IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 24, 2019, accepted December 13, 2019, date of publication December 24, 2019, date of current version February 4, 2020.

Digital Object Identifier 10.1109/ACCESS.2019.2961967

A 100% Stable Sense-Amplifier-Based Physically Unclonable Function With Individually Embedded Non-Volatile Memory

KANG-UN CHOI, SEUNGBUM BAEK, JINO HEO, AND JONG-PHIL HONG, (Member, IEEE)
School of Electrical Engineering, Chungbuk National University, Cheongju 28644, South Korea

Corresponding author: Jong-Phil Hong (jphong@cbnu.ac.kr)

This work was supported in part by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education under Grant NRF-2018R1D1A1B07042607, and in part by the Korea Electric Power Corporation under Grant R17XA05-70.

ABSTRACT In this paper is presented a sense-amplifier-based physically unclonable function (PUF) with individually embedded non-volatile memory (eNVM) that offers 100% stable random bits. The proposed eNVM, which stores the initially generated random key, biases the sense-amplifier to reproduce always the same key as the initial value through a feedback path. In order to verify the performance of the proposed architecture, a 256-bit PUF with a core area of 0.160 mm^2 was implemented in a 180 nm standard CMOS process. The measurement results of the implemented PUF show an intra-chip Hamming Distance (HD) of 0 (100% stability) and inter-chip HD of 0.5047.

INDEX TERMS CMOS, information security, IoT device, non-volatile memory, physically unclonable function.

I. INTRODUCTION

In modern communication systems, the secure and reliable transmission of information (i.e., messages) is critical and can be guaranteed by confirmation of the message confidentiality and message integrity [1]–[3]. Moreover, to prevent forgery and repudiation of a message, identification of the sender (creating the information) and of the receiver (consuming the information) should be verified via the processes of authentication and non-repudiation [1]–[3] to determine whether the information is falsified or denied. Before the implementation of these techniques, the priority procedure is establishment of a key [1]–[5] by which it is possible to manage the pre-sharing secret information (called the KEY) including the generation, the distribution, and the transfer of a key [6]–[11].

Figure 1 shows the general methodology for authentication in real applications. Among several steps, the establishment of secret keys is one of the most important building blocks for authentication of information security. To produce random and non-replicable keys, a hardware based Physically Unclonable Function (PUF) structure has been actively researched recently. Among several approaches for PUF, a CMOS process based PUF is getting attention in relation to the development of IoT technology.

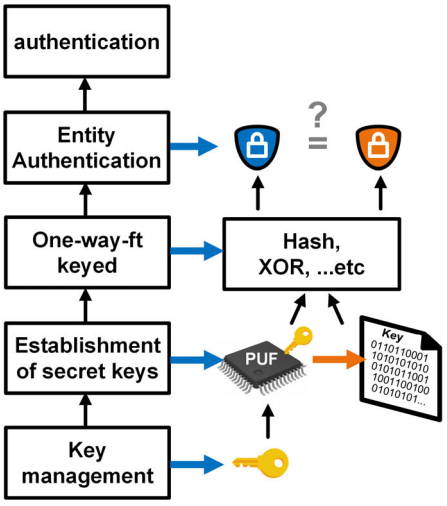

FIGURE 1. General authentication flow for information security service.

Process variation in CMOS technology is perceived as an obstacle that makes performance specifications difficult to achieve regarding circuit design; however, it also provides an ideal characteristic by which to achieve the fundamental goal

The associate editor coordinating the review of this manuscript and approving it for publication was Junaid Arshad.

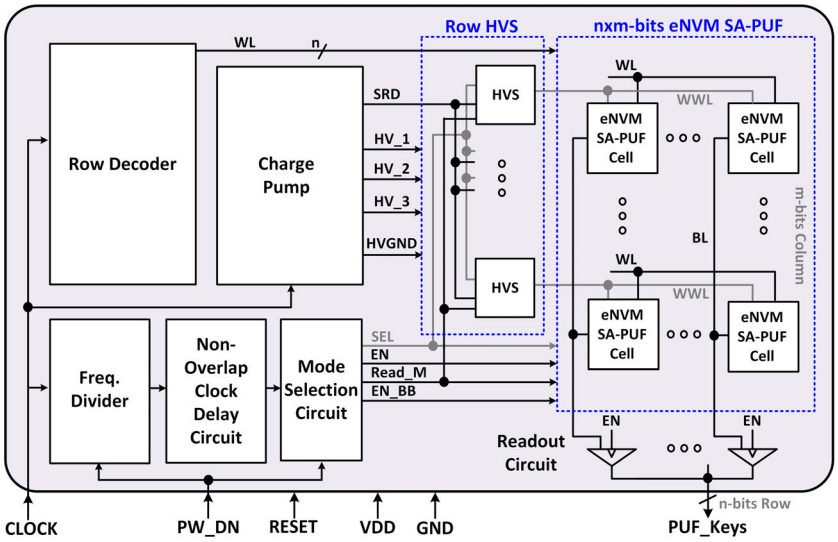

FIGURE 2. Top block diagram of proposed SA-PUF with eNVM.

of PUF, which is a physically unclonable function, because its output values are random and unpredictable.

Moreover, CMOS technology has the optimal features (compact, low-cost, and low power) for embedding the PUF into IoT sensor devices and maintaining the competitiveness of IoT sensor devices.

Randomness and reproducibility are the main properties of PUF as a secret key generator for information security. The reproducibility, which is defined with respect to the distribution of the response intra-distance of all the PUF instances, is a major problem of CMOS process based PUFs because the PUF instances can be changed by environmental variations in noise, temperature, and supply voltage. Several studies have reported overcoming reproducibility issues in CMOS process based PUFs, however these occupy a large chip area and dissipate a large power due to additional compensation blocks [12].

