# Effects of Total Ionizing Dose on SRAM Physical Unclonable Functions

S. P. Lawrence, *Student Member, IEEE,* S. C. Smith, *Student Member, IEEE,* J. M. Cannon, *Student Member, IEEE,* J. L. Carpenter, *Student Member, IEEE,* D. R. Reising, *Senior Member, IEEE,* and T. D. Loveless, *Senior Member, IEEE*

***Abstract*—The effects of total ionizing dose (TID) on SRAM physical unclonable functions (PUF) are studied through x-ray and proton irradiation of commercially available SRAM. Negative shifts in the Fractional Hamming Weight (FHW) were measured with increasing TID, indicating a migration of bistable cells towards logic low. Additionally, positive shifts in the intra-die Fractional Hamming Distance (FHD) were measured and indicate changes to the virtual fingerprint of an SRAM PUF with TID, especially in devices that were dosed while holding data. Shifts in inter-die FHD were negligible, allowing individual SRAMs still to be easily identified based on the FHD between a known and unknown sample even after moderate amounts of TID. In some cases, SRAMs could still be identified by their PUFs after the devices had failed. In all cases, the irradiated SRAM devices retain their virtual fingerprint after recovery through annealing.**

***Index Terms*—Static Random Access Memory (SRAM), Physical Unclonable Function (PUF), Total Ionizing Dose (TID)**

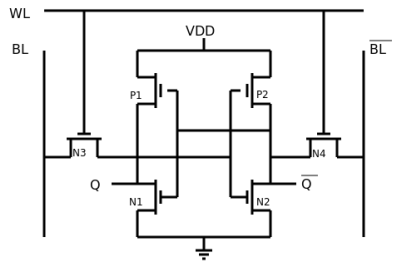



Fig. 1. The conventional SRAM 6T cell features a latch formed by two cross-coupled inverters (P1+N1 and P2+N2) along with two access transistors (N3 and N4). The initial state of the cell primarily is determined by the ratio between the strengths of transistors N1 and N2.

## I. Introduction

STATIC random access memory (SRAM) is a fast and dense form of memory consisting of an array of cells that hold binary data through the use of two cross-coupled inverters accessible through two pass-gate transistors. The conventional six-transistor (6T) cell (see Fig. 1) is commonplace in modern electronics such as field-programmable gate arrays (FPGAs) and application-specific integrated circuits (ASICs), where the memory is used to store configuration and operational data [1]–[3].

SRAM is a volatile form of memory, so data is lost when power is removed from the device. There is no way to recover previously stored data once the voltage supply ($V_{DD}$) is reduced below the minimum data retention voltage ($V_{DR}$). As seen in [4] and [5], $V_{DR}$ varies slightly from cell to cell due to variation of physical parameters such as threshold voltage. This so-called process-induced variation in device parameters is a result of the fluctuations in the physical dimensions and material composition of the devices in an integrated circuit (IC) [5]–[7]. Process variation is proportionally larger and more significant with each new technology node [6]. Although generally undesirable, random manufacturing variation results in unclonable uniqueness, *i.e.*, a virtual fingerprint, specific to each IC. In the field of security and encryption, one type of virtual fingerprint that can exploit natural manufacturing variation is known as a Physical Unclonable Function (PUF) [3].

The SRAM PUF is lightweight in terms of resources and reliable as a form of authentication and encryption. Thus, SRAM PUF can serve as a primary means of protection for intellectual property (IP) [8] or security for Internet of Things (IoT) networks [2], [9], [10]. Using SRAM PUFs for cryptographic key generation has significant advantages over the alternative of storing a key in the actual contents of the memory but often requires a perfectly reproducible key. Specially designed ICs can extract reliable PUFs for this purpose. FPGAs, for example, must be reprogrammed after each power cycle by a bitstream which contains the unencrypted intellectual property (IP) of the circuit designers. Therefore, intruders can extract the bitstream and steal the FPGA design. In devices requiring authentication keys such as members in an IoT network, a pre-generated authentication key stored in local memory is vulnerable to hackers. This pre-determined key manifests as a weak security point where attackers can spoof an IoT device. The SRAM PUF offers unique advantages to designers of systems requiring a high level of security. For example, if an SRAM array within an FPGA is used to encode and decode an encrypted bitstream, intruders have no way to clone the device since it would be

Manuscript received June 16, 2021. Revised manuscript received Sept. 30, 2021.

This work was supported in part by the the National Science Foundation (NSF), #1757777, and the Defense Threat Reduction Agency under award number HDTRA1-17-1-0003.

S. P. Lawrence, J. L. Carpenter, D. R. Reising, and T. D. Loveless are with the Electrical Engineering Department at the University of Tennessee at Chattanooga, 615 McCallie Ave, Chattanooga, TN 37403.

S. C. Smith is with the Electrical Engineering Department at the University of Tennessee at Chattanooga and the Department of Physics at Hillsdale College, 33 E College St, Hillsdale, MI 49242.

J. M. Cannon is with the Department of Aerospace Engineering Sciences at the University of Colorado Boulder, 914 Broadway, Boulder, CO 80310.

impossible to obtain another FPGA with the same SRAM PUF. Additionally, SRAM PUFs offer a built-in key that can be used for authentication, providing the advantage that the actual key is not stored in the device.

As SRAM PUFs continue to grow in prevalence among the privacy and security community, research on the effects of ionizing radiation on SRAM PUF integrity and consistency are warranted. For example, total ionizing dose (TID)-induced degradation of critical parameters, such as threshold voltage, may result in altered PUF-based encryption keys or create difficulties in device authentication. On the other hand, exposure to ionizing radiation can also be used to accelerate aging and burn-in device behavior, leading to more reliable key generation.

In this study, the effects of ionizing radiation on commercial-off-the-shelf (COTS) SRAM memories are studied using x-ray and proton sources, primarily addressing the impact of TID on SRAM PUF reliability. TID effects result from the accumulation of trapped charge within the oxide layers of a semiconductor technology [11], [12]. The resulting shifts in threshold voltage and leakage current of CMOS devices have been thoroughly studied in [11]–[13]. Here, numerous samples of a COTS SRAM with an onboard serial communications interface were used to study the influence of TID on PUF reliability. While limited to one manufacturer and part number, this study describes methods and key results that apply to all SRAM topologies (such as 7T, 8T, 9T, or 10T designs) and communications interfaces (serial versus parallel addressing). Results indicate that SRAM-based PUF technology is robust against TID; moderate shifts in PUF behavior up to TID of approximately 200 krad($SiO_2$) were observed, even when device failures were observed due to the sensitive serial interface circuitry.

## II. Background

There are two main classes of PUFs: delay-based and memory-based. Delay-based PUFs send an electrical pulse through two functionally similar paths comprised of several challenge stages [3], [14]. Latches are used at each stage to record which signal arrived first, resulting in a unique code with a length equal to the number of challenge stages. Some work has been done to characterize the effects of TID on delay-based PUFs [15], [16].

