SCIENTIFIC REPORTS
natureresearch

OPEN

Multi-bit quantum random number generation from a single qubit quantum walk

Received: 5 March 2019
Accepted: 14 August 2019
Published online: 23 August 2019

Anupam Sarkar[1,2] & C. M. Chandrashekar[1,2]

We present a scheme for multi-bit quantum random number generation using a single qubit discrete-time quantum walk in one-dimensional space. Irrespective of the initial state of the qubit, quantum interference and entanglement of particle with the position space in the walk dynamics certifies high randomness in the system. Quantum walk in a position space of dimension 2^l+1 ensures string of $(l+2)$-bits of random numbers from a single measurement. Bit commitment with the position space and control over the spread of the probability distribution in position space enable us with options to extract multi-bit random numbers. This highlights the *power of one qubit*, its practical importance in generating multi-bit string in single measurement and the role it can play in quantum communication and cryptographic protocols. This can be further extended with quantum walks in higher dimensions.

Random number plays an important role in many applications where unpredictability is a key[1,2], especially in cryptographic protocols[3–5] where security is assured because of unpredictability. Though there are some statistical tests[6–8] which can convice us about the random nature of the observed sequence, it is almost impossible to discriminate between a predetermined random string of bits that comes from a dishonest provider or malicious random number generator (RNG) and a *true* random sequence. In the first case the sequence may pass all the statistical tests but still can be completely predictable to the provider or anyone else who wants to eavesdrop. Therefore, generation of genuine randomness and its certification is generally considered impossible with only classical methods. Quantum physics brings out high unpredictability and probabilistic behaviour as an inherent property of nature[9]. Therefore, one can expect certification of *true randomness* in quantum systems to come purely from the principles of quantum physics.

The random nature of quantum mechanics[10] has gained a lot of interest from the time of it's inception. Though the description of quantum system is probabilistic, the probabilistic prediction of a theory does not necessarily imply that it is intrinsically random. There can be some limitation to the formalism and a more complete theory can describe it in a completely deterministic way[11,12]. However, previous works[13–15] suggests that using the nonlocal correlation between two particles can generate the randomness which is truly intrinsic. For example, like measuring entangled particles one can assess the randomness of the process independent of it's quantum description which cannot be described deterministically within the framework of any no-signalling theories. Nonlocality has been proved as an important resource in many information processing tasks like random number generation protocols[16,17], randomness expansion[16,18,19] and amplification[20,21] protocols, and quantum key distribution[15,22,23]. Though there is no direct connection between nonlocality and entanglement[24,25], it is known that any pure entangled states are nonlocal. Using this nonlocality of observed statistics in bipartite Bell scenario, a device independent Quantum Random Number Generator (QRNG) has been suggested[16]. Other than that, various other approaches to built an efficient QRNG have been developed and all of them can be classified under three categories, trusted device, self-testing, and semi self-testing[17]. Though the device-independent or self-testing QRNG is more secure compared to two other protocols, it is unsuitable in some cases because of the slow generation of random numbers with time constrained under current technologies.

In this report we propose a QRNG solely based on the superposition and entanglement property of the quantum walk and we use pure states which associates the nonlocal behaviour as described before. The motivation for using quantum walk is propelled by multiple advantages it can offer along with ability to generate multi-bit from a single qubit. The practical limit is bounded by the experimentally implementable number of steps of quantum walks in any system like, NMR[26],trapped ions[27,28], cold atoms[29], and photonic systems[30–33]. Our analytical and

[1]The Institute of Mathematical Sciences, C. I. T. Campus, Taramani, Chennai, 600113, India. [2]Homi Bhabha National Institute, Training School Complex, Anushakti Nagar, Mumbai, 400094, India. Correspondence and requests for materials should be addressed to C.M.C. (email: chandru@imsc.res.in)

numerical analysis shows that the randomness of an initial state of the particle is being enhanced using the quantum walk dynamics. The result suggests that it's dependency on the initial state is very weak and this ensures that a significantly high randomness is seen even when randomness in initial state is zero.

Discrete-Time Quantum Walk

The Discrete Time Quantum Walk (DTQW) is defined on the Hilbert space $\mathcal{H} = \mathcal{H}_c \otimes \mathcal{H}_p$ where $\mathcal{H}_c$ is the Hilbert space of the particle/walker and $\mathcal{H}_p$ is the position Hilbert space[34–41]. In this paper we consider one-dimensional DTQW with the particle having two internal degrees of freedom. Therefore, $\mathcal{H}_c$ is spanned by the basis states $\{| \uparrow \rangle, | \downarrow \rangle\}$ and we will call it coin space. For the position space the basis states will be $\{|i\rangle: i \in \mathbb{Z}\}$. Each step of DTQW comprises of quantum coin operation,

$$C(\theta) = \begin{bmatrix} \cos\theta & -i\sin\theta \\ -i\sin\theta & \cos\theta \end{bmatrix} \tag{1}$$

followed by a position shift operator defined as

$$\mathcal{S}_x \equiv \sum_x \Big[| \uparrow \rangle\langle \uparrow | \otimes |x-1\rangle\langle x| + | \downarrow \rangle\langle \downarrow | \otimes |x+1\rangle\langle x|\Big]. \tag{2}$$

The resulting operation $\mathcal{W}(\theta) = [\mathcal{S}_x(C(\theta) \otimes 1)]$ evolves the particle in superposition of position space which has no classical analogue and quite advantageous for many information processing tasks and an integral part of quantum simulation schemes. The state of the walker after t-steps will be $|\psi_t\rangle = \mathcal{W}(\theta)^t|\psi_{in}\rangle$, where $|\psi_{in}\rangle$ is the initial state of the walker or the particle. In our consideration

$$|\psi_{in}\rangle = (\cos\delta| \uparrow \rangle + e^{i\eta}\sin\delta| \downarrow \rangle) \otimes |x=0\rangle. \tag{3}$$

Using this initial state we will study the behaviour of the randomness under quantum walk dynamics.

Results

Randomness in coin and position space.

