Total Ionizing Dose Effects on Physical Unclonable Function From NAND Flash Memory

Sadman Sakib, *Student Member, IEEE*, Md. Raquibuzzaman, *Student Member, IEEE*, Maryla Wasiolek, Khalid Hattar, *Member, IEEE*, and Biswajit Ray, *Senior Member, IEEE*

***Abstract*— This article demonstrates the total ionizing dose (TID) impact on a NAND flash memory-based physical unclonable function (PUF). We used commercial-off-the-shelf flash memory chips to generate PUF. The flash chip is irradiated with Co-60 gamma rays up to 10 krad(Si). The irradiated chip shows significant accuracy degradation (bit error ∼ 12%) of the flash-PUF. We show that TID-induced trapped charges in the oxide alter the intrinsic cell properties causing accuracy degradation of flash-PUF. We propose two independent techniques to improve the PUF accuracy under radiation environment. The first technique relies on electrical annealing which compensates the trapped charges by program stressing. The second technique uses radiation compensation method by adaptive PUF generation process. Our experimental results show that the accuracy degradation can be as low as 1.5% for TID up to 10 krad(Si) with these radiation mitigation techniques.**

***Index Terms*— Flash memory, gamma ray, physical unclonable function (PUF), total ionizing dose (TID).**

I. Introduction

PHYSICAL unclonable function (PUF) is one of the fundamental hardware security primitives [1]. It is used for device-specific secret key generation providing a secure device authentication method analogous to physical fingerprinting [2]. While traditional approaches of storing device identifiers (or keys) on dedicated nonvolatile memory devices are stable and convenient, the stored identifiers can be easily cloned and tampered with by the adversary. Hence, PUFs are increasingly getting popular for low cost and secure device authentication. With the increasing number of small-scale satellites in space, cybersecurity issues are becoming very important. Thus, secure authentication of the satellites using PUFs will become very important for future satellite-to-satellite or satellite-to-ground station communication systems [3], [4].

The key concept behind the semiconductor PUF is the utilization of manufacturing process variation to generate an unpredictable digital signature, which is unique for a given chip. PUFs need to be robust and reproducible under the operating condition for its successful utilization. This is a critical challenge for adopting PUFs in space electronic systems, which need to operate in extreme ionizing radiation environments. Since ionizing radiation affects the physical properties of the semiconductor devices [5]–[7] by trapping charge in the oxide or creating defects at the oxide–silicon interfaces, the PUF characteristics may change with total ionizing dose (TID) absorbed by the device. Hence, it is very important to evaluate the PUF accuracy as a function of TID before adopting it in the space electronic systems.

Recent publications have investigated TID effects on PUF characteristics [3], [4]. More specifically, Wang *et al.* [4] investigated TID effects on CMOS breakdown PUF (BD-PUF). Degradation of PUF characteristics was reported under high-dose proton irradiation due to threshold voltage (V_t) shifts in the selector transistor. Martin *et al.* [3] analyzed the degradation of a ring oscillator PUF due to TID effects. They demonstrated significant degradation of the PUF characteristics and possible countermeasures at a TID level of ∼500 krad(Si). These studies demonstrate the vulnerability of current semiconductor PUFs in a TID environment and the need to further study new types of semiconductor PUFs.

In this article, we evaluate the TID response of flash-memory-based PUF using Co-60 gamma irradiation. Flash-PUF [8]–[16] has unique advantages compared with the other state-of-the-art PUF generation methods. For example, flash-PUF can be generated from commercial-off-the-shelf (COTS) memory chips without any hardware modification. In addition, the number of bits in the flash-PUF can be orders of magnitude higher compared with other PUFs due to the high bit density of flash memory chips. Since flash memory is a popular choice for nonvolatile data storage in space electronic systems, flash-PUF will offer additional security functionality without requiring any dedicated PUF circuitry. Unfortunately, there is no published report on the TID response of flash-PUF, which is a very important consideration for the viability of flash-PUF in space electronic systems. Since flash memories are known to have radiation-induced reliability concerns [7], [17]–[20], it is very important to study the TID response of flash-PUF. In this article, we systematically analyze TID effects on the flash-PUF using COTS

Manuscript received May 11, 2021; accepted May 18, 2021. Date of publication June 7, 2021; date of current version July 16, 2021. This work was supported in part by the U.S. Department of Energy, Office of Nuclear Energy, under the Department of Energy (DOE) Idaho Operations Office as part of a Nuclear Science User Facilities experiment under Contract DE-AC07-051D14517 and in part by the National Science Foundation under Grant 1929099.

Sadman Sakib, Md. Raquibuzzaman, and Biswajit Ray are with the Department of Electrical and Computer Engineering, The University of Alabama in Huntsville, Huntsville, AL 35899 USA.

Maryla Wasiolek and Khalid Hattar are with Sandia National Laboratories, Albuquerque, NM 87185, USA.

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TNS.2021.3087106.

Digital Object Identifier 10.1109/TNS.2021.3087106

single-level-cell (SLC) NAND flash memory chips from Micron Technology.

The rest of this article is organized as follows. Section II demonstrates the comparison between flash-PUF and other state-of-the-art PUF generation technique, Section III discusses the NAND flash details, chip specification, radiation details, and the experimental procedure. The device physics of flash-PUF and the implementation technique are described in Section IV. In Section V, the pre- and postradiation PUF accuracy is analyzed, and two mitigation techniques are proposed. We conclude the article in Section VI.

II. Comparison of Flash-PUF and Other Si-PUF

A large number of Si-based PUF constructions have been proposed that use random process variation in transistor characteristics [1], [21]–[28]. A dominant class of Si-based PUF uses time delay characteristics of transistors and interconnects, such as Arbiter PUF [22] and ring oscillator PUF [1], [27]. The other important class of Si-based PUFs uses cell-to-cell variability of memory array, such as static random-access memory (SRAM) PUF [23], [24], dynamic random-access memory (DRAM) PUF [29], [30], and resistive random access memory (RRAM) PUF [28]. Additionally, the randomness in the CMOS oxide breakdown location is used to generate PUFs that are found to be very robust [4], [26], [31], [32]. All these PUF constructions have certain advantages and disadvantages. For example, most of the PUF constructions (arbiter PUF, ring oscillator PUF, oxide breakdown PUF) require hardware modification during chip design, and hence they are not applicable on many existing systems that do not include these single-purpose circuits. Similarly, the state-of-the-art memory-based PUFs usually suffer from low accuracy and they commonly require inconvenient system operation, such as power on/off cycles. In addition, some of these PUFs are reported to be vulnerable to side-channel attacks [33]. In contrast, flash-PUF does not require any hardware modification and hence widely applicable on many existing electronic platforms. Second, the proposed flash-PUF generation method does not involve any inconvenient system operation which will facilitate convenient implementation. Third, due to high density of flash memory, it is possible to generate millions of different PUF signatures with high bit length offering higher security.