Memory-based PUFs are created by capturing the initial values of an array of latches or memory elements such as SRAM following a power-up sequence. The initial data pattern appears as a repeatable pseudorandom code determined at the cell level based on the drive strengths of the competing inverters (P1+N1 and P2+N2) in each 6T cell. Although by design both inverters are perfectly balanced, manufacturing process variation causes most cells (approximately 85% for the memories tested in this study) to favor either logic high or logic low in their initial states [1]–[3]. The remaining cells initialize in a bistable condition and will randomly toggle to one of the binary states. Therefore, each SRAM device has a unique virtual fingerprint based on its pseudorandom power-up state that varies by approximately 15% each time it is sampled.

### A. Identification of SRAM PUFs

SRAM PUFs are determined by power cycling the memory and reading its contents. In most cases, the power-up ramp ($V_{SS}$ to $V_{DD}$) used in this study was a near-instantaneous step function, although the impact of power-up ramp times on PUF reliability is discussed. The SRAM PUF relies on the bistable bits. Therefore, a power-up and read cycle is repeated several times to identify and characterize the bistable bits. The resulting inconsistencies can be quantified by the Fractional Hamming Weight (FHW), which is a normalized count of the non-zero values for a binary pattern, as described by (1) where $L$ is the length of binary pattern $A$.

$$\mathrm{FHW}(A) = \frac{\sum_{i=0}^{L} A[i]}{L} \tag{1}$$

Fig. 2 shows the FHW for 100 repeated 256-bit samples extracted from five unique ICs (labeled B1 through B5) from the same manufacturer. The length of the PUF samples used throughout this study is $L = 256$ bits. Fig. 2 represents pre-radiation characterization data from the DUTs designated as group B. These data may also be visualized by color-coding the initial states of the memory sample and assigning each pixel in the image a specific address, as shown in Fig. 3, where six 256-bit PUF samples from two different memories (labeled D1 and D2) are shown. Here, the initial state of the same 256-bit block of memory is visualized with a matrix in which the dark pixels correspond to logic high values, and the light pixels correspond to logic low values. The SRAM PUF samples depict the same uninitialized block of memory from the two devices under test (DUTs), visibly demonstrating the nuances that give the SRAM PUF its usefulness. A certain amount of inconsistent bits helps screen out fraudulent authentication attempts. For example, multiple PUF samples could be required to demonstrate slight fluctuation in FHW, adding an extra layer of complexity to the authentication challenge. However, too much inconsistency makes the PUF

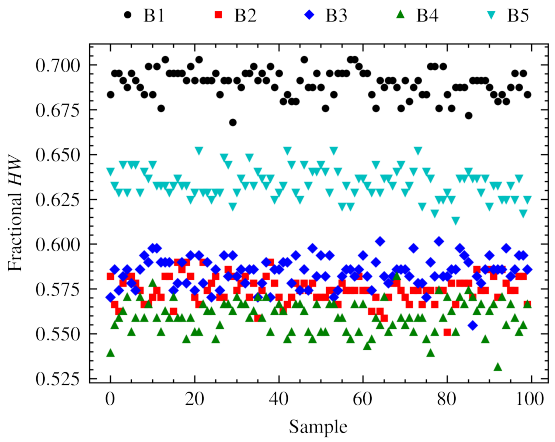
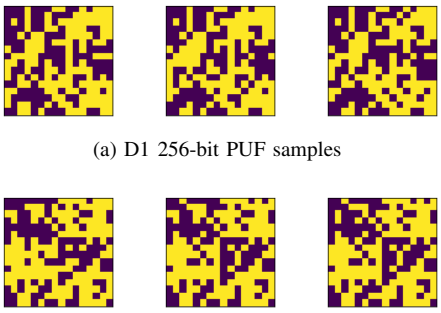



Fig. 2. One hundred repetitious SRAM PUF samples reveal fluctuations in FHW due to inconsistent bits across all five tested devices (B1 through B5). This characterization was performed pre-irradiation at room temperature in the beam chamber prior to turning on the beam. The length of the PUF samples used throughout this study is $L = 256$ bits. This chart represents pre-radiation characterization data from the DUTs designated as group B (see Section III-A for additional details).



(a) D1 256-bit PUF samples

(b) D2 256-bit PUF samples

Fig. 3. SRAM PUF samples determined from the same uninitialized block of memory from two different DUTs (D1 and D2), visibly demonstrating the nuances that give the SRAM PUF its usefulness. FHW fluctuates among samples from the same memory due to bistable cells.

unreliable for authentication. An inconsistency rate of 30% or more has been proposed as a cutoff point for usefulness [1].

### B. SRAM PUF Authentication

Instead of looking for exact matches, authentication methods are often based on Fractional Hamming Distance (FHD) which is the number of mismatched bits between two patterns, normalized by the pattern length, as defined by (2) where $L$ is the length of binary patterns $A$ and $B$.

$$\text{FHD}(A,B) = \frac{\sum_{i=0}^{L} A[i] \oplus B[i]}{L} \tag{2}$$

The FHD between PUF samples obtained from the same chip can be used to measure intra-die consistency, whereas FHD between PUF samples obtained from different chips can be used to measure inter-die consistency. Due to inconsistent bits, it is unlikely that two PUF samples will have a FHD of zero even from the same device. However, the identity of a chip can be verified by comparing a measurement from the device in question to a known FHD probability distribution for that device. Fig. 4 visualizes this approach by depicting the intra- and inter-die FHD. The samples on the lower side of the chart represent the distance between samples of the same block of the same chip (*i.e.*, intra-die variability). In contrast, the samples on the upper side of the chart represent the distance between samples of the same block of different chips (*i.e.*, inter-die variability). The notation "B1-Bx" refers to the FHD between a dosed sample from DUT B1 and an undosed sample from another randomly chosen member of group B.

The intra-die FHD comparisons can be used to determine the identity of an SRAM. The FHD between a known and unknown sample is reliably much lower than the inter-die FHD. This study found a FHD rejection threshold of $L/8$ (*i.e.*, 32 bits for a 256-bit PUF sample) to be reliable for distinguishing non-irradiated SRAMs based on their PUF. The rejection threshold should be carefully considered since some parts tested in this study showed significant positive shifts in intra-die FHD, depending mainly on power supply bias conditions. With greater key length $L$, the discernible window between the distributions grows, providing greater confidence

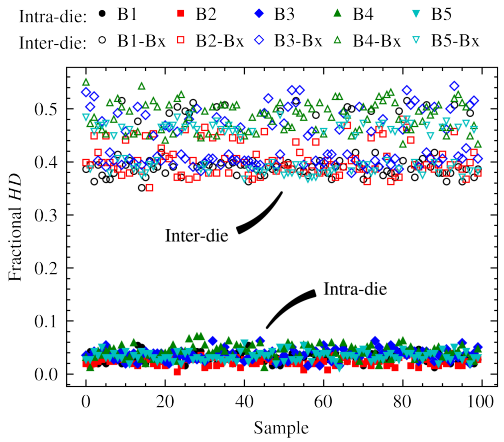



Fig. 4. Intra-die FHD (lower portion of the chart) and inter-die FHD (upper portion) for DUTs B1 through B5, with an easily discernible window separating them. The data points represent the distance between samples of the same block of the same chip (*i.e.*, intra-die variability), while the distribution on the upper side of the chart represents the distance between samples of the same block of different chips (*i.e.*, inter-die variability). The notation "B1-Bx" refers to the FHD between a dosed sample from DUT B1 and an undosed sample from another randomly chosen member of group B (see Section III-C for more details).

at the cost of a larger sample. The likelihood that two SRAMs will have identical PUFs is 1 in $2^L$ if both SRAMs have perfectly balanced cells (FHW of precisely 0.5). If most cells favor a high initial value, the likelihood of two devices having identical PUFs is larger than 1 in $2^L$.

