X-ray Radiation Effects on SRAM-based TRNG and PUF

Martin Holec[1][a], Jan Bělohoubek[2,3][b], Pavel Rous[3][c], Tomáš Pokorný[3][d],
Róbert Lórencz[2][e], František Steiner[3][f]

[1]*Faculty of Nuclear Sciences and Physical Engineering,*
Czech Technical University in Prague, Czech Republic
[2]*Faculty of Information Technology, Czech Technical University in Prague, Czech Republic*
[3]*Faculty of Electrical Engineering, University of West Bohemia in Pilsen, Czech Republic*
holecma9@fjfi.cvut.cz, {jan.belohoubek, robert.lorencz}@fit.cvut.cz,
{belohoub, rousp, pokornyt, steiner}@fel.zcu.cz

Abstract: The security primitives, such as *True-Random-Number-Generator* (TRNG) or *Physically-Unclonable-Function* (PUF), are widely used in many cryptographic devices. Properties of these primitives affect the security, reliability, and longevity of the whole device. In this work, we evaluate the influence of the total ionizing X-ray dose on hardware structures underlying conventional SRAM-based security primitives – PUF and TRNG. In contrast with other works, we aim with conventional CMOS circuits, we employ lower total ionizing dose (TID) levels, and we also take annealing into account. We quantify the induced changes in SRAM cell entropy, provide a quality analysis of related physical effects, summarize potential effects on both security primitives. Besides analyzing the experimental data, we explain experimental data by comparison to the electrical-level (SPICE) model of SRAM cells taking X-ray-induced effects – flicker noise and threshold shift – into account. Our comparative analysis points to inconsistencies and deficiencies in related literature and provides a view into effects affecting observed entropy. The novelty of our work is in the comparative analysis of experimental data combined with low-level electrical model, which is the enabler of the qualitative analysis. Our results form the basis for future work.

1 INTRODUCTION

The security primitives, such as *True-Random-Number-Generator* (TRNG) or *Physically-Unclonable-Function* (PUF), are today widely used in many digital designs incorporating security features for the secret (random or unique) value generation (Garg and Kim, 2014), (Larimian et al., 2020). Conventional CMOS implementations of TRNG employ simple structures to extract entropy from the (i) noise-originated jitter, where ring-oscillator-based TRNG is a prominent example (Valtchanov et al., 2008). Another conventional entropy source (ii) employs metastability (Kinniment and Chester, 2002), (Wang et al., 2020). An example of a metastability-based entropy source is the SRAM-cell-based TRNG. Equal basic building blocks can be used to create *Physically-Unclonable-Function* (PUF) by extracting stable and device-unique secret numbers employing the manufacturing variability. Both PUF and TRNG typically employ the same or very similar basic building blocks. The TRNG source of randomness – (i) noise-originated jitter, or (ii) metastability – represents a source of the PUF output instability.

Security primitives such as PUF or TRNG might be implemented as a dedicated hardware block or on top of conventional hardware structures, such as SRAM blocks or RC oscillators (Clark et al., 2018), (Gebali and Mamun, 2022). The natural and often choice for implementation of both TRNG and PUF is the SRAM memory block (Mikhail Platonov and Lórencz, 2013),(Wang et al., 2020), (Holcomb

[a] https://orcid.org/0009-0003-8308-8852
[b] https://orcid.org/0000-0003-4312-9931
[c] https://orcid.org/0000-0002-0158-3602
[d] https://orcid.org/0000-0001-7810-2558
[e] https://orcid.org/0000-0001-5444-8511
[f] https://orcid.org/0000-0002-5702-7015

et al., 2009). One of advantages of the SRAM is, that it is available even in devices without dedicated TRNG/PUF blocks. Such dedicated security blocks could be added e.g. to constrained designs incorporating common SRAM-equipped microcontroller(s). Such blocks could be even added to many existing designs by means of software update only, when the target hardware allows control of (parts or whole) SRAM memory, which is quite common for microcontrollers implementing different low-power modes.

This paper does not analyze intra or inter-die statistical properties of an SRAM memory important for PUF or TRNG design, but it deals with the long-term reliability of the security primitive under ionizing radiation pointing on changes in the security primitive behavior triggered by the degradation of the underlying structures.

There are many other aging mechanisms involved in silicon degradation, which could cause the degradation of the security primitives employing them. The mainstream research is concentrated on conventional factors like temperature, over/undervoltage, electromigration etc. (Wang et al., 2020), (Zhang et al., 2017). Our research deals with ionizing radiation as a source of silicon degradation, a less-discovered phenomenon in the security area (Lawrence et al., 2022). In contrast to recently published works (Lawrence et al., 2022), we concentrate on lower *total ionizing dose* (TID) levels several orders of magnitude closer to real-world doses. To accelerate experimental data acquisition, employed dose levels are still about three orders of magnitude higher than common dose sources (United Nations Environment Programme, 2016) and two orders of magnitude higher than doses (normally) caused by conventional medical or inspection X-ray equipment. Typical TID levels in experiments with SRAM-based security primitives are above 100 Gy, we work with lower TID ranging from 10 Gy up to (about) 100 Gy, while received TID from medical and inspection devices or even natural background are typically much below 0.1 Gy.

