SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

March 2026, Vol. 69, Iss. 3, 132404:1–132404:9
https://doi.org/10.1007/s11432-025-4626-6

Quaternary true random number generator comprising gated p^+–i–n^+ diodes

Hyojoo HEO[1], Yunwoo SHIN[1], Juhee JEON[1], Taeho PARK[1], Seungho RYU[2], Kyoungah CHO[1*] & Sangsig KIM[1,2*]

[1]*Department of Electrical Engineering, Korea University, Seoul 02841, Republic of Korea*
[2]*Department of Semiconductor System Engineering, Korea University, Seoul 02841, Republic of Korea*

Received 19 May 2025/Revised 17 July 2025/Accepted 15 October 2025/Published online 20 January 2026

Abstract Hardware-based true random number generators (TRNGs) have emerged as the basic unit of multivalued cryptographic systems that can significantly contribute to security technologies by lowering the risk of hacking. In this study, we propose a quaternary true random number generator (Q-TRNG) by connecting three binary true random number generators (B-TRNGs) without auxiliary circuits. The B-TRNGs are constructed using gated p^+–i–n^+ diodes with latch-up voltage variations owing to the inherent stochasticity of the band modulation mechanism. Owing to the inherent stochasticity of the gated p^+–i–n^+ diode, the Q-TRNG generates quaternary random numbers with four distinct current levels, corresponding to digit '0', '1', '2', and '3'. We demonstrate image encryption and decryption using the quaternary sequences. This study paves the way for multinary TRNGs contributing to the development of high-level hardware security technologies for edge devices.

Keywords quaternary true random number generator, gated p^+–i–n^+ diode, quaternary secret key, image encryption, data density

Citation Heo H, Shin Y, Jeon J, et al. Quaternary true random number generator comprising gated p^+–i–n^+ diodes. Sci China Inf Sci, 2026, 69(3): 132404, https://doi.org/10.1007/s11432-025-4626-6

1 Introduction

Random number generators (RNGs) are essential for securing stored information and encrypting data transmission in communication systems, thereby serving as key components in Internet of Things (IoT) security technologies [1,2]. There are two types of RNGs, software-based pseudorandom number generators (PRNGs) and hardware-based true random number generators (TRNGs), which use intrinsic stochasticity originating from physical variations in hardware components. Owing to the deterministic and periodic nature of PRNG sequences, the bit patterns generated by PRNGs can be easily revealed. Therefore, in terms of security, TRNGs are considered superior to PRNGs [3–11]. Complementary metal-oxide-semiconductor (CMOS)-based TRNGs have been most commonly used for implementing TRNGs. However, the CMOS-based TRNGs need the dedicated circuits to harness entropy sources such as timing jitter and metastability, so that they occupy large footprint due to circuit complexity, leading to increased power consumption and limited scalability [12–14]. Hence, single-device entropy sources such as resistive random-access memory and magnetic random-access memory have been proposed [1,15–17], but the alternative material-based TRNGs still require additional entropy extraction circuits to convert their inherent stochastic behavior into usable random bits. Moreover, their limited compatibility with standard CMOS processes presents further challenges for on-chip integration. On the other hand, the silicon-gated p^+–i–n^+ diode-based TRNG generates fully digitized random bits without the need for amplification or extraction circuitry, offering advantages over both conventional CMOS-based and other single-device-based TRNGs [18]. Conventional approaches to TRNGs focus on generating random binary sequences. However, adopting a multivalued system for data security can enhance security levels. Using more than two values to encode data dramatically strengthens security by lowering the risk of hacking [19–21]. Therefore, research on multivalued cryptographic systems is essential for IoT security. To date, multinary TRNGs have been demonstrated as ternary TRNGs using spin–orbit torque devices that are inherently vulnerable to temperature and difficult to produce [17,22,23]. To realize multinary TRNGs, the component devices of the TRNGs should have thermally stable electrical properties and high fabrication uniformity. Hence, we propose a TRNG comprising gated p^+–i–n^+ diodes that exhibit reliable electrical characteristics and high fabrication

[*] Corresponding author (email: chochem@korea.ac.kr, sangsig@korea.ac.kr)

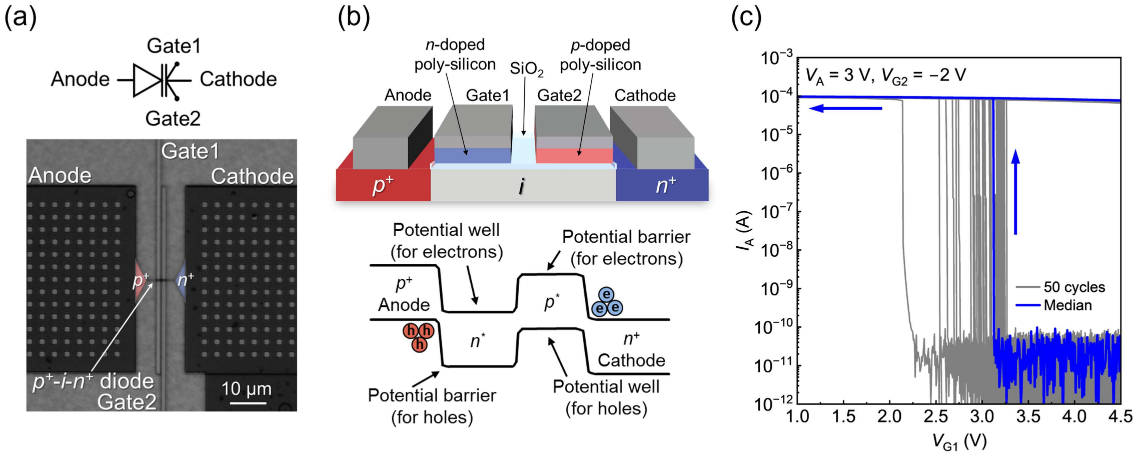

Figure 1 (Color online) Gated p^+–i–n^+ diode. (a) Symbol and optical image; (b) schematic and energy-band diagram; (c) transfer characteristics for 50 cycles.

