University of Alabama in Huntsville

LOUIS

Dissertations | UAH Electronic Theses and Dissertations

2024

Exploring the impact of ionizing radiation on security and reliability in modern semiconductor memories

Umeshwarnath Surendranathan

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

Recommended Citation

Surendranathan, Umeshwarnath, "Exploring the impact of ionizing radiation on security and reliability in modern semiconductor memories" (2024). *Dissertations*. 410.
https://louis.uah.edu/uah-dissertations/410

This Dissertation 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 Dissertations by an authorized administrator of LOUIS.

EXPLORING THE IMPACT OF IONIZING RADIATION ON SECURITY AND RELIABILITY IN MODERN SEMICONDUCTOR MEMORIES

Umeshwarnath Surendranathan

A DISSERTATION

**Submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in
The Department of Electrical & Computer Engineering
to
The Graduate School
of
The University of Alabama in Huntsville
August 2024**

Approved by:

Dr. Biswajit Ray, Research Advisor
Dr. Aleksandar Milenkovic, Committee Chair
Dr. Laurie Joiner, Committee Member
Dr. Timothy Boykin, Committee Member
Dr. Aubrey Beal, Committee Member
Dr. Aleksandar Milenkovic, Department Chair
Dr. Shankar Mahalingam, College Dean
Dr. Jon Hakkila, Graduate Dean

Abstract

EXPLORING THE IMPACT OF IONIZING RADIATION ON SECURITY AND RELIABILITY IN MODERN SEMICONDUCTOR MEMORIES

Umeshwarnath Surendranathan

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy

Electrical Engineering

The University of Alabama in Huntsville
August 2024

Radiation effects in semiconductor devices have gained great traction in recent years due to an exponential growth in space exploration. The harsh conditions of space, devoid of the atmosphere and Earth's magnetic field, pose considerable challenges to electronic systems due to ionizing radiation exposure. While radiation-hardened (rad-hard) components are continually under development, they often lag several technology generations compared to commercial off-the-shelf (COTS) parts. Notably, rad-hard memories, particularly in terms of capacity (megabytes vs. terabytes) and cost, fall short compared to regular COTS memories. This underscores the compelling need to evaluate the radiation tolerance of COTS memories. This dissertation focuses on ionizing radiation effects on NAND flash and Static Random Access Memory (SRAM). We explore the total-ionizing-dose (TID) effects on 3D NAND by studying the bit error pattern with TID. We find that electrical noise contributes to a significant percentage of bit-errors and that radiation causes noise to increase during memory read operation. We present a powerful mitigation strategy to counteract radiation-induced noise increase by pre-programming factory-erase memory

blocks before deployment. Furthermore, we investigate TID effects on the power-up characteristics of COTS-SRAM memories. The SRAM power-up state, serving as a unique digital fingerprint or physical unclonable function (PUF) for device authentication, undergoes significant alterations due to ionizing radiation exposure. This may lead to authentication failures in the space and other harsh environment. To protect SRAM PUF from ionizing radiation, we propose a robust mitigation strategy involving the storage of an appropriate data pattern during irradiation. Lastly, we explore ionizing radiation as a potential attack vector posing a significant security threat to SRAM-based computing systems. Our research uncovers data imprinting effects caused by ionizing radiation, which could be exploited by adversaries for data leakage. Additionally, ionizing radiation induces a substantial reduction in SRAM data remanence time, and we present this as a mitigation strategy against security attacks relying on SRAM data remanence.

Acknowledgements

I would like to thank my advisor, Dr. Biswajit Ray, for guiding me through this journey. He has been a wonderful teacher. I remember vividly when I first took up his class back in the fall of 2019, I would have stayed awake all night working, but I would be wide awake during his class. His style of teaching grabs your attention and keeps it. I have learned a lot from him. His work ethic has inspired me to work harder. I thank Dr. Milenkovic for being very supportive of me throughout. I am especially thankful for his tough love at all the right times. I would like to thank Dr. Joiner, Dr. Boykin, and Dr. Beal for their valuable mentorship. I would like to thank UAH and all the organizations including NSF, DOD, NSUF, and Alabama EPSCoR GRSP for supporting my research efforts. I would like to thank my seniors for their valuable guidance and support. I would like to thank my research team for being great fun to work with. I am incredibly thankful for my family, both blood and chosen, for an inexhaustible list of reasons. Finally, I am very thankful to God for making any of this possible.

A special thanks to the creators of the HBO series "Chernobyl" for bringing the historical events into stark relief. The emotional impact caused by the show sparked my interest in the field of radiation effects and laid the groundwork for my research motivation.

In loving memory of my Thatha who will forever be the most important teacher in my life.

Table of Contents

Abstract ii

Acknowledgements v

Table of Contents vii

List of Figures xi

List of Tables xv

Chapter 1. Introduction 1

1.1 Motivation 1

1.2 Key Contributions 3

1.3 Dissertation Outline 4

Chapter 2. Background 6

2.1 Radiation Effects in Semiconductor Devices 6

2.1.1 Single Event Effects 7

2.1.2 Total Ionizing Dose 9

2.2 SRAM Fundamentals 11

2.2.1 SRAM Cell Read Operation 13

2.2.2 SRAM Cell Write Operation 14

2.2.3 SRAM Cell Transistor Sizing Constraints 14

2.2.4 SRAM Array Architecture 16

2.3 NAND Flash Fundamentals 17

2.3.1 Erase/ Program Operation on Flash Memory 19

2.3.2 NAND Read Operation 20

2.3.3 MLC NAND Flash Architecture 21

Chapter 3. TID Effects on Bit Error Pattern in MLC NAND Memory 25

3.1 Introduction......25

3.2 Experimental Setup and Procedure to Study Radiation Effects in NAND Flash 28

3.2.1 Hardware Setup 28

3.2.2 Sample Details......29

3.2.3 Gamma-Ray Irradiation 30

3.3 Experimental Results and Discussion 31

3.3.1 Comparison of LSB-MSB Pages Before Irradiation 31

3.3.2 Post-Irradiation FBC Comparison of LSB and MSB Pages 32

3.3.3 Model for FBC Comparison of LSB and MSB Pages......35

3.3.4 Internal Data Randomizer and Data Pattern Dependency 38

3.3.5 MSB/LSB Page FBC in Different Vertical Layers 40

3.3.6 Analysis of Error Location on MSB vs. LSB Pages......41

3.4 Conclusion 42

Chapter 4. TID Effects on Read Noise of MLC 3D NAND 44

4.1 Introduction......44

4.2 Background Information......46

4.3 Experimental Results and Discussion 48

4.3.1 Characterization Technique for NBC 48

4.3.2 NBC Comparison for Irradiated vs. Un-Irradiated Chip with Freshly Written Data......50

4.3.3 NBC Comparison Between Erased vs. Programmed Memory Blocks on the Irradiated Chip......52

4.3.4 Layer Wise NBC Study......55

4.3.5 Room Temperature Annealing Effects 56

4.4 Conclusion 57

Chapter 5. SRAM PUF Under Ionizing Radiation 58

5.1 Introduction 58

5.2 Background Information 60

5.3 Experimental Setup to Study Radiation Effects in SRAM 62

5.4 Experimental Results and Discussion 63

5.4.1 Effects on the Power-up State of Static Random-Access Memory 63

5.4.1.1 Effects of Total Dose on SRAM-PUF 64

5.4.1.2 Total Dose Induced Unstable Power-Up Bits 67

5.4.1.3 Root Cause Analysis 69

5.4.1.4 Effect of Irradiation-Induced Defects 71

5.4.1.5 Effect of Charge Trapping in Oxide 72

5.4.1.6 Room Temperature Annealing Effects on Irradiated Chips 73

5.4.2 TID Effects of Stored Data and Technology Node 74

5.4.2.1 Baseline Characterization Results 75

5.4.2.2 Effects of Stored Data on the Power-Up State 76

5.4.2.3 Technology-Node vs. TID Effects on PUF 82

5.4.2.4 Room Temperature Anneal 83

5.5 Conclusions 84

Chapter 6. Data Pattern Imprinting Effects on SRAM Due to Ionizing Radiation 86

6.1 Introduction 86

6.2 Experimental Procedure 87

6.3 Experimental Results and Discussion 88

6.3.1 Baseline Characterization 88

6.3.2 Data Imprinting as a Function of Dose 89

6.3.3 Explanation of TID-Induced Data Imprinting 90

6.3.4 Effects of Room Temperature Anneal on Imprinting 91
6.3.5 Evaluation of Data Imprinting Effects on Multiple Chips 92
6.4 Conclusion 93
Chapter 7. Impact of Ionizing Radiation on SRAM Data Remanence 94
7.1 Introduction..94
7.2 Experimental Procedure...94
7.2.1 Baseline Characterization of Data Remanence 96
7.2.2 Post-Irradiation Data Remanence 97
7.2.3 Predictive Remanence Time Model...98
7.3 Conclusion 99
Chapter 8. Conclusion and Future Work 100
8.1 Summary of Key Findings and Contributions 100
8.2 Future Research Avenues 102
References...103

List of Figures

Figure 1.1 (a) Unresponsive moon rover which died after attempted use for Chernobyl disaster cleanup. b) “biorobots” with a 90 second timer cleaning up the disaster. 1

Figure 1.2 The rapid climb in number of nano and cube sats..2

Figure 2.1 The penetration of different types of ionizing radiation..7

Figure 2.2 Heavy ion striking a sensitive node of a transistor..7

Figure 2.3 Charge generation and collection phases in a reverse-biased junction and the resultant current pulse caused by the passage of a high-energy ion [4]......................................8

Figure 2.4 TID effects in MOS devices...10

Figure 2.5 Charge yield for x rays, low-energy protons, gamma rays, and alpha particles [6]....11

Figure 2.6 6T SRAM cell. 12

Figure 2.7 6-T SRAM Bit-Cell area trend, used by pure-player foundries. The data refer to SRAM used in Standard Logic for General Purpose technology, unless indicated differently….12

Figure 2.8 SRAM cell read operation. 13

Figure 2.9 SRAM cell write operation. 14

Figure 2.10 SRAM cell transistor sizing constraint. 15

Figure 2.11 SRAM (a) cell and (b) array architecture. 16

Figure 2.12 NAND Storage density progression over the years..18

Figure 2.13 Floating gate NAND flash memory cell. 18

Figure 2.14 Flash program/ erase operation and the corresponding change in cell Vt (and hence drain current)...19

Figure 2.15 NAND flash memory sample VT distribution. 20

Figure 2.16 NAND configurations and the corresponding read reference targets for each bit. ..21

Figure 2.17 (a) Circuit diagram of a NAND memory block, (b) Physical diagram of 3D NAND flash memory array, (c) Schematic of a 3-D NAND flash memory cell.........................23

Figure 2.18 Tapered structure of 3D NAND due to inefficient RIE process [15].......................24

Figure 3.1 (a) Arrangement of NAND flash memory cells connected to a single word line. (b) Cell threshold voltage distribution for MLC NAND. 26

Figure 3.2 Custom hardware based on FTDI controller featuring a TSOP socket (left) and BGA socket (right). 29

Figure 3.3 Logical (LSB and MSB) page distributions across different vertical layers of 3-D NAND. 30

Figure 3.4 (a) FBC comparison between LSB (blue symbols) and MSB (red symbols) pages before radiation exposure. (b) The frequency polygon for MSB and LSB FBC for all pages 32

Figure 3.5 (a) FBC comparison between LSB (blue symbols) and MSB (red symbols) pages after 10 krad(Si) of TID, (b) The frequency polygon for MSB and LSB FBC for all pages 34

Figure 3.6 Frequency plot of the FBC ratios in MSB to those in the corresponding LSB pages for random data pattern for (a) 10 krad(Si) and (b) 20 krad(Si). 35

Figure 3.7 (a) Energy band diagram of a floating gate transistor at unbiased condition. Solid lines represent energy bands for a cell in state-C whereas the dashed lines stand for state-B. 36

Figure 3.8 Illustration of the data randomization process. 38

Figure 3.9 Page-wise FBC for (a) 10 krad(Si) , (b) 20 krad(Si). Ratio of FBC in MSB and the corresponding LSB pages for all-zero data pattern for (c) TID = 10 krad(Si), and 39

Figure 3.10 Ratio of FBC in MSB and the corresponding LSB pages for the 32 different layers in 3-D-NAND from 6 different chips. 41

Figure 3.11 (a) Illustration of failed byte location (red) on LSB and MSB pages. Data are represented in hex format. (b) Probability of multi-bit error in a byte from 6 different chips. 42

Figure 4.1 (a) Energy band diagram of a programmed FG cell with all terminals grounded. (b) Illustration of cell threshold voltage distribution of MLC memory before (solid line). 47

Figure 4.2 (a) Table illustrating how we quantify noisy bits. (b) Sample read count vs. NBC% (c) Fail bit count for n = 200 consecutive reads from the same memory address 49

Figure 4.3 (a) Adjusting $Vref$ using read-retry operation to quantify NBC on freshly written data from irradiated and un-irradiated chips. (b) Experimental procedure followed 51

Figure 4.4 (a) Measured data on NBC for memory blocks that are in programmed vs erased condition during irradiation. Energy band diagrams of (b) an erased flash cell 54

Figure 4.5 Layer-wise noise analysis. NBC data are collected for two different memory blocks from the same chip. 55

Figure 4.6 Evolution of NBC with time after irradiation. 56

Figure 5.1 (a) Schematic of a six transistor (6T) SRAM cell and threshold voltage conditions for power-on. (b) SRAM array. 62

Figure 5.2 Custom SRAM Interface. 63

Figure 5.3 HD of SRAM-PUF as a function of total dose for COTS memory chips from (a) IDT and (b) Cypress. (c) Chip-to chip variation results of HD after irradiation.....................65

Figure 5.4 (a) Classification of SRAM-PUF bits as strong-0, strong-1 and unstable bits. (b) Percentage of unstable PUF bits as a function of power-up read counts (n). Unstable PUF........68

Figure 5.5 (a) Schematic of a SRAM cell used for simulation. The current distribution corresponds to the phase-1 of the power-up transient. (b) Current distribution during phase-2...70

Figure 5.6 (a) Schematic of a transistor with interface defect. (b) Current fluctuation caused by low-frequency noise. (c) & (d) Current transient leading to two different power-up.............72

Figure 5.7 Radiation induced charge trapping effect in the (a) oxide and (b) the corresponding current transients during power-up phase. 73

Figure 5.8 Relaxation effects for (a) IDT (b) Cypress chip...74

Figure 5.9 Baseline HD% and Unstable Cells% characterization of SRAM samples.................76

Figure 5.10 Effects of data stored on HD% and Unstable cells% (a) Cypress HD% (b) Cypress Unstable cells% (c) ISSI HD% (d) ISSI Unstable cells%. (e) Alliance HD% 79

Figure 5.11 Effects of data pattern on power-up state of irradiated SRAM cells. We assume two cases: (a) an SRAM cell whose power-up state is dictated by mismatched NMOS.............80

Figure 5.12 TID effects on different technology nodes (a) HD% (b) Unstable cells%. (c) Threshold voltage change as a function of oxide thickness. 83

Figure 5.13 Effects of room-temperature annealing on SRAM PUF. (a) HD (%) and (b) Unstable cell (%) are plotted as a function of anneal duration. 84

Figure 6.1 (a) Binary image of Albert Einstein, (b) Visualization of power-up state..................89

Figure 6.2 Progression of Imprint% with TID on the Cyp 250 nm sample. 90

Figure 6.3 (a) SRAM cell holding $Q = 1$, during irradiation. Charge trapping effects on (b) OFF and (c) ON transistor. 91

Figure 6.4 Effect of room temperature anneal on Imprint% of the CYP 250 nm sample............92

Figure 7.1 The procedure for the data remanence experiment. The flow is repeated with increasing tDuntil all data are lost. 95

Figure 7.2 (a) The progression of data loss on the Cypress 150 nm sample. (b) Consistency of measurement procedure (c) The compilation of data remanence results 96

Figure 7.3 The compilation of data remanence results for the 90, 150, and 250 nm samples post irradiation. 97

Figure 7.4 (a) Node capacitance discharge model in SRAM cell (green indicating cell on condition and red indicating cell off condition), (b) Derivation of remanence time $\boldsymbol{trem}$ 99

List of Tables

Table 5.1 Summary of Chip Specification..64

Table 5.2 Summary of TID effects on SRAM-PUFs. 67

Table 5.3 Hspice Simulation Parameters. 71

Table 5.4 Summary of Chip Specification..75

Table 6.1 Summary of Imprinting on Multiple Chips. 93

Chapter 1. Introduction

1.1 Motivation

The catastrophic event at Chernobyl in 1986 highlighted a critical vulnerability in our technological advancements: the limitations of robotics in disaster management. **Figure 1.1**(a) shows the image of a failed moon rover that was used during the clean-up efforts after the catastrophe. While the moon rover in question was radiation-hardened to be able to function on the surface of the moon, the intensity of the radiation on the roof of reactor building 4 was far greater. The Chernobyl liquidators (**Figure 1.1**(b)) dubbed as "biorobots" [1] who were called upon to clean up the hazardous debris because the robots of the time failed, served as a poignant reminder of the need for robust technology that can withstand extreme conditions.

https://chernobylx.com/chernobyl-robots/

Figure 1.1 (a) Unresponsive moon rover which died after attempted use for Chernobyl disaster cleanup. b) "biorobots" with a 90 second timer cleaning up the disaster.

Moreover, the exponential growth in the deployment of commercial off-the-shelf (COTS) electronics in space applications has caused radiation effects research to gain great traction in recent years. The upward trajectory of nanosatellites and CubeSats launches, as depicted in the **Figure 1.2**, indicates a future heavily reliant on such technology. Small satellite constellations are poised to provide a global wireless internet system, with projections suggesting that over 100,000 satellites may encircle the Earth by 2030.

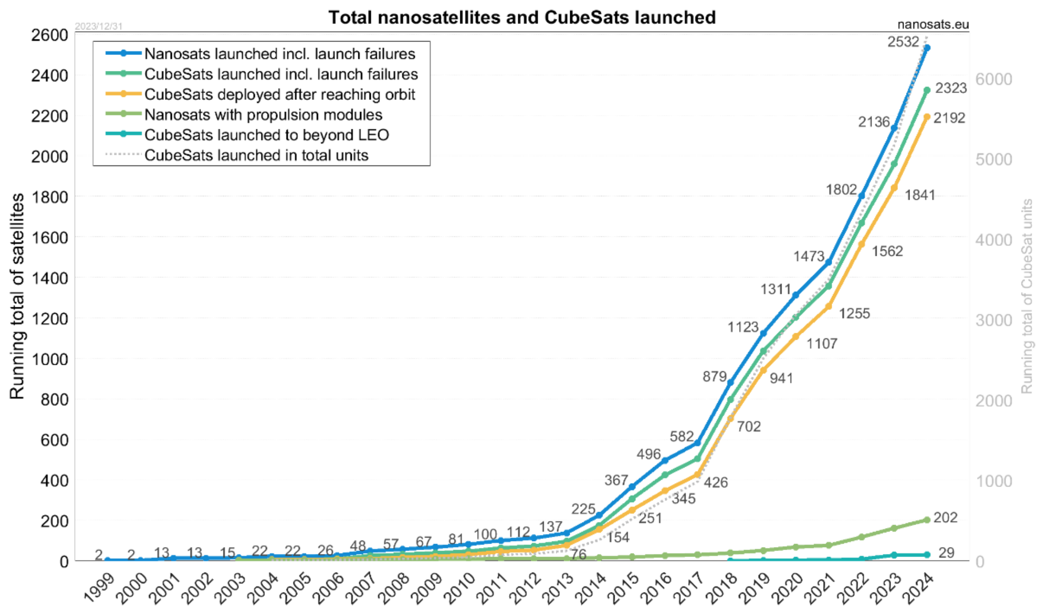


Figure 1.2 The rapid climb in number of nano and cube sats.

This presents a formidable challenge: ensuring the reliability of COTS electronics in the harsh environment of space, where radiation poses a significant threat to the integrity and longevity of semiconductor components. The motivation for my dissertation thus emerges from the intersection of historical lessons and the pressing technological needs of our expanding extraterrestrial ventures.

1.2 Key Contributions

The primary contributions of this dissertation are as follows:

1) We explore the total-ionizing-dose (TID) effects on modern multi-level cell (MLC) 3D NAND and find that the most significant bit (MSB) pages are more susceptible to radiation-induced charge loss than the least significant bit (LSB) pages. We present a physical model to understand the underlying mechanism. MSB pages are 20-50% more susceptible. We also find a layer dependence on the error ratio between MSB/ LSB pages. We find that errors are correlated, meaning that if an LSB page has errors, then the corresponding MSB page also has errors. We find that bit error locations in a byte are independent and uncorrelated, meaning there is no clustering of error bits, which is vital knowledge when it comes to designing error control codes (ECC).
2) We find that read noise is a big contributing factor to post-irradiation errors. We find read noise to be a strong function of TID. We find that one of the key contributing factors to the increase in read noise is the program state of the cells under irradiation. We present a mitigation strategy, where memory modules are primed with the initial data, as opposed to being left in a factory-erased state, before deploying them in a radiation-prone environment.

   We find that the total noise reduces as the samples anneal at room temperature, but they do not quite return to pre-irradiation conditions even after several months.
3) We find that TID significantly impacts the physical unclonable function (PUF) security aspect of static random-access (SRAM) memories. The degree of impact is a strong function of the dose. PUF hamming distance (HD) increases significantly with dose, and so does the number of unstable bits. Radiation may cause false negatives during PUF

authentication events. We propose a mitigation strategy to protect SRAM PUF under ionizing radiation. For PUF degradation, we find a strong dependence on the data pattern stored during irradiation. Depending on the manufacturer, storing either PUF data or inverted PUF data helps preserve the PUF under ionizing radiation. We also find that there is a strong dependence on technology node when it comes to SRAM PUF degradation under ionizing radiation.

4) We find that Ionizing radiation may be used to intentionally alter the natural PUF state of an SRAM array posing a significant security threat.
5) We also find that ionizing radiation may be used as a mitigation strategy against SRAM data remanence-style security attacks as it significantly reduces the data remanence time.

1.3 Dissertation Outline

This dissertation presents an analysis of Ionizing radiation effects in semiconductor memories, with a focus on TID effects on SRAM and NAND flash.

Chapter 2 provides a brief background on ionizing radiation, single event, and total ionizing dose effects in metal-oxide-semiconductor (MOS) devices, the fundamentals of SRAM operation, and the fundamentals of NAND flash operation and discusses the general direction of the research covered.

Chapter 3 presents the results of our work on TID effects on NAND flash memory. We present the hardware used in carrying out our research. We present the details of the irradiation environment and the samples we conduct our studies on. We then discuss in detail the radiation-induced error pattern analysis for modern 3D NAND Flash Memories.

Chapter 4 discusses the aspect of noise in memory transistors and how they are significant contributors to radiation-induced error. We also present a strategy for the mitigation of radiation-induced read noise.

Chapter 5 presents the results of our work on TID effects on SRAM PUF. We discuss the hardware setups used in our experiments and details of the samples used. We present the SRAM architecture. We discuss the mechanism of power-on states, how radiation affects PUF, and how to protect SRAM PUF from radiation-induced degradation. We also illustrate how the SRAM technology node plays a vital role in its PUF resilience towards ionizing radiation.

Chapter 6 presents some of the security holes in SRAM memories that are affected by ionizing radiation. First, we look at intentional radiation-induced SRAM PUF modification. We discuss the long-term impacts of the above mechanism.

Chapter 7 discusses another security attack called data remanence attack, how it scales with shrinking technology, and how ionizing radiation may be used as a mitigation strategy against data remanence style security attacks.

Finally, Chapter 8 concludes the dissertation along with some ideas for future works, and Chapter 9 presents a list of all the references.

Chapter 2. Background

This chapter discusses the fundamentals of ionizing radiation, radiation effects, the fundamentals of NAND flash, and SRAM memories.

2.1 Radiation Effects in Semiconductor Devices

Ionizing radiation is essentially very high-energy particles or electromagnetic radiation (photons) that have enough energy to ionize the material that it encounters. They may originate from several sources such as radioactive elements, from outer space, or manmade sources such as Bremsstrahlung radiation (X-rays).

High energy particles such as Alpha and Beta rays originate from nuclear decay. High-energy heavy ions are primarily found in galactic cosmic rays (GCR). Lower energy heavy ions including hydrogen ions (protons) and helium ions, may also come from coronal mass ejection (CME). The large, high-energy particles, moving at nearly the speed of light, can have devastating effects on semiconductor elements. Depending on their mass and velocity, their energies can range from GeV to as much as 10^8 TeV [2]

High energy photons such as gamma rays can be emitted by various astronomical phenomena, such as pulsars, quasars, supernova remnants, and gamma-ray bursts. X-rays are emitted by black holes, neutron stars, binary star systems, supernova remnants, and the hot gas in galaxy clusters, and even by our sun during solar flares. These high-energy photons can penetrate through a wide range of objects, so they pose a significant threat to microelectronic devices. An illustration of the penetrative capacity of various ionizing radiation is shown in **Figure 2.1**[3]. For

semiconductor radiation effects research, they may be broken down into two main categories: heavy ions causing single event effects (SEE) and beta electrons, X-rays, and gamma rays which cause total ionizing dose effects (TID).

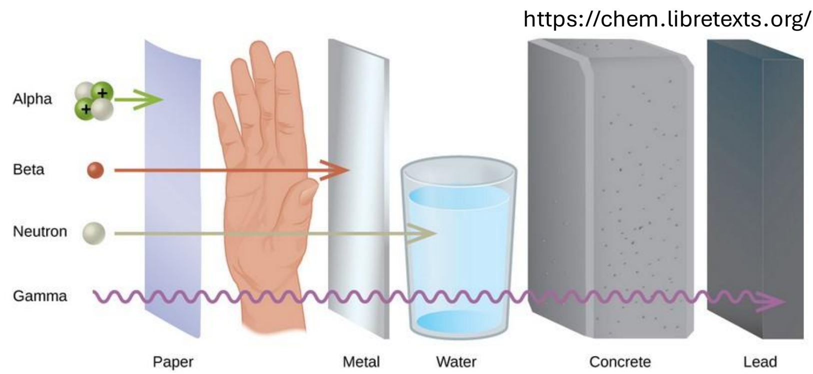


Figure 2.1 The penetration of different types of ionizing radiation.

2.1.1 Single Event Effects

Single event effects (SEE) are caused by high-energy particles (heavy ions). **Figure 2.2** illustrates the single-event mechanism. When an ionizing particle interacts with the silicon substrate, it can generate electron-hole pairs along its track. If this track is near a sensitive node of a memory cell or logic gate, it can temporarily flip its state. Upon an ionizing radiation event as depicted in **Figure 2.2**, a cylindrical track filled with high-density electron-hole pairs forms as illustrated in **Figure 2.3** (a).

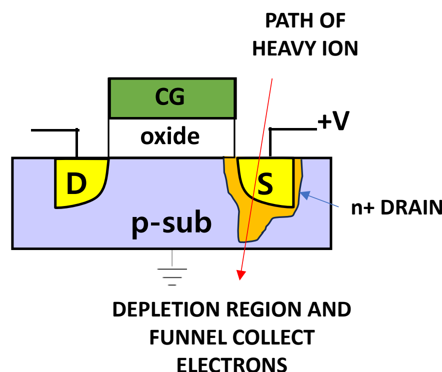


Figure 2.2 Heavy ion striking a sensitive node of a transistor.

The heavy ion track, when close to a depletion region, triggers a rapid collection of carriers by the electric field, causing a significant current/voltage transient. Simultaneously, the potential distorts into a funnel shape, enhancing drift collection by expanding the depletion region into the substrate (b), with the funnel size growing as substrate doping decreases. The swift "prompt" collection phase lasts a nanosecond, succeeded by a longer diffusion-dominated phase where additional charge is collected over hundreds of nanoseconds until equilibrium is restored (c). The current pulse profile resulting from these phases is also illustrated in **Figure 2.3**. The magnitude is not the only attribute of interest, but also the time duration during which the charge is accumulated [4]. This phenomenon can have several adverse effects:

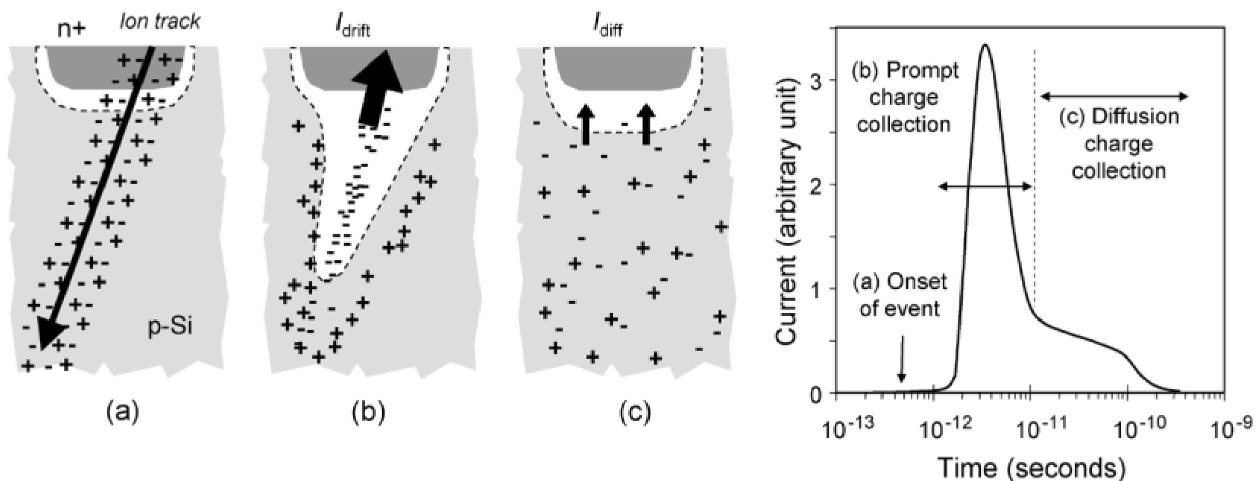


Figure 2.3 Charge generation and collection phases in a reverse-biased junction and the resultant current pulse caused by the passage of a high-energy ion [4].

1) Single Event Upset (SEU): If the ion track is near a sensitive node of a memory cell or logic gate, it can temporarily flip its state. This phenomenon is called SEU. While not permanently damaging, this can disrupt the FPGA's operation, especially if the upset occurs in a configuration memory cell [5].
2) Single Event Latchup (SEL): This effect is due to the triggering of parasitic bipolar structures (PNPN thyristor) within the CMOS technology. An energetic particle can create a current path, which may activate these structures, causing them to "latch" into a high-

current state. If not addressed, this can lead to thermal runaway and subsequent destruction of the affected region.

3) Single Event Transient (SET): When an energetic particle strikes a transistor, it can produce a temporary voltage spike (or glitch). For analog or mixed-signal circuits, this can cause brief erroneous outputs. In digital circuits, if the transient pulse is sufficiently long and reaches sequential elements like flip-flops, it can be captured and propagated, leading to functional errors.
4) Single Event Burnout (SEB): This catastrophic event occurs in power transistors. An energetic particle can create a localized region of high current density, leading to thermal feedback mechanisms that destroy the transistor.
5) Single Event Gate Rupture (SEGR): A high-energy particle can cause a strong local electric field in the gate oxide of a MOS transistor. If this field surpasses the oxide's breakdown strength, it can cause a rupture, leading to permanent device failure.

2.1.2 Total Ionizing Dose

Total Ionizing Dose (TID) refers to the cumulative impact of ionizing radiation on electronic devices, characterized by the accumulation of significant charges within the oxides and insulators that result from exposure to a total dose of ionizing radiation over time [6]. This branch often emphasizes the dose effects from sources that have substantial penetration, such as beta rays, X-rays, and gamma rays. The reason gamma rays have the most penetration is due to the fact that gamma photons are purely packets of energy causing them to interact less with the material they are passing through, while other particles such as alpha, beta, and heavy ions have significant volume that can interact more with the material and come to a stop. The mechanism of TID [6] is illustrated in **Figure 2.4**:

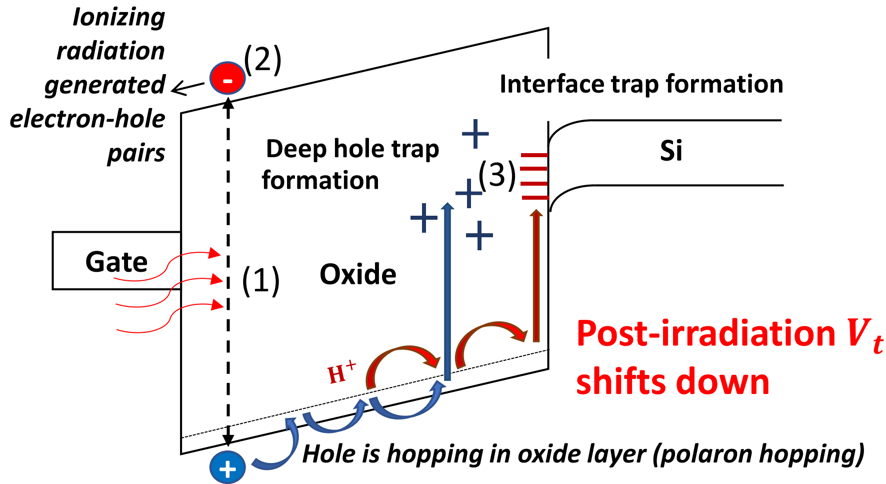


Figure 2.4 TID effects in MOS devices.

(1) Ionizing radiation causes electron-hole pairs. Some of the pairs recombine, while others do not.

(2) The fraction of electron-hole pairs that do not recombine is called the "charge yield". The electrons drift towards the gate and the holes drift towards the Oxide/ Silicon interface. Since the electrons are of higher mobility, they are quick to drift away, but the slower holes may remain trapped in the oxide.

(3) Holes trapped as positive charges in the oxide layer cause the reduction of the threshold voltage of the MOS device.

Charge yield is an important metric in TID effects and is described by the following equation:

$$N_h = f(E_{ox}) g_0 D t_{ox},$$

where $f(E_{ox})$ is the hole yield as a function of the oxide electric field, D is the dose measured in *rads(Si)*, t_{ox} is the thickness of the oxide layer, and $g_0 = 8.1 \times 10^{12}\ pairs\ per\ cm^3\ per\ rad\ for\ SiO_2$. Charge yield as a function of the electric field is

illustrated for various sources of radiation in **Figure 2.5**[6]. Essentially, the stronger the electric field, the lower the chances of recombination, and the higher the charge yield.