The rest of the paper is structured as follows: Section 2 summarizes properties of SRAM-based security primitives, Section 3 briefly describes the silicon trap formation process, Section 4 describes our experimental setup, and presents results of our preliminary experiments, while the Section 5 analyses them, Section 6 concludes the paper and presents the main open questions and future work.
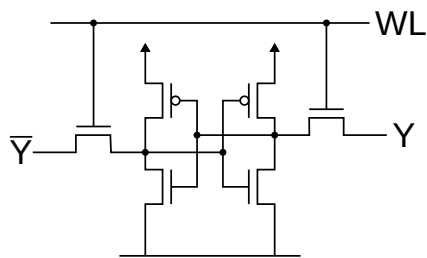

Figure 1: Symmetric structure of the conventional 6-T SRAM cell with complementary *input/output* ($\overline{Y}/Y$) is composed of two cross-coupled inverters and two access transistors controlled by a *word line* (*WL*) signal

2 SRAM-BASED SECURITY PRIMITIVES

The SRAM memory cell is appropriate for TRNG design, as it tends to provide uncertain output after power-up. The structure of the SRAM cell is typically well balanced and both inverters in the conventional 6-transistor cell – see Figure 1 – are designed to be (almost) matching. Such structure may be subject to the metastable behavior after power-up generating high entropy between (independent) power-ups. On the other hand, even a small mismatch caused by the manufacturing variability in the SRAM cell structure (Figure 1) could significantly decrease the cell value entropy between independent power-ups, as the mismatch effectively limits the metastability effect. Cells with a significant mismatch manifest higher stability. Compared to cells experiencing metastability, highly stable cells could be good PUF candidates, as they provide highly stable, while unpredictable and unique output given by the manufacturing variability.

The first step of the conventional approach to the design of SRAM-based PUF or TRNG is the characterization of the SRAM block used for security primitive design and identifying two sets of cells (S1) cells with low entropy – stable in logic 1 or logic 0, and (S2) cells with high entropy – unstable cells. These disjoint sets (with some margins) represent a set of cells appropriate for the construction of the device-specific security primitives PUF or TRNG respectively.

The long-term reliability of any such security primitives – both PUF and TRNG – depends on temporal changes in the structure of the underlying semiconductors (Garg and Kim, 2014), (Wang et al., 2020), (Zhang et al., 2017). The temporal changes may lead to both loss or increase in the entropy of any SRAM cell. In other words, cell characteristics could develop over time and cells could drift in/out of S1 and S2 sets over time causing issues for the security primitive. This is why the design of any such security

primitive involves a spatial redundancy to ensure stability (PUF) or high entropy (TRNG) over the whole device life (Wang et al., 2020), (Vijayakumar et al., 2017).

For the sake of simplicity, we formally define the following terms to be used throughout the paper to demonstrate S1 and S2 set migrations through the experiments:

- *PUF candidate (stable SRAM cell)* – the SRAM cell with at least 95 % probability of value one or the cell with at least 95 % probability of value zero after power-up, representing cells in the S1 set (low-entropy, stable cells),

- *TRNG candidate (unstable SRAM cell)* – the SRAM cell with 45 – 55 % probability of value zero (or one) after power-up representing cells in the S2 set (high-entropy, unstable cells).

- *healthy cells* – cells remaining in the same set (S1 or S2) from the beginning of the experiment (cells not drifting in/out of sets S1 and S2).

Any SRAM-based security primitive involves a significant redundancy to reduce the security primitive quality fluctuations in both the short- and long-term. The art of the SRAM-based security primitive design lies in the amount of redundancy to establish the trade-off between reliability, area utilization, power consumption, and the long-term reliability of the security primitive. This kind of decision should ideally be based on the technology-level characterization, profiling, and knowledge gained by accelerated aging and stressing experiments. On the other hand, this is not always possible, e.g. in the case, when a cryptographic feature, depending on PUF or TRNG, must be added to an existing design, where no dedicated and pre-characterized block is present, but an SRAM memory is available.

Our work aims to develop recommendations and reliability estimations to optimize design decisions concerning a realistic level of ionizing radiation stress of SRAM-based security primitives and enable quantitative modeling of TID influence on SRAM-based security primitives.

