Analyzing the Impact of X-Ray Tomography on the Reliability of Integrated Circuits

Conference Paper · November 2015

DOI: 10.31399/asm.cp.istfa2015p0154

6 authors, including:

Halit Dogan
University of Connecticut
12 PUBLICATIONS **67** CITATIONS
SEE PROFILE

Mahbub alam Md
Universiti Malaysia Perlis
6 PUBLICATIONS **44** CITATIONS
SEE PROFILE

Sina Shahbazmohamadi
University of Connecticut
55 PUBLICATIONS **497** CITATIONS
SEE PROFILE

Domenic Forte
University of Florida
197 PUBLICATIONS **2,328** CITATIONS
SEE PROFILE

Analyzing the Impact of X-ray Tomography on the Reliability of Integrated Circuits

Halit Dogan[1], Md Mahbub Alam[2], Navid Asadizanjani[2], Sina Shahbazmohamadi[3], Domenic Forte[2] and Mark Tehranipoor[2]
[1]Electrical and Computer Engineering, University of Connecticut, Storrs, CT, USA
[3]Mechanical Engineering, Manhattan College, Riverdale, NY, USA
[2]Electrical and Computer Engineering, University of Florida, Gainesville, FL, USA
Email: {dforte, tehranipoor}@ece.ufl.edu

Abstract

X-ray tomography is a promising technique that can provide micron level, internal structure, and three dimensional (3D) information of an integrated circuit (IC) component without the need for serial sectioning or decapsulation. This is especially useful for counterfeit IC detection as demonstrated by recent work. Although the components remain physically intact during tomography, the effect of radiation on the electrical functionality is not yet fully investigated. In this paper we analyze the impact of X-ray tomography on the reliability of ICs with different fabrication technologies. We perform a 3D imaging using an advanced X-ray machine on Intel flash memories, Macronix flash memories, Xilinx Spartan 3 and Spartan 6 FPGAs. Electrical functionalities are then tested in a systematic procedure after each round of tomography to estimate the impact of X-ray on Flash erase time, read margin, and program operation, and the frequencies of ring oscillators in the FPGAs. A major finding is that erase times for flash memories of older technology are significantly degraded when exposed to tomography, eventually resulting in failure. However, the flash and Xilinx FPGAs of newer technologies seem less sensitive to tomography, as only minor degradations are observed. Further, we did not identify permanent failures for any chips in the time needed to perform tomography for counterfeit detection (approximately 2 hours).

Introduction

The problem of counterfeit electronic components continues to grow given the increased complexity of the supply chain and the lack of appropriate countermeasures and detection schemes. Counterfeit components do not possess the exact same specifications as genuine parts, and can impose significant vulnerabilities and threats to the systems in which they are placed. If such parts end up in critical applications (defense, medical, aerospace, transportation, etc.), catastrophic scenarios that result in mission failures, health and safety hazards, and jeopardize national security can occur. Thus, it has become imperative that manufacturers, distributors, and users of electronic components inspect all electronic components for authentication. In addition, counterfeit parts have a negative impact on corporate identity and reputation which can trigger massive revenue losses.

Several test methods have been developed to distinguish counterfeit parts from authentic components. The most common detection methods employed by test labs are physical inspection methods which include incoming inspection, exterior test, interior test, and material analysis. Recently, X-ray Microscopy (XRM) and tomography have distinguished themselves as promising approaches to detect counterfeit ICs due to their ability to unveil the obscured features and details of parts in a nondestructive fashion [1–3]. Although limited information can be extracted from a two dimensional (2D) X-ray images such as bond wire configuration, die orientation, or lead frame, they lack critical information compared to 3D images such as presence of cracks in the die, die face delamination, reworked bond wires, and bond wires configuration in a chip. 3D images, reconstructed from a series of 2D X-ray projections obtained at various rotation angles reveal more information on both interior and exterior of samples. This technique opens up new possibilities for physical inspection procedures and may contribute in a faster and lower cost detection of counterfeit parts [2–5].

Unlike 2D real-time X-ray imaging, a device undergoing tomography is exposed to irradiation for long time. In other words, higher X-ray power and/or longer scanning is needed in order to obtain high resolution images that are free from artifacts. Even though X-Ray tomography is deemed to be non-destructive, it has been reported to affect several IC parameters [6, 7]. While there have been some efforts to show the effect of X-ray on integrated circuits [8–11], none have explicitly investigated the effect of tomography.

This paper attempt to answer many questions related to the concerns on the reliability of X-ray tomography, which is one of the most advanced and effective detection techniques for counterfeit electronic components.

In this work, we examine the effects of X-ray tomography on two types of integrated circuits with different process technologies: (i) flash memories (400 nm and 150 nm) and (ii) FPGAs (90 nm and 45 nm). For both the flash memories and FPGAs, test setups and procedures are designed to capture the parameter shifts and failures caused by repeated X-ray exposure. The effect of X-ray studied in this work is total ionized dose (TID). This is selected due to the fact the devices are not powered up when inspecting the ICs for counterfeit detection with X-ray tomography [6].

The rest of the paper is organized as follows: In Section 2, we elaborate the radiation-induced failure mechanism in CMOS, flash memory and FPGAs. The experimental set up and test procedures are described in Section 3. Section 4 presents the experimental results and its analysis. We conclude the paper in Section 5.

Preliminaries

In this section, we provide background on the sources of failure from irradiation in basic CMOS circuits, flash memory, and FPGAs. For FPGAs, we shall focus our discussion on ring oscillator (RO) circuits which will be used later to capture the degradation in our experiments.

A. Impact of Radiation on CMOS

Radiation damage in CMOS electronics based on TID effect has been described in several earlier works [6, 8, 10–12] . X-ray interacts with the atoms of the matter through photoelectric effect and scattering effect. Electron hole pairs are generated from these interactions.