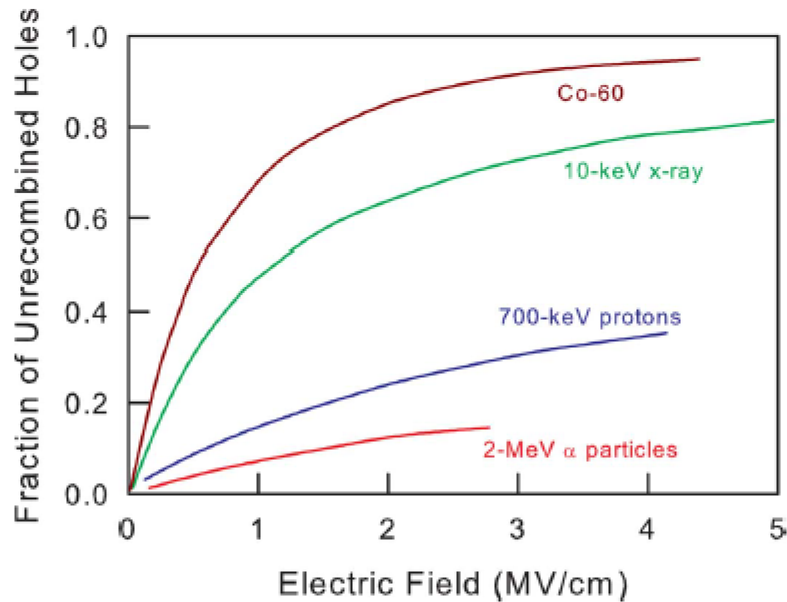


Figure 2.5 Charge yield for x rays, low-energy protons, gamma rays, and alpha particles [6].

2.2 SRAM Fundamentals

Static random-access memory (SRAM) is the fastest form of memory in a modern electronic device. It is composed of a flip-flop that retains the data as long as it remains powered on and will lose the data once powered off, making it a volatile memory. Unlike dynamic random-access memory, its static nature is due to the fact that it does not need to be refreshed periodically to retain data. Due to their high speed, they are integrated directly into CPU cache memory for computation, and the typical access times for read and write operations of modern SRAM are in the tens of nanoseconds. **Figure 2.6** shows a 6T SRAM cell. At its heart is a cross-coupled inverter pair ($P_1 - N_1$, and $P_2 - N_2$) that can either store a 0 or a 1. It has two access transistors that enable reading from and writing to the cell. Once written, the data will remain stored as long as the cell remains powered on. While SRAM memory is very fast, the total memory capacity is rather low

due to its large footprint (six transistors). The evolution of SRAM cell size as illustrated in **Figure 2.7** has been following Moore's scaling trend closely. [7].

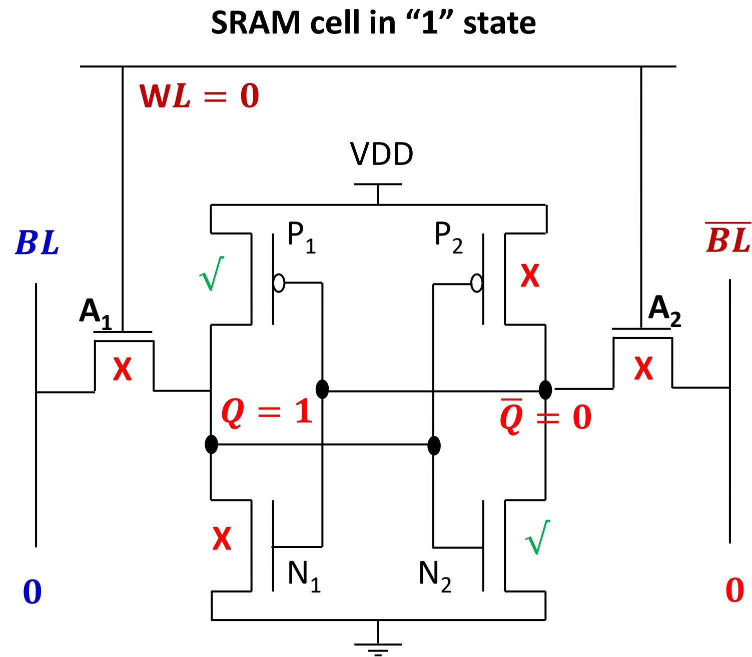


Figure 2.6 6T SRAM cell.

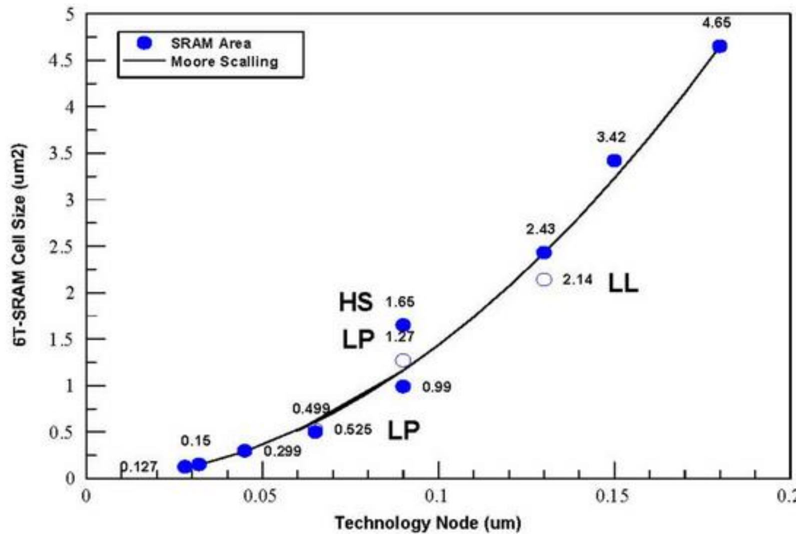


Figure 2.7 6-T SRAM Bit-Cell area trend, used by pure-player foundries. The data refer to SRAM used in Standard Logic for General Purpose technology, unless indicated differently: HS = High-Speed, LP = Low power and LL = Low Leakage [7].

2.2.1 SRAM Cell Read Operation

For illustrating the SRAM read operation, let's assume the cell is in a $\boldsymbol{Q = 0}/\ \boldsymbol{\overline{Q} = 1}$ state as shown in **Figure 2.8**. To read the contents of the cell, the bitlines $\boldsymbol{BL}/\ \boldsymbol{\overline{BL}}$ are both precharged to a logic **"1"** state (high voltage), and then the $\mathbf{W}\boldsymbol{L}$ is set to logic **"1"**. Driving the $\mathbf{W}\boldsymbol{L}$ high causes the access transistors $A_1$and A_2 to turn on. Since $N_1$is on ($\boldsymbol{\overline{Q} = 1}$), It will cause $\boldsymbol{BL}$ to discharge. The bitlines are sensed by a sense amplifier that can detect small changes in voltage. As $\boldsymbol{BL}$ starts to discharge to **"0"** (ground), the sense amplifier will produce the output **"0"** from the read operation.

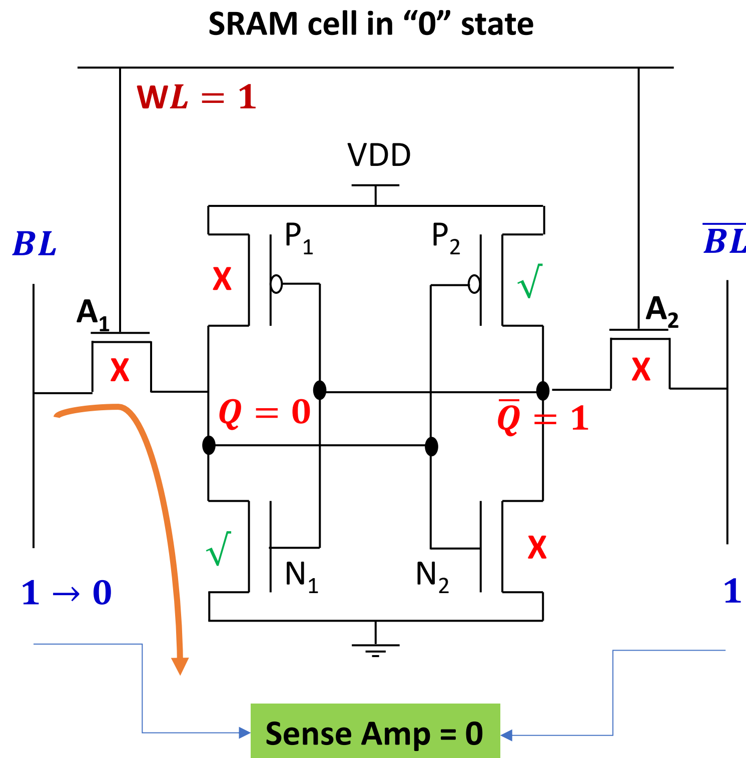


Figure 2.8 SRAM cell read operation.

2.2.2 SRAM Cell Write Operation

For illustrating the SRAM write operation, let's assume the cell is in a $\boldsymbol{Q = 0/\bar{Q} = 1}$ state as shown in **Figure 2.9**. To write **"1"** onto the cell, *i.e.*, to make $\boldsymbol{Q = 1/\bar{Q} = 0}$ the bitlines $\boldsymbol{BL}$ is set to logic **"1"** (high voltage) and $\boldsymbol{\overline{BL}}$ is set to **"0"** (ground) and held until the write operation is completed. Then the $\mathbf{W}\boldsymbol{L}$ is set to logic **"1"**. Driving the $\mathbf{W}\boldsymbol{L}$ high causes the access transistors $A_1$and A_2 to turn on. It will cause $\boldsymbol{BL}$ to charge $\boldsymbol{Q\ to\ 1}$ while $\boldsymbol{\overline{BL}}$ discharges $\boldsymbol{\bar{Q}\ to\ 0}$**.** The bitlines essentially overpower the cell state to a **"1"** causing transistors $P_2 - N_1$ to turn off and, and $P_1 - N_2$ to turn on. The write operation hence completes and the cell can hold this state as long as it remains powered on.

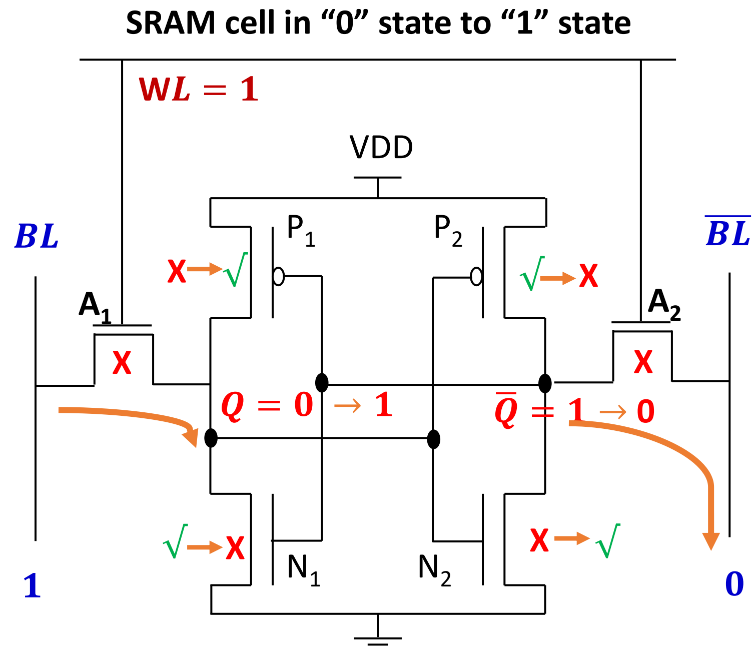


Figure 2.9 SRAM cell write operation.

2.2.3 SRAM Cell Transistor Sizing Constraints

In a conventional CMOS inverter, the PMOS is wider than the NMOS. This is to account for the lower mobility of holes (the PMOS majority carrier) compared to electrons (NMOS

majority carrier), so to balance the drive strengths, the PMOS is made wider. In the case of an SRAM cell, the design constraints are different. The sizing constraint is described in **Figure 2.10**.

1) During the read operation, the inverter states must not change, *i.e.*, to avoid inadvertently writing data while reading. For instance, in **Figure 2.8**, the access transistor $\boldsymbol{A_1}$ should be weaker than $\boldsymbol{N_1}$, otherwise, $\boldsymbol{Q}$ will flip to **"1"**.

2) During the write operation, the inverter states need to change. So, in **Figure 2.9**, if $\boldsymbol{P_2}$ is stronger then $\boldsymbol{A_2}$ then while $\boldsymbol{A_2}$ is trying to discharge $\overline{\boldsymbol{Q}}$ to "0", $\boldsymbol{P_2}$ will constantly keep charging the node $\overline{\boldsymbol{Q}}$. To avoid that, we need to ensure $\boldsymbol{A_2}$ is stronger than $\boldsymbol{P_2}$.

In summary, the pull-down NMOSs should be stronger than the access transistors, and the pull-up PMOSs should be weaker than the access transistors.

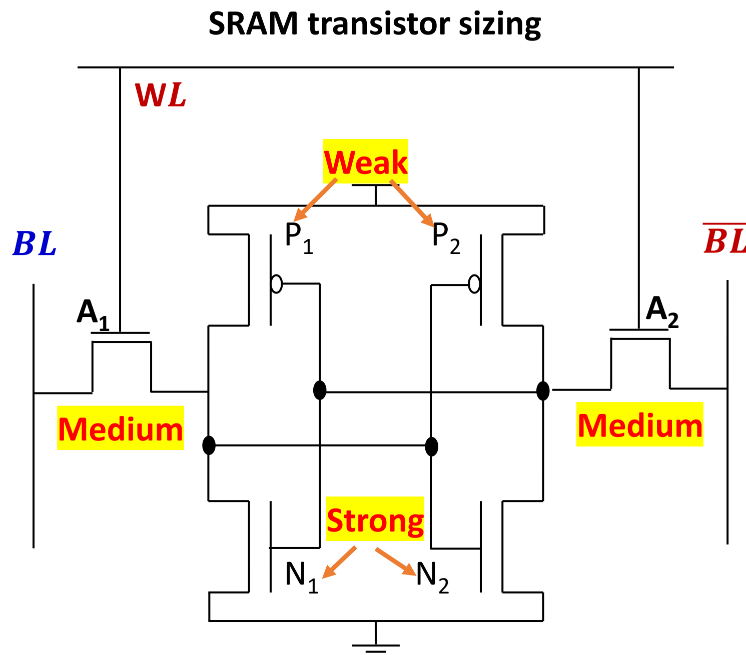


Figure 2.10 SRAM cell transistor sizing constraint.

2.2.4 SRAM Array Architecture

An SRAM chip contains an array of memory cells as shown in **Figure 2.11**. The chip with n address inputs and 2^m data lines is seen logically as an array of $2^n \times 2^m$ cells. For chip floor planning reasons, the array is physically organized into $2^{n-k} \times 2^{m+k}$ cells and an additional column decoder is used to select a word from the selected row. In addition to address and data pins, an SRAM chip has control inputs for controlling read and write operations. To read from SRAM, bitlines are pre-charged and the selected wordline is turned on. One of the two column bitlines will be pulled down by the cell and that is sensed by the corresponding column circuitry. To write to SRAM, the bitlines are driven based on the content from data pins (*e.g.*, BL=1, $\overline{BL}$=0) and the word line is turned on. The bitlines overpower the selected cells, thus writing a new value.

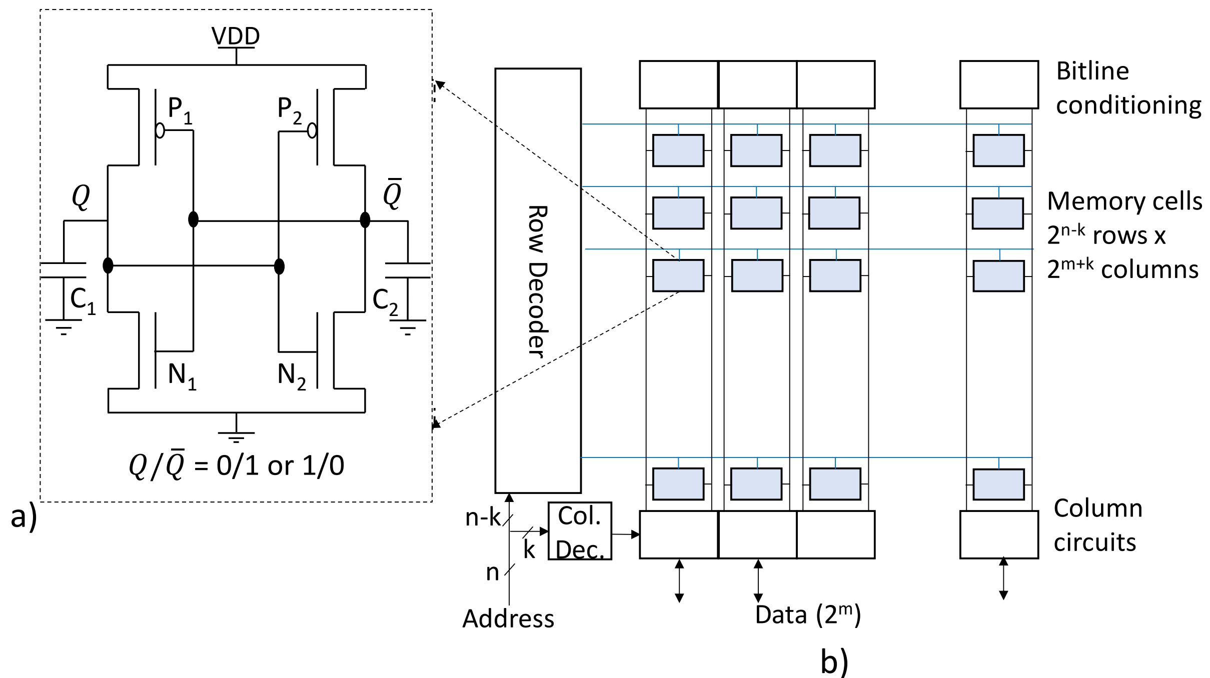


Figure 2.11 SRAM (a) cell and (b) array architecture.

2.3 NAND Flash Fundamentals

In the past couple of decades, the data density of storage media has steadily increased (**Figure 2.12** [8]). We have switched from magnetic storage media (hard disk drives) to semiconductor memory (solid state drives) since it's orders of magnitude faster and consumes a lot less power. The primary driving factor behind this growth is NAND flash memory. **Figure 2.13** shows the structure of a NAND flash memory cell. Essentially, one transistor can store one or more bits of information. NAND flash memory achieves this through a simple modification to the standard MOSFET by adding a charge storage layer (in our case a floating gate) sandwiched between two oxide layers. The data stored in the form of charge on the floating gate will remain stored for several years. Flash memory has scaled to the point where we can store terabytes of data on an inexpensive microSD card the size of a fingernail. For this reason, flash memory has become the most ubiquitous form of memory.

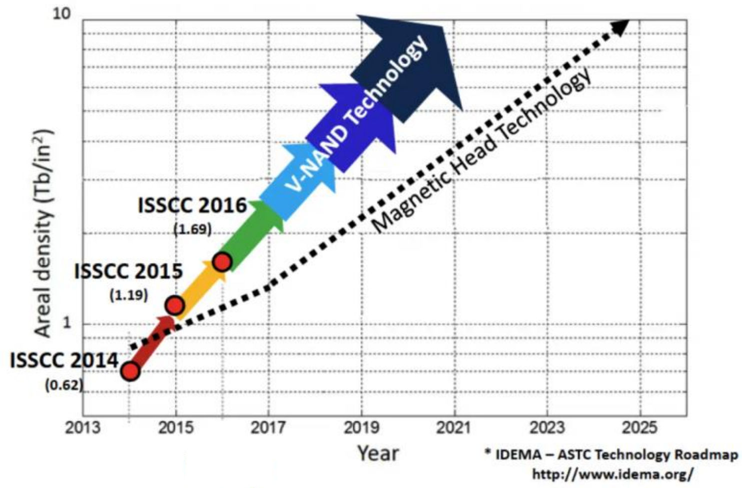


Figure 2.12 NAND Storage density progression over the years.

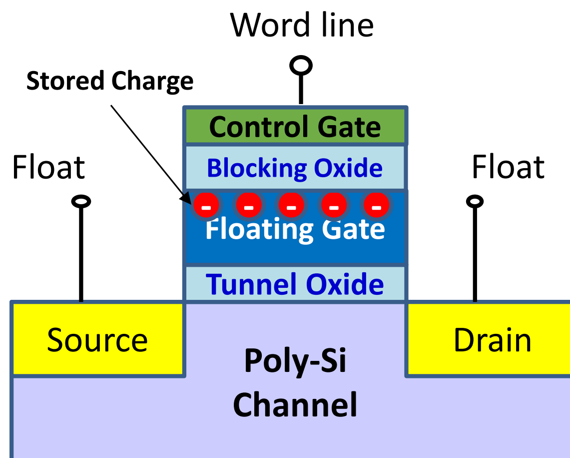


Figure 2.13 Floating gate NAND flash memory cell.

2.3.1 Erase/ Program Operation on Flash Memory

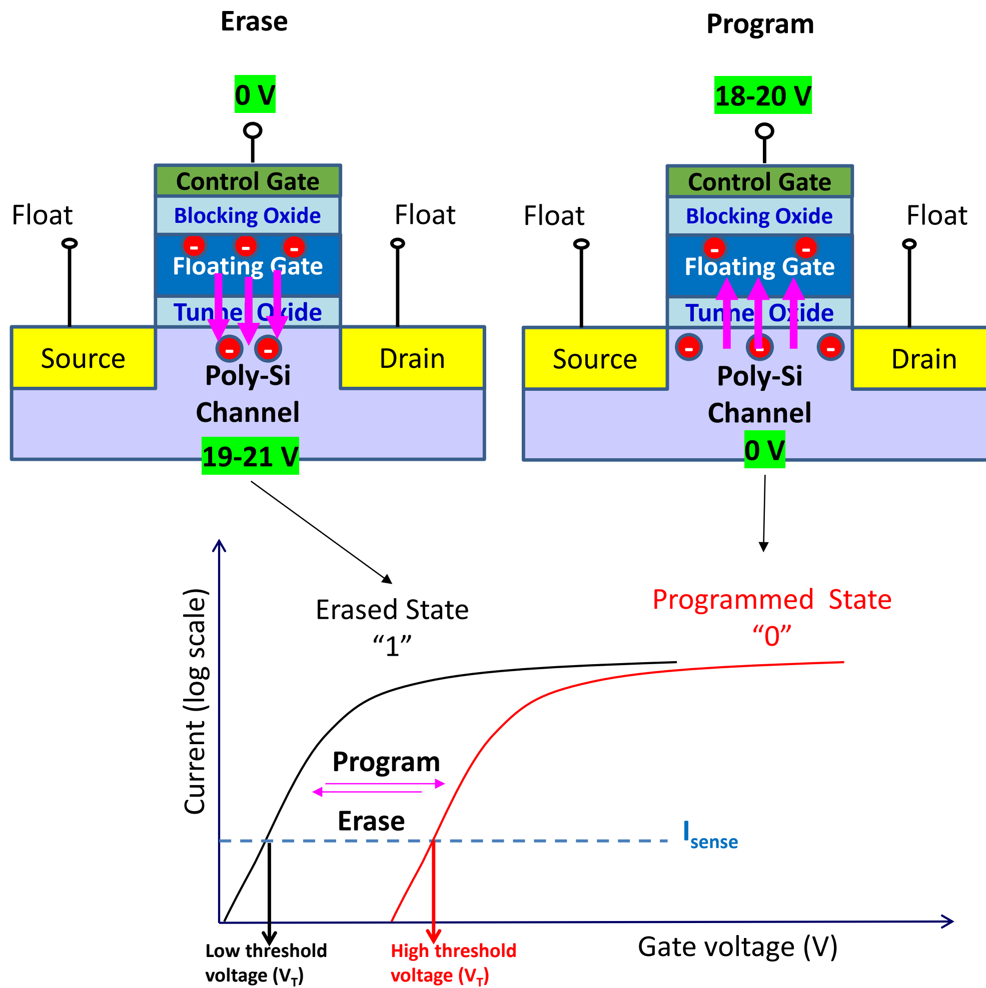


Figure 2.14 Flash program/ erase operation and the corresponding change in cell V_t (and hence drain current).

The write and erase processes work through a quantum-mechanical tunneling process commonly referred to as *Fowler–Nordheim* (FN) tunneling. Tunneling is possible because electrons have wave-like properties so that they can penetrate regions where they are classically forbidden (because they lack sufficient energy). If the region is sufficiently thin or transparent (the high electric field increases transparency) the electrons can tunnel through it. Essentially, charge can be moved into or moved out of the floating gate, via the tunnel oxide, using a strong electric field. The procedure for program and erase is illustrated in **Figure 2.14**. To program the flash cell, we need to move charge from the substrate to the floating gate. A high voltage (18-20

V) is applied to the gate while the substrate is grounded. This will pull electrons into the floating gate through FN tunneling. Adding electrons to the floating gate will result in an increase in cell threshold voltage V_T and the magnitude of change in threshold voltage can be described as $\boldsymbol{\Delta V_T} = \frac{-\Delta Q_{FG}}{C_{ONO}}$ where $\boldsymbol{\Delta Q_{FG}}$ is the charge on the number of electrons, and $\boldsymbol{C_{ONO}}$ is the capacitance of the blocking oxide. To erase the flash cell, *i.e.*, to remove charge from the floating gate, a high voltage (19-21 V) is applied to the substrate to pull the electrons out of the floating gate into the substrate through the same process of FN tunneling. Removing electrons from the floating gate will result in a decrease in cell threshold voltage V_T.

2.3.2 NAND Read Operation

A group of NAND memory cells will have small differences in V_T. A sample V_T distribution is shown in **Figure 2.15**. A reference voltage V_{ref} is applied to the gate of the memory cell. If the cell turns on (implying that its V_T is less than the V_{ref}) then the cell is in an erased state, *i.e.*, logic-1. If the cell does not turn on, then its V_T is greater than V_{ref}, meaning it's in the programmed (logic-0) state.

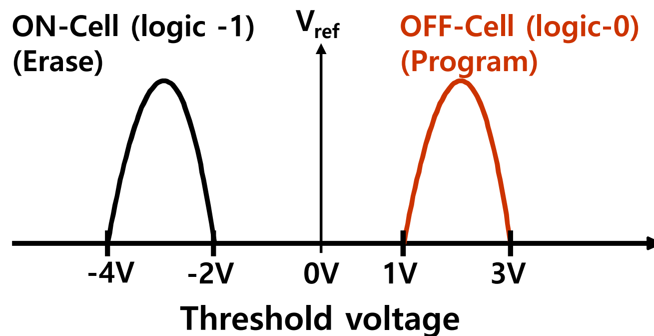


Figure 2.15 NAND flash memory sample V_T distribution.

Note: While both SRAM and NAND flash memories are affected by both SEE [4], [9], [10], [11] and TID, this dissertation focuses primarily on TID effects.

2.3.3 MLC NAND Flash Architecture

The illustrations so far were for a single level cell (SLC) which stores one bit of information per cell. In the multi-level cell (MLC) NAND flash memory, each memory cell holds two bits of information. Hence the memory cells in MLC NAND have four different logic states. The four logic states corresponding to MLC NAND are illustrated in **Figure 2.16**. Since each memory cell stores 2 bits of information, there are two logical pages sharing the same word line. The most significant bit (MSB) of the logic states of all the memory cells connected to a given word line forms the logical MSB page and the least significant bit (LSB) of the logic states of the memory cells from the same word line forms the logical LSB page. **Figure 2.16** also illustrates the corresponding program levels for triple-level cell (TLC) and quadruple-level cell (QLC) which will have three and four logical pages per wordline respectively.

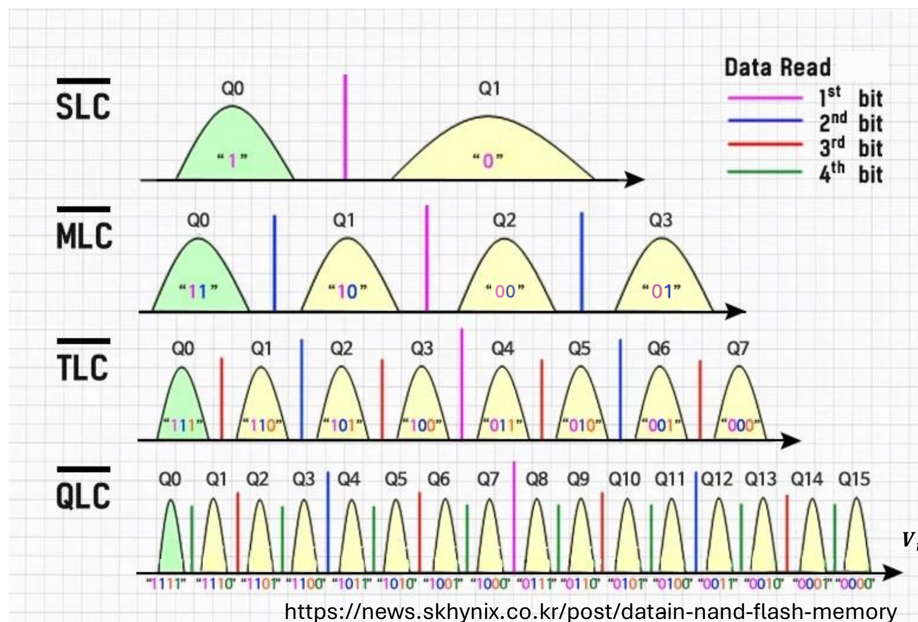


Figure 2.16 NAND configurations and the corresponding read reference targets for each bit.

The logic state of a memory cell is decided by its analog threshold voltage, V_t, which is controlled by charge injection on the floating gate during program operation. Let us consider the MLC NAND

having four distributions Q0-Q3 as shown in **Figure 2.16** which represent the analog threshold voltage distributions corresponding to the different logic states. There are variations in the analog V_t values of the cells representing a given logic state. Several physical reasons including program noise, cell-to-cell process variation, and read noise are responsible for the cell V_t variation. Hence the cells corresponding to a given logic state show a distribution of V_t values, instead of a singular threshold voltage value. In addition, **Figure 2.16** shows the different reference voltages (represented by different colors for each bit) which are used to decide the logic state of a cell. In the case of MLC NAND, there is only one reference voltage required to read the LSB page bits (pink), whereas two reference voltages are needed for the MSB page read (blue) [12]. Note that the transition from the highest V_t state to the adjacent one (from Q3 to Q2) will cause a failure in the MSB page but not in the LSB page. Similarly, the transition from state Q2 to Q1 will result in a failure in the LSB page but not in the MSB page. Since the highest V_t state loses charge more quickly than the other states during TID irradiation [13], [14], we expect to find more failures in MSB pages compared to the corresponding LSB pages. As we attempt to increase the number of bits per cell (SLC - MLC - TLC - QLC) the number of corresponding distributions increases as 2^n (where n is the number of bits per cell). The greater number of distributions we try to fit within a given voltage range, the closer the distributions are to each other, and the closer the distributions are, the greater the chances of their tails collapsing on each other causing increased chances of bit errors. In essence, the higher the bits per cell, the lesser its reliability due.

The details on the 3-D NAND fabrication process and cell structure are as follows: **Figure 2.17**(a) shows the circuit diagram of the memory cell arrangement in a NAND flash memory block. Each memory block consists of a fixed number of memory pages. The cells in each memory page are electrically connected through a metal word line (WL). WL acts as the control gate of

memory cells. Each column (or string) of cells in a block is connected to a different bit line (BL). Memory-read and program operations are performed at the page granularity, while erase is performed at the block granularity. Any flash cell that is set to a logic '0' by a program operation on a page can only be reset to a logic '1' by erasing the entire block. Depending on the cell configuration, each wordline may correspond to more than one logical page as described in the previous section.

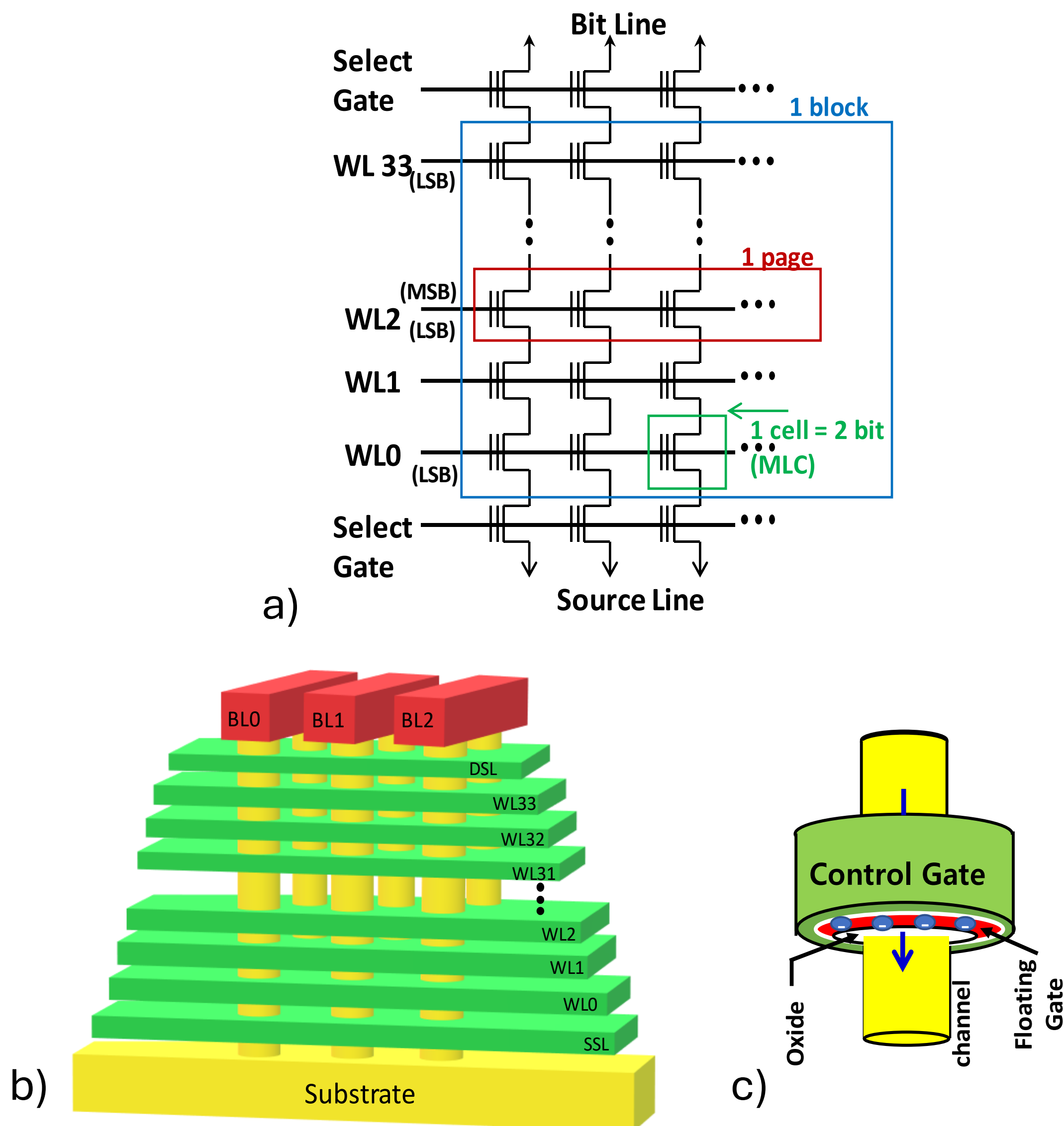


Figure 2.17 (a) Circuit diagram of a NAND memory block, (b) Physical diagram of 3D NAND flash memory array, (c) Schematic of a 3-D NAND flash memory cell.

