JOURNAL OF SEMICONDUCTOR TECHNOLOGY AND SCIENCE, VOL. 23, NO. 6, DECEMBER, 2023 ISSN(Print) 1598-1657
https://doi.org/10.5573/JSTS.2023.23.6.396 ISSN(Online) 2233-4866

A Single-ring-oscillator based True-random-number-generator with 3-edges Collapse

Eunhwan Kim[1] and Jae-Joon Kim[2]

Abstract—**This paper presents an all-digital ring oscillator (RO) based true random number generator (TRNG) that harvests entropy as a jitter. The proposed TRNG constructs upon the collapsing RO-based structure and exhibits high immunity against external power attacks. This approach senses the 3-edge collapse point using a single RO without a reference RO, reducing both area and energy consumption. A prototype chip fabricated using 65 nm technology operates between 1.08 V and 1.44 V, occupying an area of 702 μm^2. The randomness of the TRNG passed the NIST randomness test up to 2 LSB when the external power attack was below 300 mV_{PP}. This work demonstrates a throughput of 7.1 Mbits/s at 1.2 V and provides an efficiency of 40.93 Mbit/mJ at 1.08 V.**

Index Terms—**Cryptography, frequency collapse, hardware security, ring oscillator (RO), true random number generator (TRNG)**

I. INTRODUCTION

CMOS true random number generators (TRNGs) serve a key role as essential components in security integrated circuits [1-14]. As Internet of Things (IoT) devices become more popular, it is expected that the need for lightweight CMOS TRNG circuits will grow further in the future [15]. Additionally, high-quality random numbers (RNs) are indispensable for stochastic computing, machine learning/deep learning, and Ising machines designed for combinatorial optimization problems [16-18]. For applications that require high levels of security, TRNGs are favored over pseudo-random number generators (PRNGs), which generate bit sequences with fixed patterns based on a given seed. The distinguishing feature between TRNGs and PRNGs is that TRNGs generate RNs using an entropy source based on unpredictable physical noise. CMOS TRNGs typically produce random bits leveraging device-level noise such as thermal or flicker noise. TRNG types are categorized based on their use of noise amplification [7], metastability [8], and chaotic map [9] as entropy sources. There are also efforts to extend functionality by combining TRNG with a physically unclonable function (PUF), a main feature in hardware security [10]. Further advancements include attempts to embed TRNG functionality into existing memory [11].

One popular type is the ring oscillator (RO) based TRNG, which leverages timing jitter [1-6]. The throughput of RO-based TRNGs (RO-TRNGs) is relatively low, but they are known to consume lower power and occupy a small area. Hence, RO-TRNGs are repeatedly used in power-constrained IoT and portable devices. However, for an RO to function as a good entropy source, RO-TRNGs need to be tolerant to power injection noise, and the trip voltage of the inverter is required to be well-defined [6]. Numerous efforts have aimed to resolve issues within conventional RO-TRNGs. In [2], three fundamental frequencies are initiated simultaneously in the RO and then are reduced to a

Manuscript received Nov. 1, 2023; reviewed Nov. 10, 2023; accepted Nov. 13, 2023
[1]Dept. of Electrical Engineering, Pohang University of Science and Technology (POSTECH), 77, Cheongam-ro, Nam-gu, Pohang-si, Gyeongsangbuk-do, Korea 37673
[2]Dept. of Electrical and Computer Engineering, Seoul National University, 1 Gwanak-ro, Gwanak-gu, Seoul, Korea 08826
E-mail : eunhwan@postech.ac.kr, kimjaejoon@snu.ac.kr

single signal. The time from initiation to collapse serves as the entropy source for the TRNG. A characteristic of [2] is that as the number of RO stages increases, the TRNG robustness is enhanced because the oscillating signal is less likely to be affected by signal-path mismatches. However, this TRNG significantly increases power and area consumption by employing an additional RO to detect the collapse point. Other collapsing RO-TRNGs have adopted methods to modify the signal path to reduce signal-path mismatches [3, 5]. E. Kim et al. [4] adopted a differential structure with feedback resistance to reduce the mismatch in the RO cell and enhance immunity to power noise.

