Flash-DNA: Identifying NAND Flash Memory Origins Using Intrinsic Array Properties

Sadman Sakib, *Graduate Student Member, IEEE*, Aleksandar Milenković, *Senior Member, IEEE*, and Biswajit Ray, *Senior Member, IEEE*

***Abstract*— Counterfeit electronics entering the globalized supply chain are a growing problem impacting manufacturers and consumers alike. This article introduces Flash-DNA, a new technique for identifying the original chip manufacturer of NAND flash memory, which will help preventing the proliferation of rebranded or cloned flash memory chips. Flash-DNA relies on extracting intrinsic variations in NAND arrays using a partial block erase operation. Our experimental evaluation, conducted on multiple memory chips from four major manufacturers, shows that Flash-DNA captures fundamental properties of the manufacturing process, providing a unique identifier for a family of NAND flash memory chips that can be used for tracing their origins.**

***Index Terms*— Counterfeiting, flash-DNA, Flash memories, foundry identification.**

I. Introduction

COUNTERFEIT electronics entering the globalized semiconductor supply chain have become a source of significant concern for both manufacturers and consumers. Recycled, rebranded, over-produced, defective, cloned, or tempered with integrated circuits (ICs) can enter the supply chain, and thus end up in a variety of products, from low-end consumer gadgets to mission-critical systems used in transportation, finance, healthcare, and military applications [1]. For example, reports of counterfeit ICs in the supply chain quadrupled from 2009 to 2011 [2]. Sales of counterfeit parts result in substantial economic losses to the semiconductor industry, reportedly as high as U.S. $7.5 billion per year for U.S.-based companies alone [3].

Flash memory chips have become one of the primary targets of counterfeiters [4]. There are multiple pathways for counterfeit flash memory chips to enter the supply chain. First, the flash chips in electronic gadgets in most cases remain functional even after the end of the product lifecycle. This provides an opportunity for counterfeiters to retrieve the used flash memory chips from the printed circuit boards and sell them as new for higher prices. Second, the rejected dies or the fall-out chips that fail postfabrication tests can enter the supply chain through counterfeiters having access to the chip packaging sites, which are located in various countries. Even though the flash foundry marks some of the dies as rejected during die-sort testing, those dies can re-enter the supply chain through counterfeiters. Third, the counterfeiters may buy inferior flash chips from less reputed manufacturers and sell them for a higher price by rebranding the chip packaging. Finally, counterfeiters with access to foundry facilities can manufacture cloned flash memory chips. The use of inferior or defective counterfeit nonvolatile flash memories results not only in economic losses for the original chip manufacturers, but also in the failures of end-user applications, ranging from a loss of data and premature end-of-life to more serious catastrophic events.

The existing approaches for tracing the origins of flash memory chips can be easily circumvented by motivated and resolute counterfeiters. For example, flash memory chip manufacturers typically store the chip identity information (the lot and wafer number, manufacturer ID, and date) in a dedicated memory block of the die. Unfortunately, counterfeiters can erase and reprogram all this information once they get physical access to the chip. Hence several research groups have recently proposed flash memory-based physical unclonable functions (PUFs) [5]–[9] to track the memory origins. Unfortunately, a PUF-based chip authentication requires detailed characterizations of individual chips and maintenance of large databases with an entry for each manufactured flash memory chip, which is cumbersome and not a common practice in the industry. Thus, developing a cost-effective technique for tracing the origins of flash memory chips remains a significant challenge.

This article introduces Flash-DNA, a technique for securing global supply chains of nonvolatile NAND flash memory chips by using systematic variations in the properties of NAND arrays that are fundamentally related to the specific manufacturing process [10], [11]. The systematic variations within the array are usually unique for a given family of memory chips as these variations often originate from the unique nature of the underlying fabrication process. In other words, the chips manufactured from a given foundry will

Manuscript received March 30, 2021; revised May 20, 2021; accepted May 31, 2021. Date of publication June 17, 2021; date of current version July 23, 2021. This work was supported by the National Science Foundation under Grant 1929099 and Grant 2007403. The review of this article was arranged by Editor P. Narayanan. *(Corresponding author: Sadman Sakib.)*

The authors are with the Department of Electrical and Computer Engineering, The University of Alabama in Huntsville, Huntsville, AL 35899 USA (e-mail: sadman.sakib@uah.edu; milenka@uah.edu; biswajit.ray@uah.edu).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TED.2021.3087454.

Digital Object Identifier 10.1109/TED.2021.3087454

share the same variation patterns, or family traits, that are different from family traits of chips that come from different foundries/manufacturers. In this article, we utilize these flash memory family traits to identify the origins of NAND memory chips, thus the name of the proposed technique: Flash-DNA.