uniformity obtained by CMOS technology. In this study, a quaternary random number generator (Q-TRNG) was obtained as a multinary TRNG by connecting three binary true random number generators (B-TRNGs) without any auxiliary circuits. Image encryption and decryption were demonstrated using the quaternary secret keys generated by Q-TRNG. Our study can be expanded to multinary TRNGs with n distinct values by using $n-1$ B-TRNGs, in the same manner as Q-TRNGs.

2 Results

2.1 Stochastic behavior of a gated p^+–i–n^+ diode

First, we investigated the stochastic behavior of a gated p^+–i–n^+ diode. Figure 1(a) shows the symbol and optical image of the diode including two 1.5 μm wide polysilicon gates arranged side-by-side on the intrinsic channel region. The schematic and energy-band diagram of the gated p^+–i–n^+ diode are represented in Figure 1(b); the n-doped polysilicon gate near the p^+ anode is called gate1 and the p-doped polysilicon near the n^+ cathode is called gate2. The work functions of gate1 and gate2 create n-type electrostatic doping (n^*) and p-type electrostatic doping (p^*) in the intrinsic channel region, respectively, resulting in a p^+-n^*–p^*–n^+ energy-band structure. This structure enables the gated p^+–i–n^+ diode to operate with a band modulation mechanism arising from recursive and mutual interactions between the charge carriers and potential barriers. In the initial state, the potential barrier heights in the channel region are sufficiently high to block carrier injection. As the potential barrier formed in the p^* region on the n^+ cathode side is lowered by the accumulation of holes from the p^+ anode, electrons originating from the cathode accumulate in the n^* region. Consequently, electrons flow toward the anode, and the accumulation of electrons prompts the injection of holes. Accordingly, the repeated injection and accumulation of charge carriers trigger a positive-feedback loop. Consequently, when the potential barriers collapse owing to the activation of the positive-feedback loop, the gated p^+–i–n^+ diode exhibits an abrupt increase in the anode current (I_A), which is called the latch-up phenomenon.

Figure 1(c) shows the transfer characteristics of the gated p^+–i–n^+ diode obtained from 50 repeated measurements to verify the variation in the latch-up voltage ($V_{\text{latch-up}}$). Because of the probabilistic accumulation and recombination of charge carriers in the potential wells, the gated p^+–i–n^+ diode shows $V_{\text{latch-up}}$ variation, even under the same anode voltage (V_A) and gate2 voltage (V_{G2}), revealing the inherent stochasticity of the band modulation mechanism [24,25]. Such stochastic behavior enables the gated p^+–i–n^+ diode to serve as a critical component in true random number generators.

2.2 Binary true random number generator

Based on the stochastic characteristics of the gated p^+–i–n^+ diode, a B-TRNG was realized by connecting the diode to a resistor, as shown in Figure 2(a). Herein, the anode of the gated p^+–i–n^+ diode was biased with the input voltage (V_{IN}) and the cathode was connected in series with a 500 kΩ resistor.

Figure 2(b) represents the probability of the B-TRNG to generate bit '1' as a function of gate1 voltage (V_{G1}). When V_{G1} is between 2.4 and 2.2 V, the probability of '1' is determined to be 0. Within this voltage range, the

