cryptography

Article

Non-Invasive Detection Method for Recycled Flash Memory Using Timing Characteristics †

Sadman Sakib , Preeti Kumari, B. M. S. Bahar Talukder, Md Tauhidur Rahman and Biswajit Ray *

Department of Electrical and Computer Engineering, The University of Alabama in Huntsville, Huntsville, AL 35899, USA; ms0171@uah.edu (S.S.); pk0039@uah.edu (P.K.); bt0034@uah.edu (B.M.S.B.T.); tauhidur.rahman@uah.edu (M.T.R.)

* Correspondence: biswajit.ray@uah.edu; Tel.: +1-256-824-5679

† This paper is an extended version of our paper published in2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), Washington, DC, USA, 30 April–4 May 2018; pp. 89–95, doi:10.1109/HST.2018.8383895.

Received: 9 July 2018; Accepted: 10 August 2018; Published: 12 August 2018

Abstract: Counterfeiting electronic components is a serious problem for the security and reliability of any electronic systems. Unfortunately, the number of counterfeit components has increased considerably after the introduction of horizontal semiconductor supply chain. In this paper, we propose and experimentally demonstrate an approach for detecting recycled Flash memory. The proposed method is based on measurement of change in Flash array characteristics (such as erase time, program time, fail bit count, etc.) with its usage. We find that erase time is the best metric to distinguish a used Flash chip from a fresh one for the following reasons: (1) erase time shows minimal variation among different fresh memory blocks/chip and (2) erase time increases significantly with usage. We verify our method for a wide range of commercial off the shelf Flash chips from several vendors, technology nodes, storage density and storage type (single-bit per cell and multi-bit per cell). The minimum detectable chip usage varies from 0.05% to 3.0% of its total lifetime depending on the exact details of the chip.

Keywords: counterfeiting; recycled Flash memory; recycled Flash memory detection

1. Introduction

Counterfeit electronics have become a significant concern in the globalized semiconductor industry where chips might be recycled, remarked, cloned, out-of-spec/defective, and tampered [1–6]. Flash memory, which is commonly used as non-volatile data storage in many electronic systems, is one of the primary targets of the counterfeiters [7–12]. Counterfeiting of Flash memory has the severe consequence on its reliability or lifetime due to its limited endurance. The endurance of Flash is critical in many embedded applications where Flash is used for storing the operating system or other sensitive information. Hence the failure of Flash memory essentially leads to system failure, which might have a radical impact on many critical applications including healthcare, aero-space, finance, defense, etc. In this context, use of recycled or counterfeit Flash memories in critical areas may cause loss, not limiting to resources but to human life as well. Therefore, it is vital to prevent these recycled memories from entering into the IC supply chain.

Identification of counterfeit Flash memory with non-invasive technique is extremely difficult as the memory chip may remain functional at the time of selling a product and hence it may pass the standard product qualification tests. In addition, there remains chip-to-chip manufacturing variation, which makes the early stage detection of counterfeit Flash memory even harder with the standard test solutions. While there are several recent research in the area of counterfeit IC detection (details given in

Section 3), most of the existing techniques suffer from following major limitations: (i) requires hardware modification in the design phase, (ii) requires extensive chip registration process and maintenance of large database, (iii) produces a large number of false positive results, (iv) time consuming and manual labor extensive etc. In general, detection of recycled Flash memories must follow the following criteria [4,5,13]:

- Detection method has to be quick, non-invasive, and inexpensive.
- The detection approach has to be suitable for mass-volume recycled Flash chips because some detection technique (e.g., ID-based) is complex and does not support detection for mass-volume chips.
- The technique must work on all new memory and currently available memory. Approaches like on-chip sensors [14–18] are only effective for new chips.
- The detection mechanism needs to be robust against temperature and voltage variation.
- Minimal usage or no usage of the database is another criteria for the detection mechanism.
- The detection method needs to be straightforward and should provide a yes-no decision with a high confidence level. The detection technique should also identify the exact usage of the memory.
- Detection techniques should be independent of the vendor, technology node, and capacity. However, the threshold of detection parameter might vary across manufacturers, technology nodes, and capacities.

In this paper, we propose and experimentally demonstrate recycled chip detection technique based on the change in Flash parameters with usage that fulfills the above detection criteria. The key contributions in this paper include:

- We propose a universal and widely applicable framework to identify recycled Flash memories by measuring the Flash array characteristics, such as erase time, program time, fail bit counts, etc.
- Experimental data shows that erase time is the best metric to detect recycled Flash chip. We find that erase time shows minimum variation between different memory blocks and it increases significantly with usage.
- We validate our proposed method with commercial off the shelf Flash chips from several vendors, technology nodes, memory types (SLC vs. MLC), and capacity (i.e., memory size). Measurement results show that we can detect a recycled Flash chip with high accuracy if it has been used as less as 0.05% to 3.0% of its total lifetime.
- Proposed method does not require any hardware modification or any prior database maintenance. Hence it can be implemented on many existing storage solution with system updates.

The rest of the paper is organized as follows. The detail description of a Flash memory and the metrics of our interest to detect recycled Flash memory is explained in Section 2. In Section 3, the existing work in the area of detecting counterfeit IC is discussed. Flash memory characterization and our proposed recycled Flash memory detection methodology are described in Section 4. In Section 5, our experimental setup, results, and analysis are illustrated in details. We conclude our work in Section 6.

2. Background

Flash Memory Cell: Figure 1 shows the structure of a floating gate (FG) Flash memory cell, its typical current-voltage characteristics, and a Flash memory array. The memory cells are made from floating-gate MOSFETs (Metal Oxide Semiconductor Field Effect Transistor), where, the floating gate is insulated between the control gate and the channel. The floating gate in different technology is replaced with the charge trap layer. The two insulating oxide layers: blocking oxide and tunnel oxide, isolates the floating gate from the control gate and the transistor channel respectively. The floating gate store information in the form of charges (electrons) and retain that information for a long time without requiring any power.

Flash Memory Array: A typical Flash memory array has a grid of columns and rows of floating gate MOSFET cells (shown in Figure 1c). The word line (WL) electrically connects the cells in each row of a block. The bit line (BL) is the vertical line and each column of cells in a block is connected to different BL. The WL acts as the control gate of the floating gate transistor and the BL connects the drains of the floating gate cells together and represents a data bus. The voltage combinations applied to WL and BL define the program, erase and read operation. Each block consists of multiple WLs and the size of a page is defined by the number of cells in each row. For single-level cell (SLC), SLC stores only one bit per cell and each WL define one page. For multi-level cell (MLC), each WL define two or more pages of data and thereby, can store multiple bits per cell.