Flash-DNA relies on extracting variations in the physical properties among the pages of a flash memory block using partial erase operations. We find that erase efficiency varies significantly among different pages of a NAND flash block. These variations create a pattern that is unique for a given family of chips and differs significantly from patterns observed in chips from other manufacturers. We have performed an extensive experimental evaluation on a dozen of NAND flash memory chips from four major manufactures to confirm the robustness of our technique. We use the Pearson's correlation coefficient, r, to quantify the similarity of extracted pairs of Flash-DNA. The experimental evaluation shows a very high correlation ($r > 0.9$) of the Flash-DNAs extracted from the same family of chips and significantly lower correlation ($r < 0.5$) between pairs of Flash-DNAs belonging to different families.

Flash-DNA addresses many of the limitations of existing anticounterfeiting methods. For example, extraction of Flash-DNA can be done in the flash controller firmware using standard flash interface commands. Consequently, it can be fully automated without any manual intervention. Second, Flash-DNA does not require any extra hardware (e.g., antifuse memory) or modification to the chip design/fabrication process. Thus, the method is universally applicable to all flash memory chips irrespective of the manufacturer. Third, unlike PUF-based anticounterfeit methods, the proposed method does not require maintenance of large, chip-specific databases at the manufacturing sites, nor do system integrators need to contact the original chip manufacturer to verify the authenticity of each chip. Since the method fundamentally relies on systematic process variations inherent to the NAND array due to the idiosyncrasy of the specific foundry, the presence of a correct signature in chips will guarantee their authenticity to the system integrators.

The rest of this article is organized as follows. Section II gives a brief summary of related research work. Section III gives NAND flash memory preliminaries. Section IV describes our characterization method and extraction of physical properties of NAND arrays through a standard digital interface. Section V describes the proposed chip family identification scheme. Section VI describes the results of the experimental evaluation, and Section VII concludes this article.

II. Related Research

Most of the recently proposed techniques for counterfeit IC detection rely on physical and electrical inspection tests using high-tech imaging solutions and parametric/functionality tests [1]. These techniques require costly imaging instruments and rigorous analysis by an expert. In many cases, these techniques are invasive and suffer from limited effectiveness. Another approach for tracing ICs is to use electronic chip identifiers (ECIDs) programmed into antifuse or one-time-programmable memory [12]. Unfortunately, ECIDs are not common in flash memory chips; in addition, they require dedicated on-chip resources and changes to the physical chip masks. Yet another class of techniques relies on deriving PUFs that are unique for each chip [5]–[9]. However, the use of PUFs for the detection of counterfeits requires a lengthy PUF extraction as well as maintenance of large databases with entries for every manufactured chip. In addition, PUF-based chip authentication requires a method for contacting the chip manufacturer to verify the authenticity of each chip, which may place an additional burden on system integrators, increasing the time and cost of chip verification. Recently, a few techniques have been introduced that specifically target detection of recycled flash memory chips in the supply chain [4], [13]. Whereas these techniques can detect recycled flash memory chips, they may not be readily applied to detect other types of counterfeiting.

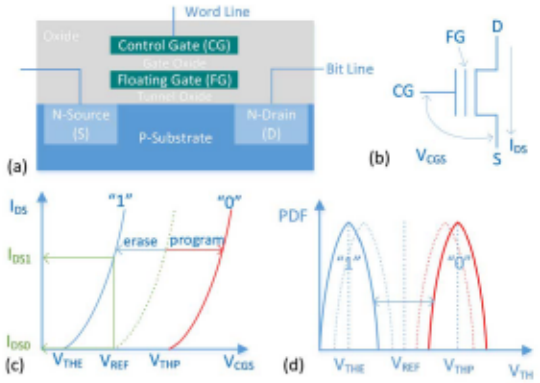

Fig. 1. (a) Cross section of a floating gate flash memory cell. (b) Symbol of FG-MOSFET. (c) I–V characteristics of FG-MOSFET. (d) Threshold voltage (V_{TH}) distribution of erased and programmed states.

There have been a few research efforts targeting IC foundry identification [14], [15]. Wendt *et al.* [14] propose extracting the distributions of channel lengths and threshold voltages after employing a variant of the Boolean satisfiability problem. Helinski *et al.* [15] manufactured a number of test ICs with on-chip circuitry that extracts variations of main device parameters for resistors, capacitors, and oscillators. Whereas the first article offers a purely theoretical framework, the latter presents a feasibility study on a limited subset of basic devices. Talukder *et al.* [16] proposed a machine learning approach to identify the DRAM and SRAM origins. Their technique requires detailed characterization data with 26 features to train a statistical one-class classifier that is then used to identify chips origins. To the best of our knowledge, our work is the first that proposes and demonstrates a technique for identifying chip origins on COTS NAND flash memories.