Here, we consider a specific form of quantification of randomness in a quantum system termed as intrinsic randomness of measurement[42]. It has been quantified as a coherence measure and clarifies the operational aspect of quantum coherence. Since the QRNG protocol we propose is solely based on DTQW dynamics, it is necessary to have a good measure of randomness contained in both position and coin space. For evaluating the randomness associated with coin space we have to trace out the part of Hilbert space associated with position space from the density matrix and from the reduced density matrix we can compute the randomness as described in Methods section. Similarly, by tracing out the coin space we can calculate the randomness incorporated with the position space. One important point to note here is that the randomness computed is explicitly of quantum origin and is of different nature from any randomness originated through classical stochastic process.

Randomness in the initial state. If the initial state of walker is of the form given in Eq. (3) (we will omit x whenever no confusion arises), corresponding density matrix would be

$$\begin{aligned}\rho_{in} &= |\psi_{in}\rangle\langle\psi_{in}| \\ &= (\cos^2\delta| \uparrow \rangle\langle \uparrow | + e^{-i\eta}\sin\delta\cos\delta| \uparrow \rangle\langle \uparrow | + e^{i\eta}\sin\delta\cos\delta| \downarrow \rangle\langle \uparrow | + \sin^2\delta| \downarrow \rangle\langle \downarrow |) \otimes |0\rangle\langle 0|.\end{aligned} \tag{4}$$

Using the preceding expression it is easy to calculate the randomness associated with coin and position space individually. For coin space it would be dependent on the parameter δ only and can be expressed as,

$$R_i(\rho_{in}^c) = -(\cos^2(\delta)\ln(\cos^2(\delta)) + \sin^2(\delta)\ln(\sin^2(\delta)). \tag{5}$$

Since the walker initially is fixed at one position their is no inherent randomness associated with position. Thus, randomness associated with initial position space will be 0. This supports the viability of randomness quantification process.

Randomness after *t*- steps.

After t-steps, the generic form of the walker can be written as $|\psi_t\rangle = (\sum_x a_{x,t}| \uparrow \rangle + b_{x,t}| \downarrow \rangle) \otimes |x\rangle$, which is the outcome of the operation $\mathcal{W}(\theta)^t$ on the initial state. Therefore, the density matrix corresponding to the state would be,

$$\rho_t = |\psi_t\rangle\langle\psi_t| = \sum_{x,y}\Big(a_{x.t}a_{y,t}^*| \uparrow \rangle\langle \uparrow | + a_{x,t}b_{y,t}^*| \uparrow \rangle\langle \uparrow | + b_{x,t}a_{y,t}^*| \downarrow \rangle\langle \uparrow | + b_{x,t}b_{y,t}^*| \downarrow \rangle\langle \downarrow |\Big) \otimes |x\rangle\langle y|. \tag{6}$$

Now using this expression we can compute the randomness associated with the position and coin space individually and both together.

Randomness in coin space. The walker has two internal degrees of freedom and total randomness is being distributed in the form of probability amplitude associated with the $| \uparrow \rangle$ and $| \downarrow \rangle$ states. By tracing out the position space, we will be remained with the reduced density matrix denoted by ρ_{in}^c expressed in the form, $\rho_t^c = \rho_{11}| \uparrow \rangle\langle \uparrow | + \rho_{12}| \uparrow \rangle\langle \downarrow | + \rho_{21}| \downarrow \rangle\langle \uparrow | + \rho_{22}| \downarrow \rangle\langle \downarrow |$. So, the randomness can be expressed as

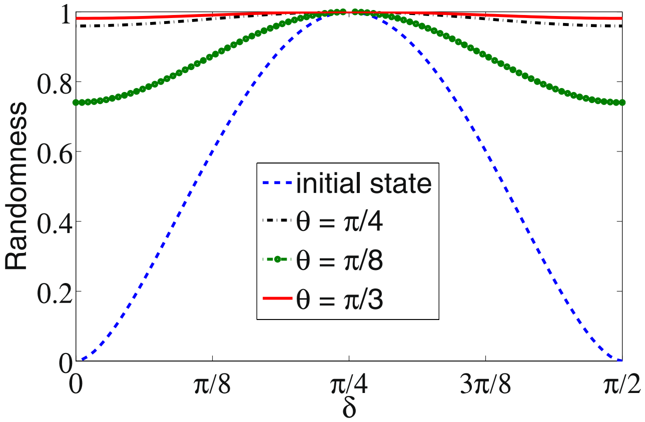

Figure 1. Intrinsic randomness in the coin space (particle) as a function of initial state parameter δ before implementing quantum walk and after implementing 50 step of quantum walk using difference coin operation parameter θ. Though we see some dependency on δ, a significant enhancement of randomness is seen even when the randomness in the initial state is zero.

$$R_i(\rho_t^c) = -\,(\rho_{11}\ln\rho_{11} + \rho_{22}\ln\rho_{22}) = \sum_x |a_{x,t}|^2\ln|a_{x,t}|^2 + |b_{x,t}|^2\ln|b_{x,t}|^2. \tag{7}$$

In Fig. 1 we show the randomness in the coin space as function of δ which fixes the initial state before the walk and after 50 step of walk using different coin operation parameter θ. Irrespective of the initial state, that is, even when initial state's randomness is zero, we can see an high value of randomness after 50 steps of DTQW. From the analytical results presented in the "Supplementary Information" and the numerical results we can say that the same behaviour will be seen even after small number of steps.

Randomness in position space. We can use the randomness of the state extended in superposition of position space to extract intrinsically random classical bit string out of it. Extraction process is discussed in *extracting randomness* section following this. For quantification of randomness in position space we will follow the same recipe as we used in quantifying randomness in coin space. If the dynamics of the walker involves t number of steps of walk then we know that generic state can be written as $\psi_t = \sum_x (a_{x,t}|\uparrow\rangle + b_{x,t}|\downarrow\rangle) \otimes |x\rangle$, and $\rho_t = |\psi_t\rangle\langle\psi_t|$. By tracing out the coin space we will get the form as $\rho_t^p = \sum_{i,i'} \rho_{i,i'}|i\rangle\langle i'|$. To calculate the randomness inherited by the reduced state, we need the diagonal entries in computational basis that is, $\rho_{i,i}$. The density matrix after time t can be written in the form,

$$\rho_t = |\psi_t\rangle\langle\psi_t| = \sum_{x,y}\Big(a_{x.t}a^*_{y,t}|\uparrow\rangle\langle\uparrow| + a_{x,t}b^*_{y,t}|\uparrow\rangle\langle\downarrow| + b_{x,t}a^*_{y,t}|\downarrow\rangle\langle\uparrow| + b_{x,t}b^*_{y,t}|\downarrow\rangle\langle\downarrow|\Big) \otimes |x\rangle\langle y| \tag{8}$$

therefore,

$$\rho_t^p = \sum_{x,y=-t}^{t} (a_{x,t}a^*_{y,t} + b_{x,t}b^*_{y,t}) \otimes |x\rangle\langle y|. \tag{9}$$

