Investigation of Physically Unclonable Functions Using Flash Memory for Integrated Circuit Authentication

Moon-Seok Kim, Dong-Il Moon, Sang-Kyung Yoo, Sang-Han Lee, and Yang-Kyu Choi

Abstract—**Flash memory devices are investigated to confirm their application as physically unclonable functions (PUFs). Inherent fluctuations in the characteristics of flash memory devices, even with identical fabrication processes, produce different outputs, which are useful for device fingerprints. A difference in programming/erasing efficiency arises from a widely distributed threshold voltage. However, statistical fluctuations in the threshold voltage represent an advantage for PUF applications. The characteristics of PUFs, such as their unclonability, uncontrollability, unpredictability, and robustness, are investigated using fabricated flash memory devices. A simulation study is performed to support the experimental results and to show that the unpredictability is induced by variations in the gate dielectric thickness.**

Index Terms—**Flash memory, SONOS (silicon/oxide/nitride/oxide/silicon), gate-all-around (GAA) transistors, process variation, physically unclonable function (PUF), programming efficiency, device fingerprint, device authentication.**

I. Introduction

INFORMATION security has been a primary concern for applications dealing with large amounts of digital information. Recently, hardware-based security systems have been designed to securely manage information against attacks [1], [2]. Thus, data encryption techniques that rely on hardware-oriented security systems [3], [33], such as true random number generators (t-RNGs) [4], [5], have been proposed. Among hardware-based security techniques, physically unclonable functions (PUFs) have attracted considerable attention for the implementation of cryptographic systems for authentication, identification, and anti-counterfeiting [6]–[8]. A PUF block is defined as circuitry that utilizes the unique, intrinsic, and uncontrollable physical features that stem from process variations during fabrication [9], [10]. These inherently unpredictable features make the security of the system significantly stronger against attacks, such as physical attacks. However, these uncontrollable and unclonable variations are undesirable for conventional semiconductor devices due to the inevitable non-uniformity among chips. While the semiconductor industry has sought to reduce manufacturing variability because it decreases the effective yield, this manufacturing variability is also an asset because it provides a basis for the construction of PUFs.

One of the most important goals in information security systems is finding a new source of unclonability related to the process variation of an integrated circuit (IC). Historically, various PUF devices, such as ring oscillators and comb-shaped capacitor structures, have been introduced in existing ICs [11], [12]. Specifically, memory-based PUF devices, such as dynamic random access memory and static random access memory (SRAM), have been reported [13]–[15]. Recently, a flash memory-based PUF has received attention. Prabhu *et al.* proposed that a PUF composed of NAND flash memory was feasible by applying either program disturbance or reading disturbance [16]. However, this approach lacks practicality for creating PUF devices because distinguishable, unique signatures are only attained after more than several thousand programming and reading operations. Thus, it is desirable to establish a PUF device based on flash memory using features that are more practical and efficiently realizable. The programming/erasing (P/E) operations adversely induce notable fluctuations in the threshold voltage (V_{TH}) due to an intrinsic physical property of flash memory. Previously, a wide distribution in V_{TH} was viewed as a drawback for exploiting multi-level cells of non-volatile memory (NVM). To address the above issue, incremental step pulse programming has been adopted [17]. However, these inherent variations can be deliberately applied to a PUF due to the uncontrollable and unpredictable characteristics of P/E operations. Wang *et al.* reported that flash memory can be applicable as a PUF device at the chip level [18]. The unique programming efficiency of flash memory has been applied to physically unclonable semiconductor devices. Thus, it is desirable to study how the physical irreproducibility is generated at the microscopic level. In this work, the unique programming efficiency of flash memory is investigated at the unit cell level. A simulation study is conducted to evaluate the unique programming efficiency for a variable gate dielectric thickness. An experimental verification is performed

Manuscript received September 6, 2013; revised September 18, 2014; accepted January 14, 2015. Date of publication February 2, 2015; date of current version March 6, 2015. The review of this paper was arranged by Associate Editor L. Dong. This work was supported by the Agency for Defense Development under Contract UC11004ED. The work of D.-I. Moon and Y.-K. Choi was supported in part by the Center for Integrated Smart Sensors funded by the Ministry of Science, ICT & Future Planning as Global Frontier Project under Grant CISS-2011-0031848, by the IT R&D program of MKE/KEIT under Grant 10035320 (Development of novel 3-D stacked devices and core materials for the next generation flash memory), by Samsung Electronics Company, Ltd., and by SK Hynix Semiconductor, Inc. *(Corresponding Author: Yang-Kyu Choi)*

M.-S. Kim and S.-H. Lee are with the Attached Institute of ETRI, Daejeon 305-600, Korea (e-mail: mskim@ensec.re.kr; freewill71@ensec.re.kr).