III. NAND Flash Memory Preliminaries

Fig. 1(a) shows the structure of a flash memory cell, essentially a floating gate (FG) metal oxide semiconductor field-effect transistor (MOSFET), fabricated using a planar

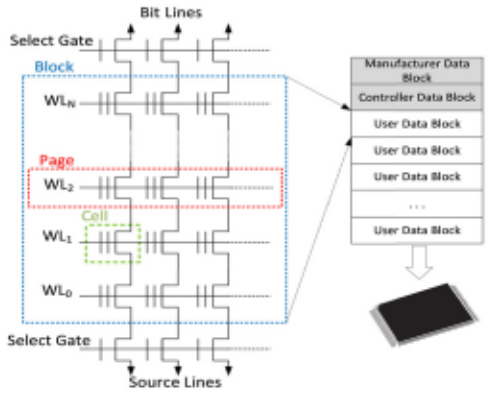

Fig. 2. NAND flash memory organization, and block diagram of a NAND flash memory chip.

process. The FG is electrically insulated from the terminals [Fig. 1(b)] and can trap charge that stays on it even when the power is turned off. The trapped negative charge effectively increases the transistor's threshold voltage ($V_{\mathrm{TH}}V_{\mathrm{TH}}$) relative to the case when there is no charge on the FG. Thus, a flash memory cell is a charge-based analog memory. The program operation charges the FG with electrons via Fowler–Nordheim tunneling, whereas the erase operation removes the charges from the FG.

A flash memory cell read operation involves applying a read voltage on the control gate (V_{REF}) and sensing the cell V_{TH} as shown in Fig. 1(c). An erased cell conducts the current, which is sensed as a logic "1," whereas a programmed cell does not conduct the current, which is sensed as a logic "0." The read reference voltage (V_{REF}) is set in between the erased and programmed state distributions, so that there is enough of a noise margin to correctly identify the cell states as shown in Fig. 1(d). Traditional flash memory cells, a.k.a. SLCs or single-level cells, store one bit of information. Recent advances [17] in controlling and sensing different levels of charge on the FG allow for flash memory cells that can store two bits of information (MLC—multilevel cell), three bits (TLC—triple-level cell), or even four bits (QLC—quad-level cell).

A NAND flash memory block is organized as a 2-D array of memory cells, as shown in Fig. 2. Cells in a row constitute a page, and their control gates are connected to a shared word line (WL). The page size varies from 2 to 16 KB depending on the manufacturer. A collection of pages forms a flash memory block. A flash memory chip typically includes multiple blocks. The cells in a vertical column are connected to a metal bit line (BL) at one end and to the ground at the other end. Thus, a BL can be pulled down to the ground only if all cells in the column are active (resembling the operation of the NAND gate). The NAND architecture means that data are read or programmed at the page level, whereas erase operations are performed at the block level. Any flash cell that is set to a logic "0" by a program operation can only be reset to a logic "1" by erasing the entire block. Thus, to change the content of a flash memory page, the new content should be programmed into a new, previously erased page.

IV. Characterizing Systematic Variation in NAND Array using Partial Erase

Exploring the physical properties of a NAND array using digital interfaces is not straightforward, because COTS flash memory chips come with a fixed command set and chip-interfacing protocol defined by Open NAND Flash Interface (ONFI) [18]. The key ONFI commands are block erase, page program, and page read, all providing digital-only information. The bit error rate (BER), or the number of flipped bits, is the only readily accessible quantity to characterize the variability within the array. However, a NAND flash memory shows a very low BER, usually zero per page for an SLC memory, right after programming. Thus, it is quite challenging to design a noninvasive, easily accessible characterization tool that can be used by system integrators for identifying foundry-specific systematic variability.

In this work, we show that the page-to-page variability of the erase efficiency after a partial erase operation provides a unique signature of the foundry-specific traits. A full block erase operation in a NAND flash memory typically takes from 1 to 10 ms, depending on the chip type. A block erase operation can be prematurely terminated using a RESET command, and this process is usually called a partial erase operation. The partial erase operation leaves the memory block in a nondeterministic state, where certain bits are read as logic-1s and others are read as logic-0s. The nondeterministic state of the memory block reveals the page-to-page variability in the erase efficiency defined by the number of erased bits expressed as a percentage of the total number of bits in a page. Mathematically, the erase efficiency of a page with index n, P_n, for a given partial erase time, t^p_{ers}, is defined as follows:

$$\eta_{\mathrm{ers}}\left(Pn, t^p_{\mathrm{ers}}\right) = \frac{\#\ \text{oferased bits in}\ Pn}{\text{page size}} \times 100\%. \qquad (1)$$

After a full block erase operation, all the pages will have $\eta_{\mathrm{ers}} = 100\%$. However, a partial erase operation will lead to differentiation of pages within a block to those with higher or lower erase efficiency.