3 X-RAY-INDUCED SILICON TRAP FORMATION

When a silicon device is exposed to ionizing X-ray radiation, the *photoelectric* and the *Compton* effects dominate in the silicon lattice (Claeys and Simoen, 2002). The continuous X-ray spectra are broad – the photon energy varies from tens of eVs to keV. The result of the stochastic effects in the silicon lattice is the
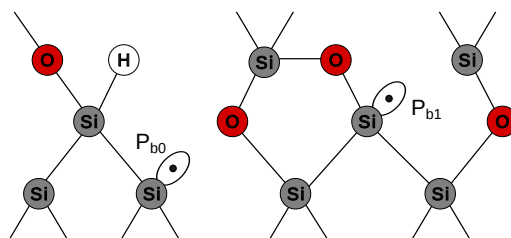

Figure 2: Si-SiO$_2$ interface includes irregularities like hydrogen bonds and dangling bonds: dangling bond defects located near the transistor channel area behave like charge traps. Novel traps emerge due to the absorbed ionizing radiation. The P$_{b0}$ type defect is formed by an unpaired valence electron of a silicon atom back-bonded to three silicon atoms, while the P$_{b1}$ type defect is connected with the silicon atom back-bonded to two other silicon atoms and an oxygen atom (Entner, 2007)

emerge of defects. The most notable defects affecting charge in the CMOS transistor channel are the silicon traps located near the Si/SiO$_2$-interface (Barnaby, 2006), (Entner, 2007). Traps emerging in the Si/SiO$_2$-interface layer – see dangling bond defects in Figure 2 – influence the device leakage and transistor transconductance (Tebina et al., 2023), but increase also the flicker noise level, and influence the transistor threshold voltage at the same time (Barnaby, 2006), (Kirton et al., 1989).

The lattice of the conventional semiconductor interface layer – see Figure 2 – is composed of Si and SiO$_2$ molecules. To ionize Si, energy about 4eV is needed, while for SiO$_2$ ionization, a slightly higher energy of 17eV is necessary (Barnaby, 2006).

An important process started by the ionizing radiation in the silicon lattice, due to the ionizing radiation exposure, is the *annealing* process. The annealing process involves trap migration in the electrical potential direction – to the interfaces (Batyrev et al., 2006). The annealing process could be accelerated by the increased temperature, while the room temperature is sufficient enough to allow it.

To be more specific about trap-formation scenarios, one of the real-world scenarios for the cryptographic device stress represents the (repeating) inspection of the personal electronics on X-ray detectors at airports, or medical X-ray scanners stressing electronic implants. An interesting, and potentially prospective case is also using ionizing radiation to compromise the cryptographic device through damage in the security primitive (Bouat et al., 2023).

The radiation load from the natural radiation background is on average 2.4 mGy/year (United Nations Environment Programme, 2016). During medical exposures, the patient is normally burdened with doses from 0.01 mGy to about 10 mGy, which corresponds

to exposure from the natural radiation background in the range from less than 1.5 days to 4.5 years.

4 EXPERIMENTAL EVALUATION

The experimental evaluation aims to quantify and explain the effects of a lower total ionizing dose (TID) on the PUF and TRNG security primitives based on SRAM. The emphasis is put on SRAM in common devices like microcontrollers. The microcontroller-SRAM-based primitives can be used in constrained applications or as an upgrade option in existing designs or even deployed products.

4.1 Experimental Setup

As an X-ray radiation source, we used a *computer tomography* (CT) device GE v|tome|x s with a 240kV micro-focus direct tube that emits a reflected signal off of a tungsten target to expose samples to the X-ray radiation. For the parameter settings, we used integrated basic SW with the timer settings option, that counts time after X-ray power is stabilized. The X-ray beam used is similar in its properties to the standardized RQT150 X-ray beam (International Electrotechnical Commission, 2005). Compared to the standardized RQT150 beam, less filtering was used – only the X-ray's own (basic) filtering to maintain the greatest possible spectrum without lower restrictions.

For our experiments, we used two types of samples: (i) simple samples, represented by discrete silicon-based transistors, and (ii) complex samples represented by conventional STM32 *microcontrollers* (MCUs) STM32L072CZ manufactured in the STMs' 130nm technology node. We used tens of simple samples and several complex samples for our initial experiments, while four of them remained operational after receiving a significant level of dose, and were used for gaining data.

The discrete transistors (BS170s and BS250) were only used for sensitivity analysis, while their technology-level similarity to complex samples is limited. By the sensitivity analysis, the characteristic energy (X-ray tube *acceleration voltage*) causing the rapid threshold voltage shift in simple samples was found. The final dose rate was ≈ 1.3 Gy/s.

Some of the obtained IV characteristics from simple sample measurements are reported in Figure 3 for illustration.

After performing the sensitivity analysis, we performed measurements on complex samples aimed at the stability of SRAM cells before and after irradiation. We applied several iterations utilizing the setup
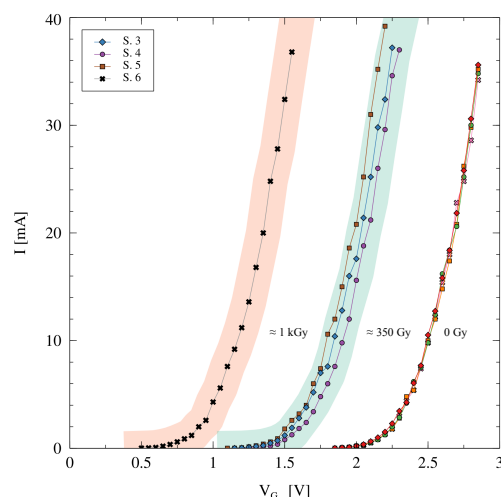