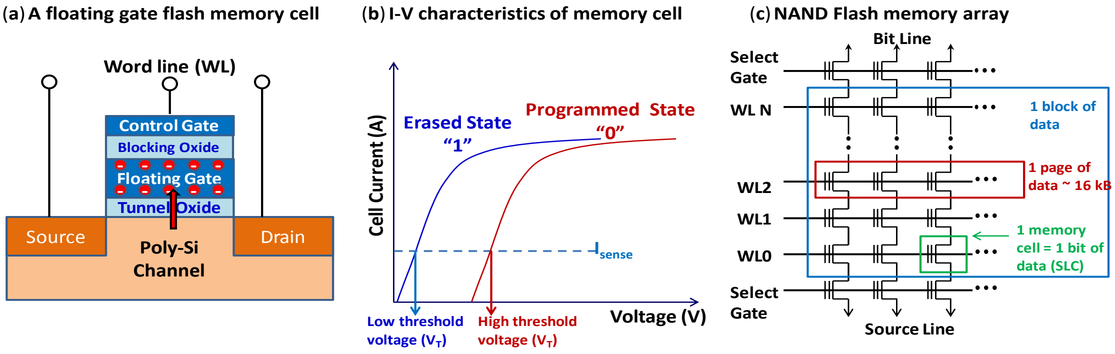

Figure 1. (**a**) A floating gate (FG) NAND Flash memory cell which stores charge in the FG. Metal word-line (WL) act as the control gate of the FG transistor. Information's are stored in the FG through tunneling of electron from Si-channel to FG. Blocking oxide prevents back tunneling of electron to control gate. (**b**) Typical current-voltage characteristics of a Flash memory, (**c**) The hierarchical storage in NAND Flash array consisting of kilo-bytes of memory cells and the WL electrically connects those cells (called a page of information). Each block consists of multiple WLs. The select gate transistors can be standard MOSFET or FG transistors, depending on manufacturer or technology node.

Flash Memory Operation: Flash devices perform three basic operations: program (write) a page, erase a block, and read a page. Flash stores the information by removing or putting charges on its floating gate and charges on the floating gate affects the threshold of the memory element. During a program operation, a high voltage is applied to the control gate (WL) to excite the electrons and consequently, excited electrons are forced to jump through the insulating layer (tunnel oxide) onto the floating gate, via a process called Fowler-Nordheim tunneling. These electrons act as a barrier between the control gate and the floating gate and thereby, increases the threshold voltage of the floating gate MOSFET. This programmed state of the memory cell can be represented as logic "0". In the erase operation, the electrons in the floating gate are pulled off and tunneled from the floating gate to the source and substrate, which is achieved by applying a high positive voltage on the substrate and the control gate is grounded. This erase state will have lower threshold voltage and the state of flash memory cells will be bit "1" because floating gates carry no negative charges. The read operation involves sensing the state (threshold voltage) of the memory cell, which is distinguished by the current flowing between the drain and the source. In read operation, a reference voltage, which is lower than the programmed voltage, is applied to the control gate (WL) to sense the cell current (cell will either conduct current or not). This cell current will be sensed as logic "1" or "0" to represent erase or program state respectively.

3. Existing Work on Detecting Counterfeit IC

Over the past few years, researchers have proposed several methods to detect counterfeit ICs, which can be categorized into different groups [5]: First method is physical and electrical tests, physical tests are invasive in nature as they are based on probing any physical modification of counterfeit ICs based on different image analysis techniques [19–22]. Electrical tests can be used to detect defects and anomalies like broken wire bond, open-short faults on the interconnect etc. and find the anomalies for the internal structures, logic gates, etc [5,22–25]. The second test method is tracking and tracing, where electronic chip ID, IP watermarking, IC metering or hardware metering are used to detect the counterfeit ICs [26–29]. The third detection method is based on on-chip aging sensors, where an on-chip structure is used to observe and realize the aging and reliability of electronic components. The age sensor usually works as an odometer to measure the performance degradation with aging [14–18,23,30]. Various methods have been proposed to sense the age of ICs, such as, the beat frequency of stressed and unstressed ring oscillators [31], NBTI and defect-induced oxide breakdown effects [32], threshold voltage degradation [33], frequency degradation of ring oscillators [34], path delay fingerprinting [35], etc.

Concerning counterfeit memory chip detection, Guo et al. [7] used partial programming concept to detect the recycled Flash memory for more than 5% of its end-of-life usage. However, their technique is time intensive and requires maintenance of extensive database, which limits its applicability for a wide range of products. In [36–38], a recycled SRAM chip is detected using an ID-based approach. In this method, the device signature is generated through the startup values of an SRAM chip, where signature shows the degradation due to aging. Then the signature from a recycled SRAM and fresh SRAM chip are compared to identify the counterfeit SRAM chip. This method is costly to perform and not suitable for mass-volume detection because it involves the application of high and low temperature to generate a useful signature. In summary, the existing works on counterfeit IC detections are mostly on FPGA, SRAM, DRAM etc. and there are a very few works on the detection of recycled Flash memory [5,23,39].

4. Recycled Flash Memory Detection

In this section, we present our framework for the detection of recycled Flash chip by analyzing memory characteristics as a function of chip usage. Specifically, we analyze the effect of usage (basically program erase operation) on program time for a page, erase time for a block and fail bit count (FBC) per page.

The aim of this study is to identify the appropriate Flash characteristics to detect a counterfeit Flash chip from an authentic one with high accuracy. As discussed in the background section, program-erase operation in a Flash memory involves high voltage on the control gate during programming and on the Si substrate during erase operation. High voltage exerts a high electric field across the tunnel oxide and creates defects in the oxide as well as at the interface between oxide and silicon substrate. Therefore, the increasing number of PE operation will increase the defect creation. The electric field across the oxide is reduced with the increasing number of defects creation and slows down the erase operation. On the contrary, the threshold voltage of a Flash cell is increased due to the defects creation, which makes the program operation slightly faster. Despite the fact that program speed increments with usage, it additionally expands the likelihood of over-programming and consequently increases the FBC in a page after programming. The FBC also increases with the fluctuation of Flash cell current during sensing due to the increments of read noise with the number of defects in the Si-channel [40]. In Section 5.3, we analyze erase time, program time and FBC as a function of PE cycle to define a complete methodology for counterfeit Flash memory identification.

The manufacturing variation in a flash chip is a major challenge and cannot be neglected, which may exist in the different blocks of the same chip and may exist in the different chip of the same technology node itself. The process variation of the chip needs to be considered and we need to confirm that there is no overlap in the distribution of the device property for a fresh memory and a recycled memory. Thus we have to define a proper memory characteristic, which is easily quantifiable and has a discernible change in its value with program-erase cycling.

