communications physics

ARTICLE

https://doi.org/10.1038/s42005-022-00915-1 OPEN

Secure random number generation from parity symmetric radiations

Toyohiro Tsurumaru[1], Toshihiko Sasaki[2✉] & Izumi Tsutsui[3]

The random number generators (RNGs) are an indispensable tool for information security. Among various approaches, the radioactive decay has been considered as a promising candidate of RNGs for over half a century, on account of its seemingly unpredictable decay timings as quantum phenomena. However, the security of these radioactive RNGs has not been proven so far. Here we prove the security by a change of tactics, that is, by rewriting decay timings into decay directions, which allows us to ensure the secrecy with the help of the parity invariance deeply rooted in the fundamental law of nature. Our result demonstrates that the foundational properties of particle physics, such as the symmetry of interactions, can be used as a firm basis for the RNGs.

[1] Mitsubishi Electric Corporation, Information Technology R&D Center, 5-1-1 Ofuna, Kamakura-shi, Kanagawa 247-8501, Japan. [2] Department of Applied Physics, Graduate School of Engineering, The University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo 113-8656, Japan. [3] High Energy Accelerator Research Organization (KEK), 1-1 Oho, Tsukuba, Ibaraki 305-0801, Japan. ✉email: sasaki@qi.t.u-tokyo.ac.jp

In information technology, random number generators (RNGs) refer in general to devices that output numbers distributed in a certain range uniformly. If one wishes to use them for information security purposes in particular, their outputs must be secret[1] as well. If, in addition, the RNG is to be usable by anyone, these two properties need to be guaranteed by some objective evidence.

Suppose, for instance, that one buys a dice from a not-necessarily-reliable vendor and throws it alone in a closed room. For this process to generate a uniform distribution, one must be sure with evidence that the dice is fair. As for the secrecy, separate evidence is needed to ensure that the outputs are unpredictable and unknown to outside, even to the vendor or the manufacturer who had all the chances to tamper with the dice such that the outputs follow a certain pattern. But how can one find an objective basis of secrecy that anyone can agree with? Arguably, the most convincing basis of secrecy would be the laws of nature, that is, if nature assures the secrecy by law, then nothing can be utilized to predict the outputs. In this respect, the laws underlying quantum phenomena look promising for providing a secure RNG for which the output is rigorously proven to be secret.

The notion of secure RNG based on the laws of quantum mechanics is not new[2–16]. In fact, RNGs using photons have been studied intensively over the years, and some of them have now been strictly proven to be secure. For example, we have the single photon RNG which employs two complementary bases $+, \times$ of the polarization. Here, the legitimate user (henceforth, Alice) generates a single photon state possessing a polarization in one basis, say, the vertical polarization state $|\updownarrow\rangle$ belonging to basis $+$, and then measures it in the other, diagonally slanted $\times$ basis. Alice adopts the measurement result as the random bits.

The major concern here is that the vendor of the light source may be an eavesdropper (henceforth, Eve). In that event, Eve could have tampered with the source to retain correlation with her own device, and may have access to the random bits as a result.

The security against such an eavesdropper can still be argued as follows. Being a pure state, the initial state $|\updownarrow\rangle$ cannot be entangled with any state on the outside, and hence has no correlation with Eve's device. When the state is measured in the complementary basis $\times$, each measurement result, $\searrow$ or $\nearrow$, occurs with probability one half exactly. Thus the random bits are distributed uniformly, and they are uncorrelated with Eve. Unfortunately, the single photon RNGs have a practical drawback because the energy of the photon used in a typical device is minute and, accordingly, the detector must be highly sensitive. For this reason, the single photon RNGs are subject to constraints for reduction both in their size and cost.

Besides the single photon RNGs, there exists another type of RNG methods which also exploit quantum phenomena, that is, those using radiations from nuclear decays[17–22]. In these radioactive RNG methods one detects radiations and adopts the timings of the detections as random numbers. These methods, proposed prior to the single photon RNGs[17], have the advantage that their device, which can be as small and simple as that of a single photon RNGs, requires no power supply[22–25] for its (radioactive) source. Radioactive RNG chips of a few square millimeters have already been manufactured using ^{241}Am[26–28].

However, there is no rigorous security proof for the radioactive RNGs so far, despite that it has been known for more than half a century that they generate a uniform distribution[19]. The basic reason for this dissatisfying situation is that the decay-timing properties, which are essential for the security proof, are difficult to obtain in a precise manner with the phenomenological models such as Gamow's theory[29,30] for nuclear decays, where adjustable parameters are introduced to describe the exponential decays pertinent to various transitions realized physically.

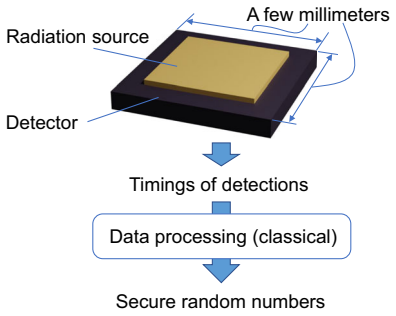

Fig. 1 Device setups for the radioactive random number generator (RNG). The setup consists of a chip-based detector covered by a surface layer including radioactive particles. Its typical size is a few millimeters.

Here we show, nevertheless, that the radioactive RNG can admit a rigorous security proof from the standpoint of the universally composable security[31], provided that the radioactive decay is parity symmetric, *i.e.*, invariant under space inversion. In fact, such cases are available generically for a nuclide (such as ^{241}Am) that exhibits alpha decays caused by the parity-conserving strong interaction. The device structure we assume is as simple as before, consisting only of a radiation source with one or two detector(s) allowing for the parity symmetry to ensure the required security.

Results

RNG method. We consider the following type of the radioactive RNG method. By using a device consisting of a radiation source and a detector D (Fig. 1), Alice executes the following procedure (Fig. 2): Alice chooses integer parameters $n_{\rm fin}$, $n_{\rm thr}$, and N satisfying $0 < n_{\rm fin} \le n_{\rm thr} \le N$. She also selects a function f_s randomly from a predetermined set of functions $\mathcal{F} = \{f_s\}$, each of which outputs an $n_{\rm fin}$ bit string (for example, $\mathcal{F}$ is a universal$_2$ function family[32]; also see Methods). Then, our radioactive RNG is implemented in two steps:

(i) Measurement of decay timings: Alice measures radiations from the source, using detector D, in time bins $i = 1, \ldots, N$. She then records the measurement result as the list of time bins where a detection occurred; *i.e.* as $\mathbf{i} = (i_1, \ldots, i_{n_{\rm det}})$, with $n_{\rm det}$ being the number of detections, and i_j being in the increasing order, $1 \le i_1 < i_2 < \cdots < i_{n_{\rm det}} \le N$. Alice aborts if $n_{\rm det} < n_{\rm thr}$.