Figure 3: The shift in the initial IV characteristics and the shift of the threshold voltage for simple NMOS samples depends on the irradiation level. We used the X-ray dose rate of ≈ 0.5 Gy/s for 720 seconds for sample 03 (500 μA, 140 kV), and dose rate of ≈ 1.9 Gy/s for 180 seconds for samples 04 and 05 (2000 μA, 140 kV) resulting in TID of ≈ 350 Gy. The dose rate of ≈ 1.9 Gy/s for 540 seconds was used for sample 06 (2000 μA, 140 kV) resulting in TID of ≈ 1 kGy

learned during the sensitivity analysis. Each iteration involves 10 Gy total dose delivered to the sample within 7 seconds. The sample ionization was followed by a delay between iterations utilized for data acquisition process. The standard delay between iterations was below 24 hours. Longer relaxation pauses were inserted between specified iterations for the selected sample only to include the effect of the annealing process.

All complex samples were not powered during the irradiation, as experiments even with relatively low total doses led to the rapid destruction of samples.

Our goal was to identify the PUF/TRNG candidate cells – and track their (in)stability over the increasing total dose. To evaluate SRAM cell stability, we performed 1,000 independent SRAM power-offs followed by power-ons and SRAM cell value readouts in every experiment iteration.

Total doses above ≈ 100 Gy lead to MCU destruction in all cases for yet unknown reason. The device destruction is probably unrelated to studied SRAM cells implemented using relatively thin-dielectric (Barnaby, 2006), but it is probably caused by a TID-sensitive part of the MCU, as relatively low survival dose levels were reported for similar complex devices (Avery et al., 2011).

4.2 Simulation Setup

For simulations, we used the SPICE model of the 6-T SRAM cell (see Figure 1) in the Sky130 technology node (SkyWater PDK, 2023). This technology node is comparable to the technology node used for manufacturing complex samples, while the PDK is available to the public under no restrictions increasing the repeatability of the conducted research.
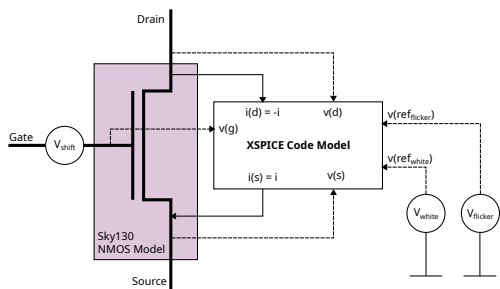

Figure 4: Employed simulation model for the transient noise simulation and threshold voltage shift in Ngspice: the Sky130 transistor model is extended by the custom XSPICE Code Model injecting the noise current in parallel to the transistor channel (solid lines); the XSPICE Code Model takes multiple references to inject noise with correct nature and amplitude (dashed lines): the transistor operating point, pre-generated random noise sequences (transient voltage sources), and noise RMS extracted from the transistor BSIM model for every operating point of the transistor

The simulation was conducted in *Ngspice* using standard SPICE primitives and the custom XSPICE extension code model – see Figure 4. The white and the flicker noise current sequence was generated and injected in parallel to the transistor channel of the MOS transistor, where the transistor model is the conventional industry-standard BSIM model.

The conventional SPICE voltage sources were used to generate the white and the flicker noise reference sequences respectively. The flicker noise sequence in Ngspice is generated by the algorithm presented in (Kasdin, 1995).

The white and flicker noise, injected by the XSPICE code model, for each simulation step, was derived from the mentioned reference voltage sources, and modulated by the noise RMS value specific for the current transistor operation point given by Drain/Gate/Source potential.

The noise RMS of the SKY130 transistors was extracted from the industry-standard BSIM model by employing the conventional small-signal noise analysis.

The complete setup was encapsulated into the Ngspice XSPICE extension. The final corner-case issue solution and verification of the XSPICE Code

Model is our current ongoing work directing to the Code Model publication.

The threshold shift was injected into the simulation model by inserting a voltage source in series to the transistor gate – see Figure 4.

The threshold shift considered in our simulations varied from 0 to 0.3V. The noise was varied by employing the noise RMS values between 1 and 3 multiples, while the character of the injected noise remained equal.

4.3 Experimental Results

Our results come from the irradiation by the relatively low total dose levels below ≈ 100 Gy, which is the safe limit we achieved, where complex samples remain operational.