Comparing the two expression for ρ_t^p we can write down the form of the randomness as

$$R_i(\rho_t^p) = \sum_x \Big(|a_{x,t}|^2 + |b_{x,t}|^2\Big)\ln\Big(|a_{x,t}|^2 + |b_{x,t}|^2\Big). \tag{10}$$

In Fig. 2, randomness in position space after 25 step of quantum walk as a function of initial state parameter δ is shown. Before the walk, randomness in position space is zero therefore, what we note after 25 steps of walk is a significant quantity of randomness in the system even though it varies a bit as function of δ and for different value of θ. In the inset of Fig. 2, randomness in complete system, coin and position space together is shown. We see an overall boost in the randomness when compared to randomness in position space alone.

Extracting randomness.

The working principle of a QRNG is to make use of the quantum phenomena such as superposition of quantum states and measurement to obtain classical output string which is desirable to be random enough to pass any statistical tests. It is known before measuring that, a two-level system can acquire random classical bit string from the random outcome of the measurement. We will see how a qubit quantum walk can generate single random bit and a multi-random bit string and its advantages over using a single copy of qubit system.

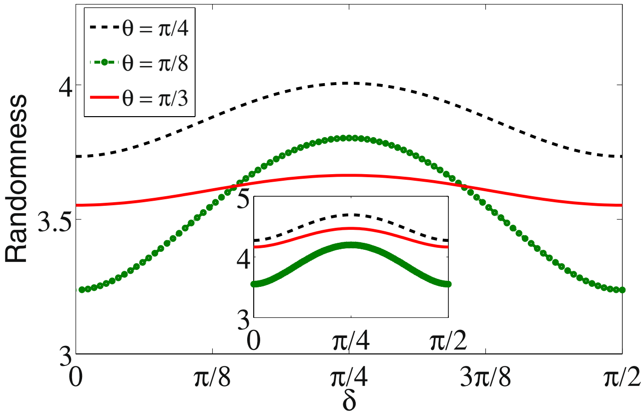

Figure 2. Intrinsic randomness in position space as a function of initial state parameter δ after 25 step of walk using different coin operation parameter θ. It is evident from the figure that randomness shows some dependency on the initial state, however, the variation is very small when compared to the zero randomness in the initial stage. Inset in the figure is the randomness when both coin and position space are taken together. We see a unit increase in the randomness when both the space are taken into account.

From coin space. We have already discussed the procedure to quantify randomness in coin space and our analysis shows it's dependence on the initial state of the walker. With evolution of the walk, a clear enhancement of the randomness in comparison to the initial state is seen. That is, after t- steps the particle evolves according to the dynamics and probability amplitude corresponding $|\uparrow\rangle$ and $|\downarrow\rangle$ states will keep changing after each step. To get the random classical bit out of it we have to use a detector to detect the state of the walker after any arbitrary number of steps. Here we will trust both, the device implementing quantum walk and detector to get intrinsically random classical bit. Walker will be in the superposition state $a_{x,t}|\uparrow\rangle + b_{x,t}|\downarrow\rangle$ before the detection and it would collapse on either of these two states after measurement and we will code a classical bit 0 or 1 for detecting $|\uparrow\rangle$ and $|\downarrow\rangle$ state, respectively. Here, the bit commitment is arbitrary and we could use the opposite commitment too. Since quantum mechanics assures us the outcome being inherently random, we cannot have a prior knowledge about the outcome before detection. Therefore, we can expect a perfectly random classical series of string as output by repeating this scheme for several times.

From position space. We will use the same kind of extraction process in the position space as in the coin space. The advantage of using the position space is its ability to generate a multiple-random bit string rather than a single bit after each round of extraction like it is in coin space. More explicitly, after t-steps walk, tracing out the coin space, we can write the generic state in position space in the form $|\psi_t\rangle = \sum_{x=-t}^{t} a_{x,t}|x\rangle$, which is in superposition of all possible states corresponding to each position. To make a measurement we have to place a position resolving detectors (or a multiple - detector at each position) where the particle will be detected. If we use the standard version of DTQW then,

$$|\psi_t\rangle = a_{t,t}|t\rangle + a_{t-2,t}|t-2\rangle + a_{t-4,t}|t-4\rangle + \cdots + a_{-t+2,t}|-t+2\rangle + a_{-t,t}|-t\rangle. \tag{11}$$

We can define the state of the detector using a simple mathematical formula, $2^n = 2t$. If n is an integer then we will use n number of quantum bits to denote the state of the detectors and if n is not an integer then the maximum number of quantum bits needed to specify all detectors is $\{n|\min_{n} 2^n \geq 2t\}$. If $2t = 2^n$ then the detector states will be defined as follows:

Bit commitment scheme with position	
Detected position of walker	Corresponding state
$-t$	$|00\cdots0\rangle$, 0 appears n times
$-t+1$	$|00\cdots1\rangle$, 0 appears $n-1$ times
$\vdots$	$\vdots$
$\vdots$	$\vdots$
$t-1$	$|11\cdots0\rangle$, 1 appears $n-1$ times
‘t	$|11\cdots1\rangle$, 1 appears n times.