Figure 2 shows our recycled Flash identification approach. We measure several Flash characteristics (such as erase time) on different memory location of a chip in order to plot the variation of that parameter within a chip. Then, we compare the same Flash characteristics as a function of memory usage as shown in Figure 2a. The figure shows that the upper tail (CDF) of Usage-0% intersects the lower tail (CDF) of Usage-u_1% at α_1, so the confidence level to detect u_1% usage is $(1 - \alpha_1)$ * 100. Whereas, the intersection point (α_2) for Usage-0% and Usage-u_2%, is α_2 = 0 and so, the confidence level to identify a used Flash chip is ∼100%, when the Flash memory is used for u_2% of their lifetime. Here, Alpha (α) defines the cumulative probability of the used chip to fall below the threshold of detection (Flash) parameter. From the value of α, we can compute the confidence level, which measures whether we can distinguish a recycled Flash chip precisely. Figure 2b shows the confidence level which can be obtained from Equation (1).

$$Confidence\ level = (1 - \alpha) * 100\% \tag{1}$$

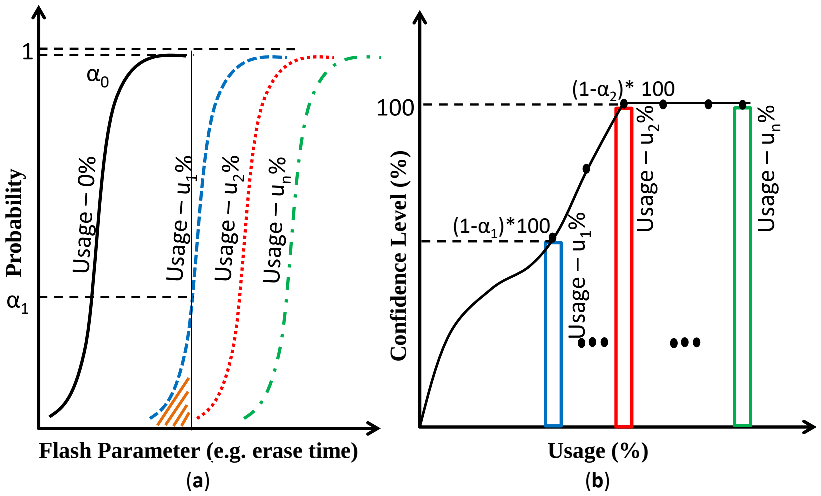

Figure 2. (**a**) The CDF of decision parameters changes with usage and (**b**) the confidence level calculation from the CDF, where Confidence level changes with usage.

A 100% confidence means that a counterfeit Flash memory is identified as a counterfeit one. From Figure 2b, we can see that we can identify a recycled chip if it has been used for u_2% of their lifetime where the confidence level is 100%. Our confidence level or detection rate becomes low for a chip if that particular chip is used for less than u_2% of its endurance. Figure 3a shows our experimental result for erase time distribution on MLC chip. We find that, there is no overlap in the distribution between fresh and used chip (50 times PE cycled). This means that a 50 times cycled chip can be detected with high accuracy by monitoring erase time. The results and data discussed in the following section confirm that the increment of erase time with usage is showing monotonic behavior. In general, there should not be any overlap between the fresh CDF and the used CDF of Flash parameters (such as erase time) for the high confidence level. However, there might be an overlap between the distributions (i.e., fresh vs. used CDF) because of low usage of a chip, which can reduce the confidence level. Therefore, in our experiment, ≥98% confidence level is considered to be an acceptable confidence level to conclude whether the chip under test is recycled or authentic; mainly because of the limited number of samples.

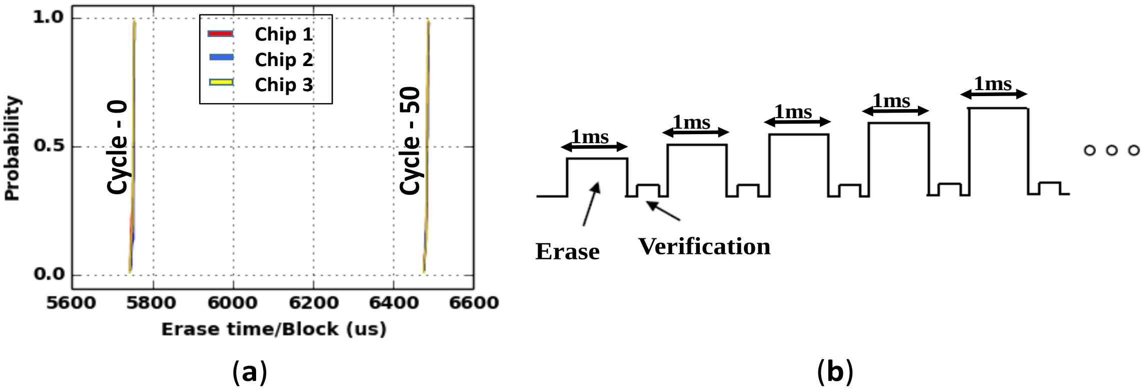

Figure 3. (**a**) Used vs. fresh Flash chip: timing parameters changes with usage. (**b**) The erase operation in the NAND Flash takes place in multiple pulses or loops.

5. Results and Analysis

5.1. Experimental Set-Up

In our experiment, we use off the shelf Flash chips (see Table 1 for the specifications) and custom flash test board to program, erase and read the Flash chips, where the board is entirely made with commercial off-the-shelf components with a custom PCB board. There is a NAND flash socket to hold a flash chip under test, an Atmel ATSAM3U4C ARM Cortex-M3 microcontroller to issue commands and receive data from the flash chip. High-speed USB interface is integrated into the ARM microcontroller. A summary of steps followed for data collection in our experiment is given below:

- At first a block is selected on which we want to perform program-erase operation.
- The selected block is then erased, or in other words, all the bits of that block is set to "1".
- Then the block is programmed with all "0" data pattern.
- Read operation is then carry out on one page at a time.
- Program time, Erase time and FBC are then recorded.
- Process is then continued for other blocks of the memory.
- Finally different plots are obtained by analyzing the recorded data.

Table 1. Summary of results for the different type of Flash chips.

Part Number	Manufacturer and Chip Description	Endurance (P/E Cycle)	Chip Count	Acceptable * Confidence Level @
MT29F64G08CBABAWP:B TR	Micron 64 Gb MLC (20 nm node)	5000	3	≥0.25% usage
MT 29F32G08CBADAWP:D	Micron 32 Gb MLC (20 nm node)	5000	3	≥1.4% usage
TC58NVG3S0FTA00-ND	Toshiba 8 Gb SLC (32 nm node)	100,000	3	≥2% usage
MT29F8G08ABABAWP:B	Micron 8 GB SLC (34 nm node)	100,000	3	≥2.7% usage
MT29F8G08ABACAWP:C	Micron 8 GB SLC (25 nm node)	100,000	3	≥0.05% usage
MT29F4G08ABADAWP:D TR	Micron 4 GB SLC (34 nm node)	100,000	3	≥3% usage

* Acceptable (i.e., ≥98% confidence level).

