

# A Non-invasive Technique to Detect Authentic/Counterfeit SRAM Chips

B. M. S. BAHAR TALUKDER, FARAH FERDAUS, and MD TAUHIDUR RAHMAN, Department of ECE, Florida International University, USA

Many commercially available memory chips are fabricated worldwide in untrusted facilities. Therefore, a counterfeit memory chip can easily enter into the supply chain in different formats. Deploying these counterfeit memory chips into an electronic system can severely affect security and reliability domains because of their sub-standard quality, poor performance, and shorter lifespan. Therefore, a proper solution is required to identify counterfeit memory chips before deploying them in mission-, safety-, and security-critical systems. However, a single solution to prevent counterfeiting is challenging due to the diversity of counterfeit types, sources, and refinement techniques. Besides, the chips can pass initial testing and still fail while being used in the system. Furthermore, existing solutions focus on detecting a single counterfeit type (e.g., detecting recycled memory chips). This work proposes a framework that detects major counterfeit static random-access memory (SRAM) types by attesting/identifying the origin of the manufacturer. The proposed technique generates a single signature for a manufacturer and does not require any exhaustive registration/authentication process. We validate our proposed technique using 345 SRAM chips produced by major manufacturers. The silicon results show that the test scores ( $F_1$  score) of our proposed technique of identifying memory manufacturer and part-number are 93% and 71%, respectively.

CCS Concepts: • **Security and privacy** → **Embedded systems security**; • **Computer systems organization** → **Embedded systems**.

Additional Key Words and Phrases: Counterfeit memory, Counterfeit SRAM, Anti-counterfeiting, Semiconductor supply-chain security

## ACM Reference Format:

B. M. S. Bahar Talukder, Farah Ferdaus, and Md Tauhidur Rahman. 2018. A Non-invasive Technique to Detect Authentic/Counterfeit SRAM Chips. *ACM J. Emerg. Technol. Comput. Syst.* 37, 4, Article 111 (August 2018), 25 pages. <https://doi.org/10.1145/1122445.1122456>

## 1 INTRODUCTION

With the globalization of the semiconductor supply chain and the growth of the semiconductor market value, counterfeit ICs have become an established threat to the semiconductor community. In the modern horizontal semiconductor supply chain, multiple facility centers are involved in the manufacturing process and facilitate different stages of chip production. In this supply chain model (Fig. 1), a chip may be designed in one place and fabricated in different places. Because of these traveling IPs (intellectual properties) in different formats, the device can be easily counterfeited in many different ways and may easily get introduced to the consumer market. Recent studies show that the global market share of counterfeit integrated circuits (ICs) worth \$169 billion [23, 27], and ~17% of

Authors' address: B. M. S. Bahar Talukder, [bbaha007@fiu.edu](mailto:bbaha007@fiu.edu); Farah Ferdaus, [fferd006@fiu.edu](mailto:fferd006@fiu.edu); Md Tauhidur Rahman, [mdtrahma@fiu.edu](mailto:mdtrahma@fiu.edu), Department of ECE, Florida International University, 10555 West Flagler Street, Miami, Florida, 33174, USA.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from [permissions@acm.org](mailto:permissions@acm.org).

© 2018 Association for Computing Machinery.

1550-4832/2018/8-ART111 \$15.00

<https://doi.org/10.1145/1122445.1122456>

those counterfeited ICs are memory chips [21, 23, 27]. Moreover, another ~28% of the counterfeit chips are contributed by programmable logic (CPLDs, FPGAs), microcontrollers, and microprocessors [21]. However, most of the modern programmable logic and microcontrollers/microprocessors are integrated with memory (e.g., BRAM in FPGA, cache in microcontrollers/microprocessors). Therefore, identifying counterfeit memory should be able to capture the majority of these counterfeit programmable logic and microcontrollers/microprocessors. Counterfeit chips are classified into the following major categories [23]: (i) recycled, (ii) remarked or forged documentation, (iii) tampered (iv) cloned, (v) reverse-engineered, (vi) out-of-spec/defective, and (vii) overproduced. Table 1 shows various types of counterfeitings along with examples [21, 23]. A counterfeit chip suffers inferior quality and, therefore, can impact the safety, security, and reliability of a system [43]. For example, Russia’s recent Fobos-Grunt mission to Mars was canceled due to a counterfeit SRAM memory chip [50]. Unfortunately, identifying counterfeit chips is tricky as they can pass the initial functional test but may fail prematurely due to their lower life expectancy than authentic chips.