Figure 2.17(b) shows the physical structure of the 3-D NAND memory array. The green layers are the wordlines and the vertical pillars are memory holes that contain the channel of the flash memory cells, and the red slabs are the bit lines. **Figure 2.17**(c) shows the device structure of a 3-D NAND flash memory cell, which is essentially a gate-all-around MOSFET (Metal Oxide Semiconductor Field Effect Transistor) with a floating gate. The 3D NAND fabrication involves the deposition of alternate metal and oxide layers. The channel of a hole is formed through the process of reactive ion etching (RIE). The gate stack (blocking oxide – floating gate – tunnel oxide) of the cells is formed by sequentially depositing blocking oxide (oxide – nitride – oxide), then the floating gate (or a charge trap layer), then the tunnel oxide along the sidewall of the cylindrical trench, and finally a thin layer of poly-Si channel [15]. RIE is not a perfect process. As the etching takes place from top to bottom, the width of the etch reduces as we move down the layers. Hence, the top layers of memory cells have a larger diameter compared to the bottom layers as shown in **Figure 2.18** [15].

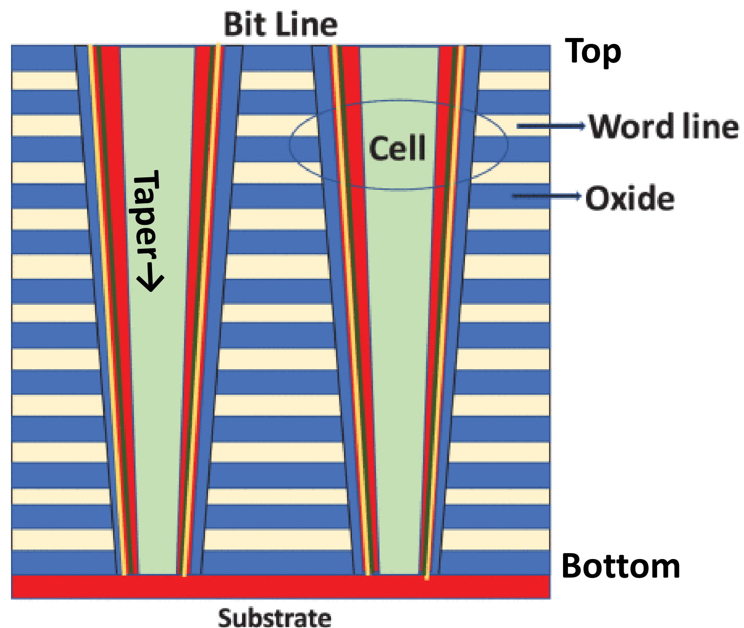


Figure 2.18 Tapered structure of 3D NAND due to inefficient RIE process [15].

Chapter 3. TID Effects on Bit Error Pattern in MLC NAND Memory

3.1 Introduction

The radiation tolerance characteristics of commercial off-the-shelf (COTS) 3-D NAND flash is a topic of great interest for both defense and the space industry [16]. While 3-D NAND offers high-density, high-capacity, and low-cost storage solutions in a small form factor, it suffers from radiation-induced data corruption issues [14], [17], [18], [19]. For a given technology node, a higher data corruption rate is observed as we go from a single-level cell (SLC) to a multi-level cell (MLC) and triple-level cell (TLC) NAND [20]. However, in terms of bit density and cost, TLC and MLC memory chips are more attractive compared to SLC memory [21]. Since MLC NAND provides a good balance between density and radiation reliability [14], there is a great economic interest in using MLC NAND instead of SLC NAND in low/moderate radiation environments (*e.g.*, Low-Earth-Orbit satellites).

In the MLC NAND flash memory, each memory cell holds two bits of information. Hence the memory cells in MLC NAND have four different logic states. We illustrate the four logic states using four different flash memory cells in **Figure 3.1**(a). **Figure 3.1**(a) illustrates the arrangement of memory cells connected to a given word line. There are thousands of memory cells connected to the same word line. The number of memory cells belonging to a given word line determines the logical page size of the memory chip. Since each memory cell stores 2 bits of information, there are two logical pages sharing the same word line. The most significant bit (MSB) of the logic states of all the memory cells connected to a given word line forms the logical

MSB page. Similarly, the least significant bit (LSB) of the logic states of the memory cells from the same word line forms the logical LSB page. The details of the logical addresses for the shared pages are provided in the datasheet of the corresponding chip.

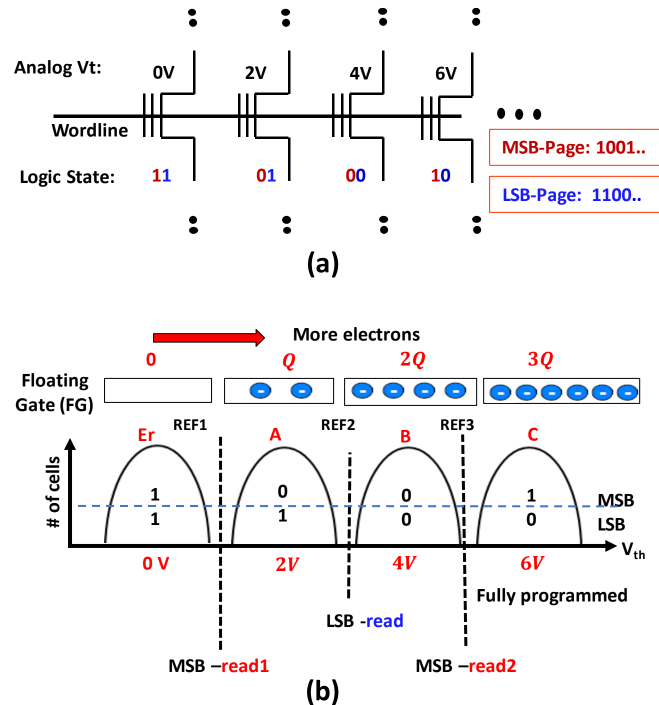


Figure 3.1 (a) Arrangement of NAND flash memory cells connected to a single word line. (b) Cell threshold voltage distribution for MLC NAND.

The logic state of a memory cell is decided by its analog threshold voltage, V_t, which is controlled by charge injection on the floating gate during program operation. **Figure 3.1**(b) shows the representative analog threshold voltages corresponding to the four different logic states. There are variations in the analog V_t values of the cells representing a given logic state. Several physical reasons including program noise, cell-to-cell process variation, and read noise are responsible for the cell V_t variation. Hence the cells corresponding to a given logic state show a distribution of V_t values, as illustrated in **Figure 3.1**(b). In addition, **Figure 3.1**(b) shows three different reference voltages which are used to decide the logic state of a cell. There is only one

reference voltage required to read the LSB page bits, whereas two reference voltages are needed for the MSB page read [12]. Note that the transition from the highest V_t state to the adjacent one (from C to B) will cause a failure in the MSB page but not in the LSB page. Similarly, the transition from state B to A will result in a failure in the LSB page but not in the MSB page. Since the highest V_t state loses charge more quickly than the other states during TID irradiation [13], [14], we expect to find more failures in MSB pages compared to the corresponding LSB pages.

Several interesting works have been done on the radiation effects on MLC 2-D NAND for both single event effects (SEE) and total ionizing dose (TID) response [22], [23], [24], [25], [26], [27]. Previous studies demonstrated that MLC NAND is more susceptible to data corruption compared to SLC NAND. Additionally, Gerardin *et al*. [27] showed that all the program states of MLC NAND incur bit errors by performing TID-induced error analysis in 25 nm 2-D MLC NAND flash from Micron. Ingalls *et al*. [23] showed a novel method of using logical decode to convert MLC NAND to SLC-like memory to increase its radiation tolerance. Unfortunately, the logical decode method does not apply to the state-of-the-art 3-D MLC NAND as modern MLC chips use internal data randomization before writing user data on the memory array. Most of the previous studies on MLC NAND were done on 2-D NAND technology which is fundamentally different than the 3-D NAND technology. Thus, it is very important to analyze the radiation susceptibility of MLC memory for 3-D NAND technology before it is adopted for high-density data storage applications in a radiation-prone environment.

In this chapter, we perform radiation-induced error analysis of COTS 3-D MLC NAND memory from Micron technology. Special emphasis is given to the relative radiation tolerance characteristics of LSB and MSB pages of the MLC memory. We analyze the TID-induced error characteristics on 6 different 3-D NAND chips of the same specifications to make

our conclusions statistically robust. The experimental set-up, chip specifications, measurement procedure, gamma irradiation conditions, and the data collection method are discussed in the following sections.

3.2 Experimental Setup and Procedure to Study Radiation Effects in NAND Flash

3.2.1 Hardware Setup

To interface the raw NAND chip with the computer, we used a custom-designed hardware board as shown in **Figure 3.2**. The board includes a socket to insert the NAND flash chip and an FT2232H mini module from Future Technology Devices International (FTDI) [28] to interface the memory chip with a computer through a Universal Serial Bus (USB) connection. The FT2232H mini module enables the USB to Universal Asynchronous Receiver/Transmitter (UART) interface. The logic analyzer is used to acquire the read/ busy pin to monitor the status of the chip when required. The hardware setup allowed us to access the raw memory bits without any error correction. The hardware setup was not exposed to gamma radiation. It was only used to write/read the memory chips that were irradiated. Before sending the chips for radiation exposure, we wrote a known random data pattern on four to six memory blocks in each chip. We read all the blocks immediately after writing the data. We then exposed the NAND memory chips to gamma radiation. Finally, we read the data from the corresponding memory blocks and then computed the failed byte count (FBC). The time gap between data write and irradiation was 3-4 hours and the time gap between irradiation and data read was around an hour. We monitored a reference (un-irradiated) chip, to observe any data retention related errors and we found little to no increase in FBC within a week's time frame.

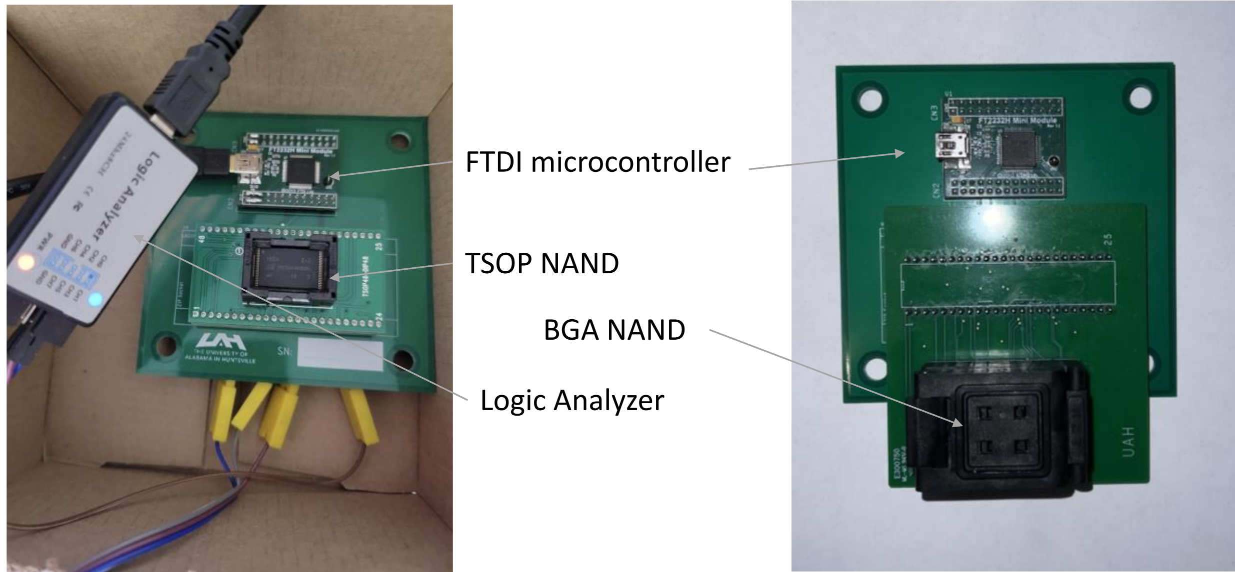


Figure 3.2 Custom hardware based on FTDI controller featuring a TSOP socket (left) and BGA socket (right).

3.2.2 Sample Details

A general overview of 3D NAND flash architecture is presented in 2.3.3. We used COTS NAND flash memory chips from Micron Technology for evaluating the radiation response. The part number for the 3-D NAND memory chips was MT29F256G08CBCBBWP-10: B, which were 256 Gb MLC memory chips from Micron. Six different chips were used to improve statistics. Each 3-D memory chip contains 2192 logical blocks, where each block consists of 1024 logical pages of size 18,592 bytes (16,384 bytes of user data with 2208 bytes of error correction codes). The logical pages of a 3-D NAND memory block are distributed across the vertical layers of the 3-D structure. Ideally, each vertical layer should hold 32 logical pages if the pages are uniformly distributed across the 32 physical layers (total 1024 pages per block). However, according to the datasheet [29], the chip under test has a non-uniform page distribution, especially on the edge layers (top two and bottom two layers) as illustrated in **Figure 3.3**. **Figure 3.3** shows the layer-

dependent page distribution for a specific sub-block structure (there are a total of 16 identical sub-blocks in a memory block) in the memory array, and **Figure 3.3** shows the shared and unshared page structures for the 34 different layers. Note that of the 34 physical layers in the 3-D stack, the bottom, as well as the top two layers, have non-shared memory pages, similar to SLC technology. In other words, the edge layer memory pages operate as SLC storage, while the remaining 30 layers operate as MLC storage. Since the manufacturer is aware of the intrinsic reliability issues on the edge layers, they designed the edge layers to operate in SLC type memory storage, which is fundamentally more robust compared to MLC storage.

Layer # 33	—	SLC
Layer # 32	—	SLC
Layer # 31	MSB	LSB
Layer # 30	MSB	LSB
	MSB	LSB
⋮	⋮	⋮
	MSB	LSB
	MSB	LSB
Layer # 3	MSB	LSB
Layer # 2	MSB	LSB
Layer # 1	—	SLC
Layer # 0	—	SLC

Figure 3.3 Logical (LSB and MSB) page distributions across different vertical layers of 3-D NAND.

3.2.3 Gamma-Ray Irradiation

The flash memory chips were irradiated using Co-60 sources to evaluate their TID response. The irradiation was carried out at Sandia National Laboratories Gamma Irradiation Facility [30]. The chips received a TID up to 20 krad(Si) at a dose rate of 18.5 rad(Si)/s. If not otherwise stated, all doses in the following are expressed as absorbed dose in silicon. Gamma

irradiation was performed on the packaged devices (TSOP) with the pins grounded. The unpowered state is a common use condition for non-volatile memories, which are designed to retain data without any external power. The unpowered state irradiation ensures minimal damage to the peripheral circuitry (*e.g.*, charge pump) of the chip, which allows us to explore radiation effects mainly on the memory cells. The direction of gamma rays during irradiation was perpendicular to the flat surface of the chip. The entire chip in unlidded condition went through gamma irradiation.

3.3 Experimental Results and Discussion

We have performed the FBC analysis for the 3-D MLC NAND chip following gamma irradiation. Data are read from the chip byte by byte and are compared to the original random data pattern to determine the FBC. In the following sections, we compare the FBC from LSB and MSB pages for different gamma-ray exposure conditions.

3.3.1 Comparison of LSB-MSB Pages Before Irradiation

First, we compare the FBC in the LSB and MSB pages for the pre-irradiation condition. **Figure 3.4**(a) shows the FBC on 1024 logical pages of a given memory block just after writing data, and **Figure 3.4**(b) shows the corresponding frequency plot. The frequency polygon plot in **Figure 3.4**(b) illustrates the histogram representation for the number of pages having a fixed FBC given on the x-axis. For the clarity of comparison, we do not show the histogram bars. Instead, we construct the frequency polygon plot using the bin centers and the page count in that bin for the corresponding histogram. The blue dots in the figure correspond to LSB pages whereas the red dots are for MSB pages. We find that FBC is very low (FBC < 5 per 18 kilobytes) in all the pages before radiation exposure. The few errors observed before irradiation are inherent in high-density

MLC NAND due to read-noise [31] associated with very minimal voltage margins between the programmed states. We did not observe a significant difference between the FBC of LSB and MSB pages before irradiation. The inherent FBC remains almost the same or slightly increases over the period of a few months while kept at room temperature.

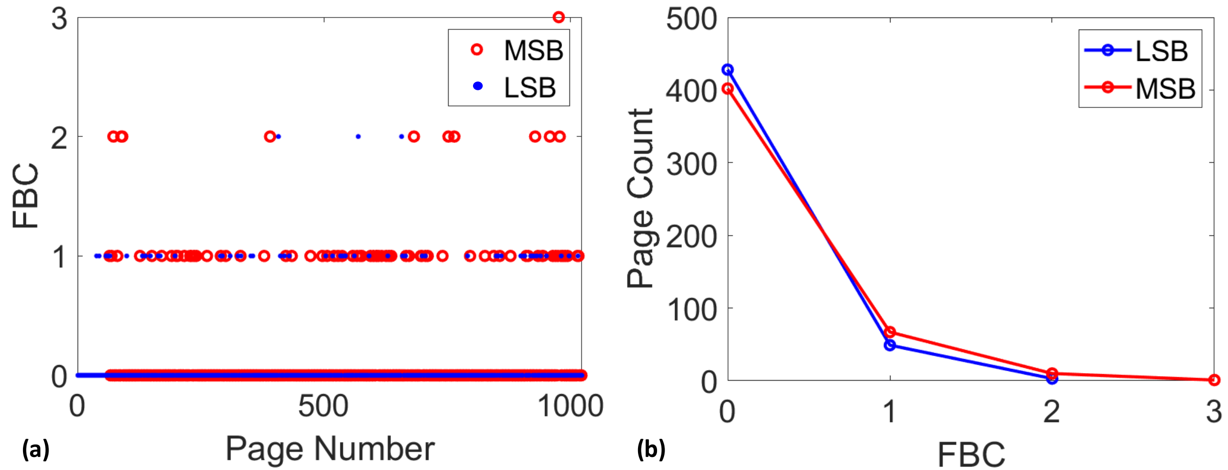


Figure 3.4 (a) FBC comparison between LSB (blue symbols) and MSB (red symbols) pages before radiation exposure. (b) The frequency polygon for MSB and LSB FBC for all pages in a block.

3.3.2 Post-Irradiation FBC Comparison of LSB and MSB Pages

In this section, we compare the FBC in the LSB and MSB pages on the irradiated chip. **Figure 3.5**(a) through (f) summarizes the experimental results; the plots (a) through (c) show the results for TID of 10 krad(Si), while the plots (d) through (f) represent the same parameters for TID of 20 krad(Si). In **Figure 3.5**(a), we plot the FBC of the LSB (blue symbols) and MSB (red symbols) pages of the same memory block after 10 krad(Si) of TID exposure. We find that the MSB pages consistently incur slightly higher FBC compared to the corresponding LSB pages. To make the comparison statistically meaningful, we show the frequency plot of FBC distribution

corresponding to the LSB and MSB pages in **Figure 3.5**(b). We find the mean FBC for the MSB pages to be 14.86 with a standard error of 0.44 and the LSB pages with a mean of 10.09 and a standard error of 0.33. Next, we compare the FBC of the LSB page and the corresponding MSB page using the correlation plot in **Figure 3.5**(c). Note that every LSB page has a unique MSB page sharing the same memory cells. The correlation plot of **Figure 3.5**(c) clearly shows that FBC is strongly correlated, with a correlation coefficient of 0.70, between the two page types, with greater than 99.99% confidence. In **Figure 3.5**(d), we compare the FBC on LSB and MSB pages for a higher TID of 20 krad(Si). The MSB pages have a mean FBC of 251 with a standard error of 6.16, compared to a mean of 218.7 for the LSB pages with a standard error of 3.7. As before, the FBC on MSB pages remains higher (**Figure 3.5**(e)) and is significantly correlated with that of the corresponding LSB pages (**Figure 3.5**(f)), with a correlation coefficient of 0.69, with greater than 99.99% confidence. The FBC correlation implies that if an LSB page is erroneous, the corresponding MSB pages will also be erroneous to a similar degree.

Another interesting observation, shown in **Figure 3.6**, is the FBC ratio between MSB and LSB pages. We find that the FBC values between MSB and LSB pages are not only correlated but also maintain an average ratio in the range of 1.2 - 1.5. **Figure 3.6** shows the frequency plot of MSB/LSB FBC ratios obtained from 6 different chips; three chips received the TID of 10 krad(Si), and the other three chips received the TID of 20 krad(Si). We find that the average FBC ratio between MSB and LSB pages remains in the range of 1.2 - 1.5 across different chips. Thus, we confirm that multiple chips show similar behavior with respect to LSB and MSB page failures under ionizing radiation.

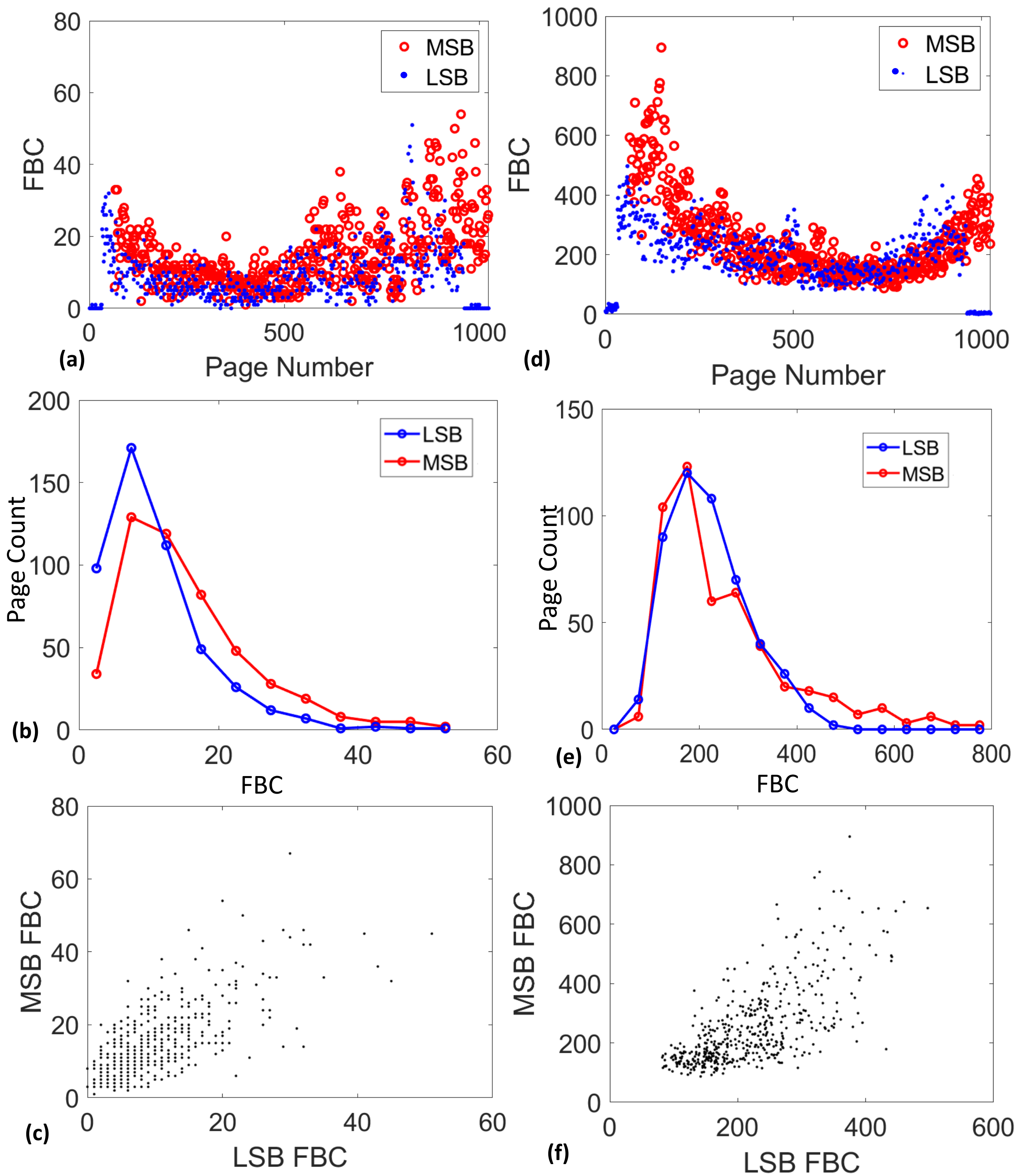


Figure 3.5 (a) FBC comparison between LSB (blue symbols) and MSB (red symbols) pages after 10 krad(Si) of TID, (b) The frequency polygon for MSB and LSB FBC for all pages in a block after 10 krad(Si) of exposure. (c) The correlation between FBC of MSB and the corresponding LSB pages. (d), (e), (f) are similar plots for 20 krad(Si) of TID exposure.

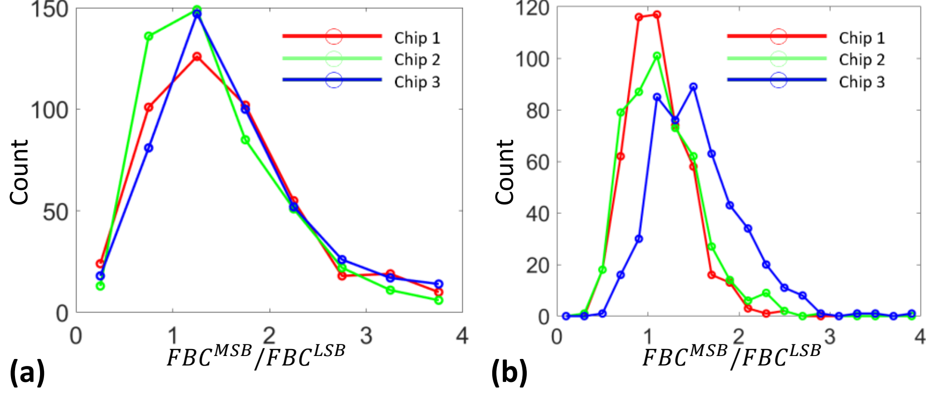


Figure 3.6 Frequency plot of the FBC ratios in MSB to those in the corresponding LSB pages for random data pattern for (a) 10 krad(Si) and (b) 20 krad(Si).

3.3.3 Model for FBC Comparison of LSB and MSB Pages

The experimental data are very roughly explained by a simple probabilistic model shown in **Figure 3.7**. The model essentially treats the memory cell as a capacitor (see **Figure 3.7**(a)) and the radiation damage as reducing the floating gate charge by a combination of removal of floating gate electrons and screening them via uncompensated positive charges in the oxide [32]. Since the electric field in the oxide layers of the memory cell is a key factor for the charge loss during irradiation [33], the failure probability depends on the initial-state floating-gate charge (Q_{FG}) that determines the field in the gate oxide (E_{ox}). For example, consider a memory cell in the V_t state-C (or "10") which has more charge (Q_{FG}^{C}) on the floating gate compared to the cell in the V_t state-B (or "00"). **Figure 3.7**(a) compares the energy band diagram for these two cells under unbiased conditions. For quantitative comparison, we assume $Q_{FG}^{C} \approx \frac{3}{2} Q_{FG}^{B}$, which is true if V_t states are equally spaced on voltage axis. Since field in the oxide layers is directly proportional to the charge on the floating gate at the unbiased condition of the memory array, the oxide fields in the state-C and state-B cells are related as follows: $E_{ox}^{C} \approx \frac{3}{2} E_{ox}^{B}$. Assuming TID induced charge loss rate being

directly proportional to the field in the oxide [33], the state transition probabilities after irradiation can be expressed as follows:

$$P(10 \rightarrow 00) \approx \left(\frac{3}{2}\right) P(00 \rightarrow 01). \qquad (3.1)$$

Since the 10 → 00 state transition is an MSB fail and the 00 → 01 state transition is an LSB fail (**Figure 3.7**(b)), we can derive the following relationship for the FBC observed on MSB and LSB pages:

$$\frac{FBC^{MSB}}{FBC^{LSB}} \approx 1.5. \qquad (3.2)$$

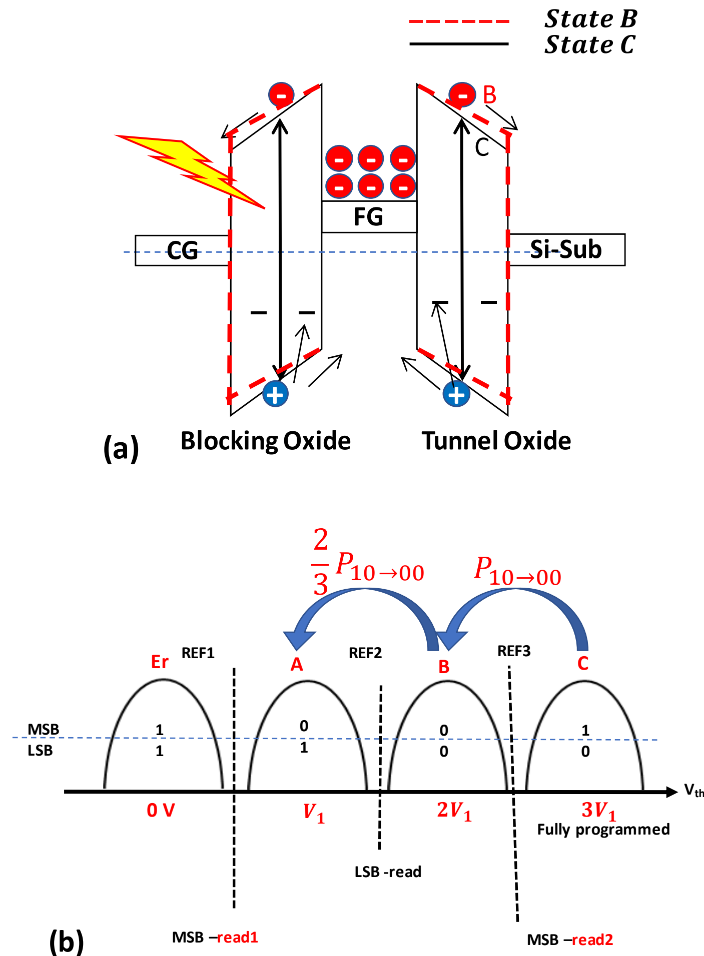


Figure 3.7 (a) Energy band diagram of a floating gate transistor at unbiased condition. Solid lines represent energy bands for a cell in state-C whereas the dashed lines stand for state-B. (b) Cell threshold voltage distribution for four different states in MLC storage. The simplified state transition probabilities are shown in the plot.

Please note that Eq. (2) is based on certain assumptions as stated below:

A1) We assume that TID effects will lower the cell threshold voltage from its pre-irradiation case. This assumption is based on the fundamental charge loss effects due to TID.

A2) We have neglected the V_t shifts for the cells in the "11" and "01" states. Since cells in these states have a lower charge on the floating gate compared to the cells in the "00" and "10" states, their oxide field will be significantly lower leading to negligible charge loss after TID irradiation. Indeed, previous work [13], [14] *on V_t distribution measurement on both 2-D and 3-D NAND array after irradiation supports this assumption.*

A3) Since the radiation dose is not extreme, we assume that radiation exposure will cause the transition of one state to its next lower V_t state. This assumption is verified from the measured data which show that none of the cells have a failure in both LSB and MSB bit.

A4) We assume all the four V_t states have an equal number of bits and the V_t states are equally spaced over the voltage range.

Note that this ratio will vary from page to page due to process variation and electronic noise inherently present in the high-density memory array. Hence, **Figure 3.6** shows a spread in the observed MSB/LSB fail ratio. However, the average MSB/LSB fail ratio lies in the range of 1.2-1.5 for all the chips that we used in this work. Thus, the measured data support the proposed simplified model and the underlying assumptions (*A1-A4*). Different flash memory manufacturers may design their chips with different amounts of voltage margins between memory states causing some deviation from this model. However, the correlation between the LSB and MSB fails will remain invariant for different memory chips as it is fundamentally tied to the data encoding process where both LSB and MSB pages share the same set of memory cells.

3.3.4 Internal Data Randomizer and Data Pattern Dependency

The FBC analysis presented in the previous section was obtained for a random data pattern. The random data pattern was used in order to ensure that all four analog V_t states have equal proportions of bits irrespective of a data randomizing algorithm. The chip under test uses an internal data randomizer that randomizes the user data before writing them on the NAND array. Essentially, the randomizer performs a bit-by-bit XOR operation on the input data using an internal key in order to randomize the input data pattern. The goal of such data randomization is to ensure memory reliability by distributing the memory cells in all four analog V_t states. However, the data encoding scheme as described in **Figure 3.7** using four different V_t states remains the same and hence our FBC analysis and the corresponding conclusions of the previous section remain valid even after data randomization. We illustrate the data randomization process in **Figure 3.8** using an all-zero data pattern. As an example, we assume two different keys for the LSB and MSB pages. In the absence of the data randomizer, all-zero data on both LSB and MSB pages would lead to all cells being programmed to the B-state. Due to data randomization, the exact cell V_t state will be decided by the randomization key, which will ensure a more even distribution of V_t states among the memory cells. An even distribution is good for cell endurance and reliability. Thus, randomization is an integral feature in the state-of-the-art flash memory which not only enhances data security but also ensures memory reliability.

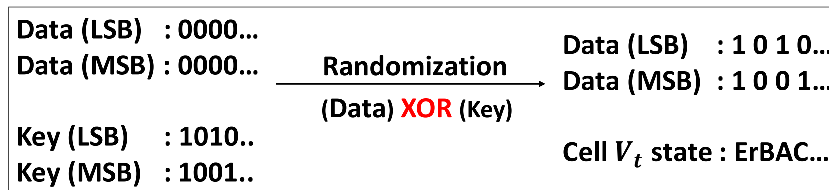


Figure 3.8 Illustration of the data randomization process.

Next, we illustrate the effects of data randomization by writing an all-zero data pattern in the memory array. **Figure 3.9** presents the FBC comparison between LSB and MSB pages for the all-zero data pattern after irradiation. **Figure 3.9**(a) and **Figure 3.9**(b) show the page-by-page FBC pattern for a 10 krad(Si) and 20 krad(Si) of TID respectively. Note that the FBC values per page with an all-zero data pattern are comparable to the FBC values observed with a random data pattern in **Figure 3.5**. This illustrates the effects of data randomizer which ensures uniform FBC irrespective of the user data pattern. In the absence of a data randomizer, all-zero data would have shown significantly higher FBC on LSB pages and significantly lower FBC on MSB pages as all the memory cells were programmed in the state-B of the V_t distribution. Such uneven FBC between memory pages is not ideal for ECC engines as it will increase the probability of uncorrectable read errors.