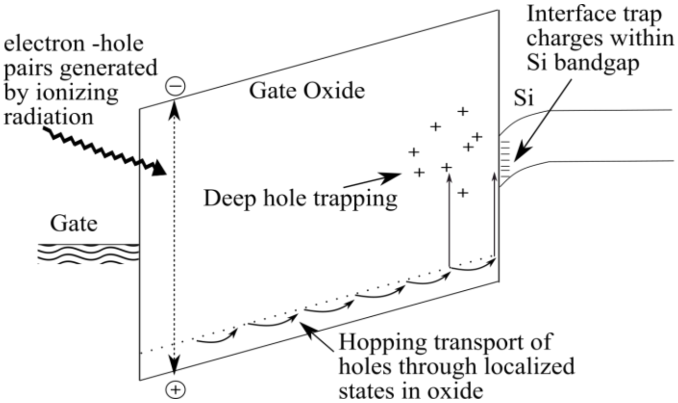
electron -hole pairs generated by ionizing radiation
⊖
Gate Oxide
Interface trap charges within Si bandgap
Si
Deep hole trapping
Gate
Hopping transport of holes through localized states in oxide
⊕

Figure 1: Total ionization dose (TID) effect in CMOS.

The ionization process due to radiation is depicted in Fig. 1. The physical process started from initial deposition of energy can be described as follows:

1. The process is initiated with the generation of electron hole pair by energy deposited on gate oxide. The density of generated pairs depends on the strength of the radiated energy. With electrons having higher mobility than holes, a fraction of the electrons are swept out quickly from the oxide.
2. Simultaneously some fraction of electrons recombine with holes as a function of the energy of incident particles [12].
3. The remaining holes move to the oxide/Si interface through the states of the oxides via hopping transport. Portions of these holes fall into deep traps in the oxide or near the interface. These trapped holes create positive charges and are known as *oxide trapped charge*. The amount of oxide trapped charge is proportional to the thickness of the oxide.
4. Another major contribution of TID effect is the radiation-induced buildup of *interface traps* at oxide/Si interface. The trapped hole defects at interface may exchange charge with bulk Si via electron tunneling and can create interface tapped charge. The reactions between holes and hydrogen containing defects or dopants also help to form the interface traps [7, 13]. These traps are localized states with energy levels in the Si band-gap.

Oxide trapped charge can have a significant impact on electrical parameters of integrated circuits such as shift in threshold voltage, and change in switching speed of the devices. The radiation-induced buildup of oxide trapped charges shifts the gate to source bias point in the negative direction. This leads to a reduction in threshold voltage and an increase in off state and drive current in NMOS. In PMOS, the threshold voltage becomes more negative and the off state and drive current are reduced [6, 7].

Interface trap charge affects the subthreshold swing of a CMOS device. This causes an increase in threshold voltage in NMOS and a decrease in threshold voltage in PMOS. It also increases the flicker or 1/f noise in CMOS devices [6].

B. Flash Memory

Flash memories have been the subject of few studies regarding TID effect [11, 14–17]. Ionization effect in complex control circuitry such as floating gate transistors and charge pump degrades the performance of flash memory. These are discussed in more detail below.

A *floating gate transistor (FG)* is the basic storage element in flash and is used to store one or more bits of data (see Fig. 2). There are three sources of degradation in the FG due TID effects.

1. Induced trapped charges are generated in the oxide due to TID effect. The trapped generation mechanism is similar to the trapped charge generation in CMOS oxide. Note that due to the thick tunnel oxide region between floating gate and the channel, flash memory in older technologies should intuitively be more susceptible to the oxide trapped charges.
2. A fraction of surviving holes generated in the oxide may drift toward the floating gate and recombine with electrons. This process leads to a reduction of electrons in floating gate.
3. Floating gate transistor can also lose charge due to *photoelectric effect*, i.e., impinging radiation provides enough energy for electrons to jump over the oxide. The transistor programmed in the high threshold

voltage moves toward a lower value after irradiation. Conversely, devices programmed in lower threshold state experience an increase in threshold voltage, that is, a positive charge loss from FG [11]. The shift in threshold voltage may corrupt the stored data and/or reduce the retention of the data.

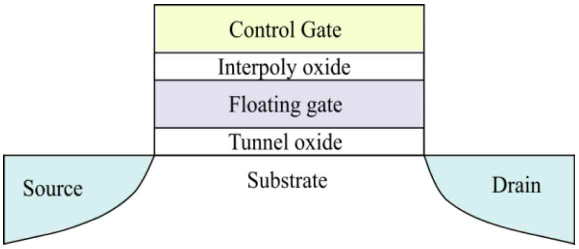

Figure 2: Cross section of a standard floating gate memory cell.

Flash memories often utilize a *charge pump* (multi-stage circuit) to convert the supply voltage (V_{DD}) to a higher voltage that is generally required for an erase operation. Charge pump circuits share a basic design as illustrated in Fig. 3. The common characteristics of a charge pump that has *m* number of stages can be described by following equation:

$$V_{out} \approx (\mathrm{m}+1)\ \left(\mathrm{V}_{DD} - \mathrm{V}_r\right) \tag{1}$$

where, the threshold voltage of each of the MOS is denoted by V_r. The generated output voltage is directly proportional to the number of charge pump stages and, therefore, can be generated even at a very low supply voltage. Output voltage strongly depends on threshold voltage of the MOS.

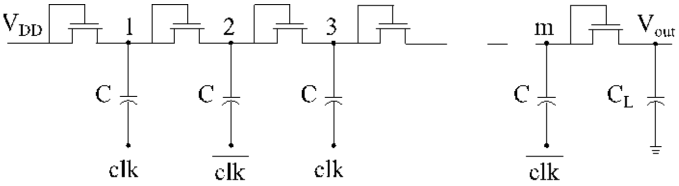

Figure 3: m stage Dickson Charge pump circuit with MOS diodes [18].

As we mentioned in earlier section, the degradation due to TID effect can cause changes in the threshold voltage of the transistors. As a result of this deviation, the output voltage of the charge pump might alter as well, which can create unexpected behavior in flash memory operations.

C. Ring Oscillator (RO)

In the FPGAs under evaluation, *Ring Oscillators (ROs)* will be created to evaluate the performance of FPGAs. A ring oscillator is a circuit that consists of an odd number of delay stages connected in series to form a closed loop chain. An example where each delay stage consists of an inverter is shown in Fig. 4.