In this paper, we propose a different structure for the collapsing RO-TRNG. Previous collapsing RO-TRNGs require additional circuits to detect the collapse cycle or face the challenge of estimating the operating frequency based on measurements [2, 3, 5]. In Section II, we present the structure of the TRNG that reduces the two ROs of the [2] structure to a single RO and explain its block diagram and operation. Section III provides peripheral circuits for chip measurement and the corresponding results. We conclude this paper in Section IV.

II. The Proposed TRNG

1. Analysis of Collapsing RO-TRNG

We illustrate an RO of the TRNG implemented with fully digital logic (Fig. 1). The RO operates initially at a 3x frequency of steady-state RO because it generates three edges row by row due to the reset pulse. The entropy source is created by accumulating jitter during the time it takes for two of the three edges to intersect and subsequently collapse, returning to the 1x frequency. The time difference T_D between the two edges is approximated by Barkhausen's criteria, expressed as

$$T_D \approx 2/3 \cdot n \cdot t_p \tag{1}$$

where n represents the number of RO stages; t_p is the average propagation delay of a NAND gate. Thus, the accumulated jitter until the occurrence of two edge collapses can be expressed as

$$\Sigma(t_{1,J} + t_{2,J}) \geq T_D - \Sigma \Delta t_s \tag{2}$$

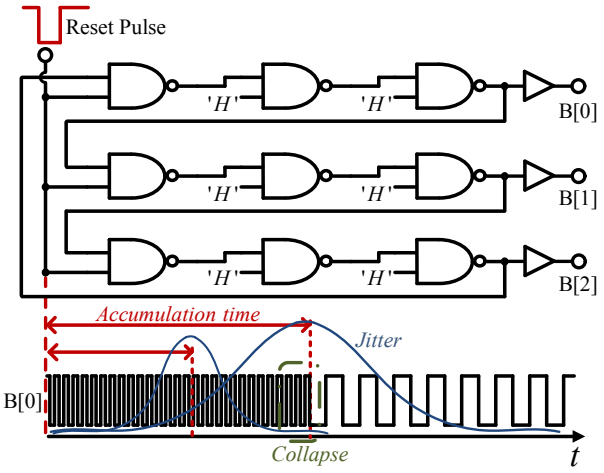

Fig. 1. The schematic of a ring-oscillator with 3-edge collapses [2], composed of 2-NAND gates.

where Δt_s represents the skew of the two edge signals that occur as they pass through each NAND gate. $t_{1,J}$ and $t_{2,J}$ represent the jitter for the first and second edge signals, respectively, produced by each NAND gate due to physical noise [3]. Hence, we can modulate by controlling the n of the T_D to extend the average collapse time, obtaining a more unpredictable source influenced by the accumulated t_J during the increased time. The change in n causes a proportional shift in the granularity of each row of RO, resulting in a corresponding variation in Δt_s [2]. The jitter t_J, which accumulated more physical noise, inherently exhibits a more complex random walk. As T_D increases and Δt_s decreases, it becomes an excellent entropy source with an inverse Gaussian distribution.

2. Implementation of Proposed TRNG

We depict the block diagram of the proposed TRNG (Fig. 2) and explain its operation through a timing diagram (Fig. 3). In Fig. 1, the TRNG begins its operation as an entropy source initiated by a reset pulse driven by an external clock. The RO that generates 3-edges sends its three outputs to a majority voter. A typical majority voter, composed of four NAND gates, generates a signal (MV) that maintains a constant 3x frequency regardless of the signal collapse (Fig. 3). Before the collapse, both MV and RO outputs (B[0:2]) operate at the 3x frequency and in phase. However, after the collapse of the RO, although all B[0:2] outputs

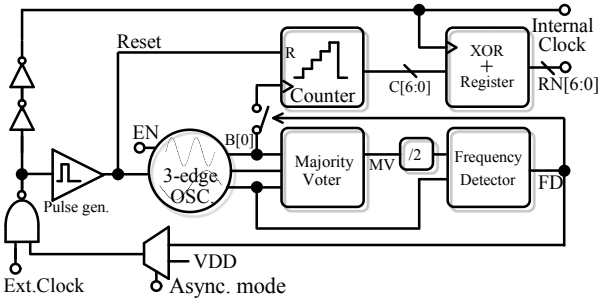

Fig. 2. Block diagram of the proposed TRNG.

