2023

Reliability of physical unclonable function derived from the power-up state of static random-access memory in extreme environments

Horace J.I Wilson

Follow this and additional works at: https://louis.uah.edu/uah-theses

Recommended Citation
Wilson, Horace J.I., "Reliability of physical unclonable function derived from the power-up state of static random-access memory in extreme environments" (2023). Theses. 618. https://louis.uah.edu/uah-theses/618

This Thesis is brought to you for free and open access by the UAH Electronic Theses and Dissertations at LOUIS. It has been accepted for inclusion in Theses by an authorized administrator of LOUIS.
RELIABILITY OF PHYSICAL UNCLONABLE FUNCTION DERIVED FROM THE POWER-UP STATE OF STATIC RANDOM-ACCESS MEMORY IN EXTREME ENVIRONMENTS

Horace J. Wilson

A THESIS

Submitted in partial fulfillment of the requirements for the degree of Master of Science in Engineering in Electrical Engineering to The Graduate School of The University of Alabama in Huntsville December 2023

Approved by:
Dr. Biswajit Ray, Research Advisor
Dr. Aleksandar Milenkovic, Committee Chair
Dr. Aubrey Beal, Committee Member
Dr. Aleksandar Milenkovic, Department Chair
Dr. Shankar Mahalingham, College Dean
Dr. Jon Hakkila, Graduate Dean
Abstract

RELIABILITY OF PHYSICAL UNCLONABLE FUNCTION DERIVED FROM THE POWER-UP STATE OF STATIC RANDOM-ACCESS MEMORY IN EXTREME ENVIRONMENTS

Horace J. Wilson

A thesis submitted in partial fulfillment of the requirements for the degree of Master of Science in Engineering

Electrical Engineering

The University of Alabama in Huntsville
December 2023

Static random-access memory (SRAM) is a high-speed, volatile memory that is ubiquitous in a wide range of computing platforms. Because of intrinsic process variations, an SRAM array’s power-up state presents a random yet distinctive, device-specific signature known as a Physical Unclonable Function (PUF). However, as SRAM dimensions continue to shrink, concerns arise about the PUF's resilience in extreme environments like outer space. Space has environmental conditions with high radiation levels and very low temperatures, so SRAM's reliability must be studied in these conditions. This research finds that ionizing radiation effects can dramatically impact the reliability of SRAM PUF. A technology node dependent study shows poor PUF-reliability for smaller nodes, and a temperature dependent study shows significant PUF-reliability degradation due to temperature variation. Encountering a combination of these factors weakens PUF reliability in space, so radiation-hardening techniques will be needed for preservation of PUF.
Acknowledgements

I would like to extend my deepest gratitude to my supervisor Dr. Biswajit Ray, and my other committee members, Dr. Aleksandar Milenkovic and Dr. Aubrey Beal, who made this work possible. Their guidance helped me through many stages of my research and the writing of this thesis. I would also like to thank my fellow members of Dr. Ray’s research group, Umesh, Farzana, Misha, Sijay, Anik, and Raqib, for our daily interactions regarding research. Discussing our research projects helped me grow as a researcher and I am very appreciative of that.

I would like to thank my family for their support and encouragement throughout this process. Knowing that there was always someone cheering me on at every point was very beneficial. I would also like to thank the UAH Ultimate club teams for helping me with my physical and mental healthy throughout my time at school.
Table of Contents

Abstract.................................................................................................................................................... ii

Acknowledgements ............................................................................................................................... iv

Table of Contents ...................................................................................................................................... v

List of Figures........................................................................................................................................... vii

List of Tables ............................................................................................................................................ ix

Epigraph ................................................................................................................................................... x

Chapter 1. Introduction .......................................................................................................................... 1

Chapter 2. Literature Review ................................................................................................................. 7

Chapter 3. Simulation Exploration of SRAM Power-Up Transients ................................................. 11

3.1 Methodology ................................................................................................................................ 11

3.2 Results ............................................................................................................................................ 13

3.3 Conclusion .................................................................................................................................... 16

Chapter 4. Temperature and Technology Node Analysis on SRAM PUF Reliability ......................... 17

4.1 PUF Metrics .................................................................................................................................. 17

4.2 Temperature Analysis .................................................................................................................... 19

4.3 Technology Node Analysis ............................................................................................................ 23

Chapter 5. Radiation Effects on SRAM Power-Up State ................................................................... 26

5.1 Methodology .................................................................................................................................. 27
5.2 Results .......................................................................................................................... 28
5.3 Conclusion.................................................................................................................. 31

Chapter 6. Conclusions and Future Work ................................................................. 32
6.1 Conclusions ............................................................................................................. 32
6.2 Future Work ............................................................................................................ 33

References ...................................................................................................................... 34

Appendix A. Supporting Graphics for Simulation ......................................................... 39

Appendix B. Supplemental Data for Chip-Level Analyses .......................................... 43

Appendix C. Supplemental Data for MOS-Level Analysis ........................................... 46
List of Figures

Figure 1.1 Visual depiction from NASA of the increase in satellites [1]. .......................... 2

Figure 1.2 Schematic of an SRAM cell represented by two cross-coupled inverters. Q and Q_bar represent logically opposite signals. ................................................................. 3

Figure 1.3 Simplified SRAM cell represented by transistors and capacitors, Q and Q_bar represent logically opposite signals. ................................................................. 4

Figure 1.4 Diagram of MOSFET. ....................................................................................... 5

Figure 3.1 Schematic of HSpice simulation........................................................................ 12

Figure 3.2 Snippet of HSpice code shown in Notepad++.................................................. 12

Figure 3.3 Transient simulation results of output voltage nodes during power-up for SRAM cell. .............................................................................................................. 14

Figure 3.4 Representation of power-up characteristic during phase one, both PMOSs are on...................................................................................................................... 14

Figure 3.5 Transient simulation results of output voltage nodes during power-up for SRAM cell in alternate state with matched PMOSs. .................................................. 15

Figure 3.6 Transient simulation results of output voltage nodes during power-up for SRAM cell ratios...................................................................................................... 16

Figure 4.1 Picture of two Cypress chips with a chip in the TSOP-54 socket
(CY7C1041G30 & CY7C1041CV33). ................................................................................. 20

Figure 4.2 Entire measurement setup with chip, chip socket, and microcontroller connected to laptop. ........................................................................................................... 20

Figure 4.3 Ultra-low temperature freezer made by So-Low, used for authentication PUFs................................................................................................................................. 21
Figure 4.4 (a) Hamming distance, (b) Hamming weight, and (c) unstable bit rate measured for each temperature ................................................................. 22

Figure 4.5 (a) Hamming distance, (b) Hamming weight, and (c) unstable bit rate measured for each technology node ................................................................. 24

Figure 4.6 Drawing of internal capacitance across gate and channel of MOSFET .... 25

Figure 5.1: Hamming distance increases with higher radiation dose in Cypress SRAM chip ........................................................................................................... 27

Figure 5.2 Transistor setup for SRAM radiation experiment ........................................ 28

Figure 5.3 The power-up state of the SRAM ................................................................. 29