Based on our experimental results, we confirmed (Garg and Kim, 2014), that the stability is a natural property of SRAM cells, indifferently on irradiation dose: effects like the mismatch, manufacturing variability, or threshold shift dominate significantly over the increased noise levels induced by irradiation. The share of highly stable cells – PUF candidate cells – remains over 80% indifferently on the irradiation dose – see Figure 5.
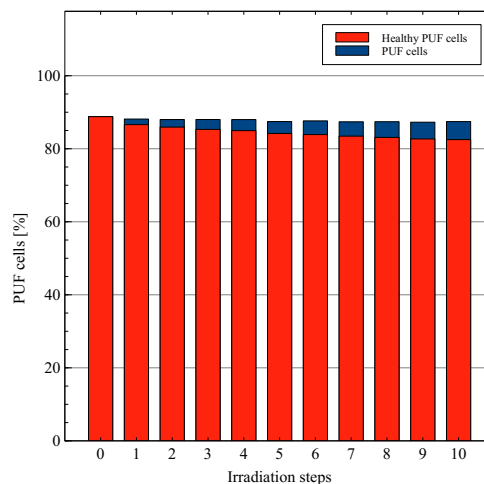
Figure 5: The number of PUF candidates among the SRAM cells on sample 04 (red) decreases slowly with increased TID, while the number of highly stable cells (current PUF candidates; red+blue) remains almost constant – independently on the received total dose

Based on a careful analysis of SRAM-cell stability data, cells being selected as highly stable cells during the initial SRAM memory characterization exhibit only a small increase of instability – up to 5% for all

samples – which is quite acceptable for any PUF design incorporating a sufficient level of redundancy.

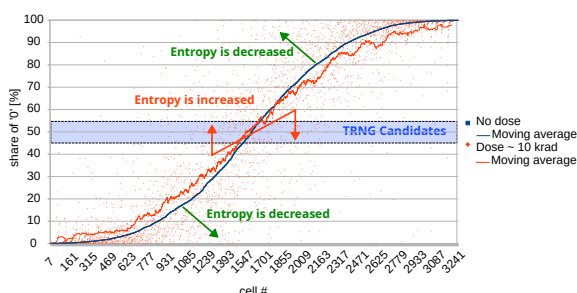Figure 6: 100 Gy X-ray ionization effects on SRAM cells on sample 03: cells were sorted according to the share of the value '0' for the cell power cycles prior to irradiation (blue square+solid line). The share of the value '0' for each cell after irradiation is shown (red diamonds), while the floating average for the irradiation-caused shift is denoted (red solid line) – slight increase in total entropy was observed for sample 03, a number of TRNG candidates remains comparable for 0 to 100 Gy TID, but number of TRNG candidates decreased significantly after irradiation

Under quantitative analysis, we observed two contradicting phenomenons: (i) the first significant phenomenon is, that many cells experience increased entropy, while (ii) the second phenomenon is the increased stability experienced by many cells as well. Both phenomenons were observed at the same time for dozens of cells under the equal total dose on the same sample – see Figure 6. These fighting phenomena lead interestingly to the increasing dominance of stable cells manifesting significant variability – most cells are/become strongly stable, low entropy, but their variability is not negligible at the same time. As a result, the total entropy computed over all SRAM cells in the sample may increase or decrease, but the change is negligible – no clear conclusion about the dominance of one or the other effect on the total sample entropy depending on the total dose could be made from our data, as the observed differences are too low and not consistent among all samples – the nature of induced total entropy changes over all SRAM cells is stochastic.

To interpret measurement results, we create SPICE models of SRAM cell (Figure 1) incorporating the dominating irradiation-induced effects: flicker noise and threshold shift in the SKY130 technology node. The transient simulations show, that increased noise increases the entropy produced by the unmatched cell after independent power-ups significantly only if there is no or only little threshold shift – compare Figures 9a and 9b, otherwise, threshold shift leading to decreased entropy dominates – see Figure 9c.

To conclude, the results of our analysis are as follows: (i) an increase in entropy (increased cell instability) is caused by increased flicker noise, while (ii) a decrease in entropy (increased cell stability) is caused by dominating shift in the threshold voltage.
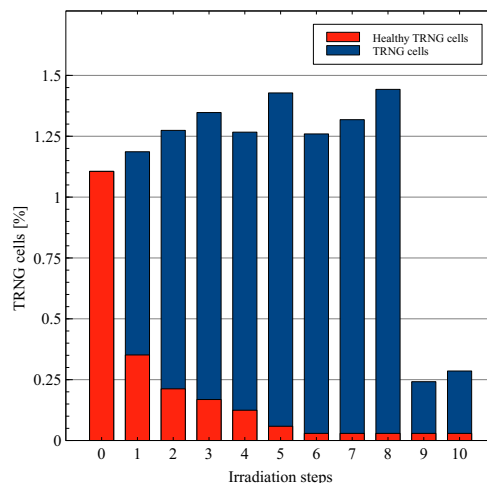

Figure 7: The number of TRNG candidates preserving the TRNG candidate properties among received TID (red) decreases with accumulated TID in sample 04, while the total share of TRNG candidate cells remains high for iterations 1 to 8 for sample 04 (red+blue)