III. Experimental Details

A. Nand Flash Device Details

In this work, we used five COTS SLC NAND flash memory chips from Micron Technology. The chips were fabricated using a 25-nm planar process which is a 2-D NAND technology. The part number of the chip was MT29F8G08ABACAWP: C. The chips were in thin small outline package (TSOP) format. The bit capacity of the chips was 8 Gb which includes 4096 logical blocks, where each block contains 64 memory pages. The page size is 4320 bytes including 4096 bytes for user data and 224 spare bytes to perform error correction.

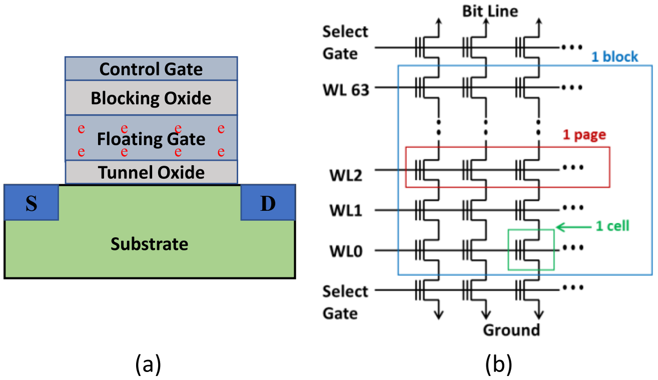

Fig. 1. (a) Planar NAND flash memory cell (e.g., program state). (b) Typical 2-D NAND flash memory array.

Fig. 1(a) shows the structure of a planar flash memory cell, which is essentially a metal oxide semiconductor field-effect transistor (MOSFET) with a floating gate. The floating gate stores information in the form of charges and retains those charges without requiring external power. The memory cell is in the programmed state (logic 0) when electrons are stored on the floating gate, whereas it is in the erased state (logic 1) when there are no electrons on the floating gate. In a 2-D flash array [Fig. 1(b)], the cells connected in a row constitute a page and a collection of pages forms a block. All the cells in a page, share a common metal word line (WL), which acts as a control gate of the memory cell. All the cells in each column of a memory block are connected to a metal bit line (BL) at one end and grounded at the other end. Depending on the manufacturer, the page size varies from 2 to 16 kB. Memory-read and program operations are performed at the page-level granularity, while erase is performed at the block granularity. Any flash cell that is set to a logic "0" by a program operation on a page can only be reset to a logic "1" by erasing the entire block. The program operation is performed by applying a high voltage on the control gate and the substrate is grounded. During the erase operation, a high voltage is applied to the substrate and the control gate is grounded.

B. Gamma-Ray Irradiation

The flash chips were irradiated using a Co-60 source located at Sandia National Laboratories' Gamma Irradiation Facility in Albuquerque, NM [34]. The dose rate of the exposures was 18.6 rad(Si)/s. The chip was irradiated up to a TID level of 10 krad(Si). The dose rate used in the irradiation experiments is high and it may not reflect the real space environment. It is difficult to perform low-dose experiment for the same TID level due to time and budget constraints. We performed gamma-ray irradiation on flash chips with all pins grounded. Since nonvolatile flash memories are designed to retain data without any power, unbiased irradiation is an important test condition. In addition, unbiased irradiation minimizes degradation in the peripheral circuitry which allows us to focus on the TID-induced failures originating from the memory cells. The direction of gamma rays during irradiation was perpendicular to the top surface of the chip, and the entire unlidded chip was irradiated.

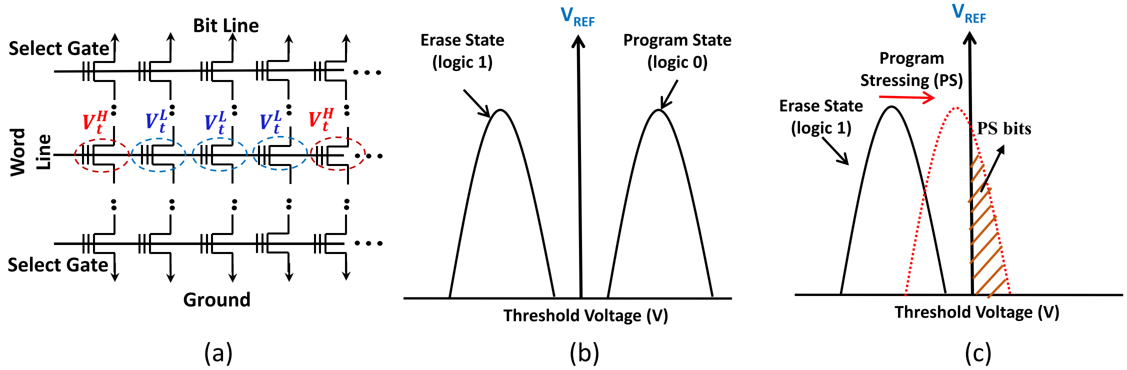

Fig. 2. (a) Typical NAND flash memory array showing the threshold voltage variation in an individual cell due to process variation. (b) Threshold voltage distribution of memory cells in the erased and programmed state. (c) Red dashed line represents the disturbed erase state distribution, which is shifted right due to PS operations.

C. Experimental Setup and Procedure

We used a custom-designed flash test board to interface the NAND flash memory chip to a computer through a universal serial bus (USB) interface. The test board contains a 48-p-i-n NAND flash socket to hold the TSOP flash chip packages and an Atmel ATSAM3U4C ARM Cortex-M3 microcontroller to issue commands and send/receive data from the chip. The hardware board allowed us to access the raw memory bits without any error correction. The hardware setup was not exposed to gamma radiation. Only the NAND flash memory chip was exposed to radiation. Before sending the chips for irradiation, we generated PUF from ten different memory blocks. The memory chips were then exposed to gamma radiation. We generated PUFs from the irradiated chips following the same procedure used during preirradiation. Note that the irradiated chips were shipped from Sandia National Laboratories to The University of Alabama in Huntsville, and we assume that the chips were under room temperature during shipping (1 week). In general, we observed that the annealing effects on these devices over a week time frame under room temperature are not very significant. Moreover, we are mainly concerned with the degradation trends and not the absolute value of degradation.

IV. Background on Flash-PUF

A. Device Physics of Flash-PUF

A flash memory page contains thousands of memory cells (the chip under test has ~32k cells), where cell-to-cell process variation is inherently observed [11], [15]. Due to process variation, the cells within the same page will have different analog V_t even when all the cells are in the erased condition. This is illustrated in Fig. 2(a) where we show the circuit diagram of a flash memory array. The arrangement of high and low V_t cells within the page is unique for a given memory location. Even if we consider another memory page address in the same chip, the V_t variation pattern will be very different. Utilization of this cell-to-cell V_t variation for generating a unique digital signature is the core of flash-PUF generation method which has been explored by several researchers in the recent past [8]–[12].