Figure 5.4 ID-VGS characteristic curves for PMOSs .................................................. 30

Figure 5.5 ID-VGS characteristic curves for NMOSs ................................................. 30

Figure A.1 HSpice code for pre-radiation simulation ................................................. 38

Figure A.2 HSpice code for post-radiation simulation ............................................. 39

Figure A.3 HSpice code for alternate simulation ..................................................... 40

Figure A.4 Snippet of Output for Pre-Radiation Simulation ..................................... 41

Figure B.1 Top module of Arduino code ................................................................. 42

Figure B.2 Snippet of output from Arduino interface and CoolTerm in text file .......... 42

Figure B.3 Code for generating gold PUF ................................................................. 43

Figure B.4 Code for analyzing Hamming distance, Hamming weight, and unstable bit rate of PUF ................................................................. 44

Figure C.1 ID-VGS characteristic curves before and after radiation ....................... 45

Figure C.2 ID-VGS characteristic curves before and after radiation ....................... 45
List of Tables

Table 3.1 Threshold voltages and sizes used for simulation in HSpice. .......................... 12

Table 3.2 Threshold voltages for width ratio simulations. ........................................... 16

Table 4.1 Example of temporal majority voting using five PUFs, columns with red boxes represent unstable cells. ............................................................................................................. 18

Table 4.2 Information for SRAM chips used in temperature experiments. ...................... 23

Table 5.1 Information for MOSFETs used in radiation experiments. .............................. 28

Table 5.2 Threshold voltages of transistors before and after radiation. ......................... 29

Table C.1 Resulting power-up state in different transistor orientations before and after radiation. ...................................................................................................................... 46
I think of space not as the final frontier but as the next frontier. Not as something to be conquered but to be explored.

– Neil deGrasse Tyson
Chapter 1. Introduction

Over the past several decades, humanity has made large strides with space technology, and that is illustrated by the colossal increase in satellites used in space. Figure 1.1 (a),(b) shows the increase in the number of satellites close to Earth from 1975 to 2019, and Figure 1.1(c),(d) shows satellites further away from Earth in the same timespan [1]. This comparison over time illustrates the growth in satellite usage since the 1970’s, and satellite usage is forecasted to continue its rapid growth going forward. Satellites like CubeSat are booming in popularity due to low cost and short development times. Their market size reached $297 million in 2022, and the manufacturers expect it to reach $860 million by 2028 [2]. Their ability to observe and analyze the state of traffic, forests, and soil while in low Earth orbit (LEO) make CubeSats attractive to many commercial industries, and the global economy depends heavily on satellites and other forms of space hardware as a result [1], [2]. The government and military of the United States also depend on space hardware for executing national security missions, detecting missiles, and communicating around the world [1], so protecting its functionality is a top concern not only for the sake of the global economy, but also national security via military defense. As a result, hardware security methods need to be developed to protect space hardware from being interfered with by global adversaries.
Physical unclonable function (PUF) is a hardware security primitive that can generate a cryptographic key and authenticate devices [3], [4]. PUF uses physical characteristics from digital electronic components to distinguish itself from other, similar components [5], [6], [7], [8]. The ability of PUF to be physically distinct with respect to similar hardware can be compared to human fingerprints being able to identify people. PUF is a highly secure solution that satellites can utilize to protect confidential information and secure communication. PUF is simple and cost-effective because it leverages the existing electronics within the satellite [9]. Adversaries can interfere with or gain control over satellites and their communications if they are inadequately secured [10], especially when considering that certain devices will remain unattended and exposed to the space environment for extended periods of time [11]. To combat this, PUF can add an extra layer of security by requiring keys to interact or communicate with a device. PUF can be very beneficial to space hardware longevity due to its simplicity and reliability.

The power-up state of static random-access memory (SRAM) is commercially used as an option for generating PUF. SRAM PUF has several advantages, including its fast-
reading speed, low power consumption, high storage density, and good compatibility with popular electronics [12], [13], [14], [15]. Figure 1.2 shows that an SRAM cell is made up of two back-to-back cross-coupled inverters with outputs on either side. Inverters are a type of digital logic gate that hold either a low voltage value of “0” or a high voltage value of “1”. For an inverter, the output is the inverse of the input, so in an SRAM cell, the outputs will be opposites of each other [16], [17]. Each inverter is made up of a pair of transistors as shown in Figure 1.3. The transistors have opposite polarities, so when one side of the pair is on and allowing current to pass through, the other side is off and blocking current [18]. Based on the circuit diagrams of SRAM, the cell can only be in two states while it is on and stable: either $Q$ is “1” and $Q_{\text{bar}}$ is “0”, or $Q$ is “0” and $Q_{\text{bar}}$ is “1”.

![Figure 1.2 Schematic of an SRAM cell represented by two cross-coupled inverters. $Q$ and $Q_{\text{bar}}$ represent logically opposite signals.](image-url)
The transistors that are used for these experiments are called bulk metal-oxide-semiconductor field-effect transistors (MOSFETs), and an example of one is shown in Figure 1.4. There is a metal gate that rests on top of a thin silicon dioxide layer that can control the state of the entire MOSFET using a voltage input. The silicon dioxide layer is an electrical insulator that separates the gate and silicon substrate. The drain and source are parts of the substrate that have been made more electrically reactive by using chemical doping. For an ideal MOSFET, nothing happens when the gate voltage biases the MOSFET to be off, but a channel forms between the drain and source that allows charge to flow between them when the MOSFET is on. Because it can be biased easily, MOSFETs are commonly used as switches and they are very popular in modern electrical circuits [19].

There are physically distinct alternatives to bulk MOSFETs considered for PUF called Fin field-effect transistors (FinFETs) [20], [21], [22], [23], and fully depleted silicon-on-insulator (FDSOI) MOSFETs [24], [25]. Because of the physical differences, experiments on one type of transistor will not necessarily yield the same results on others. A thorough
investigation using one type of technology will have stronger conclusions than a less thorough study with mixed technologies, so only bulk MOSFETs will be considered during these experiments.

![Diagram of MOSFET](image)

**Figure 1.4** Diagram of MOSFET. A thin silicon dioxide layer separates the metal gate from the substrate. The drain and source are chemically doped regions that can form a channel based on the gate voltage.