Based on a careful analysis of SRAM-cell stability data, we found, that the conditional probability of entropy loss for cells identified as TRNG candidates during the initial SRAM memory characterization (prior irradiation) is surprisingly high. Almost all cells exhibiting the highest entropy prior irradiation (entropy > 0.993; share of zeroes 45% - 55%) experienced a significant entropy loss (more than 80% for all samples) – see Figure 7 for a decrease of initially-identified TRNG candidate cells share in the sample 04.
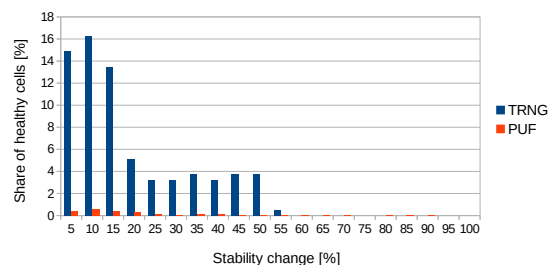

Figure 8: Stability shift of TRNG and PUF candidate cells in sample 04 after 10 Gy of the total dose (the first irradiation iteration)

The observed average entropy loss is surprisingly high – more than 0.1 bit (instability was decreased by $\pm 20\%$ in the average case) – see Figure 8. The initial set of TRNG candidate cells)healthy cells) almost vanishes after iteration 5 ($5 \cdot 10$ Gy) – see a decrease of initially-identified TRNG candidates in Figure 7 – while the total number of highly unstable cells (current TRNG candidates) remained relatively high (or even increased) for for all 10 iterations on most samples, and up to iteration 8 on sample 04. The drop after the iteration 8 for sample 04 is caused by the 15-day relaxation period inserted between iterations 8 and 9 to allow material annealing. All observed variations lead to a significant loss of entropy in the original set of TRNG candidates, and could significantly decrease the TRNG performance, while the annealing process itself caused rapid decrease of TRNG candidate cells available in the sample.

5 ANALYSIS

In this work, we performed irradiation experiments employing the available conventional X-ray source: the inspection CT device, comparable to widely used X-ray medical or baggage inspection sources. The results obtained using the conventional X-ray source are overall consistent with results reported for measurements on other ionizing radiation sources (Lawrence et al., 2022), (Surendranathan et al., 2023), (Zhang et al., 2020), but novel knowledge about cell stability development were gained, and inconsistencies and deficiencies were detected in recent works (Lawrence et al., 2022), (Surendranathan et al., 2023), (Zhang et al., 2020).

Effects of Annealing

We found, that annealing, which is omitted by current research of ionizing radiation effects on structures underlying the SRAM-based security primitives, has a significant effect and could not be omitted in any future research: our analysis provides a good starting point for further experiments. The observed effect is illustrated in Figure 7.

Flicker Noise vs. Threshold Shift

Despite the lower variability of samples and limited resources, we were able to provide a solid explanation of the observed changes in silicon due to the alignment of our results with theory and simulation results. The simulations explain the observed phenomenons in this way: the increased variability is a result of induced (flicker) noise caused by radiation-formed traps, while the increased stability is a result of the induced threshold voltage shift. These effects combine resulting in:

- a slight increase in instability for originally stable cells,
- a significant increase in stability for originally highly unstable cells.

As a result, these effects may cause a significant loss of entropy for SRAM-cell-based TRNG even for a relatively small total ionizing dose (TID), especially when combined with (natural) annealing over a reasonable period of time.

Related Research Results

Our results regarding cell stability, and the potential PUF reliability, in particular, are consistent with results reported in recent works (Lawrence et al., 2022), (Surendranathan et al., 2023), despite the referenced experiments aimed higher dose effects. PUF reliability should not be affected significantly by lower doses.

Authors of (Lawrence et al., 2022) and (Surendranathan et al., 2023) provide only poor or none security-perspective motivation, while conclusions and interpretations provided in (Lawrence et al., 2022) are in part incorrect, (1) as observed one-sided variations are too small, and (2) could not be explained by nMOS/pMOS differences as argued by authors, due to the symmetries of the considered CMOS cells. The results rather represent a stochastic mixture of fighting phenomenons (increased noise and threshold shifts) described in our paper.

Experimental Setup Properties and Limitations

Our experiments were designed to lower total doses than most of other reported experiments with silicon samples, however, they are still much higher than dose exposures from common X-ray sources. Despite this fact, X-ray irradiation is a process with a behavior of highly stochastic nature, thus behavior similar to behavior induced by higher doses could be observed on a random basis, and with low, but non-zero, probability in devices exposed to common dose levels as well. These effects can thus still influence the behavior of security primitives present in X-ray-exposed devices.