In the experiment, we used 100 blocks per chip for program-erase operation, collected data and analyzed them as a function of PE cycle count. After programming all bits should have set to "0", but it is observed that few bits flip and those are called fail bits (FBC). We count the number of fail bits per page for a given Flash chip. We also analyze the erase and program time behavior of a Flash chip for a different number of PE cycle count. We perform our analysis on the different type of Flash chips (SLC and MLC) from various manufacturers of different technology nodes.

5.2. Measurement Procedure for Flash Timing

To measure the Flash timing characteristics such as erase time, we first measure the time (t_{start}) at which the erase command is issued by a microcontroller. We again measure the time (t_{end}) after completion of erase operation. The time difference between (t_{end}) and (t_{start}) is the erase time ($t_{end} - t_{start}$) used in this work.

$$Erase\ time(t_{erase}) = t_{end} - t_{start} \tag{2}$$

Erase operation (Figure 3b) in Flash memories happens in multiple pulses (pulse width~1 ms). After every pulse, a verify operation is applied to check the state of all the cells. If the cells are not erased, then another pulse and verify operation is applied. This process will continue until all the cells get erased. Such type of pulse by pulse erasing is the reason for the step-wise increase in erase time. Figure 4a shows that the erase time increases in steps.

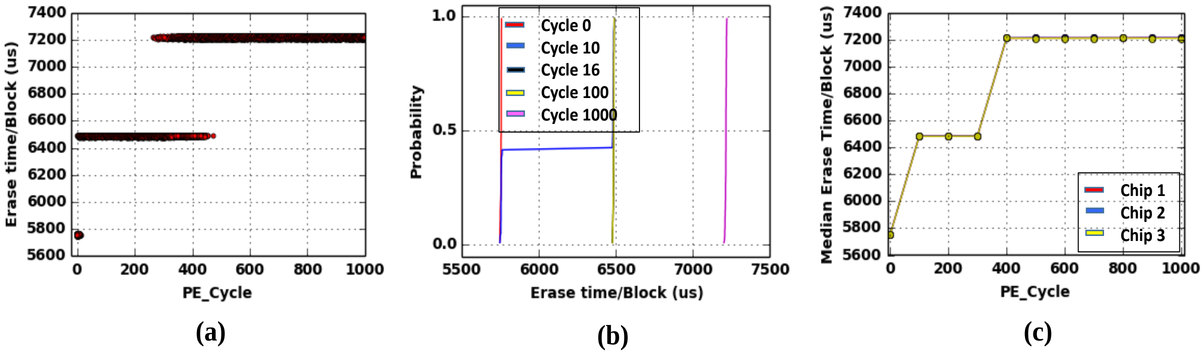

Figure 4. (**a**) Scatter plot of erase time (Y-axis) with respect to usage (PE cycle count) (X-axis), where PE cycle count is 1000 and for each PE cycle count, we have used 100 blocks to obtain the scatter plot, (**b**) Cumulative Distribution Function (CDF) of Erase time for cycle 0, 10, 16, 100, and 1000, and (**c**) Median erase time per block (Y-axis) with respect to usage (X-axis).

5.3. Evaluation of Different Flash Characteristics for Early Detection

In this section, we provide data for different memory performance parameters (erase time per block, program time per page, fail bit count per page, etc.) as a function of PE cycling. Figure 4a shows the erase time dependence on PE cycle count. Please note that erase time increases with cycling in discrete steps. Such step by step increase of erase time is a result of pulse by pulse erase operation as described in Figure 3b. Figure 4a also shows an overlap region, where two different erase time is observed for a given PE cycle count. This is due to the block to block variation in erase time degradation with cycling. In our experiment we choose 100 blocks for every PE cycle count and the overlap region shows that different block has different erase time. Block to block variability is more clearly illustrated in Figure 4b, where the cumulative distribution of erase time is plotted for a given PE cycle condition. Interestingly, we find that erase time has a very sharp distribution (or minimal variation) for fresh condition (red). However, with a few PE cycles, the erase time distribution widens (blue). This imposes a constrain on minimum usage detection threshold, since for accurate detection of cycled condition there should not be any overlap between fresh and cycled distribution. With the Micron MLC chip we find that for PE cycle count = 16, erase time distribution has no overlap with fresh (black curve) condition. Thus, minimum usage that can be detected with erase time for this chip = 0.32% (end of life PE cycle count = 5000). In Figure 4c we show the erase time dependence on PE cycling for 3 different chips of the same part number, which shows minimal chip-to-chip variation and hence the applicability of the erase time-based detection method.

In Figure 5a, we show the program time dependence on PE cycle count. The results demonstrate that the estimation of program time is decreasing with the number of PE cycle count, which is due to a slight increase of threshold voltage of an individual Flash cell. The reduction of threshold voltage in a

Flash cell is anticipated as because the increasing number of PE cycles are responsible for increasing number of defects creation in a silicon-oxide channel and thereby reduce the cell current in a Flash memory. However, the CDF of program time for a fresh and used Flash memory is wider (shown in Figure 5b), and it overlaps with each other. Hence, the program time cannot be used alone to identify new and recycled Flash chip with ∼100% precision. In Figure 5c, we plot program time data from three different chips to make sure that all the Flash chips are showing identical behavior among the chip and the plot clearly shows uniform behavior for all the chips.

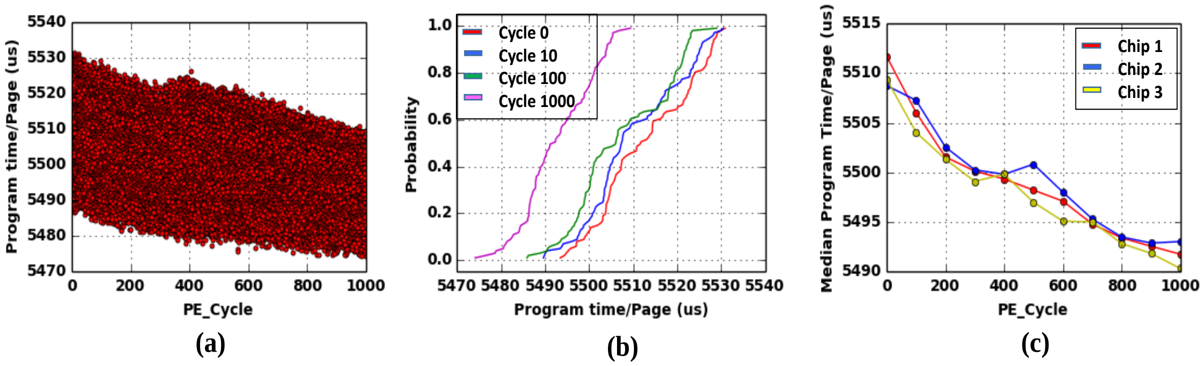

Figure 5. (**a**) Scatter plot of program time (Y-axis) with respect to usage (PE cycle count) (X-axis), where PE cycle count is 1000 and for each PE cycle count, we have used 100 blocks to obtain the scatter plot, (**b**) Cumulative Distribution Function (CDF) of program time for different PE cycle count. (**c**) Median program time per page (Y-axis) with respect to usage (X-axis).