Fig. 3(a) illustrates a partial erase operation. The solid black line represents the status of the R/B pin of the NAND chip during a regular block erase operation. The pin is low when the memory chip is busy performing an erase operation that typically takes between 1 and 10 ms (t_{ers}). The partial erase operation is implemented by issuing a RESET command after the BLOCK ERASE command; it terminates the erase operation prematurely as illustrated with red dashed line in Fig. 3(a). The exact command sequence for implementing the partial erase operation is given in Fig. 3(b). The partial erase time (t^p_{ers}) can be controlled by the time delay (t_d) parameter from the host as illustrated in line 3 of the command sequence. Usually, $t^p_{\mathrm{ers}} > t_d$ because of the fixed overhead introduced by the setup. We monitor the R/B pin status to measure the t^p_{ers} during the partial erase operation. If t_d is too short, $\eta_{\mathrm{ers}} \approx 0$, whereas a longer t_d results in $\eta_{\mathrm{ers}} \approx 100\%$ for all pages in a block. It is thus important to recognize that there is a specific transition time window suitable for partial erase characterization.

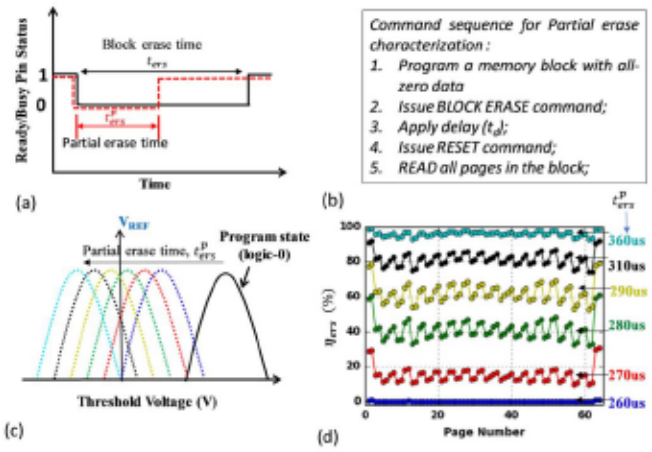

Fig. 3. (a) Illustration of partial erase operation through R/B pin status of the NAND chip. (b) Command sequence for implementing partial erase operation on an ONFI-complaint NAND chip. (c) Threshold voltage distribution as a function of t^p_{ers}. (d) Erase efficiency (η_{ers}) on different memory pages after partial erase operation.

Fig. 3(c) shows the threshold voltage distribution as a function of the partial erase time. The programmed state is represented with solid black line. If a partial erase operation is performed on the array the distribution shifts toward the left as shown with dotted lines in the figure. Longer the partial erase time, higher is the shift in the resulting distribution. The memory bits with $V_{TH} < V_{REF}$ are read as erase bits whereas the bits with $V_{TH} > V_{REF}$ are read as program bits. The cells that cross V_{REF} earlier are called fast erase bits and the cells that cross V_{REF} later are called slow erase bits. Fig. 3(d) shows the erase efficiency for individual pages (0–63) in a block as a function of t^p_{ers} on a 4-Gb SLC NAND memory chip from Toshiba. We show the partial erase results in the following transition time window: 260 μs $< t^p_{ers} <$ 360 μs since $\eta_{ers} \approx 0\%$ for $t^p_{ers} <$ 260 μs and $\eta_{ers} \approx 100\%$ for $t^p_{ers} >$ 360 μs for all pages of a block in this particular chip. More importantly, we find that η_{ers} values for pages within a block create a fixed pattern. Even though the absolute values of η_{ers} increase with an increase in the partial erase time, the page-dependent η_{ers} pattern of a memory block remains the same, as long as the partial erase time lies within the transition window. The transition window varies among chips from different manufacturers and needs to be determined experimentally. It can be formally determined for a given family of chips by defining the bounds for the average block erase efficiency, e.g., $20\% < \eta_{ers} < 80\%$. In the remainder of the article, we use the term Flash-DNA to refer to the page-by-page η_{ers} pattern extracted after a partial erase operation of a memory block.

V. Proposed Chip Identification Scheme

The proposed technique for extracting Flash-DNA is performed by system integrators to identify origins of NAND flash memory chips. It relies on extracting the η_{ers} pattern from a random sample of memory chips using the process described in Section IV. The extracted Flash-DNA is then compared to the original Flash-DNA that is provided by the chip manufacturer. A high similarity between the DNAs is accepted as a proof of chip origins.