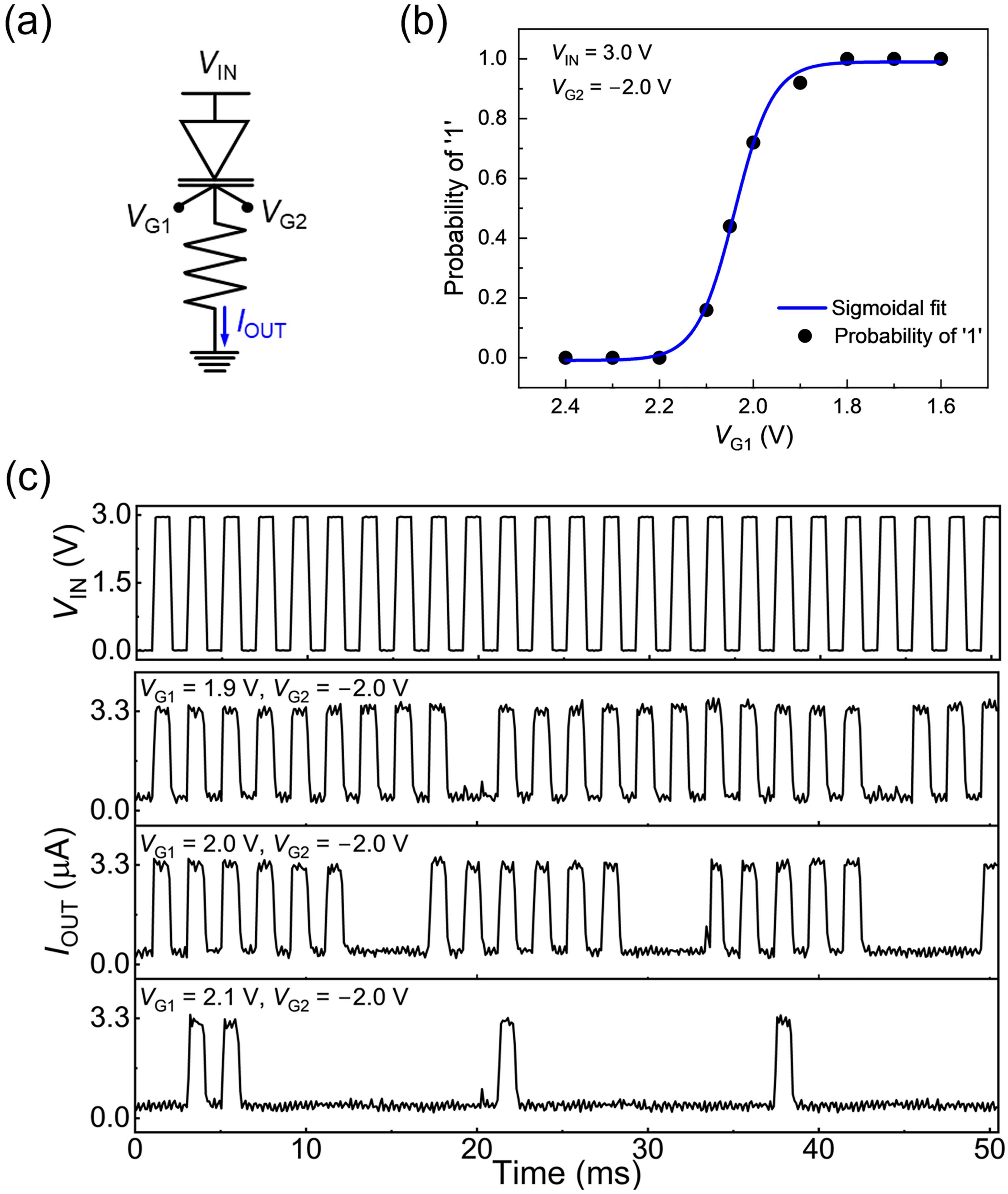

Figure 2 (Color online) Binary true random number generator (B-TRNG) comprising a gated p^+–i–n^+ diode and resistor. (a) Circuit schematic of the B-TRNG; (b) probability of '1' and sigmoidal fitting curve as a function of V_{G1}; (c) random characteristics of B-TRNG for V_{G1} values of 1.9, 2.0, and 2.1 V.

potential barrier formed under gate1 is sufficiently high to prevent carrier injection from the anode. Consequently, the gated p^+–i–n^+ diode remains in the OFF state without any fluctuation. Similarly, when V_{G1} is between 1.8 and 1.6 V, the probability of '1' is determined to be 1. Under these conditions, the potential barrier induced by V_{G1} is sufficiently low to permit carrier injection into the channel, keeping the diode in the ON state. Conversely, as V_{G1} decreases from 2.2 to 1.8 V, the probability of '1' gradually increases from 0 to 1. In this transition region, the gated p^+–i–n^+ diode is in a marginal state, where the potential barrier neither completely blocks nor fully permits current flow. Thus, the height of the potential barrier within this voltage range is closely associated with the number of charge carriers accumulated in the potential well. Because of the stochastic nature of the carrier recombination process, the height of the potential barrier varies randomly. If there are sufficient carriers in the potential well to activate the positive-feedback loop, the diode can be switched on, thereby generating bit '1'.

Figure 2(c) shows experimentally observed random characteristics of the B-TRNG in the stochastic region. The I_{OUT} of the B-TRNG randomly varies between 0.0 and 3.3 μA in response to identical input pulses. The variation corresponds to the random bits '0' and '1'. As V_{G1} increases from 1.9 to 2.1 V, the height of the potential barrier

Table 1 Comparison between gated p^+–i–n^+ diode and other single-device entropy sources.

Device	Magnetic tunnel junction [10]	Diffusive memristor [1]	Spin orbit torque [15]	FinFET [26]	Gated p^+–i–n^+ diode (this work)
Entropy source	Stochastic switching	Stochastic delay	Stochastic switching	Stochastic oscillation	Stochastic switching
Auxiliary components	Precharge sense amplifier	Series resistor, comparator, AND gate, counter	Comparator, AND gate	Series resistor, noise-coupling analog-to-digital converter	Series resistor
Bit generation rate	5 kb/s	6 kb/s	N/A	75 kb/s	2 Mb/s
Energy consumption	20 fJ/bit (simulated)	N/A	N/A	10.28 pJ/bit	40.25 pJ/bit

Table 2 NIST randomness test results of B-TRNGs.

Test	B-TRNG1		B-TRNG2		B-TRNG3	
	P-value	Result	P-value	Result	P-value	Result
Frequency (Monobit) test	0.777294	Random	0.023651	Random	0.257899	Random
Frequency testwithin a block	0.777294	Random	0.023651	Random	0.257899	Random
Runs test	0.261923	Random	0.017208	Random	0.363010	Random
Discrete Fourier transform (spectral) test	0.104754	Random	0.023140	Random	0.745602	Random
Non-overlapping template matching test	0.999999	Random	0.999999	Random	0.999999	Random
Linear complexity test	0.498530	Random	0.999999	Random	0.498530	Random
Serial test	0.498961	Random	0.999999	Random	0.498961	Random
Approximate entropy test	1.0	Random	1.0	Random	1.0	Random
Cumulative sums test	0.892023 (forward)	Random	1.011825 (forward)	Random	0.314565 (forward)	Random
	0.639929 (backward)	Random	1.008104 (backward)	Random	0.179317 (backward)	Random
Random excursive test	0.544915	Random	0.962565	Random	0.220640	Random
Random excursive variant test	0.386476	Random	1.0	Random	1.0	Random

under the gate1 region increases. Therefore, the probability of positive-feedback occurring in the channel decreases so that the probability of generating ‘1’ decreases, confirming that V_{G1} can control the probability of the random bits.