### C. Increasing the Consistency of PUF-Based Encryption Keys

Since a perfectly reliable pseudorandom PUF key is in most cases preferable for encryption, efforts have been made to increase consistency via key generation techniques [17]. The simplest of such methods is to use a mask to ignore the inconsistent cells. However, this requires extensive characterization to uncover all the bistable bits since some unstable cells can be so heavily skewed in one direction that they have the same initial value >99% of the time.

A robust technique for obtaining a reliable PUF is using fuzzy extraction to handle or mask the inconsistent bits [18], [19]. As summarized by [1], fuzzy extraction of SRAM PUFs is achieved by first enrolling helper data from an initial PUF sample and randomly-generated data of equal length. Then a consistent, repeatable key is generated from a second PUF sample based on the helper data by filtering out the inconsistent cells or applying an averaging technique. Still, fuzzy extraction requires specialized circuitry that is perhaps too complex to be manufactured into an embedded device such as FPGAs and ASICs. However, fuzzy extraction is not extraordinarily difficult to implement at the system level on standalone SRAM devices. An acceptable threshold in pattern similarity must be established in the design of the fuzzy extractor, and some reliable method for comparison such as FHD must be implemented.

Another reliable technique to increase SRAM PUF consistency is known as Temporal Majority Voting (TMV) [17], where several successive challenges are issued to the memory,

and a majority voting formula (3) is applied to the sum of the results [17].

$$M_T = \frac{N_T - 1}{2} \tag{3}$$

$M_T$ is the number of votes required for a majority, based on the number of temporal samples $N_T$. Figs. 5 and 6 shows an example of the impact of TMV on PUF consistency, as measured by the FHW and FHD, respectively. One-hundred samples of the FHW and FHD are shown for five devices (B1 through B5) for various values of $N_T$. TMV reduces variability by averaging multiple samples into a single combined key. This, in turn, lowers the average intra-die FHD while leaving inter-die FHD largely unaffected (see Fig. 6). Taken to the extreme ($N_T$ in the thousands), TMV could produce a reliable cryptographic key based on the PUF of any SRAM without the need for fuzzy extraction.

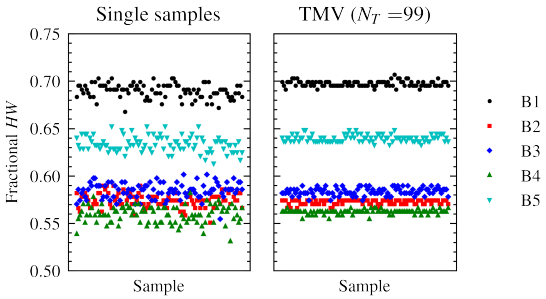



Fig. 5. Comparison of FHW of keys generated with and without Temporal Majority Voting (TMV) [17] reveal that TMV increases the consistency of FHW due to decreased variance in each generated key.

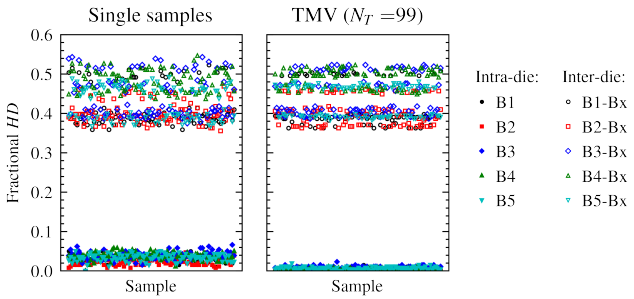



Fig. 6. Comparison of FHD between keys generated with and without Temporal Majority Voting (TMV) [17] show that PUF keys are more easily identifiable by FHD when TMV is implemented. Increasing $N_T$ results in more consistent FHD due to decreased variance in the generated keys.

### *D. PUF Reliability, TID-induced Burn-In, and Artificial Aging*

The PUF of an SRAM is a pseudorandom phenomenon, in which a seemingly patternless array of numbers can be reproduced by a repeatable process [20]. However, as previously mentioned, there is some expected inconsistency in the generated pattern within a single device. Several factors influence the outcome of the inconsistent cells, both instantaneously and gradually over time. Noise is a significant factor in the determination of an SRAM PUF. When an SRAM device is switched on by a step-function power supply curve,

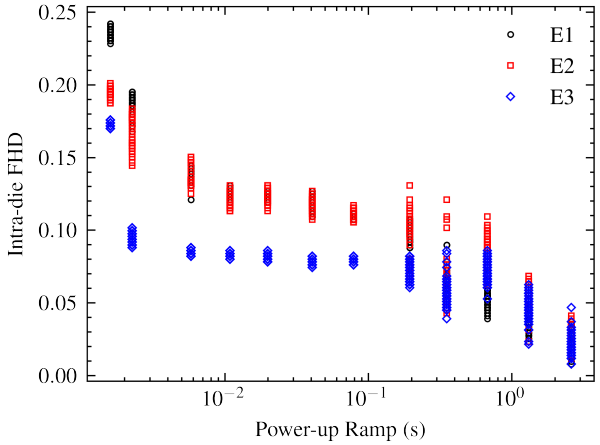



Fig. 7. The effects of power-up ramp time on intra-die FHD are shown. Ramp times ranging from 1.6 ms to 2.6 s were tested by varying the step sizes of a digital-to-analog converter. For each value for ramp time, 100 repetitions were made to verify the accuracy of the results. For the three tested COTS memories, a ramp time of 78 ms produced the most consistent results, with longer ramp times producing generally lower intra-die FHD but a greater variation.

environmental noise becomes "locked-in" to the states of the inconsistent bits [21], [22]. A more gradual supply ramp tends to increase the consistency of an SRAM's PUF by minimizing the impact of noise on the inconsistent bits [22]. Fig. 7 shows the impact of the power-up ramp time on intra-die FHD for three devices (E1 through E3) from the same manufacturer. In this study, a 2-second power supply ramp reduced intra-die FHD by approximately 90% although the ramp was less effective for other tested manufacturers. Thus, a gradual power ramp reduces PUF samples' variation, but not all SRAM cell designs benefit equally.

High temperatures accelerate a process known as bias temperature instability (BTI), where data stored for long periods and during temperature stress can skew an SRAM cell's favored outcome [7], [23]–[25]. This phenomenon weakens the cell's default preference for uninitialized cells (cells that have not been written since a power cycle). Thus, the reliability of an SRAM PUF can be diminished when a cell faces high-temperature stress while holding its favored initial state. Furthermore, as seen in [25], BTI can even cause strongly skewed cells to become inconsistent.