In order to quantify the similarity of two Flash-DNAs, we use Pearson's correlation coefficient (r). A high value of correlation coefficient ($r > 0.9$) indicates that DNAs are similar, whereas a low value of r (<0.5) indicates a mismatch between two DNAs. Thus, to ensure its effectiveness, the proposed Flash-DNA-based chip identification scheme relies on the following assumptions.

1) Flash-DNA needs to be a robust signature representing a given family, i.e., Flash-DNAs extracted from the same family of chips from a single manufacturer should be similar to each other.
2) Flash-DNA needs to be unique, i.e., Flash-DNAs extracted from similar chips fabricated by different manufacturers should be different from each other.
3) Flash-DNA needs to be unique per technology node, i.e., Flash-DNAs extracted from chips produced by a single manufacturer using different technology nodes and/or fabrication processes should be different from each other.

In Section VI, we will evaluate these assumptions by extensive experimental evaluation.

TABLE I
DETAILS OF THE EVALUATED NAND FLASH MEMORY CHIPS

Manufacturer	Part number	Page details	Block erase time (μs)	Partial erase time (μs)
Toshiba 4Gb SLC (32 nm node)	TC58NVG2S0FTA 00-ND	Pages per block: 64 Page size: 4096 byte	3000	285
Toshiba 4Gb SLC (43 nm node)	TC58NVG2S3ETA 00-ND	Pages per block: 64 Page size: 2048 byte	2500	270
Micron 8Gb SLC (25 nm node)	MT29F8G08ABA CAWP:C	Pages per block: 64 Page size: 4096 byte	2000	435
Samsung 2Gb SLC (32 nm node)	K9F2G08U0A:PC B0	Pages per block: 64 Page size: 2048 byte	1500	418
Hynix 4Gb SLC	H27UF084G2M	Pages per block: 64 Page size: 4096 byte	2000	316

VI. Experimental Evaluation

The experimental evaluation is performed on several 2-D NAND SLC chips from four major NAND manufacturers—Toshiba, Micron, Samsung, and Hynix. Table I summarizes part numbers and other relevant parameters for the selected flash memories. Please note that it may be possible to identify the original manufacturer based on several generic features of the chip such as page size, number of pages per block, number of blocks per chip, and timing characteristics of the memory. However, the goal of the article is to introduce a technique for tracing NAND flash memory origins by exploiting inherent array properties that a counterfeiter cannot copy, even if they try to emulate the exact features of a chip. With this goal, we chose chips with features as close to each other as possible. For example, all the chips have the

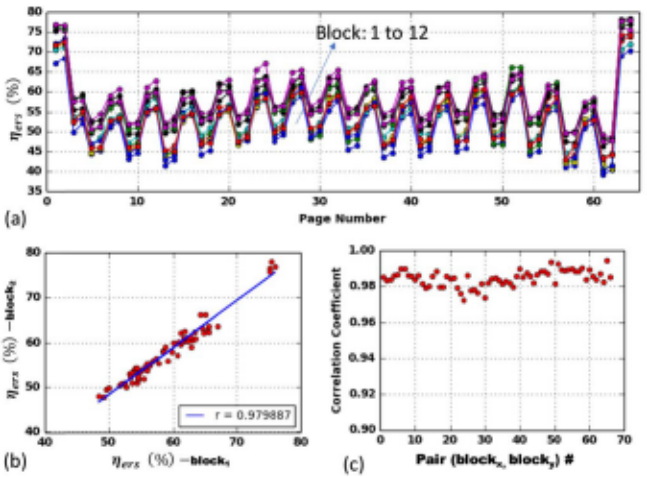

Fig. 4. (a) Flash-DNAs or η_{ers} patterns for 12 different blocks of a NAND chip for $t^p_{ers} = 285\ \mu s$. (b) Page-by-page correlation of η_{ers} patterns for two different memory blocks primed by a fixed partial erase time. (c) Pair-wise correlation coefficient between η_{ers} patterns for 12 different memory blocks from the same chip.