Table 1 presents a comparison between the gated p^+–i–n^+ diode and other single-device entropy sources [1,5,10, 26]. Regarding auxiliary components, our device requires only a series resistor, whereas the others need additional circuitry; thus, the gated p^+–i–n^+ diode offers an advantage in simplicity. In terms of bit generation rate, our device operates orders of magnitude faster than other reported single-device entropy sources. With respect to energy consumption, the gated p^+–i–n^+ diode is comparable to other devices. On the other hand, the magnetic tunnel junction has not been experimentally evaluated so that it is hard to compare its energy consumption with that of the gated p^+–i–n^+ diode. The detailed calculation procedures for the bit generation rate and energy consumption are described in Appendix B of supplementary materials. Therefore, the gated p^+–i–n^+ diode shows clear advantages over other single-device entropy sources, indicating that it is suitable for multinary TRNG applications.

2.3 Quaternary true random number generator

In this study, we constructed Q-TRNG comprising three parallel B-TRNGs (B-TRNG1, B-TRNG2, and B-TRNG3) as illustrated in Figure 3(a). Identical V_{IN} and V_{G2} values were applied to the three B-TRNGs for the Q-TRNG operation. Based on the probability of ‘1’ curves shown in Figure 3(b), the three V_{G2} values, $V_{\mathrm{G1\_1}}$, $V_{\mathrm{G1\_2}}$, and $V_{\mathrm{G1\_3}}$, were set within voltage ranges where each B-TRNG exhibited stochastic behavior. To demonstrate the randomness, the NIST test results for each B-TRNG are presented in Table 2. In this study, each B-TRNG unit in the Q-TRNG can be independently tuned to exhibit similar random behavior by using the three V_{G1} values ($V_{\mathrm{G1\_1}}$, $V_{\mathrm{G1\_2}}$, and $V_{\mathrm{G1\_3}}$) that are applied individually to compensate for the process variation among the gated p^+–i–n^+ diodes. In the Q-TRNG operation, these binary outputs are combined through current summation. Each B-TRNG contributes to a digitized current level of either 0 or 3.3 μA, and the total I_{OUT} becomes the sum of the individual currents. Consequently, I_{OUT} takes one of four discrete values, 0.0, 3.3, 6.6, or 9.9 μA, which correspond to the quaternary digits ‘0’, ‘1’, ‘2’, and ‘3’, respectively, as shown in Figure 3(c). The experimental set-up to examine the random characteristics of the Q-TRNG is shown in Figure C1 of supplementary materials. Under identical input pulses, the Q-TRNG generated a representative quaternary random sequence of ‘0023331333110033330000333310002330110333320002333’.