SRAM is a volatile memory, meaning that data are lost when power is removed, so both output node capacitors in Figure 1.3 will have a value of “0” [26]. Despite knowing that an SRAM cell must be in one of two states when powered on and stable, it is difficult to predict the state of the cell when power is reapplied to a circuit. The state of the cell when power is reapplied is also known as the power-up state. The power-up state is influenced by slight physical manufacturing variations that occur during fabrication of these devices like oxide thickness and channel length [27], [28], [29], [30]. These manufacturing variations allow the SRAM power-up state to be used as a PUF because the cells’ differences are unique to each transistor, impossible to predict or observe, and physically consistent [3]. This is relevant because thousands of SRAM cells are used to form a large array in SRAM chips [31], so obtaining a random and reliable key from SRAM PUF is trivial.
The space environment is harsher for electronics than Earth, primarily due to elevated levels of ionizing radiation and extremely low temperatures [32], [33], [34]. Thus, these environmental factors must be taken into consideration when assessing the feasibility of using SRAM for PUF generation. Another growing concern is that the trend of smaller technology causes PUF to have decreased reliability [35], so multiple technology node sizes must be studied to predict the reliability of future technology that could be even smaller. The rest of this paper will analyze the reliability of SRAM PUF in high radiation, low temperature, and varied technology node size. The reliability of SRAM PUF in these conditions will determine how useful they will be in space hardware as security primitives.
Chapter 2. Literature Review

A lot of research has been done in the last 15 years to determine the effectiveness of the power-up state of SRAM in various applications and stress environments. Holcomb et al. discuss the utility of the power-up state as a physical fingerprint and propose a method of identifying circuits using the power-up state as a PUF [3]. They state that an effective PUF can be reliably generated in a repeatable manner while externally unclonable. In an experiment comparing over 5,000 SRAM devices, they find that identification using a Hamming distance algorithm – a measure of how similar two PUFs are – is extremely reliable. They also mention that factors like noise and environment can impact how reliable the PUF is. Some environmental factors like low temperatures have not been considered in research and understating behavior of SRAM PUF in low temperatures is pivotal for usage in space.

There has been a great deal of research focused on strengthening SRAM PUF reliability. Zhang et.al. propose that ionizing irradiation can substantially improve the reliability of identification of PUF [36]. Total ionizing dose (TID) refers to the accumulation of ionizing radiation dose over time on a device and TID can cause the threshold voltage of a MOSFET to change. Since the SRAM power-up state relies on the interaction between the transistors’ threshold voltages, exposing an SRAM cell to TID can change its PUF. Despite a certain threshold of TID causing SRAM to malfunction, their simulations and experiments show that the power-up state becomes more consistent by
making an SRAM cell experience low amounts of TID while in the power-up state. They state that radiation causes threshold voltage mismatches throughout the SRAM chips in the experiment, but they are unable to verify this hypothesis. They cannot measure the threshold voltages of the transistors experiencing TID because the transistors are not accessible inside of a commercial chip, so a detailed study of radiation impacting the threshold voltage of an active SRAM cell would take their research even further.

Lawrence *et al.* concluded that TID has a negligible impact on SRAM PUF reliability instead of a positive one, but all tests were conducted with low voltage in the circuit [6]. The largest supply voltage used was 0.6 V, and the least was 0 V with all pins being grounded, but many applications use higher supply voltages of 3.3V or 5V. Experiments with larger supply voltages are necessary to confirm the results of this study for a wider range of usage.

Many researchers have considered using aging effects to improve the reliability of SRAM PUF, but this can create an environment where harmful security concerns can thrive. Garg *et al.* proposed the use of negative-bias temperature instability (NBTI) which occurs when a PMOS experiences strong negative-bias voltage at a high temperature [37]. If a transistor experiences NBTI, its threshold voltage will increase. They applied NBTI to the SRAM while in its power-up state to force an equal number of 1’s and 0’s, then they applied NBTI to the SRAM in its inverse power-up state to make the threshold voltages have a larger mismatch, making the power-up state more consistent. Bhargava and Mai proposed a different form of aging called hot carrier injection (HCI) which occurs when charge carriers move so fast through the channel that they cause high energy collisions and get trapped in the gate oxide [38]. HCI, like NBTI, results in a higher threshold voltage and
can generate large voltage mismatch, but Bhargava and Mai contend that HCI is preferred because its effects are more long-lasting. Applying aging to SRAM circuits to stabilize PUF has some unintended consequences that are not ideal for security purposes.

Hovanes et.al expressed a glaring issue with aging that can happen with recycled and discarded chips. They claimed that an adversary could determine a large part of the PUF with access to initial power-up state and the discarded SRAM chip [39]. In this case, they assumed that the chip was made by a malicious and untrustworthy manufacturer, the manufacturer recorded the initial PUF and reobtained the discarded chip to record the final PUF. Aging an SRAM cell makes the inverse of the active power-up state stronger, so the PUF becomes weaker if aging happens while the SRAM’s PUF is active. Hovanes et.al took advantage of the aging characteristic by looking for the changed bits in initial and final PUFs to piece together the PUF used initially. This group successfully derives the PUF after assuming natural, long-term aging of an SRAM, so adding NBTI or HCI to strengthen a PUF would make the cloning process even more straightforward.

Research was also conducted on small batches of power-up responses to test improvements on the SRAM PUF reliability. Shifman et.al. use a preselection method that entails gathering two PUFs from the same SRAM cells and marking them as unstable if the cell does not have the same value both times [40]. The unstable cells will be ignored when trying to analyze the PUF which would increase the consistency but would also make the PUF weaker with respect to clonability since there is a lower number of bits being identified. Mathew et.al. suggest forcing unstable bits to a predetermined value to attain 100% stable key generation for SRAM PUF, but a similar problem arises as predetermining bits makes them more prone to be cloned [41].
Research in SRAM PUF still has several unexplored areas based on the existing literature. The impact of external radiation on PUFs remains a relatively unexplored area, and the effects of both low temperatures and the downsizing of technology node dimensions have received limited attention. Given the critical implications for the future use of electronic hardware in space, conducting a comprehensive study in these areas is of paramount importance.
Chapter 3. Simulation Exploration of SRAM Power-Up Transients

A lot of prior research has covered the impact that ionizing radiation has on transistor threshold voltage, and its resulting impact on SRAM PUF [36]–[38]. The goal of this simulation is to characterize the impact of shifted threshold voltages on the power-up response and to observe the state of the transistors during the power-up response.

3.1 Methodology

The SRAM cell shown in Figure 3.1 will be powered on for two HSpice simulations which are before and after an ionizing radiation event. Since radiation can shift the threshold voltage of MOSFETs [35], [42], [43], [44], these simulations include transistors with different threshold voltages shown in Table 3.1. The first simulation has threshold voltages that represent a pre-radiation state with slightly different values to mimic process variation. The second simulation has shifted threshold voltages to represent a post-radiation state with the “on” transistors having a larger threshold voltage shift than the “off” transistors compared to the initial simulation [45]. After observing the results of the previous simulations, another alternate simulation is added with matched PMOS transistors and mismatched NMOS transistors to isolate the behavior of NMOS. The threshold voltages are also in Figure 3.1. The voltage of both outputs are recorded over time, and all four transistors in this simulation use the CASMOS MOSFET model which is supposed to function as a generic type of transistor [46]. A snippet of the HSpice code is shown in
Figure 3.2, and the code was executed in a Linux environment by using Putty to make an SSH connection to a university Blackhawk server. Note that all parameters for the simulations excluding threshold voltage are the same for both sides.