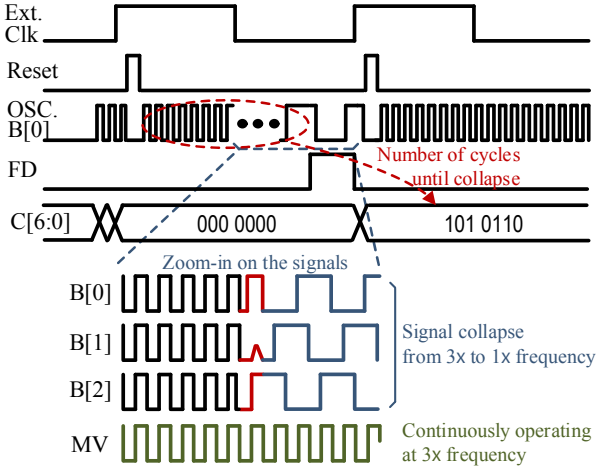

Fig. 3. Timing diagram of the proposed TRNG.

transition to a 1x frequency, MV continues to maintain a 3x frequency because the phase differences among the signals remain at 60°. MV is divided by half frequency (1.5x) and forwarded to a frequency detector, which compares with the RO output (B[2]). As the 3-edges collapse, the FD signal becomes 'H'. FD signal controls a switch that determines whether the RO output is transmitted to a counter, which then accumulates the number of cycles up to the collapse time. The counter outputs are sent to an XOR + shift register array synchronized with an external clock, enhancing entropy and generating a random number [4]. In Fig 2, TRNG can operate in an asynchronous mode concerning the clock. In asynchronous mode, the TRNG operates autonomously at its maximum or minimum speed, which facilitates the determination of an optimal clock for measurement.

3. Comparison with Related RO-TRNGs

The proposed TRNG maintains the advantages of the more straightforward collapsing RO-based structure seen in [2], which can be fabricated using fully digital logic, occupies a small area, and offers immunity against external attacks. Compared to [2], our approach allows for the detection of the moment the 3-edge collapses without a reference RO, thereby cutting both the area occupied by the reference RO and its power consumption in half. Previous collapsing RO-based TRNGs [3, 5] face challenges in detecting the point of collapse without oscillating signal, thereby requiring the aid of an extra host processor or making multiple measurements to infer the collapse moment. The phase-shifting method uses feedback resistors and differential structures inherent in analog circuit design, adding to the complexity of the design [4]. Conversely, our work provides the benefit of autonomously detecting the collapse time with a fully digital single RO.

III. Testing Environment and Results

RO-TRNGs are vulnerable to the issue of producing fixed or specific patterned values under strong power injection attacks of specific frequencies from external sources [6]. We established peripheral circuits to test the TRNG against power injection attacks (Fig. 4). We implemented two separate circuits for low and high-frequency injections to test a broad range of frequencies. For low-frequency injections into the TRNG, we utilized a function generator, and to measure the amount of power being injected, a unity gain buffer was set up as a monitoring circuit. When the injected frequency exceeds several hundred megahertz, accurately injecting a specific magnitude becomes difficult. Such high frequencies are internally generated by a PLL, regulated in magnitude by a high-voltage driver, and then injected into the TRNG. The unity gain buffer tracks the common voltage, and the hysteresis comparator activates when the magnitude of the attack injected into the TRNG exceeds the TH/TL thresholds and outputs a frequency that is a quarter of the injected frequency.