In this paper, a sense-amplifier-based PUF (SA-PUF) with individually embedded non-volatile memory (eNVM) is proposed and it has both 100% stability and good inter-chip hamming distance (HD). The proposed NVM, implemented with the standard CMOS process without an additional mask layer, was embedded individually into each SA-PUF cell. The proposed PUF with eNVM shows several advantages. First, the proposed PUF achieves 100% stability without complex and costly error-correction code circuitry. Second, the proposed PUF provides a high level of security because it has no external ports for the NVM. Finally, although NVMs are added, the chip size is still small enough to be embedded into IoT sensors.

II. PROPOSED PUF WITH eNVM

A. ARCHITECTURE AND OPERATING PRINCIPLE OF PROPOSED PUF WITH eNVM

Figure 2 presents a top block diagram of the proposed SA-PUF with eNVM. The m × n bits eNVM SA-PUF generates and regenerates unique and 100% stable keys.

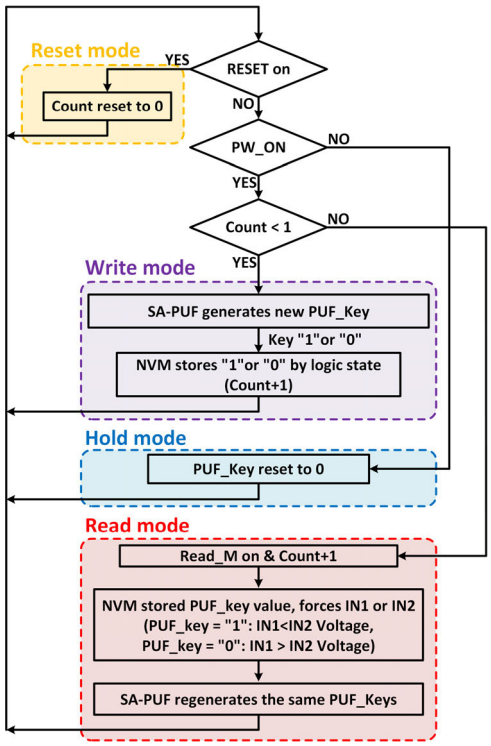

FIGURE 3. Operating flow chart of SA-PUF with eNVM for each mode.

The row decoder selects a word line (WL) signal to operate and connect to the Readout circuit among the n-bit SA-PUF cells. The Row HVS switches the voltage applied to the proposed eNVM in the SA-PUF cell to 0, regular, or high, depending on the operating mode. The Charge Pump generates three distinct levels of boosted voltage from the normal supply to operate the HVS circuit. A frequency divider is required to produce a longer period of time from the clock for eNVM write mode.

Figure 3 and 4 show the operating principle and timing diagram of the proposed SA-PUF with eNVM. The proposed

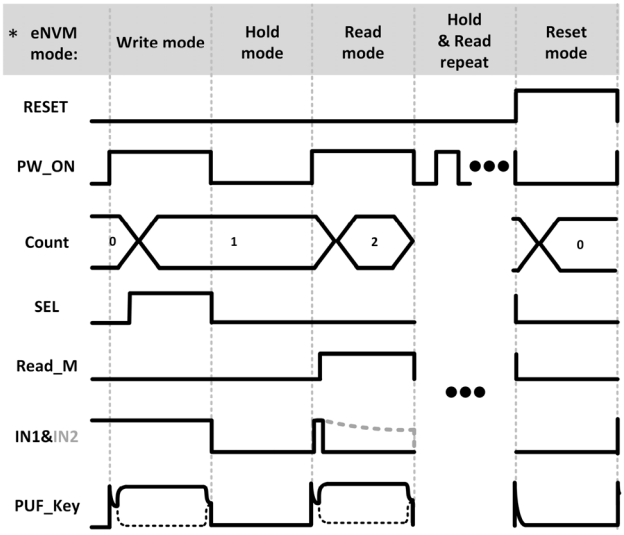

FIGURE 4. Timing diagram of SA-PUF with eNVM.

PUF has write, hold, read, and reset modes, as shown in Figure 3 and 4. When power (PW_ON) is enabled and the count number of the rising edge for PW_ON (Count) is zero, the PUF operates in write mode.

During write mode, the SA-PUF cell generates a new random output value, which is stored in the eNVM and output to the PUF_Key through the readout circuit, when SEL is enabled. In hold mode, the other signals are reset, but the proposed PUF holds the PUF_Key generated in write mode in eNVM. When the PW_ON is enabled and Count is greater than one, PUF enters read mode. Then, when Read_M is enabled, the value stored in eNVM is fed back to IN1 of the SA-PUF cell to force the regenerated PUF_Key to be the same as the initial value. When RESET is enabled, PUF operates in reset mode, in which all the signals including eNVM are reset and ready to generate a new random PUF_Key.

B. SENSE AMPLIFIER BASED PUF CELL WITH eNVM

Figure 5 shows the eNVM SA-PUF Cell in Figure 2, which consists of a SA-PUF cell, an NVM, and interstage circuits. The SA-PUF cell applies the sense-amplifier structure. The individually embedded NVM stores an initial key generated from the SA-PUF cell and forces the IN1 and IN2 bias to regenerate the same key as the initial value through a feedback path. Note that eNVM is shorted to IN only during read mode and disconnected when power is off, so the proposed eNVM is resistant to attacks through the output port of PUF_Keys.