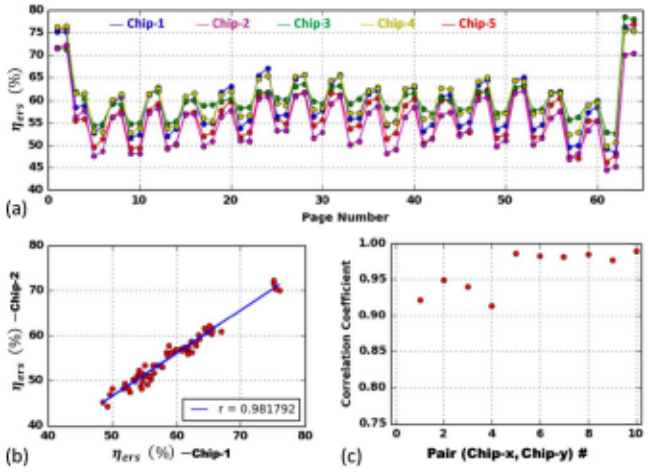

Fig. 5. (a) Flash-DNAs or η_{ers} patterns for five different NAND chips of the same family. (b) Page-by-page correlation plot between η_{ers} pattern. (c) Correlation coefficient for each pair of chips.

same number of pages in a block, similar page sizes, and bit-densities.

A. Evaluation of the Robustness of Flash-DNA

We start our evaluation by analyzing the Flash-DNAs for different memory blocks of the same chip. Fig. 4(a) illustrates the DNAs for 12 different memory blocks within a single chip, while keeping a fixed partial erase time ($t^p_{ers} = 285\ \mu s$). We observe that the block-to-block variations of the DNAs are minimal, that is, the η_{ers} pattern remains the same for all memory blocks within a chip. Fig. 4(b) shows a strong correlation between the DNAs belonging to two different memory blocks ($block_1$ and $block_2$) within a single chip. However, the most important and interesting observation is a very high correlation coefficient between DNAs from two different blocks ($r \approx 0.98$). Fig. 4(c) summarizes the pair-wise correlation coefficients for 12 memory blocks with 66 data points. All correlation coefficients are larger than 0.95, indicating that Flash-DNA is a robust and invariant property of the entire chip, i.e., the extracted Flash-DNA is not a function of the block index.

Next, we characterize the Flash-DNAs extracted from five different 4-Gb Toshiba memory chips having the same part number. Fig. 5(a) shows the extracted DNAs for five sample memory chips. First, we observe a chip-to-chip variability in the absolute η_{ers} values obtained for $t^p_{ers} = 285\ \mu s$. Such variability is common for NAND flash memory chips due to process variations. Interestingly, however, the extracted Flash-DNAs exhibit the same pattern. Fig. 5(b) shows the page-by-page correlation for randomly selected blocks from different chips. The plot shows a high correlation between Flash-DNAs extracted from two chips ($r \approx 0.98$). Fig. 5(c) summarizes correlation coefficients for all 10 pairs of chips. The plot quantitatively confirms a high similarity of Flash-DNAs extracted from different chips within the same family ($r > 0.92$).

B. Evaluation of the Uniqueness of Flash-DNA

To evaluate the uniqueness of Flash-DNA, we extract them from a population that includes four major NAND flash manufacturers, each family with three sample chips. Fig. 6 gives a graphical illustration of Flash-DNAs for all four families. The chips within a family have similar DNAs, whereas chips from different families do not. For example, Hynix SLC chips show a unique wave-like η_{ers} pattern, distinct from the other manufacturers. Similarly, Samsung chips have the lowest erase efficiency for edge pages, which is opposite to the Toshiba and Micron chips. In general, the odd and even pages of the Hynix and Micron chips show a zig-zag pattern, which is very different from the patterns observed for the Toshiba and Samsung chips that show the zig-zag only on consecutive pairs of pages. Since these features of the η_{ers} pattern are common among all the chips within the same family, we believe that they are fundamentally related to the array structure and the underlying fabrication processes.

Even though a visual inspection of the Flash-DNAs in Fig. 6 indicates their uniqueness, we quantify the dissimilarity by performing pair-wise correlation across 12 chips. Fig. 7 shows the correlation coefficients for all 66 pairs of chips. We exclude the first two and the last two pages from the calculation because those pages skew the correlation coefficient. The red points with higher r values in the figure represent correlation coefficients for Flash-DNA pairs from the same manufacturer, whereas the red points with lower r values represent the correlation coefficients of Flash-DNA pairs from different manufacturers. A significant gap between these two clusters indicates that Flash-DNA is a promising technique for identifying origins of flash memory chips.

