

Received May 30, 2021, accepted June 18, 2021, date of publication June 22, 2021, date of current version July 1, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3091491

Low-Power True Random Number Generator Based on Randomly Distributed Carbon Nanotube Networks

SUNGHO KIM¹, MOON-SEOK KIM^{2,3}, YONGWOO LEE⁴, HEE-DONG KIM¹, YANG-KYU CHOI², AND SUNG-JIN CHOI⁴

¹Department of Electrical Engineering and Convergence Engineering for Intelligent Drone, Sejong University, Seoul 05006, Republic of Korea

²School of Electrical Engineering, Korea Advanced Institute of Science and Technology (KAIST), Daejeon 34141, Republic of Korea

³ETRI, Daejeon 34141, Republic of Korea

⁴School of Electrical Engineering, Kookmin University, Seoul 02707, Republic of Korea

Corresponding author: Sung-Jin Choi (sjchoiee@kookmin.ac.kr)

This work was supported in part by the Nano Material Technology Development Program funded by the Ministry of Science, Information and Communications Technology (ICT) and Future Planning under Grant 2016M3A7B4910426, and in part by the National Research Foundation of Korea (NRF) through the Research Programs under Grant 2019R1A2C1002491, Grant 2019R1A2B5B01069988, Grant 2016R1A5A1012966, and Grant 2020R1A6A1A03038540.

ABSTRACT Although the intrinsic variability in nanoelectronic devices has been a major obstacle and has prevented mass production, this natural stochasticity can be an asset in hardware security applications. Herein, we demonstrate a true random number generator (TRNG) based on stochastic carrier trapping/detrapping processes in randomly distributed carbon nanotube networks. The bitstreams collected from the TRNG passed all the National Institute of Standards and Technology randomness tests without post-processing. The random bit generated in this study is sufficient for encryption applications, particularly those related to the Internet of Things and edge computing, which require significantly lower power consumption.

INDEX TERMS Carbon nanotube network, random number generator, stochastic carrier trapping.

I. INTRODUCTION

Random number generators are a requisite in many areas, including key generation, simulation, and secure communications. A software-based random number generator, also called a pseudo-random number generator, is preferred in many applications because of its simplicity of implementation; however, it is vulnerable to a wide range of security threats owing to its predictable algorithm. By contrast, hardware-based true random number generators (TRNGs) can generate a random bitstream using the intrinsic stochasticity in physical variables—such as thermal noise [1], telegraph noise [2], and oxide breakdown [3] which enables superior encryption. Energy-efficient TRNGs are essential components in applications that require very low power consumption—such as the Internet of Things (IoT) or edge computing [4].

Recently, the intrinsic variation of memristors has been exploited to demonstrate a TRNG in which unavoidable cycle-to-cycle variation could be intentionally used as a

physical source to generate random bitstreams [5], [6]. However, they required an additional post-processing step (i.e., Von Neumann correction) to pass the National Institute of Standards and Technology (NIST) randomness tests owing to their lack of true randomness; consequently, they suffered from drawbacks in terms of scalability, circuit complexity, and power consumption. Subsequently, more advanced TRNGs have been proposed based on the stochastic delay or relaxation time of volatile memristors which have passed all the NIST tests without any post-processing steps [7]–[9]. Nevertheless, the driving current of prior volatile memristors exceeded $1 \mu\text{A}$ [7], which lead to inevitably high TRNG power consumption, while an additional peripheral circuit (e.g., a nonlinear feedback shift register circuit [8], [9]) is required to achieve a high bit generation rate. Furthermore, the high endurance performance ($>10^{10}$) required from the TRNG cannot yet be fully guaranteed using volatile memristors [10]. Moreover, most silver-based volatile memristors have poor compatibility with the conventional complementary metal oxide semiconductor (CMOS) technology [7], [11], which prevents co-integration with existing digital circuits.

The associate editor coordinating the review of this manuscript and approving it for publication was Chaitanya U. Kshirsagar.