In the proposed structure shown in Figure 5, a sense amplifier-based PUF (SA-PUF) cell is used to achieve fast start-up time and full output swing even at low differential input voltages [13]. In addition, a current-latched SA is adopted in the proposed PUF because it has high impedance to the differential input and is insensitive to bitline capacitance. In contrast, a voltage-latched SA deteriorates the available differential input voltage level due to the voltage drop of the isolation transistors [14].

In a SA-PUF cell, when the signal strengths of the two differential nodes are similar, output key values can vary due to external environmental conditions (i.e., change of noise, temperature, and supply voltage) when a key is produced. As a result, the secret key is unstable even in the same PUF chip, which gives rise to degradation of the reproducibility. To overcome this issue and obtain 100% stability, the proposed PUF uses non-volatile memory (NVM). The proposed NVM is fully custom designed using the standard CMOS process and is embedded into each SA-PUF cell, as shown in Figure 5, rather than using external commercial memory.

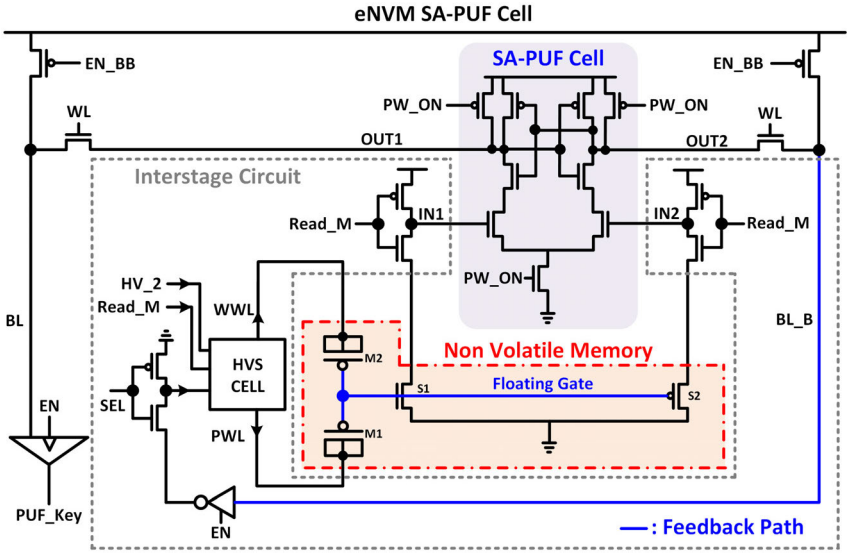

FIGURE 5. Schematic of proposed eNVM SA-PUF cell.

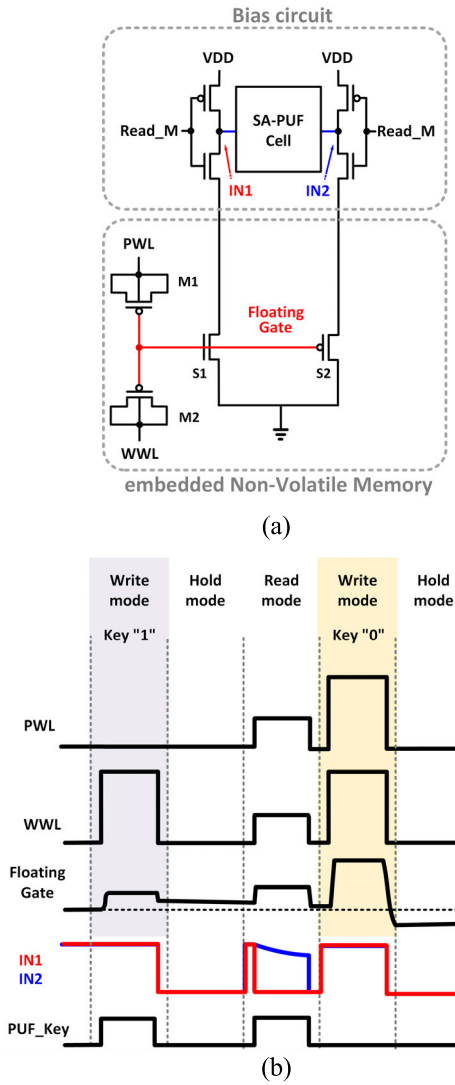

FIGURE 6. (a) 4T based eNVM for SA-PUF cell and (b) Timing diagram with Write, Hold, and Read modes.

The proposed NVM for PUF is less vulnerable to attack because it is embedded in each PUF cell, while commercial memory is connected to the PUF output through an external port, which can easily be exposed to invasive attacks [15]. In addition, the proposed NVM is cost-effective because it is implemented using only a standard CMOS process without additional mask layers [16]. Finally, compared with conventional compensation circuitry used to improve the reproducibility of PUF, the proposed eNVM scheme consumes less area and power, and achieves 100% stability.

In Figure 5, during write mode, the eNVM stores the produced initial key through the feedback path. When the PUF enters read mode, the eNVM applies the stored value to IN1 and IN2 in the form of a bias voltage, which causes the SA-PUF cell to regenerate the same value as the initial key. For instance, if the initial key of OUT2 is "0", eNVM is biased to "0" of IN1 and "1" of IN2, and vice versa.

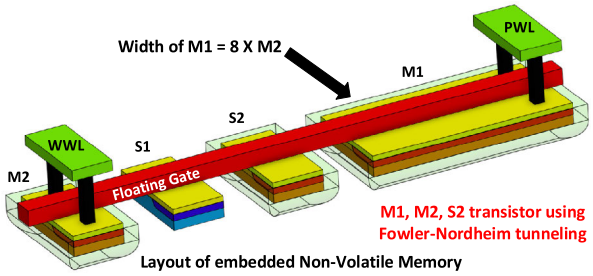

FIGURE 7. A 4T single poly structure is adopted for the eNVM.