D.-I. Moon and Y.-K. Choi are with the Department of Electrical Engineering, Korea Advanced Institute of Science and Technology, Daejeon 305-701, Korea (e-mail: dimun@nobelab.kaist.ac.kr; ykchoi@ee.kaist.ac.kr).

S.-K. Yoo with the Attached Institute of ETRI, Daejeon 305-600, Korea, and also with the Department of Electrical Engineering , Korea Advanced Institute of Science and Technology, Daejeon 305-701, Korea (e-mail: skyoo@ensec.re.kr).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TNANO.2015.2397956

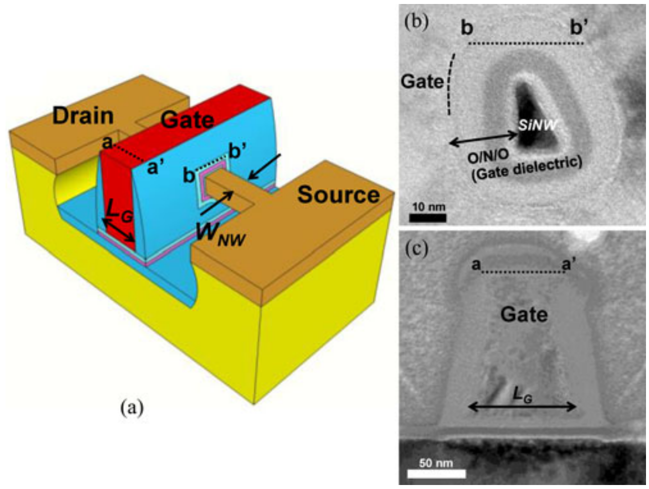


Fig. 1. Schematic and cross-sectional TEM images. (a) Schematic of the proposed devices. (b) A cross-sectional TEM image of the GAA SONOS cell along the O/N/O layer direction. (c) A TEM image along the channel length (L_{G}) direction.

with regard to the physical properties such as unclonability, uncontrollability, unpredictability, and robustness.

II. Device Fabrication

The basic structure of flash memory devices includes a gate-all-around (GAA) silicon nanowire (SiNW) field-effect transistor. Silicon nitride ($\mathrm{Si_3N_4}$) is used as a charge-trapping layer, and gate stacks composed of silicon/oxide/nitride/oxide/silicon (SONOS) are formed. Previous reports have claimed that cell-to-cell interference (program disturbance) and random telegraph noise (RTN) effects arise in flash memory-based PUFs and t-RNGs [14], [16]. However, cell-to-cell interference and RTN degrade the robustness of PUFs because these effects act as uncontrollable noise for single cells. Thus, additional effort is required to suppress cell-to-cell interference and RTN. The GAA SiNW and the gate stacks composed of SONOS are employed to enhance the robustness. The structure of the GAA SiNW suppresses RTN due to its excellent gate controllability [17], [18]. The SONOS devices show good immunity against cell-to-cell interference, which restricts flash memory scalability and degrades its robustness [19]. Therefore, the SONOS structure allows for increased packing density and superior robustness in PUF operations. Despite its lack of commercialization, the GAA-based SONOS device is a promising candidate as flash memory [22], [23]. Thus, it is valuable to investigate the PUF characteristics of the GAA-SONOS flash memory.

The process flow of the flash memory device is the same as in previous works [24], [25]. In this experiment, the width of the SiNW (W_{NW}) and the length of the gate (L_{G}) used for electrical characterization are 8 and 100 nm, respectively. The thickness of each O/N/O layer is 3, 6, and 8 nm, respectively. Fig. 1(a) presents a schematic of the fabricated flash memory cell. Fig. 1(b) shows a transmission electron microscopy (TEM) photograph of the fabricated SiNW and O/N/O layers, and Fig. 1(c) displays a TEM image of the cross-sectional gate.

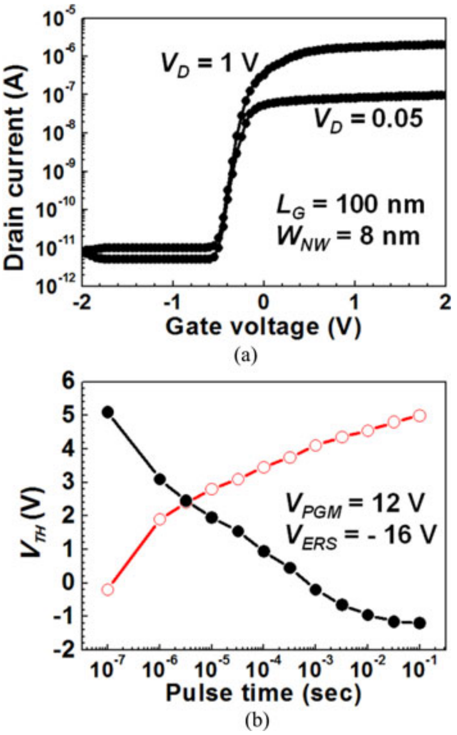


Fig. 2. (a) Typical transfer characteristics of the measured GAA-SONOS memory cell. (b) Measured programming and erasing characteristics of the GAA-SONOS memory cell.