Age is another factor to consider regarding SRAM PUF reliability. BTI causes the initial state of SRAM cells to oppose whatever data has been stored there for long periods [3], [25], [26]. If an SRAM is holding the exact information for long periods, this will increasingly affect the device's initial state. With standalone SRAM devices, where data is expected to be constantly written and overwritten, the effects of age will be less than those in SRAMs embedded within an FPGA, which typically hold the device's configuration data. When used in this manner, age can play a significant role in shaping the identity of an SRAM's PUF, and over time the inconsistent cells may begin to favor the value opposite to what they usually hold. Device aging can be used intentionally by designers to increase PUF consistency using methods discussed in [26].

As SRAM cells age, they naturally experience shifts in

balance and stability which tend to push inconsistent bits away from bistability and towards a more consistent initial state [27], [28]. Through a process commonly known as burn-in, this phenomenon is intentionally hastened by applying temperature and voltage stress. Some work has been published on quantifying the ideal amount of burn-in from a PUF reliability standpoint [27]. TID can induce a similar effect through artificial aging [13], [28], [29] which could potentially be used to reinforce the virtual fingerprint by reducing bit inconsistencies.

## III. Experimental Setup

### A. Devices Under Test: Microchip Serial SRAM

A total of sixteen Microchip 23K256 256 kbit serial SRAM memories were tested in this study. Fourteen chips were newly delidded and previously untested before the start of this study. The memory array was installed on a custom PCB where a Texas Instruments MSP430 microcontroller interfaced with the memories via SPI protocol and communicated the results to a central computer. The SRAM $V_{DD}$ was adjustable through an Analog Devices AD5235 10-bit digital potentiometer, and precision was verified by the MSP430's onboard 10-bit analog-to-digital converter.

### B. TID Radiation

Three separate radiation tests using varying methods and sources were carried out as a part of this study. One test was performed at Vanderbilt University in Nashville, TN, with an Aracor 4100 producing 10 keV x-rays. The supply current ranged from 10 to 30 mA during the test to vary the dose rate. The other two tests were performed at Provision CARES Proton Therapy Center in Knoxville, TN, with a medical proton cyclotron with particle energy ranging from 60 to 65 MeV and flux ranging from $10^7$ to $10^8$ particles/cm$^2$/s. Annealing, the heat-driven process by which semiconductors gradually recover from TID-induced degradation [11], [12], was monitored at room temperature after the x-ray tests by re-sampling the PUFs after 1, 3, and 24 hours.

TABLE I
Details on Beam Parameters and Bias Conditions for each Device Under Test (DUT) Group

| Group | Radiation Source | Dose Rate | Supply Voltage |
|---|---|---|---|
| A | 10 keV x-rays | 30 krad/min | $V_{DR}$ |
| B | 10 keV x-rays | 10 krad/min | $GND$ |
| C | 60 MeV protons | $10^8$ p/cm$^2$/s | $V_{DR}$ |
| D | 65 MeV protons | $10^7$ p/cm$^2$/s | $V_{DR}$ |
| E | 10 keV x-rays | 10 krad/min | $V_{NOM}$ |

Five groups of DUTs were tested with different bias conditions. In Table I, x-ray dose rates are given in units of krad($SiO_2$) per minute, while proton dose rates are provided in units of flux. Group A was tested with x-rays and consisted of five DUTs that were biased at 0.6V (the maximum identified $V_{DR}$) and were loaded with a checkerboard pattern during dosing. Group B was also tested with x-rays and consisted of five DUTs biased at 0V (all pins grounded) during dosing. Groups A and B were also sampled after annealing for 1, 3, and 24 hours (the DUTs were held at nominal $V_{DD}$ and room temperature for annealing). Groups C was tested with 60 MeV protons and consisted of nine DUTs biased at 0.6V during irradiation. Group D was tested with 65 MeV protons and consisted of seven DUTs biased at 0.6V during irradiation. Finally, group E was tested with x-rays and consisted of three DUTs that were biased at nominal $V_{DD}$ during dosing. For group E, current consumption was recorded during read, write, and idle operations. Also, with group E, PUF samples were obtained using a 2-second power-up ramp to reduce the effects of noise.

During both proton tests (groups C and D), DUTs were biased at the maximum cell $V_{DR}$ to increase single event upset (SEU) sensitivity as part of another study. These conditions were mimicked by group A in the x-ray test, and different results were witnessed due to the difference in energy deposition rates between x-ray and proton sources [12]. All DUTs in this study were delidded before irradiation. Group E consisted of three new non-irradiated memories, while all the other groups were a mixture of non-irradiated and previously irradiated memories. That being said, the first DUT in each group (*e.g.*, A1, B1) was a new, non-irradiated memory, and the effects of any previous tests had annealed completely before any DUTs were reused.

PUF characterization of the SRAMs was conducted by performing 100 reboot/read cycles for groups A through D and 10 reboot/read cycles for group E, according to the test flow in Fig. 8. The bias for $V_{DD}$ was 0.6V for groups A, C, and D (determined by the maximum $V_{DR}$), 0V (all pins grounded) for group B, and 3.3V ($V_{NOM}$) for group E. For all groups, pre-radiation characterization was performed at room temperature in the beam chamber at the test facility before turning on the beam. The characterization process took approximately 5 minutes, and during this time, some annealing of the effects of TID occurred. The observed quick anneal resulted in apparent dose rate effects. The decreased number of reboot/read cycles for group E was an effort to minimize this phenomenon. An evaluation of non-ionizing energy loss (NIEL) informed by [30] assured that the effects of displacement damage (DD) during the proton tests were negligible.

### C. Measuring TID-induced Changes in DUTs

The three basic measures of SRAM PUFs used in this study are Fractional Hamming Weight (FHW), intra-, and inter-die Fractional Hamming Distance (FHD). First, FHW was

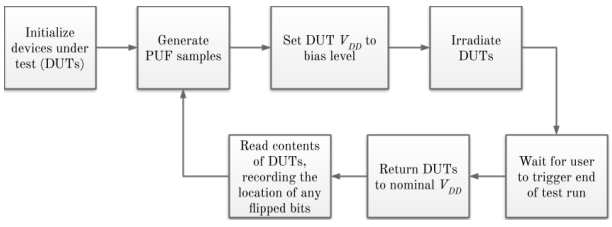



Fig. 8. The test procedure used in this study is outlined by the above block diagram. Some minor changes to the procedure depend on the DUT group. See Table I for details.