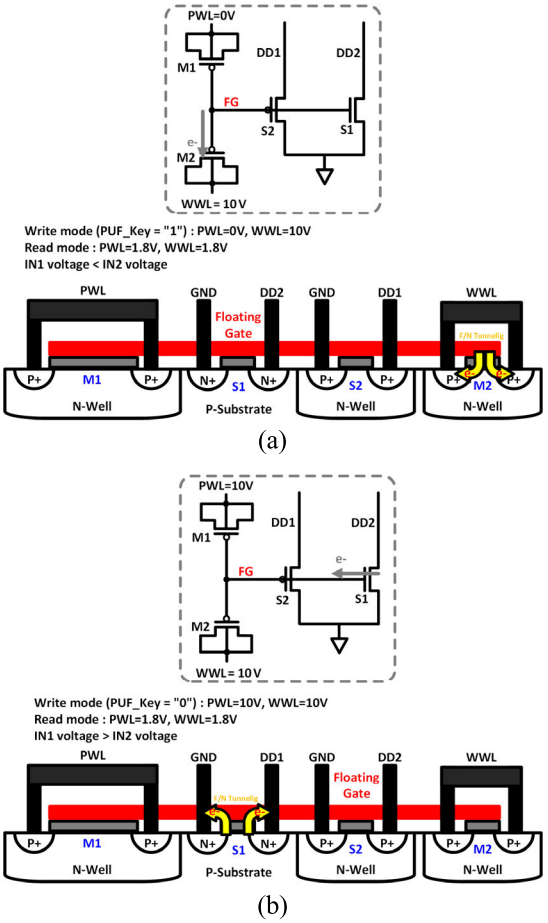

FIGURE 8. Operation principle of 4T-eNVM (a) Erase (PUF_key = "1") and (b) Program mode (PUF_key = "0").

C. IMPLEMENTATION AND OPERATING PRINCIPLE OF THE PROPOSED eNVM FOR PUF

Figure 6 shows schematic and timing diagrams of a 4T based eNVM for the proposed SA-PUF cell. A 4T based eNVM has four transistors: M1, M2, S1, and S2 (see Figure 6 a). In Figure 6, PWL and WWL signals are generated from the HVS cell (Figure 5) at one of three levels (high, 0, or regular voltage), depending on the write, hold, and read modes. Then, PWL and WWL signals are biased to the M1 and M2 terminals, respectively, where the source, drain, and body are tied together, to control the voltage of the floating gate node (Figure 6 a). As can be seen in Figure 6 (b), the roposed 4T-base eNVM has three operating modes:

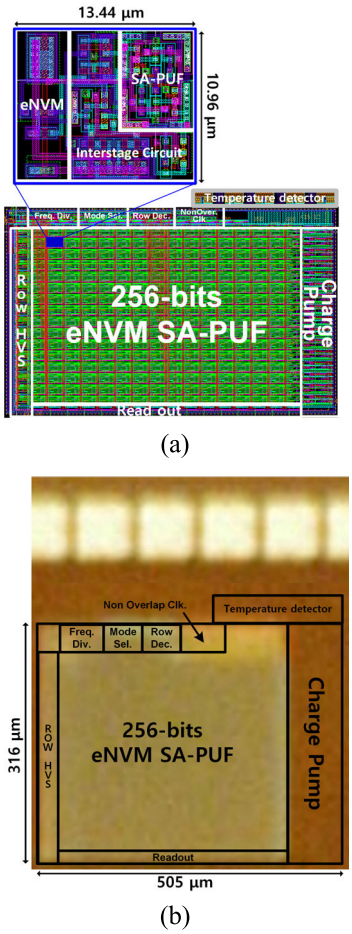

FIGURE 9. (a) Layout and (b) Die chip photograph of proposed SA-PUF with eNVM.

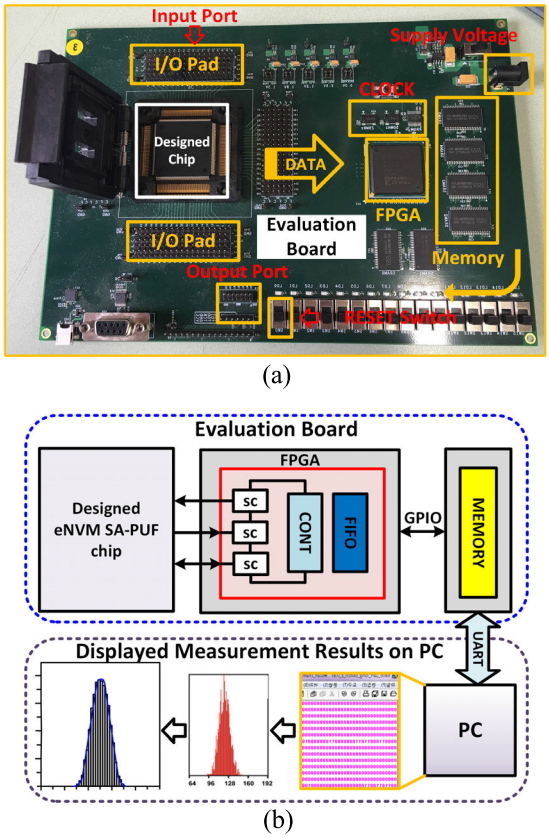

FIGURE 10. (a) Evaluation board setup and (b) Flowchart of displayed measurement results.

write, hold, and read. In Figure 6 (b), when the SEL signal is enabled and Read_M is disabled, the proposed eNVM operates in write mode and the HVS cell generates 0 or boosted high voltage of PWL and boosted high voltage of WWL. When both SEL and Read_M are disabled, the eNVM operates in hold mode and the HVS cell generates PWL and WWL with zero voltage. When SEL is disabled and Read_M is enabled, the eNVM operates in read mode and the HVS cell generates regular voltage for both PWL and WWL.

