Received: 27 March 2020 | Revised: 23 June 2020 | Accepted: 12 August 2020

DOI: 10.4218/etrij.2020-0119

ORIGINAL ARTICLE

ETRI Journal WILEY

A lightweight true random number generator using beta radiation for IoT applications

Kyunghwan Park[1] | **Seongmo Park**[1] | **Byoung Gun Choi**[1] | **Taewook Kang**[1] | **Jongbum Kim**[2] | **Young-Hee Kim**[3] | **Hong-Zhou Jin**[3]

[1]Artificial Intelligence Research Laboratory, Electronics and Telecommunications Research Institute, Gwangju, Rep. of Korea

[2]Radioisotope Research Division, Korea Atomic Energy Research Institute, Daejeon, Rep. of Korea

[3]Department of Electronic Engineering, Changwon National University, Changwon, Rep. of Korea

Correspondence
Kyunghwan Park, Artificial Intelligence Research Laboratory, Electronics and Telecommunications Research Institute, Gwangju, Rep. of Korea.
Email: khpark_2001@etri.re.kr

Funding information
This research was supported by Nuclear Technology Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (No. 2018M2A8A1083094).

Abstract

This paper presents a lightweight true random number generator (TRNG) using beta radiation that is useful for Internet of Things (IoT) security. In general, a random number generator (RNG) is required for all secure communication devices because random numbers are needed to generate encryption keys. Most RNGs are computer algorithms and use physical noise as their seed. However, it is difficult to obtain physical noise in small IoT devices. Since IoT security functions are required in almost all countries, IoT devices must be equipped with security algorithms that can pass the cryptographic module validation programs of each country. In this regard, it is very cumbersome to embed security algorithms, random number generation algorithms, and even physical noise sources in small IoT devices. Therefore, this paper introduces a lightweight TRNG comprising a thin-film beta-radiation source and integrated circuits (ICs). Although the ICs are currently being designed, the IC design was functionally verified at the board level. Our random numbers are output from a verification board and tested according to National Institute of Standards and Technology standards.

KEYWORDS

beta radiation, IoT security, radiation detection circuit, random number generator

1 | INTRODUCTION

In general, random number generators (RNGs) can be classified as software- or hardware-based. A software-based RNG called a pseudorandom number generator (PRNG) is a deterministic system to which most RNGs belong. In contrast, a hardware-based RNG is a nondeterministic system, that is, an unpredictable system. There are many physical noise sources in hardware-based RNGs: thermal noise, atmospheric noise, shot noise, photons passing through a beam splitter, nuclear decay, and so on. Among them, quantum mechanical noise is said to have perfect randomness [1–3]. Therefore, RNGs using nuclear decay, a quantum mechanical phenomenon, have been developed by several scientists [4–9]. Radiation by nuclear decay is converted into a random number by an appropriate method [7–11]. As is well-known, there are three types of radiation in physics: alpha, gamma, and beta. Alpha radiation is high in energy and can damage semiconductor devices.

Gamma radiation penetrates everything, which is dangerous to a person. In contrast, it is easy to shield things from

beta radiation, which has a low energy; thus, it is safe to use and does not damage semiconductor devices. However, it is difficult to detect owing to its low energy. Therefore, a circuit capable of detecting such low-energy beta radiation will be a key technology. We have developed a detection circuit with a very high sensitivity.

The critical disadvantage of RNGs using radiation is their low-generation rate. This is because high doses of radiation cannot be used for safety reasons. If the energy per particle is high, then the radiation dose should be reduced. Therefore, the maximum radiation dose allowed for commercial purposes depends on the energy per particle and is specified as a regulatory value [12]. In general, the regulatory exemption dose is low for alpha or gamma radiation and high for beta radiation. It is 10 kBq for americium-241, an alpha source, and 100 MBq for nickel-63, a beta source. The high-radiation dose means correspondingly faster generation. If this is true, why have others not used beta radiation for RNGs? It is probably because the performance of existing radiation detectors does not match that of the RNG. Since the performance of conventional radiation detectors is tailored to measure the amount of radiation, diodes with large sensing areas have been used. This large sensing area causes more noise. Therefore, there was no technology for detecting individual occurrences of beta radiation with a low energy. Hence, we developed a beta radiation detection circuit suitable for RNGs and used a smaller diode. As a result, an RNG with a higher speed and smaller size was developed.

The next four sections describe the development of a beta source for RNGs, the beta radiation detection circuit including an integrated circuit (IC), signal processing for conversion to random numbers, and statistical analyses of random number data.

2 | BETA SOURCE DESIGN

2.1 | Beta-emitting radioactive isotopes

A comparison of candidate beta radioisotopes suitable for RNGs is presented in Table 1.

Before making this comparison, we need to be aware of the limitations of today's beta radiation measurement technology. In fact, beta radiation measurement technology using commercial PIN diode detectors cannot detect beta particles below 5 keV without cooling [13,14]. This means that only beta radiation with an energy of 5 keV or more is detectable. Taking this into account, ^{3}H (tritium) is vulnerable to noise because of its low energy. Since a large portion of beta particles from ^{3}H are below 5 keV, the detector's count ratio is low, and the instrument's threshold is susceptible to fluctuations due to noise. In contrast, ^{147}Pm (promethium) has a high energy, but it is difficult to shield against it because it is accompanied by X-rays. Another disadvantage is that its half-life is very short.

TABLE 1 Comparison of beta radioisotopes

Radioactive isotope	Maximum energy	Average energy	Half-life	Exemption rad. dose
^{3}H	18.6 keV	5.7 keV	12.33 yr	10^{9} Bq
^{63}Ni	66.9 keV	17.1 keV	100.1 yr	10^{8} Bq
^{147}Pm	224.1 keV	62.1 keV	2.62 yr	10^{7} Bq

Finally, ^{63}Ni (nickel) emits pure beta particles with a maximum energy of 17.1 keV. At room temperature, approximately 85% of the particles can be detected. Since its half-life is almost 100 years, the count rate can be stably maintained for several decades. The long half-life of ^{63}Ni is a very useful feature in betavoltaic batteries that produce electricity with beta radiation [15]. A betavoltaic cell uses the forward current-voltage (*I-V*) characteristics of diodes, while radiation detectors use the dark current under reverse voltages. The former should use as much of the dose as possible, the latter using doses below the regulatory exemption. The regulatory exemption radiation dose of ^{63}Ni is 10^{8} Bq, which can enable high-rate random number generation. Therefore, ^{63}Ni would be best suited for RNGs.

2.2 | Detection probability for ^{63}Ni

The radiation energy spectrum of ^{63}Ni in the Evaluated Nuclear Data File (ENDF) is shown in Figure 1. The emission probability of beta particles from ^{63}Ni atomic nuclei linearly decreases as the energy of beta particles increases. The beta particles have an average energy of 17.1 keV and a maximum energy of 66.9 keV.

However, the beta radiation measured at a PIN diode in one direction exhibits the spectrum in Figure 2, which is different from the ENDF spectrum for a single nucleus. Since the