Figure 6a shows FBC plot for a page as a function of usage, where we measure FBC just after the program operation of that page. Our experiment involved with 100 blocks from a chip and 1000 PE operation on each block, and then, we recorded data and plotted a scatter plots with all the FBC (per page) values. Not surprisingly, the increasing number of PE cycle count is the reason of increasing FBC count. However, like program time, the CDF of FBC values also shows wider distribution for fresh and recycled block and there is a significant overlap between them. Hence, the recycled Flash memory cannot be detected simply with the FBC only. To ensure the identical behavior among different chip of the same part number, in Figure 6c we plot FBC data for three different memories, where the plot is showing uniform behavior within the Flash chip.

In summary, erase time is the best Flash memory parameter to use for the proposed detection technique, which can be explained as follows: erase operation in a Flash memory takes place as a block by block basis while program and read operations are page by page basis. In a Flash memory array, there remains large variation between different pages within a block. Hence the program time or read time or fail bit count per page varies significantly for the same usage. However, a memory block is a large repeatable unit in a Flash array which is very much identical for a given chip. Hence the variation of erase time between a block is very low and with usage, erase time increases in discrete steps (details given in Section 5.2). Our experimental data also shows that erase time is the best metric in order to differentiate a counterfeit Flash memory from the authentic one for the following reasons: (1) Erase time has very tight distribution (or minimal variation) on a fresh chip. Thus, the median erase time typically specified in the product data sheet is a good representation of erase time value for that class of Flash ICs, (2) With program erase cycling, erase time increases in discrete but large steps (∼1 ms). The large increase in erase time with usage and the initial tight distribution ensures that there is no overlap of erase time distribution of a fresh chip vs. used chip, (3) The minimum usage level for accurate detection of used chip using erase time will depend on the exact technology and chip details, however, the general methodology will hold for any Flash chip.

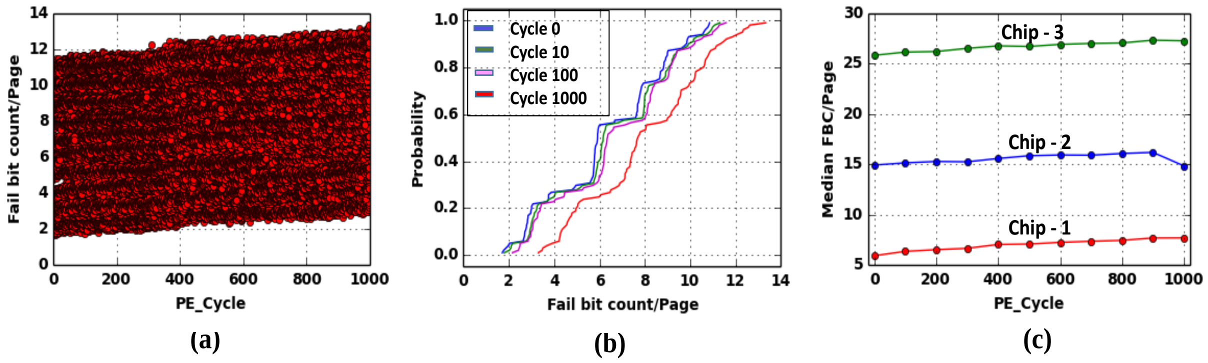

Figure 6. (**a**) Scatter plot of fail bit count (Y-axis) with respect to usage (PE cycle count) (X-axis), where PE cycle count is 1000 and for each PE cycle count, we have used 100 blocks to obtain the scatter plot, (**b**) Cumulative Distribution Function (CDF) of FBC for different PE cycle count, and (**c**) Median FBC per page (Y-axis) with respect to usage (X-axis).

5.4. Validation on Different Technology Nodes

We find that the proposed method works for different technology nodes. We validated our proposed technique with two 8GB SLC Flash memory chips from the same manufacturer of different technology nodes (34 nm and 25 nm). Figure 7a,b present that the erase time CDF for 34 nm and 25 nm technology nodes. The results show that the erase time increases with the number of program-erase operation increases. We also find that the Flash chips from different technology nodes degrade at different rates. The degradation rate is faster for a smaller technology node compared to an older technology node. As the technology node is scaled down, the number of electron/cell decreases. As cell size reduces, small number of defects created by a few program-erase cycles will cause large positive shift in the intrinsic threshold voltage of the cells. Therefore, it becomes harder to erase cells of lower technology nodes after a few cycles of usage. For 34 nm technology node (Figure 7a), the erase time changes after usage of 2700 PE cycles. A change in erase time is observed after only 67 PE cycles for the 25 nm technology node. The usage vs. confidence level plot in Figure 7c shows that a Flash chip of lower technology node (25 nm) can be detected at earlier (usage 0.05% for the sampled chips) stage than a higher technology node (usage 2.7% for the sampled chips). Table 1 shows more results and comparison from different technology nodes for a given manufacturer.

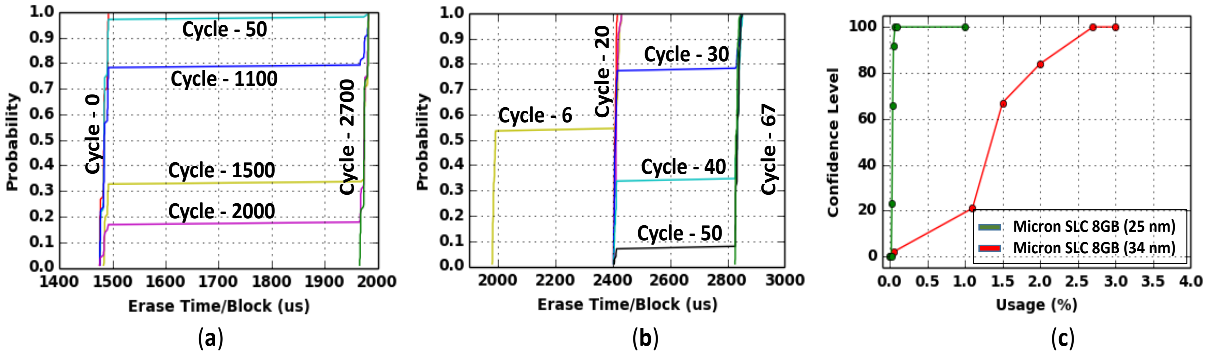

Figure 7. (**a**) CDF of erase time for PE cycle 0, 50, 1100, 1500, 2000 and 2700 for Micron 8GB SLC (34 nm). (**b**) CDF of erase time for PE cycle 6, 20, 30, 40, 50 and 67 for Micron 8GB SLC (25 nm). (**c**) The confidence level for the Flash chips of 34 nm and 25 nm technology node.