Extracting the V_t variation in the COTS memory chip using digital interfaces is not straight forward. The internal circuitry of the chip performs digitization of the analog cell V_t by applying a read reference voltage, V_{REF}, as illustrated in Fig. 2(b). The cell-to-cell V_t variation is represented in Fig. 2(b) with analog V_t distribution for both erase and program states. All the cells in the erase state ($V_t < V_{\mathrm{REF}}$) are read as logic "1" despite cell-to-cell V_t variation. The same holds for the cells in the program state, which are read as logic "0." Therefore, the digitization process hides the process variation to the user. Several memory disturbance techniques were explored in the recent past to extract the variation in flash memory cells using digital interfaces. Some of the disturbance techniques include partial program, partial erase, program disturb, read disturb, and neighbor WL interference [8]–[12]. The basic idea behind the memory disturbance technique is to force the memory to an unreliable state that will manifest the cell-to-cell V_t variation. This is illustrated in Fig. 2(c) with erase state V_t distribution. The dashed line denotes the disturbed erase state distribution due to repeated program stress (PS) operations on a given memory page. The disturbed erase state V_t distribution will manifest the V_t variation, where the high-V_t cells will be read as logic "0" and the low-V_t cells will be read as logic "1." Next, we will explain the step-by-step hardware implementation technique for flash-PUF generation.

B. Hardware Implementation Technique for Flash-PUF

PUF-based device authentication involves two phases: 1) enrolment and 2) authentication. The enrolment phase takes place in a trusted and reliable environment such as at the ground station. Enrolment PUF is usually generated on several specific memory page addresses and stored in the database for future verification. The authentication PUF is generated at the user end (spacecraft), upon receiving a request in the form of a challenge (e.g., page address) and it is sent back to the ground station for verification. The ground station compares the authentication PUF with the enrolment PUF to authenticate the device.

Note that most of the NAND flash memory chips come with standard command sets which are called Open NAND

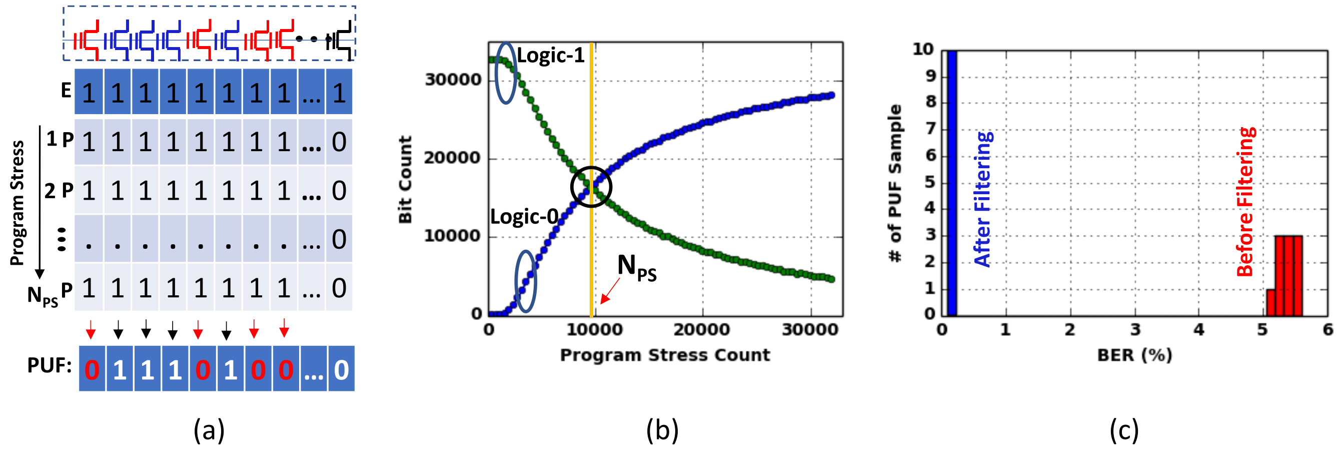

Fig. 3. (a) Illustration of flash-PUF generation technique using PS characteristics. Each row in the figure represents a bit map of the selected flash memory page. (b) Characterization process of the required number of PS operations to generate PUF. (c) Histogram plot showing the PUF bit error rate (BER), before and after filtering the noisy bit.

Flash Interface (ONFI) commands [35]. We have used those commands to implement the PUF generation technique on the COTS NAND memory chips. Fig. 3(a) illustrates the hardware implementation technique for the flash-PUF. The cell V_t variation in a physical memory page is shown with a different color on the top of the bit map table. The cells with a red color represent high V_t^H cell, whereas cells with blue color represent low V_t^L cell. Each subsequent row in the figure represents the logical bit map of the selected flash memory page obtained with a page read operation. We start with an erased memory page, as shown in the first row of the bit map table of Fig. 3(a). Then, we program the last 32 bits of a page [second row in Fig. 3(a)]. We continue programming the same physical memory page with same data pattern, without performing any erase operation, to ensure PS operations. Repeated PS operations cause weak programming of the erased cells. Therefore, after a certain number of PS operations, some of the erased cells will flip to the program state based on their initial analog V_t value (PS bits). Hence, after performing a certain number of PS operations (N_{PS}), we find a unique and unpredictable signature or PUF from that page, as shown in the last row in Fig. 3(a). The parameter N_{PS} is a chip-dependent parameter which needs to be precharacterized during the enrolment phase. We would like to emphasize that similar repeated programming technique had been previously explored by other researchers to characterize the radiation reliability of NAND flash memory [36], [37]. The novelty of our work is the application of this technique for hardware security function generation.

Fig. 3(b) illustrates the characterization process of N_{PS} for PUF generation. We plot the total number of logic “0” (blue) and logic “1” (green) bits in a given memory page as a function of N_{PS}. The zeros are essentially the erase-to-program flipped bits due to repeated PS operations. At the beginning, all the bits of the page are in erase state or logic “1”. With higher N_{PS}, more erase bits flip to zero reducing the count of logic “1” bits in the page, whereas the logic “0” bits increases monotonically. We stop PS when 50% bits get flipped to logic “0” state as shown in Fig. 3(b) with the crossover point. The value of N_{PS} needs to be characterized during PUF enrolment phase and it can be sent as a part of challenge during the authentication phase. More elaboration on flash-PUF generation technique is given in our previous publication [12].