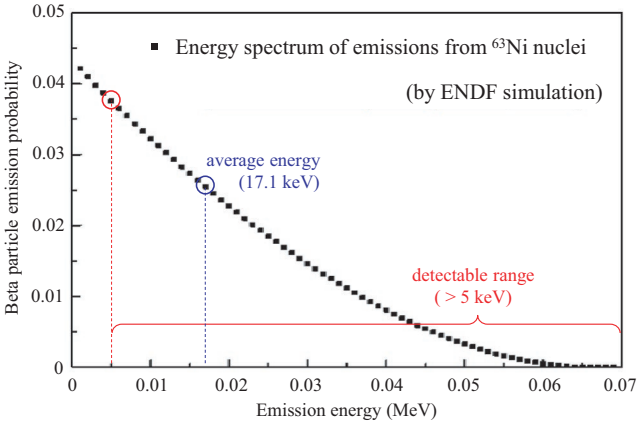


FIGURE 1 Energy spectrum of emissions from ^{63}Ni nuclei

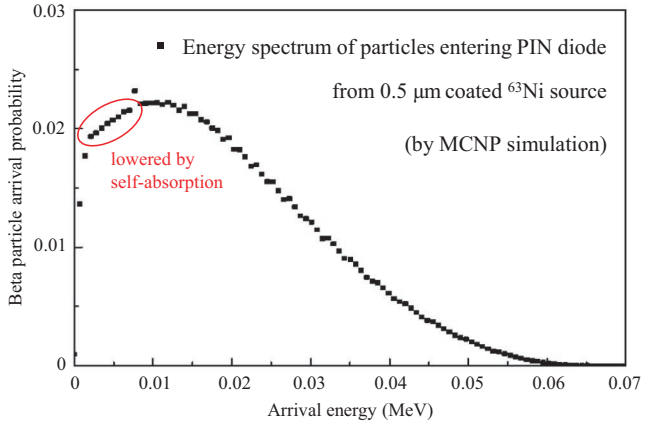


FIGURE 2 Energy spectrum of particles entering the PIN diode detector

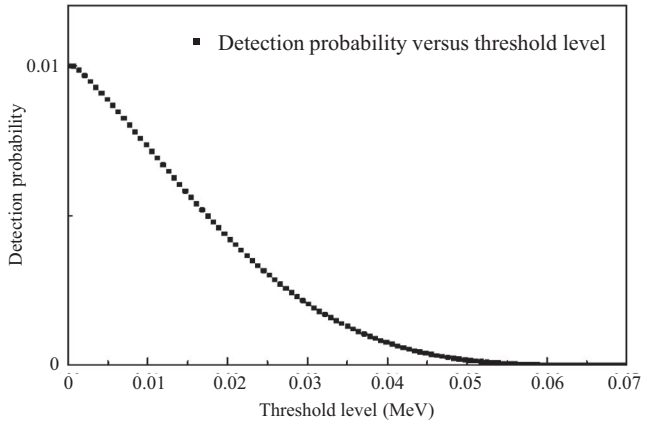


FIGURE 3 Beta-decay detection probability according to the threshold level

actual beta source used for measurement is a volume source, particles emitted from inside the source suffer energy loss by self-absorption while they are emitted from the source. As a result, the particles in the low-energy region are not able to exceed the detector's threshold energy because their energy is lowered by self-absorption. Because of this, the probability of detecting beta radiation in the low-energy region is lowered, and a peak occurs at about 10 keV.

In general, the detector's threshold energy level is set to the noise level generated by the PIN diode and a signal processing circuit. Further, it can be set to measure only radiation above a specific energy. Therefore, if the threshold level is set high, the number of measured radiation pulses decreases, as shown in Figure 3. The detection probability is the fraction of detected pulses out of all beta radiation arriving at the PIN diode according to threshold. When using a commercial PIN diode having an active area of 6 mm^2, only beta particles above 5 keV can be detected at room temperature. The detection probability at this time is about 86%.

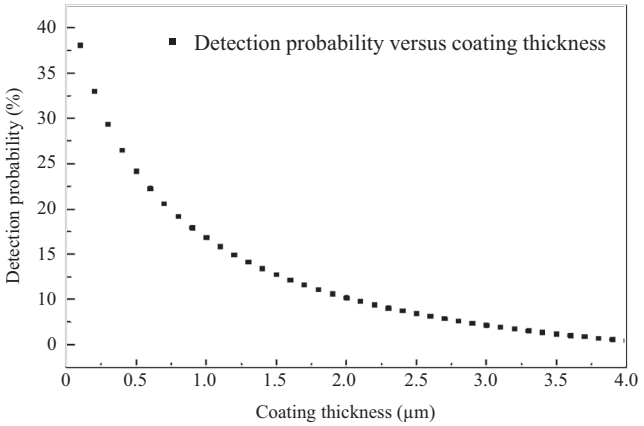


FIGURE 4 Beta-decay detection probability according to the coating thickness

Figure 4 shows the detection probability according to the plating thickness when plating is performed using a plating source with a density of 8.0 g/cm^3. Monte Carlo N-particle Transport (MCNP) simulation results are shown for a 5-keV threshold, as measured by a PIN diode detector. The detection probabilities are 38% at 0.1 μm, 24% at 0.5 μm, 16.8% at 1 μm, and 10% at 2 μm. In general, commercial ^{63}Ni calibration sources have emission rates of approximately 10%. Thus, the coating thickness of the calibration source is considered to be 2 μm to 2.5 μm if the coating conditions are the same.

The total number of pulses per unit time measured by the PIN diode detector is as follows:

$$n_{cr} = A \times d \times \rho \times R_s \times \varepsilon \left(d, E_{th}\right), \quad (1)$$

where n_{cr} is the count rate (number of pulses/s), A is the area of the ^{63}Ni calibration source (cm^2), d is the coating thickness (cm), ρ is the source density (g/cm^3), R_s is the specific radioactivity (Bq/g), ε is the detection probability per decay, and E_{th} is the threshold level (keV).

2.3 | Design for maximum count rate

With the results of the MCNP simulation in Figure 4 and (1), the radiation dose of the coating source and the estimated count rate for each specific radioactivity are presented in Table 2. Here, the *radiation dose* is the total amount of radiation calculated from the mass of the coated beta source, and the *detection probability* is the probability that radiation will be detected by the PIN diode. Hence, the *count rate* is the *radiation dose* multiplied by the *detection probability*.

For example, if you want to obtain a count rate of 3 Mcps, we can calculate the size of the source according to the coating thickness and the specific radioactivity of source. When the specific radioactivity is 0.1 Ci/g and the coating thickness

TABLE 2 Estimated count rate according to the coating source

Coating source				
Source area (mm^2)	**Coating thickness (μm)**	**Radiation dose (Bq)**	**Detection probability (%)**	**Count rate (pps)**
1	0.2	5.92×10^3	33.0	1.95×10^3
	0.6	1.78×10^4	22.3	3.95×10^3
	1.0	2.96×10^4	16.8	4.97×10^3
	2.0	5.92×10^4	10.2	6.02×10^3
2	0.2	1.18×10^4	33.0	3.91×10^3
	0.6	3.55×10^4	22.3	7.90×10^3
	1.0	5.92×10^4	16.8	9.95×10^3
	2.0	1.18×10^5	10.2	1.20×10^4
3	0.2	1.78×10^4	33.0	5.86×10^3
	0.6	5.33×10^4	22.3	1.19×10^4
	1.0	8.88×10^4	16.8	1.49×10^4
	2.0	1.78×10^5	10.2	1.81×10^4
4	0.2	2.37×10^4	33.0	7.82×10^3
	0.6	7.10×10^4	22.3	1.58×10^4
	1.0	1.18×10^5	16.8	1.99×10^4
	2.0	2.37×10^5	10.2	2.41×10^4
5	0.2	2.96×10^4	33.0	9.77×10^3
	0.6	8.88×10^4	22.3	1.98×10^4
	1.0	1.48×10^5	16.8	2.49×10^4
	2.0	2.96×10^5	10.2	3.01×10^4
10	0.2	5.92×10^4	33.0	1.95×10^4
	0.6	1.78×10^5	22.3	3.95×10^4
	1.0	2.96×10^5	16.8	4.97×10^4
	2.0	5.92×10^5	10.2	6.02×10^4

is 1 μm, the area of the thin-film source should be 6 mm^2. For a coating thickness of 2 μm, an area of 5 mm^2 should be used. Since the specific radioactivity of our ^{63}Ni solution is 12 Ci/g, the source area should be reduced to 0.05 mm^2 if used undiluted. This would be too small for fabrication. Thus, it must be diluted by adding natural nickel (^{62}Ni). When diluted to 0.2 Ci/g and coated with a thickness of 1 μm, the required area would be 3 mm^2. In order to minimize the noise coming from the diode detector, the window size of the detector should be less than 6 mm^2. Of course, the area of the thin-film beta source must also be smaller than the detector window [16]; therefore, the beta source can be designed according to this guideline.

As stated in Section 1, we intend to use the commercially acceptable maximum radiation dose because a high-radiation dose corresponds to rapid random number generation. This means using a larger beta source. However, a larger beta source results in a higher noise level. Therefore, it is desirable to use a small-area source as an array element. The regulatory exemption dose for ^{63}Ni is 100 MBq. If 128 array elements are used, the radiation dose of one array element is 100 MBq/128 = 780 kBq/element. The plating thickness in our electroplating device is about 2 μm, and the detection probability for this thickness is 10%, as shown in Figure 4. Therefore, about 78 kBq/element can be detected by the PIN diode detector. Further, the pulse generation rate at the output of detection circuit would be about 6.3×10^4 pps (pulses per second), taking into account the loss of 20% due to the dead time, baseline shift, and additive noise. If all 128 source array elements are used, the total pulse rate is about 8 Mpps.