(ii) Randomness extraction: Alice calculates the final bits $\mathbf{r} = f_s(\mathbf{i})$ of length $n_{\rm fin}$.

The purpose of each step is as follows (Fig. 2). Step (i) generates raw data $\mathbf{i}$ to be used as the source of the final bits $\mathbf{r}$. For $\mathbf{r}$ to be secure, not all, but a certain fraction of $\mathbf{i}$ need to be unknown to Eve. The standard theoretical results say that the size of this unknown fraction equals a quantity called the smooth conditional min-entropy $H^{\delta}_{\rm min}(\mathbf{I}|E)$, which is a function of the joint state $\rho_{\mathbf{I}E}$ of variable $\mathbf{i}$ and Eve (see Methods for the rigorous definitions).

In step (ii) she extracts these $H^{\delta}_{\rm min}(\mathbf{I}|E)$ bits that are unknown, and generate $\mathbf{r}$, which is completely unknown to Eve.

We denote the width of one time bin by Δt. In order to simplify later presentations, without loss of generality, we assume that in every time bin, Alice starts her measurement at the beginning of the time bin and finishes it in a finite time $\le \Delta t$.

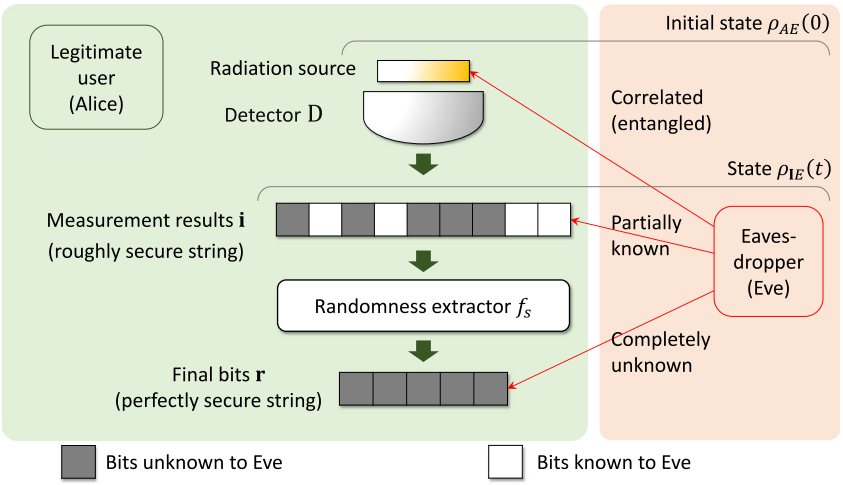

Fig. 2 Procedure of randomness extraction. The purpose of randomness extraction is to extract from a measurement result **i**, which may be partially known to Eve, random bits **r** completely unknown to Eve. In the above picture, **i** being partially known to Eve is expressed by its being a mixture of black (unknown) and white (known) elements. The number of unknown bits equals the smooth conditional min-entropy $H_{\min}^{\delta}(\mathbf{I}|E)$, a function of $\rho_{\mathbf{I}E}$.

Conditions on the device. Hence the security analysis is reduced to lower bounding $H_{\min}^{\delta}(\mathbf{I}|E)$. We are concerned with the possibility that the radiation source to be measured in step (i) may be entangled with Eve, and through that entanglement Eve may access **i**; *i.e.*, $H_{\min}^{\delta}(\mathbf{I}|E)$ may become too small to guarantee the security of **r**. The goal of this paper is to nullify such eavesdropping strategy by making use of the parity symmetry.

To this end, we assume the following three conditions on the device. The first two of them, (A) and (B), in particular, are introduced in order to realize the parity symmetry in the device.

(A) Radiation source: At the beginning of each time bin (*i.e.*, immediately before Alice's measurement), the state of radiations is parity invariant.
(B) Detector: Detector D is housed within one hemisphere around the source.
(C) Effect on radiations by measurements: Effect on radiations in the vicinity of D, caused by Alice's measurement of a time bin i, is washed away by the beginning of the next time bin $i+1$.

In addition, we introduce the following notions for later convenience.

(D) Detections, 'double' events and dark counts: Except with probability δ, there are at most n_{double}'double' events, and at most n_{dark} time bins where dark counts occur. Here the 'double' events are defined as follows: Suppose that, in addition to the actual detector D, there is another detector D′ that constitutes a parity symmetric configuration together with D. Then 'double' events are those for which detector D and D′ both detect the signal.

Note that the number n_{double} of these events can be bounded from above by that of multi-particle events, n_{multi}. Therefore, one does not actually implement the extra detector D′, if n_{multi} is known.

The statements of condition (A) and (D) require some explanation, which we give now. In regards to condition (A), there are four types of fundamental interactions (electromagnetic, weak, strong, and gravitational interactions). Since α-decay and γ-decay are caused, respectively, by the strong interaction and the electromagnetic interaction, and not by the weak interaction, its radiation is parity (space inversion) invariant. This provides us with an ideal basis for supporting the randomness we hoped for, as it is ensured by a symmetry principle afforded by the fundamental particle interactions. Let $\mathcal{H}_A$ be the Hilbert space describing radiated particles in the vicinity of detector D. Also, let $\mathcal{H}_E$ be that describing all degrees of freedom of Eve (cf. Fig. 2). We assume that in $\mathcal{H}_A$ the parity operator P_A is well defined and satisfies $P_A^2 = 1$. (Throughout the paper, we use the convention of omitting the identity operators included in a tensor product; hence *e.g.*, P_A is an abbreviation of $P_A \otimes 1_E$.) Under this setup, we say that the joint state $\rho_{AE}(t)$ of $\mathcal{H}_A$ and $\mathcal{H}_E$ at time t is parity invariant, if it satisfies

$$P_A \rho_{AE}(t) P_A = \rho_{AE}(t). \tag{1}$$

Condition (A) says that the parity invariance (1) holds at the beginning of each time bin, *i.e.* at $t = 0, \Delta t, \ldots, (N-1)\Delta t$.

Next we discuss the feasibility of each of the conditions given above.

First, condition (A) is widely believed to be true for a nuclide which decays by parity-conserving interactions (*e.g.*, strong and electromagnetic interactions, as in the α- and the γ-decays)[33]. It has been well-tested through the measurement of the energy spectrum and the angular distribution of the decay with the comparison to the phenomenological model[29,30].