V. Results and Discussion

A. PUF Accuracy Measurement

Accuracy of the flash-PUF is a very important metric for its successful implementation. PUF accuracy is typically quantified in terms of bit error ratio (BER) between the enrolment PUF and the authentication PUF. Mathematically

$$\text{BER} = \frac{\#\text{ of error bits}}{\text{Total }\#\text{ of PUF bits}}. \tag{1}$$

The error bits in the PUF are defined as the mismatched bits between the recorded PUF value during enrolment phase and the PUF value obtained during the authentication phase. The PUF length is the page size which varies between 4 and 16k bytes depending on the NAND memory chip. Ideally, BER needs to be 0%, which means that the authentication PUF exactly matches with the enrolment PUF. However, PUF generation inherently involves a certain amount of BER due to memory noise [38]. The inherent BER can be reduced by filtering out the noisy bits. The noisy bits in our flash-PUF implementation are those bits which change their state near the crossover point of Fig. 3(b). The filtering technique can be explained as follows: we apply ($N_{\text{PS}} - \Delta N_{\text{PS}}$) PSs and note down the logical bit state of the memory page. The logical zeros are stable zero bits of the PUF. Next, we apply ($N_{\text{PS}} + \Delta N_{\text{PS}}$) PSs and identify the incremental 1→0 flipped bits. These incremental 1→0 flipped bits are the noisy bits which will be marked as do not care bits. The remaining bits of the page are stable ones of the PUF. This noisy bit filtering technique is detailed in our previous publication [12]. Fig. 3(c) shows the inherent BER in the PUF before and after noise filtering. To make the result statistically robust, we generate ten different PUFs from ten physically different memory pages

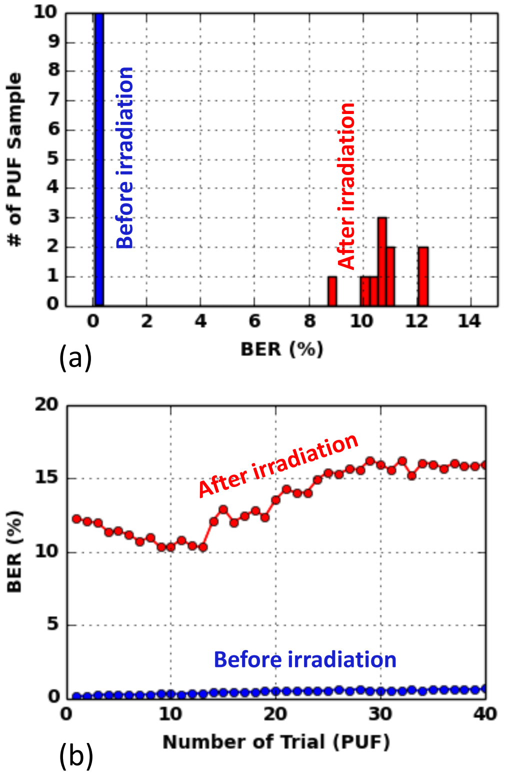

Fig. 4. (a) PUF accuracy from flash chip before and after irradiation [TID = 10 krad(Si)]. We used ten different PUFs to construct the histogram plots. (b) PUF accuracy is plotted for a number of trials. The same PUF is generated from a given memory location for several times to construct this plot.

and compute the BER for each of these PUFs. The BER from ten PUFs is summarized in Fig. 3(c) with the histogram plot. We find that noise filtering significantly improves the PUF BER. After filtering, the inherent BER is very small (around 0.2%) given the high number of PUF bits (20k bits). The authentication algorithm usually accepts such low BER as standard error correcting codes will be able to correct this low BER.

B. TID Impact on PUF Accuracy

To evaluate the impact of TID on PUF characteristics, the same flash memory chips containing the PUF were exposed to Co-60 gamma-rays up to a TID level of 10 krad(Si). After exposure, we generated authentication PUFs from the irradiated chips. We used the same memory addresses and followed the same steps that used preirradiation to generate the PUFs. We compared the corresponding PUF bits to calculate the BER. The BER distribution for ten different PUFs is shown in Fig. 4(a) using a histogram plot. The plot compares the BER distribution before and after irradiation. We find that the PUF BER increases significantly [∼12%, red bar in Fig. 4(a)] after irradiation in comparison to the BER obtained before irradiation. This means that the PUF accuracy decreases with the TID posing a significant challenge for using flash-PUF in radiation environments.

Next, we analyze the accuracy degradation by generating the authentication PUF multiple times from the same memory page. Fig. 4(b) shows that the postirradiation PUF accuracy remains poor even after repeating the PUF generation several times. For comparison purposes, we show the effect of repeated PUF generation from the same memory location for the irradiated and unirradiated chips. We find that the BER of the PUF remains the same or slightly increases with repeated trials. The reason for such a gradual increase in PUF-BER is due to limited endurance of flash memory which had been explained in detail in [12]. The important point in Fig. 4(b) is that the BER of the irradiated PUF remains consistently higher than the unirradiated case. This implies that the physical characteristics of the memory cells are changed significantly after TID exposure and the changes remain intact even after several program-erase operations. Note that the irradiated chips remain fully functional after irradiation. We confirm this by performing basic memory operations such as erase, program, and read on multiple memory locations of the irradiated chip, which does not show any bit error.

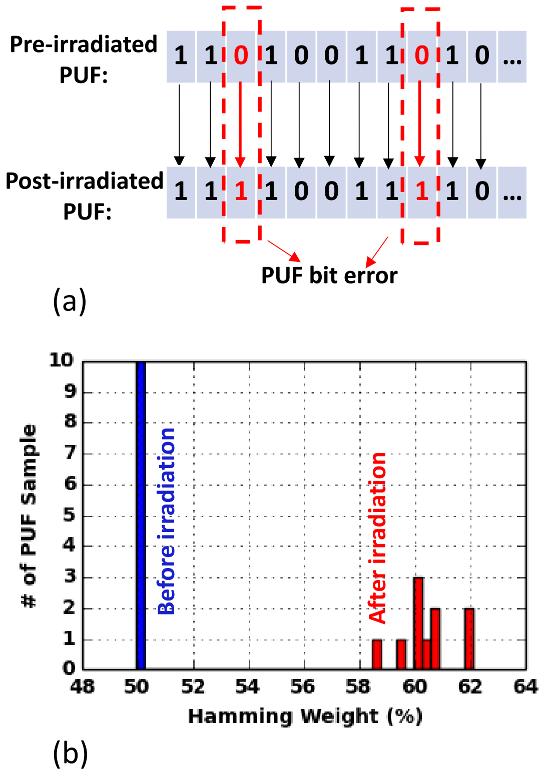

Fig. 5. (a) Illustration of PUF bit error from unirradiated and irradiated chips. (b) Hamming weight of the PUF—before and after irradiation [TID = 10 krad(Si)].