![Schematic of HSpice simulation](image)

**Figure 3.1** Schematic of HSpice simulation.

<table>
<thead>
<tr>
<th>Name</th>
<th>1st $V_{TH}$ (V)</th>
<th>2nd $V_{TH}$ (V)</th>
<th>Alt $V_{TH}$ (V)</th>
<th>Width (nm)</th>
<th>Length (nm)</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1</td>
<td>-0.49</td>
<td>-0.52</td>
<td>-0.50</td>
<td>200</td>
<td>100</td>
</tr>
<tr>
<td>P2</td>
<td>-0.47</td>
<td>-0.54</td>
<td>-0.50</td>
<td></td>
<td></td>
</tr>
<tr>
<td>N1</td>
<td>0.50</td>
<td>0.43</td>
<td>0.43</td>
<td>600</td>
<td>100</td>
</tr>
<tr>
<td>N2</td>
<td>0.49</td>
<td>0.46</td>
<td>0.54</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table 3.1** Threshold voltages and sizes used for simulation in HSpice.

```plaintext
* MOS MODEL
.MODEL p1 PMOS level = 12, vto = -0.52V
.MODEL n1 NMOS level = 12, vto = 0.43V
.MODEL p2 PMOS level = 12, vto = -0.54V
.MODEL n2 NMOS level = 12, vto = 0.46V

* Voltages
VPULSE Vdd GND PWL(0s 0v 2ps 3.3v 20m 3.3v)

* xtor node assignment D G S B
M1 Vout1 Vout2 Vdd Vdd p1 L = 100n, W = 200n
M2 Vout1 Vout2 GND GND n1 L = 100n, W = 600n
M3 Vout2 Vout1 Vdd Vdd p2 L = 100n, W = 200n
M4 Vout2 Vout1 GND GND n2 L = 100n, W = 600n

* Capacitors
C1 Vout1 GND 10f
C2 Vout2 GND 10f
```

**Figure 3.2** Snippet of HSpice code shown in Notepad++.
3.2 Results

Figure 3.3 shows the power-up state as a “voltage race” between the output nodes of the simulated SRAM cell during the powering-up phases, and the winner of the race is the side that has the PMOS that turns on first. During phase 1 of powering up, both PMOSs are on and charging their respective capacitors while the NMOSs are off as shown in Figure 3.4. The NMOSs remain off as VOUT1 and VOUT2 charge up to the NMOSs’ threshold voltages. For the pre-radiation simulation in Figure 3.3(a), the VOUT2 side has the PMOS with a lower threshold voltage and it charges to a high voltage of 3.3V. The VOUT1 side has the PMOS with a lower threshold voltage for the post-radiation simulation in Figure 3.3(b), and VOUT1 ends up charging to the high voltage.

For both simulations, the voltages on both output nodes appear the same during phase 1. Because of the threshold voltage mismatch for the PMOS transistors, one PMOS starts charging faster than the other. During phase 2, a gap in output voltage appears and widens very quickly due to the faster charging side causing the opposite NMOS to turn on. An NMOS turning on means that there is a path to ground which discharges the voltage from the capacitor on that side, and the other NMOS will stay off since its biasing voltage is connected to ground. This allows for the PMOS on the side with the off-NMOS to safely reach the high voltage as shown in the final phase of Figure 3.3. This is how the PMOS with the threshold voltage of a smaller magnitude will typically end up charging to a high voltage.
Figure 3.3 Transient simulation results of output voltage nodes during power-up for SRAM cell in (a) pre-radiation and (b) post-radiation states.

Figure 3.4 Representation of power-up characteristic during phase one, both PMOSs are on.

To confirm the understanding of the previous portion of the simulation exploration, an additional simulation is run with matched PMOS transistors and mismatched NMOS transistors to isolate the behavior of NMOS. Since the PMOSs have matched threshold voltages as shown in Table 3.1, the node capacitors will charge at the same rate. N1 has a lower threshold voltage than N2, so it is expected it to turn on and discharge the capacitor on its side. Figure 3.5 depicts $V_{\text{OUT1}}$ going to 0V which shows that NMOS mismatch also
has an impact on the power-up state, but not as much as PMOS mismatch for these simulations.

Figure 3.5 Transient simulation results of output voltage nodes during power-up for SRAM cell in alternate state with matched PMOSs.

To test the conclusion about PMOS mismatch despite the larger-sized NMOS, one more batch of simulations is run with varied width ratios for NMOS and PMOS. The transistors have even threshold voltage mismatch as shown in Table 3.2, and the results are shown in Figure 3.6 for NMOS to PMOS width ratios of 10:1, 15:1, and 20:1. If the PMOS mismatch determines the power-up state for the simulation, then $V_{OUT2}$ will reach the high voltage, and if the NMOS mismatch determines the power-up state, $V_{OUT1}$ will reach the high voltage. Figure 3.6 shows $V_{OUT2}$ reaching the high voltage for all three simulations, so it seems like PMOS mismatch determines power-up state for small threshold voltage mismatches as depicted in these simulations.
Table 3.2 Threshold voltages for width ratio simulations.

<table>
<thead>
<tr>
<th>Name</th>
<th>$V_{TH}$ (V)</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1</td>
<td>-0.50</td>
</tr>
<tr>
<td>P2</td>
<td>-0.48</td>
</tr>
<tr>
<td>N1</td>
<td>0.50</td>
</tr>
<tr>
<td>N2</td>
<td>0.48</td>
</tr>
</tbody>
</table>

Figure 3.6 Transient simulation results of output voltage nodes during power-up for SRAM cell ratios of (a) 10 to 1, (b) 15 to 1, and (c) 20 to 1.

3.3 Conclusion

If there is a threshold voltage mismatch among the PMOSs, the cross-coupling of the inverters in SRAM means that one PMOS turns on first and forces the other side to lose its capacitively-charged voltage, thus creating a stable power-up state. If the PMOSs are matched, then the power-up state can be determined by mismatched NMOSs. These simulations show that threshold voltage has a large impact on the power-up state of SRAM, so ionizing radiation needs to be carefully considered when using the power-up state as a PUF. The power-up state can lose its consistency if exposed to ionizing radiation which would make the PUF weaker and more susceptible to failure.
Chapter 4. Temperature and Technology Node Analysis on SRAM PUF Reliability

4.1 PUF Metrics

The key performance metrics for determining the quality of a PUF depend on gold and authentication PUFs. The gold PUF is treated as the reference PUF and can represent an initial state. Authentication PUFs are subsequent PUFs that will be compared to the gold PUF. For this experiment, 101 power-up responses are obtained from a SRAM array at room temperature and use temporal majority voting (TMV) to generate a gold PUF. TMV is a method of analysis that assesses the mean of a bit location and outputs a value based on the average response. Since each SRAM cell can only express its value as a ‘0’ or a ‘1’, a sum of all iterations is measured and a threshold is set at the midpoint of the range. Table 4.1 shows an example of TMV using five PUFs. This experiment uses 101 PUFs to generate the gold PUF, so a range of 0-101 will have 0-50 representing a ‘0’ and 51-101 representing a ‘1’.
Table 4.1 Example of temporal majority voting using five PUFs, columns with red boxes represent unstable cells.