5.5. Validation on Flash Chip from Different Manufacturers

Another important criterion of a detection methodology is that it has to be independent of manufacturers. Here we validate our method using two SLC Flash memories from two important manufacturers, Micron and Toshiba. Figure 8a,b show the CDF plot for the erase time for Micron and Toshiba respectively at different PE cycles. The experimental data shows that Micron and Toshiba recycled chips can be detected after 2.7% (Figure 8a) and 2% (Figure 8b) usage respectively. Figure 8c shows the usage vs. confidence level plot for Micron and Toshiba Flash chips. The results conclude that our proposed technique can detect whether a Flash memory is recycled or not with an acceptable confidence level. Table 1 shows more results and comparison from the major manufacturer.

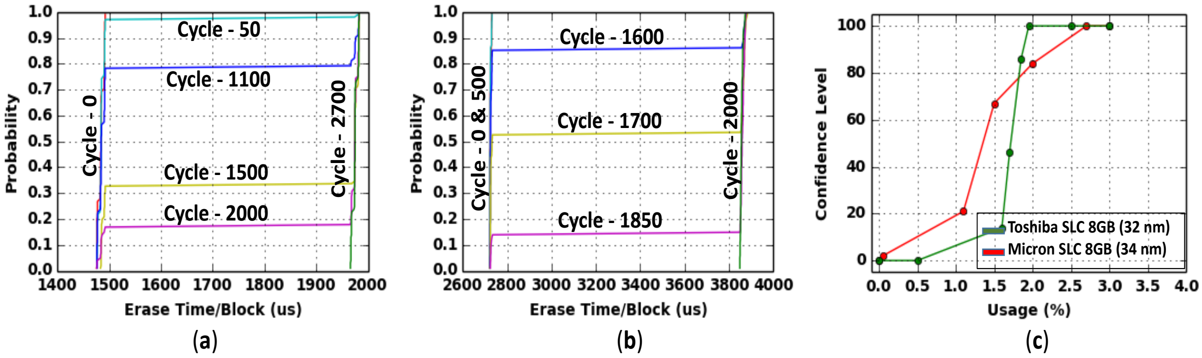

Figure 8. (**a**) CDF of erase time for PE cycle 0, 50, 1100, 1500, 2000 and 2700 for Micron 8GB SLC (34 nm). (**b**) CDF of erase time for PE cycle 0, 500, 1600, 1700, 1850 and 2000 for Toshiba 8GB SLC (32 nm). (**c**) The confidence level for the Flash chips from two manufacturers, Micron and Toshiba.

5.6. Validation on SLC and MLC Flash Chips

We applied our proposed method on both SLC and MLC Flash types from the same manufacturer. Figure 9a,b shows the same trend for the erase operation (i.e., increase in erase time with the number of PE cycles). The erase time increasing rate is much faster in MLC Flash chip than the SLC Flash chip. From Figure 9, we can see that the SLC Flash chip can be identified after 2700 PE cycles, whereas the counterfeit MLC Flash chip requires only 70 PE cycles. The density of MLC is much higher than SLC because of MLC store two or more bits per cell, whereas SLC stores only one bit per cell. Also, the MLC Flash chip has a wider range of voltage, typically 0 V to 6 V, while the SLC has lower voltage range (0 V to 3 V). Hence, the MLC degrades faster and offer very early age detection compared to SLC.

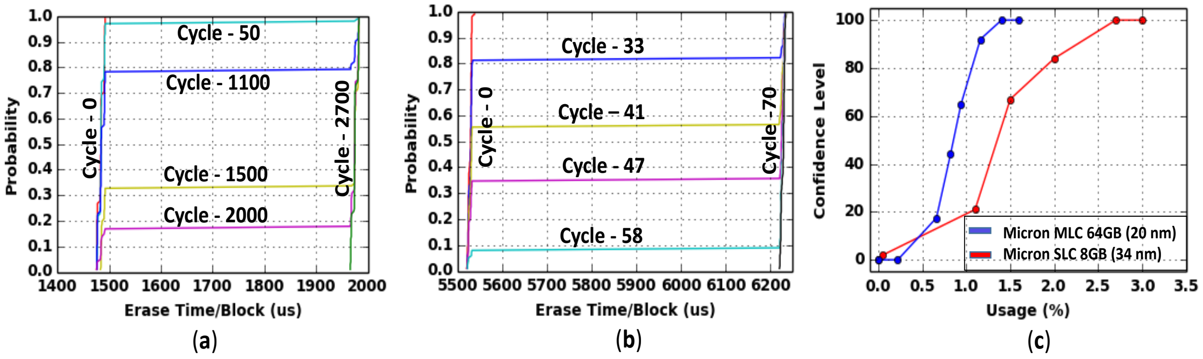

Figure 9. (**a**) CDF of erase time for PE cycle 0, 50, 1100, 1500, 2000 and 2700 for Micron 8GB SLC (34 nm). (**b**) CDF of erase time for PE cycle 0, 33, 41, 47, 58 and 70 for Micron 32GB MLC (20 nm). (**c**) The confidence level for two types Flash chips—SLC and MLC.

5.7. Usage vs. Confidence Level

Table 2 shows that the confidence level or the accuracy of detecting recycled Flash chips increases with usage. We can see the same trend for various Flash chips from different manufacturers, different technology nodes, types, etc. The results show that we cannot conclude whether the chip is recycled or not for all three vendors when the chips are used for 1% and 1.4% of their lifetime. However, vendor 1 and vendor 2 can be detected if the chip is used for 2% of their lifetime. We cannot make any conclusion for the 3rd vendor because the confidence level is not acceptable at 2% of usage. For usage of 2.7%, we can identify recycled chips for all three vendors. We can conclude that a recycled Flash chip can be detected with a better confidence level if that particular chip degrades faster.

Table 2. The confidence level for different types of Flash chips from various manufacturers.