The thicknesses of the O/N/O layers were measured using a spectroscopic ellipsometer (Woollam, M2000D). The uniformity was extracted from an average value of seven samples. The tunneling oxide was formed by thermal oxidation, and the charge-trapping layer (nitride) and blocking oxide were deposited by low-pressure chemical vapor deposition. According to the data measured by spectroscopic ellipsometry, the variation in the tunneling oxide thickness is less than 1%. However, the variation in the thickness of the charge-trapping layer and the blocking oxide is approximately 2%.

Fig. 2(a) and (b) shows the electrical characteristics of a unit NVM cell. The current–voltage (*I*–*V*) characteristics of the initial device were measured prior to introducing the P/E operations. As shown in Fig. 2(a), the GAA structure suppresses the drain-induced barrier lowering due to the excellent gate controllability. To confirm the P/E performance of flash memory operations, Fig. 2(b) exhibits representative transient curves indicating the P/E efficiency. In these measured devices, electron trapping in the nitride induces a positive shift of V_{TH} under positive bias, while hole trapping in the nitride results in a negative shift of V_{TH} under negative voltage, as expected.

III. Operational Principles

A brief operational principle for the PUF is illustrated and compared with that of a conventional NVM in Fig. 3. In this experiment, V_{READ} is modified to V_{PUF}. As shown in Fig. 3(a), V_{READ} is set to distinguish between two binary states under ordinary memory operation: "0" (erased state) and "1" (programmed state). In other words, because V_{READ} was applied to

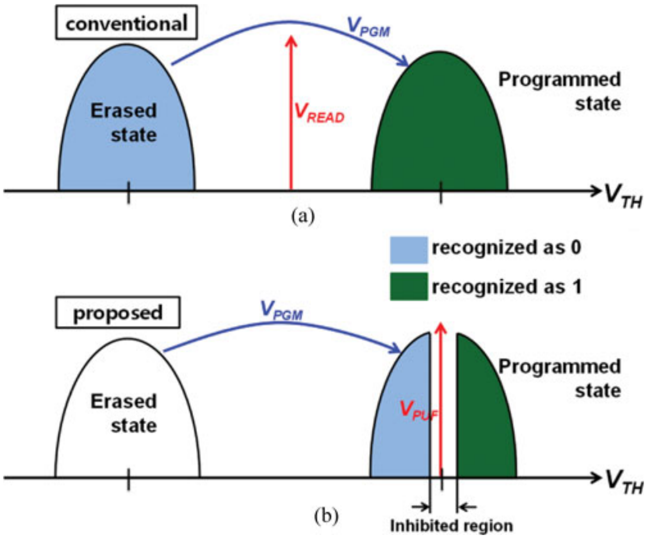


Fig. 3. Schematic illustration of (a) the ordinary operation for flash memory and (b) the proposed memory operation for PUF circuitry.

clearly distinguish the erased and programmed states, NVM operations were possible. In contrast, to experimentally generate the PUF output, V_{READ} is replaced by V_{PUF}, which is the statistical median V_{TH} of the programmed state. If $V_{\mathrm{TH}} > V_{\mathrm{PUF}}$, a logic state of “1” is extracted. Conversely, if $V_{\mathrm{TH}} < V_{\mathrm{PUF}}$, a logic state of “0” is extracted. Although the memory cells are fabricated by the same processes and equipment, each memory cell has a different P/E efficiency, which inevitably leads to induced V_{TH} variations. V_{TH} is a good metric for judging physically unclonable outputs because it is easily, quickly, and reliably measurable in the flash memory devices. Additionally, an inhibited region is set to prevent errors arising from small ΔV_{TH} values within the intermediate region between the “0” and “1” state, as shown in Fig. 3(b). The inhibited region is determined by detecting the current level.

IV. Results and Discussion

In this section, an experimental verification was conducted to determine whether the flash memory cell is feasible for PUF circuitry. The main characteristics of PUFs are unclonability, uncontrollability, unpredictability, and robustness. Unclonability indicates that reproduction is infeasible even under the same fabrication conditions, whereas uncontrollability implies that the process variation or source of randomness is uncontrollable. Unpredictability means that if some input–output pairs are uncovered, the corresponding output signal according to the other input is not predictable. Robustness means that the same value expressed by a binary number is sustained in an identical unit cell.

To investigate unclonability, the proposed method in Fig. 3(b) was experimentally performed. Fig. 4(a) and (b) shows the output between different dies fabricated by the same process conditions. The difference in the signatures shown in Fig. 4(a) and (b) reveal that a physically unclonable output is generated. These results are primarily attributed to the process variation.