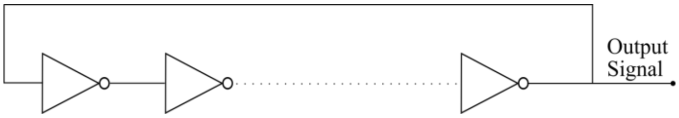

Figure 4: Ring Oscillator with odd number of inverters

The oscillation period is twice the sum of the delays of all elements that compose the loop. Thus, the oscillation frequency of *n* stage inverters can be expressed as:

$$f_o = \frac{1}{2\sum_{i=1}^{n} \tau_{d,i}} \tag{2}$$

where, $\tau_{d,i}$ delay of *i*th delay element.

It is already mentioned that oxide trapped charges and interface trapped charges are generated due to TID effects. It results in a drift in threshold voltage of the MOS transistor. Since the drain current of each transistor is a function of its threshold voltage, the drain current shifts. It causes a change in delay of the circuit.

In this experiment, ROs are mapped on FPGAs using *Look-up Tables* (LUTs). Even though the implementation of ROs in FPGAs is different than ROs implemented by inverters, the change in the DC characteristics is expected to be similar after the X-ray radiation as both implementations consist of MOS transistors. For the FPGA implementation, however, the changes drastically depend on the architecture of the FPGA, which could be either NMOS dominant or PMOS dominant.

Experimental Setup and Test Procedure

In the following subsection, we discuss the experimental setups, the devices that were used in our experiments, the X-ray tomography procedure, and the electrical tests used to test the flash memories and FPGAs before/after exposure.

A. X-ray Tomography Parameters

There are many parameters such as exposure time, source power, etc. that must be tuned carefully during a general X-ray tomography in order to achieve successful imaging process. Optimized values of such parameters have been investigated previously by the authors for different purposes including reverse engineering of Printed Circuit Boards (PCBs) [19] and Thermal Barrier Coatings (TBC) [20]. For counterfeit IC detection, however, even greater care in parameters is needed. First, the imaging must be good enough to capture the defects within a counterfeit IC with high confidence. At the same time, however, too much exposure may damage the chip under test (degrading its performance or leading to failure). Thus, the trade-off between imaging (counterfeit detection) and component failure must be carefully managed.

The impact of the X-ray tomography parameters on the ICs is better to be tracked in a systematical way which has not been investigated before. A Design of Experiments (DOE) table is prepared for this purpose. There are also four different types of semiconductor device fabrication technologies selected, based on their availability, in order to see the trend of the imposed effects on newer technologies and compare to older ones.

The X-ray exposure tests are performed using the Zeiss Versa 510 machine which is equipped with Resolution at a Distance (RaaD) system. Compared with the traditional conventional tomography, the X-rays are better focused in this new generation of the machines. This results in better quality of images and sharper edges. The source distance and the filter are selected based on the limited publications available in the literature on the X-ray impact on flash memories. Although there are general understandings about the X-ray impact on such devices, details regarding the maximum time and power of the exposure are not well understood, especially with respect to 3D imaging. The DOE is presented in the Table I.

Table 1: X-ray Exposure Settings

Tomography parameters	Value
Source distance from sample(mm)	110
Exposure time (Hrs)	0.25-0.50-1.0-2.0-4.0
[Source voltage (kV), power (W)]	[60,7] [80,8] [100,9] [120,10]
Filter	Al – 1mm

In this experiment the distance between the source and the sample is kept constant at 110 mm for all the tests. Source voltage and power are the two parameters directly related to the energy of the electrons bombarding the target metal in the x-ray source. Higher power results in photons with higher energy, which will result in better X-ray transmission through the material and less signal to noise ratio. In order to reduce the effect of hard X-rays on the chips, we have used a 1 mm aluminum filter right in front of the source, which will protect the chips from defects due to the characteristic X-ray emission.

The quality of the image and time of tomography are the two important parameters directly related to the source power and exposure time. Increasing the exposure time will result in higher number of received X-ray counts by the objector, which increases the signal-to-noise ratio for images. An increase in source power will result in higher transmission rate, better resolution, and faster tomography for high Z material. On the other hand, the contrast for low Z material will be decreased. Given that high Z material is used in electronic chips, higher power seems to be the obvious choice, but those same parameters are also responsible for creating defects in ICs. Depending on the size of the chips and the required image resolution, one can extract the 3D information about the lead frame, die rotation, bound wire configuration, and the overall internal structure from a 1-2 hour of X-ray tomography. In Section 4, we will quantify the defects using the electronic tests evaluation methods and will correlate them to the tomography parameters.

B. Electrical Tests

In our experiments, we tested two types of device: flash memories and FPGAs. We have developed different electrical test procedures for each type as shown in Fig. 5. The details of each type will be discussed in the following subsections.

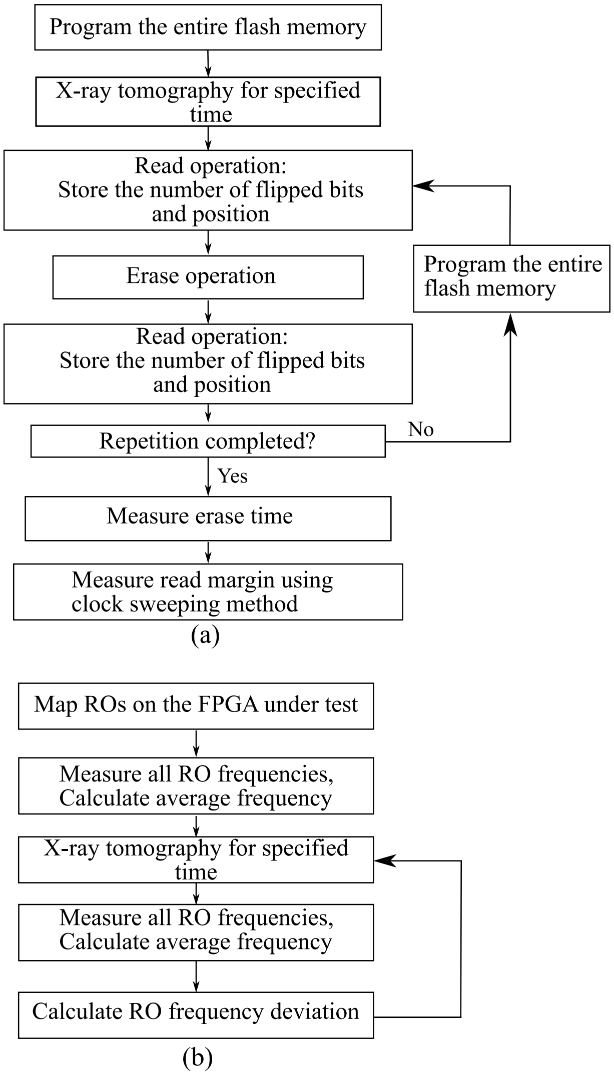
Program the entire flash memory
X-ray tomography for specified time
Read operation: Store the number of flipped bits and position
Erase operation
Program the entire flash memory
Read operation: Store the number of flipped bits and position
Repetition completed?
No
Yes
Measure erase time
Measure read margin using clock sweeping method
(a)
Map ROs on the FPGA under test
Measure all RO frequencies, Calculate average frequency
X-ray tomography for specified time
Measure all RO frequencies, Calculate average frequency
Calculate RO frequency deviation
(b)