However, as we deal here with an RNG, we must be aware of a possible scenario where such a choice may not be sufficient for guaranteeing condition (A). For instance, the nuclide could have been tampered with by Eve, before purchased by Alice, to the extent of destroying the parity invariance. We point out that, even in that event, Alice can still verify condition (A) by performing a random sampling test on the source, that is, she measures the radiation from the source and checks if the results, such as the energy spectrum and the angular distribution, are always consistent with condition (A). As far as the nuclei remain to be in the quantum domain and described by the standard nuclear theory, this is enough for ensuring condition (A). One may, however, go beyond and wonder if Eve could generate the seemingly parity invariant measurement results with a deterministic source supplied by some classical means. Although highly inconceivable given the fact that nuclear decay is intrinsically quantum and does not allow any classical intervention, this possibility will still be disposed of by examining the parity eigenvalue of the radiation state, *i.e.*, if it has a definite parity, either 'even' or 'odd', under the operation P_A. This is analogous to

the tomography performed when we examine whether the source emitting polarized photons $\nwarrow$ and $\nearrow$ with equal probability is operated deterministically or not. In that case, finding the state to be in a definite polarization, either $\updownarrow$ or $\leftrightarrow$, ensures that the source is a superposition of $\nwarrow$ and $\nearrow$, and this corresponds to finding the radiation to be in either 'even' or 'odd' state in our case of nuclear decay.

Second, condition (B) can always be verified visually.

Third, condition (C) is a pure assumption, but it is commonly presupposed in the literature of quantum key distribution and physical RNGs including the single photon RNG mentioned in the Introduction.

Finally, the parameters in condition (D) can be estimated as follows. For the dark counts n_{dark}, we simply recall that their rate can generally be bounded from the property of detector D, and hence the number n_{dark} in total round of N can be statistically evaluated by the standard interval estimation methods.

As for the number of 'double' events n_{double}, the most straightforward evaluation method is to install the additional detector D′ (which is supposed to be parity symmetric to D) mentioned in condition (D), and count the number of coincidence events where both D and D′ click. In case D and the actual detector installed for D′, which we denote by D″, is not quite parity symmetric to D and does not share exactly the same properties, we may consider the completely positive maps (elements of completely positive instruments) M'_{D} and M''_{D} describing D′ and D″, respectively. With this, if we have, *e.g.*, $M''_{\mathrm{D}} > M'_{\mathrm{D}}$ (or $M''_{\mathrm{D}} - M'_{\mathrm{D}}$ is a positive map), then we find an upperbound for n_{double} from the coincidence counts measured with D and D″.

We also mention that, although somewhat artificial, one may simplify the process by imposing an additional assumption (which amounts to relaxing the security assumptions to some extent) that the source behaves the same way regardless of whether the user is estimating the parameters or not. This allows us to estimate the rate of 'double' events n_{double} at any time, such as at the time of shipment from the factory or at the initial setting before the actual use, based on the standard interval estimation methods again.

Security of measurement result i. Under these conditions, the security of measurement result **i** can be guaranteed as follows.

Theorem 1. The smooth min-entropy $H^{\delta}_{\mathrm{min}}(\mathbf{I}|E)$ of **i**, conditioned on Eve's degree of freedom E, is bounded as

$$H^{\delta}_{\mathrm{min}}(\mathbf{I}|E) \geq n_{\mathrm{thr}} - n_{\mathrm{double}} - 2n_{\mathrm{dark}}. \tag{2}$$

By combining the leftover hashing lemma[34] and Theorem 1, we can guarantee the security of **r** as follows.

Corollary 1. For a given security parameter $\varepsilon > 0$, the sequence of the final bits **r** is $\varepsilon + \delta$-secure, if Alice uses a universal$_2$ hash function f[32] for randomness extraction, and if its output length n_{fin} satisfies

$$n_{\mathrm{fin}} \leq n_{\mathrm{thr}} - n_{\mathrm{double}} - 2n_{\mathrm{dark}} - 2\log_2 \frac{1}{\varepsilon} + 2. \tag{3}$$

Recall that n_{double} and n_{dark} depend on δ through condition (D). Hence the right hand side of (3) depends on both ε and δ.

Proof of Theorem 1. The outline of the proof is as follows. On one hand in the actual implementation, we use detection timings as the origin of randomness. On the other hand in the security analysis, we instead analyze the absence/presence (denoted by $z_i = 0, 1$) of detection in each time bin i. This is possible since they are merely two different formats of the same measurement results. Now, by temporarily limiting ourselves to an ideal situation that the radiation consists of one particle and also that the detector has a unit efficiency with no dark count and covers the entire lower hemisphere, we show that variables z_i correspond to measuring the direction, up or down, in the radiation. Hence, measuring a parity symmetric radiation in this setting means measuring a parity invariant state using a pair of projectors interchangeable under parity operation. It then follows that the values $z_i = 0, 1$ occur with an equal probability, and in addition, the resulting (sub-normalized) states on Eve's side remain fixed irrespective of the values z_i. In other words, Eve can gain no information of z_i by any measurement, which establishes the security we want. The security in non-ideal situations can also be shown by essentially the same argument.

In order to simplify the analysis, we use the virtual protocol approach (also known as game transform in modern cryptography). In this approach, instead of analyzing the actual RNG directly, one modifies it and construct a virtual RNG, as well as a quantity H' arising there which lower bounds $H^{\delta}_{\mathrm{min}}(\mathbf{I}|E)$. Then analyzing the virtual RNG, one obtains a lower bound on H', which also lower bounds $H^{\delta}_{\mathrm{min}}(\mathbf{I}|E)$ by definition. With the virtual RNG and H' designed properly, this allows one to obtain a lower bound on $H^{\delta}_{\mathrm{min}}(\mathbf{I}|E)$ by a simpler analysis. We stress that virtual RNGs will only be used for simplifying the theoretical analysis, and never need to be implemented in practice.

As the first example of such virtual RNGs, we consider the case where Alice records the measurement result **i** in a different format $\mathbf{z} = (z_1, \ldots, z_N)$ where $z_i = 0$ ($z_i = 1$) indicates the absence (presence) of a detection in time bin i (Fig. 3). In other words, Alice records measurement results z_i of all time bins $i = 1, \ldots, N$, instead of timings **i** where a detection occurs. It is straightforward to see that **i** and **z** are in a one-to-one correspondence, and are thus equally unknown to Eve,

$$H^{\delta}_{\mathrm{min}}(\mathbf{I}|E) = H^{\delta}_{\mathrm{min}}(\mathbf{Z}|E). \tag{4}$$

Thus to lower bound $H^{\delta}_{\mathrm{min}}(\mathbf{I}|E)$, it suffices to bound $H^{\delta}_{\mathrm{min}}(\mathbf{Z}|E)$; this is an example of the quantity H', mentioned above.