Effects on the PUF Security Primitive

The observed fighting phenomenons (increased noise and threshold shifts) leading to increasing dominance of stable cells manifesting significant variability at the
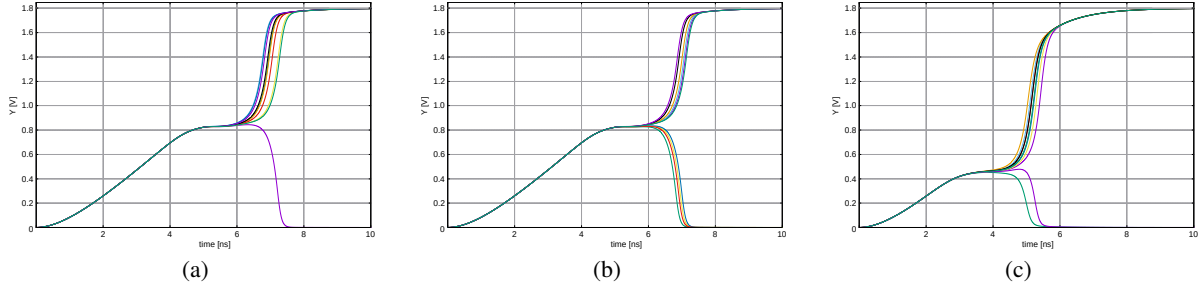
Figure 9: Simulation results for independent power-ups of the slightly unbalanced stable SRAM cell model: (a) under normal conditions, the majority of power-up states lead to logic 1 at the cell output; (b) when the noise level is increased, entropy is increased as a result; (c) under the significant threshold shift and increased noise, threshold shift effect dominates over increased noise, and the cell stability remains high

same time – could affect the long-term reliability of PUF in terms of repeatability of the output, but spatial redundancy methods should remain a successful measure in this case.

Effects on the TRNG Security Primitive

Our results related to the low ionization levels targeting metastability-based SRAM cell entropy sources are novel:

- in pointing on long-term quality limitations of SRAM-based TRNGs under ionizing radiation,

- in providing insight into wear-out mechanisms and their connection with loss or increase of entropy,

- in showing the severity of the annealing process on the SRAM cell stability.

Our results do not confirm (Zhang et al., 2020), where better TRNG properties were reported after low-dose irradiation, but do not strictly contradict them: temporary increase in number of TRNG candidate cells is possible – see Figure 7.

6 CONCLUSIONS

First, we pointed out the importance of the evaluation of the annealing process effects having a significant effect on SRAM cell stability, as it was not considered in past research (see Figure 7.). Based on our experimental data, the anealing process initiated by the ionizing radiation has higher effect on SRAM cell stability, than the immediate energy absorption effects.

We also pointed on misleading interpretations of results in related works (Lawrence et al., 2022), (Surendranathan et al., 2023) caused by incorrect in-

terpretations of a poor and false determinism in results affected by a mixture of stochastic effects, as discussed in Section 5. The mixture effect of the fighting phenomenons – increased flicker noise and threshold shift – is stochastic, and could be simply misinterpreted.

To summarize the security perspective: (i) PUF function is almost unaffected by lower X-ray doses (up to $\approx$ 100 Gy), but (ii) the TRNG function is endangered by this level of intensity of ionizing irradiation: the total number of high-entropy cells available in SRAM is decreased, and initially-unstable cells may become significantly stable.

Our results indicate, that irradiating an SRAM memory always decreases the number of the TRNG healthy cells with the highest entropy, despite the fact, that the average entropy computed over all SRAM cells might be increased due to fighting noise and threshold voltage shift phenomenons in all SRAM cells.

When implementing a SRAM-based TRNG, no simple measure can be applied to prevent the significant loss of entropy of SRAM cells, but the loss of entropy could be still detected by the (repeated) TRNG health test. Other options for potentially sensitive applications are: accepting the entropy loss and applying higher spatial redundancy and/or repeat SRAM profiling for unstable cell re-detection.

6.1 Future Work

Possible research directions include the quantification of TID and mainly irradiation-triggered annealing effects on the TRNG and PUF quality, modeling, development and validation of treatment methods (Tebina et al., 2023), (Oldham, 2004) or methods for protecting the security primitives from entropy fluctuations employable in-the-field.

Creating a simplified, statistical model of the entropy evolution for low to medium total ionization dose (TID) could bring a real benefit to circuit design.

ACKNOWLEDGMENTS

REFERENCES

Avery, K., Finchel, J., Mee, J., Kemp, W., Netzer, R., Elkins, D., Zufelt, B., and Alexander, D. (2011). Total Dose Test Results for CubeSat Electronics. In *2011 IEEE Radiation Effects Data Workshop*, pages 1–8. IEEE.

Barnaby, H. (2006). Total-Ionizing-Dose Effects in Modern CMOS Technologies. *IEEE transactions on nuclear science*, 53(6):3103–3121.

Batyrev, I. G., Rodgers, M. P., Fleetwood, D. M., Schrimpf, R. D., and Pantelides, S. T. (2006). Effects of Water on the Aging and Radiation Response of MOS Devices. *IEEE Transactions on Nuclear Science*, 53(6):3629–3635.

Bouat, S., Anceau, S., Maingault, L., Clediere, J., Salvo, L., and Tucoulou, R. (2023). X-ray Nanoprobe for Fault Attacks and Circuit Edits on 28-nm Integrated Circuits. In *2023 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, pages 1–6. IEEE Computer Society.

Claeys, C. and Simoen, E. (2002). *Radiation Effects in Advanced Semiconductor Materials and Devices*, volume 57 of *Springer Series in Materials Science*. Springer Berlin Heidelberg, Berlin, Heidelberg.