Figure 5: Electrical test procedure for (a) Flash memories and (b) FPGAs

1) Flash Memory: NOR type parallel flash memories from Intel (28F400B5) and Macronix (MX29F400C) with different process technology of 400 nm and 150 nm respectively have been used in this work. Experiments were performed on a total of 12 flash memories, 8 of them are from Intel (28F400B5) and the rest are from Macronix (MX29F400C). Since Intel (28F400B5) flash memory is obsolete, there are many counterfeits in the market. Therefore, Intel flash memories are good candidate for our experiment. On the contrary, Macronix flash memory is parallel NOR type flash memory like Intel

Flash but it has relatively newer process technology. That allows us to compare the impact of X-Ray tomography on flash memories with different process technologies. We have done X-ray tomography using the X-ray device described in earlier section on flash memories using 60 kV, 80 kV, 100 kV and 120 kV source voltages. We divided 8 Intel (28F400B5) samples into two sets, Set-1 and Set-2. Set-1 contains samples 1, 2, 3, and 4 while Set-2 contains samples 5, 6, 7, and 8. We used 60 kV for Samples 1 and 5, 80 kV for Samples 2 and 6, 100 kV for Samples 3 and 7, and 120 kV for Samples 4 and 8. We formed a single set of 4 samples of Macronix (MX29F400C) flash for each of the source voltages. The tomography was applied in the following time increments for each flash memory: 15 minutes, 30 minutes, 1 hour, 2 hours and it continued with an additional 2 hours of tomography until the devices failed to complete any of the basic operations (read, program, or erase).

For testing the flash memories after each tomography cycle, a setup was created deploying a Digilent Atlys Board, which includes a Xilinx Spartan 6 FPGA. A flash memory controller was written in VHDL to control the basic operations of the flash memory and perform the required tests. The operations that the controller can handle are *read*, *program* and chip *erase* operations. Read and program operations are in byte mode. In addition to the basic operations, erase timing is also measured using the controller. Along with the memory controller, a UART module is used to send the read data to a PC for analysis. The read margin of the flash memories was also measured using a clock sweeping method [21]. Clock sweeping involves applying a pattern at different clock frequencies from a lower speed to higher speeds. Some paths sensitized by the pattern which are longer than the current clock period start to fail when the clock speed increases. The obtained start-to-fail clock frequency can indicate the delays of the paths sensitized by the patterns.

The test procedure for flash memories is shown in Fig. 5(a). The procedure was repeated for each tomography time period (15 minutes, 30 minutes, and so forth) and it can be described as follows:

1. Program the flash memory (i.e., change the data stored in each cell to ‘0’) and perform the tomography for the specified time.
2. Execute a read operation on whole chip after tomography. If there are any bit flips from ‘0’ to ‘1’, record the number and store the associated locations.
3. Apply an erase operation on whole chip (i.e., change the data stored in each cell to ‘1’) and then a read operation to detect any ‘1’ to ‘0’ transition failures.
4. Program the entire memory again and repeat steps 2 and 3 to determine whether any failures are permanent or temporary. This process is repeated for 10 times.
5. Measure the erase time to obtain any deviation from the initial value.
6. Employ clock sweeping on read operation and record read margin information.

The Intel flash memory (28F400B5) has a pin for erase/program voltage. Either 5V or 12V can be applied to the pin. If 5V is applied, an internal charge pump boosts the voltage to the appropriate erase/program voltage. If the pin is driven with 12V, this voltage is given to the flash cells with an internal voltage control unit. In some steps of the test, we used 12V to see if the failure is due to charge pump or not. In contrast, Macronix (MX29F400C) is a single voltage flash. It needs 5V to read, program and erase operation and always uses an internal charge pump to boost the supply voltage to a higher voltage.

2) FPGAs: We have investigated the effects of X-ray for two different types of FPGA families: Xilinx Spartan 3 (Digilent Spartan-3 Starter Board) and Spartan 6 (Digilent Atlys Board). The technologies of these two FPGAs are 90 nm and 45 nm respectively. The boards contain different components other than FPGAs, so a custom holder was designed to hold both board types, one at a time during tomography. In addition, by using a lead sheet, we shielded the cage to protect other parts of the boards from irradiation effects. Hence, only the FPGA chip on the board was exposed to X-ray and we could fairly evaluate the effect of X-ray on FPGAs. In FPGA experiments, we started our tests with low energy power, but according to the small changes seen in the electronic test results we decided to conduct tests using just high energy power (120kV) for all the reporting tests.

FPGAs are difficult to test in the sense that there are billions of possible logic functions that can be implemented. Thus it is not possible to test all the functional blocks in an FPGA. In addition, in counterfeit IC detection, X-ray is used when the IC is unbiased. So, the effect of X-ray is limited to total ionizing dose (TID), which mainly affects the threshold voltage of CMOS transistors and their switching speeds. Therefore, in our tests, we focused on observing the change in the speed of the FPGA. Specifically, ring oscillators (ROs) were placed into the FPGA and measured to get the delay information of the FPGA Configurable Logic Blocks (CLBs). CLBs might have different number of logic primitives and Look-up Tables (LUTs) depending on the device family. In Spartan 3, each CLB contains 8 Look-up Tables (LUTs), so we placed 7-stage RO to each CLB and covered every CLB. In Spartan 6, because the CLBs have 16 LUTs, 15-stage ROs were created which covered almost all the CLBs in the FPGA. We created hardmacros for RO designs to make sure that internal routing of each RO in every part of the FPGA was exactly same.