Next we will modify this virtual RNG outputting **z** further, such that the parity transform P_A, is related to bit flips of z_i. Then we will make use of this relation to lower bound $H^{\delta}_{\mathrm{min}}(\mathbf{Z}|E)$.

Ideal situation. To elucidate this relation with a situation simplified from the actual one (Fig. 4(a)), we temporarily idealize conditions (A) and (B) as follows.

(A') At the beginning of each time bin, the state of radiations is parity invariant and consists of exactly one particle.

(B') Detector D is perfect (*i.e.*, with a unit efficiency and no dark counts) and covers exactly the entire lower hemisphere (Fig. 4(b)). Hence D goes off iff one particle or more go downward.

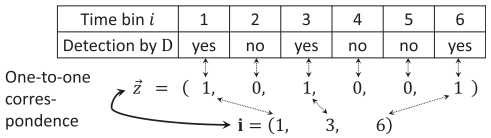

Fig. 3 Correspondence between detection timings and measurement results. This exemplifies how measurement results of all time bins $\mathbf{z} = (z_1, \ldots, z_N)$ and detection timings $\mathbf{i} = (i_1, \ldots, i_{n_{\mathrm{det}}})$ can be determined from the detections by the detector D. There is a one-to-one correspondence between **z** and **i**.

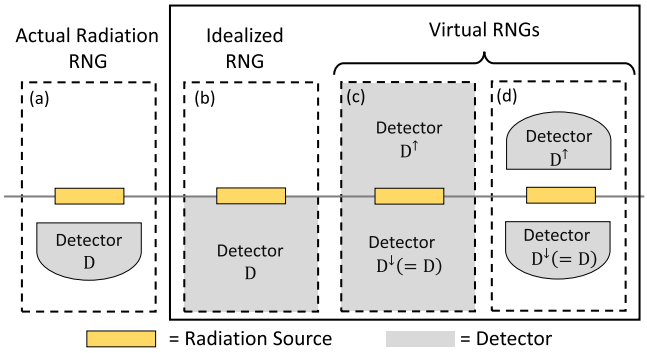

Fig. 4 Schematic layouts for the actual, idealized and virtual radioactive random number generators (RNGs). Panel (a) on the left shows the side view of our radioactive RNG. We assume that the detector D is housed within one (the lower) hemisphere (condition (B)). Panels (b), (c) and (d) depict theoretical models introduced for simplifying the description of the security proof, although these three never need to be implemented in practice. Panel (b) depicts the idealized setting satisfying conditions (A') and (B'), where the detector D alone can determine the direction, up or down, of the emitted particle. Similarly, panel (c) depicts the setting with two idealized detectors placed above and below the source. The layout given in (c) is, in effect, equivalent to the that given in (b) of the virtual RNG using two ideal detectors. Likewise, the layout depicted in (d) describes the virtual RNGs corresponding to the case (a).

Then we can modify our radioactive RNG further such that bit flips of z_i and P_A become equivalent.

To see this, first note that detector D alone can determine whether the particle went upward or downward. Indeed, if D detected the particle ($z_i = 1$), it means that it went down due to (B'); and if not ($z_i = 0$), two conditions together say that it went up.

These results $z_i = 0, 1$ can alternatively be obtained by a pair of perfect detectors, $D^{\downarrow}$ and $D^{\uparrow}$, each exactly covering the upper and the lower hemispheres (Fig. 4(c)). Thus we can define another virtual RNG satisfying (4).

Virtual RNG 1: Using $D^{\downarrow}$ and $D^{\uparrow}$, Alice measures the source in time bins $i = 1, \ldots, N$, and records the result as $w_i \in \{\uparrow, \downarrow\}$. She then lets $z_i = 0, 1$ if $w_i = \uparrow, \downarrow$.

Detectors $D^{\uparrow}$, $D^{\downarrow}$ are 'covariant' under P_A; that is, if we let $E_A^{\uparrow}$, $E_A^{\downarrow}$ be projection operators on the upper and the lower hemispheres corresponding to $D^{\uparrow}$, $D^{\downarrow}$, they satisfy

$$P_A E_A^{\uparrow} P_A = E_A^{\downarrow}. \tag{5}$$

Hence P_A is equivalent to the flip of arrows $w_i = \uparrow, \downarrow$, and thus to the bit flip of z_i.

Next we use this parity covariance to show that w_i are secure. Recall that ρ_{AE} before measurement is always parity invariant. Hence each w_i is the result of measuring a parity invariant state ρ_{AE} using parity covariant projections $E_A^{\uparrow}$, $E_A^{\downarrow}$. Thus $w_i = \uparrow, \downarrow$ occur with an equal probability, and in addition, the resulting (sub-normalized) states on Eve's side are a fixed state, irrespective of w_i,

$$\begin{aligned} \mathrm{tr}_A(E_A^{\downarrow}\rho_{AE}) &= \mathrm{tr}_A(P_A E_A^{\downarrow} P_A P_A \rho_{AE} P_A) \\ &= \mathrm{tr}_A(E_A^{\uparrow}\rho_{AE}) \end{aligned} \tag{6}$$

due to properties (1) and (5). In other words, all elements of $\mathbf{w} = (w_1, \ldots, w_N)$ are distributed uniformly, and Eve gains no information of it by any measurement. In terms of the min-entropy, this means

$$H_{\min}^{\delta}(\mathbf{Z}|E) = H_{\min}^{\delta}(\mathbf{W}|E) = N. \tag{7}$$

This completes the proof of Theorem 1 for the ideal situation.

Table 1 Relation between variables used in the proof of the general situation.

w_i	↑	none	↓	double
$z_i = g(w_i)$	0		1	
$\tilde{w}_i = h(w_i)$	single	none	single	double

The output from detector pair $D^{\downarrow}$, $D^{\uparrow}$ in the time-bin i is represented as w_i. The variable $z_i (= g(w_i))$ gives the output of the actual detector $D = (D^{\downarrow})$ that can be emulated from w_i; this corresponds to ignoring outputs of $D^{\uparrow}$. The variable $\tilde{w}_i (= (h(w_i)))$ denotes how many detectors went off out of $D^{\downarrow}$ and $D^{\uparrow}$.