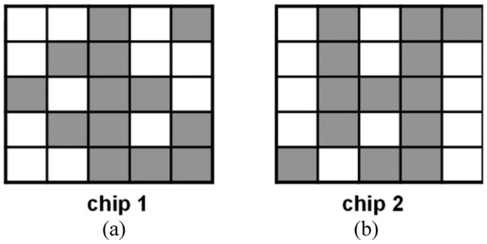


Fig. 4. Schematic illustration to exhibit a binary state. Each cell represents the logic value for (a) chip 1 and (b) chip 2 fabricated under the same conditions.

The thickness variations of the tunneling oxide, the charge-trapping layer, and the blocking oxide are unavoidable. The vertical electric field across the gate dielectrics is influenced by the fluctuations in the thickness of the O/N/O layers. The proposed PUF is intended to widen the variations of programming efficiency by deliberately using fluctuations in the vertical electric field. Thus, it is appropriate to study how the variation in gate dielectric thickness influences the programming efficiency. First, as introduced in the previous section, the thicknesses of the fabricated O/N/O layers were measured. Second, based on the measured data, 3-D numerical simulations were conducted using the ATLAS of SILVACO [26]. The electric field over the tunneling oxide was extracted with respect to the thicknesses of the O/N/O layers. From these simulated results, the Fowler-Nordheim (FN) tunneling current density was computed using the Wentzel–Kramers–Brillouin (WKB) approximation [27]. As noted earlier, the variation in the tunneling oxide thickness is below 1%, whereas the variation in the charge-trapping layer and blocking oxide thicknesses is approximately 2% from the target thickness. Based on the evaluated results, Fig. 5(a) shows the intensity of the electric field according to the thickness of the charge-trapping layer and the blocking oxide, with the assumption that the thickness of the tunneling oxide is fixed. The equivalent oxide thickness (EOT) is presented to denote the change in thickness of the charge-trapping layer and the blocking oxide. The gate voltage is set to 12 V. The SONOS is assumed to have a geometrically cylindrical form. Based on the electric field shown in Fig. 5(a), Fig. 5(b) exhibits the FN tunneling current density according to the thickness of the tunneling oxide using the WKB approximation. The FN tunneling current density is directly proportional to the V_{TH} shift. As shown in Fig. 5(b), the FN tunneling current density decreases from 3.2 to 2.2 mA/cm^2 as the EOT changes from 13.8 to 14.2 nm. The change in the FN tunneling current density indicates that the estimated fluctuation causes ΔV_{TH} to increase by a factor of 1.5 from the erased state to the programmed state. It is impossible to accurately control and predict the thickness of the gate dielectrics. Alternatively, the simulated results reveal that uncontrollable and unpredictable variations in the O/N/O layers are the primary cause of considerable variations in V_{TH}.

The proposed PUF was studied to confirm its unclonable and uncontrollable properties by experimental and theoretical procedures. In this section, specifically to confirm the robustness, the PUF state was determined after 100 reading operations. Fig. 6(a) shows the experimental procedure. A single programming

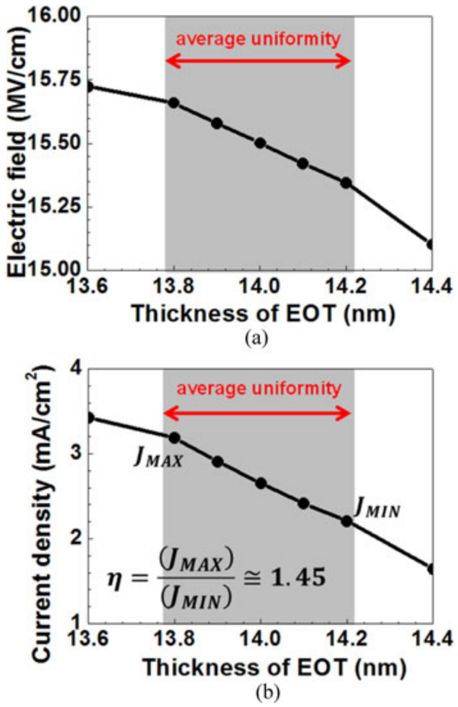


Fig. 5. (a) Simulated distribution of the electric field for cylindrical GAA-SONOS memory cells according to the variation in the O/N/O layer thickness. (b) The FN tunneling current density versus the variation in the O/N/O layer thickness based on simulated results.