The FPGA tests procedure is illustrated in Fig. 5(b) and can be described in the following steps:

1. All the RO frequencies were measured before X-ray tomography.
2. Tomography was performed for the predefined period of time.
3. The frequency of each RO in the FPGA was measured after the tomography and stored in a PC.
4. Deviations from the initial measurement for each RO were calculated according to the following equation:

$$\Delta f_{i,tn} = 100 \times \left(\frac{f_{i,tn} - f_{i,to}}{f_{i,to}}\right) \qquad (3)$$

where, $f_{i,to}$ is the initial frequency of ith RO in the FPGA, and $f_{i,tn}$ is the frequency of the ith RO after the nth tomography cycle. Finally, $\Delta f_{i,tn}$ is the percentage deviation from the initial frequency for the ith RO at time t_n. Positive and negative $\Delta f_{i,tn}$ denote RO speed-up and slow-down respectively.

The above steps were repeated for additional rounds of tomography on both FPGAs. The frequency of each ring oscillator was measured 10 times in every step. Each frequency value is the average of these 10 measurements. There were 1728 and 1476 ROs in Spartan 3 and Spartan 6 FPGAs respectively. The frequency of each FPGA is calculated by averaging the frequency of all the ring oscillators placed in that FPGA.

Results

A. Flash Memory Results

Using the devices and the setup described in experimental setup and test procedure section, the tomography and test cycles were executed. In this section, we summarize our results from each tomography cycle. After finishing all the tomography cycles for both Intel (28F400B5) and Macronix (MX29F400C), the following operations and parameters were unaffected. First, we did not observe any bit flips in any tomography cycle in any sample. This can be explained by the fact that the difference between erased state and programmed state threshold values of the flash memory cells are large enough to prevent being flipped by X-ray high energy photons. Second, there was no change in the read margin of any sample after applying the clock sweeping on read operation. This suggests that the read operation was not affected from tomography in these specific flash memories.

1. Intel Flash: We found that several parameters degraded for the Intel flash (older technology). First, the chip erase time increased exponentially with the exposure time of tomography. Figure 6 and 7 show the change in the erase time for Set-1 and Set-2 respectively. In the figures, the x-axis represents the exposure cycles and y axis corresponds to erase time. As shown in Fig. 6, sample 1 exposed by 60KV did not fail to perform any of the operations after 7 hours and 45 minutes of tomography in total. However, erase time increased by one order of magnitude. Other samples failed in different cycles. For example, samples 2 and 3 which are exposed by 80 and 100KV source failed to erase and write after the third 2 hours of tomography. As one would expect, higher source power had larger effect on the devices. Hence, 120 kV caused the Sample 4 to fail earlier than others. Sample 4 failed to erase one of the main blocks in the first 2 hours tomography cycle, but this failure was temporary. After erasing with external 12V (see Section 3.B.1), it recovered and then operated normally. However, after another 2 hours of tomography it failed to erase and write whether 5V or 12V was applied to it.

It can be seen from Fig. 7 that the second set of samples also follow very similar trends. Sample 8 failed earlier than others due to higher source power 120KV as expected. Similar to Set-1, samples 6 (80KV) and sample 7 (100KV) failed later than sample 8. Sample 5, which was only exposed to 60 kV did not fail at all similar to first set. There were only two major differences to report between the two sets. The devices in the second set lasted 2 hours more compared their counterparts in the first set. In addition, the erase time of sample 5 increased less than that of the sample 1 which was exposed to same source power.

2. Macronix Flash: Erase time of a newer technology (0.15µm) Macronix (MX29F400C) flash after X-ray tomography is shown in Fig. 8. Here, the erase time varied very little over 7 hours and 45 minutes of tomography. Even 120KV source power could not make a significant impact on erase time.

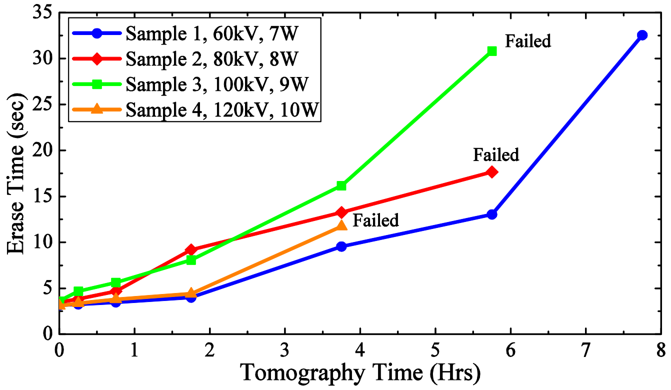

Figure 6: Change in the erase time due to X-ray tomography for Set-1 Intel flash memories.

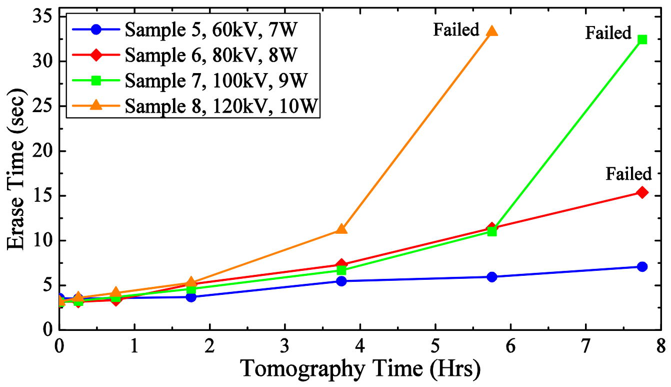

Figure 7: Change in the erase time due to X-ray tomography for Set-2 Intel flash memories.