General situation. We proceed to the proof of the general situation. We again construct a virtual RNG where a correspondence between bit flips of z_i and P_A holds. Alice again uses a detector pair $D^{\downarrow}$ and $D^{\uparrow}$ with $D^{\downarrow}$ being the actual detector D and $D^{\uparrow}$ being the parity transformed image of D (Fig. 4(d)).

As we no longer impose conditions (A') and (B'), it is possible that none or both of this detector pair, instead of one, go off in a time bin. Hence each w_i takes four values, $w_i \in \{\uparrow, \downarrow, \text{none}, \text{double}\}$ (Table 1, 1st row).

In this case, the output z_i of D ($= D^{\downarrow}$) alone can be emulated from w_i, by ignoring outputs of $D^{\uparrow}$ (Table 1, second row). Thus we can define a virtual RNG as follows.

Virtual RNG 2: Using $D^{\downarrow}$ and $D^{\uparrow}$, Alice measures the source in time bins $i = 1, \ldots, N$, and records the result as $w_i \in \{\uparrow, \downarrow, \text{none}, \text{double}\}$. She then lets $z_i = g(w_i)$, using function g specified in the second row of Table 1, where the output $g(w_i)$ satisfies

$$H_{\min}(\mathbf{Z}|E) = H_{\min}(g(\mathbf{W})|E). \tag{8}$$

We will use a similar argument to the one in the ideal situation to bound the right hand side of (8) by exploiting the relation between measurement results and the parity transform P_A. However, the argument needs to be modified, as the relation is not the same as in the ideal situation.

That is, unlike in the ideal situation, the bit flip of z_i and P_A may not be equivalent in general. This is because $z_i = 0, 1$ may come from measurement results $w_i =$ 'none' or 'double', whose quantum measurements are not in general covariant under P_A. On the other hand, measurements of $w_i = \uparrow$ and $\downarrow$ are still covariant under P_A, by definition of $D^{\downarrow}$, $D^{\uparrow}$.

Hence if we evaluate the min-entropy of w_i in single detection events (*i.e.*, time bins i where $w_i = \uparrow$ or $\downarrow$; see Table 1, 3rd row), we have the ideal situation again, and the security can be shown by the same reasoning as before. The min-entropy thus obtained lower bounds $H_{\min}(g(\mathbf{W})|E)$ on the right hand side of (8), since in general, the entropy of a part is not greater than that of the total. As a result, $H_{\min}(g(\mathbf{W})|E)$ is lower bounded by the number of single detection events. (For the rigorous proof of statements made in this paragraph, see Methods.)

We can bound the number of single detection events as follows. The number D of the detection events is no larger than the sum of the number of the single detection events and the 'double' events. The 'double' events can occur if the multiparticle emission or the dark count occurs in either detector. Then due to condition (D), the number of single detection events can be further lower bounded by $n_{\text{thr}} - n_{\text{double}} - 2n_{\text{dark}}$, except for probability δ, and we obtain Theorem 1.

As an example, we consider the performance of the RNG which has a prototype[26] based on ^{241}Am. In this RNG, the length of each time bin is 1 millisecond and the detection rate is about 0.055 per time bin. We may thus assume that it can be bounded by 0.05 from below and by 0.06 from above. Choosing the number $N = 10^5$ for the total rounds, we consider the protocol ϵ'-secure with $\epsilon' = 2^{-50}$ following the standard practice and set $n_{\rm thr} = N \times 0.05$. Although the rate of 'double' events is not measured directly, it is reasonable to estimate that the rate is bounded from above by $(0.06)^2/2$ per time bin, since each nucleus decays independently and identically. This implies that, except with probability $\epsilon'/2$, there are at most 305 'double' events in N rounds[35]. The dark count rate is negligible and can be put to zero in effect, because the energy of α-decay of ^{241}Am is around 5 MeV, which is much higher than the typical energy 1 eV of the optical photon. To sum up, the parameters in condition (D) are found to be $\delta = \epsilon'/2, n_{\rm thr} = 5000, n_{\rm double} = 305, n_{\rm dark} = 0$. Setting the parameter $\epsilon = \epsilon'/2$ in Corollary 1, we find that this protocol is ϵ'-secure and generates a random number of the length $n_{\rm fin} = 4595$ unless the protocol is aborted.

Conclusions

With the help of the parity symmetry, we solved the problem on the security of the radioactive RNG which had remained open over half a century, and further showed that this type of RNG can realize the universally composable security.

Unlike the model dependent description of decay-timing properties, the parity symmetry inherent to the system is much easier to handle from the first principle. When combined with the purely quantum nature of nuclear decays, it leads to the detection outcomes with intrinsic randomness. This is analogous to the high speed RNG[36], where the laser phase fluctuations arising from spontaneous emissions, which are purely quantum, are responsible for the randomness. These two RNGs are different in strategy in that, while our radioactive RNG exploits the parity invariance, the optical quantum RNG[36] uses a theoretical model of laser emission as the basic ingredient.

We stress that our proof method is quite distinct from those previously employed for photon RNGs. This can be seen most clearly in the property that one does not need any condition on the state ρ_{AE} except for the parity invariance Eq. (1). This gives a major merit to our method, exempting us from discussing any other properties, let alone an actual realization of the state ρ_{AE}. It should be noted that the condition in Eq. (1) is much stronger than $P_A \rho_A(t) P_A = \rho_A(t)$ which cannot ensure the security by itself.

We also note that, since previous arguments[17–22] on radiation RNGs employed phenomenological models, it was impractical to assume any reliable conditions on the state ρ_{AE} (such as being the coherent state) at an arbitrary accuracy. In contrast, the parity invariance we used is a fundamental property of particle interactions and, as such, it can provide a robust basis for ensuring the security of random numbers.

Methods

Definition of security and the leftover hashing. We review definition of the security of RNG, as well as techniques for guaranteeing it.

The sequence of final bits $\mathbf{r}$ is secure when it is distributed uniformly and unknown to Eve. This can be formalized as follows. Given an actual state $\rho_{\mathbf{RE}}$, we define the corresponding ideal state to be $\rho^{\rm ideal}_{\mathbf{RE}} = 2^{-n_{\rm fin}} \mathbb{I}_{\mathbf{R}} \otimes \rho_E$, $\rho_E = {\rm tr}_A(\rho_{AE})$, where $\mathbf{r}$ is distributed uniformly and is completely unknown to Eve. $\mathcal{H}_{\mathbf{R}}$ is the Hilbert space of the memory storing $\mathbf{r}$. However, as it is practically difficult to always guarantee this ideal situation, it is customary to relax this notion and say that $\mathbf{r}$ is ε-secure if

$$\tfrac{1}{2} \left\| \rho_{\mathbf{RE}} - \rho^{\rm ideal}_{\mathbf{RE}} \right\|_1 \le \varepsilon, \tag{9}$$

where $\|A\|_1 = {\rm tr}\left(\sqrt{AA^\dagger}\right)$ denotes the L_1-norm of an operator A. Intuitively, this says that the actual state cannot be discriminated from the ideal state except with probability ε. This notion of security using parameter ε is often called the universally composable security[31].