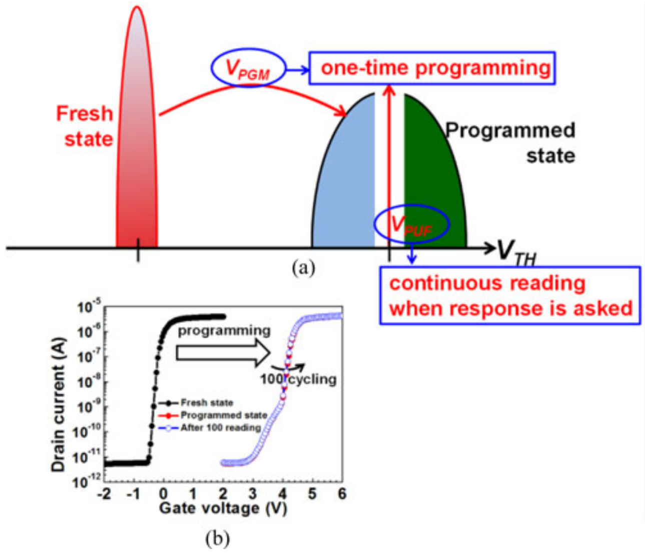


Fig. 6. (a) Schematic illustration of the proposed flash memory-based PUF operation and (b) typical transfer characteristics of the proposed device.

operation was performed before the PUF operations were enabled. To verify the robustness of the PUF response, multiple reading operations were iteratively repeated to extract a reliably robust PUF response.

Fig. 6(b) exhibits a representative *I–V* curve, which corresponds to the condition in Fig. 6(a). This operational principle is restricted by data retention characteristics. Due to the limitations of the data retention characteristics, V_{TH} is sometimes negatively shifted. Several previous works have demonstrated that ten-year retention characteristics can be guaranteed by adopting various engineering techniques such as bandgap engineering and a thicker tunneling oxide layer [28]–[30]. Thus, this experiment, assuming that reliable retention characteristics are guaranteed, focuses on the robustness according to several reading operations.

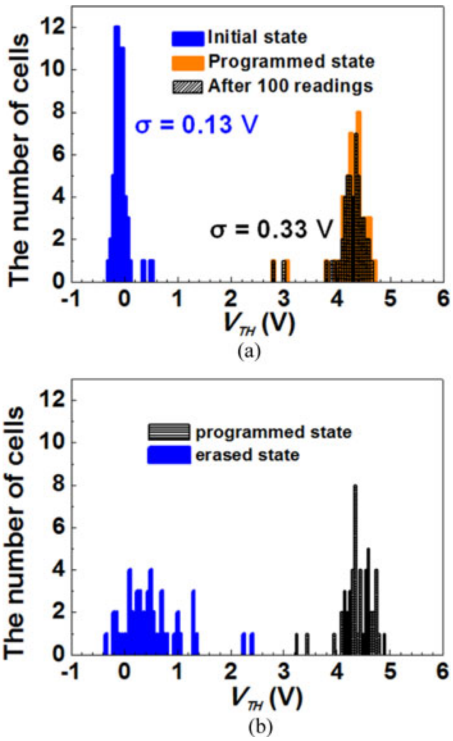
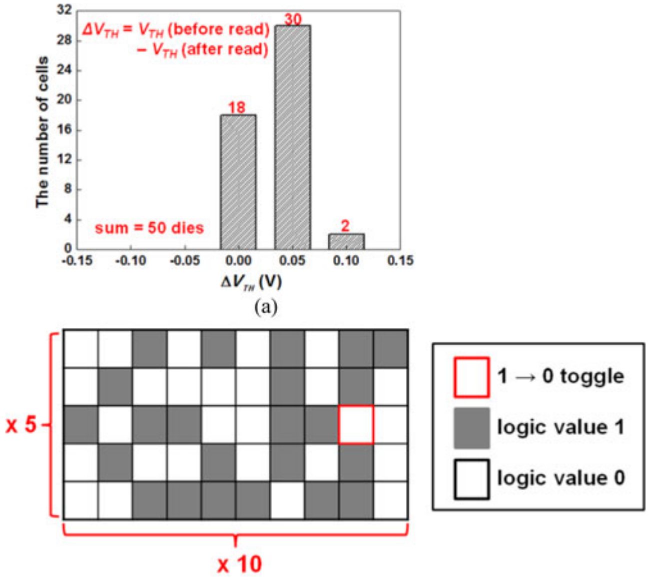


Fig. 7. (a) Measured V_{TH} distribution. (a) The V_{TH} distribution in the fresh state, programmed state, and after 100 reading operations and (b) the V_{TH} distribution in the programmed state, erased state during programming, and erasing cycling.