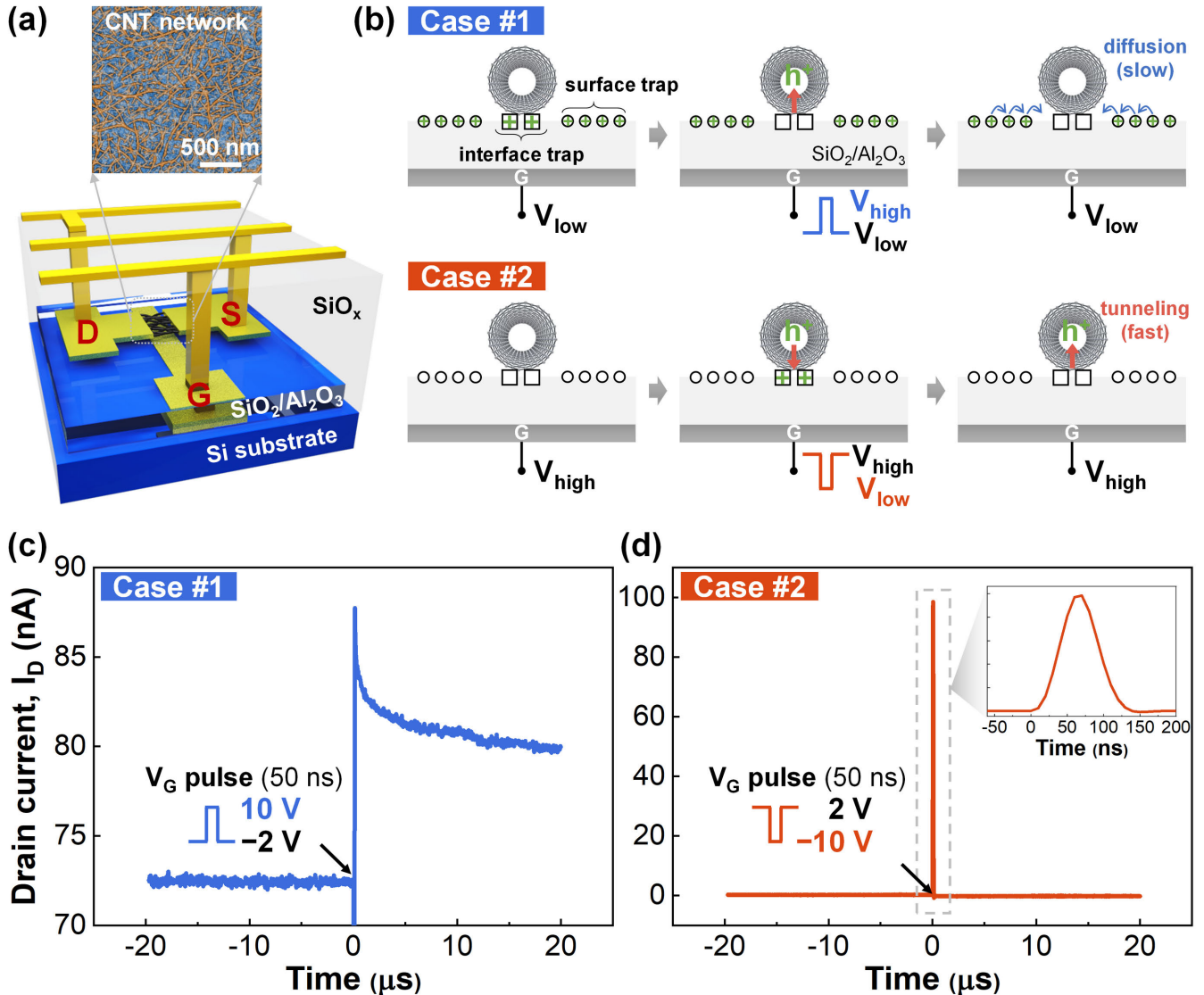


FIGURE 1. Temporal I_D response in the CNT network transistor. (a) Schematic of the CNT network transistor, and atomic microscope image of the CNT network. (b) Schematics of the trapping/detrapping of holes at the interface/surface traps. (c) Sudden I_D enhancement and gradual decay when a single V_G pulse ($V_{high} = 10\text{ V}$, $V_{low} = -2\text{ V}$) is applied, which is primarily attributed to the slow hole diffusion process at the surface trap. (d) Sudden I_D enhancement and fast recovery when a single V_G pulse ($V_{high} = 2\text{ V}$, $V_{low} = -10\text{ V}$) is applied, which is primarily attributed to the fast hole tunneling process at the interface trap.