In addition, the proposed eNVM operates in two ways depending on the initial PUF_key value applied through the feedback path shown in Figure 6 (b). First, when the initial PUF_key value is "1", the zero voltage of PWL and high voltage of WWL generated from the HVS are applied to M1 and M2, so that the floating gate has a positive voltage in write mode. During hold mode (when the power is off), the proposed eNVM stores the initial PUF_key "1" as the floating gate maintains the positive voltage. During read mode when the power is turned back on and the PUF_key is regenerated, the positive voltage of the floating gate turns on the S1 transistor. Then, the IN1 node is connected to ground and discharged to 0 volts. As a result, the SA-PUF cell reproduces a value of 1 equal to the initial PUF_key value. Second, when the initial PUF_key value is "0", high PWL voltage is generated from the HVS, and the floating gate stores a negative voltage in write and hold mode. In read mode, the negative voltage on the floating gate turns off the S1 transistor and then, the IN1 node has regular voltage precharged with VDD. As a result, the SA-PUF cell reproduces a value of 0.

For high integration and low cost, the proposed 4T-based eNVM for PUF is implemented as shown in Figure 7 by applying a CMOS 3T single-poly structure [17] that can be created using a standard CMOS process. The new eNVM for PUF utilizes the Fowler-Nordheim (F/N) tunneling effect to store the initial PUF_key value. Figure 8 shows the operation principle for a 4T-based eNVM with erase and program mode. For erase mode operating at the PUF_key of "1", PWL (0V) and high voltage (10V) of WWL are biased, and then the high electric field in the gate oxide of the M2 transistor leads to Fowler-Nordheim tunneling by which the electrons of M2 are ejected from the floating gate. As a result, the floating gate node has a positive voltage. In contrast, for the program mode with PUF_key = "0", the high voltage (10V) of both PWL and WWL are biased, and then F/N tunneling appears in the S1 transistor, and the electrons are injected into the floating gate node. Therefore, the floating gate node has a negative voltage.

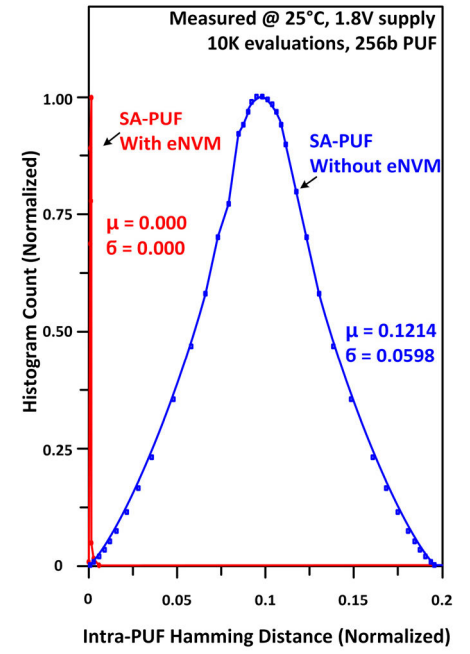

FIGURE 11. Measured (a) Intra-PUF HD and (b) Inter-PUF HD of SA-PUF with and without eNVM.

III. MEASUREMENT RESULTS

The proposed SA-PUF with eNVM was fabricated in a 180 nm standard CMOS. Figure 9 shows the layout and implemented chip photograph of the proposed architecture with 256-bits of valid Keys consisting of 16 columns and 16 rows. As can be seen in Figure 9 (a), the proposed NVM was implemented without extra layers and the unit cell area of the SA-PUF including NVM circuits is 147.302μm^2. Compared to architectures using the commercial memory, the proposed PUF is less vulnerable to invasive attacks

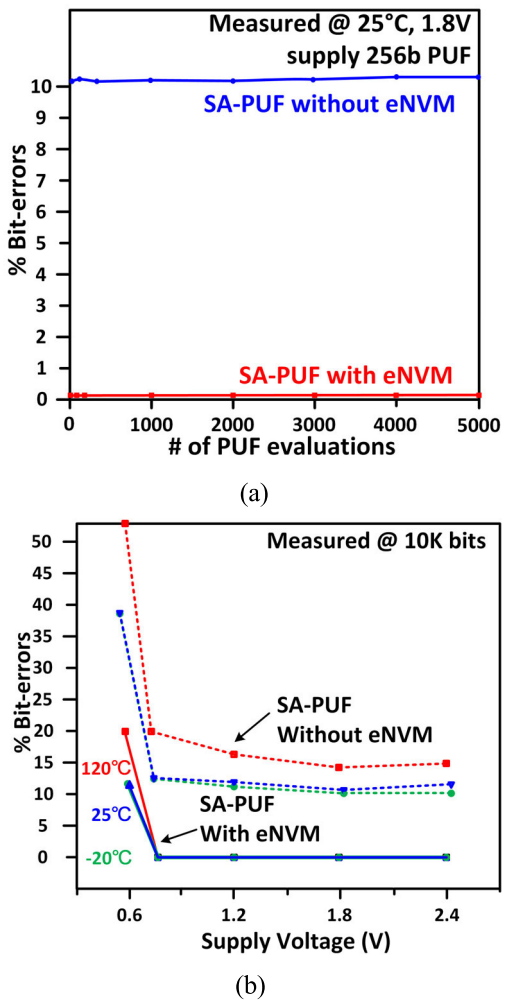

FIGURE 12. (a) Cumulative BER versus number of repeated accesses and (b) BER versus temperature and voltage variations.

because the NVMs are embedded into individual PUF cells without external ports, making it difficult to find their positions, as shown in Figure 9 (b). The area of the overall architecture in Figure 9 (b) is 0.160mm^2.