Fig. 7(a) shows the V_{TH} distribution before and after a single programming step and after 100 reading operations, as shown in Fig. 6(a), and Fig. 7(b) exhibits the V_{TH} distribution of the programmed and erased states during iterative P/E cycling. Fig. 7(a) and (b) exhibits the V_{TH} distribution before the inhibited region is set. The V_{TH} distribution of the fresh state in Fig. 7(a) is uniform compared to that of the programmed and erased state shown in Fig. 7(b). The standard deviation (σ) of the fresh state V_{TH} distribution is 0.13 V, while σ of the programmed state is 0.33 V. Thus, widely distributed V_{TH} values are clearly observed during the P/E operations. In Fig. 7(a), the orange-colored box indicates the V_{TH} distribution after a single programming step, and the black-checked box indicates the V_{TH} distribution after 100 readings. The mean value difference between the orange-colored box and the black-checked box is 0.03 V. There is a slight variation in terms of the V_{TH} distribution between the state after the single programming step and the state after 100 readings, as expected. To estimate the error rate with respect to several reading operations, it is proper to investigate ΔV_{TH} after 100 reading operations are performed. Thus, ΔV_{TH} is plotted in Fig. 8(a). The ΔV_{TH} values indicate the voltage difference with



(a)

(b)

Fig. 8. (a) The ΔV_{TH} distribution following the proposed operation. ΔV_{TH} indicates the difference between the programmed state and the state after 100 reading operations. (b) A schematic illustration comparing the logic value of the programmed state and that of the state after one hundred reading operations are performed.

respect to 100 reading operations among a block composed of 50 identical memory cells. Positive values of ΔV_{TH} are caused by slight de-trapping of the electrons from the charge-trapping layer during several reading operations.

Some cells have a variation in V_{TH} in the range of 0.05–0.1 V. Thus, the robustness is characterized by determining the logic value of the NVM cells. As proposed in Fig. 3(b), the logic value is distributed according to V_{TH}. In this study, V_{PUF} is set to 4.35 V. Fig. 8(b) exhibits a logic distribution of 50 devices during the proposed operations. There is a single bit error, i.e., 2%. As noted earlier, due to the electron de-trapping from the charge-trapping layer, the lower V_{TH} induces a small number of errors. Most PUF systems, similar to flash memory, suffer from errors. To correct errors in the encrypted data, specific error correction hardware has been developed, such as the fuzzy extractor [31]. Errors of 2% can easily be corrected by error-correcting circuitry [32]. Thus, it is possible to create a PUF composed of flash memory.

V. Conclusion

Flash memory devices were investigated at a microscopic level to confirm their application as PUFs. These devices utilize intrinsic variations in the programming efficiency. The properly modified reading voltage contributes to the functioning of the PUF. Experiments were conducted to confirm the characteristics of the PUF in terms of its uncontrollability, unpredictability, unclonability, and robustness. Sub-nanometer control of the thicknesses of the thin gate dielectrics in a SONOS memory structure is impossible. These inherent process variations are uncontrollable, unclonable, and unpredictable. These uncontrollable variations in the gate dielectric thicknesses result in widely distributed programming performances and allow ΔV_{TH} to vary by a factor of 1.5. Thus, the widely distributed threshold voltage is favorable for creating a PUF. The robustness of this device was also experimentally demonstrated. To confirm the robustness characteristics, a logic value from a cell block composed of 50 cells was carefully traced after 100 reading operations. In this experiment, a single bit error cell was detected, arising from electron de-trapping at the charge-trapping layer. Previously developed error correction hardware can be employed to resolve such errors. Therefore, the proposed flash memory-based PUF is a promising candidate for device fingerprinting and authentication.

References

[1] B. Koppel and S. Neuhaus, "Analysis of a hardware security module's high-availability setting," in *Proc. IEEE Symp. Security Privacy*, May 2013, pp. 77–80.

[2] R. Gallo, H. Kawakami, and R. Dahab, "Case study: On the security of key storage on PCs," in *Proc. 12th IEEE Int. Conf. Trust, Security Privacy Comput. Commun.*, Jul. 2013, pp. 1645–1651.

[3] B. Gassend, D. Clarke, M. Dijk, and S. Devadas, "Silicon physical random functions," in *Proc. Comput. Commun. Security Conf.*, May 2002, pp. 148–160.

[4] S. K. Yoo, D. Karakoyunlu, B. Birand, and B. Sunar, "Improving the robustness of ring oscillator TRNGs," *ACM Trans. Reconfigurable Technol. Syst.*, vol. 3, no. 2, pp. 1–30, May 2010.

[5] 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.

[6] M. O. Lehtonen, F. Michahelles, and E. Fleisch, "Trust and security in RFID-based product authentication systems," *IEEE Syst. J.*, vol. 1, no. 2, pp. 129–144, Dec. 2007.

[7] D. Puntin, S. Stanzione, and G. Iannaccone, "CMOS unclonable system for secure authentication based on device variability," *Proc. Eur. Solid State Circuits Conf.*, pp. 130–133, Sep. 2008.