TABLE II
TID-INDUCED SHIFTS IN FHW AND FHD PER KRAD($SiO_2$) FOR EACH DUT GROUP

| Group | Last Reponsive TID Level | ΔFHW per krad($SiO_2$) $\Delta\mu$ | $\Delta\sigma$ | $\Delta FHD_{intra}$ per krad($SiO_2$) $\Delta\mu$ | $\Delta\sigma$ | $\Delta FHD_{inter}$ per krad($SiO_2$) $\Delta\mu$ | $\Delta\sigma$ |
|---|---|---|---|---|---|---|---|
| A* | 75 krad($SiO_2$) | $-3.67 \times 10^{-4}$ | $2.22 \times 10^{-5}$ | $1.54 \times 10^{-3}$ | $1.61 \times 10^{-3}$ | $2.99 \times 10^{-4}$ | $5.04 \times 10^{-3}$ |
| B* | 150 krad($SiO_2$) | $-9.92 \times 10^{-5}$ | $7.52 \times 10^{-6}$ | $9.68 \times 10^{-5}$ | $6.95 \times 10^{-6}$ | $3.41 \times 10^{-5}$ | $2.22 \times 10^{-5}$ |
| C† | 106 krad($SiO_2$) | $-1.02 \times 10^{-4}$ | $-3.39 \times 10^{-6}$ | $2.87 \times 10^{-4}$ | $-2.18 \times 10^{-6}$ | $6.04 \times 10^{-5}$ | $5.13 \times 10^{-6}$ |
| D‡ | 35 krad($SiO_2$) | $-2.92 \times 10^{-4}$ | $-3.58 \times 10^{-6}$ | $1.22 \times 10^{-3}$ | $4.92 \times 10^{-6}$ | $-3.17 \times 10^{-4}$ | $1.71 \times 10^{-5}$ |
| E* | 40 krad($SiO_2$) | $-1.26 \times 10^{-3}$ | $6.24 \times 10^{-5}$ | $2.87 \times 10^{-3}$ | $1.52 \times 10^{-5}$ | $6.25 \times 10^{-4}$ | $5.14 \times 10^{-4}$ |

* Dosed with 10 keV x-rays.
† Dosed with 60 MeV protons.
‡ Dosed with 65 MeV protons.

calculated from PUF samples by computing the sum of the pattern (where logic high equals 1 and logic low equals 0) normalized by the key length. Thus, the FHW is equivalent to the percent of the PUF represented by logic high (digital 1). This computation was completed by applying equation (1) to dosed samples from the DUT in question (*e.g.*, A1) and applying a key length of $L = 256$ bits, resulting in (4).

$$\mathrm{FHW}(A1) = \frac{\sum_{i=0}^{256} A1[i]}{256} \tag{4}$$

Next, the intra-die FHD was computed by performing a bitwise XOR operation between the PUF of an irradiated DUT and a randomly selected PUF sample from the same DUT before irradiation, then normalizing by the key length. This was accomplished by using equation (2) to compare a sample from the dosed DUT in question (*e.g.*, $A1_1$) to a pre-irradiation sample from the same DUT (*e.g.*, $A1_2$), resulting in (5).

$$\mathrm{FHD}_{intra}(A1_1, A1_2) = \frac{\sum_{i=0}^{256} A1_1[i] \oplus A1_2[i]}{256} \tag{5}$$

Lastly, the inter-die FHD was computed by performing a bitwise XOR operation between the PUF of an irradiated DUT and a randomly selected pre-irradiation PUF sample from a different DUT from the same group, then normalizing by the key length. This was accomplished by using equation (2) to compare a sample from the dosed DUT in question (*i.e.*, A1) to a pre-irradiation sample from another randomly selected DUT from the same group (denoted as Ax to represent a random selection among A2, A3, A4, etc.), resulting in (6).

$$\mathrm{FHD}_{inter}(A1, Ax) = \frac{\sum_{i=0}^{256} A1[i] \oplus Ax[i]}{256} \tag{6}$$

## IV. RESULTS

Table II provides a summary of the test results for each DUT group, where TID-induced shifts in the group average ($\mu$) and group standard deviation ($\sigma$) of the FHW and FHD per krad($SiO_2$) are indicated. Since every device failure occurred at a different TID point and the groups were dosed to different levels, the data is represented as the measured shift per unit dose (in krad($SiO_2$)). A negative number indicates that the value decreased with dose, while a positive shift indicates an increase. The final average shift for a group can be found by multiplying the average shift per dose by the maximum dose point relative to that group. As the DUTs were dosed, degradation largely depended on the applied bias conditions. The groups were dosed until they failed, although the groups tested with protons (C and D) did not fail due to simultaneous annealing. The average overall shifts were negative for FHW, positive for intra-die FHD, and mixed for inter-die FHD. The most significant relative shifts were seen in intra-die FHD because the absolute values were much smaller compared to FHW and inter-die FHD. Standard deviations mostly increased with dose, indicating that there was significant part-to-part variation.

### A. TID-induced Shifts in FHW

Figs. 9 and 10 illustrate the TID-induced degradation and the subsequent annealing of the FHW of groups B and A, respectively. As the DUTs were dosed, negative shifts in FHW were observed under all of the various test conditions. In the cases where the SRAMs held data during dosing (that is, all groups except B), this shift was non-monotonic; sometimes, the average FHW would rise before it fell. Such was the case with A1 and A4, for example (see Fig. 9).

On the other hand, group B, which was biased with all pins grounded during dosing, saw a more consistent monotonic

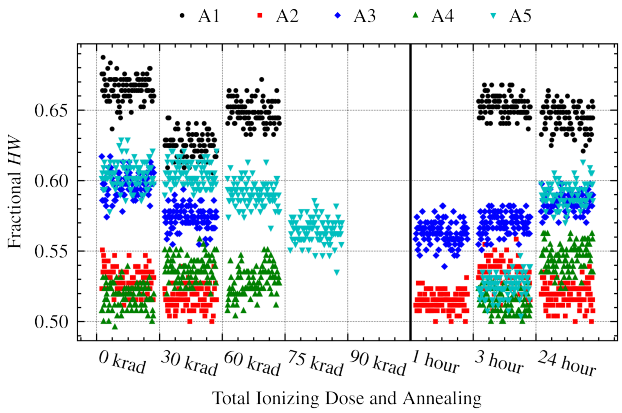



Fig. 9. TID-induced degradation and following anneal of the normalized FHW of group A. These DUTs were powered up and holding checkerboard data during dosing. This resulted in non-monotonic shifts to FHW due to artificial aging and TID-induced burn-in. After 24 hours of annealing at room temperature, all DUTs were functional but displayed a shifted average FHW compared to pre-irradiation. For all DUTs except A5, the average FHW was lower after recovery. This could be due to permanent or semi-permanent degradation of NMOS gates.