3 | DETECTION CIRCUIT

3.1 | Beta radiation detection module

This section discusses the development of an analog circuit for beta radiation detection, where a commercial PIN diode and other chip parts are used. In the detection circuit, the detection of beta radiation in the high-energy region is not difficult, and the frequency of occurrence is low. Therefore, it should be designed to detect beta radiation in the lowest energy region possible. For this, a noise analysis of the detection circuit is required. First, the noise levels for three commercial PIN diodes were calculated and are listed in Table 3. The detection circuit was designed to detect all radiation with an energy above these noise levels. When the upper limit on the noise was set to 5 keV, the feedback resistor was adjusted so that the noise generated by the PIN diode and preamplifier circuit was 5 keV or less.

Fortunately, we found an equation for calculating the total noise of the radiation detector in [13,14,17]. The *delta noise* is affected by the diode capacitance, and the *step noise* is affected by both the dark current of the diode and the feedback currents of the preamplifier. The combined root mean square (RMS) noise from these two contributions determines the maximum noise level. There is less noise as the capacitance of the PIN diode, the reverse leakage current of the PIN diode, and the leakage current of the FET become smaller. Less noise is reduced when the feedback resistance and transconductance of the field-effect transistor (FET) are greater. For the commercial PIN diodes, the overall noise levels are 5.1 keV, 5.3 keV, and 7.3 keV for the S1223, S1223-01, and S3590-09 diodes. In order to reduce the noise to 5 keV or less, it is important to design the detection diode to have a capacitance and leakage current equal to or less than the specifications of the S1223 diode. These factors are related to the size and bias voltage of the PIN diode. As the diode area increases, the capacitance and leakage current increase. As the bias voltage increases, the capacitance decreases, and the leakage

TABLE 3 Noise levels of commercial PIN diodes

	S1223	S1223-1	S3590-09		Hamamatsu PIN diodes
Size	2.4 × 2.8	3.6 × 3.6	10 × 10	mm^2	Sensing area of PIN diode
τ	4	4	4	μs	Pulse-shaping time constant
C	10	20	40	pF	Total input capacitance
R	300	300	300	MΩ	Feedback resistance
I_d	0.1	0.2	2	nA	Dark current at a reverse 50 V
I_f	2.0	2.0	2.0	nA	Leakage current of SK152 FET
I_s	0.17	0.17	0.17	nA	Noise current ($2kT/qR$)
I	2.3	2.4	4.2	nA	$I = I_d + I_f + I_s$
g_m	20	20	20	mS	Transconductance of SK152
E_d	102	205	409	eV	Delta noise
E_s	866	885	1,174	eV	Step noise
E_n	872	908	1,243	eV	RMS noise (σ)
N_{max}	5.14	5.35	7.32	keV	$N_{max} = (5/2) \times \text{FWHM}$, FWHM ≈ 2.355σ

$E_d \cong 2\left(\frac{kT}{g_m \tau}\right)^{1/2} \frac{\epsilon_{eh}}{q} C \quad E_S \cong \epsilon_{eh}\sqrt{(\tau I)/q} \quad E_n = \sqrt{E_s^2 + E_d^2}$

current increases. Therefore, it is necessary to develop a PIN diode with an area of 6 mm^2 or less, which is smaller than that of the S1223 diode.

A PIN diode is a device that increases the detection sensitivity by increasing the number of carriers reacting to photons and radiation by widening the depletion layer of a PN diode. A PIN diode absorbs the energy of beta particles emitted from the ^{63}Ni source, creating an electron-hole pair (EHP), a charge carrier. This charge carrier causes charge to flow over a short period owing to the diode's reverse bias. The following charge-sensitive amplifier (CSA) is used to convert the short-term flow of charge in the PIN diode into a voltage proportional to the amount of charge input. The input charge generates a voltage by accumulating charge in the parasitic capacitance of the detection element and the feedback capacitance of the operational amplifier (OPAMP) and then discharges it through the feedback resistor of the OPAMP to generate a kind of voltage pulse. However, since the energy of ^{63}Ni beta radiation is low, the voltage pulse output from the CSA is very weak. Thus, a second amplifier was added to the preamplifier stage.

Figure 5 shows the beta radiation detection module including the beta source, the PIN diode, the preamplifier, and other analog signal processing circuitry. The amplified signal is a long-tailed sawtooth waveform that rapidly rises and then slowly falls. When beta particles are continuously released for a short period of time, the long tail of the preceding detected signal interferes with the detection of beta particles released later. In the field of radiation measurement, the time over which particles emitted later are not detected is called the *dead time*. Depending on the type of measurement device (semiconductor- or gas-type), detection may be weak or not at all during the dead time. Therefore, it is necessary to use a pulse-shaping circuit that converts a long-tailed waveform into a short bell-shaped pulse. This can be solved simply with differentiator and integrator circuits. Differentiators are used to emphasize the rapid rise of a voltage. However, because the rising period is too short, an integrator circuit is used to create a pulse with a finite width.

The last part of the analog signal processing circuits is the pulse discriminator. It is a circuit that outputs the actual entropy signal to be used for random number conversion. In this paper, we utilize the timing of radioactive decay to obtain a random number. Hence, a pulse stream with a constant voltage level [transistor-transistor logic (TTL) level] is output in accordance with the decay time. To this end, the pulse discriminator outputs a rectangular waveform with a TTL level when a signal above the reference voltage level is incoming. However, the pulse width is widened and narrowed when

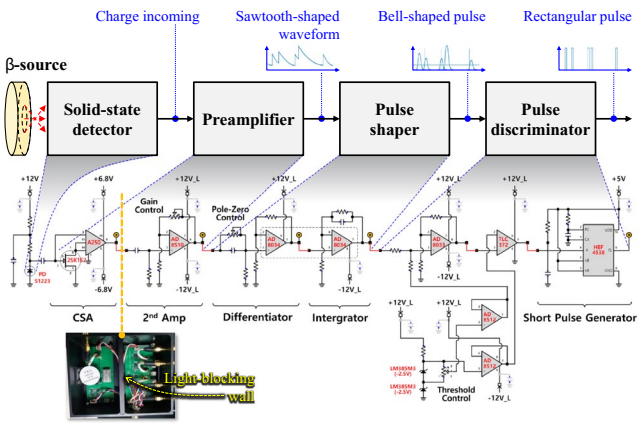


FIGURE 5 Beta radiation detection module

the voltage of the input signal to the discriminator is high and low, respectively. Monostable multivibrators are used to output pulses of constant width. Figure 6 shows the signal output from the preamplifier (sawtooth waveform) and the pulse train at the output end of the detection board when beta radiation occurs.

3.2 | Integrated circuit design

In the previous section, we watched the detected pulse output by integrating a ^{63}Ni beta source, a commercial PIN diode, and the analog circuits implemented at the board level. This result provides functional requirements for the analog block for our RNG. Analog ICs are designed to meet functional requirements and are optimized using components from the 0.18-μm complementary metal-oxide-semiconductor (CMOS) library. Figure 7 shows the functional block diagram of an analog IC. A direct current (DC)-coupled CSA structure is used instead of the alternating current (AC)-coupled CSA for IC design [18]. This can make the CSA input circuit simpler, but it was adjusted using an external voltage, V_{COM}, since there is a DC offset at the output [19]. The anode of the PIN diode is directly connected to the negative input of the OPAMP in the CSA circuit, and the cathode of the PIN diode is connected to the external reverse voltage V_H. Of the EHP charges generated by ^{63}Ni beta radiation, electrons move to the V_H terminal, and holes move to the OPAMP's negative input port.

If there is no feedback resistor in the CSA circuit, it operates like an integrator and maintains the signal voltage V_{OUT}. In this case, as shown in Figure 8, the output of the preamplifier is proportional to the signal charge Q and inversely proportional to the feedback capacitor C_f. That is, the charge gain is $1/C_f$.

$$V_{OUT} \approx -Q/C_{f.} \tag{2}$$

Here, Q is the signal charge generated by the beta particles in the PIN diode and contributes to the current entering the input of the OPAMP.

If we connect a feedback resistor R_f in parallel with the CSA circuit, then the CSA output signal has a time constant of $\tau = R_f C_f$, and it discharges to the V_{COM} level. The discharge time is faster when R_f is smaller; thus, high-speed detection is possible. In contrast, V_{OUT} is lowered owing to rapid discharge by R_f while integrating the signal charge. If polysilicon is used in the CMOS process as a feedback resistor, some parasitic capacitance exists between the polysilicon and p-type substrate. Because of this, we used a p-type metal-oxide-semiconductor (PMOS) transistor as a feedback resistor. Table 4 summarizes the corner simulation results for the CSA output according to process, voltage, and temperature (PVT) variations when a circuit that applies a stable DC voltage to the gate of the PMOS transistor is used. The minimum and maximum signal voltages of the CSA output signal are 79 mV and 105 mV, respectively.