[8] Y. S. Lee, T. Y. Kim, and H. J. Lee, "Mutual authentication protocol for enhanced RFID security and anti-counterfeiting," in *Proc. 26th Int. Conf. Adv. Inf. Netw. Appl. Workshops*, Mar. 2012, pp. 558–563.

[9] R. Maes and I. Verbauwhede, "Physically unclonable functions: A study on the state of the art and future research directions," in *Proc. Towards Hardware-Intrinsic Security Inf. Cryptography*, 2010, pp. 3–37.

[10] U. Ruhrmair, C. Jaeger, M. Bator, M. Stutzmann, P. Lugli, and G. Csaba, "Applications of high-capacity crossbar memories in cryptography," *IEEE Trans. Nanotechnol.*, vol. 10, no. 3, pp. 489–498, May 2011.

[11] H. Yu, P. H. W. Leong, and Q. Xu, "An FPGA chip identification generator using configurable ring oscillators," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 20, no. 12, pp. 2198–2207, Dec. 2012.

[12] D. Roy, J. H. Klootwijk, N. A. M. Verhaegh, H. H. A. J. Roosen, and R. A. M. Wolters, "Comb capacitor structures for on-chip physical uncloneable function," *IEEE Trans. Semicond. Manuf.*, vol. 22, no. 1, pp. 96–102, Feb. 2009.

[13] S. Rosenblatt, D. Fainstein, A. Cestero, J. Safran, N. Kirihata, and S. S. Iyer, "Field tolerant dynamic intrinsic chip ID using 32 nm high-k/metal gate SOI embedded DRAM," *IEEE J. Solid-State Circuits*, vol. 48, no. 4, pp. 940–947, Apr. 2013.

[14] D. E. Holcomb, W. P. Burleson, and K. Fu, "Power-up SRAM state as an identifying fingerprint and source of true random numbers," *IEEE Trans. Comput.*, vol. 58, no. 9, pp. 1198–1210, Sep. 2009.

[15] M. Cortez, A. Dargar, S. Hamdioui, and G.-J. Schrijen, "Modeling SRAM start-up behavior for physical unclonable functions," in *Proc. IEEE Int. Symp. Defect Fault Tolerance VLSI Nanotechnol. Syst.*, Oct. 2012, pp. 1–6.

[16] P. Prabhu, A. Akel, L. M. Grupp, W.-K. S. Yu, G. E. Suh, E. Kan, and S. Swanson, "Extracting device fingerprints from flash memory by exploiting physical variations," in *Proc. 4th Int. Conf. Trust Trustworthy Comput.*, Jun. 2011, pp. 1–17.

[17] K.-D. Suh, B.-H. Suh, Y.-H. Lim, J.-K. Kim, Y.-J. Choi, Y.-N. Koh, S.-S. Lee, S.-C. Kwon, B.-S. Choi, J.-S. Yum, J.-H. Choi, J.-R. Kim, and H.-K. Lim, "A 3.3 V 32 Mb NAND flash memory with incremental

step pulse programming scheme," *IEEE J. Solid-State Circuits*, vol. 30, no. 11, pp. 1149–1156, Nov. 1995.

[18] Y. Wang, W.-K. Yu, S. Wu, G. Malysa, G. E. Suh, and E. C. Kan, "Flash memory for ubiquitous hardware security functions: true random number generation and device fingerprints," in *Proc. IEEE Symp. Security Privacy*, May 2012, pp. 33–47.

[19] K. Fukuda, Y. Shimizu, K. Amemiya, M. Kamoshida, and C. Hu, "Random telegraph noise in flash memories—model and technology scaling," in *Proc. IEDM Tech. Dig.*, Dec. 2007, pp. 169–172.

[20] H. Lee, L.-E. Yu, S.-W. Ryu, J.-W. Han, K. Jeon, D.-Y. Jang, K.-H. Kim, J. Lee, J.-H. Kim, S.-C. Jeon, G. S. Lee, J. S. Oh, Y. C. Park, W. H. Bae, H. M. Lee, J. M. Yang, J. J. Yoo, and Y.-K. Choi, "Sub-5 nm all-around gate FinFET for ultimate scaling," in *Proc. VLSI Tech. Symp. Dig.*, Jun. 2006, pp. 58–59.

[21] J.-D. Lee, S.-H. Hur, and J.-D. Choi, "Effects of floating-gate interference on NAND flash memory cell operation," *IEEE Electron Device Lett.*, vol. 23, no. 5, pp. 264–266, May 2002.

[22] K. H. Lee, H. C. Lin, and T.-Y. Huang, "A novel charge-trapping-type memory with gate-all-around poly-si nanowire and HfAlO trapping layer," *IEEE Electron Device Lett.*, vol. 34, no. 3, pp. 393–395, Mar. 2013.