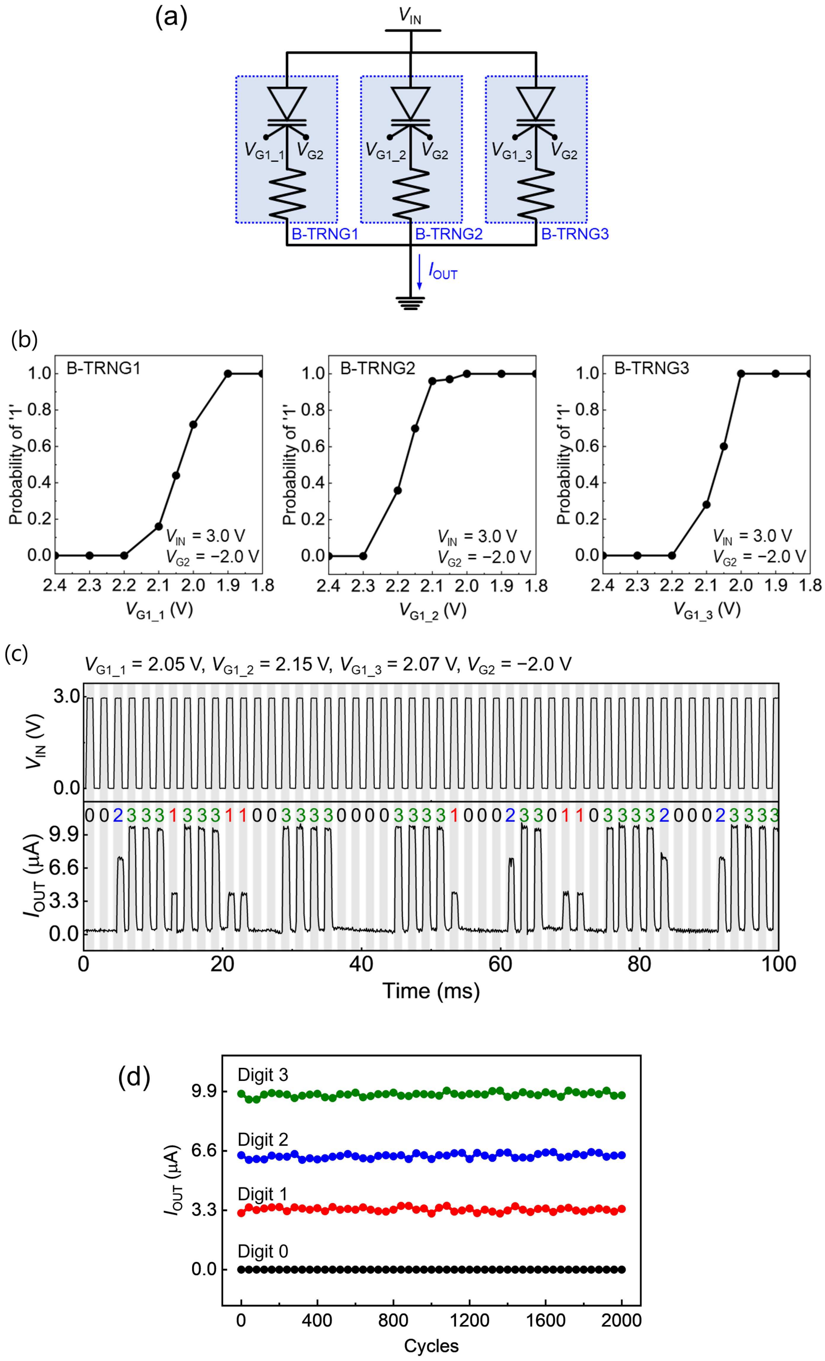

Figure 3 (Color online) Quaternary true random number generator (Q-TRNG). (a) Circuit schematic of Q-TRNG; (b) probability of '1' curve of each B-TRNGs constituting the Q-TRNG; (c) random characteristic of Q-TRNG; (d) endurance of each digit over 2000 cycles.

As shown in the raw output distribution in Figure 3(c), the Q-TRNG generates certain digits more frequently. Although each $V_{\rm G1}$ value ($V_{\rm G1\_1}$, $V_{\rm G1\_2}$, and $V_{\rm G1\_3}$) was initially set based on the voltage range at which the corresponding B-TRNG exhibited approximately 50% switching probability in the individual operation, the actual operating conditions may differ when the three B-TRNGs are connected in parallel within the Q-TRNG structure. Hence, the post-processing module of the Q-TRNG needs actual device offsets. Moreover, setting the B-TRNGs to $\sim$50% probability is still essential even though the post-processing is carried out for the Q-TRNG; the distribution of the post-processed random numbers is not uniform when the probability of the B-TRNGs deviates significantly from $\sim$50%. Owing to the steep switching characteristics of the gated p^+–i–n^+ diodes, each digit of the quaternary random numbers generated by Q-TRNG can be clearly distinguished without any auxiliary circuits. Moreover, our

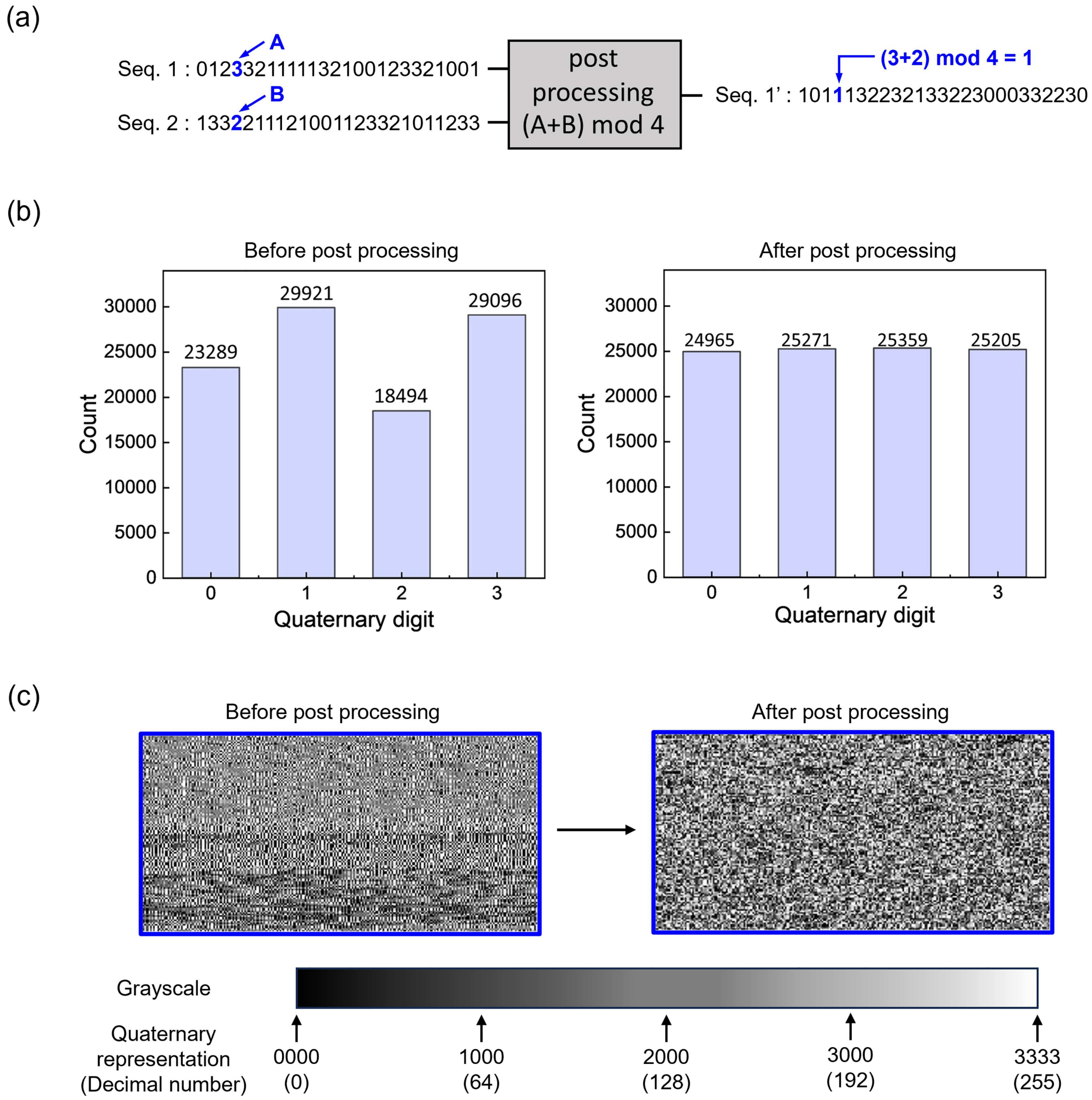

Figure 4 (Color online) Post-processing of quaternary random numbers. (a) Post-processing scheme for quaternary random numbers; (b) distribution of quaternary digits before and after post-processing; (c) grayscale representation of quaternary random numbers before and after post-processing.