Therefore, if the particle is being detected at position t then we will note the n bit string associated with the detector at which it is measured. Below we present a table with an example of bit commitment scheme after 8 step of quantum walk

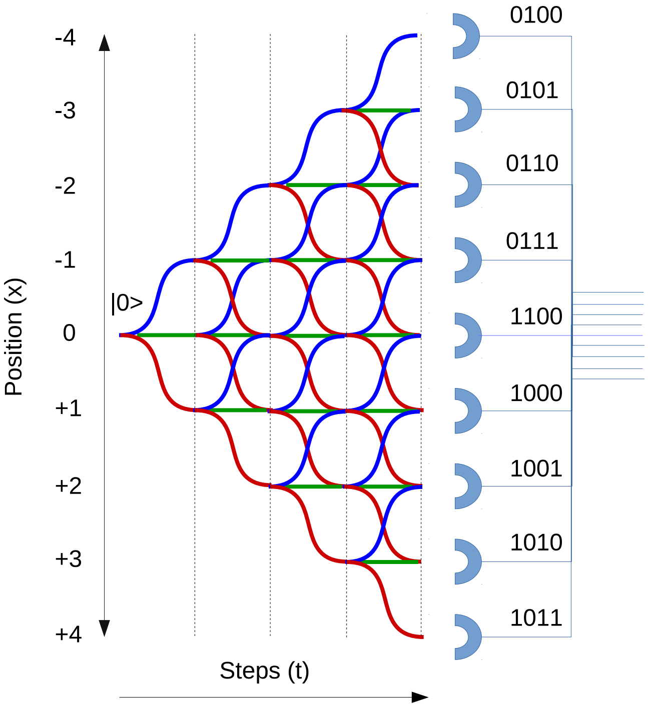

Figure 3. Schematic representation four bit random number generation from a single qubit after four step of SS-QW. If the state of the walker is also considered, we will effectively have five bit random number after measurement.

Bit commitment scheme after 8 step of walk	
Detected position of walker	State of the walker
−8	$\|0000\rangle$
−7	$\|0001\rangle$
−6	$\|0010\rangle$
−5	$\|0011\rangle$
−4	$\|0100\rangle$
−3	$\|0101\rangle$
−2	$\|0110\rangle$
−1	$\|0111\rangle$
1	$\|1000\rangle$
2	$\|1001\rangle$
3	$\|1010\rangle$
4	$\|1011\rangle$
5	$\|1100\rangle$
6	$\|1101\rangle$
7	$\|1110\rangle$
8	$\|1111\rangle$

Here we have not committed any bit string for position 0. However, we can assign a bit 0 or 1 arbitrarily or we can avoid committing a bit string for this or any specific position according to the choice of the client who wants to generate the random number. In DTQW evolution we know that after odd (even) number of steps of walk, positions identified with even (odd) number will have zero probability of finding a particle. This will eliminate the occurrence of half of the configuration of multi-bit random number. To address this concern we can use split-step quantum walk[43,44] or directed quantum walk[45,46].

Split-step quantum walk. In a one-dimensional split-step quantum walk (SS-QW) the shift operator is divided into two parts denoted by S_- and S_+. These operations are defined as

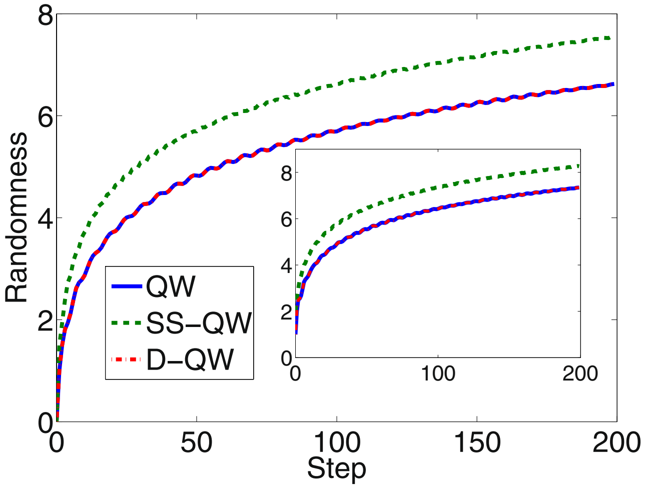

Figure 4. Randomness with number of steps in standard DTQW, SS-QW, and D-QW. Due to non-zero probability at all position space in SS-QW we can see a maximum randomness compared to other two. Amount of randomness measure corresponds to equivalent number of qubit it can mimic in the process. Inset in the figure is the randomness when both coin and position space are taken together.

$$\begin{aligned} S_- &= \sum_x |x-1\rangle\langle x| \otimes |\uparrow\rangle\langle\uparrow| + 1 \otimes |\downarrow\rangle\langle\downarrow|; \\ S_+ &= \sum_x 1 \otimes |\uparrow\rangle\langle\uparrow| + \langle x+1|\langle x| \otimes |\downarrow\rangle\langle\downarrow|. \end{aligned} \tag{12}$$

Unlike standard form of DTQW, here two different coin operators dependent on two different parameters θ_1 and θ_2 are used. Therefore, the resulting operation will be defined as,

$$\mathcal{W}(\theta_1, \theta_2) = [1 \otimes C(\theta_2)]S_-[1 \otimes C(\theta_1)]S_+, \tag{13}$$

where for the coin operator we used the same form as above. After t steps of walk the state will be

$$|\psi_t\rangle = \mathcal{W}(\theta_1, \theta_2)^t |\psi_{in}\rangle \tag{14}$$

and it can be written in the form $|\psi_t\rangle = \sum_{x=-t}^{t} (a_{x,t}|\uparrow\rangle + b_{x,t}|\downarrow\rangle) \otimes |x\rangle$. Here the probability amplitude will be non-zero for each position and state will be of the form,

$$|\psi_t\rangle = a_{t,t}|t\rangle + a_{t-1,t}|t-1\rangle + a_{t-2,t}|t-2\rangle + \cdots + a_{-t+1,t}|-t+1\rangle + a_{-t,t}|-t\rangle. \tag{15}$$

We can calculate the randomness using the pure state density matrix and by tracing out the coin space as we did in standard DTQW case. In Fig. 3 we show the schematic representation of generation of four bit random number after four step of SS-QW.