We fabricated a prototype chip in 65 nm technology and showed the random bit sequence measured with an oscilloscope at 1.2 V (Fig. 5). The single RO is constructed from NAND gates arranged in 3x5 stages and occupies an area of 285 μm^2. Including the peripheral circuits, the total area is 702 μm^2. The PLL

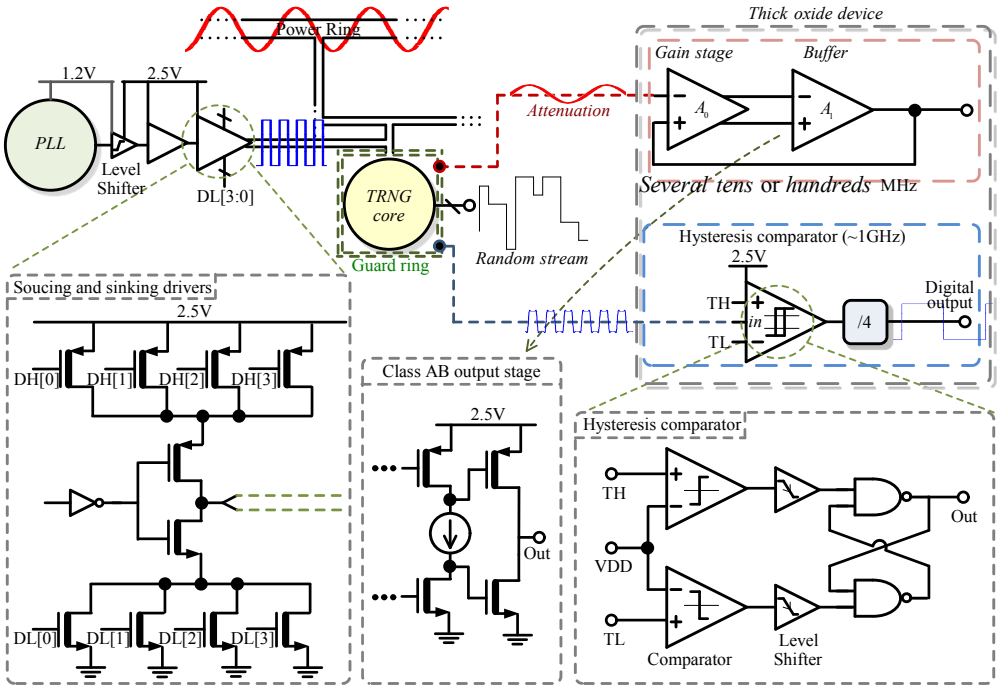

Fig. 4. Power injection attack and monitoring circuit.

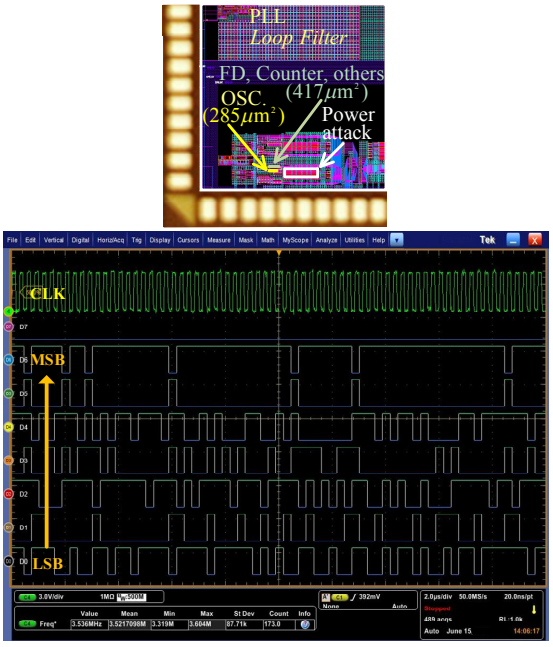

Fig. 5. Layout and measured bit stream.

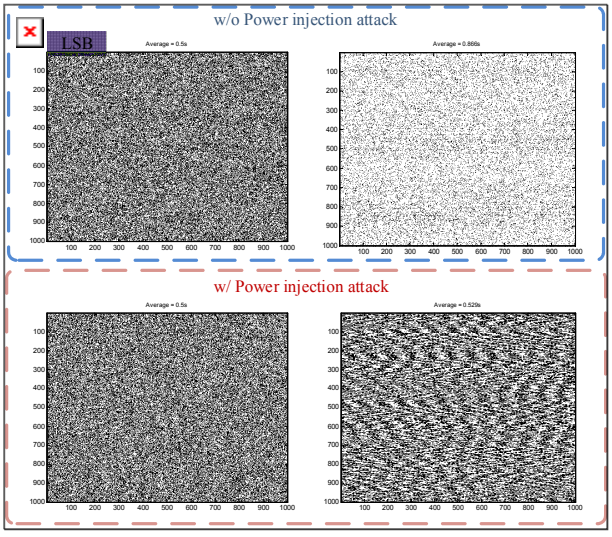

Fig. 6. Bit sequences under power attack: LSB vs. upper bit.

and the driver for the power attack are positioned around the TRNG core in the layout.