Usage (%)	Confidence Level		
	Vendor 1	**Vendor 2**	**Vendor 3**
1%	Not Acceptable	Not Acceptable	Not Acceptable
1.4%	* Acceptable	Not Acceptable	Not Acceptable
2%	Acceptable	Acceptable	Not Acceptable
2.7%	Acceptable	Acceptable	Acceptable

* Acceptable (i.e., $\geq$98% confidence level).

Summary of results for the different type of Flash chips: Table 1, Figures 7–9 present the summary of results for the different type of Flash chips from various manufacturers of different technology nodes, types (SLC vs. MLC), and capacities. The results show that MLC Flash chips can be detected much earlier than SLC Flash chips from the same manufacturer. In general, the degradation of MLC chips is quicker than SLC because the operating voltage of MLC is higher. In another case, the Flash chips from different technology nodes from the same manufacturer degrade at different rates. The result shows that a Flash chip of lower technology node can be detected earlier than the older technology node. The reason for such trend is mostly due to the smaller size and lower gate oxide thickness of the memory cells in lower technology nodes. The results also conclude that the proposed detection methodology works for different manufacturers and recycled Flash chip can be detected with acceptable confidence level.

Summary of Results:

- Timing investigation ensures that erase time distribution can be applied for the detection of recycled and fresh Flash memory at acceptable accuracy.
- How early a Flash chip can be detected (i.e., the "usage") with acceptable confidence depends on manufacturers, technology nodes, memory types (SLC vs. MLC), and capacity.
- Among three Flash memory parameters, erase time is the best to identify a recycled Flash memory as early as possible (i.e., with minimal usage). Program time and FBC also demonstrate changes over time however not sufficient to use to identify a recycled Flash memory from fresh one with minimal usage.

Limitations and Scopes of Future Work:

- **Impact of Testing on Wear-out:** Our technique involves one erase operation per block, which have minimal impact on aging (typical erase count for a chip is $\sim$100,000).
- **Test Time:** Testing the entire chip can take a few seconds because a typical erase operation take 1 to 10 milliseconds per block and a chip can contain more than 1000 blocks.
- **Temperature Effect:** Our methodology works for all different temperatures; however, the exact detection threshold depends on the operating temperature.

6. Conclusions

Recycled or used Flash memory in the complex electronic component supply chain increases the security and reliability concerns and puts the innovation, health, and safety of consumers worldwide at risk. In this paper, we proposed a non-invasive detection technique to distinguish between a counterfeit and fresh Flash memory with the help of Flash array parameters such as erase time, program time, fail bit counts, etc. We validated our proposed methodology with the experimental results with high accuracy and without requiring any database maintenance. We find that the minimum detectable usage depends on the manufacturers, technology nodes, types (SLC vs. MLC), and capacity. Our proposed methodology is inexpensive, non-destructive, and does not require any hardware modification or maintenance of extensive database apart from the standard product data-sheet.

Author Contributions: Conceptualization and Methodology, B.R., S.S. and P.K.; Investigation and Data Analysis, S.S., P.K. and B.M.S.B.T.; Writing—Original Draft Preparation, M.T.R., B.R. and S.S.; Writing—Review & Editing, M.T.R. and B.R.

Funding: : This research received no external funding

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Karri, R; Koushanfar, F. Trustworthy Hardware [Scanning the Issue]. *Proc. IEEE* **2014**, *102*, 1123–1125.
2. Fern, N.; San, I.; Koç, Ç.K.; Cheng, K.T.T. Hiding Hardware Trojan Communication Channels in Partially Specified SoC Bus Functionality. *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.* **2017**, *36*, 1435–1444.
3. Our E-Waste Problem Is Ridiculous, and Gadget Makers Aren't Helping. 2012. Available online: https://www.wired.com/2014/12/product-design-and-recycling/ (accessed on 23 January 2018).
4. Sinanoglu, O.; Karimi, N.; Rajendran, J.; Karri, R.; Jin, Y.; Huang, K.; Makris, Y. Reconciling the IC test and security dichotomy. In Proceedings of the 2013 18th IEEE European Test Symposium (ETS), Avignon, France, 27–30 May, 2013; pp. 1–6.
5. Guin, U.; Huang, K.; DiMase, D.; Carulli, J.M.; Tehranipoor, M.; Makris, Y. Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain. *Proc. IEEE* **2014**, *102*, 1207–1228.
6. Kumari, P.; Talukder, B.M.S.B.; Sakib, S.; Ray, B.; Rahman, M.T. Independent detection of recycled flash memory: Challenges and solutions. In Proceedings of the 2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), Washington, DC, USA, 30 April–4 May 2018; pp. 89–95.
7. Guo, Z.; Xu, X.; Tehranipoor, M.M.; Forte, D. FFD: A Framework for Fake Flash Detection. In *Proceedings of the 54th Annual Design Automation Conference 2017 (DAC '17)*; ACM: New York, NY, USA, 2017; p. 8.
8. "Global Report – eBay Fake Memory 2008 – 2009," Fake Flash Memory Information - FlashChipDirector, 10-Jan-2010. Available online: https://flashfakecentral.wordpress.com/2010/01/10/global-report-ebay-fake-memory-2008-2009/ (accessed on 23 January 2018).
9. "Fake Flash News - Internet & eBay Fraud," Fake Flash News - Internet & eBay Fraud. Available: https://fakeflashnews.wordpress.com/ (accessed on 29 Jul 2018).
10. "Fake and counterfeit USB flash drives spreading on Amazon," Myce.com. Available online: https://www.myce.com/news/fake-and-counterfeit-usb-flash-drives-spreading-on-amazon-72165/ (accessed on 18 June 2018).
11. "Feds close huge chip counterfeiting case (exclusive)," VentureBeat, 25-Sep-2011. Available online: https://venturebeat.com/2011/09/25/feds-close-the-books-on-a-huge-chip-counterfeiting-scheme/ (accessed on 29 July 2018).
12. "Report A Fake," SOSFakeFlash, 10-May-2010. Available online: https://sosfakeflash.wordpress.com/report-a-fake/ (accessed on 18 June 2018).
13. Samarin, P.; Lemke-Rust, K. Detection of counterfeit ICs using public identification sequences. In Proceedings of the 2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), McLean, VA, USA, 1–5 May 2017; pp. 163–163.
14. Liu, M.; Kim, C.H. A powerless and non-volatile counterfeit IC detection sensor in a standard logic process based on an exposed floating-gate array. In Proceedings of the 2017 Symposium on VLSI Technology, Kyoto, Japan, 5–7 June 2017; pp. T102–T103.
15. He, K.; Huang, X.; Tan, S.X.D. EM-Based On-Chip Aging Sensor for Detection of Recycled ICs. *IEEE Des. Test* **2016**, *33*, 56–64.
16. Alam, M.; Chowdhury, S.; Tehranipoor, M.M.; Guin, U. Robust, Low-Cost, and Accurate Detection of Recycled ICs using Digital Signatures. In Proceedings of the 2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), Washington, DC, USA, 30 April–4 May 2018; pp. 209–214.