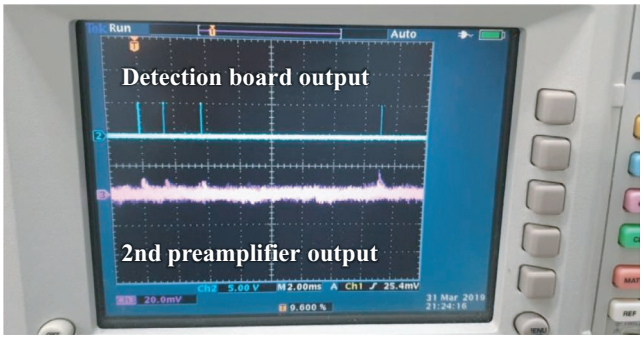


FIGURE 6 Detection signal and output pulses

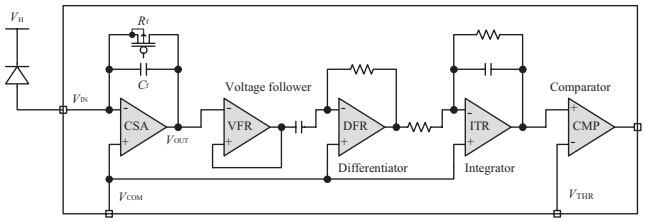


FIGURE 7 Block diagram of the analog integrated circuit

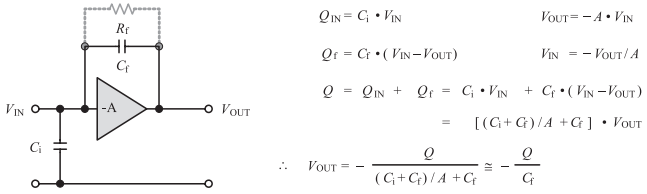


FIGURE 8 Charge gain in the CSA with only C_f

Figure 9 shows the carrier current waveform modeled by the equivalent circuit of a Si photodiode and the simulation results for the change in the CSA output according to PVT variations. It shows the signal for each corner simulation condition according to the MOS transistor model parameters (SS/SF/TT/FS/FF), VDD (4.5/5/5.5 V), and temperature (–40/25/85°C). Here, the magnitude of the CSA output voltage refers to a voltage that drops by approximately ΔV from the V_{COM} level by integrating the input charge generated by the PIN diode.

The simulation results for the subsequent differentiator, integrator, and comparator outputs are shown in Figure 10.

The corner simulation results for the pulse width at the comparator output are listed in Table 5.

Figure 11 shows an image of the layout of a CMOS silicon die for the radiation detection circuit designed with a 0.18-μm CMOS process.

This circuit is still in the design phase to verify its functional operation. A system-in-package (SiP) design for IoT devices and an array-type circuit design for a high rate are also in progress.

TABLE 4 Corner simulation results for the CSA output

VDD (V)	TEMP (°C)	SS (mV)	SF (mV)	TT (mV)	FS (mV)	FF (mV)
4.5	–40	90.15	97.82	97.79	97.45	102.96
	25	83.36	90.22	89.86	89.69	94.35
	85	78.67	84.34	83.77	83.41	86.31
5.0	–40	91.16	79.25	98.18	98.31	103.56
	25	84.14	90.57	90.33	90.26	94.81
	85	79.25	84.93	84.18	84.32	87.47
5.5	–40	91.40	99.15	99.02	98.68	104.58
	25	85.05	91.59	90.82	90.87	94.55
	85	80.14	85.18	84.87	84.80	87.88

TABLE 5 Corner simulation for pulse width at comparator

VDD (V)	TEMP (°C)	SS (µs)	SF (µs)	TT (µs)	FS (µs)	FF (µs)
4.5	–40	1.044	0.725	0.715	0.705	0.490
	25	0.980	0.689	0.676	0.668	0.467
	85	0.925	0.653	0.641	0.630	0.444
5.0	–40	1.042	0.719	0.706	0.698	0.484
	25	0.975	0.679	0.669	0.658	0.461
	85	0.914	0.644	0.630	0.624	0.438
5.5	–40	1.028	0.708	0.699	0.690	0.478
	25	0.961	0.671	0.658	0.650	0.452
	85	0.900	0.631	0.620	0.613	0.425

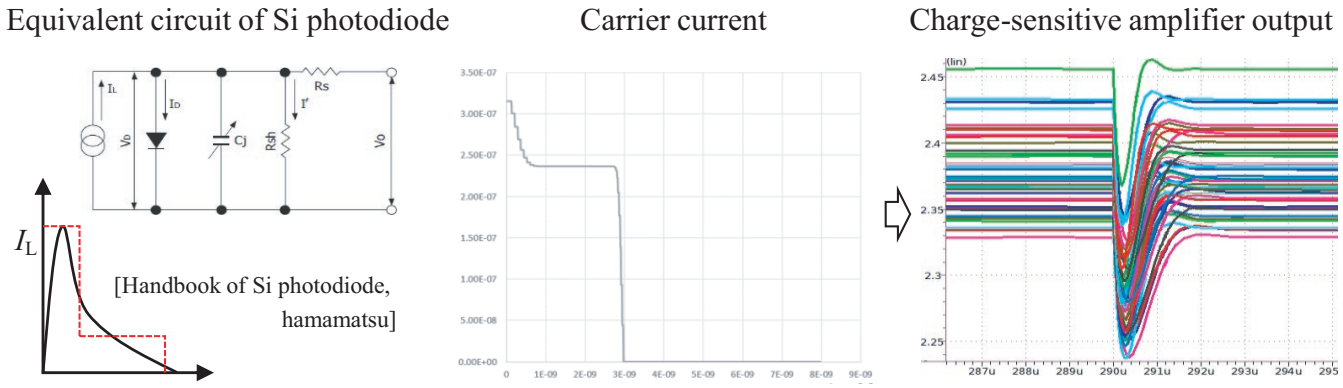


FIGURE 9 Carrier current and CSA output simulation

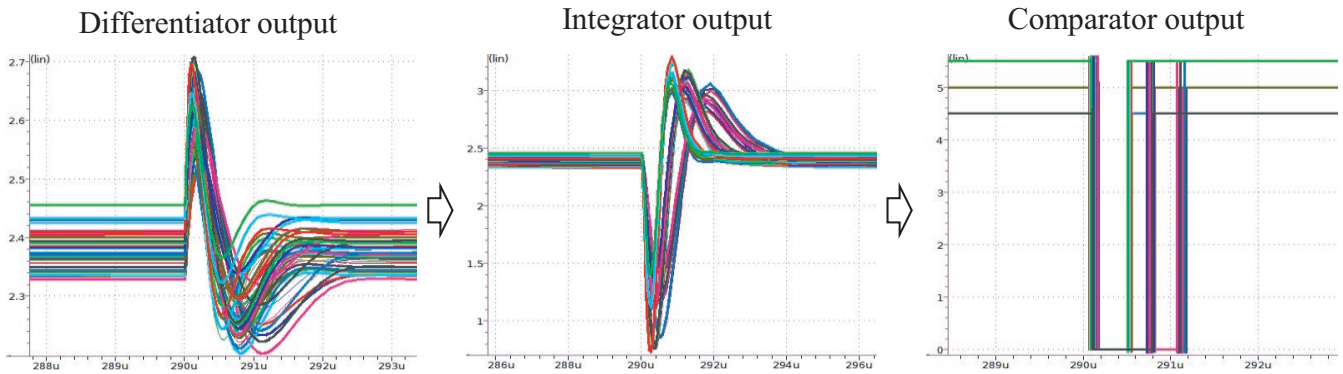


FIGURE 10 Pulse shaper and comparator output simulation

4 | DIGITAL SIGNAL PROCESSING

4.1 | Conversion to a random number

Since the beta radiation detection module provides a TTL-level signal, digital signal processing can be directly performed without an additional separate signal converter. Here, the purpose of digital signal processing is to change the TTL-level pulse train to a random number. To do this, we have used a general-purpose compact data acquisition (cDAQ) device, built-in functions (an internal clock generator and a counter), and LabVIEW, as shown in Figure 12.

The data acquisition device accepts a digital input (TTL-level pulse train) to perform a specific function related to the built-in counter on the rising or falling edge of a pulse. Since counters can be built-in or easily implemented in a data acquisition device or field-programmable gate array (FPGA), these counters are used to collect temporal information from pulse trains.