Q-TRNG can operate with lower energy consumption compared to other TRNGs [17,22]. Although most multinary TRNGs generate ternary random sequences, our Q-TRNG offers higher data density by generating quaternary random sequences. We demonstrated reliable endurance characteristics of Q-TRNG, as shown in Figure 3(d). The random outputs of the Q-TRNG maintained their initial current levels corresponding to the digits ‘0’, ‘1’, ‘2’, and ‘3’ under the voltage condition of $V_{\rm G1\_1} = 2.05$ V, $V_{\rm G1\_2} = 2.15$ V, and $V_{\rm G1\_3} = 2.07$ V over 2000 cycles, generating approximately 1×10^5 digits. Endurance characteristics are associated with the fundamental limit of the length of the generated random sequences, which contributes to the long-term reliability and suitability for demanding computational tasks [27–29]. The endurance characteristics of Q-TRNG demonstrate its potential for secure and reliable random number generation, making it suitable for securing or encrypting information.

As hacking techniques advance, ensuring a high level of security is essential for protecting data from attackers. For a high level of security, a high level of randomness should be obtained from a uniform distribution across all digits of the random sequences [30]. Therefore, we applied the ‘(A+B) mod 4’ operation as a post-processing method to the quaternary random numbers generated by the Q-TRNG as shown in Figure 4(a). In this approach, the digits A and B, located at the corresponding positions in each random sequence, were summed and then divided by four. The resulting remainders from these calculations formed a new random sequence. Figure 4(b) shows the distribution of each quaternary digit before and after the post-processing. Among the 100800 digits, the occurrences

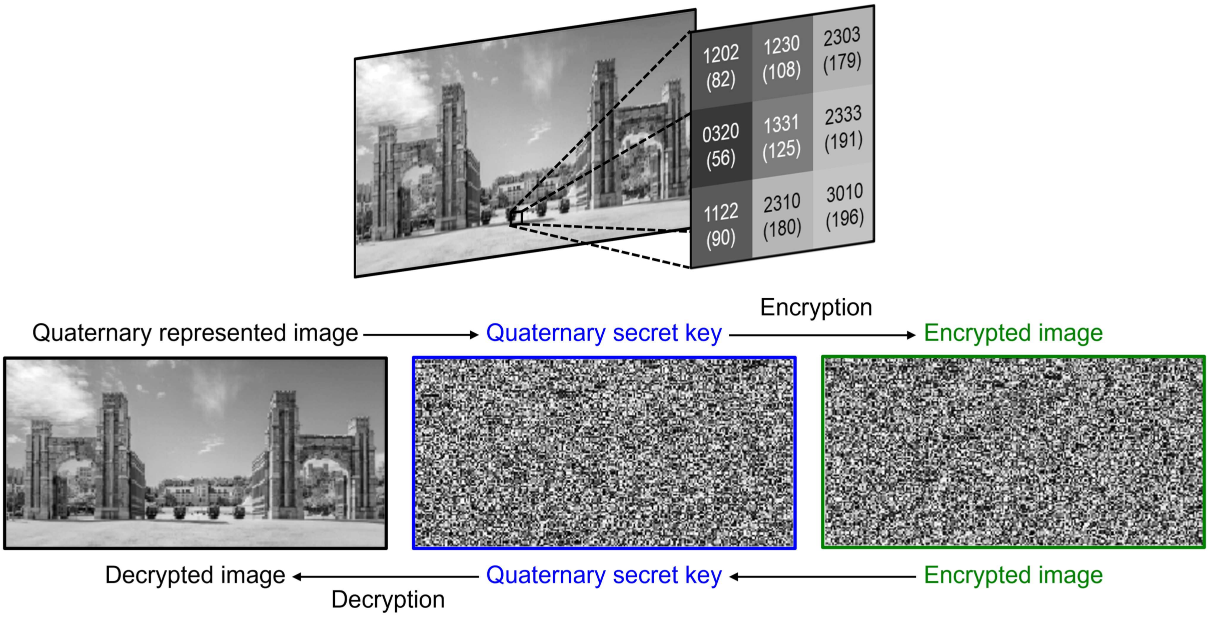

Figure 5 (Color online) Image encryption and decryption processes using Q-TRNG. The grayscale image comprises 4-digit quaternary pixel information. The quaternary random digits experimentally generated by Q-TRNG are exploited as the secret key.

of ‘1’ and ‘3’ are more frequent than ‘0’ and ‘2’ before the post-processing. However, after the post-processing, the random sequences exhibited a uniform distribution across all digits, indicating higher randomness and an enhanced level of security. The post-processed quaternary random numbers generated by the Q-TRNG yielded a p-value of 0.4027 in the chi-square test as shown in Appendix A of supplementary materials, indicating low correlation among digits and consequently a high degree of randomness. Figure 4(c) shows the grayscale representations of the quaternary random sequences before and after the post-processing. Grayscale pixel information can be represented with 256 levels, where ‘0000’ corresponds to the darkest black and ‘3333’ to the brightest white. Therefore, the 100800 digits were chunked into 4-digit groups to be displayed as grayscale images. The post-processed quaternary random sequences formed a completely random noise image without detectable periodic patterns.