17. Guin, U.; Zhang, X.; Forte, D.; Tehranipoor, M. Low-cost On-Chip Structures for Combating Die and IC Recycling. In Proceedings of the 2014 51st ACM/EDAC/IEEE Design Automation Conference (DAC), San Francisco, CA, USA, 2–5 June 2014; pp. 1–6.
18. Lin; C.W.; Ghosh, S. Novel self-calibrating recycling sensor using Schmitt-Trigger and voltage boosting for fine-grained detection. In Proceedings of the Sixteenth International Symposium on Quality Electronic Design, Santa Clara, CA, USA, 2–4 March 2015; pp. 465–469.
19. Shahbazmohamadi, S.; Forte, D.; Tehranipoor, M. Advanced Physical Inspection Methods for Counterfeit IC Detection. In Proceedings of the 40th International Symposium for Testing and Failure Analysis (ISTFA), Houston, TX, USA, 9–13 November 2014; pp. 55-64.
20. Ahi, K.; Asadizanjani, N.; Shahbazmohamadi, S.; Tehranipoor, M.; Anwar, M. Terahertz characterization of electronic components and comparison of terahertz imaging with x-ray imaging techniques. In *Terahertz Physics, Devices, and Systems IX: Advanced Applications in Industry and Defense*; SPIE: Bellingham, WA, USA, 2015; Volume 9483; p. 94830K.
21. Hu, B.B.; Nuss, M.C. Imaging with terahertz waves. *Optics Letters* **1995**, *20*, 1716–1718.
22. Bushnell, M.; Agrawal, V.D. *Essentials of Electronic Testing for Digital, Memory and Mixed-Signal VLSI Circuits*; Springer: New York, NY, USA, 2002.
23. Guin, U.; Forte, D.; Tehranipoor, M. Design of Accurate Low-Cost On-Chip Structures for Protecting Integrated Circuits Against Recycling. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2016**, *24*, 1233–1246.
24. Guin, U.; DiMase, D.; Tehranipoor, M. A Comprehensive Framework for Counterfeit Defect Coverage Analysis and Detection Assessment. *J. Electron. Test.* **2014**, *30*, 25–40.
25. Galey, J.M.; Norby, R.E.; Roth, J.P. Techniques for the diagnosis of switching circuit failures. *IEEE Trans. Commun. Electron.* **1964**, *83*, 509–514.
26. Koushanfar, F. Can EDA Combat the Rise of Electronic Counterfeiting? In Proceedings of the 49th Annual Design Automation Conference, New York, NY, USA, 3–7 June 2012; pp. 133–138.
27. Kahng, A.B.; Kirovski, D.; Mantik, S.; Potkonjak, M.; Wong, J.L. Copy Detection for Intellectual Property Protec-tion of VLSI Designs. In Proceedings of the 1999 IEEE/ACM International Conference on Computer-aided Design, Piscataway, NJ, USA, 7–11 November 1999; pp. 600–605.
28. Wei, S.; Meguerdichian, S.; Potkonjak, M. Gate-level Characterization: Foundations and Hardware Security Applications. In Proceedings of the 47th Design Automation Conference, New York, NY, USA, 13–18 June 2010; pp. 222–227.
29. Wei, S.; Nahapetian, A.; Potkonjak, M. Robust Passive Hardware Metering. In *Proceedings of the International Conference on Computer-Aided Design*; IEEE Press: Piscataway, NJ, USA, 2011; pp. 802–809.
30. Ye, Y.; Kim, T.; Chen, H.; Wang, H.; Tlelo-Cuautle, E.; Tan, S.X.D. Comprehensive detection of counterfeit ICs via on-chip sensor and post-fabrication authentication policy. In Proceedings of the 2017 14th International Conference on Synthesis, Modeling, Analysis and Simulation Methods and Applications to Circuit Design (SMACD), Giardini Naxos, Italy, 12–15 June 2017; pp. 1–4.
31. Kim, T.H.; Persaud, R.; Kim, C.H. Silicon Odometer: An On-Chip Reliability Monitor for Measuring Frequency Degradation of Digital Circuits. *IEEE J. Solid-State Circuits* **2008**, *43*, 874–880.
32. Karl, E.; Singh P.; Blaauw, D.; Sylvester, D. Compact In-Situ Sensors for Monitoring Negative-Bias-Temperature-Instability Effect and Oxide Degradation. In Proceedings of the 2008 IEEE International Solid-State Circuits Conference—Digest of Technical Papers, San Francisco, CA, USA, 3–7 February 2008; pp. 410–623.
33. Kim, K.K.; Wang, W.; Choi, K. On-Chip Aging Sensor Circuits for Reliable Nanometer MOSFET Digital Circuits. *IEEE Trans. Circuits Syst. II Express Briefs* **2010**, *57*, 798–802.
34. Dogan, H.; Forte, D.; Tehranipoor, M.M. Aging Analysis for Recycled FPGA Detection. In Proceedings of the 2014 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), Amsterdam, The Netherlands, 1–3 October 2014; pp. 171–176.
35. Zhang, X.; Xiao, K.; Tehranipoor, M. Path-delay fingerprinting for identification of recovered ICs. In Proceedings of the 2012 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), Austin, TX, USA, 3–5 October 2012; pp. 13–18.
36. Guo, Z.; Rahman, M.T.; Tehranipoor, M.M.; Forte, D. A zero-cost approach to detect recycled SoC chips using embedded SRAM. In Proceedings of the 2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), McLean, VA, USA, 3–5 May 2016; pp. 191–196.

37. Guo, Z.; Xu, X.; Rahman, M.T.; Tehranipoor, M.M.; Forte, D. SCARe: An SRAM-Based Countermeasure Against IC Recycling. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2018**, *26*, 744–755.
38. Rahman, M.T. Systematic Correlation and Cell Neighborhood Analysis of SRAM PUF for Robust and Unique Key Generation. *J. Hardw. Syst. Secur.* **2017**, *1*, 137–155.
39. Tehranipoor, M.; Guin, U.; Forte, D. *Counterfeit Integrated Circuits: Detection and Avoidance*, 1st ed.; Springer: Berlin, Germany, 2015.
40. Ray, B.; Milenkovic, A. True Random Number Generation Using Read Noise of Flash Memory Cells. *IEEE Trans. Electron Devices* **2018**, *65*, 963–969.