<table>
<thead>
<tr>
<th>PUF 1</th>
<th>0</th>
<th>1</th>
<th>1</th>
<th>0</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>PUF 2</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>PUF 3</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>PUF 4</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>PUF 5</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Sum</td>
<td>0</td>
<td>5</td>
<td>5</td>
<td>0</td>
<td>4</td>
<td>5</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>Gold</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

Average intra-die Hamming distance (HD), Hamming weight (HW), and unstable bit rate will be the key measurement used in this experiment. HD calculates how much error an authentication PUF has with respect to the chip’s gold PUF and represents how similar new PUFs are to the original PUF. HD is shown in Equation 4.1:

\[
\text{Hamming Distance} \, (\%) = \frac{1}{N} \left\{ \sum_{n=0}^{N} \text{Gold Bit}_n \oplus \text{Authentication Bit}_n \right\} \times 100 . \tag{4.1}
\]

HW depicts how often ‘1’ appears in the PUF and is shown in Equation 4.2:

\[
\text{Hamming Weight} \, (\%) = \frac{1}{N} \left\{ \sum_{n=0}^{N} \text{PUF Bit}_n \right\} \times 100. \tag{4.2}
\]

An SRAM array with an HW that is close to 50% is much harder to clone than an array with an of 0% or 100% because the data pattern is harder to discern. As a result, a HW of 50% is most desirable for SRAM PUF [36]. Unstable bit rate is the percentage of cells that are not consistently ‘0’ or ‘1’ for the whole data sample. It is a representation of the consistency of authentication PUFs which is shown in Equation 4.3, and Figure 4.1 shows cells with unstable bits in red boxes:

\[
\text{Unstable Bit Rate} \, (%) = \left( 1 - \left( \frac{1}{N} \ast \# \text{of consistent 0 or 1 bits} \right) \right) \times 100 . \tag{4.3}
\]
4.2 Temperature Analysis

Temperature-dependent reliability studies express that SRAM functionality diminishes in high temperature due to NBTI [37], [47], but SRAM PUF reliability at low temperatures have not been thoroughly explored. Extremely low temperatures are very common in space, so observing the reliability of SRAM PUF in those conditions is very important.

4.2.1 Methodology of Temperature Analysis

This analysis uses a commercial off-the-shelf (COTS) SRAM chip from Cypress at 25 °C, 0 °C, and -25 °C. The chip is at the 65nm technology node with part number CY7C104G30. An Arduino Due microcontroller and a TSOP-54 socket are attached using a printed circuit board (PCB) to interact with the chips. The PCB makes individual pin connections between the socket and microcontroller to link the two, and the pins are mapped in Arduino software to create a direct interface. A couple of chips and the TSOP-54 socket are shown in Figure 4.1, and the entire setup is shown in Figure 4.2. Code is prepared in Arduino that could cycle power on, read data, and write data on the chip. Using this setup, the power-up response is simulated by turning the power to the chip off, turning it back on and reading the PUFs. The data go into a text file using a CoolTerm serial terminal, and MATLAB scripts parse the output file and analyze the PUFs.
101 PUFs are recorded at about 25 °C and use TMV to generate a gold PUF for the chip, then 50 authentication PUFs are collected at 25 °C, 0 °C, and -25 °C for obtaining PUF metrics detailed in Section 4.1. Measurements at 25 °C are conducted at room temperature, and lower measurements are conducted with the setup in an ultra-low temperature freezer shown in Figure 4.3. There are authentication PUFs that are measured at a temperature different than the gold PUF, so temperature variation effects of SRAM will be observed. There seems to be consensus that SRAM has better performance at lower
temperatures [47], [48], but this experiment with temperature variation effect will bring new findings on PUF specifically.

Figure 4.3 Ultra-low temperature freezer made by So-Low, used for authentication PUFs.

4.2.2 Results of Temperature Analysis

Temperature has a minor impact on PUF reliability for SRAM based on the data sample used. Figure 4.4 shows minimal differences in Hamming weight and unstable bit rate as temperature changes for the 65nm technology nodes, but the Hamming distance does change. These data give credence to the idea that the power-up characteristic changes slightly as temperature changes. The Hamming distance measures how similar the authentication PUFs are to the gold PUF, and the data show there that HD increases from about 6% to nearly 10% as the temperature decreases and gets further away from the 25°C that the gold PUF was recorded at. The unstable bit rate measures how similar the experimental PUFs are to themselves, and the results show that it is close to 40% for
measurements at each temperature. With the consistency of the unstable bit rate, the power-up response at different temperatures could be used as their own PUF for the same chip.

![Figure 4.4](image)

**Figure 4.4** (a) Hamming distance, (b) Hamming weight, and (c) unstable bit rate measured for each temperature.

### 4.2.3 Conclusion of Temperature Analysis

The highest HD value of about 10% may be within the acceptable limit for error correction [38], [49], so -25 °C may not be enough to apply this, but lower temperatures have the potential to go beyond the acceptable limit given the trend shown in this experiment. There are two ideas that can be proposed with this finding. First, the acceptable range for device authentication may need to increase depending on the temperature that the SRAM chip is used in. Second, a user could attempt to use multiple gold PUFs for the same chips at different temperatures. This would require recording the gold PUF at multiple temperatures and checking the temperature of the chip during authentication to compare it to the proper gold PUF. More research needs to be done to determine the relevance of either of these ideas, but these are effects that need to be considered when using the SRAM power-up state as a PUF in extremely low temperatures.
4.3 Technology Node Analysis

SRAM technology is continuously scaling to smaller sizes over time [35], and the effects of the scaling on commercial SRAM technologies have not been thoroughly investigated for SRAM PUF. The goal of this analysis is to determine if the current scaling trend will have an impact on the future reliability of SRAM PUF by isolating technology node size.

4.3.1 Methodology of Technology Node Analysis

The methodology of this analysis is very similar to temperature analysis. COTS SRAM chips from Cypress are used at 65nm, 90nm, and 150nm technology node sizes. More information is provided about the SRAM chips in Table 4.2. The same setup using Arduino is used and all PUFs are recorded at room temperature. 101 PUFs are recorded for each technology node and TMV is applied to generate gold PUFs for each chip. An additional 50 authentication PUFs are recorded at each technology node for obtaining PUF metrics detailed in Section 4.1.

Table 4.2 Information for SRAM chips used in temperature experiments.

<table>
<thead>
<tr>
<th>Part Number</th>
<th>Tech. Node (nm)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CY7C1041G30</td>
<td>65</td>
</tr>
<tr>
<td>CY7C1041D33</td>
<td>90</td>
</tr>
<tr>
<td>CY7C1041C33</td>
<td>150</td>
</tr>
</tbody>
</table>
4.3.2 Results of Technology Node Analysis

Technology node size has a large impact on the consistency of the SRAM power-up state. Figure 4.3 shows that Hamming distance and unstable bit rate are substantially higher with smaller technology node size. These experiments show that smaller technology node sizes have less consistency and reliability across the temperatures observed. The main cause of this is ambient electrical noise that the circuits experience [43], [44], [50], and Equations 4.4 and 4.5 express why that is the case. Figure 4.4 shows that there is an internal capacitance across the gate and the channel with silicon dioxide acting as a dielectric. The area of the internal capacitor rapidly decreases with a smaller node size even if the distance is also shrinking. This means that the internal capacitance is shrinking according to Equation 4.4: 

\[ C = \frac{\varepsilon A}{d}. \]  (4.4)

Therefore, a single charge \( q \) would cause a greater change in threshold voltage according to Equation 4.5: 

\[ \Delta V_t = \frac{q}{C}. \]  (4.5)

This varied voltage caused by noise creates a random boost for an SRAM’s power-up characteristic towards one of the two possible states, thus impacting the reliability of the PUF.