Herein, we demonstrate a TRNG based on a solution-processed carbon nanotube (CNT) network by employing a transistor structure, as the CNT is a well-known material that is compatible with the CMOS process [12]. Similar CNT-based TRNGs have already been reported; however, a number of device groups (crossbar array [13], static random access memory circuits [14], or a couple of device [15]) were required to generate a random bitstream, thereby limiting scalability. We overcame this limitation by implementing a single CNT transistor-based TRNG in this study. The stochastic carrier trapping/detrapping process between the CNT channel and the traps in the gate insulator is a source of randomness, which is further enhanced by the randomly distributed CNT networks. The electronic process attributed to carrier trapping/detrapping enables lower power consumption and better reliability than the ionic switching used in previous volatile

memristors. A bit generation rate of 5 kb s^{-1} was achieved without using complex peripheral circuits, and finally our TRNG passed all 15 NIST randomness tests. This work presents a promising methodology for improving security in low-power-consumption systems.

II. RESULTS AND DISCUSSION

Fig. 1a presents the schematic of our CNT network transistor (see Methods) [16]–[18]. The solution processing method yields randomly distributed single-walled semiconducting CNTs, which serve as the channel of the transistor. Our previous studies [16]–[18] have demonstrated that CNT transistors have a drain current (I_D) hysteresis based on the gate voltage (V_G) sweep (Fig. S1a). Although the cause of the hysteresis is still debatable, the hysteresis can be attributed to the trapping/detrapping of holes at the traps [19] (see Fig. S1 and

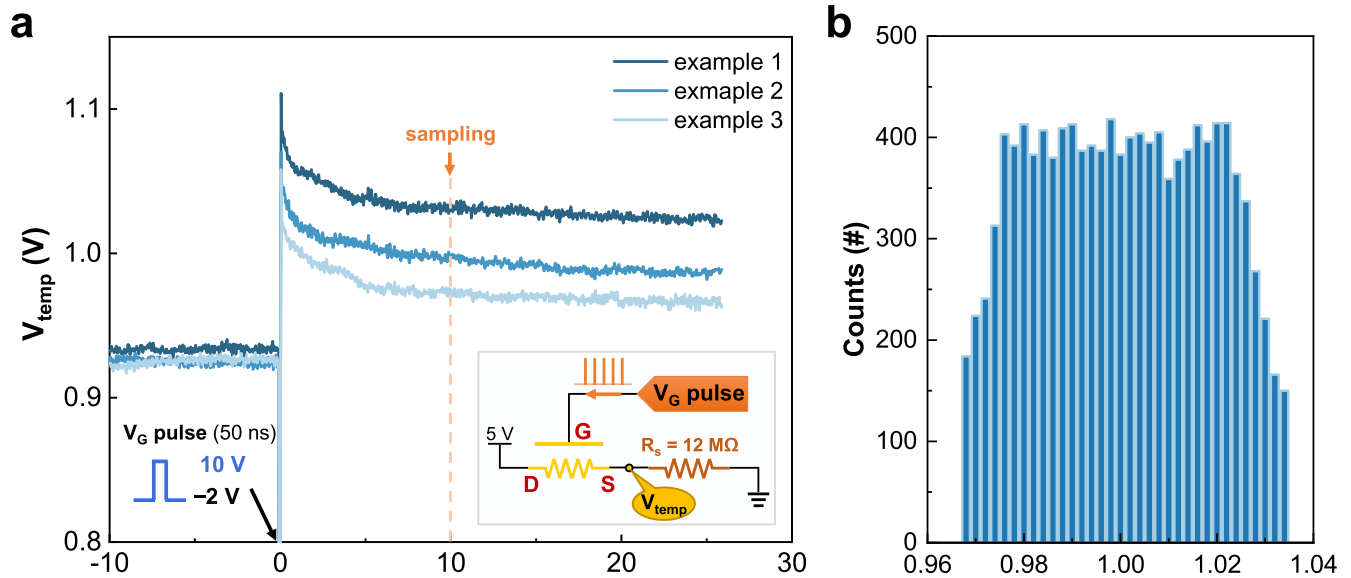


FIGURE 2. Stochasticity of the temporal I_D response. (a) Three examples of temporal I_D responses under the same V_G pulse condition. The inset shows the measurement setup where a series resistor (R_S) is connected to the source electrode that converts I_D (current) to V_{temp} (voltage). (b) The collected V_{temp} from 12000 trial measurements.