Fig. 6 illustrates the change in the random bit sequence of the TRNG when a power attack is injected. Two-bit streams (LSB and 5th LSB) are represented using 'black/white' to indicate the '0/1' states. Fig. 6 top shows the 1 Mbits without a power attack, while the bottom displays the bit stream during the low-frequency injection of a strong power attack with 0.6 V_{PP}. In both cases, the LSB retains good random bits. However, the upper bits exhibit a specific pattern and lose their randomness depending on the injected frequency. We utilized the NIST randomness test to precisely evaluate the randomness of each bit stream [19]. The results from testing 1Mbits generated 100 times are presented in

Table 1. NIST randomness test

NIST SP 800-22. Rev1a	No attack				Injection attack (Amplitude : 0.3 Vpp)			
	Operating Voltage : 1.2V				RO. Frequency (Worst case)			
Minimum pass rate = 0.951	2nd LSB		3rd LSB		1st LSB		2nd LSB	
	p value	prop.	p value	prop.	p value	prop.	p value	prop.
Frequency	0.198	0.958	0.158	0.733	0.243	0.967	0.024	0.800
Block Frequency	0.218	0.967	0.058	0.733	0.517	1.000	0.262	0.933
Cumulative Sums	0.159	0.963	0.062	0.733	0.258	0.958	0.035	0.800
Runs	0.291	0.958	0.171	0.733	0.227	1.000	0.254	0.867
Longest Run	0.371	1.000	0.682	1.000	0.368	1.000	0.388	1.000
Rank	0.642	1.000	0.402	1.000	0.461	1.000	0.527	1.000
FFT	0.342	1.000	0.502	1.000	0.373	1.000	0.635	1.000
Non Overlapping Temp.	0.393	0.997	0.429	0.948	0.495	1.000	0.458	0.998
Overlapping Temp.	0.297	0.967	0.295	0.800	0.420	1.000	0.457	0.933
Universal	0.197	1.000	0.637	0.933	0.590	1.000	0.702	1.000
Approximate Entropy	0.219	0.967	0.252	0.800	0.654	1.000	0.388	1.000
Random Excursions	0.325	1.000	0.309	1.000	0.408	1.000	0.091	1.000
Random Excursions Var.	0.303	1.000	0.351	1.000	0.264	1.000	0.136	1.000
Serial	0.185	1.000	0.370	0.933	0.361	1.000	0.632	1.000
Linear Complexity	0.362	1.000	0.483	1.000	0.477	1.000	0.254	1.000

Each test using 100x1 Mbits

Table 2. Comparison with previous works

	This work		TIFS'23 [14]	TCASII'20 [13]	SSCL'20 [12]	TCASII'22 [5]	ISSCC'17 [4]	JSSC'16 [3]	ISSCC'14 [2]
Technology	65 nm		180 nm	65 nm	65 nm	40 nm	65 nm	45 nm	65 nm
Entropy Type	RO (Jitter)		ROs (Jitter)+ Chaotic map	SAR (residue) + charge injt.	$\Delta\sum$ (q-noise)	RO (Jitter)	RO (Jitter)	RO (Jitter)	RO (Jitter)
Supply voltage (measured)	1.08 V	1.2 V	1.8 V	0.8 V	0.8 V	0.9 V	1.08 V	0.9 V	0.9 V
Bit Rate (Mbit/s)	6.5	7.1	450	1.3	52.0	6.3	8.2	2	2.8
Power (mW)	0.158	0.249	N/A	0.270	0.360	0.067	0.289	0.046	0.159
Effciency (Mbit/mJ)	40.93	28.34	30.30	4545.45	144.93	93.46	28.19	43.48	17.54
Area (μm^2)	702		62000	90000	60000	306	920	836	960
Operating Voltage	1.08~1.44 V		1.4~3.2 V	0.6~1.2 V	0.8~1.2 V	0.5~1.4 V	1.08~1.44 V	0.6~1 V	N/A
Power attack	Up to 250 mVpp*		N/A	N/A	140 mVpp	600 mVpp	400 mVpp	400 mVpp	380 mVpp

*2 LSBs pass all NIST tests.