C. Postradiation PUF Degradation Analysis

To understand the irradiation effects on the PUF characteristics, we examine bit-by-bit errors of the PUF from the irradiated chips. As an illustration, we show the PUF bits generated from the same memory location before and after irradiation in Fig. 5(a). We find that most of the errors on the irradiated chips come from the 0→1 bit flip as illustrated in Fig. 5(a). In other words, PUF bits from the irradiated chips are predominantly at logic one states. This is a serious concern for the randomness of the PUF. A good PUF needs

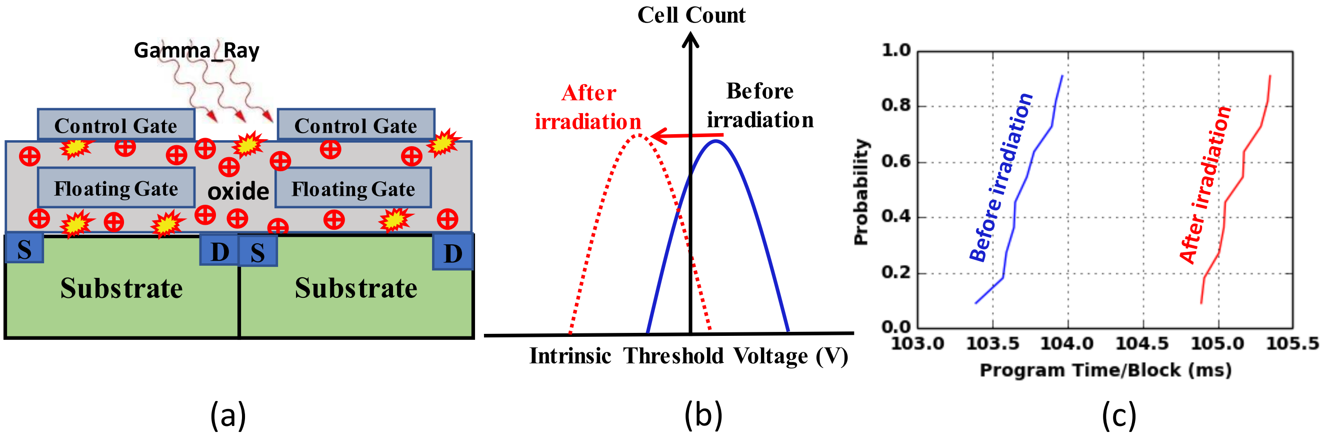

Fig. 6. (a) Illustration of trapped positive charges and oxide defects of the irradiated chip. (b) Schematic of intrinsic cell V_t distribution before and after irradiation. (c) Measured program time on the same memory chip before and after irradiation [TID = 10 krad(Si)].

to be random, meaning that it must have around 50% zeros and 50% ones. Hamming weight (HW) is usually specified to measure the randomness of the PUF. HW simply counts the percentage of ones in the PUF. Fig. 5(b) shows the measured HW of the flash-PUF where we compare HW before and after irradiation. On the unirradiated chip, the HW is ~50%, which is the ideal value for a good PUF. However, on the irradiated chip the HW is significantly greater than 50% implying more ones than zeros in the PUF. Since flash-PUF is generated by stressing an all-one page, we conclude that TID effects slow down the one-to-zero-bit flipping rate.

Our hypothesis about the TID effects on the irradiated flash memory cells is explained in Fig. 6(a), where we show that positive charges are trapped in the oxides of the flash memory cells after irradiation. The trapped charges in the inter-cell region of the oxides are the most difficult one to neutralize by the usual flash program and erase operations as they are not directly affected by the gate electric field. The trapped positive charge will lower the intrinsic (or erase) cell V_t distribution as shown in Fig. 6(b). This will degrade the program speed of the memory array as more program pulses will be required to achieve the program V_t. We confirmed this hypothesis by measuring the program time before and after irradiation from the same chip. Fig. 6(c) shows the measured program time distribution from ten different blocks before and after irradiation. We find that the program time increases after irradiation confirming our hypothesis. Note that it is hard to perform simulation for COTS flash memory where the details of cell geometry, insulating stacks, and the array structures are not clearly known. In addition, there are several proprietary algorithms used during programming and reading of the NAND array which make the simulation exploration very hard. Hence, we relied on qualitative hypothesis for the experimentally observed behavior and supported our hypothesis with the measurements of array characteristics. All the experimental results in this work are based on high-dose-rate irradiation experiments; however, we observed considerable reduction in PUF BER with longer duration of time. For example, the irradiated PUF BER decreased from ~10% to 6% after one year of idle period at room temperature. Thus, the trap-charge annealing effects [39], [40] need to be taken into consideration for accurately estimating the PUF BER in a real irradiation condition with lower dose rate.

D. TID-Induced Error Mitigation Technique for PUF

In this section, we provide two independent methods for mitigating the TID-induced errors in flash-PUF. Although PUF BER decreases with time due to trap-charge annealing effects, it still remains significantly higher than the preirradiation condition suggesting the requirement of error mitigation technique. Below we discuss these methods using the experimental evaluation results.

E. Electrical Annealing

We propose an electrical annealing technique, which compensates the effects of trapped positive charges by a specially designed repeated program operation. The annealing technique is illustrated in Fig. 7(a), where we show the exact data pattern used for repeated program operation. As shown in Fig. 7(a), we increment one program bit in the data pattern for every program operation. In other words, only one bit gets programmed after each programming step. Therefore, we have to repeat the programming operation 32k times to program all the bits in a page. Because the program operation involves application of a high positive voltage on the WL, we believe that the annealing step will push out the trapped charges from the oxide region of the physical memory cells. Even though the PUF generation method [Fig. 3(a) and the electrical annealing process [Fig. 7(a)] involve repeated PS operations, their implementation differs in terms of data pattern used during stressing. For PUF generation [Fig. 3(a), the data pattern during PS operation remains fixed, whereas during electrical annealing, the data pattern changes in each PS operation.

Fig. 7(b) illustrates the effect of electrical annealing on the PUF accuracy. We compute the BER of ten different PUFs after annealing on irradiated chips. The BER distribution is

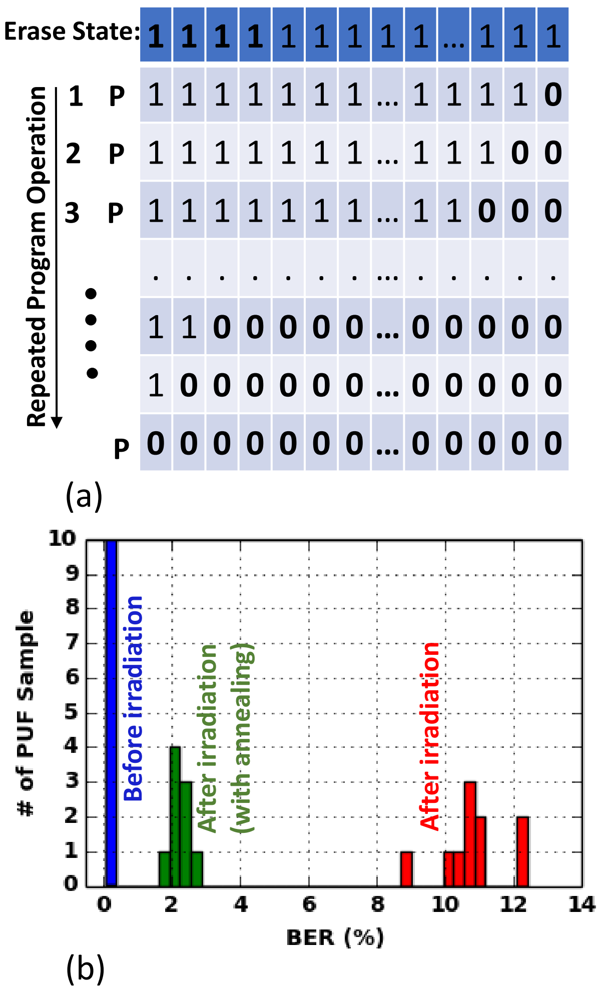

Fig. 7. (a) Step-by-step implementation of electrical annealing technique. (b) PUF accuracy after electrical annealing on the irradiated chips. PUF accuracy without annealing is also shown for comparison.