Figure 10 shows the evaluation board setup and display flowchart for the measurement results of the fabricated package chip for the proposed SA-PUF with eNVM. The PUF keys generated in the proposed architecture are measured at supply of 1.8V, clock period of 20ns, and SEL period of 1ms. In Figure 10 (b), the 256 bits of the valid PUF key are extracted into the FPGA and stored in memory sequentially for 16 clock cycles through a readout circuit connected to 16-bit rows. Then the PUF key values transferred from memory to PC via UART communication are analyzed using a Matlab simulator and converted to main performance for display.

The stability (reproducibility) of the PUF can be proved by calculation of intra-PUF hamming distance (HD) [18-19]. Figure 11 (a) shows the measured intra-PUF HD of the proposed SA-PUF with and without eNVM at supply voltage of 1.8V and the temperature of 25°.

TABLE 1. Performance comparison with other state-of-the-art studies.

	This work	SA-PUF without eNVM	ISSCC'17 [24]	JSSC' 16 [23]	ISSCC' 15 [22]	ISSCC' 14 [21]
Technology	180nm	180nm	180nm	65nm	65nm	22nm
Archeitecture	SA-PUF	SA-PUF	LVT PUF	PTAT	SA-PUF	ADH-PUF
Number of Bit	256	256	64	256	256	256
Total Area(mm^2)	0.16	0.11	0.0016*	0.0019	0.42**	24.00***
Efficiency(pJ/bit)	1.77	0.31	0.011	0.55	0.16	0.19
Autocorrelation Function @ 95% confidence	0.0121	0.0671	0.0173	0.0188	0.0363	0.0088
Temperature(℃)	-20-120	-20-25	-40-120	0-80	25-85	25-50
Supply voltage(V)	0.8-2.4	0.8-2.4	0.8-1.8	0.6-1.2	0.7-1.0	0.7-0.9
Stabilizing Methods	eNVM	-	TMV, Mask	TMV, thresholding	Mask	Voting, Burn-in, Mask, ECC
Inter- PUF Hamming Distance (uniqueness)	0.5047	0.5056	0.498	0.5001	0.5018	0.49
Intra- PUF Hamming Distance	0	0.1214	0.0018	0.0057	0.003	0.026
BER (%) (Worst case) (reproducibility)	0	12	0.18	1.46	4.51	0.97

*: 64bit LVT PUF cell size
**: 0.623mm^2 X (SA-PUF/INV+SA-PUF) excluding I/O pad
***: Area including 256 tiles and I/O pad

As shown in Figure 11 (a), the measured values of the proposed SA-PUF with eNVM have an average (μ) of 0 and a standard deviation (σ) of 0, while those of the SA-PUF without eNVM have 0.1214 and 0.0598 across the 10K evaluations. Therefore, the proposed eNVM achieves 100% stability of the SA-PUF.

The term Uniqueness represents the ability of PUF to uniquely distinguish a particular chip among a group of chips of the same type and was quantified by the inter-PUF HD [19-20]. Figure 11 (b) illustrates the measured inter-PUF HD of the SA-PUF, of which the value from 10K evaluations and 40 dies with each of the 256-bit keys, has a mean of 0.5047 and a standard deviation of 0.0471 under the same environmental conditions.

The stability of the PUF output is affected by noise, supply voltage, and temperature variation. The stability degradation due to the noise was quantified by the cumulative bit error rate (BER) in Figure 12 (a), which was measured at 1.8V, temperature of 25°, and 5000 repeated readout cycles. Compared to the SA-PUF without eNVM, the cumulative BER of the proposed SA-PUF is 0% in 5000 evaluations as shown in Figure 12 (a) because of applying the eNVM circuit. Further degradation of the stability by supply and temperature fluctuation is shown in Figure 12 (b). Measured BERs were performed with 10K repeated readouts, supply voltage ranging from 0.6 to 2.4V, and temperature of -20, 25, and 120°. From Figure 12 (b), the BER of the SA_PUF with and without eNVM is significantly increased at supply voltages lower than 0.8V. In the supply voltage range between 0.8 and 2.4V, the BER of the SA-PUF without eNVM is between 19 and 12%, and the stability tends to degrade at higher temperature. However, the proposed SA-PUF with eNVM has 0% BER over the entire temperature range and supply-voltages higher than 0.8V. Therefore, the proposed PUF structure can achieve 100% stability regardless of the voltage, temperature, and noise fluctuation over the guaranteed supply (0.8V-2.4V).