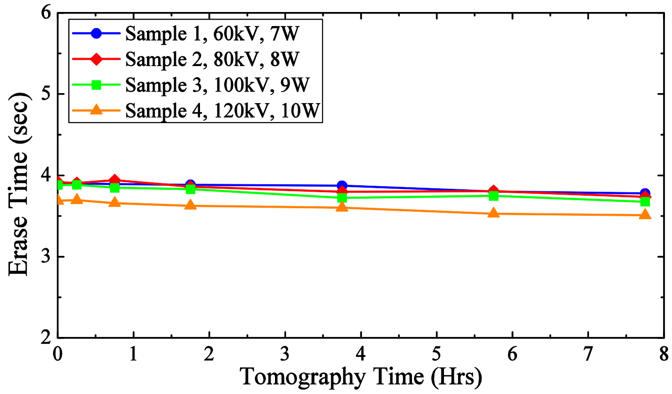

Figure 8: Change in the erase time due to X-ray tomography for Macronix flash memories.

B. Discussion of Flash Memory Results

As the results clearly show, there can be large change in the erase time. This can be explained as follows. The erase operation in NOR flash is described by Fowler Nordheim injection shown in following equation [15, 22].

$$i_{FN} = A \times S_{TUN} \times E_{TUN}^2 \times \exp(B / E_{TUN}) \tag{4}$$

E_{TUN} is the electrical field through the thin oxide. S_{TUN} is the injecting area under the floating gate, A and B are the Fowler-Nordheim parameters. From above relation it is obvious that the most important parameter affecting the total charge injection or erase time of a floating gate transistor is the electric field in the tunnel oxide. The electric field is directly proportional with the erase speed so when the electric field goes up, the erase speed goes up as well. The electric field itself is also directly proportional with the source power [23]. Based on these we have two explanations for the degradation.

First, the failures may be a result of degradation in the charge pump unit of the flash memory. Charge pump degradation due to X-ray tomography can be understood from output voltage (see Equation (1)). Since ionizing dose effect shifts the threshold voltage V_r, the output voltage of the charge pump is reduced. Any increase in stage-to-stage leakage might also reduce the output voltage. The reduced output voltage of charge pump is responsible for slowing down the erasing and it can fail the erasing operation. Our explanation is partially supported by the above results. When the device failed to complete the erase operation with charge pump (5V), it was later erased successfully with 12V. Erase time of second set of Intel flash without charge pump, i.e., with 12V has also been measured in each tomography cycle and it showed the same increase trend with a longer erasing time (see Fig. 9). This observation concluded that charge pump degradation is not the only unit responsible for the change in erase speed.

Second, radiation-induced defects may be created in the tunnel oxide as described Section 2A. Oxide trapped charges and interface trapped charges can affect the electric field across the tunnel oxide, and therefore cause the increase in erase time. In addition, both interface and oxide traps increases monotonically with radiation dose [7]. Therefore with the increase of time, the number of defects increases. This leads to higher erase time and eventually failure. In addition, higher energy radiation enhances the ionization process and makes the failure process faster.

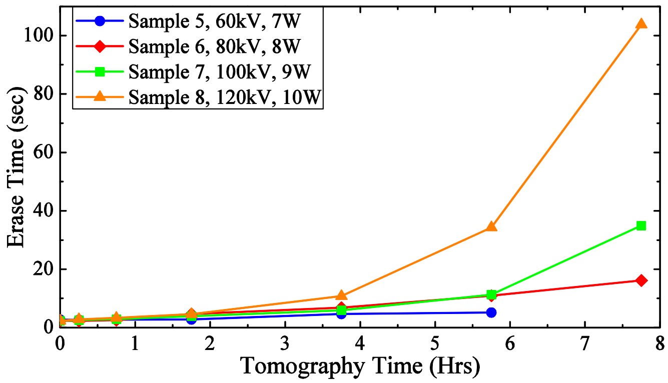

Figure 9: Change in the erase time due to X-ray tomography for Set-2 Intel flash memories with 12V.

The above-mentioned effects are a strong function of the thickness of the oxide. The number of defects in oxide is reduced with the thickness of the oxide. Charge pump degradation is expected to be lower in new technology with a thinner oxide as well. Hence, it can be anticipated that newer technology is more resistant to X-ray tomography. As we see from Macronix flash memory result (Fig. 8), radiation effect has little impact, if any, on erase time. This supports our earlier anticipation.

It has been observed that 2 hours of X-ray scan with high source power such as 120 kV can ensure high-resolution images with enough information that can detect counterfeit IC. If the source power decreases, the scan time should be kept longer to maintain the quality. It has been seen that the erase time went up to 9.5 seconds (initially 3.17) and 5.4 seconds (initially 3.5) for sample 1 and sample 5, respectively after 3 hours and 45 minutes of tomography at 60KV source power. This number goes up with higher source power. These numbers are less than the datasheet specifications. However, as degradation is observed, it might not be safe to use X-ray tomography for this specific flash memory. On the other hand, tomography seems to be safer when carried out for comparatively newer technology flash because of their resistive nature to long term radiation.

C. FPGA Results

For the FPGA experiments, two Spartan 3 and two Spartan 6 FPGAs were tested. Our aim was to utilize as many CLBs in both FPGA types as possible to get a uniform distribution of change in the frequency of the ROs. The test procedure mentioned in earlier section was applied to the FPGAs. Since FPGAs were not powered on, we only expected to observe total ionizing doze effects, which could change the DC characteristics of the transistors [6].

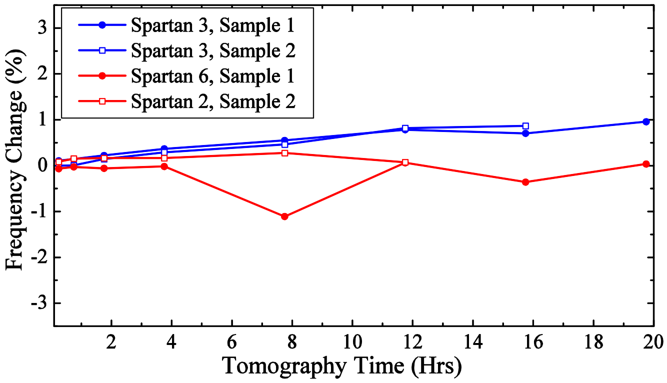

Figure 10: Percentage change in the frequency in Spartan 3 and Spartan 6 FPGAs due to X-ray tomography.