[23] S.-D. Yang, J.-S. Oh, H.-J. Yun, K.-S. Jeong, Y.-M. Kim, S.-Y. Lee, H.-D. Lee, and G.-W. Lee, "The short channel effect immunity of silicon nanowire SONOS flash memory using TCAD simulation," *Trans. Elect. Electron. Mater.*, vol. 14, no. 3, pp. 139–142, Jun. 2013.

[24] M.-S. Kim, S.-J. Choi, D.-I. Moon, J. P. Duarte, S. Kim, and Y.-K. Choi, "Investigation of gate length and fringing field effects for program and erase efficiency in gate-all-around SONOS memory cells," *Solid-State Electron.*, vol. 79, no. 12, pp. 7–10, Jan. 2013.

[25] D.-I. Moon, S.-J. Choi, C.-J. Kim, J.-Y. Kim, J.-S. Lee, J.-S. Oh, G.-S. Lee, Y.-C. Park, D.-W. Hong, D.-W. Lee, Y.-S. Kim, J.-W. Kim, J.-W. Han, and Y.-K. Choi, "Silicon nanowire all-around gate MOSFETs built on a bulk substrate by all plasma-etching routes," *IEEE Electron Device Lett.*, vol. 32, no. 4, pp. 452–454, Apr. 2011.

[26] *Atlas User's Manual: Device Simulation Software*, Silvaco International Inc., Santa Clara, CA, USA, 2010.

[27] H.-T. Lue, S.-C. Lai, T.-H. Hsu, P.-Y. Du, S.-Y. Wang, K.-Y. Hsieh, R. Liu, and C.-Y. Lu, "Understanding barrier engineered charge-trapping NAND flash devices with and without high-k dielectric," in *Proc. IEEE Int. Rel. Phys. Symp.*, Apr. 2009, pp. 874–882.

[28] H.-T. Lue, S.-Y. Wang, E.-K. Lai, Y.-H. Shih, S.-C. Lai, L.-W. Yang, K.-C. Chen, J. Ku, K.-Y. Hsieh, R. Liu, and C.-Y. Hu, "BE-SONOS: A bandgap engineered SONOS with excellent performance and reliability," in *Proc. IEDM Tech. Dig.*, pp. 547–550, Dec. 2005.

[29] S. H. Lin, H. J. Yang, W. B. Chen, F. S. Yeh, S. P. McAlister, and A. Chin, "Improving the retention and endurance characteristics of charge-trapping memory by using double quantum barriers," *IEEE Trans. Electron Device*, vol. 55, no. 7, pp. 1708–1713, Jul. 2008.

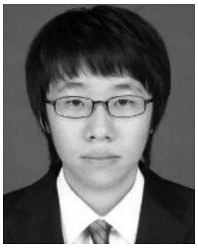
[30] S.-H. Gu, C.-W. Hsu, T. Wang, W.-P. Lu, Y.-H. J. Ku, and C.-Y. Lu, "Numerical simulation of bottom oxide thickness effect on charge retention in SONOS flash memory cells," *IEEE Trans. Electron Device*, vol. 54, no. 1, pp. 90–97, Jan. 2007.

[31] M.-D. Yu and S. Devadas, "Secure and robust error correction for physical unclonable functions," *IEEE Des. Test Comput.*, vol. 27, no. 1, pp. 48–65, Jan. 2011.

[32] C. Bosch, J. Guajardo, and A. Sadeghi, "Efficient helper data key extractor on FPGAs," in *Proc. Cryptographic Hardware Embedded Syst.*, Aug. 2008, pp. 181–197.

[33] B. Koppel and S. Neuhaus, "Analysis of a hardware security module's high-availability setting," in *Proc. IEEE Symp. Security Privacy*, pp. 77–80, May 2013.

Moon-Seok Kim received the M.S. degree from the Department of Electrical Engineering, Korea Advanced Institute of Science and Technology, Daejeon, Korea, in 2013. His research interests include resistance random access memory and flash memory.



Dong-Il Moon received the M.S. degree from the Department of Electrical Engineering, Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Korea, in 2010, where he is currently working toward the Ph.D. degree in electrical engineering.

Sang-Kyung Yoo received the M.S. degree in information and communication from the Korea Advanced Institute of Science and Technology, Daejeon, Korea, in 2001. He joined the Attached Institute of ETRI, Daejeon, in 2003, where he is a Senior Member of the engineering staff. He has focused on designing and developing secure and dependable systems.

Sang-Han Lee received the M.S. degree in electrical engineering from Kyungpook National University, Daegu, Korea, in 1997. In 2000, he joined the Attached Institute of ETRI, Daejeon, Korea, where he is currently a Principal Member of the engineering staff.

Yang-Kyu Choi received the Ph.D. degree from the University of California, Berkeley, CA, USA, in 2001. He is currently a Professor with the Department of Electrical Engineering, Korea Advanced Institute of Science and Technology.