Directed quantum walk. To define the directed discrete time quantum walk (D-QW) in one dimension, we will be using one directed edge connecting two vertices of the graph and $(n-1)$ self looping edges at each vertex and we will assign a basis vector to each edge. Then every state at each edge can be expressed as linear combination of the states $|x, \rightarrow\rangle$, $|x, 1\rangle$, $|x, 2\rangle \cdots |x, n-1\rangle$ where x is non-negative integer and → indicates edge along the line and each number comes from distinct self loop. The action of shift operation is defined as $S_x|x, \rightarrow\rangle = |x+1, \rightarrow\rangle$ and $S_x|x, i\rangle = |x, i\rangle$, $i \in [1, n-1]$. Therefore, the shift operator takes the form

$$S_x = \sum_{x,i} |\rightarrow\rangle\langle\rightarrow| \otimes |x+1\rangle\langle x| + |i\rangle\langle i| \otimes |x\rangle\langle x|. \tag{16}$$

Coin operation has the form $C \equiv \begin{bmatrix} \alpha & \beta \\ \beta & -\alpha \end{bmatrix}$ where $\alpha = 1/\sqrt{n}$ and $\beta = \sqrt{\frac{n-1}{n}}$. Therefore, one step of D-QW comprises of two operation $\mathcal{W}_d = S_x[C \otimes \ ]$. After t steps of D-QW the state will be $|\psi\rangle_t = \mathcal{W}_d^t|\psi_{in}\rangle$.

$$|\psi_t\rangle = a_{0,t}|0\rangle + a_{1,t}|1\rangle + a_{2,t}|2\rangle + \cdots + a_{t-1,t}|t-1\rangle + a_{t,t}|t\rangle. \tag{17}$$

In Fig. 4, randomness in the system as function of number of steps is shown when measurement are made only in the position space and in both, position and coin space (inset). *The increase in randomness shows the way number of equivalent quantum bit the system mimics using a single qubit*. The plot shows the randomness for all three types of quantum walk evolution. Due to non-zero probability at all position space, the randomness is more (maximizes) for the SS-QW than the randomness obtained for standard DTQW (Fig. 4). In D-QW the number

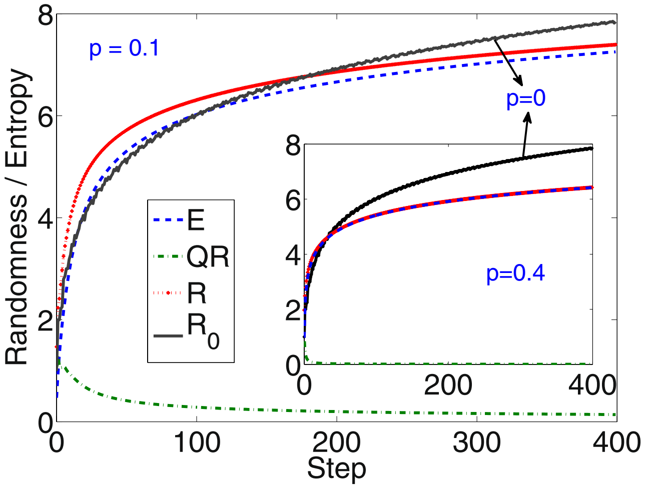

Figure 5. Randomness with number of steps in standard DTQW in presence of bit flip noise in coin space. With increase in noise some decrease in randomness is seen. The randomness in system with noise will have contribution from both, quantum origin as well as noise. To show that we have plotted randomness (R) for noiseless evolution and for evolution with different noise level p. The van Neumann entropy (E) and the randomness of quantum origin is also shown. Though overall randomness does not see a significant decrease, a substantial decrease in randomness from quantum origin is seen.

of positions on which probability amplitude is non-zero is equivalent to number of position space with non-zero probability in standard DTQW, the randomness measure is also identical (Fig. 4). In the inset we have shown the randomness in both, coin and position space together. Inclusion of coin space enhances the randomness in the system by a small amount.

Advantages of using both space. If we take into account both, the coin and position degrees of freedom, we can generate an extra bit compared to the string of bits from position space alone. The reason is very obvious as we have seen already how internal degrees of freedom of the particle is able to generate one classical random bit after a single round of evolution. Therefore, when we use both, we will get random classical bit string coming from both spaces. The extraction process is same as discussed before but the detectors at each possible positions should be capable of capturing the information about internal state of the walker along with detecting the position of the walker.

In this scheme using dynamic evolution of qubit, from a given position space we can generate a uniform length classical multi-bit string rather than a single bit from a standard single particle QRNG. The randomness depends only on the device's trustedness.

Randomness quantification under noise. An important part of any cryptographic protocol is to ensure it's security under many possible attacks. It is in general impossible to make it secure under any arbitrary attacks but we can prove its security considering some realistic cases. One of these cases will be the difficulty to create a perfect pure state as different kind of noises will mix it up resulting a mixed state. Now the concern is that an Eavesdropper can have access of these noises and he or she might be able to get some information about the measurement outcomes using this correlation with the system. This is highly undesirable as we want to use this measurement outcome as random number in other cryptographic protocols. Let us consider the case where instead of starting with pure state some noise is mixed and we will consider a purified state $|\psi^{CPE}\rangle$ which is being shared by the walker and the adversary Eve. This is the state in the larger Hilbert space $\mathcal{H}_{\mathcal{C}} \otimes \mathcal{H}_{\mathcal{P}} \otimes \mathcal{H}_{\mathcal{E}}$ where the walker does not have the access to the Hilbert space $\mathcal{H}_{\mathcal{E}}$. Purification implies that the state of the walker will be $\rho^{CP} = Tr_E(|\psi^{CPE}\rangle\langle\psi^{CPE}|)$. Upon obtaining the outcome e with probability p_e by doing projective measurement on Eve's system, the state of the walker will be $|\psi_e^{CP}\rangle = \langle\psi_e^E|\psi^{CPE}\rangle$. The measurement of randomness corresponding to the walker's state would be $R_i(|\psi_e^{CP}\rangle)$ and the total randomness can be quantified as $\sum_e p_e R_i(|\psi_e^{CP}\rangle)$. Now Eve's optimal strategy would be to choose a measurement basis which will maximize her side information about the measurement outcome, equivalently saying minimizing the randomness of the walker's measurement outcome. Therefore, the total randomness can be quantified as

$$R_i(\rho^{CP}) = \sum_{min(p_e, \psi_e^E)} p_e R_i(|\psi_e^{CP}\rangle). \tag{18}$$

An other description of effect noise on the randomness in the system will be in the form of decoherence in DTQW evolution. A simple form of introducing decoherence into DTQW evolution will be in the form of bit flip noise, that is, $\rho(t)$ of the complete system as outlined in Eq. (6) after every time step t will be in the form $\rho(t) = p[(\sigma_x \otimes 1)\rho(t)(\sigma_x \otimes 1)^{\dagger}] + (1 - p)\rho(t)$. Here p is the noise level and σ_x is bit flip operation. This bit flip noise results in decrease in spread of the wavepacket in position and correspondingly the randomness in the system also decreases. However, when we calculate the randomness after such evolution we will have contribution from both, quantumness in the system and from the noise process. Therefore, while using DTQW with noise, all the randomness we obtain cannot be attributed to the quantum origin. To give a quantitative picture of the randomness of quantum origin in DTQW system, in Fig. 5 we present a plot of extractable randomness in complete DTQW system with noise of different level and the randomness of quantum origin for the corresponding noise level.