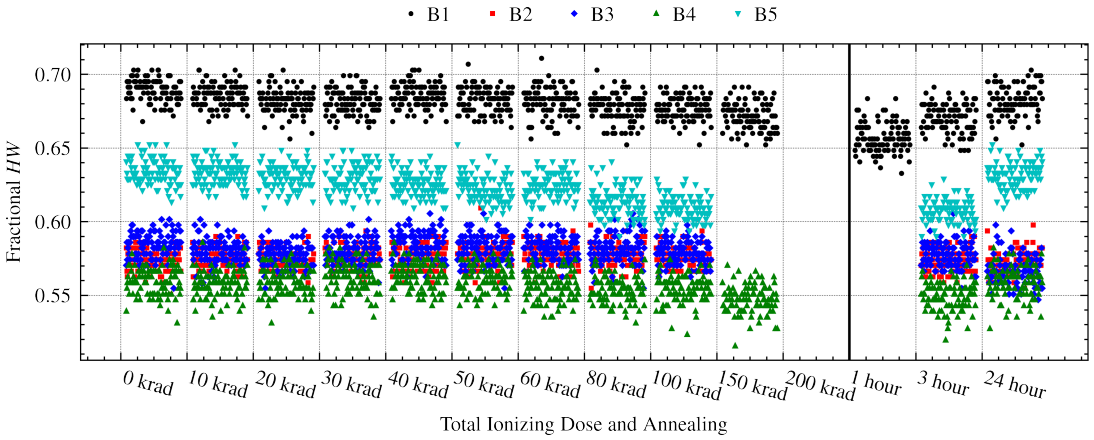



Fig. 10. TID-induced degradation and following anneal of the normalized FHW of group B. All DUT pins were grounded during irradiation, and therefore no data was burned into the SRAM cells. Characterization after each dosing run took about 5 minutes, and rapid annealing occurred during this time. Still, negative shifts to FHW were witnessed until the devices failed at 150-200 krad($SiO_2$). After annealing at room temperature for 24 hours, all the DUTs recovered to approximately the same average FHW, except for B3, which was slightly lower.

decrease of FHW with dose (see Fig. 10). A reduction in FHW reflects a shift of inconsistent cells towards logic low, potentially resulting from the weakening of NMOS gates at a higher rate relative to their PMOS counterparts. The change in the relative inconsistency of PUF samples (in other words, the shift in percent of inconsistent bits) was negligible for all groups, indicating that very few if any, consistent cells became inconsistent after irradiation. In other words, the shifts in average FHW were likely due to migration of the bistable cells (those with closely matched inverters) towards logic low. The more chaotic changes seen in the average FHW of the DUT groups, which held data during dosing, likely reflect the effects of TID-induced artificial aging. The resulting burn-in of the checkerboard data pattern produced an inverted image on the PUF via leakage current pathways burned into the transistors by radiation in a manner somewhat similar to BTI.

The devices were dosed until they failed for the DUT groups tested with x-rays (A, B, and E). For groups A, B, and E, failure occurred between 60 and 90 krad($SiO_2$), 150 and 200 krad($SiO_2$), and 40 and 60 krad($SiO_2$), respectively. In all cases, the devices recovered quickly enough that they were responsive again after 24 hours. In addition, a slightly lower average FHW was observed in most of the recovered devices, potentially due to permanent or semi-permanent damage to the NMOS devices. The devices never failed for the DUT groups tested with protons (C and D) due to the relatively low dose rate and simultaneous annealing.

### *B. TID-induced Shifts in Intra- and Inter-Die FHD*

Degradation of both intra- and inter-die FHD depends strongly on the voltage supplied to the SRAM during irradiation. Figs. 11 and 12 illustrate the TID-induced degradation and the subsequent annealing of the FHD of groups B and A, respectively. In the cases where the DUTs were biased on and held data during dosing, some erratic shifts in both intra- and inter-die FHD were observed (see Fig. 11). However, with group B, in which the DUTs were grounded during dosing, the shifts in both types of FHD were negligible, even after device failure (see Fig. 12). Interestingly, SRAM PUF authentication based on intra-die FHD was more resilient than the memories themselves since the PUF could still be read even after the sensitive control circuitry for write operations had failed.

It is possible that the checkerboard data stored in the memories during the irradiation of groups A, C, D, and E played a role in the chaotic nature of the intra-die FHD. Since in these cases, half of the cells held digital 0 and the other half had digital 1, the biasing of the PMOS and NMOS devices was inconsistent from cell-to-cell and followed a pattern that was completely independent of the device's PUF. In general, the tested SRAMs saw small positive shifts to the intra-die FHD and only minor changes to the inter-die FHD. This result relieves concerns about false-positive authentication results

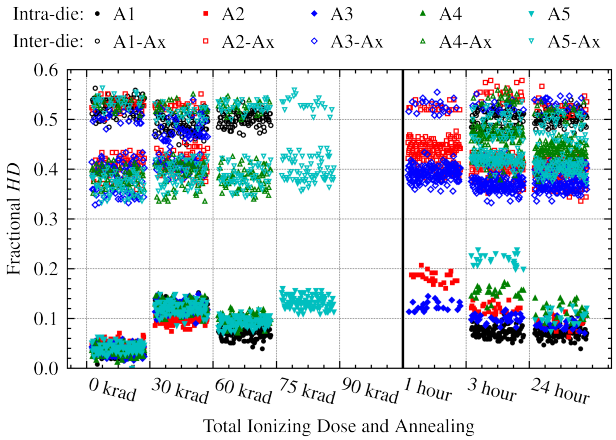



Fig. 11. TID-induced degradation and following anneal of the normalized intra- and inter-die FHD of group A. As with FHW, non-monotonic shifts in intra- and inter-die FHD due to the DUTs were powered up during dosing. Intra-die FHD shifts were mostly positive, hindering discernability. Inter-die FHD shifts were negligible. All five DUTs eventually failed by 90 krad($SiO_2$), and after 24 hours of annealing at room temperature they were all responsive again – but with higher average intra-die FHD.

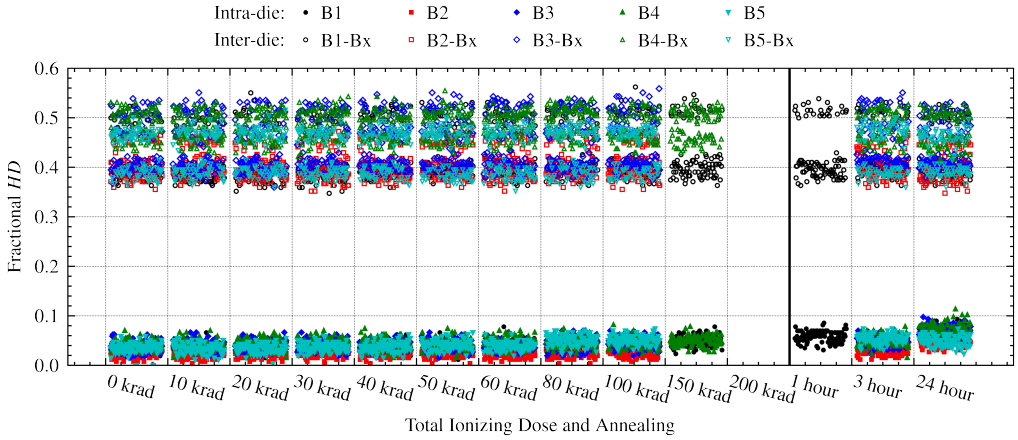



Fig. 12. TID-induced degradation and following anneal of the normalized intra- and inter-die FHD of group B. Since they were given more time to anneal between x-ray dosing runs, group B lasted to a higher apparent TID than group A, with all DUT eventually failing by 200 krad($SiO_2$). Minor shifts were observed in both intra- and inter-die FHD. Since all pins were grounded during dosing, there was no TID-induced burn-in, leading to more overall consistency in FHD comparisons within a die and between dies. All five DUTs recovered after 24 hours of annealing at room temperature, although there were slight positive shifts to intra-die FHD of the recovered DUTs.

using an FHD rejection threshold method for authenticating devices at high doses. On the other hand, major positive shifts to the intra-die FHD could result in false-negative authentication outcomes.