Supporting Information Note 1 for a more detailed explanation). When a negative V_G is applied, the trapped holes bend the energy band of the CNT downward, resulting in the suppression of I_D owing to the enlarged Schottky barrier at the drain/CNT junction (left inset of Fig. S1a). By contrast, a positive V_G leads to ejection of the trapped holes, and the consequent upward band bending leads to I_D enhancement (right inset of Fig. S1a). Notably, the hysteresis is attributed to two different types of traps: the interface trap and the surface trap (Fig. 1b) [19]. The interface trap is adjacent to the CNT channel; thus, the holes can move between them relatively quickly and easily through the tunneling process. Conversely, the diffusion of holes through the surface trap in the lateral direction is relatively slow and difficult. Considering the contact area between the CNT channel and the gate insulator, it is clear that the surface trap is much larger than the interface trap, allowing the surface trap to act as a hole reservoir. The different timescales of the hole movement at the interface and surface traps enable a temporal I_D change in the CNT network transistor.

Fig. 1c and Fig. 1d depict the transient I_D response following the application of a single V_G pulse. We designed two different conditions for the V_G pulses. In case #1, all traps were initially filled with holes by applying a negative V_G bias (-6 V for 1 s). The V_G pulse was designed such that the low level of the pulse (V_{low}) was negative (-2 V), and the high level of the pulse (V_{high}) was positive ($+10$ V). The magnitude of V_{low} was sufficiently small to prevent any hole trapping/detrapping processes. When this V_G pulse (-2 V to $+10$ V) was applied for 50 ns, the trapped holes at the interface trap were ejected through the tunneling process (case #1 in Fig. 1b). The emptied interface trap was then re-filled gradually from holes at the surface trap through the

diffusion process. As a result, I_D increased suddenly and then gradually decreased to its initial state (Fig. 1c). In case #2, all the traps were initially emptied by applying a positive V_G bias ($+6$ V for 1 s). In this case, we designed the V_G pulse to have $V_{low} = -10$ V and $V_{high} = +2$ V. When this V_G pulse was applied—from $+2$ V to -10 V—the interface trap was filled with holes through the tunneling process (case #2 in Fig. 1b). However, because these trapped holes were easily ejected again through the tunneling process, the temporal I_D enhancement returned to its initial state as soon as the pulse ended (Fig. 1d). Consequently, a gradual and temporal I_D change could be obtained in the CNT network transistor by exploiting the different time responses of the hole trapping/detrapping process at the interface and surface traps.

The stochastic hole trapping/detrapping process has an intrinsic cycle-to-cycle variation. Because the tunneling and diffusion processes do not occur in a single CNT but in an entangled CNT network, the temporal I_D response to the same V_G pulse is not identical in every trial. Fig. 2a presents an example of the cycle-to-cycle variation in the temporal I_D responses (here, a resistor (R_S) is serially connected with the source electrode to convert the I_D value into the voltage value (V_{temp}), as shown in the inset of Fig. 2a). Despite applying the V_G pulse under the same conditions, differences occur among the measured I_D responses. Fig. 2b presents the V_{temp} from 12000 trials, where V_{temp} was sampled $10 \mu\text{s}$ after the applied V_G pulse. The collected V_{temp} data are close to a uniform distribution, which implies that the stochastic hole movement in the CNT network exhibits true randomness and is not determined by a specific physical mechanism. Therefore, the intrinsic cycle-to-cycle variation of the temporal I_D response can be used as a physical source of randomness for TRNG implementation. The driving current