When their is no noise in the dynamics ($p=0$, R_0) we see a study increase in randomness with number in steps and all the randomness can be attributed to the quantum origin. With increase in noise level ($p=0.1$ and $p=0.4$, R) we first seen a steep increase in randomness and with time it will be lower than the randomness of quantum origin when $p=0$. For non-zero p we have show the value of von Neumann entropy, $E(t)=-tr[\rho(t) \ln (\rho(t)]$, a good measure of randomness due to noise in the system. Therefore, the contribution of randomness of quantum origin can be quantified in the form $QR(t)=R(t)-E(t)$. This value becomes very small with increase in p and time t and for $p=0.4$ its almost zero. We should note that this method of evaluating randomness of quantum origin is valid only for the system with $\rho(t)$ is a pure state when their is no noise (that is, when $E(t)=0$ for $p=0$). However, though contribution of randomness from quantum origin decrease with in increase in noise level, the overall randomness of the system will continue to scale the same way as the spread of the DTQW scales with noise.

Randomness as guessing probability. Out of many possible attacks one can consider is the fact that the detectors are correlated with an adversary's system. Upon obtaining a specific outcome, the state of the adversary would be changed accordingly and measuring the correlated system in her lab, Eve can get some useful information about the outcome of the QRNG. However, considering our case, the detectors are placed at every possible positions where the particle can be detected and corresponding state can be written as i where i is a $n-$ bit string as we suggested in the extraction procedure.

If the probability distribution of the random variable (measurement outcome) being denoted by P_I then consider an adversary whose states ρ_i^E depends on the random variable I which corresponds to the Classical-Quantum state $\rho_{PE}:=\sum_{i\in I} P_I(i)|i\rangle\langle i|\otimes\rho_{E}^{i}$. If $P(I|E)=\sum_{i\in I} P_I(i)Tr(\pi_i\rho_i^E)$ (π_i is the POVM on Eve's system), it is the probability of guessing the outcome of position measurement using the optimal measurement strategy by the adversary. For this it has been proved[47] that $P(I|E)$ is related to the $min-$ entropy by the relation $P(I|E)=2^{-H_{min}(I|E)}$ where the $min-$ entropy is defined by $H_{min}(I|E):=-\inf_{\sigma_E}D_\infty(\rho_{PE}\|_P\otimes\sigma_E)$ and $D_\infty(\rho|\sigma):=\inf\{\lambda\in\mathbb{R}: \rho\leq 2^\lambda\sigma\}$.

Methods

Randomness quantification. The intrinsic randomness of a quantum system is related to the random outcomes of the measurement on the system[42]. If we measure a pure state $\rho=|\psi\rangle\langle\psi|$, (where $|\psi\rangle=\sum_i a_i|i\rangle$) in the basis $|i\rangle$ considering projective measurement, then measurement outcomes are intrinsically random.

According to Born's rule $p_i=Tr[P_i\rho]=\langle i|\rho|i\rangle=\langle i|\sum_{j,k}a_ja_k|j\rangle\langle k||i\rangle=|a_i|^2$ will be the probability of obtaining the i'th outcome. P_i are the rank one projectors on the basis states. Then randomness of the output random variable is defined as

$$R_i(\rho=|\psi\rangle\langle\psi|)=-\sum_i p_i \ln p_i .$$

Which is the Shannon entropy function of the probability distribution $\{p_i\}$. In another way it can be written as $R_i(\rho=|\psi\rangle\langle\psi|)=S(\rho^{diag})$, where ρ^{diag} is the density matrix that has only diagonal terms of ρ in the computational basis $\{i\}$. If we think ρ as a $n\times n$ matrix, having only diagonal terms ρ_{ii} in the computational basis then the randomness inherited by state ρ can be quantified as

$$R_i(\rho)=-\sum_{i=1}^{n}\rho_{ii}\ln\rho_{ii}. \tag{19}$$

From the preceding expression we can note that the information of diagonal elements which corresponds to probability distribution of each of the two basis state quantum walk in position space is sufficient to obtain the randomness in the system. Therefore, an analytical expression for $a_{x,t}$ and $b_{x,t}$, amplitudes of the basis state $|\uparrow\rangle$ and $|\downarrow\rangle$ at position x and time t for noiseless and decoherent quantum walk can be obtained from the Fourier analysis of the walk as described in refs. [48,49]. respectively. Using the first and the second moments, analytical expression for the asymptotic behaviour has also been presented in the same references.

Discussion and Conclusion

Many of the existing protocols for Quantum Random Number Generator (QRNG) are based on quantum state preparation and measurement schemes. We introduce here a QRNG based on quantum dynamics which can be controlled rather than the "prepare and measure" methods. In addition to that, our paper includes the following important results and advantages to develop a QRNG protocol using quantum walk.

For Discrete Time Quantum Walk (DTQW), the quantification process for the randomness inherited by the state (for both, pure and mixed) has been prescribed.

After implementing the DTQW, we have analysed the dependency of the quantified intrinsic randomness on the initial state parameter δ and walk evolution parameter θ. We have provided the analytical calculation (see Appendix) for short time and numerical results for long time evolution to prove the fact that in both, position and coin space, the randomness is almost independent of the walk evolution parameter θ. Though the randomness in position space shows some dependence on the initial state parameter δ, the degree of dependence is very small compared to the initial state randomness, which is being calculated as zero. A significant enhancement of randomness with the increase in number of steps of DTQW is an other important thing that has been highlighted.