shown with histogram plot in Fig. 7(b). For easy comparison, we show the PUF BER distribution from the same chip for three different conditions: before irradiation (blue), after irradiation (red), and postannealing (green). We find that the PUF accuracy improves significantly after annealing. Before annealing, the BER was around 12% (irradiated chip), and post annealing, the BER is reduced to around 2%. Hence, this annealing technique ensures the applicability of authentication PUF in a radiation environment.

Note that identification of the exact underlying mechanism for the observed electrical annealing effects is difficult as the irradiated parts are COTS chips which limits our in-depth cell-by-cell experimental evaluation. Hence, we hypothesize that the proposed electrical annealing technique compensates for the effects of trapped positive charge possibly by trapping new electrons on the oxide layer. Since electrical annealing involves application of high positive voltage on the WL, it may cause electron trapping in the oxide layer. Since cell threshold voltage depends on the total charge, the trapped electrons will essentially compensate the effects of trapped holes in the oxide. Note that electrical annealing is distinctively different than the temperature-induced annealing effects [41]–[43]. We find that the temperature-induced annealing of PUF degradation takes place over a long period of time. However, the electrical annealing technique instantly compensates for the radiation effects.

There is a significant latency (∼1 min) involved in the annealing process as we had to perform repeated PS operation for 32k times. However, electrical annealing can be performed in the background or idle state of the memory, which will not directly affect the user operation. In general, the annealing process can be further optimized to improve the latency. For example, instead of programming one bit at a time, we may choose one-byte programming at a time, which will reduce the latency by a factor of 8. However, the goal of this analysis is to demonstrate the feasibility of this interesting technique to compensate the positive trapped charges, which may improve memory reliability and performance. Note that the annealing process on unirradiated chip may degrade the physical characteristics (e.g., cell endurance, data retention) of flash memory cells as it involves repeated program operations [36], [37]. We have evaluated the impact of annealing on the cell physical characteristics by writing different data patterns and computing the fail bit count before and after annealing. We find that the cell characteristics of an unirradiated chip are not noticeably affected by the annealing step. According to the flash memory reliability literature, erase operation is the most harmful for cell reliability as it creates defects in the oxides [44]. Since there was no erase operation involved during the electrical annealing process, the cell endurance remains relatively unaffected.

1) Adaptive PS to Compensate for TID: In this technique, we propose to adapt our PUF generation method based on irradiation condition. More precisely, we propose to adapt the value of N_{PS} for PUF generation after irradiation. Since TID damage lowers the intrinsic cell V_t distribution, a higher number of N_{PS} will be needed to disturb the erase state of the irradiated chip. Similar conclusions were made in previous publications where the number of pulsed programming steps was found to be increasing with TID exposure [36], [37]. We illustrate this in Fig. 8(a), where we plot the 1→0 bit flipping rate as a function of N_{PS} before (blue) and after (red) irradiation. We find that the 50% bit flipping (or the crossover point) on the memory page takes place at a higher N_{PS} value after irradiation. This is the main reason for the degraded PUF accuracy. In other words, if we follow the same PUF generation procedure with $N_{\text{PS}} \sim 10\,000$ on the irradiated chip, the resulting PUF will have more ones than zeros. This is exactly what we found in the measured data as explained using the HW in Fig. 5(b).

Our experimental evaluation in Fig. 8(a) shows that the unirradiated chip requires $N_{\text{PS}} \sim 10\,000$ to achieve 50% bit flips (1→0), whereas the irradiated chip requires around $N_{\text{PS}} \sim 20\,000$ PSs. This means the parameter NPS can be used to compensate the effect of TID. Since we used a fixed number of N_{PS} to generate the PUF after irradiation, the PUF accuracy after irradiation was poor. If we increase N_{PS} based on the absorbed dose, the PUF accuracy improves significantly. Fig. 8(b) shows the experimental result of this compensation method, where PUF is generated from the irradiated chip with

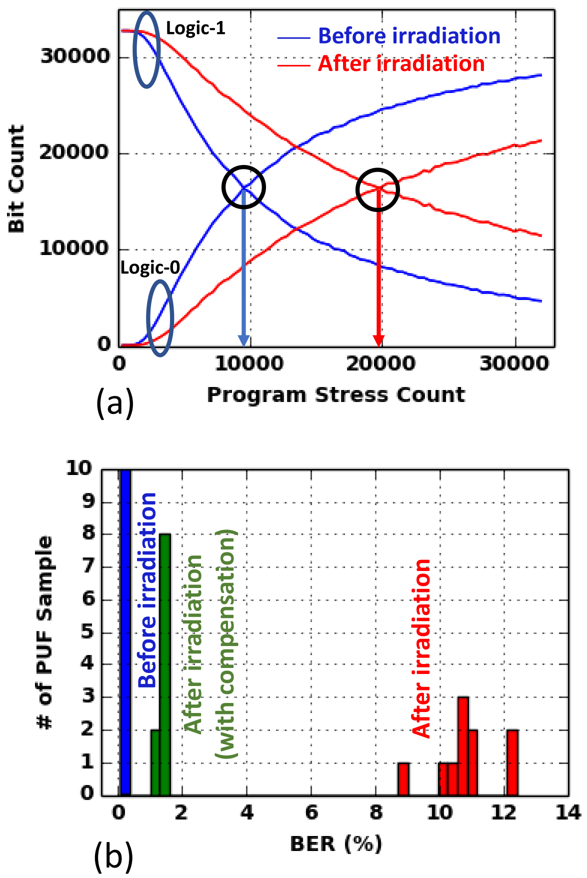

Fig. 8. (a) Comparison of 1→0 bit flipping rate with N_{PS} before (blue) and after (red) irradiation [TID = 10 krad(Si)] from the same chip. The postirradiation crossover point shifts right, which means slower 1→0 bit flipping. (b) PUF accuracy with adaptive PS technique.

the application of optimal N_{PS}. However, the optimum N_{PS} count depends on the type of flash memory, absorbed dose, and the type of radiation which needs to be precharacterized in a controlled environment. Alternatively, the controller can adapt the PUF generation method by monitoring the HW as a function of N_{PS} value and keep stressing the memory page till the HW reaches 50%. Thus, instead of fixed PS count, the controller will decide on the PS count value based on HW. In this way, adaptive stressing will be very effective to correct TID-induced errors. Another advantage of the adaptive PS technique is that it can be used to mitigate the aging-induced effects during PUF generation [12].