Figure 13 reveals additional measurement results of randomness and uniqueness for the proposed SA-PUF across 10K response bits at temperature of 25° and supply of 1.8V. For the evaluation of randomness, the Hamming weight of [26], which indicates whether the responses are biased towards 0 or 1, was measured and illustrated in Figure 13 (a). The hamming weight of the proposed SA-PUF averaged 0.4983 and had a standard deviation of 0.0631, which values are close to the ideal values of 0.5 and 0, respectively. Additional uniqueness was quantified through the Auto-correlation function (ACF) of 10K bits from 40 dies. This finds repeated patterns in a bitstream response at different lags or locations [27], as shown in Figure 13 (b). In the proposed SA-PUF, the ACF value at 95% confidence level is close to the ideal value of 0 (<0.01). The measured performance of the proposed PUF is compared to that in state-of-the-art work. In this work, the SA-PUF with eNVM achieve the lowest reproducibility with intra-PUF HD of 0 and BER of 0%. Table 1 shows the detailed comparisons.

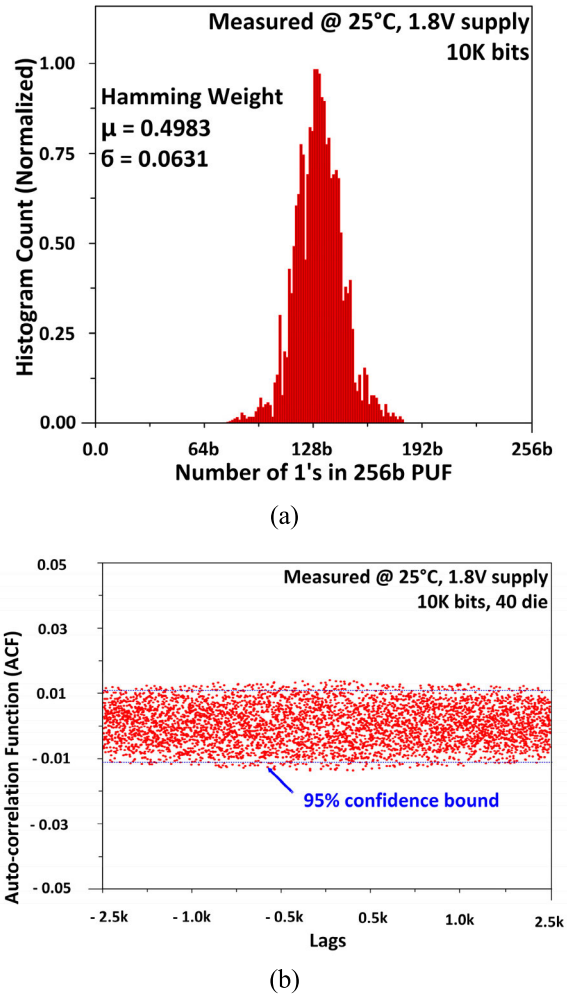

FIGURE 13. Measurement results of (a) Hamming weight distribution and (b) Auto-correlation function waveform across 10K response bits.

IV. CONCLUSION

In this paper, a sense amplifier based PUF with 100% stability was presented. By adopting an NVM circuit, the proposed SA-PUF can reproduce the same values as the random keys generated initially, regardless of the noise, supply voltage, and temperature change. In addition, the proposed PUF can be designed to be low cost and compact because the applied 4T-based NVM can be implemented in a standard CMOS process without additional layers. Furthermore, because the NVM is embedded in an individual PUF cell, there are no external connections, so the proposed PUF is less vulnerable to invasive attack than a structure using external memory.

Among several potential topologies for a PUF, a sense amplifier structure was adopted for the proposed PUF to achieve fast response time and good characteristics of uniqueness and randomness. The measured PUF showed an intra-PUF HD of 0.5047 average and 0.0471 standard deviation and an ACF of 95% confidence bound. The proposed PUF can be adopted for low cost, compact and reliable secure key generation systems such as identification, encryption keys, and true random number generation.