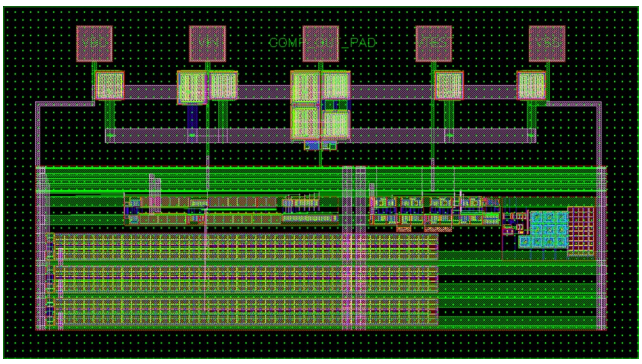


FIGURE 11 Layout of the radiation detection circuits

The first task for conversion to a random number is to read the built-in counter value at the rising edge of a pulse when the beta radiation detection pulse enters the data acquisition device. The built-in counter continues to increase until overflow ($2^{32} - 1$); thus, the incremented counter value is read each time this detection pulse is input. Although the read counter value continues to increase, the increment value is irregular. Therefore, if this counter value is divided by 256 ($=2^8$), then the rest of the values are also irregular. A simple way to find the rest is to use only the eight least significant bits (LSBs) when converting coefficients to binary numbers. The eight bits obtained in this way are one random number and one of the numbers 0 to 255.

4.2 | Random number generation rate

In our experiment, a calibrated beta source of 700 Bq was used. In order to predict the random number generation rate according to the radiation dose of the source, it is necessary to measure the detection rate. To obtain a meaningful random number, it must be adjusted to output only pulses generated by pure beta radiation. Figure 13 shows the pulse output according to the threshold voltage in the pulse discriminator. If the threshold voltage is low, the noise signal is also converted to a random number, which lowers the quality of the random number. Therefore, it plays the role of filtering signals that detect pure beta particles and affects the random number generation rate.

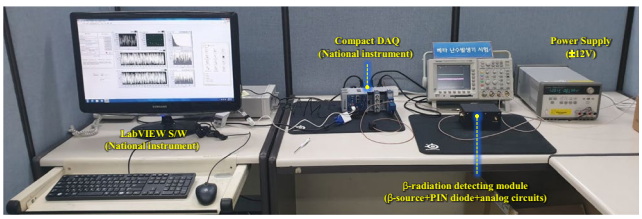


FIGURE 12 Random number generator testbed

The pulse generation rate was measured after adjusting the threshold voltage so that a pulse is generated only when the analog pulse is visible. As the measurement method, the internal counter value of the data acquisition device in Figure 12 was increased by one each time a square-wave pulse was input; then, the change in the counter value was measured. Figure 14 shows the repetition of the changes in the counter value over 10 s, 20 s, 30 s, and 100 s. In the LabVIEW program, we set *while loop time* = 1 s and read the number of pulses every second. The number of pulses every 1, 2, 3, … s was accumulated, and the output stopped when *while loop iteration* = 10 s, 20 s, 30 s, or 100 s. The value was read and recorded. This process was carried out again to restart the counter from zero and repeated 10 times for each time period of 10 s, 20 s, 30 s, or 100 s.

As summarized in Table 6, 20 pps were generated on average. This means that the ratio of detected pulses to total amount of beta radiation is about 2.86% (=20 pulses/700 occurrences of radiation) for a radiation dose of 700 Bq.

The results in Table 7 indicate that the ratio of the detected pulses to total amount of beta radiation rises to 14.3% when the threshold voltage is lowered. However, these detected pulses contain a noise component; therefore, they did not pass a statistical analysis test when converted to random numbers. Of course, the random number data obtained under the conditions in Table 6 passed the test.

The counter used in the experiment is a 32-bit counter, but since it uses only 8 LSBs, it is the same as using an 8-bit counter. Therefore, when an 8-bit counter is operated with a clock of 80 MHz, the counter is reset every 3.2 μs, and the update rate is 312.5 kHz. Since this is much faster than the pulse rates in Tables 6 and 7, it ensures the independence of the counter values read per pulse.

5 | STATISTICAL ANALYSIS

5.1 | Uniform distribution of random number data

For statistical analysis, 1 048 576 bytes of random number data were collected. One byte, 8 bits means a number in 0 to 255. Figure 15 shows the uniform distribution of the collected random number data. This is the distribution of how many times each number from 0 to 255 was generated. The average value of this distribution is exactly 4096 (up to 20 significant digits). The standard deviation is 65.1, and (standard deviation)/(average) = 1.59%, indicating a very stable and even probability for random number generation.

Figure 16 shows the constellation of random numbers in the order of the output. The first 1,024 random numbers are plotted in the graph. They seem to be irregular and

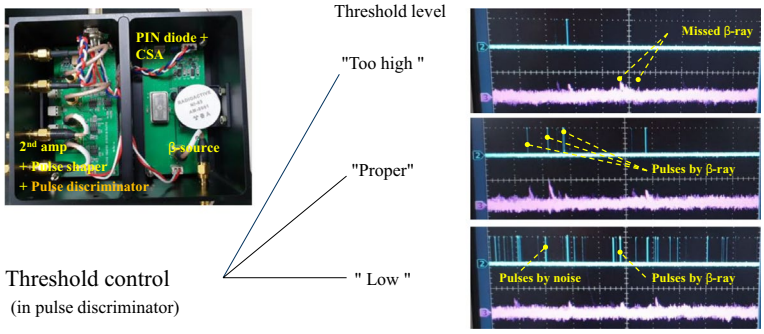


FIGURE 13 Pulse train according to the threshold of the discriminator

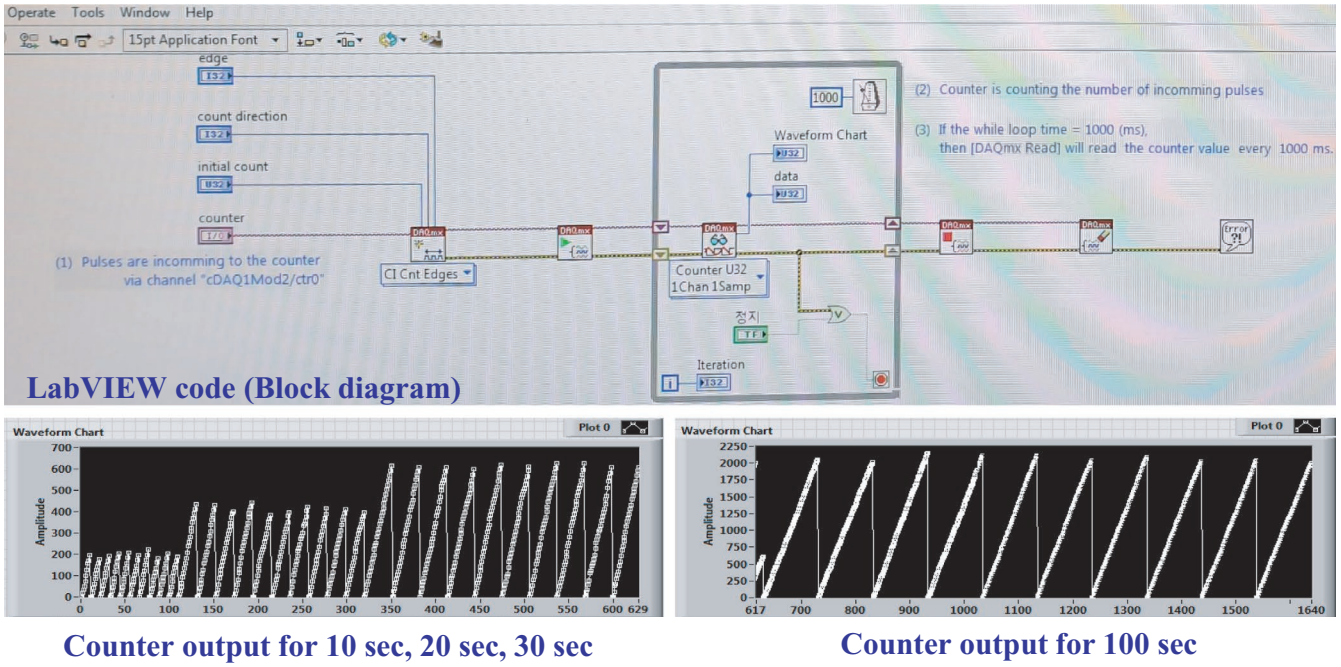


FIGURE 14 Counter value during periods of 10 s, 20 s, 30 s, 100 s

TABLE 6 Average number of pulses at a 2.86% detection rate

Counting Period =		10 s	20 s	30 s	100 s
Counter value after 10 s, 20 s, 30 s, or 100 s					
At 1st	Measure	198	433	616	2058
At 2nd	Measure	178	429	608	2010
At 3rd	Measure	191	400	607	2153
At 4th	Measure	204	443	601	2118
At 5th	Measure	208	385	621	2112
At 6th	Measure	196	397	613	2041
At 7th	Measure	224	424	626	2091
At 8th	Measure	181	414	628	2032
At 9 th	Measure	204	410	607	2044
At 10th	Measure	190	398	609	1999
Average		197.4	413.3	613.6	2065.8
Standard deviation		12.85	17.66	8.49	47.92
Standard deviation/ average (%)		6.5	4.3	1.4	2.3
Pulse rate (s^{-1})		19.7	20.7	20.5	20.7

inclined. Numbers from 0 to 255 occur irregularly, and there is no tendency for specific numbers to occur more or less.