Figure 4.5 (a) Hamming distance, (b) Hamming weight, and (c) unstable bit rate measured against temperature for each technology node.
The Hamming weight for the 90nm technology node is unexpectedly lower than it is for the other two technology nodes. This appears to be consistent for 90 nm SRAM chips from Cypress. There is a strong trend that all three technology nodes share with respect to Hamming distance and unstable bit rate, so Hamming weight does not seem to have major influence in this portion of the analysis.

4.3.3 Conclusion of Technology Node Analysis

Smaller technology nodes have worse PUF reliability for SRAM, so the scaling trend of SRAM technologies would have a negative impact on the utility of SRAM PUF going forward. The shrinking internal capacitances are much more susceptible to random noise causing fluctuation in the power-up response. This result signals the need for noise protection with smaller technologies for SRAM PUF in the future.
Chapter 5. Radiation Effects on SRAM Power-Up State

Research dealing with radiation effects on SRAM PUF typically revolves around COTS memory chips with undisclosed physical attributes. Such an analysis on COTS memory chips is indeed crucial, as it offers vital insights into the chip's radiation tolerance limits. Nevertheless, there is still ample opportunity for a more comprehensive, physics-based understanding of SRAM PUF. For example, a chip-level radiation analysis is performed with the same experimental setup described for other chip-level analyses. The findings, illustrated in Figure 5.1, demonstrate an increase in Hamming distance with higher radiation dose. One of the primary causes for this effect is the shifted threshold voltage of the constituent transistors, a deduction based on simulations of the memory cell. Consumers are unable to measure or interact with physical aspects of individual SRAM cells in a chip, so the conclusion cannot be properly verified by an external party with a chip-level analysis by itself. Discrete MOSFETs are used in this experiment to have more control over the experimental procedure and to derive the threshold voltage from specific transistors in an SRAM cell. This allows a more definite conclusion to be made based on the experimental results.
5.1 Methodology

This analysis uses four individual MOSFETs placed on a breadboard to form an SRAM cell which is shown in Figure 5.2, and the part numbers of the components used are shown in Table 5.1. For the analysis, the power-up response is measured for each of the four possible orientation combinations and the drain current/gate-source voltage ($I_D-V_{GS}$) characteristic curve for each transistor to determine the threshold voltages. To generate the characteristic curve, each transistor is isolated and a DC power supply applies a voltage on the gate while measuring the current travelling through the drain. The threshold voltage of each MOSFET can be roughly approximated by visually estimating the beginning of the plateau of the curve.

At Ohio State University's Nuclear Reactor Laboratory, the SRAM cell is exposed to gamma irradiation using a Co-60 source with a dose rate of 11.7 krad(Si)/h. The SRAM cell is exposed to ionizing radiation in a settled state, so two MOSFETs are on and the other two are off. After radiation, the power-up response of the four possible orientations and the $I_D-V_{GS}$ curve of each transistor are measured again to determine threshold voltage.
5.2 Results

The radiation experiment proves that the threshold of an “on” transistor shifts more than that of an “off” transistor. Figure 5.3(a) shows the power-up state of the SRAM cell before radiation with P2 and N1 “on” and P1 and N2 “off”. This is consistent with the findings from the simulation exploration because Table 5.2 shows a lower threshold voltage for P2 with respect to magnitude. The initial power-up state is the state that the SRAM cell was in while being dosed with radiation, and Figure 5.3(b) shows the intensity of the threshold voltage shifts after radiation. P2 and N1 experience the largest shifts in threshold voltage which decrease by about 1.3V while P1 and N2 have shifts less than 1V. These data show that the radiation causes the threshold voltage of MOSFETs to become
more negative and that “on” transistors experience more drastic shifts. The shifts in threshold voltage are caused by charge carriers becoming trapped in the oxide layer of the MOSFETs. When a transistor is on, charge is flowing through the channel which is adjacent to the oxide layer, so more charge carriers are susceptible to becoming trapped in the oxide [31], [50].

![Diagram](image1)

**Figure 5.3** (a) The power-up state of the SRAM before and during irradiation, (b) the SRAM cell with arrows depicting the intensity of change in threshold voltage after irradiation and, (c) the power-up state of SRAM after irradiation.

![Table](image2)

Table 5.2 Threshold voltages of transistors before and after radiation.

<table>
<thead>
<tr>
<th>Transistor</th>
<th>Pre-Rad $V_{TH}$ (V)</th>
<th>Post-Rad $V_{TH}$ (V)</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1</td>
<td>-2.05</td>
<td>-2.65</td>
</tr>
<tr>
<td>P2</td>
<td>-2.03</td>
<td>-3.35</td>
</tr>
<tr>
<td>N1</td>
<td>3.10</td>
<td>1.85</td>
</tr>
<tr>
<td>N2</td>
<td>3.05</td>
<td>2.35</td>
</tr>
</tbody>
</table>

Figure 5.3(c) shows that the power-up state after irradiation of the SRAM cell is opposite of the pre-radiation state. Table 5.2 shows that the PMOS with the smaller threshold voltage magnitude post-radiation is P1, so P1 is expected to be on. N2 is on even
though it has a higher threshold voltage, so the threshold voltage mismatch of the NMOSs
does not seem to matter as much as it does for PMOSs.

Figures 5.4 and 5.5 show the $I_D$ vs $V_{GS}$ characteristic curves before and after
radiation for the PMOSs and NMOSs. There is a larger difference between the
characteristic curves after radiation, so the threshold voltage mismatch between the
transistors is larger after radiation.

![ID-VGS characteristic curves for PMOSs](image1)

**Figure 5.4** ID-VGS characteristic curves for PMOSs (a) before radiation (b) and after radiation.

![ID-VGS characteristic curves for NMOSs](image2)

**Figure 5.5** ID-VGS characteristic curves for NMOSs (a) before radiation (b) and after radiation.
5.3 Conclusion

Ultimately, the physical characteristics of MOSFETs can cause an SRAM cell to flip its power-up state after experiencing a radiation event which would cause PUF reliability to degrade. This degradation is due to PMOS threshold voltage mismatch dictating the power-up state, and “on” transistors experiencing a larger threshold voltage shift. In some cases, the PMOS with the lower negative threshold voltage will become the PMOS with a more negative threshold voltage after a radiation event, so an SRAM cell that experiences radiation while in the power-up state will be likelier to flip in its subsequent power-up states. An environment with a lot of radiation, like space, can be devastating to the reliability of SRAM PUF if it is not accounted for.
Chapter 6. Conclusions and Future Work

6.1 Conclusions

This paper has demonstrated that radiation and technology nodes can greatly impact the utility of SRAM PUF while low temperatures do not seem too significant for SRAM PUF, especially with using larger technology nodes. The radiation experiments show that “on” transistors experience a larger threshold voltage shift in the presence of radiation than “off” transistors while quantifying the shift as well. This can flip the power-up behavior of an SRAM cell, so it is an effect that can negatively impact PUF reliability, thus ruining its use as a hardware security primitive in space applications. The temperature experiment shows that PUF at low temperature has some slight changes but remains relatively consistent. Small technology nodes with low temperature can be concerning, but there are a couple of potential workarounds such as allowing a higher HD if the gold and authentication PUFs are recorded at different temperatures or storing an alternate gold PUF for lower temperatures. For the purposes of space hardware security, using the power-up response for PUF seems fine with respect to low temperatures but needs some method of protection against radiation and noise at small technology nodes. This research can be taken further to yield more concrete conclusions about the SRAM power-up state as a PUF for space applications.
6.2 Future Work

Since the chips were made commercially instead of self-fabricated, important details like oxide thickness and channel length remain unknown for the experiments. A future study that would take this research further could look at the threshold voltage shifts for different oxide thicknesses and technology nodes to determine the characteristics that are best suited to endure the space environment. This would likely require partnership with an electronic device fabrication lab to select the characteristics for the SRAM array used.