Next, we evaluate the uniqueness of Flash-DNA based on the underlying technology node. Fig. 8 shows Flash-DNAs extracted from a pair of Toshiba flash memory chips that share the same array parameters (SLC, 4 Gb, identical organization),

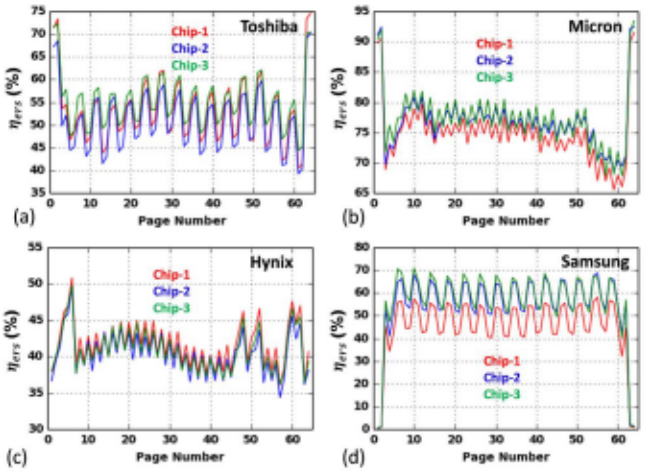

Fig. 6. Flash-DNAs (or η_{ers} pattern) extracted from four major NAND manufacturers. (a) Toshiba. (b) Micron. (c) Hynix. (d) Samsung.

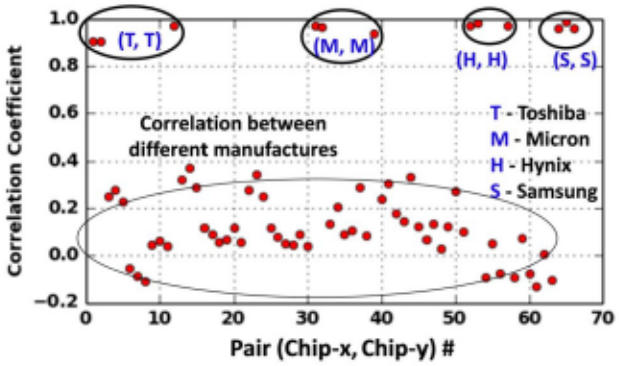

Fig. 7. Pair-wise correlation coefficients for the Flash-DNAs extracted from 12 different memory chips from four major NAND manufacturers.

but differ in the technology node used in their fabrication (32 versus 43 nm). Visual inspection indicates a sufficient difference in the Flash-DNAs that is also confirmed by the correlation coefficient ($r = 0.168038$).

C. Limitations

We acknowledge the fact that the conclusions made in this article are based on a relatively small sample size. A larger population size study would be more accurate but would require resources that may exceed capacity of a University research group. Although larger sample sizes may reduce the gap between the correlation coefficients of pairs of Flash-DNAs extracted from chips within a single family and pairs coming from different families, the results from Fig. 7 give us confidence in the proposed technique. Even though our experimental evaluation exclusively focuses on SLC memory chips, we believe the technique can be extended for other flash technologies, such as MLC, TLC, and QLC by choosing the appropriate page type for Flash-DNA extraction. However, the proposed technique needs to be extended to perhaps deal with the effects of the internal data randomizer typically employed in the advanced flash chips. In addition, we would like to mention that all our measurements are

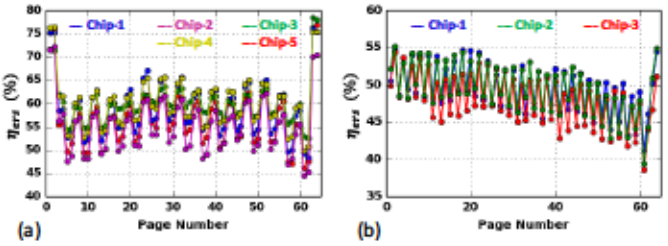

Fig. 8. Flash-DNAs extracted from a pair of Toshiba chips with two different technology nodes. (a) 32 nm. (b) 43 nm.

performed at room temperature. However, cross temperature issues will not alter the Flash-DNA shape as the relative erase efficiency between different pages should remain the same under different temperatures.

VII. Conclusion

This article describes Flash-DNA, a technique for extracting the fundamental array properties that are unique and robust for a given family of NAND flash memory chips. The technique relies on partial erase operations to enable extraction of page-to-page variation of erase efficiency. The technique is successfully demonstrated on a number of chips from four major flash memory manufactures. The experimental evaluation shows a very high correlation ($r > 0.9$) in the Flash-DNAs extracted from the same family of chips and significantly lower correlation ($r < 0.5$) in the Flash-DNAs extracted from chips belonging to different families.

References

[1] U. Guin, K. Huang, D. DiMase, J. M. Carulli, M. Tehranipoor, and Y. Makris, "Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain," *Proc. IEEE*, vol. 102, no. 8, pp. 1207–1228, Aug. 2014, doi: 10.1109/JPROC.2014.2332291.

