** 199–203 (1992).
44. Webber, C. L. & Zbilut, J. P. Dynamical assessment of physiological systems and states using recurrence plot strategies. *J. Appl. Physiol.* **76,** 965–973 (1994).
45. Benítez, R., Bolós, V. J. & Ramírez, M. E. A wavelet-based tool for studying non-periodicity. *Comput. Math. Appl.* **60,** 634–641 (2010).
46. Baggett, L. W., Medina, H. A. & Merrill, K. D. Generalized multi-resolution analyses and a construction procedure for all wavelet sets in R-n. *J. Fourier Anal. Appl*. **5,** 563–573 (1999).
47. Chandre, C., Wiggins, S. & Uzer, T. Time-frequency analysis of chaotic systems. *Physica D* **181,** 171–196 (2003).
48. Wei, W. & Guo, H. Bias-free true random-number generator. *Opt. Lett*. **34,** 1876 (2009).
49. Gabriel, C. *et al.* A generator for unique quantum random numbers based on vacuum states. *Nat. Photonics* **4,** 711 (2010).
50. Ren, M. *et al.* Quantum random-number generator based on a photon-number-resolving detector. *Phys. Rev. A* **83,** 023820 (2011).
51. Marandi, A., Leindecker, N. C., Vodopyanov, K. L. & Byer, R. L. All-optical quantum random bit generation from intrinsically binary phase of parametric oscillators. *Opt. Exp*. **20,** 19322 (2012).
52. England, D. G. *et al.* Efficient Raman generation in a waveguide: a route to ultrafast quantum random number generation. *Appl. Phys. Lett*. **104,** 051117 (2014).
53. Sanguinetti, B., Martin, A., Zbinden, H. & Gisin, N. Quantum random number generation on a mobile phone. *Phys. Rev. X* **4,** 031056 (2014).
54. Das, A. & Chakrabarti, B. K. Quantum annealing and analog quantum computation. *Rev. Mod. Phys*. **80,** 1061 (2008).
55. Johnson, M. *et al.* Quantum annealing with manufactured spins. *Nature* **473,** 194–198 (2011).

Acknowledgements

This work was supported by the National Natural Science Foundation of China (Grant No. 61572053); The Importation and Development of High-Caliber Talents Project of Beijing Municipal Institutions (No. CIT&TCD201304039); National Cipher Development Fund during the 12th Five-Year Plan Period (No. MMJJ201401006); The Scientific Research Common Program of Beijing Municipal Commission of Education (No. KM201510005016); The Basic Research Foundation of Beijing University of Technology (Nos. X4007999201501, 007000514315501); Jing-Hua Talents Project of Beijing University of Technology (2014-JH-L06); Beijing Natural Science Foundation (Grant No. 4152038); Postgraduate Science and Technology Innovation Foundation of Beijing University of Technology (Nos. ykj-2015-12063, ykj-2015-12113, yjk-2015-11957, yjk-2015-11949).

Author Contributions

Y.Y.G. proposed the theoretical method and wrote the main manuscript text. Z.Q.Q. made the simulations. All authors reviewed the manuscript.

Additional Information

Supplementary information accompanies this paper at http://www.nature.com/srep

Competing financial interests: The authors declare no competing financial interests.

How to cite this article: Yang, Y.-G. and Zhao, Q.-Q. Novel pseudo-random number generator based on quantum random walks. *Sci. Rep.* **6**, 20362; doi: 10.1038/srep20362 (2016).