Also, there will be temperatures below -25 °C that space equipment will have to endure, but the equipment used for this experiment was not able to. An experiment that covers even lower technology node sizes and lower temperatures could uncover an even higher HD which would render SRAM PUF unusable in those conditions without protection.

Ultimately, the purpose of these experiments was to find flaws in SRAM PUF that would need to be protected using external systems. Radiation-hardening, error-correction code, and temperature regulation systems are a couple of solutions to the issues brought up, but more external protection would increase the cost necessary to properly use SRAM to generate PUF. Every solution has some flaw or inefficiency that needs to be monitored, and the effectiveness of a solution is balanced by its cost. These experiments succeeded in going a step further in assessing the effectiveness of SRAM power-up state as PUF in the harsh space environment so that the cost of using and maintaining it will be easier to ascertain.
References


[38] M. Bhargava and K. Mai, “A High Reliability PUF Using Hot Carrier Injection Based Response Reinforcement”.


Appendix A. Supporting Graphics for Simulation

* MOS MODEL
 .MODEL p1 PMOS level = 12, vto = -0.49V
 .MODEL n1 NMOS level = 12, vto = 0.5V
 .MODEL p2 PMOS level = 12, vto = -0.47V
 .MODEL n2 NMOS level = 12, vto = 0.49V

* Voltages
 VPULSE Vdd GND PWL(0s 0v 2ps 3.3v 20m 3.3v)

* xtor node assignment D G S B
 M1 Vout1 Vout2 Vdd Vdd p1 L = 100n, W = 200n
 M2 Vout1 Vout2 GND GND n1 L = 100n, W = 600n
 M3 Vout2 Vout1 Vdd Vdd p2 L = 100n, W = 200n
 M4 Vout2 Vout1 GND GND n2 L = 100n, W = 600n

* Capacitors
 C1 Vout1 GND 10f
 C2 Vout2 GND 10f

.TRAN 20p 1.6n

.OPTION POST
.PRINT TRAN V(Vout1) V(Vout2)

.END

Figure A.1 HSpice code for pre-radiation simulation.
* MOS MODEL

```
.MOS p1 PMOS level = 12, vto = -0.52V
.MOS n1 NMOS level = 12, vto = 0.43V
.MOS p2 PMOS level = 12, vto = -0.54V
.MOS n2 NMOS level = 12, vto = 0.46V
```

* Voltages

```
VPULSE Vdd GND PWL(0s 0v 2ps 3.3v 20m 3.3v)
```

* xtor node assignment D G S B

```
M1 Vout1 Vout2 Vdd Vdd p1 L = 100n, W = 200n
M2 Vout1 Vout2 GND GND n1 L = 100n, W = 600n
M3 Vout2 Vout1 Vdd Vdd p2 L = 100n, W = 200n
M4 Vout2 Vout1 GND GND n2 L = 100n, W = 600n
```

* Capacitors

```
C1 Vout1 GND 10f
C2 Vout2 GND 10f
```

```
.TRAN 20p 1.6n
```

```
.OPTION POST
.PRINT TRAN V(Vout1) V(Vout2)
```

```
.END
```

**Figure A.2** HSpice code for post-radiation simulation.
* MOS MODEL
  .MODEL p1 PMOS level = 12, vto = -0.50V
  .MODEL n1 NMOS level = 12, vto = 0.43V
  .MODEL p2 PMOS level = 12, vto = -0.50V
  .MODEL n2 NMOS level = 12, vto = 0.54V

* Voltages
  VPULSE Vdd GND PWL(0s 0v 2ps 3.3v 20m 3.3v)

* xtor node assignment D G S B
  M1 Vout1 Vout2 Vdd Vdd p1 L = 100n, W = 200n
  M2 Vout1 Vout2 GND GND n1 L = 100n, W = 600n
  M3 Vout2 Vout1 Vdd Vdd p2 L = 100n, W = 200n
  M4 Vout2 Vout1 GND GND n2 L = 100n, W = 600n