The conditional min-entropy $H_{\min}(\mathbf{I}|E)_{\rho_{\mathbf{IE}}}$ of a sub-normalized state $\rho_{\mathbf{IE}}$ is defined to be the maximum real number λ, satisfying $2^{-\lambda} \mathbb{I}_{\mathbf{I}} \otimes \sigma_E \ge \rho_{\mathbf{IE}}$ for a normalized state σ_E[34,37]. We abbreviate $H_{\min}(\mathbf{I}|E)_{\rho_{\mathbf{IE}}}$ as $H_{\min}(\mathbf{I}|E)$, whenever the subscript $\rho_{\mathbf{IE}}$ is obvious from the context. The smooth conditional min-entropy $H^{\delta}_{\min}(\mathbf{I}|E)_{\rho_{\mathbf{IE}}}$ is the maximum value of $H_{\min}(\bar{\rho}_{AE}|E)_{\bar{\rho}_{\mathbf{IE}}}$ of sub-normalized states $\bar{\rho}_{\mathbf{IE}}$ that are δ-close to $\rho_{\mathbf{IE}}$ in terms of the purified distance[37].

If Alice performs randomness extraction using a universal$_2$ function family $\mathcal{F}$[32], the security of its output $\mathbf{r}$ satisfies the following.

Lemma 1. (Leftover hashing lemma (LHL,[34])) Suppose a random function f_s is universal$_2$; *i.e.*, $f_s \in \mathcal{F}$ is chosen with a probability $p(s)$ satisfying

$$\forall x, y, x \ne y, \ \sum_s p(s) \delta_{f_s(x) f_s(y)} \le 2^{-n_{\rm fin}}. \tag{10}$$

Then, we have

$$\sum_s p(s) \left\| \rho_{\mathbf{RE}} - \rho^{\rm ideal}_{\mathbf{RE}} \right\|_1 \le 2\delta + 2^{\frac{1}{2}[n_{\rm fin} - H^{\delta}_{\min}(\mathbf{I}|E)]}. \tag{11}$$

By combining this lemma and Theorem 1, we obtain Corollary 1.

Detailed descriptions of Radioactive RNG and Virtual RNG 2. We here give a detailed mathematical description of Radioactive RNG and Virtual RNG 2. We will describe Virtual RNG 2 only, but the same description applies also to Radioactive RNG if one neglects output of virtual detector $\mathrm{D}^{\uparrow}$ (cf. Table 1, 1st and 2nd rows).

Description of the procedures of Virtual RNG 2. We will denote by $\bar{\mathrm{D}}$ the measurements setup consisting of detector pair $\mathrm{D}^{\uparrow}, \mathrm{D}^{\downarrow}$. We denote four output patterns of from $\bar{\mathrm{D}}$ in one time bin by $w \in \mathcal{W}$, where $\mathcal{W} := \{\uparrow, \downarrow, \text{none}, \text{double}\}$ (Table 1, 1st row). For the convenience of the security proof, we classify w by how many of the detector pair $\mathrm{D}^{\uparrow}, \mathrm{D}^{\downarrow}$ go off in the time bin, using symbols $\tilde{\mathcal{W}} := \{\text{none}, \text{single}, \text{double}\}$, where 'single' event means $w = \uparrow$ or $\downarrow$. A function h can be defined corresponding to this classification (Table 1, third row).

We continue to describe radiated particles by the Hilbert space $\mathcal{H}_A$. In addition, we introduce $\mathcal{H}_B$ to describe the radiation source.

We describe the quantum process (measurement and time evolution) occurring inside the RNG device, during the beginnings of adjacent time bins, by a completely positive map $M^w_{AB} : \mathcal{H}_A \otimes \mathcal{H}_B \to \mathcal{H}_A \otimes \mathcal{H}_B$. That is, if Alice measures the state $\sigma_{ABE}(j\Delta t)$ at the beginning of time bin $j+1$ and obtains output w, the state at the beginning of next time bin is $\sigma^w_{ABE}((j+1)\Delta t) = M^w_{AB}(\sigma_{ABE}(j\Delta t))$.

(We here extend the convention for operators, introduced above Eq. (1), to maps of states, and omit the identity operation included in a tensor product; hence *e.g.*, $M^w_{AB} = M^w_{AB} \otimes {\rm id}_E$ with ${\rm id}_E$ being the identity operation in $\mathcal{H}_E$.)

Hence if Alice started Virtual RNG 2 with the state $\rho_{ABE}(0)$, and measured $w_1, \ldots, w_j$ in time bins $1, \ldots, j$, the (sub-normalized) state at the beginning of time bin $j+1$ takes the form

$$\rho^{(w_1, \ldots, w_j)}_{ABE}(j\Delta t) := M^{w_j}_{AB} \circ \cdots \circ M^{w_1}_{AB}(\rho_{ABE}(0)). \tag{12}$$

When Virtual RNG 2 is finished, the joint state of the memory that stores the entire measurement result $\mathbf{w} = (w_1, \ldots, w_N)$ and of Eve takes the form

$$\rho_{\mathbf{WE}} = \sum_{\mathbf{w} \in \mathcal{W}^N} |\mathbf{w}\rangle\langle\mathbf{w}|_{\mathbf{W}} \otimes \rho^{\mathbf{w}}_E, \tag{13}$$

$$\rho^{\mathbf{w}}_E = \rho^{(w_1, \ldots, w_N)}_E = {\rm tr}_{AB}\left(\rho^{(w_1, \ldots, w_N)}_{ABE}(N\Delta t)\right) \tag{14}$$

Parity invariance of the measurement result $\mathrm{w_i}$. In this setting, we can argue that $\rho^{\mathbf{w}}_E$ are invariant under flips of arrows $\uparrow$ and $\downarrow$ included in w_i, by essentially the same argument as in Eq. (6).