REFERENCES

[1] J. Katz, A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, 1996.
[2] B. Schneier, *Applied Cryptography*, Hoboken, NJ, USA: Wiley, 1995.
[3] D. R. Stinson, *Cryptography: Theory and Practice*, 3rd ed. Boca Raton, FL, USA: CRC Press, 2005.
[4] *Information Technology—Open Systems Interconnection—The Directory: Public-Key and Attribute Certificate Frameworks*, document ITU-T X.509, 2003.
[5] B. A. Forouzan, *Cryptography and Network Security (International Edition)*. New York, NY, USA: McGraw-Hill, 2008.
[6] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.
[7] R. M. Needham and M. D. Schroeder, "Using encryption for authentication in large networks of computers," *Commun. ACM*, vol. 21, no. 12, pp. 993–999, Dec. 1978.
[8] J. Kohl and C. Neuman, *The Kerberos Network Authentication Service (V5)*, document RFC 1510, 1993.
[9] R. C. Merkle, *Secrecy, Authentication, and Public Key Systems*. Ann Arbor, MI, USA: UMI Research Press, 1979.
[10] B. Prenfel, "Analysis and design of cryptographic hash functions," Ph.D. dissertation, Katholieke Universiteit Leuven, Leuven, Belgium, 1993.
[11] R. Soja, "Automotive security: From standards to implementation," Freescale, White Paper, 2014.
[12] T. Xu, J. B. Wendt, and M. Potkonjak, "Security of IoT systems: Design challenges and opportunities," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design (ICCAD)*, San Jose, CA, USA, Nov. 2014, pp. 417–423. [Online]. Available: http://dl.acm.org/citation.cfm?id=2691365.2691450
[13] M. Bhargava, C. Cakir, and K. Mai, "Attack resistant sense amplifier based PUFs (SA–PUF) with deterministic and controllable reliability of PUF responses," in *Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust (HOST)*, Jun. 2010, pp. 106–111.
[14] S. L. M. Hassan, I. Dayah, and I. S. A. Halim, "Comparative study on 8T SRAM with different type of sense amplifier," in *Proc. IEEE Int. Conf. Semiconductor Electron. (ICSE)*, Aug. 2014, pp. 321–324.
[15] S. P. Skorobogatov and R. J. Anderson, "Optical fault induction attacks," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.*, 2002, pp. 2–12.
[16] H. Kojima, T. Ema, T. Anezaki, J. Ariyoshi, H. Ogawa, K. Yoshizawa, S. Mehta, S. Fong, R. Smoak, S. Logie, and D. Rutledge, "Embedded flash on 90 nm logic technology & beyond for FPGAs," in *IEDM Tech. Dig.*, Dec. 2007, pp. 677–680.
[17] S.-H. Song, K. C. Chun, and C. H. Kim, "A logic–compatible embedded flash memory for zero–standby power system-on-chips featuring a multi–story high voltage switch and a selective refresh scheme," *IEEE J. Solid-State Circuits*, vol. 48, no. 5, pp. 1302–1314, May 2013.
[18] M. Majzoobi, M. Rostami, F. Koushanfar, D. S. Wallach, and S. Devadas, "Slender PUF protocol: A lightweight, robust, and secure authentication by substring matching," in *Proc. IEEE Symp. Secur. Privacy Workshops*, May 2012, pp. 33–44.
[19] A. Maiti, V. Gunreddy, and P. Schaumont, "A systematic method to evaluate and compare the performance of physical unclonable functions," in *Embedded Systems Design With FPGAs*. New York, NY, USA: Springer, 2013, pp. 245–267.
[20] M. S. Mispan, B. Halak, Z. Chen, and M. Zwolinski, "TCO-PUF: A subthreshold physical unclonable function," in *Proc. 11th Conf. Ph. D. Res. Microelectron. Electron. (PRIME)*, Jun./Jul. 2015, pp. 105–108.
[21] S. K. Mathew, S. K. Satpathy, M. A. Anders, H. Kaul, S. K. Hsu, A. Agarwal, G. K. Chen, R. J. Parker, R. K. Krishnamurthy, and V. De, "16.2 A 0.19 pJ/b PVT-variation-tolerant hybrid physically unclonable function circuit for 100% stable secure key generation in 22 nm CMOS," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2014, pp. 278–279.
[22] A. Alvarez, W. Zhao, and M. Alioto, "14.3 15 fJ/b static physically unclonable functions for secure chip identification with < 2% native bit instability and 140× inter/intra PUF hamming distance separation in 65 nm," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2015, pp. 1–3.
[23] J. Li and M. Seok, "Ultra–compact and robust physically unclonable function based on voltage–compensated proportional-to-absolute-temperature voltage generators," *IEEE J. Solid-State Circuits*, vol. 51, no. 9, pp. 2192–2202, Sep. 2016.

[24] K. Yang, Q. Dong, D. Blaauw, and D. Sylvester, "8.3 A 553F 2 2-transistor amplifier-based physically unclonable function (PUF) with 1.67% native instability," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2017, pp. 146–147.
[25] S. Taneja, A. B. Alvarez, and M. Alioto, "Fully synthesizable PUF featuring hysteresis and temperature compensation for 3.2% native BER and 1.02 fJ/b in 40 nm," *IEEE J. Solid-State Circuits*, vol. 53, no. 10, pp. 2828–2839, Oct. 2018.
[26] A. Maiti, J. Casarona, L. Mchale, and P. Schaumont, "A large scale characterization of RO–PUF," in *Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust (HOST)*, Jun. 2010, pp. 94–99.
[27] C. Böhm, M. Hofer, and W. Pribyl, "A microcontroller SRAM-PUF," in *Proc. 5th Int. Conf. Netw. Syst. Secur.*, 2011, pp. 269–273.

KANG-UN CHOI received the B.S. and M.S. degrees in electronic-electrical engineering from Chungbuk National University, Cheongju, South Korea, in 2015, and the M.S. degree from the Department of Electrical Engineering, Chungbuk National University, in 2017, where he is currently pursuing the Ph.D. degree in electrical engineering. His research interests include the IoT security device, Stable Sense-Amplifier, and THz and sub-THz integrated circuits, such as oscillator for source generator based on CMOS technology.

SEUNGBUM BAEK received the B.S. and M.S. degrees in information and communication engineering from Chungbuk National University, Cheongju, South Korea, in 2015 and 2017, respectively, where he is currently pursuing the Ph.D. degree. His current research interests include VLSI design for security services targeting resource-constrained devices, and embedded systems.

JINO HEO received the B.S. degree in physics, and the M.S. and Ph.D. degrees in information security from Korea University, Seoul, South Korea. He has been with Chungbuk National University, since 2016. His major interests are information security (cryptography), quantum communications, and quantum algorithms using quantum optics.

JONG-PHIL HONG received the B.Sc. degree in electronic engineering from Korea Aerospace University, Seoul, South Korea, in 2005, and the M.S. and Ph.D. degrees from the Department of Information and Communications Engineering, Korea Advanced Institute of Science and Technology (KAIST), Daejeon, South Korea, in 2007 and 2010, respectively. In 2010, he joined the Mixed-Signal Circuit Design Team, Samsung Electronics, Giheung, South Korea, as a Senior Engineer. Since 2012, he has been an Associate Professor with the Department of Electrical Engineering, Chungbuk National University, Cheongju, South Korea. His main research interests include RF integrated circuits, such as LNA, mixer, VCO, and frequency synthesizer for wireless and wire-line communication systems. His current research interests are toward high frequency (THz) circuit design, and integrated security chip based on CMOS technology.