VI. Conclusion

The key contributions of this article are as follows.

1) We investigate the TID impact on SLC NAND flash-memory-based PUF. We find that the intrinsic threshold voltage of flash memory cells is affected by TID exposure and thereby reduces the PUF accuracy of irradiated memory chip.
2) We find that the change in the intrinsic threshold voltage of the flash cells cannot be reversed by several erase/program operations.
3) We propose an adaptive PS technique and an electrical annealing technique to improve the PUF accuracy. Adaptive PS involves the application of optimal PS during PUF generation, whereas annealing technique removes the TID-induced trap charges by repeated program operation with specially designed data pattern. The experimental data show that the proposed mitigation techniques improve the PUF accuracy significantly.
4) The electrical annealing technique involves longer latency to implement but improves the overall memory performance and PUF accuracy. Adaptive PS technique is faster to implement but requires a prior knowledge of absorbed dose.

In general, the proposed TID effects' mitigation techniques are easy to implement, do not require any hardware modification, and can be applied on a wide range of flash memory chips.

Acknowledgment

The work of Maryla Wasiolek, Khalid Hattar, and Michael McLain was supported by the Sandia National Laboratories, a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. DOE's National Nuclear Security Administration under Contract DE-NA-0003525. The views expressed in the article do not necessarily represent the views of the U.S. DOE or the United States Government.

References

[1] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. 44th ACM/IEEE Design Autom. Conf.*, Jun. 2007, pp. 9–14.

[2] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proc. IEEE*, vol. 102, no. 8, pp. 1126–1141, Aug. 2014, doi: 10.1109/JPROC.2014.2320516.

[3] H. Martin, P. Martin-Holgado, Y. Morilla, L. Entrena, and E. San-Millan, "Total ionizing dose effects on a delay-based physical unclonable function implemented in FPGAs," *Electronics*, vol. 7, no. 9, p. 163, Aug. 2018, doi: 10.3390/electronics7090163.

[4] P. F. Wang *et al.*, "X-ray and proton radiation effects on 40 nm CMOS physically unclonable function devices," *IEEE Trans. Nucl. Sci.*, vol. 65, no. 8, pp. 1519–1524, Aug. 2018, doi: 10.1109/TNS.2017.2789160.

[5] J. R. Schwank *et al.*, "Radiation effects in MOS oxides," *IEEE Trans. Nucl. Sci.*, vol. 55, no. 4, pp. 1833–1853, Aug. 2008, doi: 10.1109/TNS.2008.2001040.

[6] D. M. Fleetwood, "Radiation-induced charge neutralization and interface-trap buildup in metal-oxide-semiconductor devices," *J. Appl. Phys.*, vol. 67, no. 1, pp. 580–583, Jan. 1990, doi: 10.1063/1.345199.

[7] M. Bagatin, S. Gerardin, and A. Paccagnella, "Space and terrestrial radiation effects in flash memories," *Semicond. Sci. Technol.*, vol. 32, no. 3, Feb. 2017, Art. no. 033003, doi: 10.1088/1361-6641/32/3/033003.

[8] P. Prabhu *et al.*, "Extracting device fingerprints from flash memory by exploiting physical variations," in *Proc. Trust Trustworthy Comput.*, 2011, pp. 188–201, doi: 10.1007/978-3-642-21599-5_14.

[9] S. Jia, L. Xia, Z. Wang, J. Lin, G. Zhang, and Y. Ji, "Extracting robust keys from NAND flash physical unclonable functions," in *Proc. Inf. Secur.* Cham, Switzerland: Springer, 2015, pp. 437–454, doi: 10.1007/978-3-319-23318-5_24.

[10] 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. Secur. Privacy*, May 2012, pp. 33–47, doi: 10.1109/SP.2012.12.

[11] M.-S. Kim, D.-I. Moon, S.-K. Yoo, S.-H. Lee, and Y.-K. Choi, "Investigation of physically unclonable functions using flash memory for integrated circuit authentication," *IEEE Trans. Nanotechnol.*, vol. 14, no. 2, pp. 384–389, Mar. 2015, doi: 10.1109/TNANO.2015.2397956.

[12] S. Sakib, A. Milenković, M. T. Rahman, and B. Ray, "An aging-resistant NAND flash memory physical unclonable function," *IEEE Trans. Electron Devices*, vol. 67, no. 3, pp. 937–943, Mar. 2020, doi: 10.1109/TED.2020.2968272.

[13] T. Saito *et al.*, "High-temperature stable physical unclonable functions with error-free readout scheme based on 28 nm SG-MONOS flash memory for security applications," in *Proc. IEEE Int. Memory Workshop (IMW)*, May 2017, pp. 1–4, doi: 10.1109/IMW.2017.7939086.

[14] T.-N. Nguyen, S. Park, and D. Shin, "Extraction of device fingerprints using built-in erase-suspend operation of flash memory devices," *IEEE Access*, vol. 8, pp. 98637–98646, 2020, doi: 10.1109/ACCESS.2020.2995891.

[15] S. Larimian, M. R. Mahmoodi, and D. B. Strukov, "Lightweight integrated design of PUF and TRNG security primitives based on eFlash memory in 55-nm CMOS," *IEEE Trans. Electron Devices*, vol. 67, no. 4, pp. 1586–1592, Apr. 2020, doi: 10.1109/TED.2020.2976632.

[16] M. Mahmoodi, H. Nili, S. Larimian, X. Guo, and D. Strukov, "ChipSecure: A reconfigurable analog eFlash-based PUF with machine learning attack resiliency in 55 nm CMOS," in *Proc. 56th Annu. Design Autom. Conf.*, Jun. 2019, pp. 1–6, doi: 10.1145/3316781.3324890.

[17] M. Bagatin *et al.*, "Total ionizing dose effects in 3-D NAND flash memories," *IEEE Trans. Nucl. Sci.*, vol. 66, no. 1, pp. 48–53, Jan. 2019, doi: 10.1109/TNS.2018.2878911.

[18] M. J. Kay, M. J. Gadlage, A. R. Duncan, D. Ingalls, A. Howard, and T. R. Oldham, "Effect of accumulated charge on the total ionizing dose response of a NAND flash memory," *IEEE Trans. Nucl. Sci.*, vol. 59, no. 6, pp. 2945–2951, Dec. 2012, doi: 10.1109/TNS.2012.2220156.

[19] F. Irom, D. N. Nguyen, R. Harboe-Sorensen, and A. Virtanen, "Evaluation of mechanisms in TID degradation and SEE susceptibility of Single- and multi-level high density NAND flash memories," *IEEE Trans. Nucl. Sci.*, vol. 58, no. 5, pp. 2477–2482, Oct. 2011, doi: 10.1109/TNS.2011.2161885.