1. Spartan 3: The results of tomography cycles for Spartan 3 and Spartan 6 FPGAs have been illustrated in Fig. 10. Tomography time is represented in the x axis and the y axis corresponds to percentage change in ring oscillator's frequency. Average RO frequency increases with tomography time for both Spartan 3 FPGAs. Both of them showed an identical trend. Maximum variation was found at 19 hours and 45 minutes of tomography. As it is mentioned earlier that each frequency value of FPGAs were calculated by taking averages of all the ring oscillator frequencies, we checked the consistency of the standard deviation of each data points. Standard deviation are within 2288 ± 3 and 1923± 4 for sample 1 and 2 respectively. This justifies the consistency of the data.

2) Spartan 6: Unlike Spartan 3, Spartan 6 results are less consistent. For the first sample, there was no change until the first 4 hours of tomography. After the 4 hours of tomography, the frequency of the ROs decreased a little but it recovered after that cycle. The second sample experienced an increase in the frequencies of ROs but it did not have the same trend as in Spartan 3 FPGAs. Percentage frequency change in sample 1 at 7.75 hours tomography exhibited a large discrimination. This might come from measurement noise (imprecision of equipment, environmental temperature, etc.) or variations in the text procedure (e.g., more recovery time between exposure and measurements). While standard deviation of other data points of sample 1 is around 720, this particular data point has standard deviation of 697. Thus, this point is inconsistent with others.

D. Discussion of FPGA Results

It is observed that both Spartan 3 FPGAs experienced an increase in their average RO frequencies. Since we do not have access to the proprietary architectural details of the Spartan 3 FPGA, it is difficult to give a definitive explanation to the results. One possible reason of frequency degradation can be obtained considering total ionization dose effect. It is already mentioned that oxide trapped charges leads to reduction in the NMOS transistor threshold voltage and negatively increases the PMOS transistor threshold voltage [6]. The delay of a MOS transistor is inversely proportional to the overdrive voltage. A lower threshold voltage results in a decrease of delay of the circuit and thus increases oscillation frequency. Following increasing trend of average frequency it seems that Spartan 3 FPGAs might be NMOS dominant.

Spartan 6 FPGAs are newer technology so the gate oxide is thinner. Thus, it is expected to have less oxide trapped charges due to TID. Instead of oxide trapped charges, border charges and interface traps are expected to be more dominant. It is known that these defects leads to an increase of noise in the transistors, so that the frequencies of ROs might be noisier. This may be partially responsible for the observed inconsistency.

We should note here again that 2 hours of tomography with 120 kV provides very detailed 3D image for the counterfeit IC detection. Therefore, we are mostly interested in the results up to the cycle with 2 hours of tomography which is in total 3 hours and 45 minutes of tomography in this experiment. We can see from Fig. 10 that before the first 4 hours of tomography, the percentage change in RO frequencies are insignificant. While we cannot directly conclude that it is safe to use X-ray but it is obvious that there is little impact on the performance or DC characteristics of the FPGAs.

E. Summary of Major Findings

We summarize the major results of this section as follows:

- High resolution 3D imaging of ICs require 2 hours of tomography at 120KV source power. The Intel flash memory failed the erase operation with charge pump after 3 hours and 45 minutes, and 5 hours 45 minutes of tomography for sets 1 and 2 respectively. While the Imaging process by tomography may degrade the performances of ICs, it seems that counterfeit ICs can be detected without failing the device.
- Some parameters and devices were not impacted much by tomography. The tomography process did not corrupt the read and write operation of either flash memory. It also has little impact on the switching characteristics of the FPGAs.
- New technology devices are friendlier to the tomography imaging process. Electrical characteristics of 150 nm Macronix flash memory, 90 nm and 45 nm FPGAs used in this work did not change by much. Hence, it may be safe to perform tomography on new chips. However, we stress that more experimentation should be performed on many different chips of different technologies, especially regarding the time-to-failure between exposed and unexposed devices.

Future Work

In x-ray tomography, filter is used to remove that undesirable part of the x-ray spectrum. The amount of filtration is generally dependent on the composition and thickness of filter material. The shape of the low-energy end of the x-ray spectrum curve is also determined by filter material. It is recommended that appropriate filtering be used in x-ray inspection to get good image with minimum damage of IC.

Silicon based integrated circuits are vulnerable to very short x-rays (9 KeV and smaller). Zinc filter is very effective to absorb very soft x-rays and it provides suitable x-ray energy beam to ensure good image. The use of aluminum filter also has been effective in protecting the proper performance of ICs. But it is worth to mention that having the combination of high Z and low Z material will force to use a wider range of X-ray power in order to capture a clear image. Other common filter materials are beryllium, copper and stainless steel. The effect of different filter materials on x-ray tomography will be investigated in future research by authors to find the vulnerability of integrated circuits in terms of filter materials.

The KV (kilovoltage) applied to the x-ray tube establishes the energy of the electrons as they reach the anode. The photon energy depends on the applied voltage that can be adjusted. In addition maximum applied voltage plays a major role in determining the quantity of radiation produced for a given number of electrons striking anode. So, the general efficiency of x-ray production can be controlled by applied voltage. The electrical changes of ICs under harsh conditions are targeted in this experiment. These conditions were created by varying applied voltage and power. From imaging point of view the higher KV and power will provide more penetration to emitted photons and results in higher transmission and better quality of image. However, lower KV results in less transmission, longer time period before the chip fails but no good quality for scanned images. Another x-ray equipment adjustment factor is beam current. The change in electrical parameters of IC due to different beam current with constant KV will be carried out in future research.

Conclusions

In this work we presented the impact of X-ray tomography on two different types of ICs. Our results suggest that the FPGAs are more resilient to TID effect and there is not much change in the monitored parameter up to the first 2 hours of tomography cycle. However, we observed some degradation in the erase speed of the flash memories even with 60 kV source power after 2 hours of tomography. With the scaling of the devices this effect is reducing in both cases. It is clearly unsafe to use X-ray tomography for old technology devices. Although there is little observable impact on new technology devices from our experiments, the overall reliability and time-to-failure should also be investigated in future work.