Table 1. Without a power attack, two-bit streams up to the 2nd LSB passed the NIST results, but during a power attack at the oscillating frequency of RO with 0.3 V_{PP}, only the LSB passed.

We have summarized and compared previous TRNGs and their key features with our design (Table 2). Table 2 shows that our design has a smaller area and higher throughput than previous RO-TRNG styles.

IV. CONCLUSIONS

In this paper, we introduced a collapsing RO-based TRNG composed of 15 stages using 65 nm technology, and our contributions are as follows: (i) This work is implemented entirely with digital logic and senses the 3-edge collapse moment without requiring the reference RO. (ii) Entropy source composed of a single RO has improved energy and area efficiency. (iii) We proposed a configuration of peripheral circuits for testing against externally injected power attacks, confirming the robustness of the TRNG. Evaluation results from the NIST randomness test showed that the proposed TRNG exhibited sufficient randomness performance up to the 2nd LSB. This work offers high efficiency, compactness, and excellent production capabilities, making it suitable for portable applications.

ACKNOWLEDGMENTS

The chip fabrication and EDA tool were supported by the IC Design Education Center(IDEC), Korea.

REFERENCES

[1] P. Choi, J. H. Kim, and D. K. Kim, “Improving Ring-Oscillator-based True Random Number Generators using Multiple Sampling,” JSTS, Vol. 19, No. 4, June, 2019.

[2] K. Yang, D. Fick, M. B. Henry, Y. Lee, D. Blaauw and D. Sylvester, "16.3 A 23Mb/s 23pJ/b fully synthesized true-random-number generator in 28nm and 65nm CMOS," *Solid-State Circuits Conference, 2014. ISSCC 2014. Digest of Technical Papers. IEEE International*, 9-13, pp. 280-281, Feb., 2014.

[3] K. Yang, D. Blaauw and D. Sylvester, "An All-Digital Edge Racing True Random Number Generator Robust Against PVT Variations," *Solid-State Circuits, IEEE Journal of*, Vol. 51, No. 4, pp. 1022-1031, Apr., 2016.

[4] E. Kim, M. Lee and J. -J. Kim, "8.2 8Mb/s 28Mb/mJ robust true-random-number generator in 65nm CMOS based on differential ring oscillator with feedback resistors," *Solid-State Circuits Conference, 2017. ISSCC 2017. Digest of Technical Papers. IEEE International*, 5-09, pp. 144-145, Feb., 2017.

[5] J. Park, B. Kim and J. -Y. Sim, "A PVT-Tolerant Oscillation-Collapse-Based True Random Number Generator With an Odd Number of Inverter Stages," *Circuits and Systems II: Express Briefs, IEEE Transactions on*, Vol. 69, No. 10, pp. 4058-4062, Oct., 2022.

[6] A. T. Markettos, A. Theodore, and S. W. Moore, "The frequency injection attack on ring-oscillator-based true random number generators," *Cryptographic Hardware and Embedded Systems*, *International Workshop on*, 6-9, pp. 317-331, Sep., 2009.

[7] J. Brown et al., "A low-power and high-speed True Random Number Generator using generated RTN," *VLSI Technology*, *2018 IEEE Symposium on,* 18-22, pp. 95-96, June, 2018.

[8] S. K. Mathew et al., "2.4 Gbps, 7 mW All-Digital PVT-Variation Tolerant True Random Number Generator for 45 nm CMOS High-Performance Microprocessors," *Solid-State Circuits*, *IEEE Journal of*, vol. 47, no. 11, pp. 2807-2821, Nov., 2012.

[9] P. Z. Wieczorek and K. Gołofit, "True Random Number Generator Based on Flip-Flop Resolve Time Instability Boosted by Random Chaotic Source," *Circuits and Systems I: Regular Papers*, *IEEE Transactions on*, vol. 65, no. 4, pp. 1279-1292, Apr., 2018.