When 1 048 576 random numbers are plotted in a graph, it appears to have been colored in a solid color, as shown in Figure 17. If there is a specific pattern or bias in the random number data, the pattern can be identified by color, as shown in Figure 18. This means that the random numbers are incomplete.

5.2 | Test using NIST Standards

The National Institute of Standards and Technology (NIST) standards related to random number testing are NIST SP 800-90B [20] and NIST SP 800-22 [21]. Briefly, as shown in Figure 19, NIST SP 800-90B is a standard for testing entropy sources, and NIST SP 800-22 is a standard for testing RNGs used in cryptographic modules.

Figure 20 shows that our RNG can be used for two purposes: an entropy source and random number generation

TABLE 7 Average number of pulses at a 14.3% detection rate

Counting Period =		10 s	20 s	30 s	100 s
Counter value after 10 s, 20 s, 30 s, or 100 s					
At 1st	Measure	975	2143	3006	6227
At 2nd	Measure	1029	2024	3069	6142
At 3rd	Measure	928	2049	3056	6098
At 4th	Measure	1041	1985	2967	5957
At 5th	Measure	939	2001	3071	6223
At 6th	Measure	995	2042	2967	6032
At 7th	Measure	999	2080	2947	6224
At 8th	Measure	1015	2082	3079	5983
At 9 th	Measure	985	1939	3057	6147
At 10th	Measure	1039	1971	2979	6220
Average		994.5	2031.6	3019.8	6125.3
Standard deviation		37.08	57.55	48.96	98.68
Standard deviation/ average (%)		3.7	2.8	1.6	1.6
Pulse rate (s^{-1})		99.5	101.6	100.7	102.1

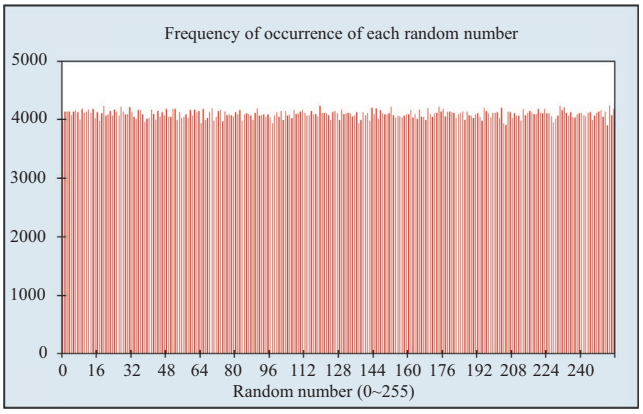


FIGURE 15 Frequency of occurrence of each random number

for cryptographic modules. This is because an RNG using beta radiation can generate random numbers as fast as a PRNG.

NIST SP 800-90B verifies the randomness of the hardware entropy itself. There are three verification items: independent and identically distributed (IID), non-IID, and restart tests. Figure 21 shows a diagram of the test procedure.

This test was performed on 1000000 pieces of data in a Python-based Linux environment. There are dataset requirements.

- Continuous data set: 1 000 000 consecutive pieces of data from a noise source.
- Restart data set: 1000 restarts and 1000 samples; all three tests passed.

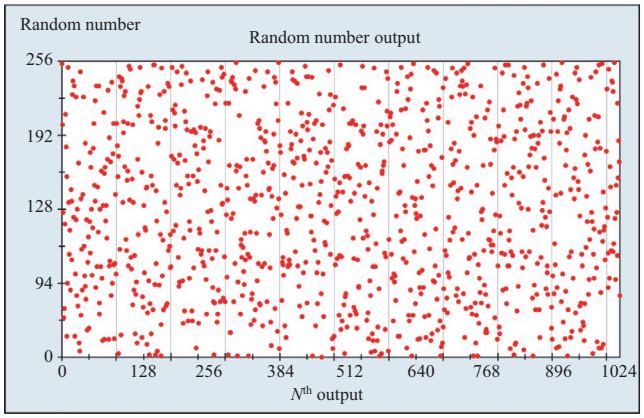


FIGURE 16 First 1,024 random numbers

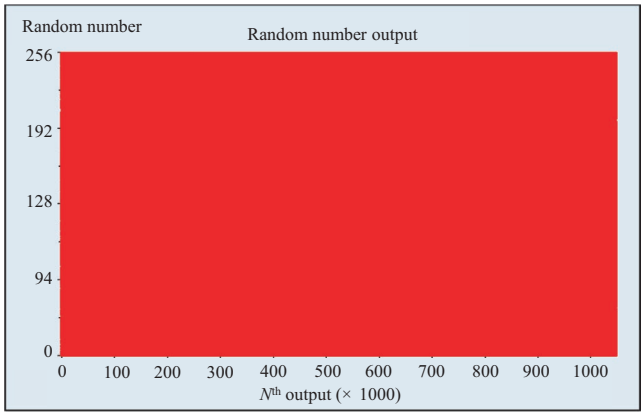


FIGURE 17 All 1048576 random numbers

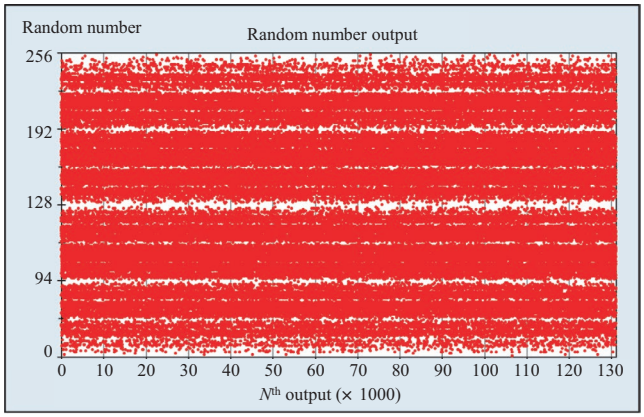


FIGURE 18 Example of incomplete random number data

Our random number data passed all three tests of NIST SP 800-90B according to Figure 22. The minimum entropy was 7.9 for an 8 bits dataset and 5.8 for a 6 bits dataset. These results indicate that our beta radiation RNG is a very good entropy source.

NIST SP 800-22 checks the random numbers output from a PRNG that uses hardware entropy as a seed. This standard verifies the statistical randomness of random bits that will be used in a cryptographic module. NIST SP 800-22 has 15

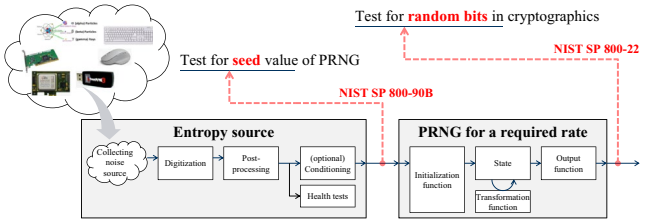


FIGURE 19 NIST SP 800-90B and NIST SP 800-22

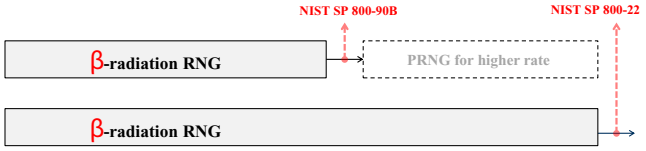


FIGURE 20 Beta radiation RNG for NIST SP 800-90B and −22

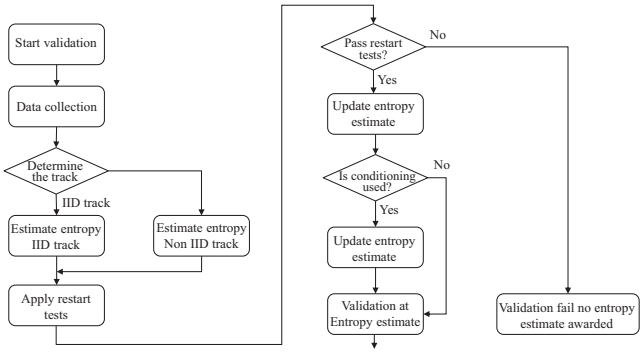


FIGURE 21 Test procedure for NIST SP 800-90B

statistical test items, as shown in Figure 23. We passed all 15 tests. Thus, our beta radiation-based RNG can be directly used in cryptographic modules without a PRNG.