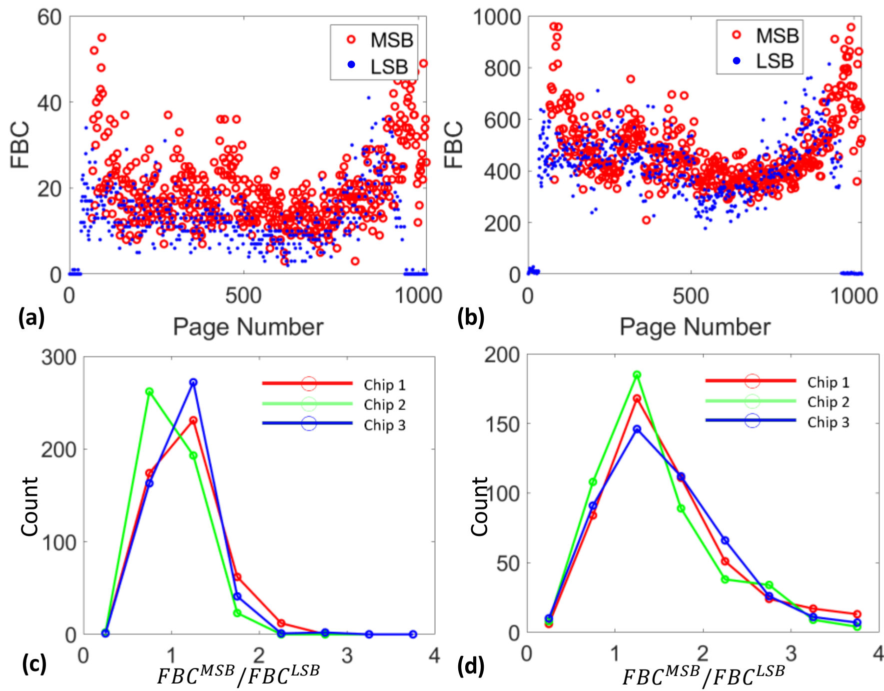


Figure 3.9 Page-wise FBC for (a) 10 krad(Si) , (b) 20 krad(Si). Ratio of FBC in MSB and the corresponding LSB pages for all-zero data pattern for (c) TID = 10 krad(Si), and (d) TID =20 krad(Si).

Thus, data randomization improves data reliability by ensuring relatively uniform FBC across different memory pages. We have also analyzed the MSB/LSB FBC ratio for the all-zero data in **Figure 3.9**(c) and **Figure 3.9**(d). Since data randomization (depending on the efficiency of the algorithm) ensures the presence of all four V_t states in the memory array with an equal proportion of cells in each state, our model assumptions (Section III-C) hold good even for all-zero data, and hence the MSB/LSB FBC ratio predominantly lies in the range of 1.2-15.

3.3.5 MSB/LSB Page FBC in Different Vertical Layers

Previous work [15] had shown a significant layer-to-layer variability under ionizing radiation, potentially due to a variation in geometric structure, causing a differential V_t-shift between different layers of the 3-D stack. The data shown in **Figure 3.5**(a) and **Figure 3.5**(d) essentially represent the page-to-page variability within a block which arises from layer-to-layer variability. Here, we study the FBC ratio between MSB/LSB pages across the different vertical layers in a block. We explore this FBC ratio by taking 5 different blocks of data (random data pattern) from two different chips that underwent 20 krad(Si) of ionizing radiation. The data are then split into the 32 corresponding layers for each block. Upon plotting the FBC ratio for each corresponding layer and the corresponding error bars in **Figure 3.10**, we see a distinct "U" shaped pattern with the FBC ratio being much closer to 2 in the lower layers, close to 1.2 in the middle layers, and close to 1.5 in the top layers. The difference in MSB/LSB FBC ratio across different layers could be due to different program V_t levels and read reference voltages in different layers of the 3-D structure. Since the exact program V_t levels are proprietary information, we speculate that the flash manufacturer introduced different program V_t levels across different layers to counter

the geometric variations of the 3-D structure which might have resulted in different FBC ratios between the MSB and LSB pages across different layers.

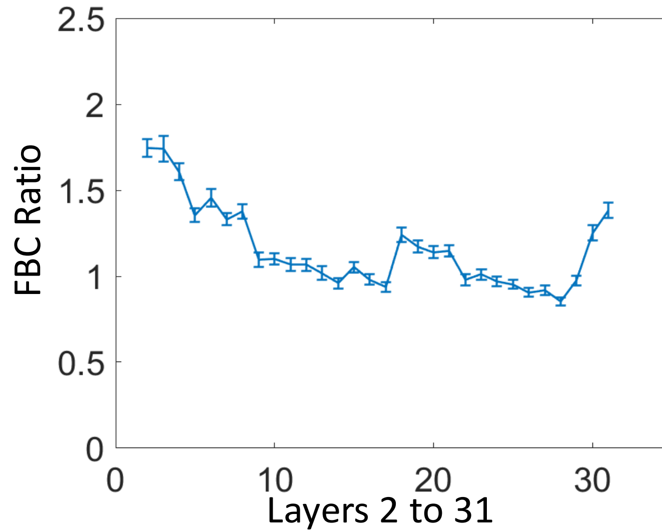
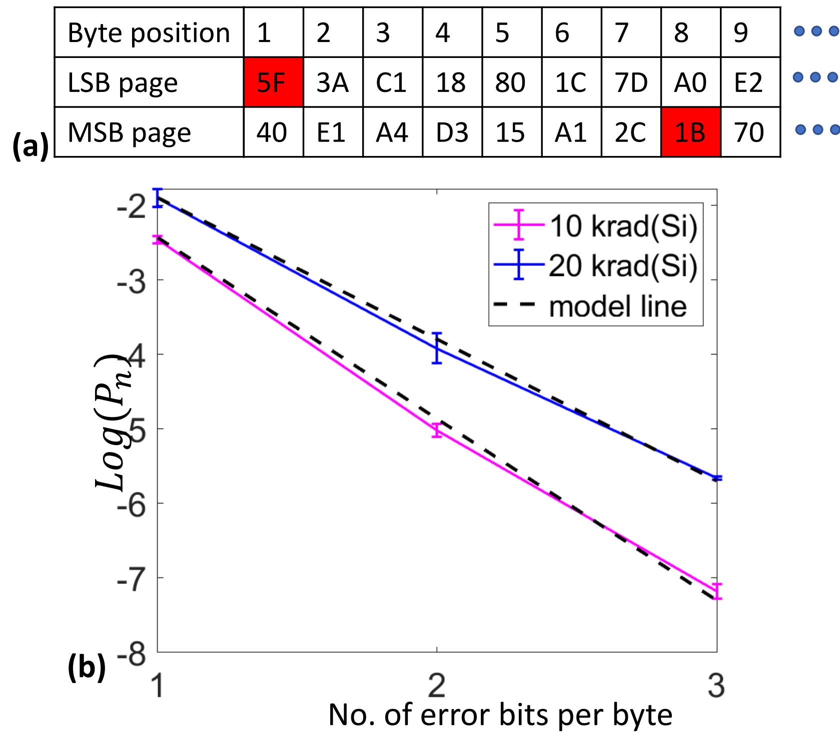


Figure 3.10 Ratio of FBC in MSB and the corresponding LSB pages for the 32 different layers in 3-D-NAND from 6 different chips.

3.3.6 Analysis of Error Location on MSB vs. LSB Pages

In this section, we analyze if there is any relationship between the error location of the LSB and MSB pages. The analysis process is illustrated in **Figure 3.11**(a), where we show the byte position and the corresponding data values of the LSB and MSB pages in the hexadecimal format. There are 18 kilobytes in a page whereas only the first 9 bytes are shown in **Figure 3.11**(a) as an example. We find that the fails in the LSB and MSB pages seldom occur at the same byte position. This is true for all the chips that we analyzed in this work. Thus, we can conclude that even though the FBC values are correlated between the LSB and MSB pages, the fail locations of LSB and MSB pages are not correlated. We also analyzed the number of bit errors per byte for the irradiated chips in order to confirm if there is any clustering of error locations. We find that most of the error bytes have only one error bit. However, a few bytes have more than one bit in error. If B_n is

denoted for the number of bytes having n error bits and B_{Total} as the total number of bytes in a memory block, the probability of having erroneous bytes with n error bits is $P_n = B_n/B_{Total}$. **Figure 3.11**(b) shows the measured probability P_n from 6 different chips as a function of n in the semi-log plot. We find that the data in **Figure 3.11**(b) obeys the following relationship: $P_n = P_1^n$ as the slope of each line is very close in value to P_1. This implies that the location of bit errors in a byte are independent and uncorrelated, *i.e.*, one memory cell being in error does not force neighboring cells into error.



Byte position	1	2	3	4	5	6	7	8	9	•••
LSB page	5F	3A	C1	18	80	1C	7D	A0	E2	•••
MSB page	40	E1	A4	D3	15	A1	2C	1B	70	•••

Figure 3.11 (a) Illustration of failed byte location (red) on LSB and MSB pages. Data are represented in hex format. (b) Probability of multi-bit error in a byte from 6 different chips.

3.4 Conclusion

In conclusion, we find that the MSB pages have a higher FBC compared to the corresponding LSB pages for a given TID irradiation. The FBC ratio between MSB and LSB pages varies from 1 to 2 depending on the vertical layer number. We also find a significant

correlation between LSB and MSB page FBC which implies that if an LSB page is erroneous, the corresponding MSB page will also be erroneous. The fail locations on the LSB/MSB pages are not correlated. In other words, the failures do not occur at the same byte position of the LSB/MSB page. In addition, we show that there is no clustering of error bits. These findings help in designing more intelligent and robust memory controllers for use in high-radiation environments. For example, the controller can selectively populate more important data into the LSB pages and relatively less important data into the MSB pages. Additionally, the controller can allocate more parity bits and deploy stronger ECC for MSB pages, especially the lower layers of 3-D NAND as they are more susceptible to errors.

Chapter 4. TID Effects on Read Noise of MLC 3D NAND

4.1 Introduction

The device noise characteristics significantly affect the read operation of NAND flash memory by causing bit errors in the data. Flash manufacturers usually counter the effects of noise by keeping a sufficient voltage margin between analog threshold voltage (V_t) states of the memory cells in the single-level cell (SLC) technology. However, high-density MLC technology uses a lower voltage margin between memory states, and hence noise effects may cause bit errors even in freshly written data. The memory controller usually employs error correction codes (ECCs) to correct bit errors caused by noise; however, the ECC engine has a finite error-correcting capability [34]. Once the bit error percentage exceeds the ECC limit, data become unrecoverable and corrupted. Since commercial off-the-shelf (COTS) NAND flash memories are widely used in space and other radiation-harsh environments, it is important to analyze the effects of noise on bit errors after irradiation.

Even though the radiation-induced data corruption issue in the COTS NAND flash memories is well documented in the literature [32], [35], [36], the effects of radiation on memory noise are not well studied. Through experimental measurements, it was demonstrated that ionizing radiation causes charge loss from the floating gate and charge trapping in the oxide layers, which shifts the cell V_t distribution causing bit flip events on the irradiated memory chip. Ionizing radiation not only causes charge loss but also induces defect states in the oxide layers of the flash memory cells. Since defect states contribute to noise in metal oxide semiconductor (MOS)

technologies [37], percentages of noisy bits in NAND flash memory are likely to increase in radiation environments, leading to risks of data corruption even in the presence of ECC.

Cell V_t fluctuation due to noise has been extensively studied for un-irradiated NAND flash memory cells [31], [38], [39], [40]. Charge capture/emission in the defect states of the tunnel oxide is shown to be responsible for the noisy behavior of memory cells. For irradiated flash memory arrays, Bagatin *et al.* [41] demonstrated error instability originating from cell V_t evolution with annealing time. However, no quantitative analysis was performed on the effects of TID on noisy bits of the flash array. Several studies have been performed on how ionizing radiation affects MOS and similar devices in terms of charge trapping and defect generation [37], [42], [43], [44]. Low-frequency noise measurements are typically performed on discrete MOS devices to provide insight into the radiation-induced defect densities and their energy distribution [37], [45], [46], [47]. However, similar measurements are not applicable to COTS NAND flash memory chips due to the complexity of the underlying array structure and limited access to the memory array. Hence, there exists a need for an array-level noise characterization method for COTS NAND flash memory chips that can quantify their impact on the overall bit error response of the memory chips as a function of TID.

In this chapter, we propose a noise characterization technique for COTS flash memory chips using a digital read-out method. Using this characterization method, we quantify the percentage of noisy bits in the total fails of an irradiated MLC 3-D NAND flash memory chip. We also evaluate the increase in noisy cells in the irradiated chip as a function of TID. Finally, we discuss a method that will reduce the impact of TID on the noise characteristics of the memory chip.

4.2 Background Information

The effects of ionizing radiation on a flash memory cell are illustrated in **Figure 4.1**(a) with the energy band diagram of a programmed flash memory cell in the unbiased condition. The figure shows three primary mechanisms of charge loss when a memory cell is exposed to ionizing radiation [32]: (1) thermionic emission of electrons from the floating gate, (2) electron-hole recombination, and (3) hole trapping in the oxide. Charge loss reduces cell V_t, which can lead to bit errors [32], [35], [36]. **Figure 4.1**(b) illustrates the effects of TID on cell V_t distribution of MLC memory states. Since MLC memory stores 2 bits of information per cell, it has 4 different V_t states after programming. The V_t states are labeled as L_0, L_1, L_2 and L_3 in **Figure 4.1**(b). The Gray code is commonly used to encode the states ($L_0 = 11,\ L_1 = 01,\ L_2 = 00\ and\ L_3 = 10$) [48]. Three different read reference voltages (V_{ref}) are used to digitize analog cell V_t values into binary data. There is sufficient voltage margin between V_{ref} and the V_t states for freshly written data (solid blue lines in **Figure 4.1**(b)), resulting in minimal numbers of bit errors. NAND flash manufacturers keep this voltage margin to mask the effects of noise during the read operation. However, this voltage margin is reduced after irradiation, as shown with dashed red lines in **Figure 4.1**(b), causing a percentage of memory bits to be vulnerable to noise fluctuation during the read operation [8], [49].

There are two distinct types of fail bits caused by irradiation, as illustrated in **Figure 4.1** (b). Consider the lower tail of the programmed state distributions (**Figure 4.1**(b)) to the left of each V_{ref}. If the V_t of the cell is reduced significantly below V_{ref} (blue bars), they will be read as fail bits consistently over multiple read operations. The count of such bits is termed a steady fail bit count (SFBC). Similarly, for a significant number of programmed bits, the V_t distribution may fall very close or overlap the V_{ref} value (yellow bars). These bits may change logic states during

successive read operations; hence, the total count of such bits is termed as noisy bit count (NBC). Note that NBC may come from the upper tails of the V_t distributions as well. Since V_t distribution generally shifts down after TID, we emphasize the NBC coming from the lower tail of V_t distribution in **Figure 4.1**(b).

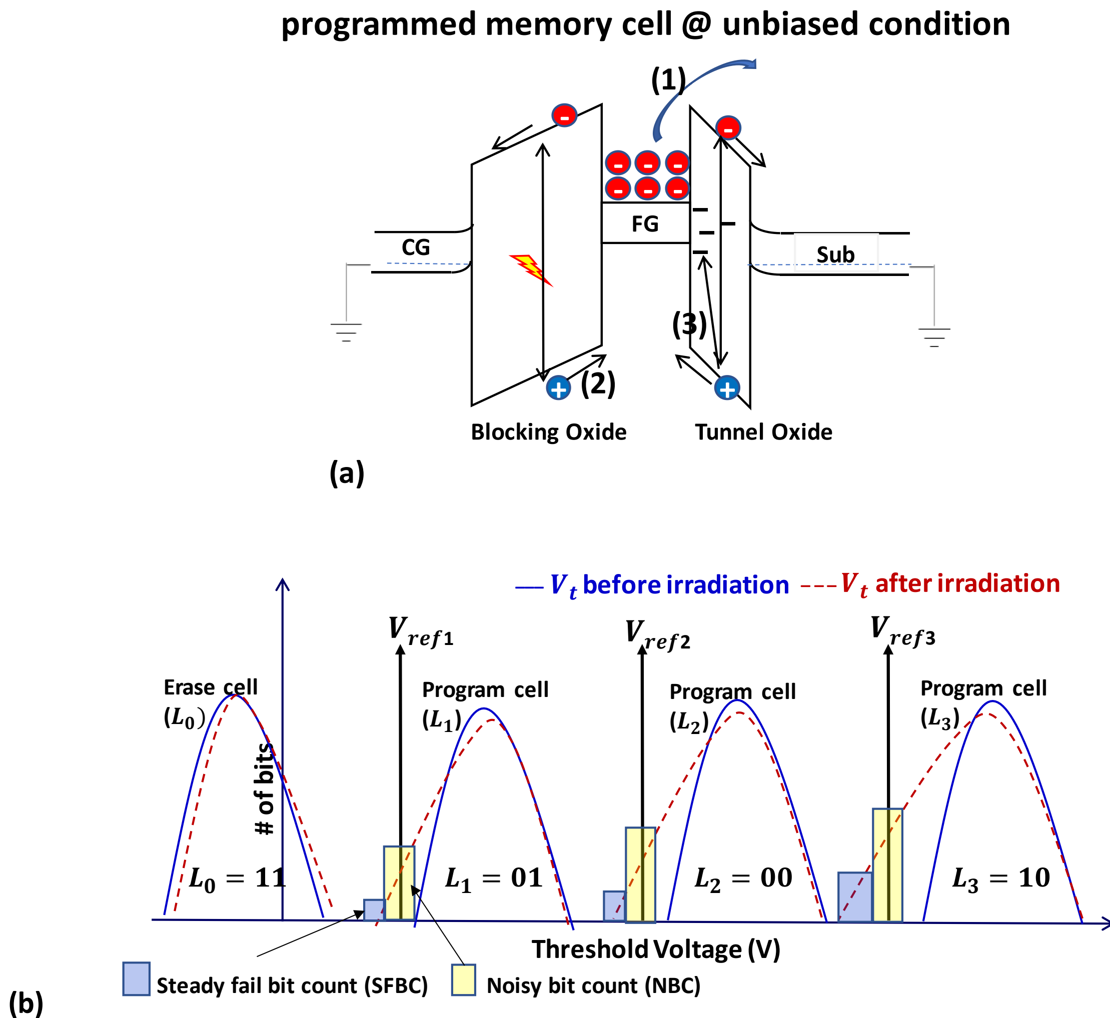


Figure 4.1 (a) Energy band diagram of a programmed FG cell with all terminals grounded. (b) Illustration of cell threshold voltage distribution of MLC memory before (solid line) and after irradiation (dashed line).

4.3 Experimental Results and Discussion

The experimental hardware setup, samples, and gamma irradiation procedure remain identical to 3.2. Following are the experimental results.

4.3.1 Characterization Technique for NBC

To quantify NBC on the irradiated chip, we have developed a characterization scheme that can be applied to any NAND memory chip using a standard digital interface. The characterization method is illustrated in **Figure 4.2**(a). The first row in the table represents the data pattern that is written to the memory. The subsequent rows represent data from the memory chip after irradiation via successive read operations to the same memory address. We look through the data to see if the bits in each position flip during successive reads. If so, bits are considered noisy, as illustrated in **Figure 4.2**(a). If the bit never flips but consistently registers a value different from the originally written data, then such a bit is a steady failed bit, also illustrated in **Figure 4.2**(a). **Figure 4.2**(b) illustrates the effect of increasing the number of successive read operations on the NBC percentage. NBC percentage is calculated by reading a given memory page a certain number of times and subsequently counting the fluctuating bit positions. The following formula is used to quantify NBC percentage:

$$NBC\ (\%) = \frac{Total\ NBC\ in\ a\ page\ after\ 200\ reads}{Total\ number\ of\ bits\ in\ the\ page}. \qquad (4.1)$$

Since NBC shows a saturating trend after 200 successive read operations, we choose 200 successive reads for NBC characterization. Higher sample counts take a significantly longer time to record and process characterization data while having minimal impact on NBC percentage.

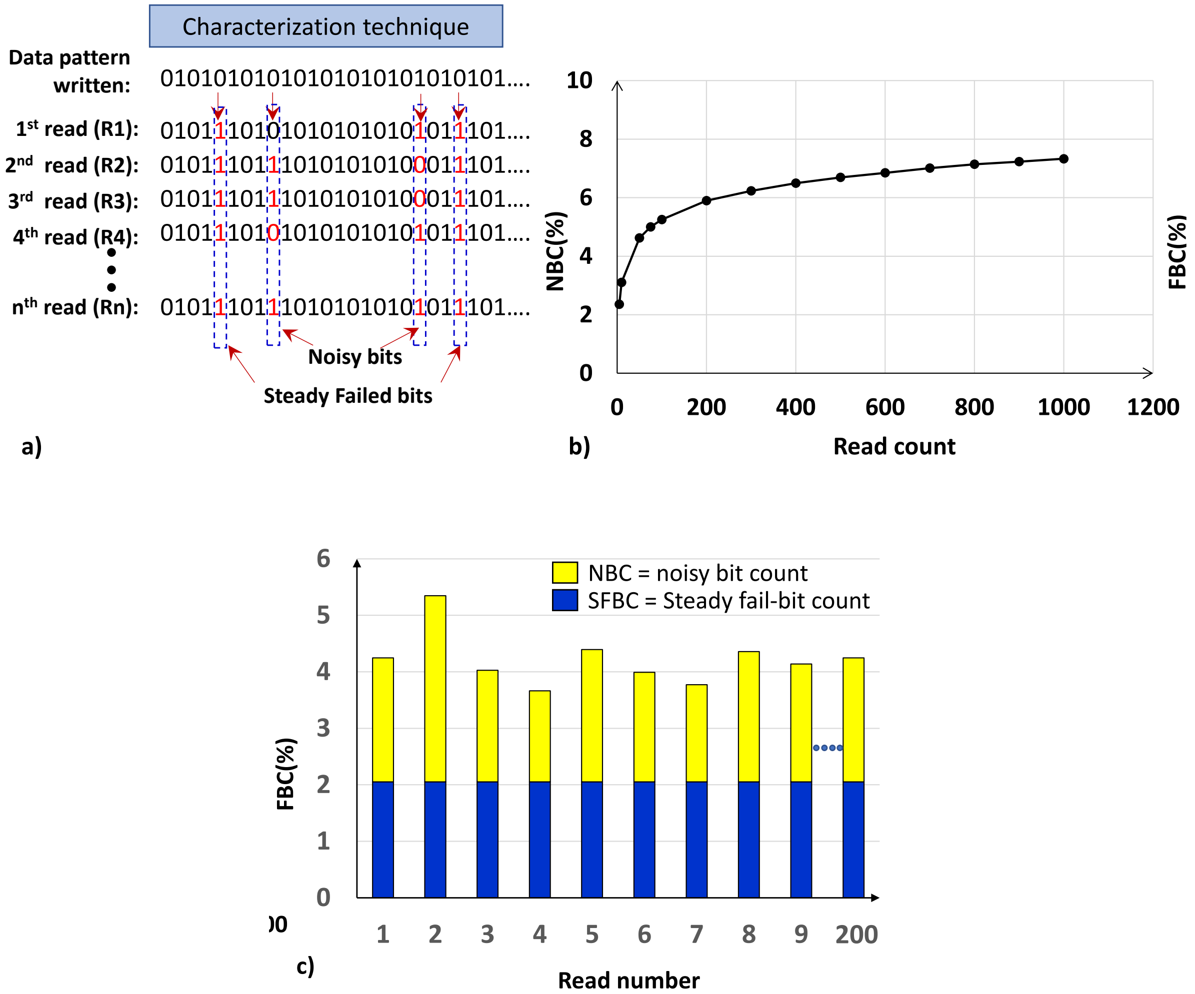


Figure 4.2 (a) Table illustrating how we quantify noisy bits. (b) Sample read count vs. NBC% (c) Fail bit count for n = 200 consecutive reads from the same memory address of the irradiated chip.

Figure 4.2(c) illustrates measured FBC fluctuation on successive memory read operations from the same memory address of an irradiated chip (TID = 50 krad(Si)). A random data pattern was written on the chip before irradiation. After irradiation, we read back the data 200 times and compute the FBC percentage for each reading, which is shown as a bar plot in **Figure 4.2**(c). The bar height represents the total number of read fails obtained in that read operation, which changes during successive read operations. We classify the total fails into two groups, SFBC and NBC, as illustrated in blue and yellow colors, respectively. Since SFBC is the fixed fail-bit count in each

read operation, their number remains the same, while NBC changes. **Figure 4.2**(c) illustrates that a significant fraction of the total fails (about 40% of total FBC) after irradiation is due to NBC.

4.3.2 NBC Comparison for Irradiated vs. Un-Irradiated Chip with Freshly Written Data.

Since ionizing radiation increases low-frequency noise in MOS technologies [37], [50], it is reasonable to expect that a memory chip will show more NBC with increasing TID. However, it is difficult to capture noisy bits with freshly written data on the irradiated parts. Typically, freshly written data on both irradiated and unirradiated chips show very few errors (<0.003% of total bits) once the data are read back. Since voltage margins between V_{ref} and V_t distribution are high for freshly written data, as illustrated in **Figure 4.3**(a), read failures are less likely for the default read operations. Note that V_t distributions for irradiated and un-irradiated chips are similar in **Figure 4.3**(a). This similarity occurs because the NAND memory chip internally uses an alternative program-verify feedback-based writing technique that ensures similar V_t distributions, irrespective of the irradiation condition of the memory chips, as long as the chips are functional.

To compare noise characteristics from the freshly written data, we first adjust the V_{ref} value by applying the Read-Retry technique as illustrated with V'_{ref} in **Figure 4.3**(a). For simplicity, we show only the first two V_t states, L_0 and L_1, and the corresponding values of V_{ref1} in **Figure 4.3**(a). In practice, all three V_{ref} values are shifted during the Read-Retry operation. The implementation details of the Read-Retry technique are given in a previous publication [51]. We implement the RR operation in our hardware setup through a firmware change. The RR operations are a coordination of the NAND page Read command and Set Features (0xEF) command. The Set Feature command allows the selection of different internal read-reference voltages during the page read operation. Nominally, this command is used to help recover data when standard ECC

correction fails at the default read reference voltage. The 3-D NAND chips under test offer 16 different reference voltage options for RR operation. However, the precise voltage shift corresponding to these options is not specified in the datasheet. The command sequence used to implement the RR operation for ONFI-compliant NAND flash memory is:

1) Send Command SET FEATURES (0xEF).

2) Send Address (0x89).

3) Send Read Option Value.

4) Send Command PAGE READ.

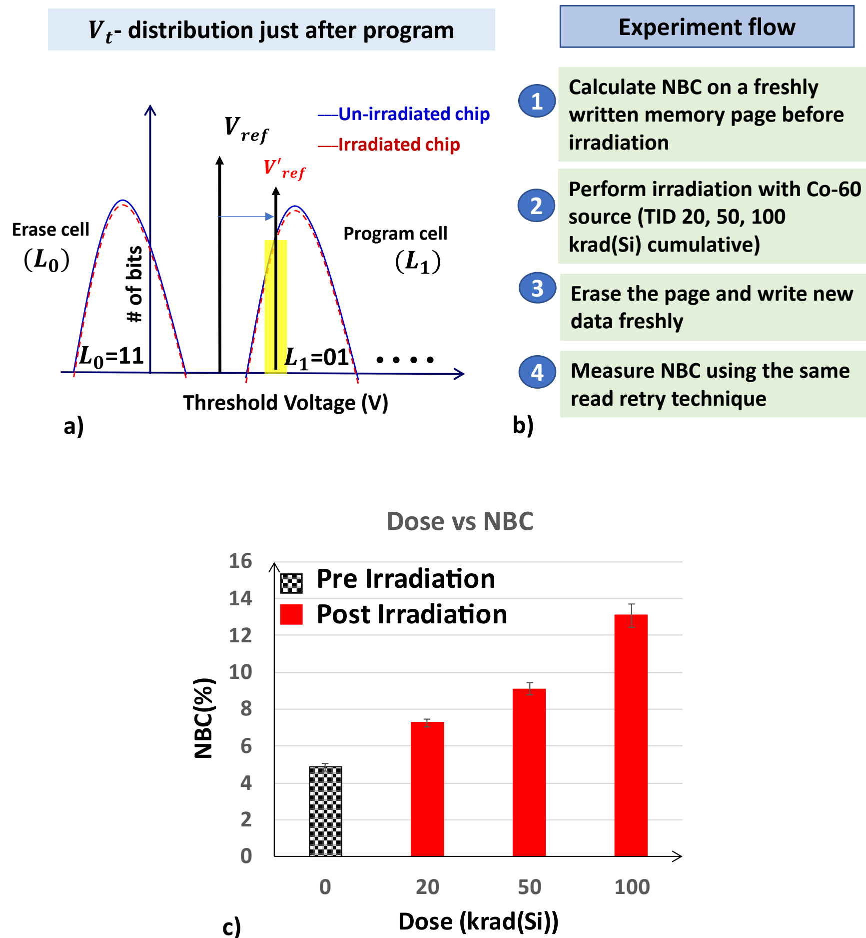


Figure 4.3 (a) Adjusting V_{ref} using read-retry operation to quantify NBC on freshly written data from irradiated and un-irradiated chips. (b) Experimental procedure followed for the NBC comparison. (c) Pre- vs Post-irradiation NBC response of the same memory address for four different chips.

We perform the noise characterization using V'_{ref} following the procedure described in 4.3.1. For a fair comparison, we calculate NBC from the same chip and the same memory address before and after irradiation. The step-by-step experimental procedure for NBC comparison is shown in **Figure 4.3**(b). Results are summarized in **Figure 4.3**(c). The plot represents data from 4 memory chips, 10 blocks each, encompassing all 4 planes. For each block, we pick one sample page per layer. The NBC percentage monotonically increases with TID. For the analysis to be statistically meaningful, we chose four different memory chips, and find that NBC increases in each chip compared to pre-irradiation values. The results in **Figure 4.3**(c) confirm that ionizing radiation significantly increases the noise amplitude of flash memory cells. The NBC does not change even with multiple reprogramming cycles. These changes will limit the long-term data integrity of NAND memory if they exceed the threshold for on-chip error correction.

We emphasize that the increase in NBC with irradiation is mainly due to the memory cells and not from the peripheral read circuitry. Note that the peripheral read circuitry is common for all memory blocks. If read circuitry were the origin of the read noise, there could have been a correlation of noisy bit positions from different memory blocks. However, we do not observe any correlation between noisy bit positions. Also, in the next section, we show that there is a clear distinction in noise characteristics between memory blocks that were in the erased vs. programmed condition during irradiation. The peripheral read circuitry is the same for both. Hence it is likely that the observed increased noise is mainly due to the impact of irradiation on memory cells.

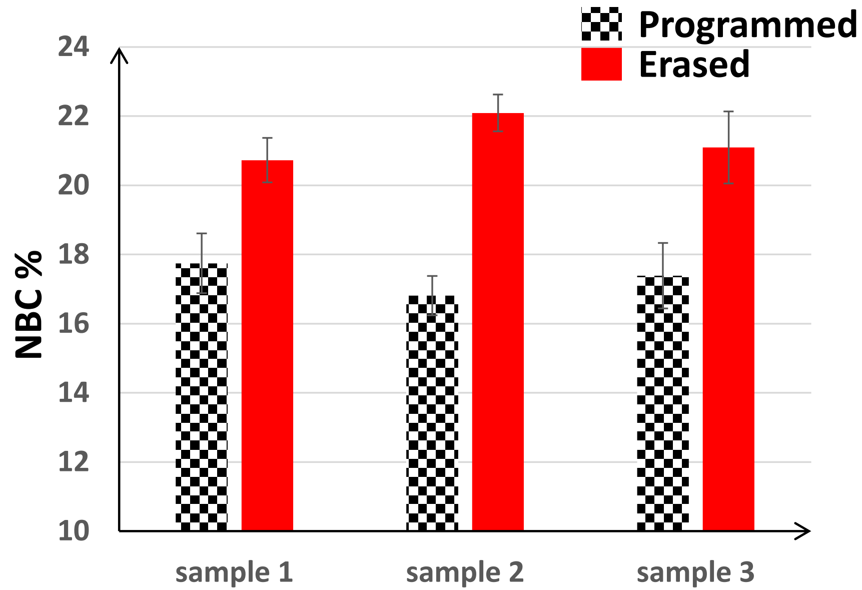
4.3.3 NBC Comparison Between Erased vs. Programmed Memory Blocks on the Irradiated Chip

In this section, we compare noise characteristics on blocks that were in a programmed state versus blocks that were in the factory-out erased state during irradiation (100 krad(Si)). The

programmed block was written with an all-zero data pattern. After irradiation, we erase both these blocks and write the same random data pattern. The total FBC just after writing was very low and comparable on both these blocks. Next, we measure the NBC following the same technique as discussed in **Figure 4.3**(a). **Figure 4.4**(a) summarizes our measurement results; these were made one week after the irradiation. The NBC in blocks that were in an erased state during irradiation is up to 35% greater than the NBC of blocks in a programmed state. This result was confirmed on three different memory chips.

Figure 4.4(b) and **Figure 4.4**(c) show energy band diagrams for erased and programmed flash memory cells, respectively. The electric field direction in the oxide layers of the programmed and erased cells are opposite due to the presence (absence) of electrons on the floating gate of the programmed cell (erase cell). Hence, in a programmed cell, the holes generated by the ionization in the oxide layer move toward the floating gate, leading to an increased density of trapped charge near the floating gate. However, the direction of hole movement is opposite in the case of erased cells, increasing the probability of hole trapping at the oxide-channel (Si) interface.

Figure 4.4(d) and **Figure 4.4**(e) show TID-induced trap locations in erased and programmed cells, respectively. Since traps near the oxide-channel interface are more detrimental to the device noise characteristics during the read operation [6], [21], more degradation of the erased memory cells takes place compared to the programmed cells on the irradiated chip. Hence, we observe more NBC on the factory-out erased memory blocks compared to the programmed memory blocks after irradiation. This result suggests it is beneficial to pre-program the factory-out memory blocks to a programmed state before deploying the chips in a radiation environment.



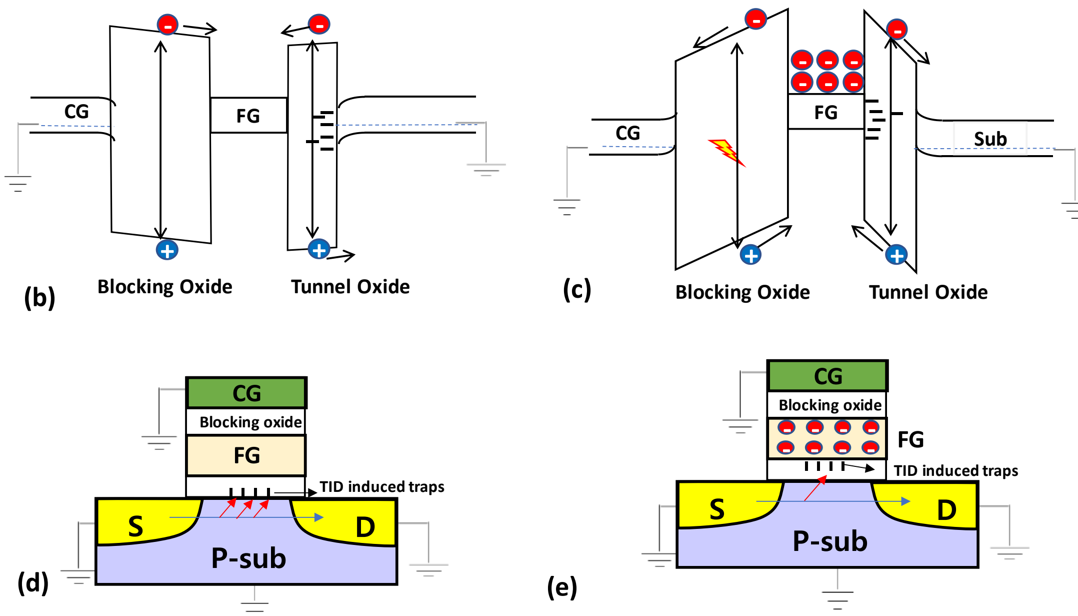


Figure 4.4 (a) Measured data on NBC for memory blocks that are in programmed vs erased condition during irradiation. Energy band diagrams of (b) an erased flash cell and (c) a programmed flash cell. TID induced trap locations for (d) erased flash memory cell and (e) programmed memory cell.