Acknowledgments

The authors would like to acknowledge the support from National Science Foundation (grants CCF-1423282).

References

[1] K. A. M. Ahmood, P. E. L. A. C. Armona, S. I. N. A. S. Hahbazmohamadi, F. I. P. La, and B. A. J. Avidi, “Real-time automated counterfeit integrated circuit detection using x-ray microscopy,” *Appl. Opt.*, vol. 54, no. 13, pp. D25–D32, 2015.

[2] S. Shahbazmohamadi, D. Forte, and M. Tehranipoor, “Advanced Physical Inspection Methods for Counterfeit IC Detection,” in *40th International Symposium for Testing and Failure Analysis*, 2014, pp. 55–64.

[3] S. Bord, A. Clement, J. C. Lecomte, and J. C. Marmeggi, “An X-ray tomography facility for I.C. industry at STMicroelectronics Grenoble,” *Microelectron. Eng.*, vol. 61–62, pp. 1069–1075, 2002.

[4] U. Guin, D. DiMase, and M. Tehranipoor, “A Comprehensive Framework for Counterfeit Defect Coverage Analysis and Detection Assessment,” *J. Electron. Test.*, vol. 30, no. 1, pp. 25–40, Jan. 2014.

[5] M. M. Tehranipoor, U. Guin, and D. Forte, “Counterfeit Integrated Circuits: Detection and Avoidance,” Springer, 2015, pp. 133–151.

[6] H. J. Barnaby, “Total-ionizing-dose effects in modern CMOS technologies,” *IEEE Trans. Nucl. Sci.*, vol. 53, no. 6, pp. 3103–3121, 2006.

[7] P. V. Ma, T.P. and Dressendorfer, “Ionizing Radiation Effects in MOS Devices and Circuits,” in *John Wiley & Sons*, 1989, pp. 35–43.

[8] M. Bagatin, G. Cellere, S. Gerardin, A. Paccagnella, A. Visconti, and S. Beltrami, “TID sensitivity of NAND Flash memory building blocks,” *IEEE Trans. Nucl. Sci.*, vol. 56, no. 4, pp. 1909–1913, 2009.

[9] D. M. Fleetwood, P. S. Winokur, and J. R. Schwank, “Using laboratory X-ray and Cobalt-60 irradiations to predict CMOS device response in strategic and space environments,” *IEEE Trans. Nucl. Sci.*, vol. 35, no. 6 pt 1, pp. 1497–1505, 1988.

[10] X. Yao, N. Hindman, L. T. Clark, K. E. Holbert, D. R. Alexander, and W. M. Shedd, “The impact of total ionizing dose on unhardened SRAM cell margins,” *IEEE Trans. Nucl. Sci.*, vol. 55, no. 6, pp. 3280–3287, 2008.

[11] G. Cellere, A. Paccagnella, A. Visconti, M. Bonanomi, S. Beltrami, J. R. Schwank, M. R. Shaneyfelt, and P. Paillet, “Total ionizing dose effects in NOR and NAND flash memories,” *IEEE Trans. Nucl. Sci.*, vol. 54, no. 4, pp. 1066–1070, 2007.

[12] T. R. Oldham and F. B. McLean, “Total ionizing dose effects in MOS oxides and devices,” *IEEE Trans. Nucl. Sci.*, vol. 50, no. 3, pp. 483–499, Jun. 2003.

[13] L. Tsetseris, R. D. Schrimpf, D. M. Fleetwood, R. L. Pease, and S. T. Pantelides, “Common origin for enhanced low-dose-rate sensitivity and bias temperature instability under negative bias,” *IEEE Trans. Nucl. Sci.*, vol. 52, no. 6, pp. 2265–2271, Dec. 2005.

[14] M. Bagatin, G. Cellere, S. Gerardin, A. Paccagnella, A. Visconti, and S. Beltrami, “TID Sensitivity of NAND Flash Memory Building Blocks,” *IEEE Trans. Nucl. Sci.*, vol. 56, no. 4, pp. 1909–1913, Aug. 2009.

[15] D. N. Nguyen, S. M. Guertin, G. M. Swift, and A. H. Johnston, “Radiation effects on advanced flash memories,” *IEEE Trans. Nucl. Sci.*, vol. 46, no. 6, pp. 1744–1750, 1999.

[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.

[17] T. R. Oldham, R. L. Ladbury, M. Friendlich, H. S. Kim, M. D. Berg, T. L. Irwin, C. Seidleck, and K. A. LaBel, “SEE and TID Characterization of an Advanced Commercial 2Gbit NAND Flash Nonvolatile Memory,” *IEEE Trans. Nucl. Sci.*, vol. 53, no. 6, pp. 3217–3222, Dec. 2006.

[18] G. Palumbo and D. Pappalardo, “Charge Pump Circuits: An Overview on Design Strategies and Topologies,” *IEEE Circuits Syst. Mag.*, vol. 10, no. 1, pp. 31–45, 2010.

[19] Quadir S.E and Chen J. and Forte D. and Asadizanjani N. and Shahbazmohamadi S. and Wang L. and Chandy J. and Tehranipoor M., “A survey on chip to system reverse engineering,” *ACM J. Emerg. Technol. copmuting Syst. (accepted for Publication)*, 2015.

[20] Asadizanjani N. and Shahbazmohamadi S. and Jordan E.H., “Investigation of Surface Geometry Change in Thermal Barrier Coatings Using Computed X-ray Tomography,” *Dev. Strateg. Mater. Comput. Des. V Ceram. Eng. Sci. Proc.*, vol. 35, no. 8, 2015.

[21] K. Xiao, X. Zhang, and M. Tehranipoor, “A Clock Sweeping Technique for Detecting Hardware Trojans Impacting Circuits Delay,” *IEEE Des. Test Comput.*, vol. 30, no. 2, pp. 26–34, 2013.

[22] P. Canet, V. Bouquet, F. Lalande, J. Devin, and B. Leconte, “Fowler-nordheim erasing time prediction in flash memory,” in *Symposium Non-Volatile Memory Technology 2005.*, pp. 15–18.

[23] P. Cappelletti, C. Golla, P. Olivo, and E. Zanoni, *Flash Memories*, Springer, 1999.