[2] E. Products. (Feb. 14, 2012). *Reports of Counterfeit Parts Quadruple Since 2009, Challenging US Defense Industry and National Security*. Electronic Products. Accessed: Mar. 11, 2021. [Online]. Available: https://www.electronicproducts.com/reports-of-counterfeit-parts-quadruple-since-2009-challenging-us-defense-industry-and-national-security/

[3] M. Pecht and S. Tiku, "Bogus: Electronic manufacturing and consumers confront a rising tide of counterfeit electronics," *IEEE Spectr.*, vol. 43, no. 5, pp. 37–46, May 2006, doi: 10.1109/MSPEC.2006.1628506.

[4] S. Sakib, P. Kumari, B. Talukder, M. Rahman, and B. Ray, "Non-invasive detection method for recycled flash memory using timing characteristics," *Cryptography*, vol. 2, no. 3, p. 17, Aug. 2018, doi: 10.3390/cryptography2030017.

[5] Y. Wang, W.-K. Yu, S. Wu, G. Malysa, G. E. Suh, and E. C. Kan, "Flash memory for ubiquitous hardware security functions: True random number generation and device fingerprints," in *Proc. IEEE Symp. Secur. Privacy*, May 2012, pp. 33–47, doi: 10.1109/SP.2012.12.

[6] P. Prabhu *et al.*, "Extracting device fingerprints from flash memory by exploiting physical variations," in *Trust and Trustworthy Computing*. Berlin, Germany: Springer, Jun. 2011, pp. 188–201, doi: 10.1007/978-3-642-21599-5_14.

[7] M.-S. Kim, D.-I. Moon, S.-K. Yoo, S.-H. Lee, and Y.-K. Choi, "Investigation of physically unclonable functions using flash memory for integrated circuit authentication," *IEEE Trans. Nanotechnol.*, vol. 14, no. 2, pp. 384–389, Mar. 2015, doi: 10.1109/TNANO.2015.2397956.

[8] S. Sakib, A. Milenkovic, M. T. Rahman, and B. Ray, "An aging-resistant NAND flash memory physical unclonable function," *IEEE Trans. Electron Devices*, vol. 67, no. 3, pp. 937–943, Mar. 2020, doi: 10.1109/TED.2020.2968272.

[9] Z. Guo, X. Xu, M. M. Tehranipoor, and D. Forte, "FFD: A framework for fake flash detection," in *Proc. 54th Annu. Design Automat. Conf.*, Jun. 2017, pp. 1–6, doi: 10.1145/3061639.3062249.

[10] P.-Y. Wang and B.-Y. Tsui, "A novel approach using discrete grain-boundary traps to study the variability of 3-D vertical-gate NAND flash memory cells," *IEEE Trans. Electron Devices*, vol. 62, no. 8, pp. 2488–2493, Aug. 2015, doi: 10.1109/TED.2015.2438001.

[11] A. Spessot, C. M. Compagnoni, F. Farina, A. Calderoni, A. S. Spinelli, and P. Fantini, "Compact modeling of variability effects in nanoscale NAND flash memories," *IEEE Trans. Electron Devices*, vol. 58, no. 8, pp. 2302–2309, Aug. 2011, doi: 10.1109/TED.2011.2147319.

[12] N. Robson *et al.*, "Electrically programmable fuse (eFUSE): From memory redundancy to autonomic chips," in *Proc. IEEE Custom Integr. Circuits Conf.*, Sep. 2007, pp. 799–804, doi: 10.1109/CICC.2007.4405850.

[13] S. Sakib, A. Milenkovic, and B. Ray, "Flash watermark: An anti-counterfeiting technique for NAND flash memories," *IEEE Trans. Electron Devices*, vol. 67, no. 10, pp. 4172–4177, Oct. 2020, doi: 10.1109/TED.2020.3015451.

[14] J. B. Wendt, F. Koushanfar, and M. Potkonjak, "Techniques for foundry identification," in *Proc. 51st ACM/EDAC/IEEE Design Automat. Conf. (DAC)*, Jun. 2014, pp. 1–6, doi: 10.1145/2593069.2593228.

[15] R. L. Helinski, E. I. Cole, G. Robertson, J. Woodbridge, and L. G. Pierson, "Electronic forensic techniques for manufacturer attribution," in *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST)*, May 2016, pp. 139–144, doi: 10.1109/HST.2016.7495572.

[16] B. M. S. B. Talukder, V. Menon, B. Ray, T. Neal, and M. T. Rahman, "Towards the avoidance of counterfeit memory: Identifying the DRAM origin," in *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST)*, Dec. 2020, pp. 111–121, doi: 10.1109/HOST45689.2020.9300125.

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

[18] *Home—ONFI*. Accessed: Mar. 11, 2021. [Online]. Available: https://www.onfi.org/