### C. Effects of TID on PUF Authentication

The positive shifts in intra-die FHD with dose pose a moderate threat to SRAM PUF authentication based on FHD rejection thresholds. A threshold set too low could eventually result in false-negative outcomes after significant TID degradation. The SRAMs tested in this study never strayed over the rejection threshold of $L/4$ (normalized to 0.25). However, this is twice as high as the threshold of $L/8$, which was reliable before x-ray exposure. A rejection threshold that is too high risks false-positive outcomes, although no significant negative shifts to inter-die FHD were observed due to TID.

After annealing for 24 hours at room temperature, the DUTs did not fully recover to their original intra-die FHD, but a value slightly higher. It is unknown whether re-exposure would add to this effect and gradually make an SRAM PUF unrecognizable based on PUF samples before exposure. The positive shift to intra-die FHD after annealing may be a symptom of TID-induced artificial aging.

### D. Effects of TID on Reliable Key Generation using TMV

The use of averaged PUF samples through TMV was evaluated at each dose level. Degradation in the ability of TMV to reduce variation-generated encryption keys was negligible. However, applying TMV did not reduce the TID-induced shifts in average FHW (Fig. 13) or intra- or inter-die FHD (Fig. 14). The inter-die FHD of one-on-one TMV key comparisons are separated into distinct strata, with each different combination of DUTs (A1 vs. A2, A1 vs. A3, etc.) falling in an easily discernible line. The average FHD from the different combinations experience chaotic shifts because the TID-induced shifts within both devices impact inter-die FHD measurements. TID

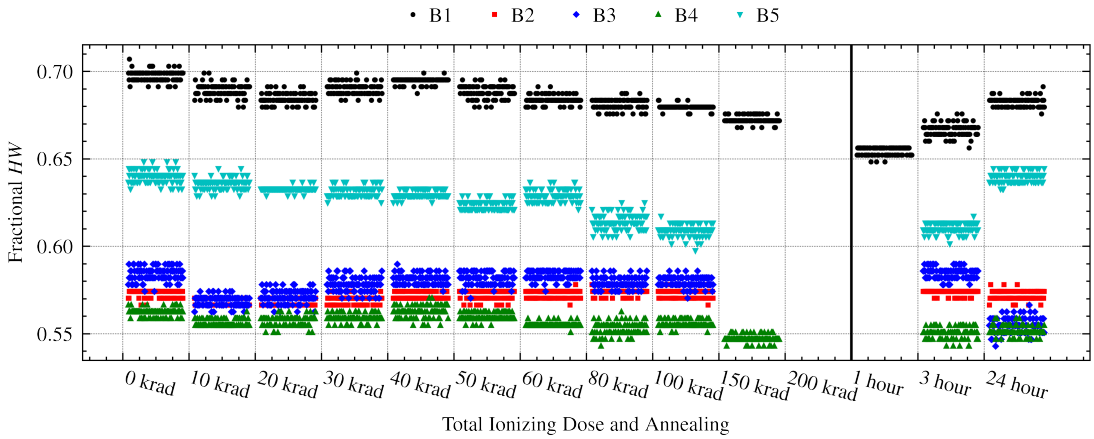



Fig. 13. TID-induced degradation and following anneal of the FHW of TMV-generated keys ($N_T = 99$) for group B. TMV key generation is not adversely affected by TID, although the resulting distributions are more narrow. TMV is unable to mitigate the TID-induced shifts FHW.

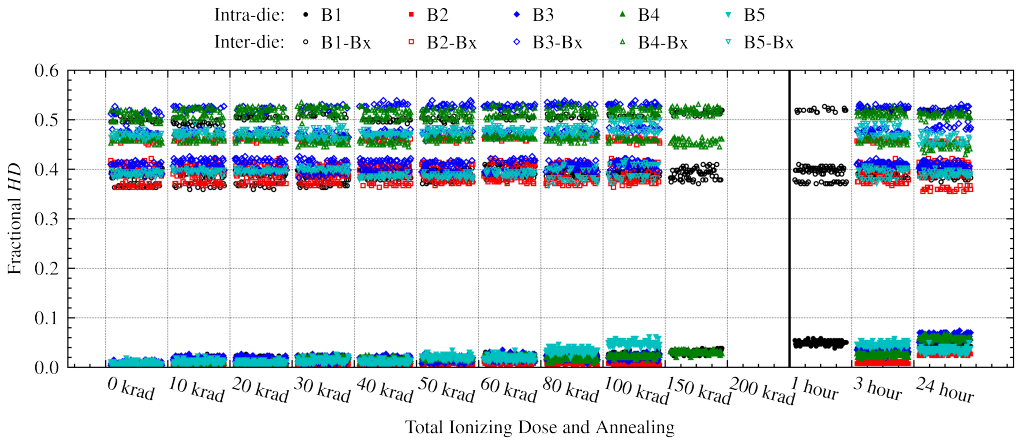



Fig. 14. TID-induced degradation and following anneal of the intra- and inter-die FHD of TMV-generated keys ($N_T = 99$) for group B. TMV key generation is not affected by TID, though the resulting distributions are more narrow. Like with FHW, TMV is unable to mitigate the TID-induced shifts FHD.

appears to influence the average values of both the FHW and FHD but does appear to influence the variance. Thus, TMV is ineffective in mitigating the TID-induced shifts in either intra- or inter-die FHD. Instead, mitigation efforts should be directed towards biasing the memory so that BTI stress and the artificial aging effect of TID do not greatly alter the PUF over time. There is the potential of using artificial aging to increase the reliability of PUF key generation techniques [25]–[27].

## V. Conclusion

In this study, the TID-induced degradation of SRAM PUFs has been presented in terms of the cyber-security measures of FHW, intra-die FHD, and inter-die FHD. 10 keV x-rays and 60-65 MeV protons were used as radiation sources on several DUT bias conditions. During dosing, DUTs that were powered on during irradiation experienced the most significant degradation, while the DUTs that were powered off experienced minor shifts to the observed measures.

In all cases, negative shifts to FHW reflected a change in PUF code composition towards slightly more digital zeros and fewer ones. This result is due to a higher rate of degradation in NMOS devices compared to their PMOS counterparts. The shifts were non-monotonic in all bias conditions, but the DUTs which were powered on during dosing saw more extreme and chaotic changes.

Intra-die FHD saw monotonic positive shifts induced by TID, indicating a more significant number of mismatched bits when comparing irradiated and non-irradiated samples from the same device. This result follows expectations according to TID-induced artificial aging. While effective in producing a more consistent PUF, TMV was unable to mitigate the degradation induced by TID. Inter-die FHD did not change significantly due to TID, indicating that SRAM PUF uniqueness is not compromised by TID degradation.

## References

[1] H. Handschuh, "Hardware-Anchored Security Based on SRAM PUFs, Part 1," *IEEE Security Privacy*, vol. 10, no. 3, pp. 80–83, 2012.

[2] A. Alheyasat, G. Torrens, S. Bota, and B. Alorda, "Weak and Strong SRAM Cells Analysis in Embedded Memories for PUF Applications," *IEEE Conference on Design of Circuits and Integrated Systems*, vol. XXXIV, pp. 63–68, Nov 2019.