4.3.4 Layer Wise NBC Study

To study the TID effects in different memory layers, we measured NBC from memory pages located at different vertical layers of the 3D stack. **Figure 4.5** summarizes our measurement results from two different memory blocks from the same chip. The initial layer numbers represent the bottom layers of the 3D stack, whereas the top layers have higher layer numbers. Edge layers exhibit higher NBC compared to middle layers. In a previous publication [52] we observed a similar trend in terms of TID-induced fail bit count and provided an explanation for such a trend using the unique array structure of 3D NAND. It is likely that the same explanation holds for the observed layer-dependent NBC after irradiation. That is, memory cells in the bottom layers are smaller in size due to the reactive ion etching (RIE) process [52], making them more susceptible to noise fluctuations. Likewise, the top layers of the 3D stack are more affected by dose enhancement effects due to their proximity to the back end of line (BEOL) metal layers [53], [54] also making them more vulnerable to errors associated with noise fluctuation.

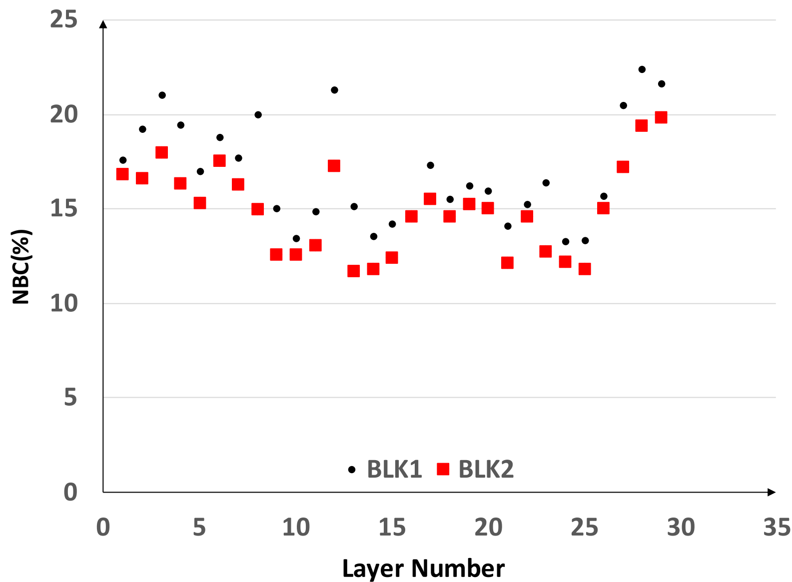


Figure 4.5 Layer-wise noise analysis. NBC data are collected for two different memory blocks from the same chip.

4.3.5 Room Temperature Annealing Effects

In this section, we present our characterization results on room-temperature annealing effects of TID-induced defect states. We monitored the evolution of noise in the irradiated chips over a long duration of time. **Figure 4.6** shows the data collected. We observed an increase in NBC for the first few days after irradiation and subsequently a reduction in NBC over a longer period of time. The noisy bit count can be affected strongly by both the position and energy of traps near the blocking oxide/FG, FG/tunnel oxide, and tunnel oxide/channel interface. The increase in NBC during the initial portion of the annealing may be due to the post-irradiation emission of electrons from shallow traps in the FG in response to trapped positive charges in the nearby blocking and/or tunnel oxides [55]. The reduction in NBC at longer times may result from the thermal or tunnel annealing of trapped holes [56], [57], and/or the neutralization of trapped charge in the tunnel oxide via reactions with diffusing H_2 molecules, as observed in aging studies of MOS devices [58], [59]. While plausible and consistent with previous results, more work is needed to determine whether other possible mechanisms are causing the observed effects in these devices.

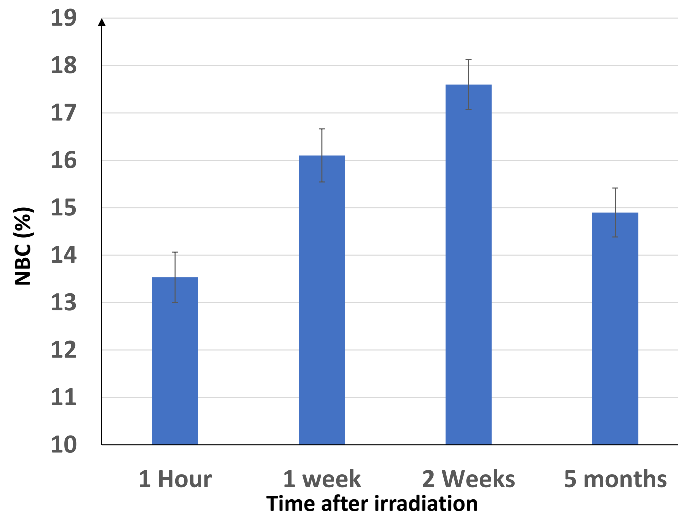


Figure 4.6 Evolution of NBC with time after irradiation.

4.4 Conclusion

We see how noisy bits contribute to the total fail bit count, despite not being hard fails, and thus significantly contribute towards the increase in errors with TID exposure. We observe a noisy bit count increase as a strong function of the total dose. We find that radiation-induced noisy bit count depends on several factors, such as the location of the page in the 3D stack, the time gap between irradiation and read operation, and the program condition of the memory block during irradiation. Specifically, we find that erased memory blocks during irradiation acquire more noisy bits compared to the blocks that are in programmed condition during irradiation. Hence, if memory modules sent to space are preprogrammed with data instead of being left in a factory-erased state, noise effects can be reduced. These results should help further enhance the effectiveness of using COTS NAND flash in space missions and other high-radiation environments.

Chapter 5. SRAM PUF Under Ionizing Radiation

5.1 Introduction

Physical Unclonable Functions (PUFs) are an important hardware security primitive that can be used for device-specific key generation and device authentication. The power-up state of static random access memory (SRAM) is routinely used for generating PUF [60], [61]. SRAM power-up state is a random bit stream that is unique for a particular memory chip. Its uniqueness is closely tied to the manufacturing process variations. SRAM PUFs are commonly used in commercial electronic systems because of the ubiquitousness of SRAM memories [62], [63], [64], [65],[66], [67], [68]. SRAM PUFs are also of interest in space applications and electronic systems operating in radiation-prone environments (*e.g.*, nuclear energy).

Radiation effects on PUFs have recently gained significant traction with the ever-growing satellite constellations and the requirement for radiation-hardened hardware security primitives. An array of recent research investigations [69], [70], [71], [72], [73] have delved into the radiation effects on PUF circuits. For example, Sakib *et al.* [69] explored the TID effects on a PUF derived from NAND flash memory chips. The results unveiled a substantial decline in PUF accuracy after irradiation. Wang *et al.* [71] investigated X-Ray and Proton radiation effects on 40 nm CMOS PUF circuits, named BD-PUF, that utilize the randomness of oxide breakdown (BD) positions in transistors to generate the PUF. Their results show that BD-PUF is robust under X-ray irradiation up to 2 Mrad (SiO_2), but it shows significant degradation at high-fluence proton irradiation, attributed primarily to a threshold-voltage (V_t) shift of the selector device. Similarly, Martin *et al.*

[70] studied TID effects on delay-based CMOS Ring-Oscillator PUF. They observed significant degradation of PUF reliability, exceeding 10% intra-die Hamming Distance after 300 krad(Si) of irradiation.

In the context of SRAM PUF, multiple interesting works have been published. For example, Su *et al.* analyze radiation effects on an SRAM-PUF built using the fully depleted silicon on insulator (FDSOI) process [74]. Their study shows an increased number of unstable PUF bits after irradiation. However, the study does not provide an analysis of the SRAM-PUF before and after irradiation, so the changes in the original PUF due to irradiation remain unclear. Similarly, Calienes *et al.* studied the radiation tolerance difference for single event effects between bulk vs. FDSOI SRAM devices [75]. Interestingly, Zhang *et al.* propose irradiating chips as a means to improve the total ionizing dose (TID) response of SRAM-PUFs [73]. Lawrence and his colleagues [72] explored the effects of X-ray and proton irradiation on SRAM PUFs using commercially available standalone SRAM memory chips. They observed significant degradation in the accuracy of SRAM PUFs after 100 krad(SiO_2) of irradiation. It is then also important to understand the gamma ray effects on commercial SRAM.

Multiple works have attempted to improve the SRAM PUF response under ionizing radiation. Zhang *et al*. [73] proposed a stability improvement method for SRAM PUF using ionizing irradiation. They found that by irradiating the SRAM memory array to a moderate amount of TID of 40 krad(SiO_2), the intra-chip Hamming Distance can be improved significantly. Su *et al*. [76] proposed a novel SRAM cell design with 8 transistors (8T) to enhance the reliability and radiation tolerance of SRAM PUF. Their approach involved the incorporation of two cascading PMOS transistors into the standard 6T cell configuration fabricated using 28 nm FDSOI process technology. This modification yielded superior radiation tolerance in comparison to the standard

6T design. Lawrence *et al*. [72] demonstrated a majority voting procedure called temporal majority voting (TMV) to help reduce PUF mismatch post-irradiation which yielded a small improvement. Although several prior studies have examined the TID effects on SRAM PUFs, questions regarding the impact of technology node on the TID response of SRAM PUFs remain unanswered. Similarly, a comprehensive analysis regarding the impact of data patterns held in memory during irradiation on the integrity of SRAM PUFs is missing in the published literature.

5.2 Background Information

A basic building block of an SRAM chip is an SRAM cell that holds one bit of information. The common SRAM cell known as the six-transistor (6T) cell consists of a cross-coupled CMOS inverter pair along with two access transistors as shown in **Figure 5.1**(a), with the access transistors modeled as capacitances. The cross-coupled inverter pair has two stable states corresponding to logic 0 and 1 as shown in **Figure 5.1**(a). After power-up, SRAM cells can end up in either state, depending on discrepancies in the size and drive strength of transistors in cross-coupled inverters. These discrepancies are an artifact of minuscule process variations that are unique for each chip [77], [78], [79], [80]. The threshold voltage conditions for power-on in each state are pictured in the table in **Figure 5.1**(a).

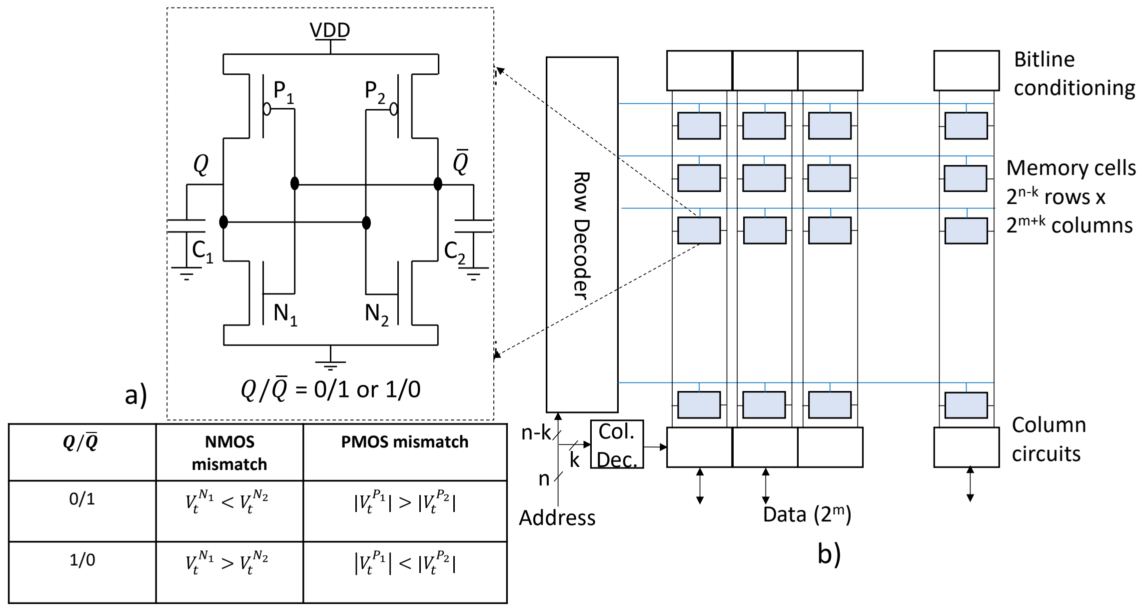
An SRAM chip contains an array of memory cells as shown in **Figure 5.1**(b). The chip with n address inputs and 2^m data lines is seen logically as an array of $2^n \times 2^m$ cells. For chip floor planning reasons, the array is physically organized into $2^{n-k} \times 2^{m+k}$ cells and an additional column decoder is used to select a word from the selected row. In addition to address and data pins, an SRAM chip has control inputs for controlling read and write operations. To read from SRAM, bitlines are pre-charged and the selected wordline is turned on. One of the two column bitlines will

be pulled down by the cell and that is sensed by the corresponding column circuitry. To write to SRAM, the bitlines are driven based on the content from data pins (*e.g.*, BL=1, $\overline{BL}$=0) and the word line is turned on. The bitlines overpower the selected cells, thus writing a new value.

The power-up state of the cells in the array is random and unique for each SRAM block. This power-up state can be used for generating SRAM-based PUFs or fingerprints. The power-up states, repeatedly captured on the same chip or an SRAM block, produce similar random sequences of bits, albeit not identical, as some memory cells change their power-up state due to electric noise. We generate 5 instances of the power-up state and perform bit by bit comparison to create the reference GoldPUF. If there is a mismatch in any bit position of the five power-up states, we use the majority voting to decide the value of the GoldPUF bit. To quantify mismatches between the GoldPUF and any subsequent power-up state, we measure the intra-die Hamming Distance (HD) as follows:

$$HD = \frac{\text{\# of set bits (GoldPUF xor CurrentPUF)}}{Total\ \#\ of\ PUF\ bits}. \qquad (5.1)$$

Hamming Weight (HW) is another important metric that is computed as the percentage of cells with the power-up state at logic 1. Ideally, the HW of SRAM-PUFs is 50%.



$Q/\bar{Q}$	NMOS mismatch	PMOS mismatch
0/1	$V_t^{N_1} < V_t^{N_2}$	$\lvert V_t^{P_1}\rvert > \lvert V_t^{P_2}\rvert$
1/0	$V_t^{N_1} > V_t^{N_2}$	$\lvert V_t^{P_1}\rvert < \lvert V_t^{P_2}\rvert$

Figure 5.1 (a) Schematic of a six transistor (6T) SRAM cell and threshold voltage conditions for power-on. (b) SRAM array.

5.3 Experimental Setup to Study Radiation Effects in SRAM

To interface the SRAM chips with a workstation, we have used a custom-designed setup as shown in **Figure 5.2**. The setup includes an Arduino Due interfacing the workstation via the Universal Serial Bus (USB) and a TSOP-54 socket holding an SRAM chip. The Arduino firmware supports powering up/down of SRAM chips, reading the SRAM chips' power-up states, and writing selected data patterns/ images into the SRAM chip. Powering off the SRAM chips is carried out through a PMOS switch by driving its gate voltage to 3.3 V for five seconds, while concurrently keeping data, address, and control pins of the SRAM chip at 0 V. The manner of irradiation and the type of data collected post-irradiation depends on the experiment and is detailed in the following sections. The data are then processed in MATLAB.

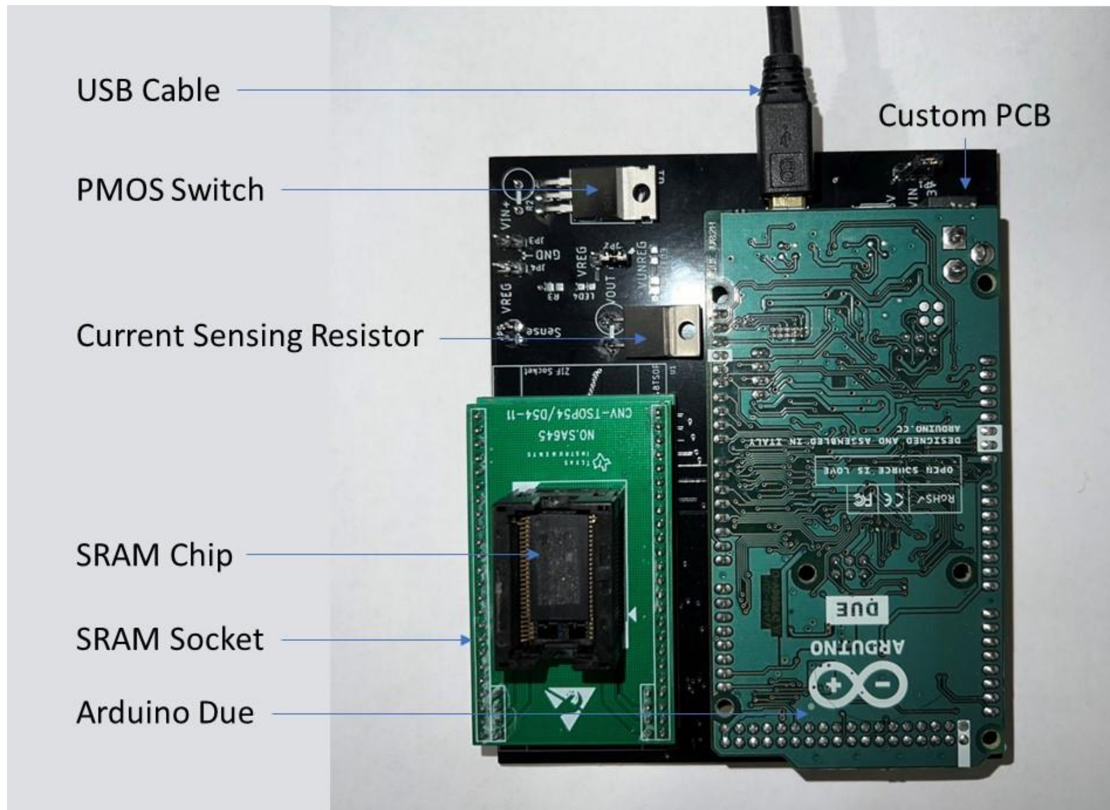


Figure 5.2 Custom SRAM Interface.

5.4 Experimental Results and Discussion

5.4.1 Effects on the Power-up State of Static Random-Access Memory

To study the effects of Ionizing radiation in SRAM arrays, we use COTS SRAM chips from IDT (IDT71V416S) and Cypress (CY7C1041C) for our tests. They are both 256k × 16 bits SRAM chips. **Table 5.1** describes the main characteristics of both chips. They are functionally identical; the only difference is in the technology node used in fabrication.

The irradiation experiments are performed at the Sandia National Laboratories Gamma Irradiation Facility using a Co-60 source with a dose rate of 18.6 rad(Si)/s. Gamma irradiation was performed on the packaged TSOP (thin small outline package) devices with all the pins of the chip

grounded. The direction of gamma rays during irradiation is perpendicular to the top surface of the chip.

The step-by-step experimental flow is as follows: Before irradiating the chips, we pre-characterize each chip to evaluate its baseline power-up states. We perform 5 consecutive power ON/OFF cycles and read each power-up state of the SRAM array. We read word-by-word the first 64k words of the SRAM array, resulting in a total of 1 Mbit ($64k \times 16$) of the power-up state per one power-up cycle. We generate the GoldPUF by taking a majority vote from 5 power-up states of a fresh chip. We then expose the memory chips to gamma rays up to a certain dose level. We retrieve the power-up state of the irradiated chip within 45-60 minutes after irradiation. The PUF generated from the irradiated chip is called authentication PUF. We generate 5 authentication PUFs and they are individually compared with the GoldPUF to compute HD and the average is reported.

Table 5.1 Summary of Chip Specification.

Manufacturer	IDT	Cypress
Part number	IDT71V416S	CY7C1041C
Capacity	4 Mbits	4 Mbits
Supply voltage	3.3 V	3.3 V
Word size	16 bits	16 bits
Tech. node	130 nm	150 nm
Timing	10 ns	10 ns

5.4.1.1 Effects of Total Dose on SRAM-PUF

Figure 5.3(a) and **Figure 5.3**(b) show the HD of SRAM-PUFs as a function of the total irradiation dose for IDT and Cypress chips, respectively. **Figure 5.3**(a) and (b) show the intra-die HD values between the GoldPUF and the corresponding authentication PUFs. We find that intra-die HD before irradiation is relatively small (~2%). Error correction codes (ECC) can be used to

correct bit errors in the PUFs. However, we observe a monotonic increase in HD with an increase in the total dose with both vendors. We find that the HD exceeds 15% after TID = 100 krad(Si) for the IDT chip, and 9% for the Cypress chip. While the errors can be corrected using powerful ECCs, most ECC implementations require significant on-chip area and time overheads that scale up with the number of errors that need to be corrected. Furthermore, the ECCs require the generation and storage of helper data that are used later for error correction. The overhead due to helper data scales up exponentially with the bit error rate. For example, correcting 6% of errors requires ~3.68 bits per one valid PUF bit, whereas correcting 15% of errors requires ~23.43 bits per one valid PUF bit [81]. In addition, helper data, typically stored in non-volatile memory, can be a source of information leakage if not handled properly.

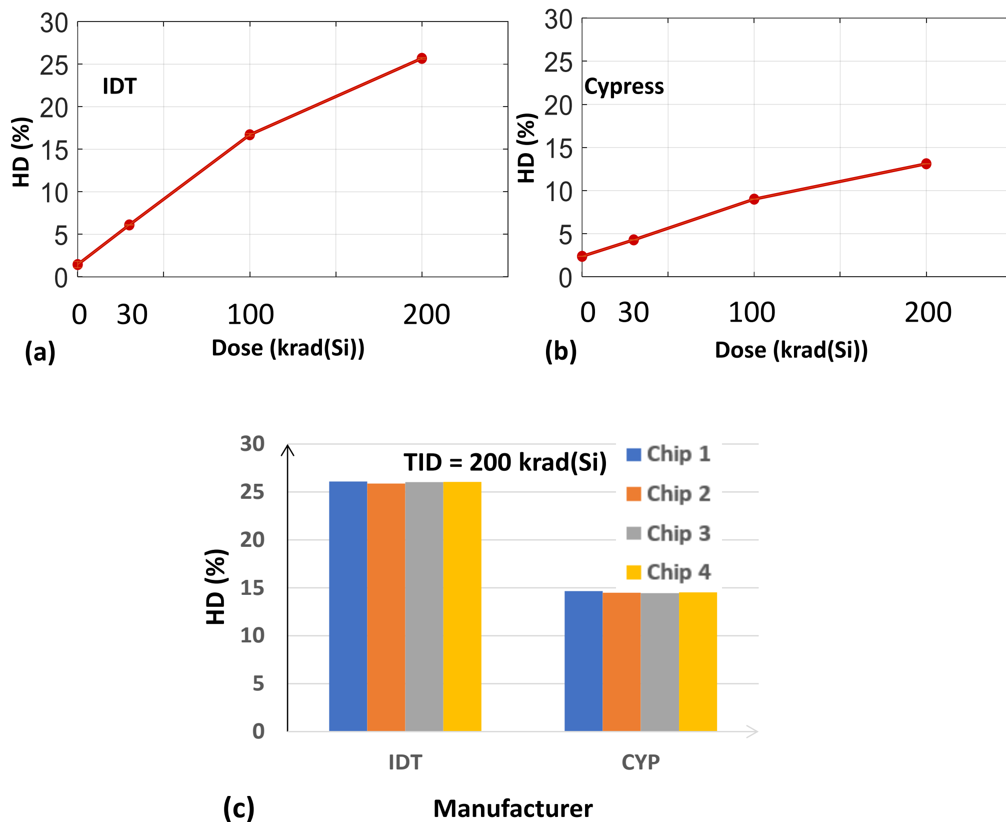


Figure 5.3 HD of SRAM-PUF as a function of total dose for COTS memory chips from (a) IDT and (b) Cypress. (c) Chip-to chip variation results of HD after irradiation (TID = 200 krad(Si)). Four identical SRAM chips from IDT and Cypress are used.

For the reasons discussed above we conclude that the SRAM PUFs may not be an ideal choice for encryption-key generation purposes which require zero bit-error rate (BER) after they are exposed to a moderate amount of irradiation ($TID = 100\ krad(Si)$). If they are used in radiation-prone environments, their implementations should involve powerful ECCs and provisions to prevent information leakage through helper data. However, SRAM PUFs may still be usable for device authentication applications. Since the inter-die HD remains close to 50% even after irradiation, there exists a significant gap between intra-die and inter-die HD values. Hence, depending on the rejection thresholds, the PUF may still be used for authentication purposes, similar to what Lawrence *et al*. [72] concluded.

Figure 5.3(c) shows chip-to-chip variation in the HD values after irradiation. Four identical standalone SRAM chips from IDT and Cypress were used in this study. We find minimal variation across different chips within the same family of chips. Relatively high HDs are observed in all SRAM chips after irradiation. The IDT chips are seemingly more susceptible to power-up state degradation than the Cypress chips. This might be due to differences in the process technology between the two families of chips. Note that our goal in this work is not the comparison between two different SRAM chips, but to highlight the universality of SRAM PUF characteristics under irradiation. **Table 5.2** summarizes the characterization results by reporting HD and HW as a function of TID. We do not find any significant changes in the HW due to irradiation. We tested the chips up to 100 krad(Si) as parts in a geosynchronous earth orbit (GEO) satellite receive around 100 krad(Si) during their average lifetime of 10 years [82]. Note that we have verified the basic functionality of the chip after irradiation by performing write and read operations with random data. We find that all the SRAM chips remain fully functional after irradiation.

Table 5.2 Summary of TID effects on SRAM-PUFs.

	IDT		CYPRESS	
TID (krad(Si)	HD(%)	HW(%)	HD(%)	HW(%)
0	1.45	44.75	2.38	50
30	6.11	45.05	4.29	49
100	16.71	44.90	9.01	49
200	25.69	45.62	13.11	50

5.4.1.2 Total Dose Induced Unstable Power-Up Bits

We perform a bit-by-bit analysis of total dose effects on SRAM PUF degradation. We classify SRAM-PUF bits into three categories as follows: strongly skewed to zero, strongly skewed to one, and unstable bits [60]. **Figure 5.4**(a) illustrates our classification method. We define unstable PUF bits as those bits which flip their state during consecutive PUF generation whereas strongly skewed bits are those that retain their state (zero or one) during successive PUF generation. The strongly skewed bits are stable PUF bits because random electric noise is not sufficient to change their states on consecutive power-up read operations.

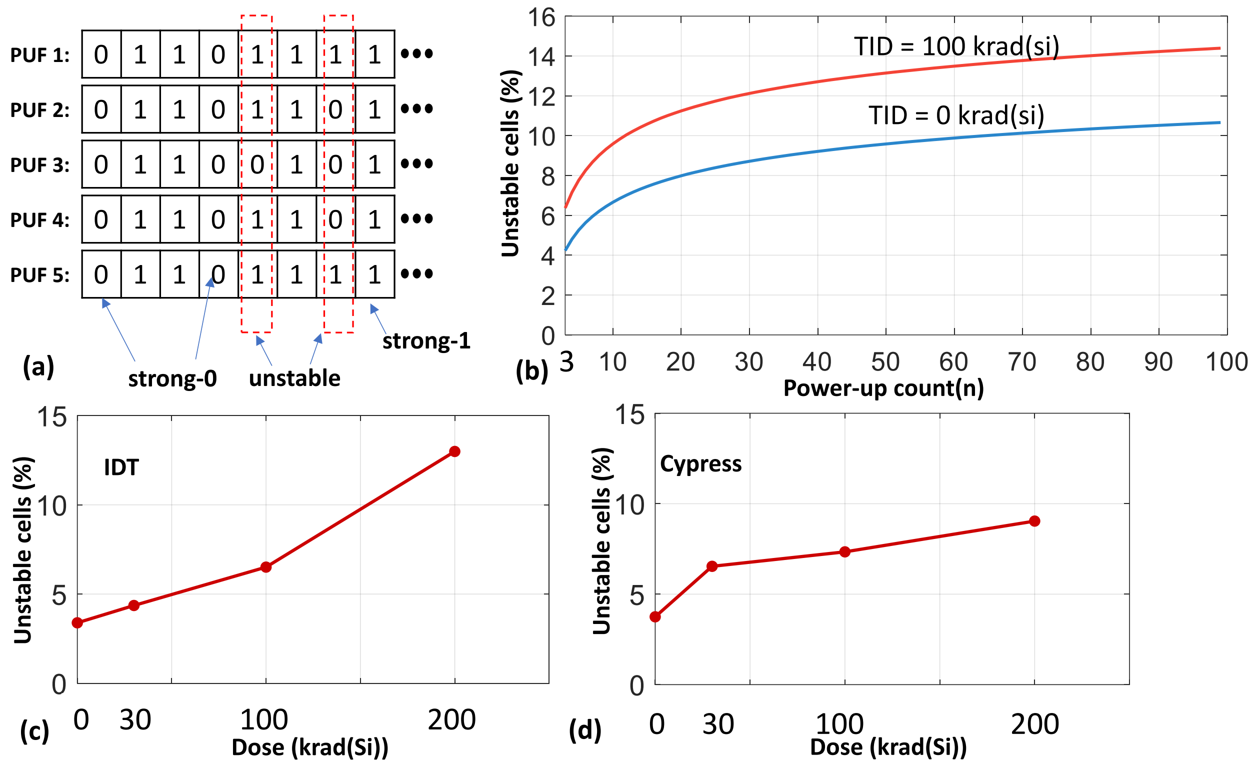


Figure 5.4 (a) Classification of SRAM-PUF bits as strong-0, strong-1 and unstable bits. (b) Percentage of unstable PUF bits as a function of power-up read counts (n). Unstable PUF bits as a function of the total dose for COTS memory chips from (c) IDT and (d) Cypress.

Figure 5.4(b) shows the percentage of unstable bits in 1Mb SRAM PUF as a function of the number of power-up read operations (n). The number of unstable PUF bits is increasing with an increase in the number of power-ups. However, only a tiny fraction of additional unstable bits is identified after a certain number of power-up operations ($n > 50$). Ideally, a larger number of power-up reads are necessary for accurately estimating the percentage of unstable PUF bits. Unfortunately, we have used only $n = 5$ power-up reads to estimate the number of unstable bits to minimize measurement time during irradiation experiments. Thus, the percentage of unstable bits we report here underestimates the actual percentage of unstable PUF bits. Nevertheless, our main focus here is the exploration of a relative trend in the percentage of unstable bits as a function of total dose and we believe that $n = 5$ is sufficient to capture this trend.

Figure 5.4(c) and (d) show the percentage of unstable PUF bits as a function of the total dose for IDT and Cypress chips, respectively. Chips from both vendors show a similar-looking trend where the percentage of unstable bits gradually increases with an increase in the total irradiation dose. It is well known that ionizing radiation introduces defect states in the MOS structures, which increases the low-frequency or 1/f noise in semiconductor devices [37], [49], [83]. We believe the effects of radiation-induced defects in the MOS structure are reflected in terms of an increased count of unstable PUF bits which in turn increases the HD of the SRAM PUF after irradiation.

5.4.1.3 Root Cause Analysis

We first provide a conceptual framework to understand the power-up transients of SRAM cells and then provide an explanation of the effects of irradiation on it. During the first few picoseconds after power-up (Phase-1 of transient behavior), the behavior of the cross-coupled CMOS inverters is critical in determining its steady state power-up state. **Figure 5.5**(a) shows the schematic of the SRAM cell with the ON/OFF conditions of the individual transistors during the initial phase (Phase-1) of power-up. Note that all the NMOS transistors (2 access transistors and 2 pull-down NMOS transistors) are turned off during the initial phase of power-up. The access transistors connected to the output nodes remain OFF throughout the power-up phase as word lines remain grounded. The NMOS transistors of the cross-coupled inverters remain OFF during the first few nanoseconds after power-up as output node voltages (V_{out1} and V_{out2}) take some time to reach a value greater than the threshold voltages of NMOS transistors.

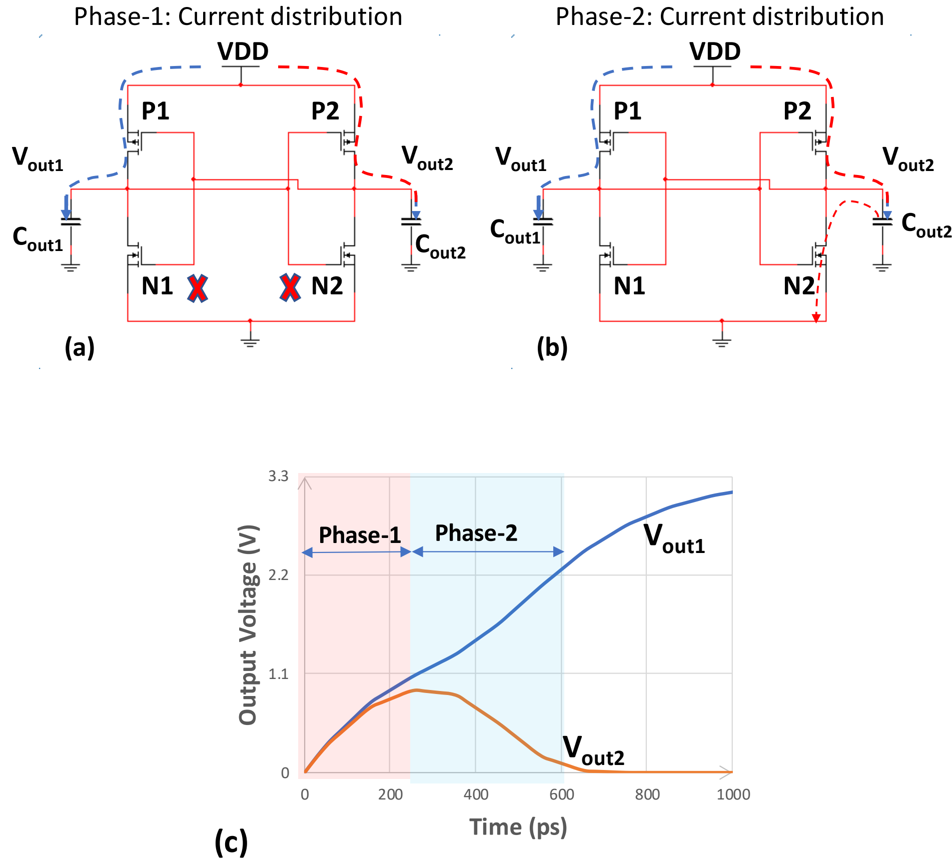


Figure 5.5 (a) Schematic of a SRAM cell used for simulation. The current distribution corresponds to the phase-1 of the power-up transient. (b) Current distribution during phase-2 of the power-up transient. (c) Transient power-up characteristics of the output nodes.