We have suggested a scheme to extract random number both, from measurement on coin space and position space outcomes individually and together. Our extraction scheme shows the use of single particle and incorporating position degrees of freedom with it to generate a bit string of random number after measurement. We have also established that the long bit string out of single run of the single particle system can be obtained by increasing the dimension of position Hilbert space. This clearly implies that the bit-rate can be made higher depending on the position space dimension we can control under current technologies. Many earlier results have demonstrated ways to control probability distribution of the DTQW[50–56]. Therefore, the probability distribution of the walk can be engineered to get a uniform probability distribution which is desired in any cryptographic protocols or any other distribution. This helps us to design a QRNG protocol which is capable enough to give us the random numbers from a desired probability distribution and any undesired nature will directly indicate the presence of adversary or hardware failure.

The main idea of our work was to construct a protocol for generating multiple random bits using quantum walk of a single particle. Recent experimental demonstration of using position degree of freedom along with polarization and orbital angular momentum degree of freedom, a muti-qubit entangled state has been reported[57]. Therefore, realization of multi qubit state using extended position space is not far from experimental feasibility. We have also shown the advantages of using SS-QW over D-QW or standard DTQW in extracting higher randomness with all possible combination of multi-bit string. This behaviour is expected because for the SS-QW where the degrees of freedom in position space with non-zero probability is double. In comparison with other two, the probability amplitude at all the possible positions using SS-QW effectively contribute to the expression of randomness.

Now the question can arise about the probability distribution of the position space, where uniformity of the distribution is desired for the security purpose. Controlled distribution of quantum walk can in general be engineered to pick the desired distribution using position dependent coin operations and along with phase operations. Recently, an experimental demonstration of engineering any arbitrary state by controlled dynamics generated by quantum walk has been reported[56]. This strongly supports feasibility of our scheme where a desired probability distribution will act as an additional resource. However, a crucial point of our QRNG scheme is that, we use the inherent randomness of the quantum dynamics which is completely controlled under the person or organization who wants to produce random bits for any further cryptographic application.

QRNG based on state preparation and measurement scheme where state can be manipulated in such a way that the observer of the random sequence of bits can think of it as a perfectly random whereas the output can be completely predictable to the adversary who is sending the states. In our scheme we have shown how the randomness is almost independent of the initial state after few steps of quantum walk and since dynamics involves quantum interference, the output is random enough to produce random bits string in a secure lab where he/she has the full control of the quantum walk dynamics. The only issue with the hardware failure or malfunctioning, such that dynamics can be highly localized i.e the probability distribution of finding particle within some specific range of positions is really high therefore there might be some chances that it can be predicted but we have been able to produce a solution for that by using an engineered state and dynamics which are capable of producing the uniform or any desired probability distribution, non-occurrence of this desired probability distribution can signal the hardware malfunction therefore the person or organization are ready to rectify it or completely abandon the protocol.

Noise on quantum walk affects the spread of the wavepacket in position space that will proportionally decrease the randomness in the systems. As shown in our results, though a overall randomness does not significantly decrease with noise, contribution of randomness from quantum origin does see a substantial decrease. This goes well with an established understanding to decrease in entanglement between the coin and position space of the quantum walker with increase in noise.

Data Availability

All data generated or analyzed during this study are included in this article itself.

References

1. Rubinstein, R Y. & Kroese, D P. Simulation and the Monte Carlo method. *John Wiley and Sons*. **10** (2016).
2. Metropolis, N. & Ulam, S. The monte carlo method. *Journal of the American Statistical Association* **44**, 247 (1949).
3. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145–195 (2002).
4. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661–663 (1991).
5. Bennett, C. H., Bessette, F., Brassard, G., Salvail, L. & Smolin, J. Experimental quantum cryptography. *Journal of Cryptology* **5**, 3–28 (1992).
6. Rukhin, A., Soto, J., Nechvatal, J., Smid, M. & Barker, E. A statistical test suite for random and pseudorandom number generators for cryptographic applications. *Booz-Allen and Hamilton Inc Mclean Va* (2001).
7. Maurer, U. M. A universal statistical test for random bit generators. *Journal of Cryptology* **5**, 89–105 (1992).
8. Soto, J. Statistical testing of random number generators. *Proceedings of the 22nd National Information Systems Security Conference* **10** (2004).
9. Born, M. Statistical interpretation of quantum mechanics. *Science* **122**, 675–679 (1955).
10. Bera, M. N., Acín, A., Kuś, M., Mitchell, M. W. & Lewenstein, M. *Reports on Progress in Physics* **80**, 124001 (2017).
11. Einstein, A., Podolsky, B. & Rosen, N. Can quantummechanical description of physical reality be considered complete? *Phys. Rev.* **47**, 777–780 (1935).
12. Bell, J. S. Speakable and unspeakable in quantum mechanics: Collected papers on quantum philosophy. *Cambridge university press* (2004).
13. Acín, A. & Masanes, L. Certified randomness in quantum physics. *Nature* **540**, 213–219 (2016).
14. Masanes, L., Acín, A. & Gisin, N. General properties of nonsignaling theories. *Phys. Rev. A* **73**, 012112 (2006).
15. Barrett, J., Hardy, L. & Kent, A. No signaling and quantum key distribution. *Phys. Rev. Lett.* **95**, 010503 (2011).
16. Pironio, S. *et al*. Random numbers certified by Bells theorem. *Nature* **464**, 1021–1024 (2010).
17. Ma, X. *et al*. Quantum random number generation. *npj Quantum Information* **2**, 16021 (2016).