2.4 Image encryption and decryption of Q-TRNG

Figure 5 shows the image encryption and decryption procedures using the quaternary random numbers obtained from Figure 4(c). The original image and secret key which consist of 225 × 112 pixels are represented by 100800 quaternary digits, whereas 201600 bits are required for binary representation. Cybersecurity is enhanced as a key space is increased; a key space in cryptology means the set of all valid, possible, and distinct keys of a given cryptosystem. Q-TRNG generates a larger key space than B-TRNG, so that Q-TRNG is superior to B-TRNG in terms of cybersecurity. For instance, a 10-digit quaternary sequence yields a 1048576 key space, which is three orders of magnitude greater than that of a 10-bit binary sequence (1024 key space). On the other hand, a secret key is a specific key chosen from the key space to encrypt or decrypt data. In this sense, a secret key used in the Q-TRNG offers higher security in image encryption, enhancing resistance to cyberattacks. Furthermore, the security strength of the secret key can be quantified by the min-entropy, which is calculated using the most common value (MCV) estimator [31]. In the ideal case, where all digits occur with equal probability, the min-entropy values of binary and quaternary secret keys are 1 and 2, respectively. In other words, a quaternary secret key provides double the entropy compared to a binary key, thereby offering significantly enhanced security strength for the same key length. For the quaternary secret key used in this work, the min-entropy value obtained from the MCV estimator is 1.97, which is very close to the ideal value of 2. This demonstrates that the proposed key exhibits high entropy and provides strong security assurance. The calculation procedures for the min-entropy using the MCV estimator are described in Appendix D of supplementary materials. Details of the encryption and decryption processes are presented in Section 5. The original image is encrypted into a noisy image format after implementing a quaternary XOR with a secret key, providing secure transmission and storage against external attackers. The encrypted image is completely restored to its original form by applying quaternary XOR with the secret key.

3 Discussion

Compared to conventional binary systems, Q-TRNG can significantly enhance the processing efficiency of image encryption and decryption by reducing the computational complexity. Typically, during image processing, grayscale pixel information is encoded as 8-bit binary sequences. On the other hand, employing a 4-digit quaternary system reduces the number of required digits by half, significantly improving data efficiency. Accordingly, adopting a quaternary secret key for image encryption and decryption can reduce the required data throughput by more than 50%, when quaternary-based peripheral circuitry is supported. Moreover, owing to the larger number of possible combinations in the quaternary system, the quaternary secret key offers higher security than the binary secret key. In addition, our Q-TRNG can generate random sequences without auxiliary circuits, whereas most previous approaches require additional components to convert entropy sources into random digits. The four current values generated by Q-TRNG were clearly defined owing to the steep switching characteristics of the gated p^+–i–n^+ diodes. Therefore, I_{OUT} from our Q-TRNG can be directly used as a digitized quaternary random sequence.

4 Conclusion

In summary, we designed a Q-TRNG consisting of three gated p^+–i–n^+ diodes and series resistors without auxiliary circuits. The Q-TRNG generates four distinct current levels with high endurance owing to the intrinsic stochasticity of the band modulation mechanism and the steep switching characteristics of the gated p^+–i–n^+ diodes. Furthermore, we demonstrated the applicability of Q-TRNG for image encryption and decryption. Compared to conventional binary systems, our Q-TRNG not only improves image processing efficiency but also offers enhanced security by using more than two values for data representation. Consequently, the proposed Q-TRNG is a promising candidate for multivalued hardware security technologies that enable compact and robust data encryption.

5 Materials and methods

5.1 Device fabrication

Gated p^+–i–n^+ diodes were fabricated on a p-type silicon-on-insulator wafer using a fully CMOS-compatible top-down process. The 100-nm thick silicon active layer was patterned with a width of 180 nm using photolithography and dry etching. The 400 nm thick and 1.5 μm length poly-Si gates were formed with a 1 μm wide gap by low-pressure chemical vapor deposition on a 25 nm thick $\mathrm{SiO_2}$ gate oxide layer that was thermally grown on the intrinsic channel region at 850°C. The cathode and gate1 of the gated p^+–i–n^+ diode were heavily doped with P^+ ions at a dose of 3×10^{15} cm^{-2} at 50 keV, and the anode and gate2 were heavily doped with BF_2^+ ions at a dose of 3×10^{15} cm^{-2} at 30 keV. The implanted dopants were thermally activated at 1050°C for 30 s. Finally, the Ti/TiN/Al/TiN metal alloy was deposited in the anode, cathode, and gate contact regions after interlayer dielectric deposition at 400°C for 30 min.

5.2 Measurement

The switching characteristics of the gated p^+–i–n^+ diode were measured using a semiconductor parameter analyzer (HP4155C, Agilent). Keithley 2636A and 2636B source meters were used to obtain the binary and quaternary random numbers, respectively. The morphology of the fabricated device was observed using an optical microscope (Nikon, Eclipse L150S).

5.3 Image encryption and decryption

Python was used for the image processing and encryption/decryption. The original image consisted of 225 × 112 pixels. The experimentally extracted random bits were combined and reshaped into 225 × 112 × 4 to match the size of the original image data. To obtain a large secret key, random bit sequences were extracted multiple times from Q-TRNG. A quaternary XOR cipher was employed for image encryption and decryption.

Acknowledgements This work was partially supported by National Research Foundation of Korea Grant Funded by the Korean Government (MSIT) (Grant No. RS-2023-00260876), Samsung Electronics (Grant No. IO201223-08257-01), Brain Korea 21 Plus Project, and Korea University Grant.