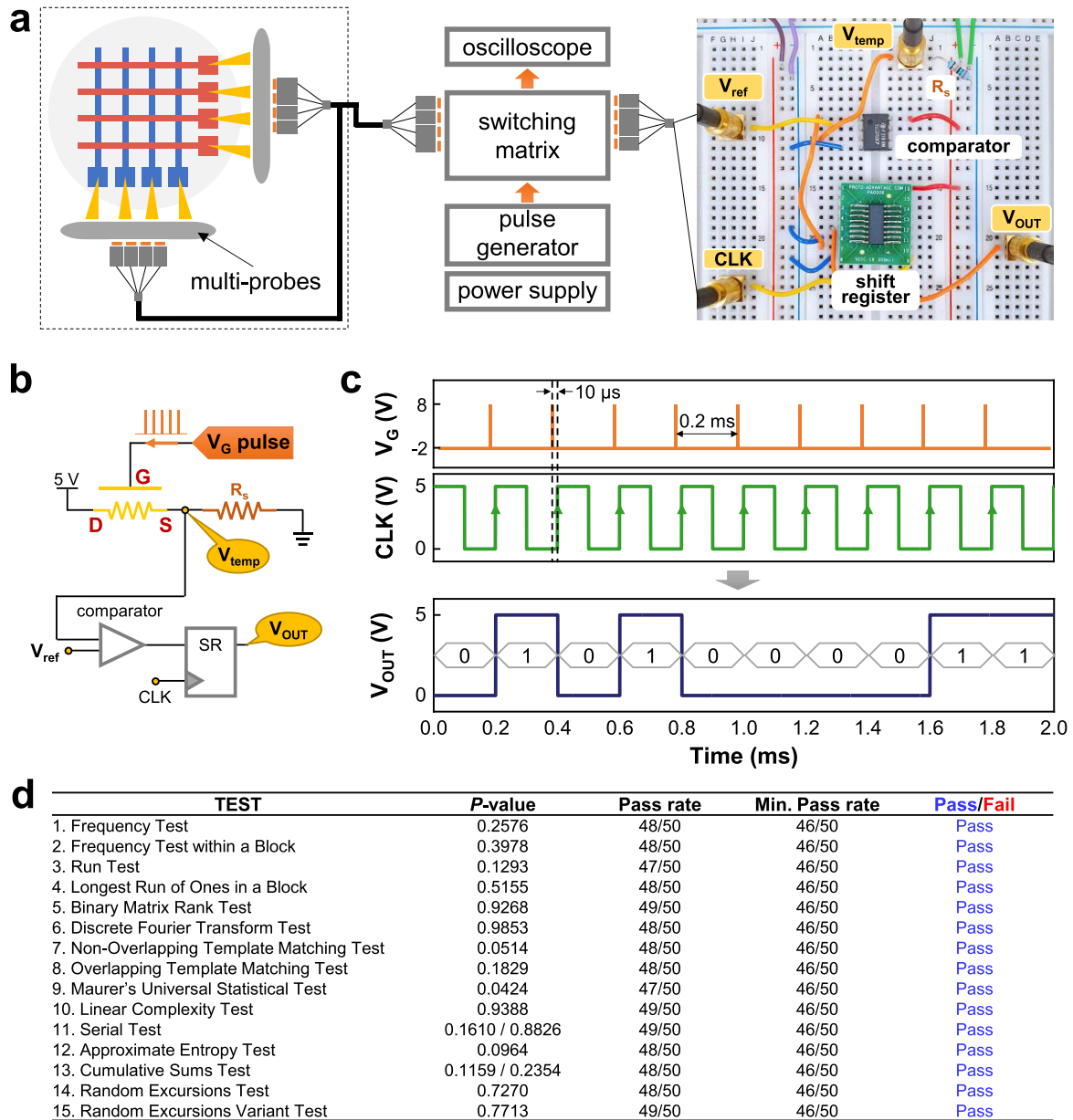


FIGURE 3. Implementation of the TRNG. (a) Schematics of the measurement setup. (b) Circuit diagram of the TRNG. (c) Timing information of the V_G pulse train, clock signal, and output of the TRNG. (d) The result of the NIST randomness test, where all tests were passed.

required for a temporal I_D switching (of the order of several tens of nanoamperes, as shown in Fig. 1c) is smaller than that required by prior volatile memristors (typically exceeding $1 \mu A$ [7], [11]), thereby exhibiting great potential for low-power TRNG implementation. In addition, volatile memristors have poor thermal stability because temperature critically affects ion movement [20]; however, the electronic process attributed to the hole trapping/detrapping in the CNT network exhibits better thermal stability and higher reliability [9], [21]. Furthermore, the CNT network is formed by a simple solution process and offers excellent CMOS compatibility.

Fig. 3a presents our experimental setup, in which the TRNG operation was implemented by integrating the CNT network transistor with a simple circuit built on a breadboard. The CNT network transistor crossbar array (see Methods and Supporting Information Note 2) was connected to the circuit through a switching matrix. The pulse generator generated the V_G pulse and the clock signal, and the power supply generated the reference voltage for the comparator. The random bitstream output from the TRNG was monitored using an oscilloscope. To demonstrate the TRNG operation, we exploited a comparator and a shift register (Fig. 3b). Because the V_{temp} response to the V_G pulse has an intrinsic