18. Colbeck, R. & Kent, A. Private randomness expansion with untrusted devices. *Journal of Physics A: Mathematical and Theoretical* **44**(9), 095305 (2011).
19. Coudron, M. & Henry Y. Infinite randomness expansion with a constant number of devices *Proceedings of the forty-sixth annual ACM symposium on Theory of computing* 427–436 (2014).
20. Colbeck, R. Quantum and relativistic protocols for secure multi-party computation. Ph.D Thesis (2009).
21. Colbeck, R. & Renner, R. Free randomness can be amplified. *Nature Physics* **8**, 450–453 (2012).
22. Acin, A., Gisin, N. & Lluis., M. From Bells theorem to secure quantum key distribution. *Phys. Rev. Lett.* **97**, 120405 (2006).
23. Pironio, S. *et al.* Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics* **11**, 045021 (2009).
24. Horodecki, R., Horodecki, P., Horodecki, M. & Horodecki, K. Quantum entanglement. *Rev. Mod. Phys.* **81**(2), 865 (2009).
25. Brunner, N. *et al.* Bell nonlocality. *Rev.Mod. Phys.* **86**(2), 419 (2014).
26. Ryan, C. A., Laforest, M., Boileau, J. & Laamme, R. Experimental implementation of a discrete-time quantum random walk on an NMR quantum-information processor. *Phys. Rev. A* **72**(6), 062317 (2005).
27. Schmitz, H. *et al.* Quantum walk of a trapped ion in phase space. *Phys. Rev. Lett.* **103**(9), 090504 (2009).
28. Zähringer, F. *et al.* Realization of a quantum walk with one and two trapped ions. *Phys. Rev. Lett.* **104**(10), 100503 (2010).
29. Karski, M. *et al.* Quantum walk in position space with single optically trapped atoms. *Science* **325**, 174–177 (2009).
30. Peruzzo, A. *et al.* Quantum walks of correlated photons. *Science* **329**, 1500–1503 (2010).
31. Schreiber, A. *et al.* Photons walking the line: a quantum walk with adjustable coin operations. *Phys. Rev. Lett.* **104**(5), 050502 (2010).
32. Perets, H. B. *et al.* Realization of quantum walks with negligible decoherence in waveguide lattices. *Phys. Rev. Lett.* **100**(17), 170506 (2008).
33. Broome, M. A. *et al.* Discrete single-photon quantum walks with tunable decoherence. *Phys. Rev. Lett.* **104**(15), 153602 (2010).
34. Venegas-Andraca, S. E. Quantum walks: a comprehensive review. *Quantum Information Processing* **11**(5), 1015–1106 (2012).
35. Feynman, R. Quantum mechanical computers. *Foundations of Physics* **16**(6), 507–531 (1986).
36. Riazanov, G. V. The Feynman path integral for the Dirac equation. *Soviet Journal of Experimental and Theoretical Physics* **6**, 1107 (1958).
37. Meyer, D. A. From quantum cellular automata to quantum lattice gases. *Journal of Statistical Physics* **85**, 551–574 (1996).
38. Aharonov, Y., Davidovich, L. & Zagury, N. Quantum random walks. *Phys. Rev. A* **48**(2), 1687 (1993).
39. Chandrashekar, C. M. Disordered-quantum-walkinduced localization of a Bose-Einstein condensate. *Phys. Rev. A* **83**(2), 022320 (2011).
40. Chandrashekar, C. M. Disorder induced localization and enhancement of entanglement in one-and twodimensional quantum walks. *arXiv:1212.5984* (2012).
41. Singh, S. & Chandrashekar, C. M. Interference in localized quantum walk. *arXiv:1711.06217* (2017).
42. Yuan, X., Zhou, H., Cao, Z. & Ma, X. Intrinsic randomness as a measure of quantum coherence. *Phys. Rev. A* **92**(2), 022124 (2015).
43. Kitagawa, T., Rudner, M. S., Erez, B. & Demler, E. Exploring topological phases with quantum walks. *Phys. Rev. A* **82**(3), 033429 (2010).
44. Mallick, A. & Chandrashekar, C. M. Dirac cellular automaton from split-step quantum walk. *Scientific Reports* **6**, 25779 (2016).
45. Hoyer, S. & Meyer, D. A. Faster transport with a directed quantum walk. *Phys. Rev. A* **79**(2), 024307 (2009).
46. Chandrashekar, C. M. & Busch, T. Quantum percolation and transition point of a directed discrete-time quantum walk. *Scientific Reports* **4**, 6583 (2014).
47. Konig, R., Renner, R. & Schaffner, C. The operational meaning of min-and max-entropy. *IEEE Transactions on Information theory* **55**, 4337–4347 (2009).
48. Nayak, A. & Vishwanath, A. Quantum walk on the line. *DIMACS Technical Report*, 2000–43 (2001).
49. Brun, T. A., Carteret, H. A. & Ambainis, A. Quantum random walks with decoherent coins. *Phys. Rev. A* **67**, 032304 (2003).
50. Tregenna, B., Flanagan, W., Maile, R. & Kendon, V. Controlling discrete quantum walks: coins and initial states. *New J. Phys.* **5**, 83 (2003).
51. Panahiyan, S. & Fritzsche, S. Controlling quantum random walk with a step-dependent coin. *New J. Phys.* **20**, 083028 (2018).
52. Ambarish, C. V. *et al.* Dynamics and energy spectra of aperiodic discrete-time quantum walks. *Phys. Rev. E* **96**, 012111 (2017).
53. Kumar, N. P., Balu, R., Laamme, R. & Chandrashekar, C. M. Bounds on the dynamics and entanglement in a periodic quantum walks. *Phys. Rev. A* **97**, 012116 (2018).
54. Chandrashekar, C. M., Srikanth, R. & Laamme, R. Optimizing the discrete time quantum walk using a SU(2) coin. *Phys. Rev. A* **77**, 032326 (2008).
55. Singh, S., Balu, R., Laamme, R. & Chandrashekar, C. M. Accelerated quantum walk,two particle entanglement generation and localization. *Journal of Physics Communications* **3**(5), 055008 (2019).
56. Giordani, T. *et al.* Experimental Engineering of Arbitrary Qudit States with Discrete-Time Quantum Walks. *Phys. Rev. Lett.* **122**, 020503 (2019).
57. Wang, X. *et al.* 18-Qubit Entanglement with Six Photons Three Degrees of Freedom. *Phys. Rev. Lett.* **120**, 260502 (2018).

Acknowledgements

C.M.C. would like to thank Department of Science and Technology, Government of India for the Ramanujan Fellowship Grant No.: SB/S2/RJN-192/2014. C.M.C. and Anumpam Sarkar would like to thank Shivani Singh and R. Srikanth for useful discussions.

Author Contributions

C.M.C. designed the study, carried out numerical analysis and prepared the figures. A.S. and C.M.C. together carried out analytical derivation and wrote the manuscript.

Additional Information

Supplementary information accompanies this paper at https://doi.org/10.1038/s41598-019-48844-4.

Competing Interests: The authors declare no competing interests.

Publisher's note: Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.