To see this, first note that condition (A) asserts that

$$\tilde{P}_A(\rho^{(w_1, \ldots, w_j)}_{ABE}(j\Delta t)) = \rho^{(w_1, \ldots, w_j)}_{ABE}(j\Delta t). \tag{15}$$

Also note that the following relation holds for maps $M^{\uparrow}_{AB}$ and $M^{\downarrow}_{AB}$,

$$M^{\uparrow}_{AB} \circ \tilde{P}_A = M^{\downarrow}_{AB}, \tag{16}$$

where $\tilde{P}_A(\rho_A) := P_A \rho_{ABE} P_A$. Eq. (16) holds for the following two reasons: (i) Due to the construction of $\bar{\mathrm{D}}$, obtaining the measurement result $\downarrow$ is equivalent to first applying the parity transform and then obtaining $\uparrow$. (ii) Due to condition (C), the effect caused on radiations by the measurement of a time bin i (which may depend on results $w_i = \downarrow, \uparrow$) is washed away before the measurement of the next time bin $i+1$ starts.

From relations (15), (16), we see that the (sub-normalized) state at the beginning of time bin $j+1$ satisfies

$$\begin{aligned}
&\rho_{ABE}^{(w_1,\cdots,w_{j-1},\downarrow)}(j\Delta t)\\
&= M_{AB}^{\downarrow}(\rho_{ABE}^{(w_1,\cdots,w_{j-1})}((j-1)\Delta t))\\
&= M_{AB}^{\uparrow}\circ P_A(\rho_{ABE}^{(w_1,\cdots,w_{j-1})}((j-1)\Delta t))\\
&= M_{AB}^{\uparrow}(\rho_{ABE}^{(w_1,\cdots,w_{j-1})}((j-1)\Delta t))\\
&= \rho_{ABE}^{(w_1,\cdots,w_{j-1},\uparrow)}(j\Delta t).
\end{aligned} \tag{17}$$

Further, combining this with Eq. (12), we see that $\rho_E^{\mathbf{w}}$ are invariant under flips of arrows $\uparrow$ and $\downarrow$ included in w_i. Or in terms of classification $\tilde{\mathcal{W}} = \{\text{none}, \text{single}, \text{double}\}$

$$\rho_E^{\mathbf{w}} = \rho_E^{\mathbf{w}'} \quad \text{if} \quad h(\mathbf{w}) = h(\mathbf{w}'), \tag{18}$$

where $h(\mathbf{w}) := (h(w_1), \ldots, h(w_N))$. That is, $\rho_E^{\mathbf{w}}, \rho_E^{\mathbf{w}'}$ are equal, if it holds for all time bin i that the number of detectors that went off in time bin i is equal, $h(w_i) = h(w') \in \tilde{\mathcal{W}}$.

Supplement to the proof of Theorem 1. We argued that the right hand side of (8) is lower bounded by the number of single detection events. The argument made there was in fact rather intuitive and not sufficiently rigorous. Below we give a rigorous proof.

Under these settings, we consider the following virtual RNG. This corresponds to the situation where Alice intentionally reveals $h(\mathbf{w})$ to Eve.

Virtual RNG 3: After executing Virtual RNG 2, Alice tells Eve $h(\mathbf{w})$.

The min-entropy corresponding to this case lower bounds the right hand side of (8), since Eve's ambiguity never increases on receiving an extra information $h(\mathbf{w})$.

$$H_{\min}(g(\mathbf{W})|E) \geq H_{\min}(g(\mathbf{W})|h(\mathbf{W}), E). \tag{19}$$

After Virtual RNG 3, Alice and Eve both know the classical random variable $\tilde{\mathbf{w}} = h(\mathbf{w})$, so the overall state becomes a classical ensemble of those labeled by $\tilde{\mathbf{w}}$. Thus it suffices to analyze each $\tilde{\mathbf{w}}$ separately. We rephrase this rigorously[34] (See Lemma 3.1.8) as

$$H_{\min}(g(\mathbf{W})|h(\mathbf{W}), E) \geq \min_{\tilde{\mathbf{w}}} H_{\min}(g(\mathbf{W})|h(\mathbf{W}) = \tilde{\mathbf{w}}, E), \tag{20}$$

where the minimum is evaluated for all values of $\tilde{\mathbf{w}}$ possible, *i.e.*, all $\tilde{\mathbf{w}} \in \tilde{\mathcal{W}}^N$ satisfying $\Pr(h(\mathbf{w}) = \tilde{\mathbf{w}} \,|\, \rho_{\mathrm{WE}}) > 0$.

$H_{\min}(g(\mathbf{W})|h(\mathbf{W}) = \tilde{\mathbf{w}}, E)$ on the right hand side of (20) measures the fraction of $g(\mathbf{w})$ unknown to Eve, under the restriction that $\mathbf{w}$ takes values satisfying $h(\mathbf{w}) = \tilde{\mathbf{w}}$. As can easily be seen by definition of functions g and h in Table 1, under this restriction, function g becomes one-to-one, and thus the min-entropies of $g(\mathbf{w})$ and $\mathbf{w}$ are equal,

$$H_{\min}(g(\mathbf{W})|h(\mathbf{W}) = \tilde{\mathbf{w}}, E) = H_{\min}(\mathbf{W}|h(\mathbf{W}) = \tilde{\mathbf{w}}, E). \tag{21}$$

The right hand side of (21) can be evaluated using the parity symmetry (18). Let $s(\tilde{\mathbf{w}})$ be the number of 'single' symbols included in $\tilde{\mathbf{w}}$ (*i.e.*, the number of single events), then there are $2^{s(\tilde{\mathbf{w}})}$ values of $\mathbf{w}$ satisfying $h(\mathbf{w}) = \tilde{\mathbf{w}}$. Because of (18), Eve's (sub-normalized) states $\rho_E^{\tilde{\mathbf{w}}}$ are equal for all these values of $\tilde{\mathbf{w}}$, and thus the corresponding entropy takes the value

$$H_{\min}(\mathbf{W}|h(\mathbf{W}) = \tilde{\mathbf{w}}, E) = s(\tilde{\mathbf{w}}). \tag{22}$$

Finally, combining Eqs. (19)–(22) together, we obtain

$$H_{\min}(g(\mathbf{W})|E) \geq \min_{\tilde{\mathbf{w}}} s(\tilde{\mathbf{w}}). \tag{23}$$

Data availability

The authors declare that the data supporting the findings of this study are available within the paper.