We use two equivalent output capacitors on the output nodes of the cross-coupled inverters to capture the total output capacitance including the access transistors. Note that both the PMOS transistors are turned on initially and transient current flows through them charging the output nodes (V_{out1} and V_{out2}). If there is a mismatch in the PMOS transistors' current, one output node may charge faster than the other which may eventually decide the steady power-up state of the cell. For example, if the current through the P1 transistor is higher than the current through P2, the output voltage V_{out1} will rise faster than V_{out2}. It will turn on the NMOS transistor N2 earlier than N1 causing faster discharge of the capacitor C_2. We illustrate the discharging event in **Figure 5.5**(b) as the second phase of the power-up transient. Eventually, V_{out1} reaches V_{DD} and V_{out2} reaches

ground potential as illustrated in **Figure 5.5**(c). We use HSPICE simulation to generate **Figure 5.5**(c). Simulation parameters are summarized in **Table 5.3**. Note that we have chosen all device parameters for both inverters to be identical, except for the threshold voltage (V_t) magnitude which is chosen slightly lower for the P1 transistor than P2. Such a small mismatch in V_t values eventually decides the power-up state of a cell as shown in **Figure 5.5**(c). There can be several process variables that can cause the mismatch between the transient current, deciding the ultimate power-up state. Thus, **Figure 5.5**(c) needs to be treated as an illustrative example to understand the transient behaviors of the SRAM cell during the power-up phase.

Table 5.3 Hspice Simulation Parameters.

Parameters	Value
Sizing of pull-up PMOS	W=200 nm, L=100 nm
Sizing of pull-down NMOS	W=600 nm, L=100 nm
Output capacitor	10 pF

Ionizing radiation significantly changes the power-up transient current of the SRAM cell due to the following reasons: (a) irradiation introduces defects in the MOS structure causing random current fluctuations, and (b) irradiation causes charge trapping in the oxide layer altering the threshold voltage of transistor [37], [49], [83]. Based on these two effects, we illustrate the PUF degradation with the total dose in the following paragraphs.

5.4.1.4 Effect of Irradiation-Induced Defects

Figure 5.6 illustrates the effects of interface defects during the power-up transient. Defects near the Oxide-Si interface in the MOS structure (see **Figure 5.6**(a)) cause fluctuation in current conduction characterized by low-frequency noise [37], [49], [83]. **Figure 5.6**(b) shows a sketch for

random current fluctuation through the PMOS transistors affected by noise. If the current fluctuation is significant during the power-up transient (Phase-1), unstable power-up states will be observed. For example, **Figure 5.6**(c) and **Figure 5.6**(d) show two cases where current fluctuation during Phase-1 of the power-up transient forces a cell to either of the two power-up states. Since noise amplitude increases after irradiation, such unstable behavior is expected to increase on the irradiated chip as confirmed by our experimental evaluation in **Figure 5.4**.

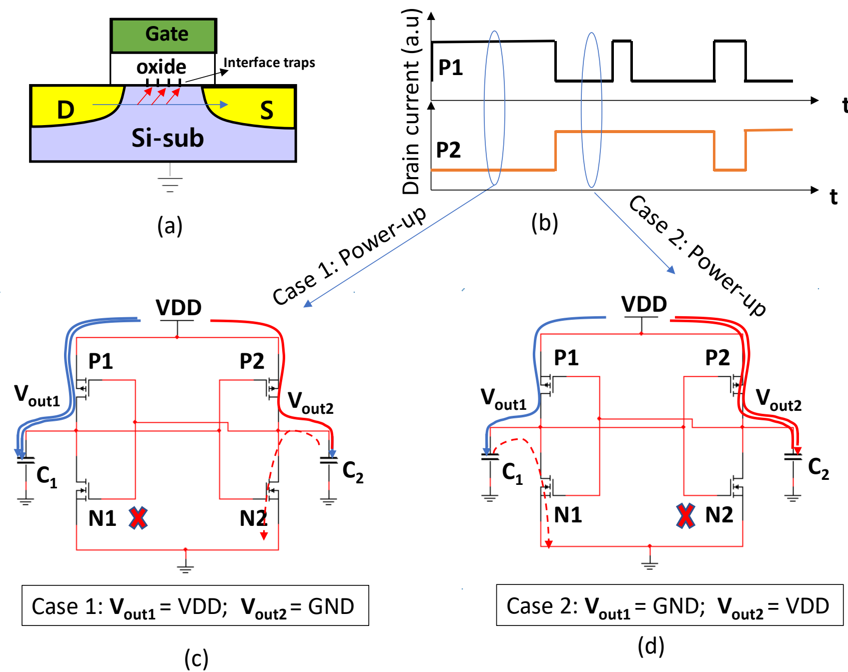


Figure 5.6 (a) Schematic of a transistor with interface defect. (b) Current fluctuation caused by low-frequency noise. (c) & (d) Current transient leading to two different power-up states corresponding to different drain current values during power-up.

5.4.1.5 Effect of Charge Trapping in Oxide

Ionizing radiation causes charge trapping in the oxide layer (mainly holes) causing an increase in threshold voltage magnitude for PMOS and a decrease in threshold voltage magnitude for NMOS (see **Figure 5.7**(a)). If the radiation-induced V_t shift of one of the PMOS transistors of a single memory cell is considerably higher than the other, then the output node corresponding to

that PMOS transistor will have a lower charging current, forcing that node to settle at the ground state irrespective of its power-up state before irradiation. Similarly, if one of the NMOS transistor's V_t gets significantly lower compared to the other NMOS, then the output node corresponding to the low-V_t NMOS will end up at the ground state (see **Figure 5.7**(b)). In other words, a PUF bit that remains in the "1" state during several subsequent power-on states (Strong-1) may get converted to a PUF bit that remains in the "0" state during several subsequent power-on states (Strong-0) after irradiation, and vice versa, due to significant and unequal shifts of threshold voltages of the individual transistors.

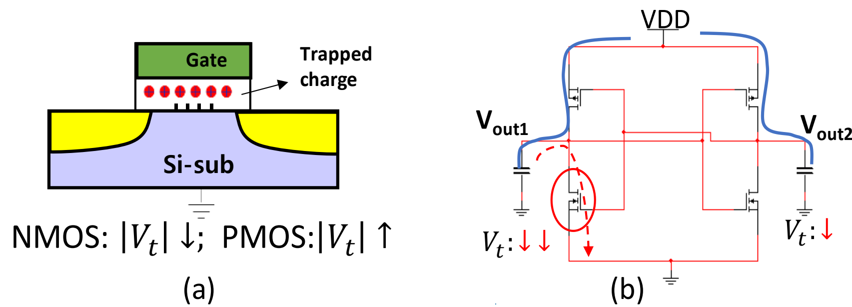


Figure 5.7 Radiation induced charge trapping effect in the (a) oxide and (b) the corresponding current transients during power-up phase.

5.4.1.6 Room Temperature Annealing Effects on Irradiated Chips

In this section, we analyze the room temperature annealing effects on irradiated SRAM chips. The irradiated chips were kept at room temperature with all pins floating. We measure the power-up state and compute the PUF Hamming distance following the same procedure described by Eq.(5.1) in 5.2. **Figure 5.8**(a) and (b) show the results for the IDT and Cypress chip respectively. The chips are allowed to anneal at room temperature for over 5 months. We observe a consistent trend of decreasing HD over time from both vendors. A significant decrease in HD seems to

happen in the first few days after irradiation. However, even after 5 months of room temperature annealing period, more than 60% of the erroneous PUF-bits remained in the erroneous state. We know that trapped holes in the oxide layers anneal through thermal or tunnel annealing [84] and also neutralize through hydrogen diffusion [85]. This possibly causes the transistor's threshold voltage to partially regress to its initial state. Lawrence, S. P., *et al.* observed a small increase in HD in a 24-hour anneal period [72]. In general, the post-irradiation annealing response of SRAM cells depends on several factors including bias conditions during irradiation and annealing, anneal duration, total dose during irradiation, and device layout [86].

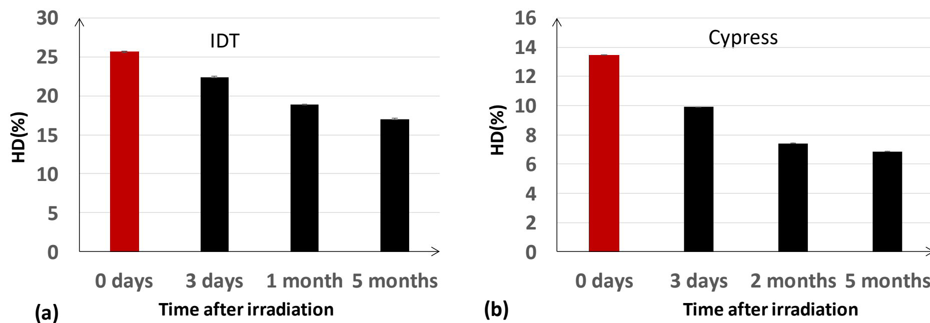


Figure 5.8 Relaxation effects for (a) IDT (b) Cypress chip.

5.4.2 TID Effects of Stored Data and Technology Node

The irradiation experiments were conducted at The Ohio State University Nuclear Reactor Laboratory, utilizing the underwater Gamma Irradiator [87]. The Co-60 source employed in the experiments provided a dose rate of 11.7 krad(Si)/h. The Gamma Irradiator consists of a vertically extending 6-inch diameter dry tube positioned within a light water pool. Twenty-five Co-60 pins were placed around the tube to ensure a uniform radiation field featuring gamma rays at energies of 1.173 MeV and 1.332 MeV. The gamma irradiation process involved subjecting packaged TSOP (thin small outline package) devices to radiation, while the chips remained powered on.

Commercial off-the-shelf (COTS) SRAM chips from Cypress, ISSI, and Alliance were utilized in the experiments. Details of the chips are given in **Table 5.4** [88], [89].

Table 5.4 Summary of Chip Specification.

	Cypress 150 nm	Cypress 90 nm	Cypress 65 nm	ISSI 110 nm	Alliance 200 nm
Part Number	CY7C1041CV33	CY7C1041DV33	CY7C1041G30	IS61WV25616BLL	AS7C34098A
Capacity	4 Mb	4 Mb	4 Mb	4 Mb	4 Mb
Input voltage	–0.5 V to 4.6 V	–0.3 V to 4.6 V	–0.5 V to 3.8 V	–0.3 V to 3.9 V	–0.5 V to 3.8 V
Word size	16 bits	16 bits	16 bits	16 bits	16 bits
Temperature	–40 °C to +85 °C	–40 °C to +85 °C	–40 °C to +85 °C	–40 °C to +85 °C	0 °C to +70 °C
Timing	10 ns	10 ns	10 ns	10 ns	10 ns

The experimental flow is as follows. We gather 101 power-up states and create a majority voting-based GoldPUF. Before irradiating the chips, we pre-characterize each chip to obtain their baseline performance. We prime the chips with different data patterns and then irradiate them to analyze the effects of stored data during irradiation on power-up states. The chips remain powered on during irradiation for each dose step. We then retrieve the power-up states of the irradiated chip immediately after irradiation (within 5 minutes). We generate 25 different authentication PUFs from each chip using power on/off cycling. Each authentication SRAM PUF is compared to the corresponding GoldPUF to compute HD. We take the average of the 25 different HD values and plot it in the subsequent analysis. For the technology-node analysis, the procedure remains the same as above, however, the chips are exposed to irradiation in a powered-off state with all pins grounded.

5.4.2.1 Baseline Characterization Results

The baseline power-up states for different SRAM chips are characterized for the unirradiated condition. The corresponding HD% and Unstable cells% are shown in **Figure 5.9**. We define unstable cells as those that flip their state during consecutive PUF generations. The

procedure to determine unstable cells is described in 5.4.1.2. The percentage of cells with power-up state at logic-1 is about 50% for all chips. We use 25 authentication PUFs to obtain the HD% and Unstable cells%. Variation among the 25 PUFs is not significant as shown in the Box Whisker plot for HD%. We observe a monotonic increase in HD% for different Cypress SRAM chips, where chips manufactured using lower technology nodes have a higher HD%. We have also analyzed the PUFs generated from different locations of the chips and have found that the PUF metrics, such as HD% and Unstable cell%, remain relatively stable across different regions of a given memory chip.

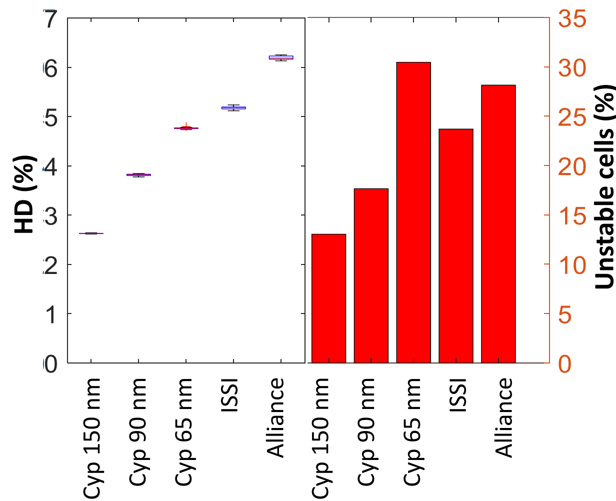


Figure 5.9 Baseline HD% and Unstable Cells% characterization of SRAM samples.

5.4.2.2 Effects of Stored Data on the Power-Up State

Figure 5.10 shows the effects of priming SRAM chips with various data patterns during radiation exposure. We divide every chip into 4 quarters and then program every quarter with a different data pattern, as follows: All-zero, All-one, GoldPUF, and inverted GoldPUF. **Figure 5.10**(a) shows the HD% for the 150 nm Cypress chip. We observe a monotonic increase in HD% with an increase in TID, regardless of the data stored. Interestingly, we observe a distinct difference in the slope of HD% increase as a function of the data pattern. The rate of increase in HD% with

TID is significantly lower for the cells primed with the GoldPUF than for the cells primed with the inverted GoldPUF. The HD% of regions primed with the All-zero and All-one data pattern is identical, and they are approximately the average value of the HD% of the regions primed with the GoldPUF and inverted GoldPUF. Since the All-zero and All-one data pattern can be considered as a superposition of the GoldPUF and the inverted GoldPUF, their effects on PUF degradation show the averaging behavior. **Figure 5.10**(b) shows the percentage of unstable cells as a function of TID. Holding the GoldPUF in SRAM during irradiation lowers the percentage of unstable bits, whereas holding the inverted GoldPUF increases the percentage of unstable bits. The results in **Figure 5.10**(a) and (b) thus imply that it is advantageous to keep the Cypress SRAM memory in the typical power-up state, which is very similar to the GoldPUF, during irradiation to minimize PUF degradation due to TID effects. However, these trends are not universal for SRAM chips coming from different manufacturers.

Figure 5.10(c) and (d) show the HD% and Unstable cells% for the ISSI chip, respectively. A notable contrast in behavior is evident between the Cypress and ISSI chips. In the case of the ISSI chips, the rate of increase in HD% is markedly lower when holding the inverted GoldPUF compared to holding the GoldPUF. In fact, we even observe a reduction in HD% for the ISSI chip holding the inverted GoldPUF after TID = 10 krad(Si). Hence, it proves advantageous to toggle the power-up state of the ISSI chip when it is in an idle state during irradiation, to minimize TID effects on its PUF characteristics.

Figure 5.10(e) and (f) show the HD% and Unstable cells% for the Alliance chip, respectively. Similar to the ISSI chip, we observe a lower rate of increase of HD% when holding the inverted GoldPUF during irradiation. Unlike the other chips, we find a saturation in HD% for

regions holding the GoldPUF for TID > 50 krad(Si). Thus, we find a converging HD% for different data patterns for TID > 50 krad(Si).

Figure 5.11 provides an elucidation for the disparate behavior exhibited by these chips. In our analysis, we leverage two key observations concerning the effects of TID on MOS structures. Firstly, we find that TID induces a downshift in the threshold voltage of MOS transistors, leading to a decrease in the magnitude of V_t for NMOS transistors and an increase in the magnitude of V_t for PMOS transistors. This shift is observed assuming a positive V_t values for NMOS and negative V_t values for PMOS transistors. Secondly, we note that there is an asymmetry between the V_t shifts between NMOS/PMOS in the ON/OFF states [73], [90]. By taking these observations into account, we provide a plausible explanation for the dependency of SRAM PUF integrity on data patterns held during irradiation in the following paragraphs.

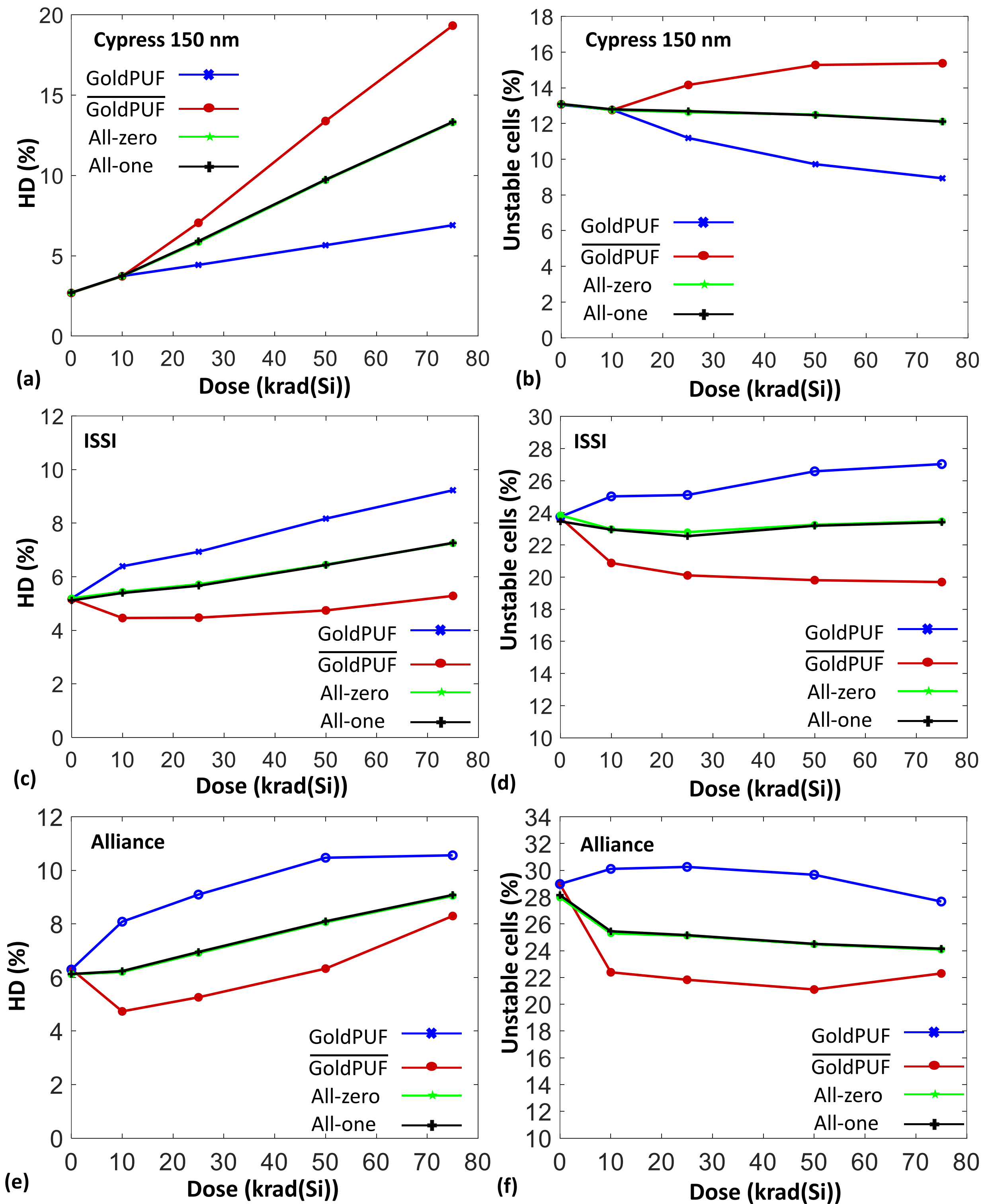


Figure 5.10 Effects of data stored on HD% and Unstable cells% (a) Cypress HD% (b) Cypress Unstable cells% (c) ISSI HD% (d) ISSI Unstable cells%. (e) Alliance HD% (f) Alliance Unstable cells%.

Figure 5.11(a) elucidates the TID effects on Cypress SRAM chips. Consider an SRAM cell with a default power-up state set to “0” (**Figure 5.11** (a)), denoting $Q/\bar{Q} = 0/1$. Assume that its power-up state is determined by the mismatch between the NMOS transistors. In this case, the threshold voltage relation $V_t^{N_1} < V_t^{N_2}$ will lead to power-up $Q/\bar{Q} = 0/1$. If the cell is irradiated in its default state (N_1 turned ON and N_2 is OFF) as per [73], we can expect $\Delta V_t^{N_1} > \Delta V_t^{N_2}$, implying $V_t^{N_1} \ll V_t^{N2}$ after irradiation (since ON-NMOS experience a larger threshold voltage shift than ON-PMOS, *i.e.*, NMOS dominant). This preserves the power-up state as explained in Ref. [73], reinforcing PUF stability. In contrast, if the cell is irradiated in its inverted PUF state (N_1: OFF and N_2: ON) we can expect $\Delta V_t^{N_2} > \Delta V_t^{N_1}$, which may lead to $V_t^{N1} > V_t^{N2}$ after irradiation. This will flip the preferred power-up state leading to a higher HD%, as observed in Cypress chips.

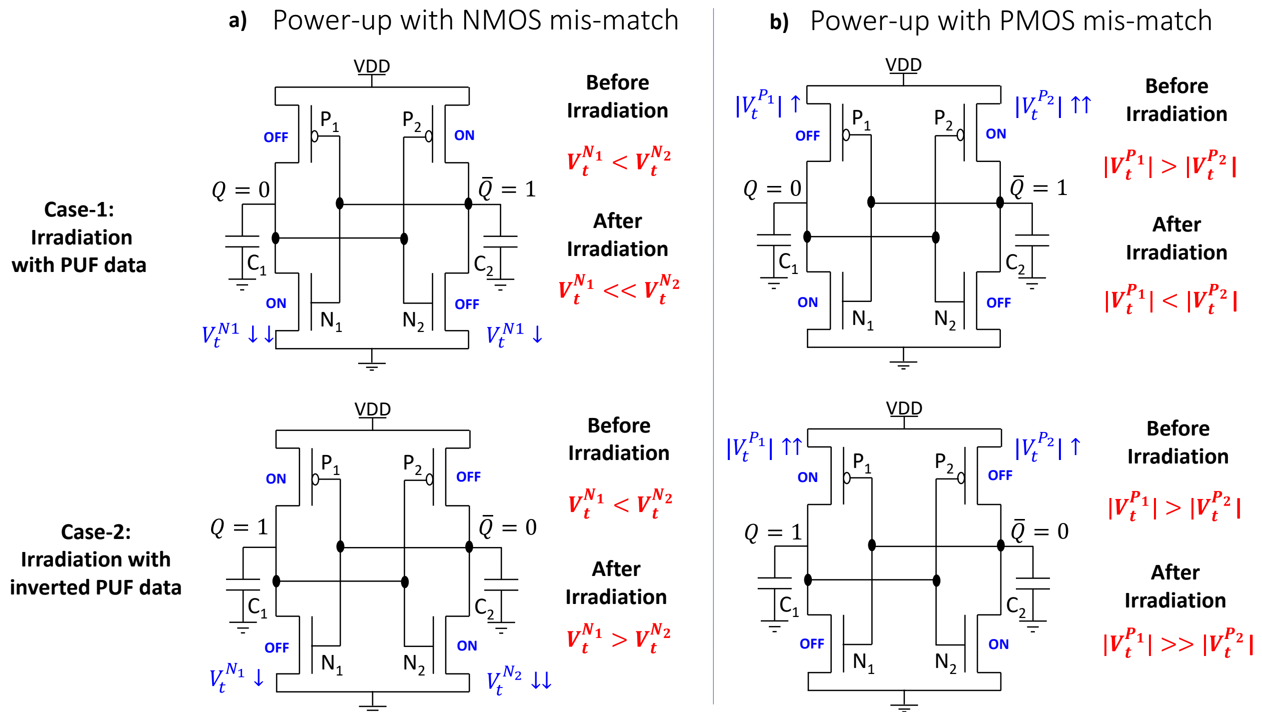


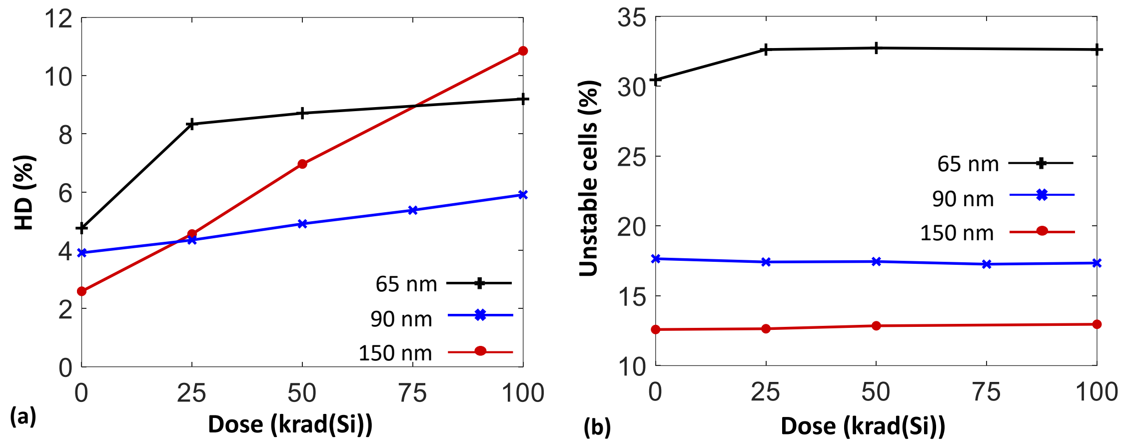
Figure 5.11 Effects of data pattern on power-up state of irradiated SRAM cells. We assume two cases: (a) an SRAM cell whose power-up state is dictated by mismatched NMOS transistors and (b) an SRAM cell whose power-up state is dictated by mismatched PMOS transistors.

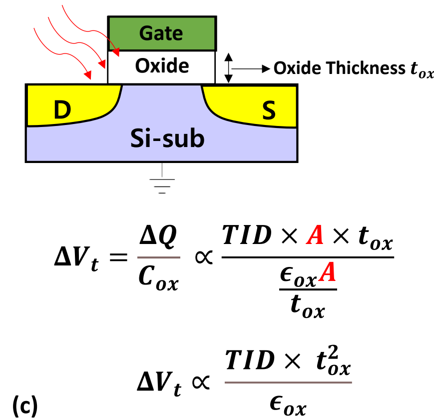
The behavior of the ISSI and Alliance chips is explained in **Figure 5.11**(b). In contrast to the Cypress chips, we assume the Alliance and ISSI chip's post-radiation power-up characteristics are predominantly determined by the PMOS transistors, as noted in Ref. [90]. In other words, for a preferred power-up state of $Q/\bar{Q} = 0/1$, if the cell is exposed in its PUF state (P_1: OFF and P_2: ON) we can expect $|\Delta V_t^{P2}| > |\Delta V_t^{P1}|$, potentially leading to $|V_t^{P1}| < |V_t^{P2}|$ after irradiation. This would result in switch of the preferred power-up state of the cell, leading to a higher HD% after irradiation. Ref. [90] reaches a similar conclusion regarding the explanation of reverse pattern imprinting after irradiation. In contrast, if the cell is exposed in its inverted state (P_1: ON and P_2: OFF), we can expect $\Delta V_t^{P1} > \Delta V_t^{P2}$ resulting in $|V_t^{P1}| \gg |V_t^{P2}|$ after irradiation. This would preserve the power-up state. More importantly, this stabilizes the power-up state of memory cells that show unstable power-up characteristics. Hence the HD% of the PUF will decrease after irradiation as observed for the ISSI and Alliance chips after TID = 10 krad (Si).

Based on the aforementioned explanation, we propose that TID effects cause an asymmetric V_t shifts between NMOS and PMOS transistors, as reported in Ref. [73], [90]. Specifically, in the Cypress chip, the TID-induced threshold voltage reduction in the ON NMOS transistor is more pronounced compared to the ON PMOS transistor. Conversely, the ISSI and Alliance chips exhibit the opposite trend. Please note that the specific properties of individual transistors within the SRAM memory arrays are proprietary, preventing us from confirming our hypothesis. Nonetheless, our explanations and hypothesis offer a straightforward yet consistent framework for understanding the TID effects on the power-up characteristics of SRAM memory. In general, both NMOS and PMOS transistors' mismatch can simultaneously affect the power-up transients. Consequently, a more detailed modeling framework is required to predict the TID effects on SRAM PUF characteristics for a broader TID range [86].

5.4.2.3 Technology-Node vs. TID Effects on PUF

In this section, we compare the PUF response of different Cypress SRAM chips manufactured using 65 nm, 90 nm, and 150 nm technology nodes (see **Table 5.4** for chip details). **Figure 5.12**(a) and (b) show the HD% and Unstable cells% as a function of TID, respectively. We find that SRAM PUFs from smaller technology nodes show a higher HD% and Unstable cells% before irradiation than the corresponding ones manufactured using larger technology nodes. This can be explained by a higher vulnerability of smaller-node SRAM cells to thermal noise. The 65 nm chip shows the highest resilience to radiation (with the smallest slope) beyond 25 krad(Si). The 90 nm chip performs the second best with a gradual but less steep slope when compared to the 150 nm sample. The 150 nm shows the highest increase in HD% overall. This result suggests that even though smaller cells are more susceptible to thermal noise, they may be less affected by TID. We can explain this through the equations in **Figure 5.12**(c). We see that the TID-induced change in the threshold voltage (ΔV_t) depends on the square of the oxide thickness (t_{ox}), *i.e.*, $\Delta V_t \propto t_{ox}^2$. The 65 nm chip will have the smallest gate oxide thickness, resulting in the gentle HD% slope after TID = 25 krad(Si). The 150 nm chip will have the thickest gate oxide layer resulting in the highest change in V_t values of its constituent transistors. Thus, the SRAM PUFs from 150 nm node chips exhibit the highest HD% after a TID of 100 krad(Si). The 65 nm chip starts at the highest HD% and also a significantly higher unstable cells% compared to the 90 nm chip, possibly accounting for the steep rise in HD% between 0 and 25 krad(Si). Note that there could be more factors at play, for example, trap location (oxide vs. oxide-interface traps), but these are believed to be less impactful in nano-scale devices [6]. From our analysis, it appears that the 90 nm technology node offers a good balance between TID resistance and initial HD% suggesting its use could be more suitable for TID prone environment.





$$\Delta V_t = \frac{\Delta Q}{C_{ox}} \propto \frac{TID \times A \times t_{ox}}{\frac{\epsilon_{ox} A}{t_{ox}}}$$

(c)

$$\Delta V_t \propto \frac{TID \times t_{ox}^2}{\epsilon_{ox}}$$

Figure 5.12 TID effects on different technology nodes (a) HD% (b) Unstable cells%. (c) Threshold voltage change as a function of oxide thickness.

5.4.2.4 Room Temperature Anneal

In this study, we allow the irradiated chips from various technology nodes to anneal over time at room temperature. The chips are kept grounded during the anneal. From previous works, we can expect a decrease in the overall HD% due to small threshold voltage regression [86], [91], [92]. **Figure 5.13**(a) and (b) show the HD% and Unstable cell% as a function of annealing time, respectively. Expectedly, the HD% decreases over time. However, even after an extended period of annealing, the HD% is significantly higher than the pre-irradiation baseline. The 150 nm chip

that showed the highest increase in HD% also shows the highest degree of annealing. Despite a higher degree of annealing from the 150 nm sample, the 90 nm chip shows the best HD% performance for the same reasons discussed in the previous section. The Unstable cells% remains relatively unchanged even after an extended period of time.

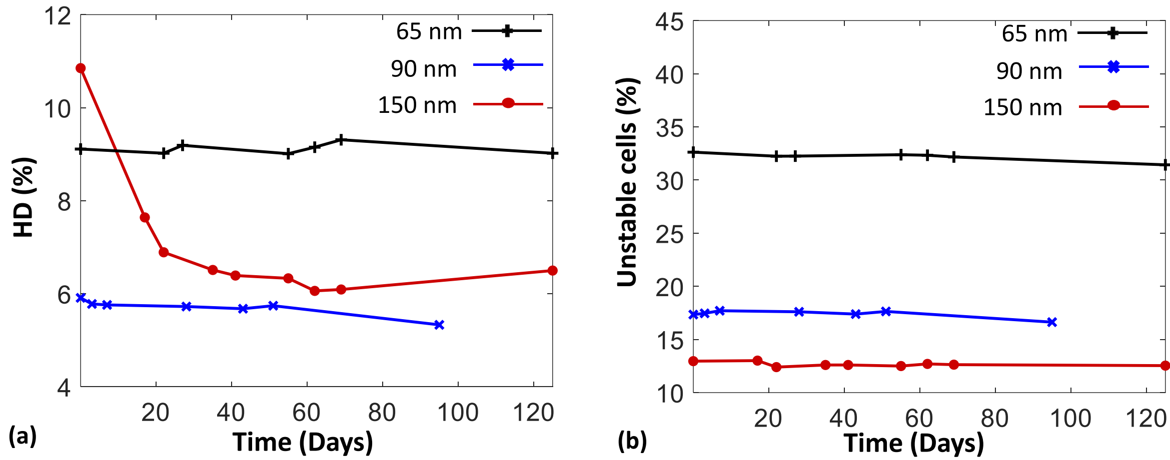


Figure 5.13 Effects of room-temperature annealing on SRAM PUF. (a) HD (%) and (b) Unstable cell (%) are plotted as a function of anneal duration. The chips were kept in the unpowered state with all pins grounded during annealing.

5.5 Conclusions

In summary, we find that the power-up states of SRAM cells in commercial SRAM chips are significantly altered by ionizing radiation. The intra-die HD of PUFs drastically increases with an increase in the total irradiation dose exceeding more than 15% after 100 krad(Si) for a family of chips. Thus, SRAM PUFs are not suitable for encryption key generation purposes after a moderate amount of irradiation ($TID = 100\ krad(Si)$) unless they are accompanied by strong error-correction codes. However, depending on the selection of rejection thresholds, the SRAM PUF may still be used for authentication purposes. We observe small annealing effects over time, but the HD remains high even five months after irradiation. This reveals an urgent need for active mitigation strategies to protect the PUF from Ionizing radiation.