variation (Fig 2b), a random bit of “0” (0 V) or “1” (5 V) can be generated by comparing V_{temp} with a specific reference voltage (e.g., $V_{\text{ref}} = 1$ V) via the comparator. As shown in Fig. 3c, we designed the V_G pulse train with a width of 50 ns and a spacing of 0.2 ms (i.e., a frequency of 5 kHz). The clock signal also had the same frequency as the V_G pulse train but was not in phase, with the rising edge being delayed by 10 μs from each V_G pulse. Consequently, a random bit was determined by the sampled V_{temp} value 10 μs after each applied V_G pulse. Subsequently, the shift register generated a continuous random bitstream (V_{OUT}) based on the rising edge of the clock signal. To assess the randomness of the generated bitstream, we performed the NIST randomness test [22] for 50 sequences of 10^6 bits. Fig. 3d presents the results of 15 NIST tests, where each test was considered to have been ‘passed’ if the P -value was greater than 0.01 and the pass rate exceeded the minimum value defined by NIST. Notably, all 15 NIST tests were passed, and the bit generation rate obtained for our TRNG was 5 kb s^{-1} , which is sufficient for several encryption applications [23]. Our TRNG achieved a generation rate (5 kb s^{-1}) similar to those of previous volatile memristor-based TRNGs (bit generation rate = 16 kb s^{-1}) [9] without the help of additional peripheral circuits (i.e., a nonlinear feedback shift register circuit), exhibiting good potential for low-power TRNG implementation.

III. CONCLUSION

We demonstrated a TRNG using stochastic carrier trapping/detrapping processes in a randomly distributed CNT network. By appropriately biasing the CNT network transistor to have a temporal I_D response, stochastic cycle-to-cycle variation was exploited to generate a random bitstream. Notably, this electronic process in the CNT network transistor exhibits lower power consumption and higher reliability than previous memristor-based TRNGs. Moreover, solution-processed CNT networks are compatible with existing CMOS technology. The output bits generated by the TRNG passed all the NIST randomness tests without using additional complex circuits. This study provides a pathway for the development of low-cost and energy-efficient security devices in the IoT era.

IV. EXPERIMENTAL SECTION

A. FABRICATION OF CNT TRANSISTOR CROSSBAR ARRAY

CNT transistors were fabricated on p-doped rigid silicon substrates with a 50 nm thick thermally grown SiO_2 layer. To form the local back-gate used to modulate the channels in the CNT transistors, a Ti layer with a thickness of 20 nm was deposited via e-beam evaporation and patterned using a subsequent lift-off process. An Al_2O_3 layer (thickness of 40 nm) and a SiO_2 layer (thickness of 10 nm) were then deposited sequentially by atomic layer deposition to form a gate insulator. The top surface of the SiO_2 layer was then functionalized with a 0.1 g/mL poly-L-lysine solution for 20 min to form an amine-terminated layer which acted as an effective adhesion layer for the deposition of the CNTs.

The CNT network channel was then formed by immersing the chip into a 0.01 mg/mL 99% semiconducting CNT solution (NanoIntegris, Inc.) for eight minutes at 100 °C. The source/drain electrodes—consisting of Ti and Pd layers (2 nm and 30 nm, respectively)—were then deposited and patterned using conventional thermal evaporation and a lift-off process, respectively. Thereafter, additional photolithography and oxygen plasma etching steps were conducted to remove the excess CNTs, i.e., those not in the channel area, thereby isolating the devices from one another. Finally, to form the crossbar array, Cu (thickness of 80 nm) and SiO_x (thickness of 150 nm) were sequentially deposited and patterned to form the metal line and the dielectric interlayer, respectively.

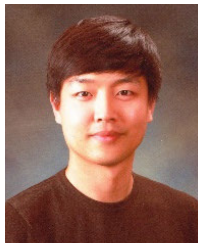
V. ACKNOWLEDGMENT

(Sungho Kim and Moon-Seok Kim contributed equally to this work.)