In order to use a beta radiation-based RNG instead of a PRNG, an intermediate device that outputs random bits at a constant speed is required. This can be done by providing an interface that acts as a buffer to match the required random number generation speed and random length.

6 | CONCLUSION

We have introduced a lightweight true RNG (TRNG) consisting of a thin-film beta radiation source and an IC. The most important technology in this paper is an analog circuit design that can detect beta radiation with a very low energy. Analog circuits proven at the board level will soon be replaced by ICs to be designed. The next significant technology is the development of the world's first RNG using beta radiation. This technology includes a beta source, a PIN diode detector, an analog signal processing circuit, a random number conversion algorithm, and random number analysis technology. It was demonstrated that our device generates perfect random numbers through international standard tests.

At the beginning of this paper, we emphasized that this technique is a lightweight TRNG for IoT devices. This is based on making proven board-level analog circuits into ICs. Moreover, it is not very difficult to develop an IC with current

```
[etri:/user/smpark/proj2019/TRNG/SP800-90B_EntropyAssessment-master] ./run_iid
reading 1000000 bytes of data
Read in file /user/smpark/proj2019/TRNG/dataconv/0311/TRNG_1M_0311_8.bin, 1000
Dataset: 1000000 8-bit symbols, 256 symbols in alphabet.
Output symbol values: min = 0, max = 255

Calculating statistics on original sequence
Calculating statistics on permuted sequences
permutation tests:      99.99 percent complete
                 statistic  C[i][0]  C[i][1]
-----------------------------------------------
                 excursion     5991        0
       numDirectionalRuns      467        0
       lenDirectionalRuns     3907     6034
   numIncreasesDecreases     4062       10
            numRunsMedian      329        2
            lenRunsMedian      291      290
             avgCollision     5263        1
             maxCollision     5333     1147
            periodicity(1)      999       37
            periodicity(2)     7733       41
            periodicity(8)     3006       62
           periodicity(16)     7769       47
           periodicity(32)     8521       41
             covariance(1)     9615        0
             covariance(2)     2358        0
             covariance(8)     1181        0
            covariance(16)     6061        0
            covariance(32)     1185        0
               compression     2921       13
(* denotes failed test)
** Passed IID permutation tests

Chi square independence
        score = 64936.1, degrees of freedom = 65535, cut-off = 66659.4
** Passed chi-square independence test

Chi square goodness-of-fit
        score = 2340.71, degrees of freedom = 2295 cut-off = 2510.06
** Passed chi-square goodness-of-fit test

** Passed chi square tests

LRS test
        W: 4, Pr(E>=1): 1.000000
** Passed LRS test

IID = True
min-entropy = 7.88898
```

(A)

```
[etri:/user/smpark/proj2019/TRNG/SP800-90B_EntropyAssessment-master] ./run_non
reading 1000000 bytes of data
Read in file /user/smpark/proj2019/TRNG/dataconv/0311/TRNG_1M_0311_8.bin, 1000
Dataset: 1000000 8-bit symbols, 256 symbols in alphabet.
Output symbol values: min = 0, max = 255

Running entropic statistic estimates:
- Most Common Value Estimate: p(max) = 0.0042187, min-entropy = 7.88898
- Collision Estimate: p(max) = 0.011426, min-entropy = 6.45153
- Markov Estimate (map 6 bits): p(max) = 6.79845e-223, min-entropy = 5.76582
- Compression Estimate: p(max) = 0.00945395, min-entropy = 6.72487
- t-Tuple Estimate: p(max) = 0.00608277, min-entropy = 7.36106
- LRS Estimate: p(max) = 0.00391021, min-entropy = 7.99854

Running predictor estimates:
Computing MultiMCW Prediction Estimate: 100 percent complete
        Pglobal: 0.004161
        Plocal: 0.002136
MultiMCW Prediction Estimate: p(max) = 0.00416082, min-entropy = 7.90892

Computing Lag Prediction Estimate: 100 percent complete
        Pglobal: 0.004080
        Plocal: 0.010010
Lag Prediction Estimate: p(max) = 0.0100098, min-entropy = 6.64245

Computing MultiMMC Prediction Estimate: 100 percent complete
        Pglobal: 0.004049
        Plocal: 0.002136
MultiMMC Prediction Estimate: p(max) = 0.00404934, min-entropy = 7.9481

Computing LZ78Y Prediction Estimate: 100 percent complete
        Pglobal: 0.004049
        Plocal: 0.002136
LZ78Y Prediction Estimate: p(max) = 0.0040494, min-entropy = 7.94808
----------------------
min-entropy = 5.76582
```

(B)

```
[etri:/user/smpark/proj2019/TRNG/SP800-90B_EntropyAssessment-master] ./run_res
reading 1000000 bytes of data
Read in file /user/smpark/proj2019/TRNG/dataconv/0311/TRNG_1M_0311_8.bin, 1000
Dataset: 1000000 8-bit symbols, 256 symbols in alphabet.
Output symbol values: min = 0, max = 255

Running sanity check on row dataset:
- F_R: 16
Running sanity check on column dataset:
- F_C: 16
U: 42.232907
Passed the restart tests
*** Final entropy estimate: 5.765820
```

(C)

FIGURE 22 NIST SP 800-90B test results: pass/fail result, *p*-value, and minimum entropy value (A) IID test, (B) non-IID test, and (C) restart test results

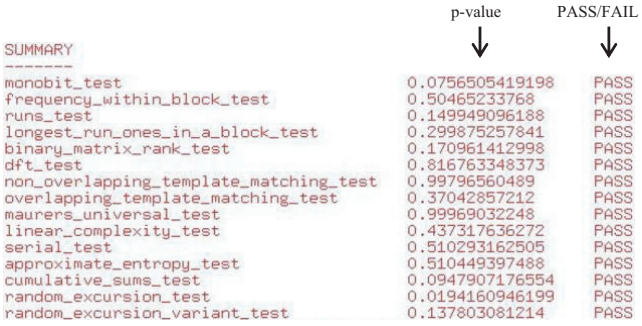


FIGURE 23 NIST SP 800-22 test results: p-value and pass/fail results

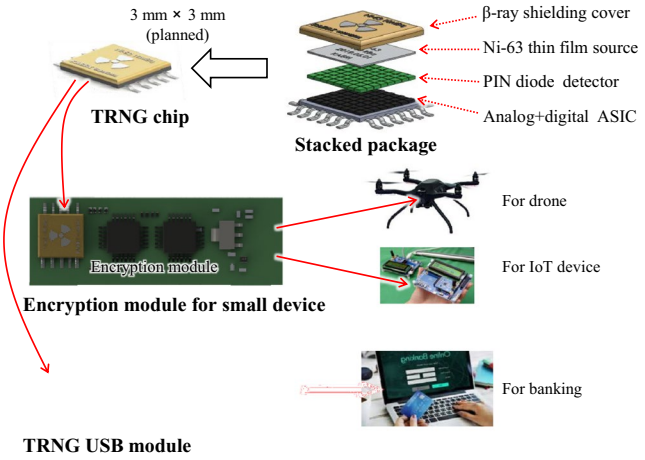


FIGURE 24 Beta radiation based TRNG chip and its applications

design technology. Therefore, the design specifications of ICs that can match the beta source and diode detector well are important. As shown in Figure 24, a small package design for IoT devices and an array-type circuit design for faster random number generation are also in progress. The coating source, a PIN diode detector, and an ASIC will be package in a TRNG chip. Since the self-made coating source and self-made PIN diode detector are very small (about 1×1 mm^2), it would be possible to make 3×3 mm^2 TRNG chip at most. This TRNG chip can be mounted on the security module of small devices like the drones or IoT devices, and can be carried by individuals in the form of USB for banking or authentication.

Looking at recent papers on TRNG for IoT applications [22,23], it emphasizes that it must be low power in hardware and pass statistical quality tests in accordance with NIST standards. Recently, a physically unclonable function (PUF), a kind of hardware-based RNG, has been widely used to secure IoT devices. A PUF has unpredictable and physically nonreplicable properties but its irregularities and statistical properties have not been verified for use as an entropy source or cryptographic modules, respectively.