[3] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical Unclonable Functions and Applications: A Tutorial," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1126–1141, 2014.

[4] J. M. Cannon, T. D. Loveless, R. Estrada, R. Boggs, S. P. Lawrence, G. Santos, M. W. McCurdy, A. L. Sternberg, D. R. Reising, T. Finzell, and A. Cannon, "Electrical Measurement of Cell-to-Cell Variation of Critical Charge in SRAM and Sensitivity to Single-Event Upsets by Low-Energy Protons," *IEEE Trans. Nucl. Sci.*, vol. 68, no. 5, pp. 815–822, 2021.

[5] D. Kobayashi, N. Hayashi, K. Hirose, Y. Kakehashi, O. Kawasaki, T. Makino, T. Ohshima, D. Matsuura, Y. Mori, M. Kusano, T. Narita, S. Ishii, and K. Masukawa, "Process Variation Aware Analysis of SRAM SEU Cross Sections Using Data Retention Voltage," *IEEE Trans. Nucl. Sci.*, vol. 66, no. 1, pp. 155–162, 2019.

[6] M. Alioto, G. Palumbo, and M. Pennisi, "Understanding the Effect of Process Variations on the Delay of Static and Domino Logic," *IEEE Trans. VLSI Syst.*, vol. 18, no. 5, pp. 697–710, 2010.

[7] J. Wang, S. Nalam, Z. Qi, R. W. Mann, M. Stan, and B. H. Calhoun, "Improving SRAM Vmin and yield by using variation-aware BTI stress," in *IEEE Custom Integrated Circuits Conference*, 2010, pp. 5–8.

[8] J. Guajardo, S. Kumar, G. Schrijen, and P. Tuyls, "FPGA Intrinsic PUFs and Their Use for IP Protection," *Information and System Security Group*, 2007.

[9] A. R. Korenda, F. Afghah, B. Cambou, and C. Philabaum, "A Proof of Concept SRAM-based Physically Unclonable Function (PUF) Key Generation Mechanism for IoT Devices," in *IEEE International Conference on Sensing, Communication, and Networking*, 2019, pp. 18–25.

[10] Z. He, W. Chen, L. Zhang, G. Chi, Q. Gao, and L. Harn, "A Highly Reliable Arbiter PUF With Improved Uniqueness in FPGA Implementation Using Bit-Self-Test," *IEEE Access*, vol. 8, pp. 181 751–181 762, 2020.

[11] T. Oldham, "Basic Mechanisms of TID and DDD Response in MOS and Bipolar Microelectronics," 2012.

[12] H. J. Barnaby, "Total-Ionizing-Dose Effects in Modern CMOS Technologies," *IEEE Trans. Nucl. Sci.*, vol. 53, no. 6, pp. 3103–3121, 2006.

[13] I. Sanchez Esqueda, H. J. Barnaby, and M. P. King, "Compact Modeling of Total Ionizing Dose and Aging Effects in MOS Technologies," *IEEE Trans. Nucl. Sci.*, vol. 62, no. 4, pp. 1501–1515, 2015.

[14] W. Che, F. Saqib, and J. Plusquellic, "PUF-based authentication," in *IEEE/ACM International Conference on Computer-Aided Design*, 2015, pp. 337–344.

[15] H. Martin, P. Martin-Holgado, Y. Morilla, and L. E. and, "Total Ionizing Dose Effects on a Delay-Based Physical Unclonable Function Implemented in FPGAs," *MDPI Electronics*, vol. 7, no. 163, Aug 2018.

[16] P. F. Wang, E. X. Zhang, K. H. Chuang, W. Liao, H. Gong, P. Wang, C. N. Arutt, K. Ni, M. W. Mccurdy, I. Verbauwhede, E. Bury, D. Linten, D. M. Fleetwood, R. D. Schrimpf, and R. A. Reed, "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, 2018.

[17] R. Maes, P. Tuyls, and I. Verbauwhede, "Intrinsic PUFs from flip-flops on reconfigurable devices," Jan. 2008.
[18] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data," *SIAM Journal on Computing*, vol. 38, no. 1, pp. 97–139, January 2008.
[19] M. Hiller, M.-D. Yu, and G. Sigl, "Cherry-Picking Reliable PUF Bits With Differential Sequence Coding," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 9, pp. 2065–2076, 2016.
[20] S. Vadhan, *Pseudorandomness*, Jan. 2012.
[21] K. Takeuchi, T. Mizutani, T. Saraya, M. Kobayashi, T. Hiramoto, and H. Shinohara, "Measurement of SRAM power-up state for PUF applications using an addressable SRAM cell array test structure," in *International Conference on Microelectronic Test Structures*, 2016, pp. 130–134.
[22] H. Shinohara, B. Zheng, Y. Piao, B. Liu, and S. Liu, "Analysis and reduction of SRAM PUF Bit Error Rate," in *International Symposium on VLSI Design, Automation and Test*, 2017, pp. 170–173.
[23] S. Kumar, K. Kim, and S. Sapatnekar, "Impact of NBTI on SRAM read stability and design for reliability," in *International Symposium on Quality Electronic Design*, 2006, pp. 210–218.
[24] R. Wang, G. Selimis, R. Maes, and S. Goossens, "Long-term Continuous Assessment of SRAM PUF and Source of Random Numbers," in *Design, Automation, and Test in Europe Conference and Exhibition*, 2020, pp. 7–12.
[25] A. Roelke and M. R. Stan, "Controlling the Reliability of SRAM PUFs With Directed NBTI Aging and Recovery," *IEEE Trans. VLSI Syst.*, vol. 26, no. 10, pp. 2016–2026, 2018.
[26] A. Garg and T. T. Kim, "Design of SRAM PUF with improved uniformity and reliability utilizing device aging effect," in *IEEE International Symposium on Circuits and Systems*, 2014, pp. 1941–1944.
[27] M. N. Islam, V. C. Patil, and S. Kundu, "A guide to graceful aging: How not to overindulge in post-silicon burn-in for enhancing reliability of weak PUF," in *IEEE International Symposium on Circuits and Systems*, 2017, pp. 2367–2370.
[28] R. Pease, "Total-Dose Issues for Microelectronics in Space Systems," *IEEE Trans. Nucl. Sci.*, vol. 43, no. 2, pp. 442–452, 1996.
[29] D. M. Fleetwood and P. V. Dressendorfer, "A simple method to identify radiation and annealing biases that lead to worst-case cmos static ram postirradiation response," *IEEE Trans. Nucl. Sci.*, vol. 34, no. 6, pp. 1408–1413, 1987.
[30] J. R. Schwank, P. E. Dodd, M. R. Shaneyfelt, J. A. Felix, G. L. Hash, V. Ferlet-Cavrois, P. Paillet, J. Baggio, P. Tangyunyong, and E. Blackmore, "Issues for Single-Event Proton Testing of SRAMs," *IEEE Trans. Nucl. Sci.*, vol. 51, no. 6, pp. 3692 – 3700, Dec 2004.