REFERENCES

- [1] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. Varanano, “A high-speed oscillator-based truly random number source for cryptographic applications on a smart card IC,” *IEEE Trans. Comput.*, vol. 52, no. 4, pp. 403–409, Apr. 2003.
- [2] R. Brederlow, R. Prakash, C. Paulus, and R. Thewes, “A low-power true random number generator using random telegraph noise of single oxide-traps,” in *IEEE Int. Solid State Circuits Conf. Dig. Tech. Papers*, Feb. 2006, pp. 1666–1675.
- [3] S. Yasuda, H. Satake, T. Tanamoto, R. Ohba, K. Uchida, and S. Fujita, “Physical random number generator based on MOS structure after soft breakdown,” *IEEE J. Solid-State Circuits*, vol. 39, no. 8, pp. 1375–1377, Aug. 2004.
- [4] M. A. Khan and K. Salah, “IoT security: Review, blockchain solutions, and open challenges,” *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018.
- [5] S. Balatti, S. Ambrogio, R. Carboni, V. Milo, Z. Wang, A. Calderoni, N. Ramaswamy, and D. Ielmini, “Physical unbiased generation of random numbers with coupled resistive switching devices,” *IEEE Trans. Electron Devices*, vol. 63, no. 5, pp. 2029–2035, May 2016.
- [6] T. Zhang, M. Yin, C. Xu, X. Lu, X. Sun, Y. Yang, and R. Huang, “High-speed true random number generation based on paired memristors for security electronics,” *Nanotechnology*, vol. 28, no. 45, Oct. 2017, Art. no. 455202.
- [7] H. Jiang, D. Belkin, S. E. Savel'ev, S. Lin, Z. Wang, Y. Li, S. Joshi, R. Midya, C. Li, M. Rao, M. Barnell, Q. Wu, J. J. Yang, and Q. Xia, “A novel true random number generator based on a stochastic diffusive memristor,” *Nature Commun.*, vol. 8, no. 1, p. 882, Dec. 2017.
- [8] K. S. Woo, Y. Wang, J. Kim, Y. Kim, Y. J. Kwon, J. H. Yoon, W. Kim, and C. S. Hwang, “A true random number generator using threshold-switching-based memristors in an efficient circuit design,” *Adv. Electron. Mater.*, vol. 5, no. 2, Feb. 2019, Art. no. 1800543.
- [9] K. S. Woo, Y. Wang, Y. Kim, J. Kim, W. Kim, and C. S. Hwang, “A combination of a volatile-memristor-based true random-number generator and a nonlinear-feedback shift register for high-speed encryption,” *Adv. Electron. Mater.*, vol. 6, no. 5, May 2020, Art. no. 1901117.
- [10] R. Wang, J.-Q. Yang, J.-Y. Mao, Z.-P. Wang, S. Wu, M. Zhou, T. Chen, Y. Zhou, and S.-T. Han, “Recent advances of volatile memristors: Devices, mechanisms, and applications,” *Adv. Intell. Syst.*, vol. 2, no. 9, Sep. 2020, Art. no. 2000055.
- [11] B. Dang, J. Sun, T. Zhang, S. Wang, M. Zhao, K. Liu, L. Xu, J. Zhu, C. Cheng, L. Bao, Y. Yang, H. Wang, Y. Hao, and R. Huang, “Physically transient true random number generators based on paired threshold switches enabling Monte Carlo method applications,” *IEEE Electron Device Lett.*, vol. 40, no. 7, pp. 1096–1099, Jul. 2019.
- [12] D. Akinwande, S. Yasuda, B. Paul, S. Fujita, G. Close, and H.-S.-P. Wong, “Monolithic integration of CMOS VLSI and carbon nanotubes for hybrid nanotechnology applications,” *IEEE Trans. Nanotechnol.*, vol. 7, no. 5, pp. 636–639, Sep. 2008.