Received: 19 July 2021; Accepted: 13 May 2022;
Published online: 01 July 2022

References

1. Shannon, C. E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **28**, 656–715 (1949).
2. Acín, A. & Masanes, L. Certified randomness in quantum physics. *Nature* **540**, 213–219 (2016).
3. Ma, X., Yuan, X., Cao, Z., Qi, B. & Zhang, Z. Quantum random number generation. *npj Quantum Inf.* **2**, 16021 (2016).
4. Herrero-Collantes, M. & Garcia-Escartin, J. C. Quantum random number generators. *Rev. Modern Phys.* **89**, 015004 (2017).
5. Bierhorst, P. et al. Experimentally generated randomness certified by the impossibility of superluminal signals. *Nature* **556**, 223–226 (2018).
6. Stefanov, A., Gisin, N., Guinnard, O., Guinnard, L. & Zbinden, H. Optical quantum random number generator. *J. Modern Opt.* **47**, 595–598 (2000).
7. Rarity, J. G., Owens, P. C. & Tapster, P. R. Quantum random-number generation and key sharing. *J. Modern Opt.* **41**, 2435–2444 (1994).
8. Dynes, J. F., Yuan, Z. L., Sharpe, A. W. & Shields, A. J. A high speed, postprocessing free, quantum random number generator. *Appl. Phys. Lett.* **93**, 031109 (2008).
9. Ma, H.-Q., Xie, Y. & Wu, L.-A. Random number generation based on the time of arrival of single photons. *Appl. Opt.* **44**, 7760 (2005).
10. Nie, Y. Q. et al. Practical and fast quantum random number generation based on photon arrival time relative to external reference. *Appl. Phys. Lett.* **104**, 051110 (2014).
11. Wayne, M. A., Jeffrey, E. R., Akselrod, G. M. & Kwiat, P. G. Photon arrival time quantum random number generation. *J. Modern Opt.* **56**, 516–522 (2009).
12. Wahl, M. et al. An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements. *Appl. Phys. Lett.* **98**, 171105 (2011).
13. Yan, Q., Zhao, B., Liao, Q. & Zhou, N. Multi-bit quantum random number generation by measuring positions of arrival photons. *Rev. Sci. Instru.* **85**, 103116 (2014).
14. Ren, M. et al. Quantum random-number generator based on a photon-number-resolving detector. *Phys. Rev. A—Atomic Mol. Opt. Phys.* **83**, 023820 (2011).
15. Applegate, M. J. et al. Efficient and robust quantum random number generation by photon number detection. *Appl. Phys. Lett.* **107**, 071106 (2015).
16. Wayne, M. A., Jeffrey, E. R., Akelsrod, G. M. & Kwiat, P. G. High-speed quantum random number generation. *Conference on Quantum Electronics and Laser Science (QELS) - Technical Digest Series* **18**, 13029 (2008).
17. Ishida, M. & Ikeda, H. Random number generator. *Ann. Inst. Stat. Math.* **8**, 119–126 (1956).
18. Manelis, B. Generating random noise. *Electronics* **8 Sep.**, 66–69 (1961).
19. Schmidt, H. Quantum-mechanical random-number generator. *J. Appl. Phys.* **41**, 462–468 (1970).
20. Silverman, M. P., Strange, W., Silverman, C. R. & Lipscombe, T. C. Tests of alpha-, beta-, and electron capture decays for randomness. *Phys. Lett. Section A: Gen. Atomic Solid State Phys.* **262**, 265–273 (1999).
21. Walker, J. "HotBits: Genuine random numbers, generated by radioactive decay" (1996).
22. Alkassar, A., Nicolay, T. & Rohe, M. Obtaining true-random binary numbers from a weak radioactive source. In *Lecture Notes in Computer Science*, vol. 3481, 634-646 (Springer, Berlin, Heidelberg, 2005).
23. Lutz, G. Semiconductor radiation detectors (Springer- Verlag, Berlin/ Heidelberg, 2007).
24. Knoll, G. F. Radiation detection and measurement (Wiley, New York, 2010).
25. Rochas, A. et al. First fully integrated 2-d array of single-photon detectors in standard CMOS technology. *IEEE Photonics Tech. Lett.* **15**, 963–965 (2003).
26. Quantaglion Co. Ltd. QNT series.
27. Tsuyuzaki, N. Random pulse generation source, and semiconductor device, method and program for generating random number and/or probability using the source (2005).
28. EYL Inc. Quantum Entropy Chip-EYL.
29. Segre, E.Nuclei and particles : an introduction to nuclear and subnuclear physics (Reading, Mass. : W. A. Benjamin, 1977).
30. Stephens, F. The study of nuclear states observed in alpha decay. *Pure Appl. Phys.* **9**, 170 (1960).
31. Ben-Or, M., Horodecki, M., Leung, D. W., Mayers, D. & Oppenheim, J. The universal composable security of quantum key distribution. In *Lecture Notes in Computer Science*, vol. 3378, 386-406 (Springer Verlag, 2005).
32. Carter, J. L. & Wegman, M. N. Universal classes of hash functions. *J. Comput. Syst. Sci.* **18**, 143–154 (1979).
33. Evaluated Nuclear Structure Data File, http://www.nndc.bnl.gov/ensdf (2022).
34. Renner, R. Security of Quantum Key Distribution. Diss. eth no. 16242, ETH ZURICH (2005).
35. Hoeffding, W. Probability inequalities for sums of bounded random variables. *J. Am. Stat. Assoc.* **58**, 13–30 (1963).
36. Zhou, H., Yuan, X. & Ma, X. Randomness generation based on spontaneous emissions of lasers. *Phys. Rev. A* **91**, 062316 (2015).
37. Tomamichel, M.A Framework for non-asymptotic quantum information. Theory. Diss. eth no. 20213, ETH ZURICH (2012).

Acknowledgements

T.S. is supported in part by Cross-ministerial Strategic Innovation Promotion Program (SIP) (Council for Science, Technology and Innovation (CSTI)); CREST (Japan Science and Technology Agency) JPMJCR1671; JSPS KAKENHI Grant Number JP18K1 3469. T.S. also thanks Quantaglion Co. Ltd. for useful information and discussion about the actual implementation of the radioactive RNG.

Author contributions

T.T., T.S, and I.T. contributed to the initial conception of the ideas, to the working out of details, and to the writing and editing of the manuscript.

Competing interests

T.S. borrowed a radioactive RNG from Quantaglion Co. Ltd. All other authors declare no competing interests.

Additional information

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s42005-022-00915-1.

Correspondence and requests for materials should be addressed to Toshihiko Sasaki.

Peer review information *Communications Physics* thanks Xiongfeng Ma and the other, anonymous, reviewer(s) for their contribution to the peer review of this work. Peer reviewer reports are available.

Reprints and permission information is available at http://www.nature.com/reprints

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