In conclusion, we can say that the RNG introduced in this paper has three advantages. First, it is most suitable for ultra-small RNGs because of its relatively simple structure, low-cost elements and materials, and small volume. Second, since it is an entropy source based on quantum mechanics, it generates almost perfect random numbers, which is verified by NIST test. Third, the problem of a low-generation rate, which is the biggest drawback of existing TRNGs, was solved.

ORCID

Kyunghwan Park https://orcid.org/0000-0001-9852-6155
Seongmo Park https://orcid.org/0000-0001-8656-9094
Taewook Kang https://orcid.org/0000-0001-9147-3898
Young-Hee Kim https://orcid.org/0000-0002-2541-9276

REFERENCES

1. M. N. Hera et al., *Randomness in quantum mechanics: philosophy, physics and technology*, Rep. Prog. Phys. **80** (2017), 2–26.
2. A. Ananthaswamy, *How to Turn a Quantum Computer into the Ultimate Randomness Generator*, Quanta Magainge, June 19, 2019, https://www.quantamagazine.org/how-to-turn-a-quantum-computer-into-the-ultimate-randomness-generator-20190619/
3. C. H. Holbrow, E. Galvez, and M. E. Parks, *Photon quantum mechanics and beam splitters*, Am. J. Phys. **70** (2002), 260–265.
4. H. Schmidt, *Quantum-mechanical random-number generator*, J. Appl. Phys. **41** (1970), 462–468.
5. H. Schmidt, *A quantum mechanical random number generator for psi tests*, J. Parapsychol. **34** (1970), 219–224.
6. D. Rüschen et al., *Generation of True Random Numbers Based on Radioactive Decay*, in Proc. Int. Student Conf. Electr. Eng. (Prague, Czech Rep.), May 2017, pp. 1–4.
7. M. Rohe, *RANDy – A True Random Generator Based on Radioactive Decay*, Dissertation, Saarland Univ. 2003.
8. J. Walker, *Hotbits*, 2003, Available at: http://www.fourmilab.ch/hotbits/
9. A. Figotin et al., *Random Number Generator Based on the Spotaneous Alpha-Decay*, U.S. Patent Appl. No.: 10/127,221, 2003.
10. M. Gude, *Ein quasi-idealer Gleichverteilungsgenerator basierend auf physikalischen Zufallsphanomenen*, Ph.D thesis, RWTH Aachen (1987).
11. C. H. Vincent, *The generation of truly random binary numbers*, J. Phys. E: Sci. Instrum. **3** (1970), 594–598.
12. Korea NSSC Regulation, *Regulation on Materials, etc. Excluded from Radioisotopes,* Notice No.2013-34, Jan. 2012, Available at: www.nssc.go.kr
13. W. R. Wampler and B. L. Doyle, *Low-energy beta spectroscopy using pin diodes to monitor tritium surface contamination*, Nuclear Instrum. Meth. Phys. Res. A **349** (1994), 473–480.
14. M. Culcer et al., *Tritium Contaminated Surface Monitoring with a Solid-State Device*, in Proc. Int. Conf. Nuclear Energy New Eur. (Portoroz, Slovenia), Sept. 2004, pp. 713:1–6.
15. T. Kang et al., *Evaluation of a betavoltaic energy converter supporting scalable modular structure*, ETRI J. **41** (2014), 254–261.
16. G. F. Knoll, *Radiation detection and measurement* 3rd ed., John Wiley & Sons Inc., 2000.

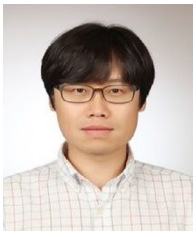
17. M. Iliescu et al., *Tritium Detector Behaviour at Low Temperatures*, in Proc. Int. Conf. Nuclear Energy New Eur. (Portoroz, Slovenia), Sept. 2004, pp. 714:1–4.
18. P. J. Windpassinger et al., *Ultra low-noise differential ac-coupled photodetector for sensitive pulse detection applications*, Meas. Sci. Technol. **20** (2009), 1–7.
19. Solid State Division Technical Information, *Characteristics and Use of Charge Amplifier*, HAMAMATSU, Vol. October 2001.
20. NIST SP 800-90B, *Recommendation for the Entropy Sources Used for Random Bit Generation*, 2016.
21. NIST SP 800-22, *A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications*, 2010.
22. J. C. Hsueh and V. H. Chen, *An ultra-low voltage chaos-based true random number generator for IoT applications*, Microelectronics J. **87** (2019), 55–64.
23. M. Crujic et al., *INVITED: Design Principles for True Random Number Generators for Security Applications*, in Proc. Design Autom. Conf. (Las Vegas, NV, USA), June 2019, pp. 1–3.

AUTHOR BIOGRAPHIES

Kyung-Hwan Park received the MS and PhD degrees in electrical and electronic engineering from Korea Advanced Institute of Science and Technology, Daejeon, Korea, in 1993 and 1997, respectively. From 1997 through 2000, he worked at DACOM R&D Center, Daejeon Korea. Since January 2001, he has been with the Electronics and Telecommunications Research Institute, Daejeon, Korea as a Principal Member of Engineering Staff. His research interests include RF/Analog IC for wireless communications, RFID chips, radiation detection circuits, and random number generators based on radiation and betavoltaic battery.

Seong-Mo Park received the BS, MS, and PhD degrees in electronic engineering from Kyungpook University, Taegu, Korea, in 1985, 1987, and 2006, respectively. He joined the Electronics and Telecommunications Research Institute (ETRI), Daejeon, Korea, in 1992. He worked at Multi-Format Multimedia SoC based on MPCore Platform as a team leader. He received Marquis Who's Who 2014 –2017 Achievement Award, the IBC Cambridge "2000 Outstanding Intellectuals of the 21st Century 2016" Achievement Award, and the 2017 Albert Nelson Marquis Lifetime Achievement Award. He is currently working as a project member on neuromorphic SoC design and the development of a true random number generator device. He is a senior member of IEEE, a principal member of the engineering staff at ETRI, and a professor of UST. His interests include machine learning algorithms, neuromorphic architecture design, video compression algorithms, SoC architecture design, and true random number generator devices based on betavoltaic battery.

Byoung-Gun Choi received the BS degree in electronic engineering from Yeungnam University in 1995 and the MS and PhD degrees from the Information and Communications University (ICU) in 2000 and 2005, respectively. He was with Samsung Electronics Co. as a semiconductor engineer from 1995 to 1996. His research interests include betavoltaic battery technology and semiconductor devices. Since 2005, he has been with the Electronics and Telecommunications Research Institute, Daejeon, Republic of Korea, where he is currently a Principal Researcher.



Tae-Wook Kang was born in Daejeon, Korea, in May 1980. He received the BS and MS degrees in electrical engineering from Pohang University of Science and Technology (POSTECH), Pohang, Korea, in 2005 and 2007, respectively. Since February 2007, he has been with the Electronics and Telecommunications Research Institute (ETRI), Daejeon, Korea, where he is currently a Senior Researcher. He has been primarily studying human body communications. His research interests include communication systems, radio channel modeling, and power management of energy harvesting systems.

Jong-Bum Kim received the MS degree in electrical engineering from ChungNam National University and the PhD degree in nuclear and quantum engineering from Korea Advanced Institute of Science and Technology, Daejeon, Korea, in 2000 and 2011, respectively. Since January 2000, he has been with the Korea Atomic Energy Research Institute, Daejeon, Korea as a Principal Researcher. His research interests include radioisotope application, radiation measurement, and quantum random number generator.

Young-Hee Kim received the B.S. degree from Kyoung-Pook National University, Daegu, Korea, in 1989, the M.S. and Ph.D. degrees in electrical engineering from Pohang University of Science and Technology (POSTECH), Pohang, Korea, in 1997 and 2000, respectively. In 1989 he joined the Memory Research and Development Division, Hyundai Electronics Industries, Ltd., Icheon, Korea. From 1989 to 2001, he worked on the design of 4M, 16M, 64M and 256M DRAM chips. In 2001, he joined the faculty of Electronic Engineering, Changwon National University, Changwon, Korea. His research interests are designs of 1T-SRAM IPs, non-volatile memory IPs, high-speed I/O interfaces, x-ray CMOS image sensors, and analog ICs.

Hong-Zhou Jin received the B.S. degree in communication engineering from Yanbian University, Yanbian, China, in 2017. His research interests are non-volatile memory IPs received the B.S. degree in communication engineering from Yanbian University, Yanbian, China, in 2017. His research interests are non-volatile memory IPs.