- [13] Z. Hu, J. M. M. L. Comeras, H. Park, J. Tang, A. Afzali, G. S. Tulevski, J. B. Hannon, M. Liehr, and S.-J. Han, "Physically unclonable cryptographic primitives using self-assembled carbon nanotubes," *Nature Nanotechnol.*, vol. 11, no. 6, pp. 559–565, Jun. 2016.
- [14] W. A. Gaviria Rojas, J. J. Mcmorrow, M. L. Geier, Q. Tang, C. H. Kim, T. J. Marks, and M. C. Hersam, "Solution-processed carbon nanotube true random number generator," *Nano Lett.*, vol. 17, no. 8, pp. 4976–4981, Aug. 2017.
- [15] Y. Sun and D. Wen, "Physically transient random number generators based on flexible carbon nanotube composite threshold switching," *J. Alloys Compounds*, vol. 844, Dec. 2020, Art. no. 156144.
- [16] S. Kim, Y. Lee, H.-D. Kim, and S.-J. Choi, "Precision-extension technique for accurate vector–matrix multiplication with a CNT transistor crossbar array," *Nanoscale*, vol. 11, no. 44, pp. 21449–21457, Nov. 2019.
- [17] S. Kim, Y. Lee, H.-D. Kim, and S.-J. Choi, "Parallel weight update protocol for a carbon nanotube synaptic transistor array for accelerating neuromorphic computing," *Nanoscale*, vol. 12, no. 3, pp. 2040–2046, Jan. 2020.
- [18] S. Kim, Y. Lee, H.-D. Kim, and S.-J. Choi, "16-bit fixed-point number multiplication with CNT transistor dot-product engine," *IEEE Access*, vol. 8, pp. 133597–133604, 2020.
- [19] R. S. Park, M. M. Shulaker, G. Hills, L. S. Liyanage, S. Lee, A. Tang, S. Mitra, and H.-S.-P. Wong, "Hysteresis in carbon nanotube transistors: Measurement and analysis of trap density, energy level, and spatial distribution," *ACS Nano*, vol. 10, no. 4, pp. 4599–4608, Apr. 2016.
- [20] Z. Wang, M. Rao, R. Midya, S. Joshi, H. Jiang, P. Lin, W. Song, S. Asapu, Y. Zhuo, C. Li, H. Wu, Q. Xia, and J. J. Yang, "Threshold switching of ag or cu in dielectrics: Materials, mechanism, and applications," *Adv. Funct. Mater.*, vol. 28, no. 6, Feb. 2018, Art. no. 1704862.
- [21] D. S. Jeong, K. M. Kim, S. Kim, B. J. Choi, and C. S. Hwang, "Memristors for energy-efficient new computing paradigms," *Adv. Electron. Mater.*, vol. 2, no. 9, Sep. 2016, Art. no. 1600090.
- [22] A. Rukhin, J. Soto, and J. Nechvatal, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," *NIST Spec. Publ.*, vol. 22, pp. 22–800, Apr. 2010.
- [23] C.-Y. Huang, W. C. Shen, Y.-H. Tseng, Y.-C. King, and C.-J. Lin, "A contact-resistive random-access-memory-based true random number generator," *IEEE Electron Device Lett.*, vol. 33, no. 8, pp. 1108–1110, Aug. 2012.



SUNGHO KIM received the M.S. and Ph.D. degrees in electrical engineering from the Korea Advanced Institute of Science and Technology (KAIST), Republic of Korea, in 2008 and 2012, respectively. He is currently an Associate Professor in electrical engineering at Sejong University, Republic of Korea. His current research interests include neuronal and synaptic nano-devices for neuromorphic systems and at both device and circuit levels.

MOON-SEOK KIM received the B.S. degree from Chung-Ang University, Seoul, Republic of Korea, in 2011, and the M.S. degree from the Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Republic of Korea, in 2013. He is currently pursuing the Ph.D. degree with ETRI. He is also a Senior Researcher with ETRI. His current research interests include triboelectric energy harvesting and security devices, such as physically unclonable functions and true random number generators.



YONGWOO LEE received the B.S. degree in electrical engineering from the School of Electrical Engineering, Kookmin University, Seoul, Republic of Korea, where he is currently pursuing the Ph.D. degree.



HEE-DONG KIM received the B.S., M.S., and Ph.D. degrees in electrical engineering from Korea University, Seoul, Republic of Korea, in 2007, 2009, and 2014, respectively. From 2014 to 2015, he was with the Technology Department, Leibniz-Institut für innovative Mikroelektronik (IHP), Germany, as a Postdoctoral Fellow. He is currently with the Department of Electrical Engineering, Sejong University. His current research interests include electrical/optical semiconductor devices and nonvolatile memory devices.



YANG-KYU CHOI received the B.S. and M.S. degrees from Seoul National University, Seoul, Republic of Korea, in 1989 and 1991, respectively, and the Ph.D. degree from the University of California at Berkeley, Berkeley, in 2001. He is currently a Distinguished Professor with the School of Electrical Engineering, Korea Advanced Institute of Science and Technology (KAIST). He has authored or coauthored more than 420 articles and he holds more than 20 U.S. patents and 100 Korean patents. He received the Sakrison Award for the Best Dissertation from the Department of Electrical Engineering and Computer Sciences, University of California at Berkeley, Berkeley, in 2002. He was also a recipient of the Scientist of the Month Award from the Ministry of Science and Technology, Republic of Korea, in July 2006.



SUNG-JIN CHOI received the Ph.D. degree in electrical engineering from the Korea Advanced Institute of Science and Technology, Daejeon, Republic of Korea, in 2012. He is currently an Associate Professor with the School of Electrical Engineering, Kookmin University, Seoul, Republic of Korea.

...