Supporting information Appendixes A–C. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Jiang H, Belkin D, Savel'ev S E, et al. A novel true random number generator based on a stochastic diffusive memristor. Nat Commun, 2017, 8: 882

2 van der Leest V, Maes R, Schrijen G-J, et al. Hardware intrinsic security to protect value in the mobile market. In: Proceedings of the Information Security Solutions Europe Conference, 2014. 188–198

3 Stipčević M, Koç Ç K. True random number generators. In: Open Problems in Mathematics and Computational Science. Berlin: Springer, 2014. 275–315

4 Blackman D, Vigna S. Scrambled linear pseudorandom number generators. ACM Trans Math Softw, 2021, 47: 1–32

5 Sathya K, Premalatha J, Rajasekar V. Investigation of strength and security of pseudo random number generators. IOP Conf Ser-Mater Sci Eng, 2021, 1055: 012076

6 Sahay S, Suri M. Recent trends in hardware security exploiting hybrid CMOS-resistive memory circuits. Semicond Sci Technol, 2017, 32: 123001

7 Zhou S, Zhang W, Wu N J. An ultra-low power CMOS random number generator. Solid-State Electron, 2008, 52: 233–238

8 Ma Y, Lin J, Chen T, et al. Entropy evaluation for oscillator-based true random number generators. In: Proceedings of the 16th International Workshop on Cryptographic Hardware and Embedded Systems, 2014. 544–561

9 Huang C Y, Shen W C, Tseng Y H, et al. A contact-resistive random-access-memory-based true random number generator. IEEE Electron Device Lett, 2012, 33: 1108–1110

10 Vodenicarevic D, Locatelli N, Mizrahi A, et al. Low-energy truly random number generation with superparamagnetic tunnel junctions for unconventional computing. Phys Rev Appl, 2017, 8: 054045

11 Balatti S, Ambrogio S, Wang Z, et al. True random number generation by variability of resistive switching in oxide-based devices. IEEE J Emerg Sel Top Circuits Syst, 2015, 5: 214–221

12 Frustaci F, Spagnolo F, Perri S, et al. A high-speed FPGA-based true random number generator using metastability with clock managers. IEEE Trans Circuits Syst II, 2022, 70: 756–760

13 Yang B, Rožić V, Grujić M, et al. On-chip jitter measurement for true random number generators. In: Proceedings of Asian Hardware Oriented Security and Trust Symposium, 2017. 91–96

14 Baturone I, Román R, Corbacho Á. A unified multibit PUF and TRNG based on ring oscillators for secure IoT devices. IEEE Internet Things J, 2022, 10: 6182–6192

15 Xing X, Huang S, Gong Y, et al. Stochastic current response in diffusive memristor for security applications. Mater Today Nano, 2023, 22: 100315

16 Rangarajan N, Parthasarathy A, Rakheja S. A spin-based true random number generator exploiting the stochastic precessional switching of nanomagnets. J Appl Phys, 2017, 121: 223905

17 Chen H, Zhang S, Xu N, et al. Binary and ternary true random number generators based on spin orbit torque. In: Proceedings of IEEE International Electron Devices Meeting (IEDM), 2018. 1–4

18 Jeon J, Shin Y, Heo H, et al. Cryptographic characteristics of true random number generators using gated silicon nanosheet diodes. Sci China Inf Sci, 2025, 68: 162401

19 Shou X, Kalantari N, Green M M. Design of CMOS ternary latches. IEEE Trans Circuits Syst I, 2006, 53: 2588–2594

20 Sokolov A, Zhdanov O. Prospects for the application of many-valued logic functions in cryptography. In: Proceedings of Advances in Computer Science for Engineering and Education, 2019. 331–339

21 Wang H, Ouyang S, Chen X, et al. Using reconfigurable multi-valued logic operators to build a new encryption technology. Comput Sci Math Forum, 2023, 8: 99

22 Khodayari F, Amirany A, Moaiyeri M H, et al. A variation-aware ternary true random number generator using magnetic tunnel junction at subcritical current regime. IEEE Trans Magn, 2023, 59: 1–8

23 Khodayari F, Amirany A, Jafari K, et al. Low-cost and variation-aware spintronic ternary random number generator. Circuits Syst Signal Process, 2024, 43: 1175–1191

24 Lim D, Cho K, Kim S. Single silicon neuron device enabling neuronal oscillation and stochastic dynamics. IEEE Electron Device Lett, 2021, 42: 649–652

25 Lim D. Single silicon synaptic device for stochastic binary spike-timing-dependent plasticity. Semicond Sci Technol, 2023, 38: 075015

26 Kim S I, You H J, Kim M S, et al. Cryptographic transistor for true random number generator with low power consumption. Sci Adv, 2024, 10: eadk6042

27 Zhao X, Chen L W, Li K, et al. Memristive true random number generator for security applications. Sensors, 2024, 24: 5001

28 Zhang T, Yin M, Xu C, et al. High-speed true random number generation based on paired memristors for security electronics. Nanotechnology, 2017, 28: 455202

29 Le Gallo M, Tuma T, Zipoli F, et al. Inherent stochasticity in phase-change memory devices. In: Proceedings of the 46th European Solid-State Device Research Conference (ESSDERC) 2016. 373–376

30 Marton K, Suciu A, Sacarea C, et al. Generation and testing of random numbers for cryptographic applications. In: Proceedings of the Ramanian Academy, 2012. 368–377

31 National Institute of Standards and Technology. Recommendation for the entropy sources used for random bit generation. NIST Special Publication 800-90B, 2018. https://doi.org/10.6028/NIST.SP.800-90B