In pursuing mitigation strategies, we find that the following:

1. The data stored in the SRAM memory array during irradiation impacts post-irradiation power-up states. The cells containing either their default power-up state or the inverted power-up state are more immune to TID effects, contingent on their physical properties. For Cypress chips, holding the PUF state during irradiation proves effective in reducing PUF degradation, while in the case of ISSI and Alliance chips holding the inverted PUF state proves advantageous.
2. Chips manufactured using smaller technology nodes (90 and 65 nm) seem to exhibit greater resilience to TID effects compared to those manufactured using larger technology nodes (150 nm). However, due to higher instability in power-up transients of cells in smaller technology nodes, striking a balance between baseline performance and radiation response is crucial.
3. A room temperature anneal of chips in the grounded state reduces the HD% of the irradiated chips, approaching its pre-irradiation level over a span of several months.

Armed with these insights, we can make more informed choices in the parts selection phase of the design of systems operating in space and other radiation-prone environments. Through meticulous prior characterization, we can proactively counteract the effects of TID on the integrity of SRAM PUFs by priming a specific location of the SRAM array reserved for PUF with the appropriate data patterns. These findings will help further solidify the use of SRAM PUFs in radiation-prone environments.

Chapter 6. Data Pattern Imprinting Effects on SRAM Due to Ionizing Radiation

6.1 Introduction

Static Random Access Memory (SRAM) is a critical component in modern computing systems. Although it is a volatile memory, recent studies have highlighted a significant issue of data remanence in the SRAM arrays even after power off. The most common method of exploiting this vulnerability is through low-temperature data remanence attacks (cold boot) [93]. This attack involves using very low temperatures to briefly maintain data on the chip (~ few milli-seconds) after power is turned off. Additionally, a recent study introduces the concept of a *volt boot attack* [94], where external power is used to keep the SRAM module active, while the rest of the device remains powered down. Another area of research has revealed the phenomenon of data imprinting or burn-in effects in SRAM arrays. This phenomenon occurs due to prolonged data retention that is exacerbated by high temperatures [95].

Previous research has extensively studied the impact of ionizing radiation on the power-up state of SRAM in the context of the reliability of SRAM physical unclonable functions (PUFs) [96], [97]. However, using radiation to intentionally imprint data and intentionally alter power-up characteristics has been less explored. G. J. Brucker [98] used a high dose rate 10 MeV electron pulses to study data imprinting and found that the data present during exposure becomes imprinted onto the SRAM array, with a stronger dose resulting in a greater degree of imprint. J. T. Schott *et al.* [99] used gamma rays and showed that the imprinted data might be the opposite of the data held during exposure and confirmed the findings on radiation-hardened SRAM samples. These

studies, however, involved parts (~5 μm) that are considered obsolete in contemporary technology. Therefore, it is crucial to understand how modern components respond. J. Cui *et al.* [100] studied the effect of high-dose ionizing radiation on SRAM cell stability and noise margins and observed reverse imprinting in newer 65 nm technology node at very high doses (200 Mrad(Si)).

Recent studies have revealed that prolonged data retention or aging, especially when combined with high temperatures, can cause data imprinting effects in SRAM arrays [95]. During extended data retention periods, the threshold voltage mismatch between the two PMOS transistors intensifies, primarily due to negative bias temperature instability (NBTI). Numerous studies have delved into potential attack vectors relying on the NBTI phenomenon. A. Garg *et al.* [101] demonstrated the use of artificial aging through overvolting, which accelerates NBTI effects, to increase the predictability of the power-on state. J. Hovanes *et al.* [95] demonstrated imprinting an image on SRAM, by subjecting it to elevated temperatures, thus speeding up the NBTI. They achieved noticeable imprinting after about 12 hours of accelerated aging. While aging-induced imprinting can take a significant amount of time, ranging from days to years, radiation can cause imprinting much more rapidly, depending on the dose rate, posing a more substantial security risk.

6.2 Experimental Procedure

The irradiation experiments are performed at the Ohio State University's Nuclear Reactor Laboratory, in the underwater Gamma Irradiator using a Co-60 source with a dose rate of 11.4 krad(Si)/h. Gamma irradiation was performed on the packaged TSOP (thin small outline package) devices with SRAM chips powered on. Several COTS SRAM chips from Cypress, ISSI, Alliance, and IDT are used. They are all operated at their nominal power supply of 3.3 V.

In our experiment, we used a binary image of Albert Einstein **Figure 6.1**(a) containing 71.34% ones and 28.66% zeros. The image is of size 450×305 pixels and is stored as a linear array of size 137,250 bits. Each binary pixel is stored on one SRAM cell.

The experimental flow is as follows. Before irradiating the chips, we pre-characterize each SRAM chip to extract its baseline power-up state, referred to as the default power-up state. We prime the chips by writing the image and then irradiate them using a Co-60 source. The chips remain powered on during irradiation for each dose step. Immediately upon irradiation, we extract the new power-up state of the irradiated chip. The post-irradiation power-up state is compared to the original image to compute the percentage of matching locations, *Current Match%*. We can then calculate the *Imprint%* using the following equation:

$$Imprint\% = \frac{Current\ Match\,\% \ - Default\ Match\,\%}{100\% \ - Default\ Match\,\%} \times 100. \qquad (6.1)$$

Here, the *Default Match%* represents the percentage of matching locations between the image written onto the SRAM and the SRAM's default power-up state. The *Imprint%* ranges from 0% to 100%, where 0% indicates the unaltered default power-up state and 100% indicates a complete alteration or perfect imprinting with written data.

6.3 Experimental Results and Discussion

6.3.1 Baseline Characterization

To be able to study the effect of irradiation, we first obtain the baseline characteristics of the samples. We do so by obtaining 101 power-up states and computing the majority vote. **Figure**

6.1(b) shows the pre-irradiation visualization of the power-up state from the memory locations that will have the Albert Einstein image written onto during irradiation. We find that the baseline power-on has about 43% of the cells that match with the Einstein image (*Default Match%*). This then becomes our reference point with the *Imprint%* being 0%.

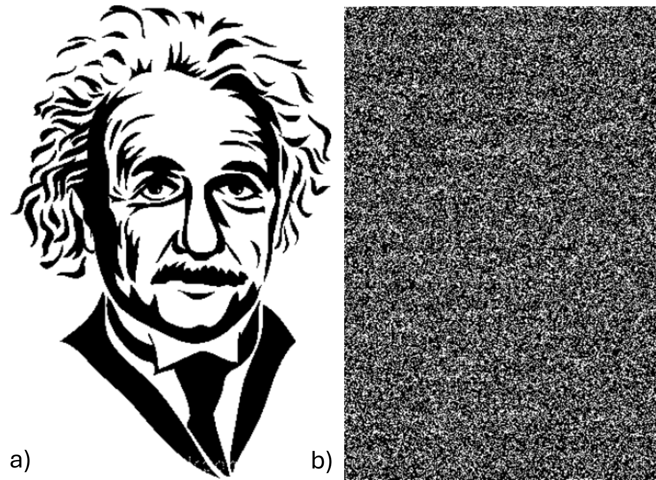


Figure 6.1 (a) Binary image of Albert Einstein, (b) Visualization of power-up state.

6.3.2 Data Imprinting as a Function of Dose

In this experiment, we used a COTS SRAM chip manufactured using a 250 nm CMOS process by Cypress (CYP 250 nm). The chip is primed by writing the Albert Einstein image. Figure 6.2 illustrates the power-up states of the SRAM chip as a function of the total ionizing dose (TID). The unirradiated SRAM's default power-up state, illustrated on the leftmost image, shows no signs of imprinting (*Imprint%=0*). In other words, merely writing the Einstein image onto the SRAM array at room temperature has no effect on its subsequent default power-up states. However, when subjected to irradiation, the power-up state undergoes significant changes due to imprinting. Images in Figure 6.2, corresponding to the same memory location, demonstrate these changes as a function of the TID level. Notably, the Einstein image begins to become apparent at 30 krad(Si)

with an imprint percentage of 15.65% and nearly reaches complete imprinting at 50 krad(Si) with a 96.75% imprint percentage.

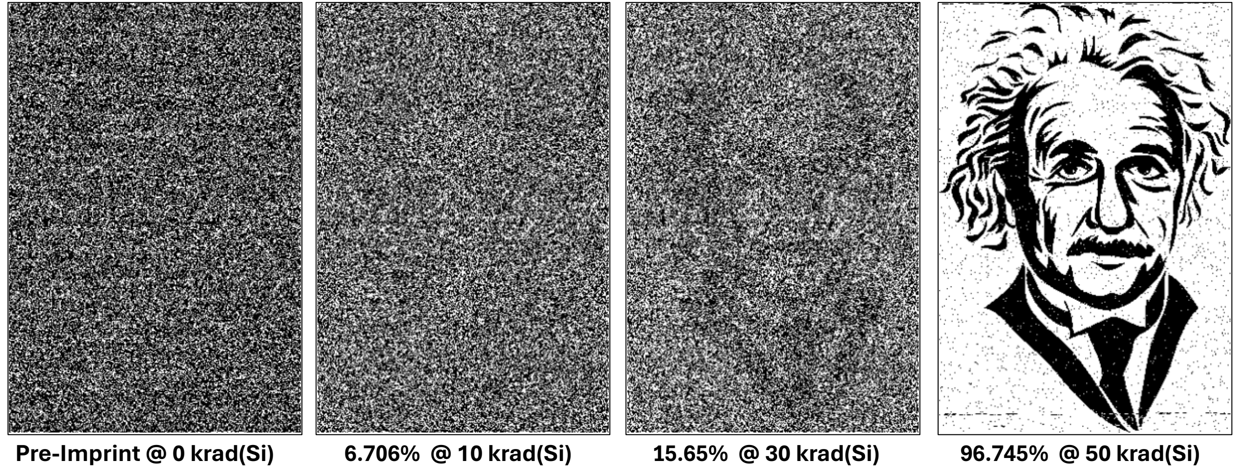


Figure 6.2 Progression of Imprint% with TID on the Cyp 250 nm sample.

6.3.3 Explanation of TID-Induced Data Imprinting

Ionizing radiation induces the trapping of positive charges in the oxide layers of transistors, leading to a reduction in the magnitude of the NMOS threshold voltage and an increase in the magnitude of the PMOS threshold voltage. The electric field across the oxide layer is a critical factor determining the density of trapped charges [6]. Consequently, there is a differential charge trapping based on whether the transistors are in their ON or OFF states. This charge trapping modifies the transistor's threshold voltage (V_{th}), meaning that the power-up state of the post-irradiated SRAM array can reveal previously stored data.

In **Figure 6.3** we delve deeper into the mechanism behind data imprinting. Consider a scenario where a state $Q = 1$ is written onto an SRAM cell, as depicted in **Figure 6.3**(a). Upon exposure to ionizing radiation, the ON transistors experience a greater threshold voltage shift than the OFF transistors. Let's assume that the power-up state of the SRAM cell is mainly dictated by the V_{th} mismatch between NMOS transistors (N_1 and N_2). Additionally, assume that $V_{th}^{N_2} > V_{th}^{N_1}$

before irradiation, which sets the default power-up state of the cell to $Q = 0$. However, post-irradiation this mismatch between the NMOS transistors may invert becoming $V_{th}^{N_2} < V_{th}^{N_1}$ due to differential charge trapping influenced by their ON/OFF states [102], as illustrated in **Figure 6.3**(b and c). Consequently, the SRAM cell's power-up state could shift to $Q = 0$ post-irradiation, effectively imprinting the data held by the cell during irradiation exposure.

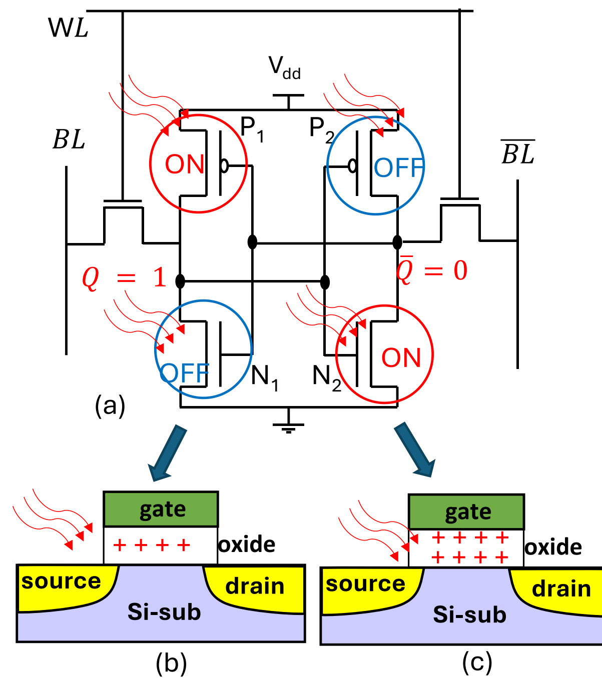


Figure 6.3 (a) SRAM cell holding $Q = 1$, during irradiation. Charge trapping effects on (b) OFF and (c) ON transistor.

6.3.4 Effects of Room Temperature Anneal on Imprinting

To examine the durability of the imprinting effects, we allow all irradiated samples to anneal with all pins grounded at room temperature. We monitor the progression of the *Imprint%* over time by reading their power-up states. **Figure 6.4** illustrates a gradual decrease in *Imprint%* in the CYP 250 nm sample as time passes. Consistent with previous studies, we anticipate charge de-trapping from the irradiated transistors with anneal duration [56], leading to a fading of the

imprinted data. Most of this regression appears to occur within the first week, slowing down in the subsequent weeks. Remarkably, even after 110 days, the power-on state still retains a somewhat discernable image with an imprint percentage of 17.477%.

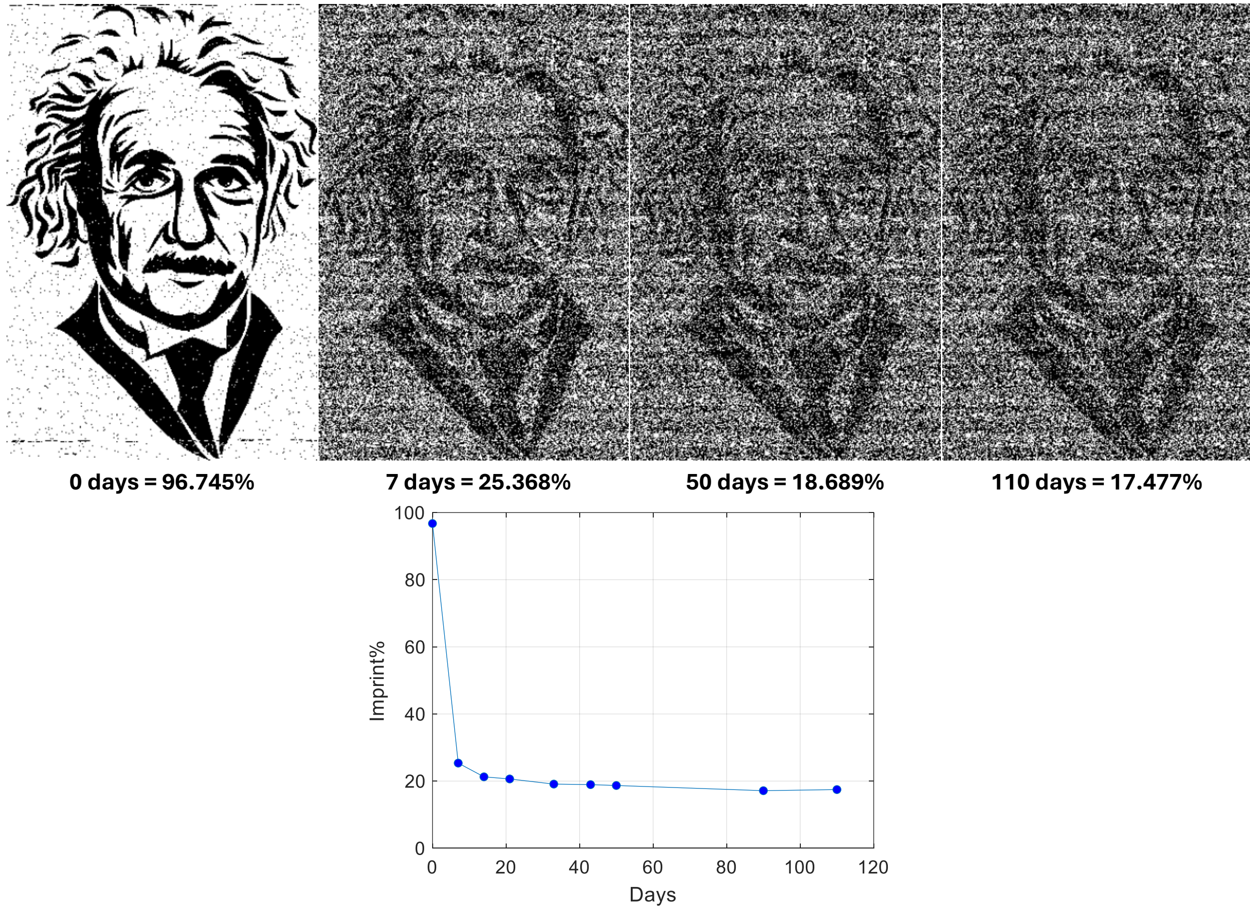


Figure 6.4 Effect of room temperature anneal on Imprint% of the CYP 250 nm sample.

6.3.5 Evaluation of Data Imprinting Effects on Multiple Chips

To validate our results further, we conducted the same experiment using different SRAM chips. **Table 6.1** shows the change in the imprint percentage as a function of TID across these samples. Notably, the 150 nm Cypress (CYP 150 nm) sample exhibited a positive imprint, whereas the ISSI and Alliance samples demonstrated a reverse imprint, meaning that holding one during irradiation converts its power-up state to zero. This reverse *Imprint%* can be attributed to the

power-on state being dominated by the PMOS transistors as explained in 5.4.2.2. For the IDT sample, which was directly exposed to 75 krad(Si), we noted an almost perfect imprint percentage of 98.699%.

Another critical aspect to consider is the total dose required to achieve a certain level of imprinting, which largely depends on the oxide thickness, and by extension, the device's feature length [102], [103]. This relationship is evident when comparing the CYP 250 nm and CYP 150 nm samples, which share similar construction. As noted earlier, the CYP 250 nm sample nearly achieves full imprinting at a TID of 50 krad(Si), whereas the CYP 150 nm sample reaches 13.691% at 75 krad(Si). This indicates that newer technology nodes with smaller feature sizes are more resilient to data imprinting.

Table 6.1 Summary of Imprinting on Multiple Chips.

Imprint%					
	CYP 250	CYP 150	ISSI	ALLIANCE	IDT
Dose (krad (Si))	CY7C1041BNV33	CY7C1041CV33	IS61WV25616BLL	AS7C34098A	IDT71V416S
10	6.706	1.670	-1.697	-2.912	-
25	-	4.195	-2.126	-3.309	-
50	96.745	9.091	-2.938	-3.597	-
75	-	13.691	-3.455	-1.630	98.699

6.4 Conclusion

In conclusion, our study reveals that modern SRAM memories remain highly susceptible to data imprinting during irradiation, even at low to moderate doses. Our findings indicate that SRAM samples manufactured using smaller technology nodes exhibit greater resilience to imprinting. Additionally, we have established that data imprinting is a transient phenomenon that can be reversed through annealing. This insight is crucial for developing strategies to mitigate potential security threats posed by ionizing radiation-based data imprinting attacks.

Chapter 7. Impact of Ionizing Radiation on SRAM Data Remanence

7.1 Introduction

Continuous technological scaling of static random-access memory (SRAM) has produced chips that are smaller, faster, and more energy efficient. SRAM is a volatile memory, and its data remanence refers to the persistence of data after the chip is powered down. As SRAM memory is prevalent in CPU cache and embedded systems, it frequently stores critical information such as cryptographic keys, passwords, and other confidential data. Consequently, a data remanence-based attack on SRAM can result in significant damage. Previous studies [93], [104], [105] suggest that data does not disappear immediately upon power-off but persists for a duration ranging from microseconds to seconds, depending on the SRAM sample. Therefore, a fundamental understanding of the data remanence of commercial SRAM memory is crucial for the security assessment of SRAM-based computing systems.

7.2 Experimental Procedure

We performed experiments on Cypress 250, 150, and 90 nm SRAM samples. To study the data remanence effect, we first generate a reference power-up state for each chip (PU_{ref}), by analyzing data from 101 consecutive power-up cycles. Since PU_{ref} is the natural power-up state of the SRAM, it will serve as our reference to know when all user data are lost. We then write a black-and-white (binary) image of Albert Einstein ($Image_{original}$) similar to 6.2. Note that the image is written multiple times throughout the chip for statistical significance. The SRAM is then

powered off. We then wait for a certain period of time (t_d) before turning it back on and reading the contents of the SRAM module to observe how much of the written data are lost. The percentage of data lost is then calculated using the following equation:

$$Data\ Loss\ \% = \frac{\#\ of\ set\ bits\ (Image_{original}\ XOR\ PU_{read})}{\#\ of\ set\ bits\ (Image_{oroginal}\ XOR\ \ PU_{ref)}} \times 100\%. \qquad (7.1)$$

We repeat the above procedure multiple times by incrementing t_d to study how long it takes for all data to be lost. The experimental flow is illustrated in **Figure 7.1**. All experiments are performed at room temperature. The irradiation experiments are performed at the Ohio State University's Nuclear Reactor Laboratory, in the underwater gamma irradiator using a Co-60 source with a dose rate of 11.7 krad(Si)/h. Gamma irradiation was performed on the packaged TSOP (thin small outline package) devices with SRAM chips powered off and pins grounded. Several COTS SRAM chips from Cypress (250 nm, 150 nm, 90 nm) are used. The details are the chips are mentioned in the previous sections.

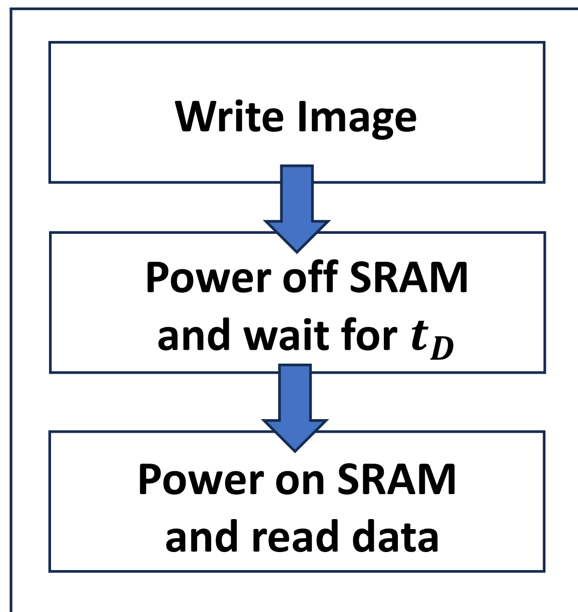


Figure 7.1 The procedure for the data remanence experiment. The flow is repeated with increasing $t_D$until all data are lost.

7.2.1 Baseline Characterization of Data Remanence

Figure 7.2(a) shows the Data Loss% for increasing t_d for the 150 nm sample. The corresponding states of the recovered images are also shown in the figure. Interestingly, there is no data loss for the first several milliseconds and then we observe a gradual data loss over the next 20 milliseconds until all data are lost. The trend of data loss is observed to be consistent over several runs for the sample. **Figure 7.2**(b) shows the consistency of the experimental procedure. **Figure 7.2**(c) shows the compilation of the remanence data for all three samples where the 250 nm sample is in the thousands of milliseconds range, the 150 nm sample is in the tens of milliseconds range, and the 90 nm sample is in the hundreds of microseconds range, indicating an exponential decrease in remanence time with decreasing transistor size.

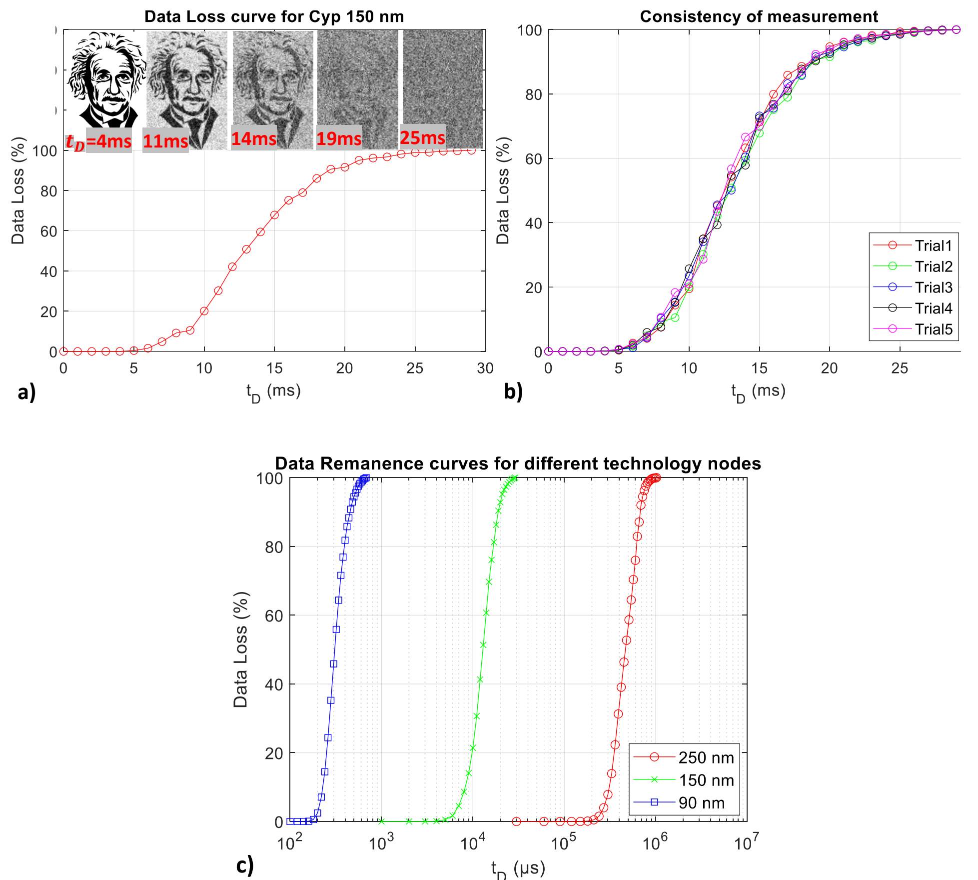


Figure 7.2 (a) The progression of data loss on the Cypress 150 nm sample. (b) Consistency of measurement procedure (c) The compilation of data remanence results for the 90, 150, and 250 nm samples.

7.2.2 Post-Irradiation Data Remanence

The samples are irradiated to 100 krad(Si) and they are characterized to study their data remanence post irradiation. **Figure 7.3** shows the compilation of results for the 250, 150, and 90 nm Cypress samples. All three samples show a similar trend of significantly faster data loss post-irradiation.

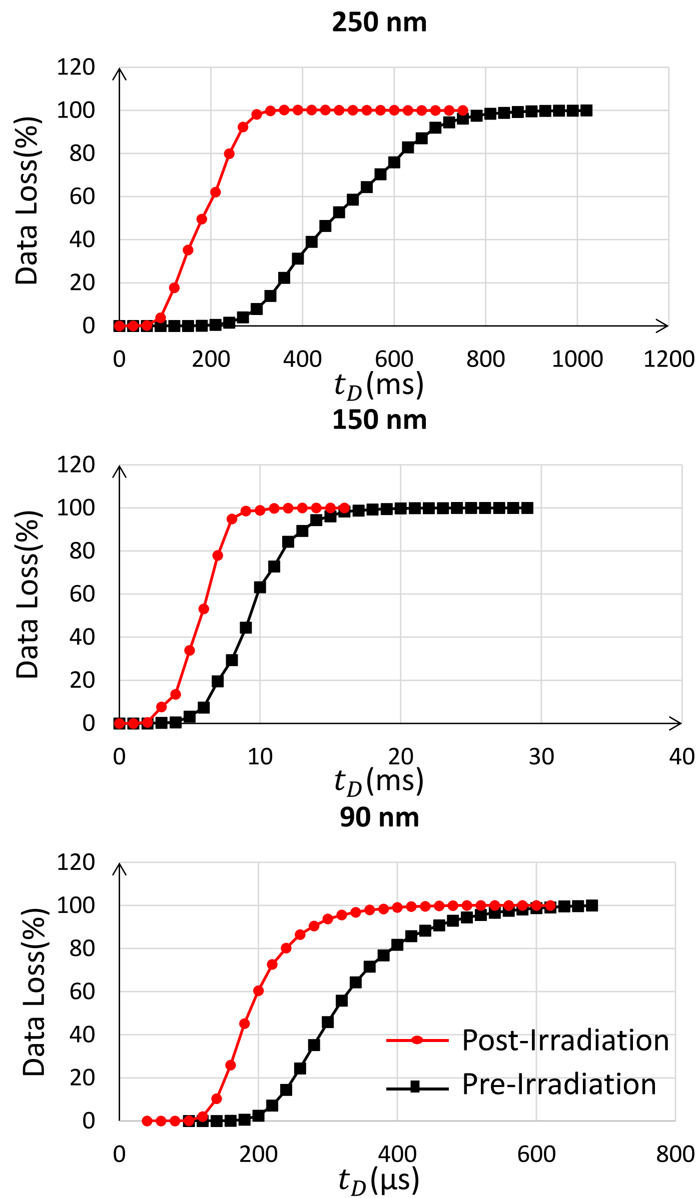


Figure 7.3 The compilation of data remanence results for the 90, 150, and 250 nm samples post irradiation.

7.2.3 Predictive Remanence Time Model

We hypothesize that the data remanence effect is due to node capacitance slowly discharging through the transistors in the form of subthreshold leakage current as illustrated with red dashed lines in **Figure 7.4**(a). The predictive model for data remanence time $\boldsymbol{t_{rem}}$ is derived in **Figure 7.4**(b). As the discharge is in the form of transistor leakage current, $\boldsymbol{I_{leak}}$, it can be written as the change in charge over time. The charge on node Q is an effect of several capacitive elements but primarily from the gate capacitance C of the P1 which was previously on while holding "1" data. Since we know the transistor leakage current equation, we may write the time taken for charge loss as seen from the equations. The primary contributors to remanence time $\boldsymbol{t_{rem}}$ then become: the gate area $\boldsymbol{A}$, oxide thickness $\boldsymbol{T_{ox}}$, threshold voltage $\boldsymbol{V_{th}}$, and subthreshold slope $\boldsymbol{\eta}$. The first revelation is then, $\boldsymbol{t_{rem}}$ decreases exponentially as the technology node size decreases [106] ($\boldsymbol{t_{rem}}$ 90 nm < $\boldsymbol{t_{rem}}$ 150 nm < $\boldsymbol{t_{rem}}$ 250 nm) which agrees with the findings in **Figure 7.2**.

The next revelation is then that post-irradiation remanence time $\boldsymbol{t'_{rem}}$ will reduce since the $\boldsymbol{V_{th}}$ of the NMOSs reduce ($\boldsymbol{V_{th}}'$) as an effect of ionizing radiation. Of course, there is the caveat that the threshold voltage of the PMOS transistor increases due to ionizing radiation but recall that transistor sizing constraints for SRAM dictate that the pull-down NMOSs should be stronger than the access transistors, and the pull-up PMOSs should be weaker than the access transistors (2.2.3), meaning that the $\boldsymbol{V_{th}}$ changes (and hence $\boldsymbol{I_{leak}}$) of the NMOS access transistors and the NMOS pull-down transistors will dominate causing an overall decrease in data remanence time post-irradiation, as observed in **Figure 7.3**.

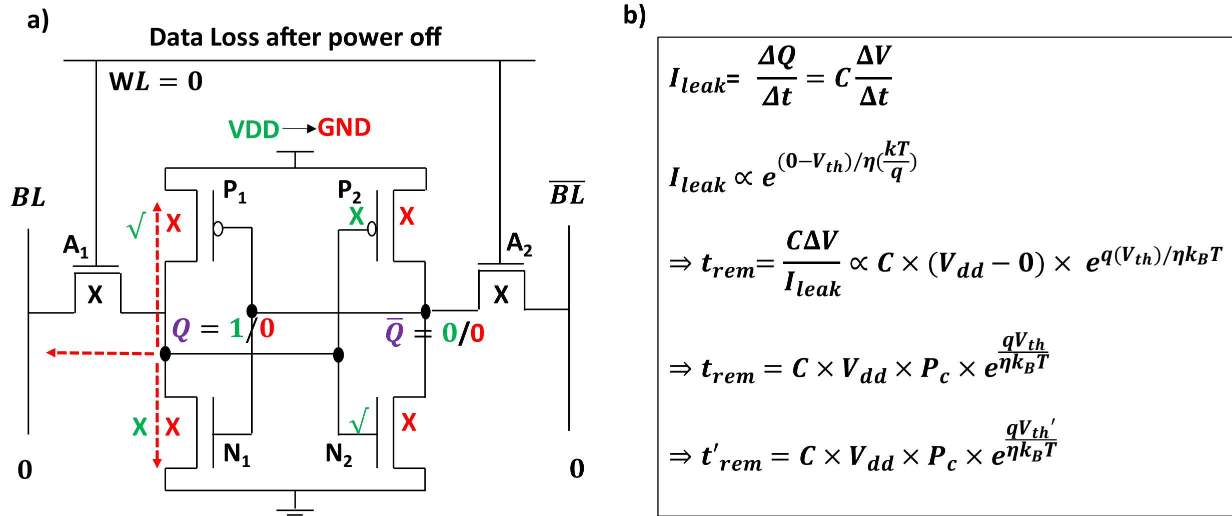


Figure 7.4 (a) Node capacitance discharge model in SRAM cell (green indicating cell on condition and red indicating cell off condition), (b) Derivation of remanence time t_{rem} and post irradiation t'_{rem} .

7.3 Conclusion

We learn that ionizing radiation can be used as a mitigation strategy against data remanence-style security attacks that take advantage of data remanence to steal valuable information. Standard SRAM circuit operation is seen to be extremely robust to ionizing radiation, meaning a moderate dose will not affect SRAM operation but will significantly improve its volatility to defend against data remanence attacks. We also find that as the device feature size decreases, the data remanence decreases rapidly.

Chapter 8. Conclusion and Future Work

8.1 Summary of Key Findings and Contributions

The primary contributions of this dissertation are as follows:

1) We explore the TID effects on modern MLC 3D NAND and find that the MSB pages are more susceptible to radiation-induced charge loss than LSB pages. We present a physical model to understand the underlying mechanism. MSB pages are 20-50% more susceptible. We also find a layer dependence on the error ratio between MSB/ LSB pages. We find that errors are correlated, meaning, if the LSB page is in error, then the corresponding MSB page is also in error. We find that bit error locations in a byte are independent and uncorrelated, meaning there is no clustering of error bits, which is vital knowledge when it comes to designing ECC.
2) We find that read noise is a big contributing factor to post-irradiation errors. We find read noise to be a strong function of TID. We find that one of the key contributing factors to the increase in read noise is the program state of the cells under irradiation. We present a mitigation strategy, where memory modules are pre-primed data as opposed to being used in a factory-erased state, before deploying them in a radiation-prone environment.
   We find that the total noise reduces as the samples anneal at room temperature, but they do not quite return to pre-irradiation conditions even after several months.
3) We find that TID significantly impacts the PUF security aspect of SRAM memories. The degree of impact is a strong function of the dose. PUF HD increases significantly with

dose, and so does the number of unstable bits. Radiation may cause false negatives during PUF authentication events. We propose a mitigation strategy to protect SRAM PUF under ionizing radiation. For PUF degradation, we find a strong dependence on the data pattern stored during irradiation. Depending on the manufacturer, storing either PUF data or inverted PUF data helps preserve the PUF under ionizing radiation. We also find that there is a strong dependence on technology node when it comes to SRAM PUF degradation under ionizing radiation.