* Capacitors
  C1 Vout1 GND 10f
  C2 Vout2 GND 10f

.TRAN 20p 1.6n
.OPTION POST
.PRINT TRAN V(Vout1) V(Vout2)
.END

Figure A.3 HSpice code for alternate simulation.
#### Figure A.4 Snippet of output for pre-radiation simulation.

```plaintext
<table>
<thead>
<tr>
<th>time</th>
<th>voltage</th>
<th>voltage</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>vout1</td>
<td>vout2</td>
</tr>
<tr>
<td>0.</td>
<td>1.2168e-19</td>
<td>-1.1159e-20</td>
</tr>
<tr>
<td>20.000000p</td>
<td>124.1564m</td>
<td>126.1009m</td>
</tr>
<tr>
<td>40.000000p</td>
<td>240.3841m</td>
<td>244.4413m</td>
</tr>
<tr>
<td>60.000000p</td>
<td>345.7635m</td>
<td>352.1626m</td>
</tr>
<tr>
<td>80.000000p</td>
<td>431.5914m</td>
<td>440.7454m</td>
</tr>
<tr>
<td>100.000000p</td>
<td>517.4192m</td>
<td>529.3282m</td>
</tr>
<tr>
<td>120.000000p</td>
<td>603.2471m</td>
<td>617.9110m</td>
</tr>
<tr>
<td>140.000000p</td>
<td>689.0749m</td>
<td>706.4937m</td>
</tr>
<tr>
<td>160.000000p</td>
<td>760.4287m</td>
<td>781.7457m</td>
</tr>
<tr>
<td>180.000000p</td>
<td>805.6963m</td>
<td>832.9720m</td>
</tr>
<tr>
<td>200.000000p</td>
<td>850.9638m</td>
<td>884.1983m</td>
</tr>
<tr>
<td>220.000000p</td>
<td>896.2314m</td>
<td>935.4245m</td>
</tr>
<tr>
<td>240.000000p</td>
<td>941.4989m</td>
<td>986.6508m</td>
</tr>
<tr>
<td>260.000000p</td>
<td>974.9246m</td>
<td>1.0300m</td>
</tr>
<tr>
<td>280.000000p</td>
<td>987.0080m</td>
<td>1.0592m</td>
</tr>
<tr>
<td>300.000000p</td>
<td>999.0915m</td>
<td>1.0883m</td>
</tr>
<tr>
<td>320.000000p</td>
<td>1.0112m</td>
<td>1.1175m</td>
</tr>
<tr>
<td>340.000000p</td>
<td>1.0233m</td>
<td>1.1466m</td>
</tr>
<tr>
<td>360.000000p</td>
<td>1.0242m</td>
<td>1.1768m</td>
</tr>
<tr>
<td>380.000000p</td>
<td>1.0052m</td>
<td>1.2089m</td>
</tr>
<tr>
<td>400.000000p</td>
<td>986.1507m</td>
<td>1.2409m</td>
</tr>
<tr>
<td>420.000000p</td>
<td>967.1087m</td>
<td>1.2730m</td>
</tr>
<tr>
<td>440.000000p</td>
<td>948.0667m</td>
<td>1.3050m</td>
</tr>
<tr>
<td>460.000000p</td>
<td>912.6897m</td>
<td>1.3467m</td>
</tr>
<tr>
<td>480.000000p</td>
<td>847.8722m</td>
<td>1.4060m</td>
</tr>
<tr>
<td>500.000000p</td>
<td>783.0548m</td>
<td>1.4652m</td>
</tr>
<tr>
<td>520.000000p</td>
<td>718.2374m</td>
<td>1.5244m</td>
</tr>
<tr>
<td>540.000000p</td>
<td>653.4199m</td>
<td>1.5836m</td>
</tr>
<tr>
<td>560.000000p</td>
<td>583.4665m</td>
<td>1.6511m</td>
</tr>
<tr>
<td>580.000000p</td>
<td>504.2568m</td>
<td>1.7335m</td>
</tr>
<tr>
<td>600.000000p</td>
<td>425.0470m</td>
<td>1.8159m</td>
</tr>
<tr>
<td>620.000000p</td>
<td>345.8372m</td>
<td>1.8983m</td>
</tr>
<tr>
<td>640.000000p</td>
<td>266.6274m</td>
<td>1.9807m</td>
</tr>
<tr>
<td>660.000000p</td>
<td>202.2161m</td>
<td>2.0618m</td>
</tr>
<tr>
<td>680.000000p</td>
<td>164.4756m</td>
<td>2.1407m</td>
</tr>
<tr>
<td>700.000000p</td>
<td>126.7352m</td>
<td>2.2196m</td>
</tr>
</tbody>
</table>
```
Appendix B. Supplemental Data for Chip-Level Analyses

```c
#include "sram.h"
#include "serial.h"

// Define serial port used, should match that in sram.h and serial.h
#define SERIAL_PORT SerialUSB

void setup() {
    // Configure serial interface
    SERIAL_PORT.begin(115200);
    SERIAL_PORT.setTimeout(10);

    while(!SERIAL_PORT);

    SERIAL_PORT.print("\n\rInitializing Serial Interface...\n\r");

    configurePins();
}

void loop() []
    // Listen for and act upon serial input
    if (SERIAL_PORT.available() > 0) {
        dispatchCommand();
    }
}
```

**Figure B.1** Top module of Arduino code.

```
3 Dumping SRAM as hex many times:
4
5 BEGIN DATA DUMP
6 614E 4925 5E08 40D0 1421 4022 308
7 600E 4925 5E09 40E0 1429 4020 208
8 630E 4925 5E08 40F0 1421 4020 208
```

**Figure B.2** Snippet of output from Arduino interface and CoolTerm in text file.
% Constants
numPUFs = 101;
numBits = 4194304;
umiWords = numBits/16;

% Initialize array for overall sum of PUF
binTMV = zeros(numiWords, 16);

filePath = fopen('J4_90mmgold.txt', 'r'); % Opening file w/ PUF
dPUFs = strings(numPUFs, numiWords);

for i = 1:numPUFs
    for j = 1:numiWords
        dPUFs(i, j) = fscan(filePath, '%s', 1);
    end
end

% Obtain PUF and add it summing array
binPUF = hexToBinaryVector(dPUFs(i,:));
binTMV = binTMV + binPUF;

fclose(filePath);

% Use Temporal Majority Voting to get the Gold PUF
goldBit = zeros(numiWords, 16);
goldOneCU = ceil(numPUFs/2);
goldZeroCU = floor(numPUFs/2);

for i = 1:numiWords
    for j = 1:16
        if(binTMV(i,j)>=goldOneCU)
goldBit(i,j) = 1; % already padded with zeros
    end
end
end

Figure B.3 Code for generating gold PUF.
Figure B.4 Code for analyzing Hamming distance, Hamming weight, and unstable bit rate of PUF.
Appendix C. Supplemental Data for MOS-Level Analysis

Figure C.1 ID-VGS characteristic curves before and after radiation for (a) P1 and (b) P2.

Figure C.2 ID-VGS characteristic curves before and after radiation for (a) N1 and (b) N2.
Table C.1 Resulting power-up state in different transistor orientations before and after radiation.

<table>
<thead>
<tr>
<th>Orientation</th>
<th>P1 N1</th>
<th>P2 N2</th>
<th>P1 N2</th>
<th>P2 N1</th>
<th>P1 N1</th>
<th>P2 N2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pre-Rad</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>V_{OUT1} (V)</td>
<td>V_{OUT2} (V)</td>
<td>V_{OUT1} (V)</td>
<td>V_{OUT2} (V)</td>
<td>V_{OUT1} (V)</td>
<td>V_{OUT2} (V)</td>
</tr>
<tr>
<td>Samples</td>
<td>0.00</td>
<td>5.02</td>
<td>0.00</td>
<td>5.01</td>
<td>5.04</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>0.00</td>
<td>5.02</td>
<td>0.00</td>
<td>5.02</td>
<td>5.04</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>0.00</td>
<td>5.01</td>
<td>0.00</td>
<td>5.02</td>
<td>5.03</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>0.00</td>
<td>5.01</td>
<td>0.00</td>
<td>5.02</td>
<td>5.03</td>
<td>0.00</td>
</tr>
<tr>
<td><strong>Post-Rad</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>V_{OUT1} (V)</td>
<td>V_{OUT2} (V)</td>
<td>V_{OUT1} (V)</td>
<td>V_{OUT2} (V)</td>
<td>V_{OUT1} (V)</td>
<td>V_{OUT2} (V)</td>
</tr>
<tr>
<td>Samples</td>
<td>5.04</td>
<td>0.00</td>
<td>5.04</td>
<td>0.00</td>
<td>5.02</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>5.04</td>
<td>0.00</td>
<td>5.04</td>
<td>0.00</td>
<td>5.01</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>5.04</td>
<td>0.00</td>
<td>5.04</td>
<td>0.00</td>
<td>5.01</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>5.04</td>
<td>0.00</td>
<td>5.04</td>
<td>0.00</td>
<td>5.01</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>5.04</td>
<td>0.00</td>
<td>5.04</td>
<td>0.00</td>
<td>5.01</td>
<td>0.00</td>
</tr>
</tbody>
</table>