[10] S. Satpathy et al., "An All-Digital Unified Static/Dynamic Entropy Generator Featuring Self-Calibrating Hierarchical Von Neumann Extraction for Secure Privacy-Preserving Mutual Authentication in IoT Mote Platforms," *VLSI Circuits, IEEE Symposium on*, 18-22, pp. 169-170, Jun., 2018.

[11] S. Taneja, V. K. Rajanna and M. Alioto, "36.1 Unified In-Memory Dynamic TRNG and Multi-Bit Static PUF Entropy Generation for Ubiquitous Hardware Security," *Solid-State Circuits Conference, 2021. ISSCC 2021. Digest of Technical Papers. IEEE International*, 13-22, pp. 498-500, Feb., 2021.

[12] S. T. Chandrasekaran, V. E. G. Karnam and A. Sanyal, "0.36-mW, 52-Mbps True Random Number Generator Based on a Stochastic Delta–Sigma Modulator," *Solid-State Circuits Letters, in IEEE*, vol. 3, pp. 190-193, Jul., 2020,

[13] A. Jayaraj, N. Nitin Gujarathi, I. Venkatesh and A. Sanyal, "0.6–1.2 V, 0.22 pJ/bit True Random Number Generator Based on SAR ADC," *Circuits and Systems II: Express Briefs, IEEE Transactions on*, vol. 67, no. 10, pp. 1765-1769, Oct. 2020.

[14] X. Wei, L. Xiu and Y. Cai, "A Perspective of Using Frequency-Mixing as Entropy in Random Number Generation for Portable Hardware Cybersecurity IP," *Information Forensics and Security, IEEE Transactions on,* Oct., 2023.

[15] K. Yang, D. Blaauw and D. Sylvester, "Hardware Designs for Security in Ultra-Low-Power IoT Systems: An Overview and Survey," *Micro, IEEE*, vol. 37, no. 6, pp. 72-89, Nov./Dec., 2017.

[16] A. Alaghi, and J. P. Hayes. "Survey of stochastic computing," *Embedded computing systems (TECS), ACM Transactions on,* vol. 12, no. 92, pp. 1-19, 2013.

[17] S. Gupta et al., "Deep learning with limited numerical precision," *Machine Learning (PMLR), International conference on,* pp. 1737-1746, 2015.

[18] J. Bae, W. Oh, J. Koo, C. Yu and B. Kim, "CTLE-Ising: A Continuous-Time Latch-Based Ising Machine Featuring One-Shot Fully Parallel Spin Updates and Equalization of Spin States," *Solid-State Circuits, IEEE Journal of*, pp. 1-11, Oct., 2023.

[19] E. Lawrence et al., "SP 800-22 rev. 1a. a statistical test suite for random and pseudo-random number generators for cryptographic applications," *National Institute of Standards and Technology (NIST)*, Apr., 2010.

Eunhwan Kim received the B.S. and M.S. degrees in electrical engineering from Kookmin University, Seoul, South Korea, in 2010 and 2012, respectively. He is currently pursuing the Ph.D. degree with the Pohang University of Science and Technology (POSTECH), Pohang, South Korea. From 2012 to 2014, he worked on the design of the display driver interface at DB Hitek, Seoul. From 2014 to 2018, he was a Research Associate with the i-Lab, POSTECH, working on hardware security. His current research interests include computing-in-memory and hardware security circuit.

Jae-Joon Kim received the B.S. and M.S. degrees in electronics engineering from Seoul National University, Seoul, South Korea, in 1994 and 1998, respectively, and the Ph.D. degree from the School of Electrical and Computer Engineering, Purdue University, West Lafayette, IN, USA, in 2004. He is currently a Professor with Seoul National University. From 2004 to 2013, he was a Research Staff Member with IBM Thomas J. Watson Research Center, Yorktown Heights, NY, USA. He was a Professor with the Pohang University of Science and Technology, Pohang, South Korea, from 2013 to 2021. His current research interests include the design of deep learning hardware accelerator, neuromorphic processor, hardware security circuit, and circuit for exploratory devices.