4) We find that Ionizing radiation may be used to intentionally alter the natural PUF state of an SRAM array posing a significant security threat.
5) We also find that ionizing radiation may be used as a mitigation strategy against SRAM data remanence-style security attacks as it significantly reduces the data remanence time.

In conclusion, the studies conducted on the radiation effects on semiconductor memories shed more light on the dangers faced by modern microelectronics in a radiation-prone environment. The knowledge of error patterns in modern 3D flash memories helps in making better controllers and designing more efficient error correction codes. Preprogramming of factory-erased blocks helps substantially mitigate the effects of radiation-induced transistor noise that causes errors. The knowledge of data pattern dependence helps protect SRAM PUF from ionizing radiation. The knowledge of superior radiation resilience of smaller transistors helps better parts selection when it comes to designing radiation-ready hardware. The knowledge of intentional data imprinting using radiation will help protect against attack vectors of its nature. Since a moderate TID does not affect SRAM operation, we may use it as a preventative measure for data remanence style attacks.

8.2 Future Research Avenues

While we covered a lot of ground in the field of TID effects on semiconductor memories, there remain a few unexplored venues:

1) Isolating the effects of ionizing radiation on peripheral devices: While we observed the effects of radiation on the memory arrays, it would help to have a deeper understanding of peripheral circuits that play a supportive role in memory architecture. For instance, we have found that the voltage pump on NAND flash memories fails with dose, and the erase operation begins to slow down and eventually fail completely. Poorly erased portions will often lead to a failed write operation as well.
2) Extending the noise study to the state-of-the-art QLC and PLC memories that store 4 and 5 bits of information per cell respectively. Since the basic phenomenon will remain the same, we may expect to see even better results with our strategies such as the pre-programming of blocks, which we intend to call "electrostatic shielding".
3) Extending the data imprinting study using X-rays, since X-rays are more easily accessible and may prove to have a stronger impact due to a phenomenon known as "dose enhancement".

References

[1] W. C. Roberts, “Facts and ideas from anywhere,” *Proc. Bayl. Univ. Med. Cent.*, vol. 33, no. 2, pp. 310–316, Feb. 2020, doi: 10.1080/08998280.2020.1725731.

[2] “Cosmic rays: particles from outer space,” CERN. Accessed: Mar. 09, 2024. [Online]. Available: https://home.cern/science/physics/cosmic-rays-particles-outer-space

[3] “11.6: Penetrating Power of Radiation,” Chemistry LibreTexts. Accessed: Feb. 26, 2024. [Online]. Available: https://chem.libretexts.org/Bookshelves/Introductory_Chemistry/Chemistry_for_Changing_Times_(Hill_and_McCreary)/11%3A_Nuclear_Chemistry/11.06%3A_Penetrating_Power_of_Radiation

[4] P. E. Dodd and F. W. Sexton, “Critical charge concepts for CMOS SRAMs,” *IEEE Trans. Nucl. Sci.*, vol. 42, no. 6, pp. 1764–1771, Dec. 1995, doi: 10.1109/23.488777.

[5] “Single Event Effects in Aerospace | IEEE eBooks | IEEE Xplore.” Accessed: Oct. 15, 2023. [Online]. Available: https://ieeexplore.ieee.org/book/6047596

[6] J. R. Schwank *et al.*, “Radiation Effects in MOS Oxides,” *IEEE Trans. Nucl. Sci.*, vol. 55, no. 4, Art. no. 4, Aug. 2008, doi: 10.1109/TNS.2008.2001040.

[7] E. N. Shauly, “CMOS Leakage and Power Reduction in Transistors and Circuits: Process and Layout Considerations,” *J. Low Power Electron. Appl.*, vol. 2, no. 1, Art. no. 1, Mar. 2012, doi: 10.3390/jlpea2010001.

[8] T. Coughlin, “Flash Memory Areal Densities Exceed Those of Hard Drives,” Forbes. Accessed: Feb. 27, 2024. [Online]. Available: https://www.forbes.com/sites/tomcoughlin/2016/02/03/flash-memory-areal-densities-exceed-those-of-hard-drives/

[9] S. L. Clark, K. Avery, and R. Parker, “TID and SEE testing results of Altera Cyclone field programmable gate array,” in *2004 IEEE Radiation Effects Data Workshop (IEEE Cat. No.04TH8774)*, Jul. 2004, pp. 88–90. doi: 10.1109/REDW.2004.1352911.

[10] F. Irom, D. N. Nguyen, R. Harboe-Sorensen, and A. Virtanen, “Evaluation of Mechanisms in TID Degradation and SEE Susceptibility of Single- and Multi-Level High Density NAND Flash Memories,” *IEEE Trans. Nucl. Sci.*, vol. 58, no. 5, Art. no. 5, Oct. 2011, doi: 10.1109/TNS.2011.2161885.

[11] T. R. Oldham *et al.*, “TID and SEE Response of an Advanced Samsung 4Gb NAND Flash Memory,” in *2007 IEEE Radiation Effects Data Workshop*, Jul. 2007, pp. 221–225. doi: 10.1109/REDW.2007.4342570.

[12] Y. Cai, E. F. Haratsch, O. Mutlu, and K. Mai, “Error patterns in MLC NAND flash memory: Measurement, characterization, and analysis,” in *2012 Design, Automation Test in Europe Conference Exhibition (DATE)*, Mar. 2012, pp. 521–526. doi: 10.1109/DATE.2012.6176524.

[13] G. Cellere, A. Paccagnella, A. Visconti, M. Bonanomi, A. Candelori, and S. Lora, “Effect of different total ionizing dose sources on charge loss from programmed floating gate

cells," *IEEE Trans. Nucl. Sci.*, vol. 52, no. 6, pp. 2372–2377, Dec. 2005, doi: 10.1109/TNS.2005.860681.

[14] M. Bagatin *et al.*, "Total Ionizing Dose Effects in 3D NAND Flash Memories," *IEEE Trans. Nucl. Sci.*, pp. 1–1, 2018, doi: 10.1109/TNS.2018.2878911.

[15] P. Kumari, S. Huang, M. Wasiolek, K. Hattar, and B. Ray, "Layer Dependent Bit Error Variation in 3-D NAND Flash Under Ionizing Radiation," *IEEE Trans. Nucl. Sci.*, pp. 1–1, 2020, doi: 10.1109/TNS.2020.3014261.

[16] S. Gerardin and A. Paccagnella, "Present and Future Non-Volatile Memories for Space," *IEEE Trans. Nucl. Sci.*, vol. 57, no. 6, pp. 3016–3039, Dec. 2010, doi: 10.1109/TNS.2010.2084101.

[17] D. Chen *et al.*, "Heavy Ion and Proton-Induced Single Event Upset Characteristics of a 3-D NAND Flash Memory," *IEEE Trans. Nucl. Sci.*, vol. 65, no. 1, pp. 19–26, Jan. 2018, doi: 10.1109/TNS.2017.2764852.

[18] M. Bagatin *et al.*, "Effects of Heavy-Ion Irradiation on Vertical 3-D NAND Flash Memories," *IEEE Trans. Nucl. Sci.*, vol. 65, no. 1, pp. 318–325, Jan. 2018, doi: 10.1109/TNS.2017.2777887.

[19] M. J. Gadlage, D. I. Bruce, J. D. Ingalls, D. P. Bossev, M. McKinney, and M. J. S. Kay, "Directional Dependence of Co-60 Irradiation on the Total Dose Response of Flash Memories," *IEEE Trans. Nucl. Sci.*, vol. 66, pp. 148–154, 2019.

[20] M. J. Gadlage, M. J. Kay, J. D. Ingalls, A. R. Duncan, and S. A. Ashley, "Impact of X-Ray Exposure on a Triple-Level-Cell NAND Flash," *IEEE Trans. Nucl. Sci.*, vol. 60, no. 6, pp. 4533–4539, Dec. 2013, doi: 10.1109/TNS.2013.2280432.

[21] C. Monzio Compagnoni, A. Goda, A. S. Spinelli, P. Feeley, A. L. Lacaita, and A. Visconti, "Reviewing the Evolution of the NAND Flash Technology," *Proc. IEEE*, vol. 105, no. 9, pp. 1609–1633, Sep. 2017, doi: 10.1109/JPROC.2017.2665781.

[22] F. Irom, D. N. Nguyen, R. Harboe-Sorensen, and A. Virtanen, "Evaluation of Mechanisms in TID Degradation and SEE Susceptibility of Single- and Multi-Level High Density NAND Flash Memories," *IEEE Trans. Nucl. Sci.*, vol. 58, no. 5, pp. 2477–2482, Oct. 2011, doi: 10.1109/TNS.2011.2161885.

[23] J. D. Ingalls, M. J. Gadlage, A. R. Duncan, M. J. Kay, P. L. Cole, and K. K. Hunt, "Implications of the Logical Decode on the Radiation Response of a Multi-Level Cell NAND Flash Memory," *IEEE Trans. Nucl. Sci.*, vol. 60, no. 6, pp. 4451–4456, Dec. 2013, doi: 10.1109/TNS.2013.2282699.

[24] M. J. Gadlage, M. J. Kay, J. D. Ingalls, A. R. Duncan, and S. A. Ashley, "Impact of X-Ray Exposure on a Triple-Level-Cell NAND Flash," *IEEE Trans. Nucl. Sci.*, vol. 60, no. 6, pp. 4533–4539, Dec. 2013, doi: 10.1109/TNS.2013.2280432.

[25] S. Gerardin *et al.*, "Radiation Effects in Flash Memories," *IEEE Trans. Nucl. Sci.*, vol. 60, no. 3, pp. 1953–1969, Jun. 2013, doi: 10.1109/TNS.2013.2254497.

[26] F. Irom, D. N. Nguyen, and G. R. Allen, "Single Event Effect and Total Ionizing Dose Results of Highly Scaled Flash Memories," in *2013 IEEE Radiation Effects Data Workshop (REDW)*, Jul. 2013, pp. 1–4. doi: 10.1109/REDW.2013.6658209.

[27] S. Gerardin, M. Bagatin, A. Paccagnella, and V. Ferlet-Cavrois, "Degradation of Sub 40-nm NAND Flash Memories Under Total Dose Irradiation," *IEEE Trans. Nucl. Sci.*, vol. 59, no. 6, pp. 2952–2958, Dec. 2012, doi: 10.1109/TNS.2012.2222928.

[28] "FT2232H." Accessed: Jul. 08, 2020. [Online]. Available: https://www.ftdichip.com/Products/ICs/FT2232H.html

[29] "3D NAND." Accessed: Jul. 08, 2020. [Online]. Available: https://www.micron.com/products/nand-flash/3d-nand
[30] "Sandia National Laboratory." Accessed: Feb. 23, 2020. [Online]. Available: https://www.sandia.gov/
[31] B. Ray and A. Milenković, "True Random Number Generation Using Read Noise of Flash Memory Cells," *IEEE Trans. Electron Devices*, vol. 65, no. 3, pp. 963–969, Mar. 2018, doi: 10.1109/TED.2018.2792436.
[32] E. S. Snyder, P. J. McWhorter, T. A. Dellin, and J. D. Sweetman, "Radiation response of floating gate EEPROM memory cells," *IEEE Trans. Nucl. Sci.*, vol. 36, no. 6, pp. 2131–2139, Dec. 1989, doi: 10.1109/23.45415.
[33] J. R. Schwank *et al.*, "Radiation Effects in MOS Oxides," *IEEE Trans. Nucl. Sci.*, vol. 55, no. 4, pp. 1833–1853, Aug. 2008, doi: 10.1109/TNS.2008.2001040.
[34] F. Chen, T. Zhang, and X. Zhang, "Software Support Inside and Outside Solid-State Devices for High Performance and High Efficiency," *Proc. IEEE*, vol. 105, no. 9, pp. 1650–1665, Sep. 2017, doi: 10.1109/JPROC.2017.2679490.
[35] F. Irom, D. N. Nguyen, M. L. Underwood, and A. Virtanen, "Effects of Scaling in SEE and TID Response of High Density NAND Flash Memories," *IEEE Trans. Nucl. Sci.*, vol. 57, no. 6, pp. 3329–3335, Dec. 2010, doi: 10.1109/TNS.2010.2084102.
[36] M. Bagatin *et al.*, "Total Ionizing Dose Effects in 3-D NAND Flash Memories," *IEEE Trans. Nucl. Sci.*, vol. 66, no. 1, pp. 48–53, Jan. 2019, doi: 10.1109/TNS.2018.2878911.
[37] D. M. Fleetwood, "Total-Ionizing-Dose Effects, Border Traps, and 1/f Noise in Emerging MOS Technologies," *IEEE Trans. Nucl. Sci.*, vol. 67, no. 7, pp. 1216–1240, Jul. 2020, doi: 10.1109/TNS.2020.2971861.
[38] C. M. Compagnoni, M. Ghidotti, A. L. Lacaita, A. S. Spinelli, and A. Visconti, "Random Telegraph Noise Effect on the Programmed Threshold-Voltage Distribution of Flash Memories," *IEEE Electron Device Lett.*, vol. 30, no. 9, pp. 984–986, Sep. 2009, doi: 10.1109/LED.2009.2026658.
[39] A. Goda, C. Miccoli, and C. M. Compagnoni, "Time dependent threshold-voltage fluctuations in NAND flash memories: From basic physics to impact on array operation," in *2015 IEEE International Electron Devices Meeting (IEDM)*, Dec. 2015, p. 14.7.1-14.7.4. doi: 10.1109/IEDM.2015.7409699.
[40] G. Nicosia *et al.*, "Impact of temperature on the amplitude of RTN fluctuations in 3-D NAND flash cells," in *2017 IEEE International Electron Devices Meeting (IEDM)*, Dec. 2017, p. 21.3.1-21.3.4. doi: 10.1109/IEDM.2017.8268434.
[41] M. Bagatin *et al.*, "Error Instability in Floating Gate Flash Memories Exposed to TID," *IEEE Trans. Nucl. Sci.*, vol. 56, no. 6, pp. 3267–3273, Dec. 2009, doi: 10.1109/TNS.2009.2033364.
[42] S. K. Dixit *et al.*, "Radiation Induced Charge Trapping in Ultrathin $\rm HfO_2$-Based MOSFETs," *IEEE Trans. Nucl. Sci.*, vol. 54, no. 6, pp. 1883–1890, Dec. 2007, doi: 10.1109/TNS.2007.911423.
[43] P. Wang *et al.*, "Radiation-Induced Charge Trapping and Low-Frequency Noise of Graphene Transistors," *IEEE Trans. Nucl. Sci.*, vol. 65, no. 1, pp. 156–163, Jan. 2018, doi: 10.1109/TNS.2017.2761747.
[44] C. D. Liang *et al.*, "Defects and Low-Frequency Noise in Irradiated Black Phosphorus MOSFETs With HfO2 Gate Dielectrics," *IEEE Trans. Nucl. Sci.*, vol. 65, no. 6, pp. 1227–1238, Jun. 2018, doi: 10.1109/TNS.2018.2828080.

[45] D. M. Fleetwood *et al.*, “Unified model of hole trapping, 1/f noise, and thermally stimulated current in MOS devices,” *IEEE Trans. Nucl. Sci.*, vol. 49, no. 6, pp. 2674–2683, Dec. 2002, doi: 10.1109/TNS.2002.805407.

[46] C. D. Liang *et al.*, “Defects and Low-Frequency Noise in Irradiated Black Phosphorus MOSFETs With HfO2 Gate Dielectrics,” *IEEE Trans. Nucl. Sci.*, vol. 65, no. 6, pp. 1227–1238, Jun. 2018, doi: 10.1109/TNS.2018.2828080.

[47] D. M. Fleetwood, M. R. Shaneyfelt, and J. R. Schwank, “Estimating oxide-trap, interface-trap, and border-trap charge densities in metal-oxide-semiconductor transistors,” *Appl. Phys. Lett.*, vol. 64, no. 15, pp. 1965–1967, Apr. 1994, doi: 10.1063/1.111757.

[48] U. Surendranathan, P. Kumari, M. Wasiolek, K. Hattar, T. Boykin, and B. Ray, “Gamma-Ray-Induced Error Pattern Analysis for MLC 3-D NAND Flash Memories,” *IEEE Trans. Nucl. Sci.*, vol. 68, no. 5, pp. 733–739, May 2021, doi: 10.1109/TNS.2021.3059186.

[49] D. M. Fleetwood, T. L. Meisenheimer, and J. H. Scofield, “1/f noise and radiation effects in MOS devices,” *IEEE Trans. Electron Devices*, vol. 41, no. 11, pp. 1953–1964, Nov. 1994, doi: 10.1109/16.333811.

[50] D. M. Fleetwood, “$1/f$ Noise and Defects in Microelectronic Materials and Devices,” *IEEE Trans. Nucl. Sci.*, vol. 62, no. 4, pp. 1462–1486, Aug. 2015, doi: 10.1109/TNS.2015.2405852.

[51] P. Kumari, U. Surendranathan, M. Wasiolek, K. Hattar, N. P. Bhat, and B. Ray, “Radiation-Induced Error Mitigation by Read-Retry Technique for MLC 3-D NAND Flash Memory,” *IEEE Trans. Nucl. Sci.*, vol. 68, no. 5, pp. 1032–1039, May 2021, doi: 10.1109/TNS.2021.3052909.

[52] P. Kumari, S. Huang, M. Wasiolek, K. Hattar, and B. Ray, “Layer-Dependent Bit Error Variation in 3-D NAND Flash Under Ionizing Radiation,” *IEEE Trans. Nucl. Sci.*, vol. 67, no. 9, pp. 2021–2027, Sep. 2020, doi: 10.1109/TNS.2020.3014261.

[53] M. J. Gadlage, D. I. Bruce, J. D. Ingalls, D. P. Bossev, M. Mckinney, and M. J. Kay, “Directional Dependence of Co-60 Irradiation on the Total Dose Response of Flash Memories,” *IEEE Trans. Nucl. Sci.*, vol. 66, no. 1, pp. 148–154, Jan. 2019, doi: 10.1109/TNS.2018.2879685.

[54] A. Dasgupta, D. M. Fleetwood, R. A. Reed, R. A. Weller, and M. H. Mendenhall, “Effects of Metal Gates and Back-End-of-Line Materials on X-Ray Dose in $\rm HfO_2$ Gate Oxide,” *IEEE Trans. Nucl. Sci.*, vol. 58, no. 6, pp. 3139–3144, Dec. 2011, doi: 10.1109/TNS.2011.2169279.

[55] P. J. McWhorter, S. L. Miller, and T. A. Dellin, “Radiation Response of SNOS Nonvolatile Transistors,” *IEEE Trans. Nucl. Sci.*, vol. 33, no. 6, pp. 1413–1419, Dec. 1986, doi: 10.1109/TNS.1986.4334615.

[56] P. J. McWhorter, S. L. Miller, and W. M. Miller, “Modeling the anneal of radiation-induced trapped holes in a varying thermal environment,” *IEEE Trans. Nucl. Sci.*, vol. 37, no. 6, pp. 1682–1689, Dec. 1990, doi: 10.1109/23.101177.

[57] D. M. Fleetwood, “Total Ionizing Dose Effects in MOS and Low-Dose-Rate-Sensitive Linear-Bipolar Devices,” *IEEE Trans. Nucl. Sci.*, vol. 60, no. 3, pp. 1706–1730, Jun. 2013, doi: 10.1109/TNS.2013.2259260.

[58] B. R. Tuttle, D. R. Hughart, R. D. Schrimpf, D. M. Fleetwood, and S. T. Pantelides, “Defect Interactions of $\hbox{H}_2$ in $\hbox{SiO}_2$: Implications for ELDRS and Latent Interface Trap Buildup,” *IEEE Trans. Nucl. Sci.*, vol. 57, no. 6, pp. 3046–3053, Dec. 2010, doi: 10.1109/TNS.2010.2086076.

[59] J. Ding, E. X. Zhang, K. Li, X. Luo, M. Gorchichko, and D. M. Fleetwood, "Aging Effects and Latent Interface-Trap Buildup in MOS Transistors," *IEEE Trans. Nucl. Sci.*, pp. 1–1, 2021, doi: 10.1109/TNS.2021.3128835.
[60] D. E. Holcomb, W. P. Burleson, and K. Fu, "Power-Up SRAM State as an Identifying Fingerprint and Source of True Random Numbers," *IEEE Trans. Comput.*, vol. 58, no. 9, pp. 1198–1210, Sep. 2009, doi: 10.1109/TC.2008.212.
[61] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "FPGA Intrinsic PUFs and Their Use for IP Protection," in *Cryptographic Hardware and Embedded Systems - CHES 2007*, P. Paillier and I. Verbauwhede, Eds., in Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2007, pp. 63–80. doi: 10.1007/978-3-540-74735-2_5.
[62] R. Wang, G. Selimis, R. Maes, and S. Goossens, "Long-term Continuous Assessment of SRAM PUF and Source of Random Numbers," in *2020 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Mar. 2020, pp. 7–12. doi: 10.23919/DATE48585.2020.9116353.
[63] Y. Gao, Y. Su, W. Yang, S. Chen, S. Nepal, and D. C. Ranasinghe, "Building Secure SRAM PUF Key Generators on Resource Constrained Devices," in *2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, Mar. 2019, pp. 912–917. doi: 10.1109/PERCOMW.2019.8730781.
[64] F. Gondesen, S. Mitra, and K.-Y. Lam, "Feasibility of PUF-Based Authentication on ATtiny Devices with Off-the-Shelf SRAM," in *Proceedings of the 6th ACM on Cyber-Physical System Security Workshop*, in CPSS '20. New York, NY, USA: Association for Computing Machinery, Oct. 2020, pp. 2–10. doi: 10.1145/3384941.3409591.
[65] R. Maes, *Physically Unclonable Functions: Constructions, Properties and Applications*. Springer Science & Business Media, 2013.
[66] "Secure Storage with SRAM PUF on NXP LPC54S0xx (Rev 1.0)," vol. 2018, p. 17, 2018.
[67] Nathalie, "Embedded Microcontrollers," Intrinsic ID | Home of PUF Technology. Accessed: Jul. 07, 2022. [Online]. Available: https://www.intrinsic-id.com/markets/embedded-microcontrollers/
[68] R. Maes, "Physically Unclonable Functions: Constructions, Properties and Applications (Fysisch onkloonbare functies: constructies, eigenschappen en toepassingen)," Aug. 2012, Accessed: Mar. 21, 2021. [Online]. Available: https://lirias.kuleuven.be/1662210
[69] S. Sakib, Md. Raquibuzzaman, M. Wasiolek, K. Hattar, and B. Ray, "Total Ionizing Dose Effects on Physical Unclonable Function From NAND Flash Memory," *IEEE Trans. Nucl. Sci.*, vol. 68, no. 7, pp. 1445–1453, Jul. 2021, doi: 10.1109/TNS.2021.3087106.
[70] H. Martin, P. Martin-Holgado, Y. Morilla, L. Entrena, and E. San-Millan, "Total Ionizing Dose Effects on a Delay-Based Physical Unclonable Function Implemented in FPGAs," *Electronics*, vol. 7, no. 9, Art. no. 9, Sep. 2018, doi: 10.3390/electronics7090163.
[71] P. F. Wang *et al.*, "X-Ray and Proton Radiation Effects on 40 nm CMOS Physically Unclonable Function Devices," *IEEE Trans. Nucl. Sci.*, vol. 65, no. 8, pp. 1519–1524, Aug. 2018, doi: 10.1109/TNS.2017.2789160.
[72] S. P. Lawrence, S. C. Smith, J. M. Cannon, J. L. Carpenter, D. R. Reising, and T. D. Loveless, "Effects of Total Ionizing Dose on SRAM Physical Unclonable Functions," *IEEE Trans. Nucl. Sci.*, vol. 69, no. 3, pp. 349–358, Mar. 2022, doi: 10.1109/TNS.2022.3146279.
[73] X. Zhang, C. Jiang, K. Gu, L. Zhong, W. Fang, and G. Dai, "A Novel SRAM PUF Stability Improvement Method Using Ionization Irradiation," *Electronics*, vol. 9, no. 9, Art. no. 9, Sep. 2020, doi: 10.3390/electronics9091498.

[74] Z. Su *et al.*, “Reliability Improvement on SRAM Physical Unclonable Function (PUF) Using an 8T Cell in 28 nm FDSOI,” *IEEE Trans. Nucl. Sci.*, vol. 69, no. 3, pp. 333–339, Mar. 2022, doi: 10.1109/TNS.2021.3126587.

[75] W. Calienes, R. Reis, C. Anghel, and A. Vladimirescu, “Bulk and FDSOI SRAM resiliency to radiation effects,” in *2014 IEEE 57th International Midwest Symposium on Circuits and Systems (MWSCAS)*, College Station, TX, USA: IEEE, Aug. 2014, pp. 655–658. doi: 10.1109/MWSCAS.2014.6908500.

[76] Z. Su *et al.*, “Reliability Improvement on SRAM Physical Unclonable Function (PUF) Using an 8T Cell in 28 nm FDSOI,” *IEEE Trans. Nucl. Sci.*, vol. 69, no. 3, pp. 333–339, Mar. 2022, doi: 10.1109/TNS.2021.3126587.

[77] D. Kobayashi *et al.*, “Data-Retention-Voltage-Based Analysis of Systematic Variations in SRAM SEU Hardness: A Possible Solution to Synergistic Effects of TID,” *IEEE Trans. Nucl. Sci.*, vol. 67, no. 1, pp. 328–335, Jan. 2020, doi: 10.1109/TNS.2019.2956760.

[78] J. M. Cannon *et al.*, “Electrical Measurement of Cell-to-Cell Variation of Critical Charge in SRAM and Sensitivity to Single-Event Upsets by Low-Energy Protons,” *IEEE Trans. Nucl. Sci.*, vol. 68, no. 5, pp. 815–822, May 2021, doi: 10.1109/TNS.2021.3061672.

[79] T. Fischer *et al.*, “A 1 Mbit SRAM test structure to analyze local mismatch beyond 5 sigma variation,” in *2007 IEEE International Conference on Microelectronic Test Structures*, Mar. 2007, pp. 63–66. doi: 10.1109/ICMTS.2007.374456.

[80] J. Wang, A. Singhee, R. A. Rutenbar, and B. H. Calhoun, “Two Fast Methods for Estimating the Minimum Standby Supply Voltage for Large SRAMs,” *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, vol. 29, no. 12, pp. 1908–1920, Dec. 2010, doi: 10.1109/TCAD.2010.2061810.

[81] M. Bhargava and K. Mai, “A High Reliability PUF Using Hot Carrier Injection Based Response Reinforcement,” in *Cryptographic Hardware and Embedded Systems - CHES 2013*, G. Bertoni and J.-S. Coron, Eds., in Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2013, pp. 90–106. doi: 10.1007/978-3-642-40349-1_6.

[82] M. P. Petkov, “The effects of space environments on electronic components,” 2003, Accessed: Oct. 17, 2022. [Online]. Available: https://trs.jpl.nasa.gov/handle/2014/7193

[83] T. L. Meisenheimer, D. M. Fleetwood, M. R. Shaneyfelt, and L. C. Riewe, “1/f noise in n- and p-channel MOS devices through irradiation and annealing,” *IEEE Trans. Nucl. Sci.*, vol. 38, no. 6, pp. 1297–1303, 1991.

[84] P. J. McWhorter, S. L. Miller, and W. M. Miller, “Modeling the anneal of radiation-induced trapped holes in a varying thermal environment,” *IEEE Trans. Nucl. Sci.*, vol. 37, no. 6, pp. 1682–1689, Dec. 1990, doi: 10.1109/23.101177.

[85] B. R. Tuttle, D. R. Hughart, R. D. Schrimpf, D. M. Fleetwood, and S. T. Pantelides, “Defect Interactions of ${\hbox{H}}_{2}$ in ${\hbox{SiO}}_{2}$: Implications for ELDRS and Latent Interface Trap Buildup,” *IEEE Trans. Nucl. Sci.*, p. 5658003, Dec. 2010, doi: 10.1109/TNS.2010.2086076.

[86] D. M. Fleetwood and P. V. Dressendorfer, “A Simple Method to Identify Radiation and Annealing Biases That Lead to Worst-Case CMOS Static Ram Postirradiation Response,” *IEEE Trans. Nucl. Sci.*, vol. 34, no. 6, pp. 1408–1413, Dec. 1987, doi: 10.1109/TNS.1987.4337489.

[87] C. Tan *et al.*, “Ex-situ and in-situ observations of the effects of gamma radiation on lithium ion battery performance,” *J. Power Sources*, vol. 357, pp. 19–25, Jul. 2017, doi: 10.1016/j.jpowsour.2017.04.098.

[88] Z. Guo, X. Xu, Md. T. Rahman, M. M. Tehranipoor, and D. Forte, “SCARe: An SRAM-Based Countermeasure Against IC Recycling,” *IEEE Trans. Very Large Scale Integr. VLSI Syst.*, vol. 26, no. 4, pp. 744–755, Apr. 2018, doi: 10.1109/TVLSI.2017.2777262.

[89] R. García Alía *et al.*, “SEL Hardness Assurance in a Mixed Radiation Field,” *IEEE Trans. Nucl. Sci.*, vol. 62, no. 6, pp. 2555–2562, Dec. 2015, doi: 10.1109/TNS.2015.2477597.

[90] J. Cui, Q. Zheng, Y. Li, and Q. Guo, “Impact of High TID Irradiation on Stability of 65 nm SRAM Cells,” *IEEE Trans. Nucl. Sci.*, vol. 69, no. 5, pp. 1044–1050, May 2022, doi: 10.1109/TNS.2022.3164654.

[91] A. P. Karmarkar, B. K. Choi, R. D. Schrimpf, and D. M. Fleetwood, “Aging and baking effects on the radiation hardness of MOS capacitors,” *IEEE Trans. Nucl. Sci.*, vol. 48, no. 6, pp. 2158–2163, Dec. 2001, doi: 10.1109/23.983189.

[92] D. M. Fleetwood, W. L. Warren, J. R. Schwank, P. S. Winokur, M. R. Shaneyfelt, and L. C. Riewe, “Effects of interface traps and border traps on MOS postirradiation annealing response,” *IEEE Trans. Nucl. Sci.*, vol. 42, no. 6, pp. 1698–1707, Dec. 1995, doi: 10.1109/23.488768.

[93] N. A. Anagnostopoulos, T. Arul, M. Rosenstihl, A. Schaller, S. Gabmeyer, and S. Katzenbeisser, “Attacking SRAM PUFs using very-low-temperature data remanence,” *Microprocess. Microsyst.*, vol. 71, p. 102864, Nov. 2019, doi: 10.1016/j.micpro.2019.102864.

[94] J. Mahmod and M. Hicks, “SRAM has no chill: exploiting power domain separation to steal on-chip secrets,” in *Proceedings of the 27th ACM International Conference on Architectural Support for Programming Languages and Operating Systems*, in ASPLOS ’22. New York, NY, USA: Association for Computing Machinery, Feb. 2022, pp. 1043–1055. doi: 10.1145/3503222.3507710.

[95] J. Hovanes, Y. Zhong, and U. Guin, “Beware of Discarding Used SRAMs: Information is Stored Permanently,” in *2022 IEEE Physical Assurance and Inspection of Electronics (PAINE)*, Oct. 2022, pp. 1–7. doi: 10.1109/PAINE56030.2022.10014900.

[96] S. P. Lawrence, S. C. Smith, J. M. Cannon, J. L. Carpenter, D. R. Reising, and T. D. Loveless, “Effects of Total Ionizing Dose on SRAM Physical Unclonable Functions,” *IEEE Trans. Nucl. Sci.*, vol. 69, no. 3, pp. 349–358, Mar. 2022, doi: 10.1109/TNS.2022.3146279.

[97] U. Surendranathan, H. Wilson, M. Wasiolek, K. Hattar, A. Milenkovic, and B. Ray, “Total Ionizing Dose Effects on the Power-Up State of Static Random-Access Memory,” *IEEE Trans. Nucl. Sci.*, vol. 70, no. 4, pp. 641–647, Apr. 2023, doi: 10.1109/TNS.2023.3236625.

[98] G. J. Brucker, J. Wert, and P. Measel, “Transient Imprint Memory Effect in MOS Memories,” *IEEE Trans. Nucl. Sci.*, vol. 33, no. 6, pp. 1483–1486, Dec. 1986, doi: 10.1109/TNS.1986.4334627.

[99] J. T. Schott and M. H. Zugich, “Pattern Imprinting in CMOS Static RAMs from Co-60 Irradiation,” *IEEE Trans. Nucl. Sci.*, vol. 34, no. 6, pp. 1403–1407, Dec. 1987, doi: 10.1109/TNS.1987.4337488.

[100] J. Cui, Q. Zheng, Y. Li, and Q. Guo, “Impact of High TID Irradiation on Stability of 65 nm SRAM Cells,” *IEEE Trans. Nucl. Sci.*, vol. 69, no. 5, pp. 1044–1050, May 2022, doi: 10.1109/TNS.2022.3164654.

[101] A. Garg, Z. C. Lee, L. Lu, and T. T.-H. Kim, “Improving uniformity and reliability of SRAM PUFs utilizing device aging phenomenon for unique identifier generation,” *Microelectron. J.*, vol. 90, pp. 29–38, Aug. 2019, doi: 10.1016/j.mejo.2019.05.013.

[102] U. Surendanathan, H. Wilson, L. R. Cao, A. Milenkovic, and B. Ray, “Analysis of SRAM PUF integrity under ionizing radiation: Effects of stored data and technology node,” *IEEE Trans. Nucl. Sci.*, pp. 1–1, 2023, doi: 10.1109/TNS.2023.3340949.
[103] N. J. Pieper, Y. Xiong, J. Pasternak, D. R. Ball, and B. L. Bhuva, “Effects of TID on SRAM Data Retention Stability at the 5-nm Node,” *IEEE Trans. Nucl. Sci.*, pp. 1–1, 2023, doi: 10.1109/TNS.2023.3346178.
[104] S. Skorobogatov, “Low temperature data remanence in static RAM”.
[105] C. Cakir, M. Bhargava, and K. Mai, “6T SRAM and 3T DRAM data retention and remanence characterization in 65nm bulk CMOS,” in *Proceedings of the IEEE 2012 Custom Integrated Circuits Conference*, Sep. 2012, pp. 1–4. doi: 10.1109/CICC.2012.6330672.
[106] A. Khakifirooz and D. A. Antoniadis, “MOSFET Performance Scaling—Part II: Future Directions,” *IEEE Trans. Electron Devices*, vol. 55, no. 6, pp. 1401–1408, Jun. 2008, doi: 10.1109/TED.2008.921026.