[20] D. N. Nguyen, S. M. Guertin, G. M. Swift, and A. H. Johnston, "Radiation effects on advanced flash memories," *IEEE Trans. Nucl. Sci.*, vol. 46, no. 6, pp. 1744–1750, Dec. 1999, doi: 10.1109/23.819148.

[21] Y. Su, J. Holleman, and B. Otis, "A 1.6 pJ/bit 96% stable chip-ID generating circuit using process variations," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2007, pp. 406–611, doi: 10.1109/ISSCC.2007.373466.

[22] J. W. Lee, D. Lim, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas, "A technique to build a secret key in integrated circuits for identification and authentication applications," in *Symp. VLSI Circuits. Dig. Tech. Papers*, Jun. 2004, pp. 176–179, doi: 10.1109/VLSIC.2004.1346548.

[23] 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, doi: 10.1109/TC.2008.212.

[24] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in *Proc. Cryptograph. Hardw. Embedded Syst. (CHES)*, Berlin, Germany, 2007, pp. 63–80, doi: 10.1007/978-3-540-74735-2_5.

[25] R. Hesselbarth, F. Wilde, C. Gu, and N. Hanley, "Large scale RO PUF analysis over slice type, evaluation time and temperature on 28 nm Xilinx FPGAs," in *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST)*, Apr. 2018, pp. 126–133, doi: 10.1109/HST.2018.8383900.

[26] K.-H. Chuang, E. Bury, R. Degraeve, B. Kaczer, D. Linten, and I. Verbauwhede, "A physically unclonable function using soft oxide breakdown featuring 0% native BER and 51.8 fJ/bit in 40-nm CMOS," *IEEE J. Solid-State Circuits*, vol. 54, no. 10, pp. 2765–2776, Oct. 2019, doi: 10.1109/JSSC.2019.2920714.

[27] 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, doi: 10.1109/HST.2010.5513108.

[28] P.-Y. Chen, R. Fang, R. Liu, C. Chakrabarti, Y. Cao, and S. Yu, "Exploiting resistive cross-point array for compact design of physical unclonable function," in *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST)*, May 2015, pp. 26–31, doi: 10.1109/HST.2015.7140231.

[29] S. Rosenblatt *et al.*, "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, doi: 10.1109/JSSC.2013.2239134.

[30] F. Tehranipoor, N. Karimian, K. Xiao, and J. Chandy, "DRAM based intrinsic physical unclonable functions for system level security," in *Proc. 25th Ed. Great Lakes Symp. (VLSI)*, New York, NY, USA, May 2015, pp. 15–20, doi: 10.1145/2742060.2742069.

[31] N. Liu, S. Hanson, D. Sylvester, and D. Blaauw, "OxID: On-chip one-time random ID generation using oxide breakdown," in *Proc. Symp. VLSI Circuits*, Jun. 2010, pp. 231–232, doi: 10.1109/VLSIC.2010.5560287.

[32] K.-H. Chuang *et al.*, "Physically unclonable function using CMOS breakdown position," in *Proc. IEEE Int. Rel. Phys. Symp. (IRPS)*, Apr. 2017, pp. 4C-1.1–4C-1.7, doi: 10.1109/IRPS.2017.7936312.

[33] J. Delvaux and I. Verbauwhede, "Fault injection modeling attacks on 65 nm arbiter and RO sum PUFs via environmental changes," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 61, no. 6, pp. 1701–1713, Jun. 2014, doi: 10.1109/TCSI.2013.2290845.

[34] *Sandia National Laboratories: Research: Facilities: Gamma Irradiation Facility and Low-Dose-Rate Irradiation Facility*. Accessed: Jan. 30, 2020. [Online]. Available: https://www.sandia.gov/research/facilities/gamma_irradiation_facility.html

[35] *Home-ONFI*. Accessed: Dec. 15, 2020. [Online]. Available: http://www.onfi.org/

[36] A. J. Narasimham, K. M. Han, A. A. Gonzalez, and J. Yang-Scharlotta, "Effect of radiation and endurance on pulsed programming of commercial NAND flash memory," in *Proc. IEEE Int. Integr. Rel. Workshop (IIRW)*, Oct. 2017, pp. 57–62, doi: 10.1109/IIRW.2017.8361236.

[37] A. H. Roach, M. J. Gadlage, A. R. Duncan, J. D. Ingalls, and M. J. Kay, "Interrupted PROGRAM and ERASE operations for characterizing radiation effects in commercial NAND flash memories," *IEEE Trans. Nucl. Sci.*, vol. 62, no. 6, pp. 2390–2397, Dec. 2015, doi: 10.1109/TNS.2015.2490019.

[38] B. Ray and A. Milenković, "True random number generation using read noise of flash memory cells," *IEEE Trans. Electron Devices*, vol. 65, no. 3, pp. 963–969, Mar. 2018, doi: 10.1109/TED.2018.2792436.

[39] M. Bagatin *et al.*, "Error instability in floating gate flash memories exposed to TID," *IEEE Trans. Nucl. Sci.*, vol. 56, no. 6, pp. 3267–3273, Dec. 2009, doi: 10.1109/TNS.2009.2033364.

[40] M. Bagatin *et al.*, "Annealing of heavy-ion induced floating gate errors: LET and feature size dependence," *IEEE Trans. Nucl. Sci.*, vol. 57, no. 4, pp. 1835–1841, Aug. 2010, doi: 10.1109/TNS.2010.2045131.

[41] M. M. Pejovic, M. M. Pejovic, and A. B. Jaksic, "Contribution of fixed oxide traps to sensitivity of pMOS dosimeters during gamma ray irradiation and annealing at room and elevated temperature," *Sens. Actuators A, Phys.*, vol. 174, pp. 85–90, Feb. 2012, doi: 10.1016/j.sna.2011.12.011.

[42] H. Schmidt, D. Walter, M. Bruggemann, F. Gliem, R. Harboe-Sorensen, and P. Roos, "Annealing of static data errors in NAND-flash memories," in *Proc. 9th Eur. Conf. Radiat. Effects Compon. Syst.*, Sep. 2007, pp. 1–5, doi: 10.1109/RADECS.2007.5205505.

[43] S. M. Guertin, D. N. Nguyen, and J. D. Patterson, "Microdose induced data loss on floating gate memories," *IEEE Trans. Nucl. Sci.*, vol. 53, no. 6, pp. 3518–3524, Dec. 2006, doi: 10.1109/TNS.2006.885861.

[44] S. Sakib, P. Kumari, B. Talukder, M. Rahman, and B. Ray, "Non-invasive detection method for recycled flash memory using timing characteristics," *Cryptography*, vol. 2, no. 3, p. 17, Aug. 2018, doi: 10.3390/cryptography2030017.