Clark, L. T., Medapuram, S. B., and Kadiyala, D. K. (2018). Sram circuits for true random number generation using intrinsic bit instability. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 26(10):2027–2037.

Entner, R. (2007). *Modeling and Simulation of Negative Bias Temperature Instability*. Ph.d. thesis, Technical University Wien.

Garg, A. and Kim, T. T. (2014). Design of SRAM PUF with improved uniformity and reliability utilizing device aging effect. In *2014 IEEE international symposium on circuits and systems (ISCAS)*, pages 1941–1944. IEEE.

Gebali, F. and Mamun, M. (2022). Review of physically unclonable functions (pufs): Structures, models, and algorithms. *Frontiers in Sensors*, 2.

Holcomb, D. E., Burleson, W. P., and Fu, K. (2009). Power-Up SRAM State as an Identifying Fingerprint and Source of True Random Numbers. *IEEE Transactions on Computers*, 58(9):1198–1210.

International Electrotechnical Commission (2005). Medical diagnostic X-ray equipment - Radiation conditions for use in the determination of characteristics. IEC 61267:2005, 2.0.

Kasdin, N. (1995). Discrete Simulation of Colored Noise and Stochastic Processes and $1/f^{\alpha}$ Power Law Noise Generation. *Proceedings of the IEEE*, 83(5):802–827.

Kinniment, D. and Chester, E. (2002). Design of an On-Chip Random Number Generator Using Metastability. In *Proceedings of the 28th European Solid-State Circuits Conference*, pages 595–598.

Kirton, M., Uren, M., Collins, S., Schulz, M., Karmann, A., and Scheffer, K. (1989). Individual Defects at the Si:SiO2 Interface. *Semiconductor science and technology*, 4(12):1116.

Larimian, S., Mahmoodi, M. R., and Strukov, D. B. (2020). Lightweight Integrated Design of PUF and TRNG Security Primitives Based on eFlash Memory in 55-nm CMOS. *IEEE Transactions on Electron Devices*, 67(4):1586–1592.

Lawrence, S., Smith, S., Cannon, J., Carpenter, J., Reising, D., and Loveless, T. (2022). Effects of Total Ionizing Dose on SRAM Physical Unclonable Functions. *IEEE Transactions on Nuclear Science*, 69(3):349–358.

Mikhail Platonov, J. H. and Lórencz, R. (2013). Using Power-Up SRAM State of Atmel ATmega1284P Microcontrollers as Physical Unclonable Function for Key Generation and Chip Identification. *Information Security Journal: A Global Perspective*, 22(5-6):244–250.

Oldham, T. R. (2004). Switching Oxide Traps. *International journal of High Speed Electronics and Systems*, 14(02):581–603.

SkyWater PDK (2020 – 2023). SkyWater SKY130 PDK's documentation.

Surendranathan, U., Wilson, H., Wasiolek, M., Hattar, K., Milenkovic, A., and Ray, B. (2023). Total Ionizing Dose Effects on the Power-Up State of Static Random-Access Memory. *IEEE Transactions on Nuclear Science*, 70(4):641–647.

Tebina, N.-E. O., Zergainoh, N.-E., Hubert, G., and Maistri, P. (2023). Simulation Methodology for Assessing X-Ray Effects on Digital Circuits. In *2023 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, pages 1–6. IEEE; IEEE.

United Nations Environment Programme (2016). Radiation: effects and sources. https://wedocs.unep.org/bitstream/handle/20.500.11822/7790/-Radiation_Effects_and_sources-2016Radiation_-_Effects_and_Sources.pdg.pdf.pdf. United Nations Environment Programme, 2016.

Valtchanov, B., Aubert, A., Bernard, F., and Fischer, V. (2008). Modeling and observing the jitter in ring oscillators implemented in FPGAs. In *2008 11th IEEE Workshop on Design and Diagnostics of Electronic Circuits and Systems*, pages 1–6.

Vijayakumar, A., Patil, V. C., and Kundu, S. (2017). On Improving Reliability of SRAM-Based Physically Unclonable Functions. *Journal of Low Power Electronics and Applications*, 7(1). .

Wang, W., Guin, U., and Singh, A. (2020). Aging-resilient SRAM-based True Random Number Generator for Lightweight Devices. *Journal of Electronic Testing*, 36:301–311.

Zhang, R., Liu, T., Yang, K., and Milor, L. (2017). Modeling of the Reliability Degradation of a FinFET-based SRAM due to Bias Temperature Instability, Hot Carrier Injection, and Gate Oxide Breakdown. In *2017 IEEE International Integrated Reliability Workshop (IIRW)*, pages 1–4.

Zhang, X., Jiang, C., Dai, G., Zhong, L., Fang, W., Gu, K., Xiao, G., Ren, S., Liu, X., and Zou, S. (2020). Improved performance of SRAM-based true random number generator by leveraging irradiation exposure. *Sensors*, 20(21):6132.