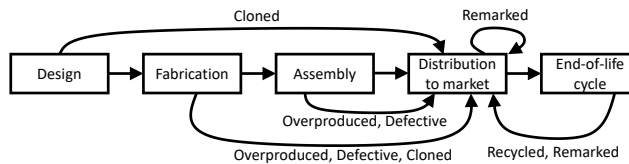


Fig. 1. Device counterfeiting at different stages of the horizontal semiconductor supply chain [64].

Table 1. Different types of counterfeiting [21, 23].

Counterfeit Types	Definition
Recycled	Recycling chips from old PCB and selling them as new. In a more sophisticated recycling process, the plastic/ceramic encapsulation of the chip die is removed and repackaged to make its appearance new. Recycled chips shares >80% of the counterfeit market [21].
Remarked	Inferior quality chips are marked as the superior one.
Forged documented	Faking the chip documentation (e.g., faking safety and security certification).
Reverse Engineered	Recover the functional netlist from the chip by an electro-chemical process. Counterfeiter may use this netlist to avoid the R&D cost.
Cloned	The untrusted fabrication facility can copy the chip design (netlist, GDSII); later, they can produce unauthorized chips.
Overproduced	Untrusted fabrication facility can produce and market chips outside of the contract, i.e., without authorization of the IP (intellectual properties) owner.
Tampered	Tampering the original chip design. For example, untrusted physical design house can insert hardware trojan in the netlist and create a security backdoor.
Out-of-spec/defective	Selling chips that are failed in the functionality test (manufacturer name and part-number are removed and replaced with a superior one).

To combat the recent trend of increasing fake parts, the U.S. Government passed the National Defense Authorization Act (NDAA) in August 2018 [14]. Section 818 of this Act requires defense

contractors to tighten supply chain traceability and parts procurement to minimize counterfeit risk [29]. Researchers and industries have developed several techniques to detect and avoid counterfeit electronic components, such as physical inspections, imaging techniques, electrical testings, etc. [22–24, 27, 28, 71, 72]. Unfortunately, most solutions focus on identifying a single type of counterfeit chips, e.g., detecting recycled memory chips [26–28]. Furthermore, many of those techniques require either hardware modification, complex supply chain management, complex authentication schemes, or unique laboratory facilities [2, 24, 25, 40, 54, 59]. Hence, those are not suitable for low-cost memory chips. Deploying counterfeit chips into an electronic system can severely compromise system security and reliability because of their sub-standard quality, poor performance, and shorter life span. Unfortunately, identifying counterfeit chips is tricky as they can pass the initial functional test but may fail prematurely due to their lower life expectancy than authentic chips.

Our recent studies [64] show that analyzing latency-based error patterns can capture manufacturers' information and DRAM module specifications. In this paper, we present a more generalized technique to detect and avoid major counterfeit SRAM types. In our proposed technique, we attest and identify the origin of SRAM chips (i.e., manufacturer and specification) by characterizing the start-up behavior of SRAM chips. Attesting and identifying memory manufacturers and specifications might be a powerful tool in avoiding the remarked, defective, tampered, and cloned memory chips. We find that the start-up behavior of SRAM chips varies from one manufacturer to another manufacturer and from one set of specifications to another set specifications because of intentional architectural/layout differences and the manufacturing process variations. Furthermore, we show that a similar analysis of SRAM start-up data can be used to identify recycled SRAM chips as the SRAM start-up behavior is directly correlated with its usage time. We also explore the robustness of our proposed technique and provide a guideline for practical implementation. The major contributions of this paper include:

- We have extracted a set of features from the start-up state of SRAM chips to capture the architectural, layout, and process variations. We found that our proposed set of features can be used to identify the memory manufacturer and part-number<sup>1</sup>.
- We have tested the robustness of our proposed method by varying operating temperature and testing platforms.
- We have also compared the extracted features between the fresh and aged (recycled) chips. The practical aging state of SRAM memory has been emulated by stressing the memory chip under high-temperature and supply-voltage conditions.
- We have validated our proposed technique with the data collected from 345 commodity SRAM chips (produced by five major manufacturers).
- We have provided a practical guideline to improve the accuracy of our proposed method with a realistic demonstration.

The rest of the paper is organized as follows- in Sec. 2, we have briefly discussed SRAM structure, the aging effect on SRAM chips, and existing anti-counterfeit techniques. In Sec. 3, we have proposed our method of extracting an appropriate set of features from SRAM start-up data. In Sec. 4, we have presented our experimental results and analyzed them. We have highlighted the scope and limitations of this work along with the future work in Sec. 5. We have concluded our work in Sec. 6.

## 2 BACKGROUND AND MOTIVATIONS

This section briefly describes SRAM architecture, the aging effect on SRAM cells, and the existing approach to detect counterfeit memory chips.

<sup>1</sup>A unique part-number is usually assigned to a group of electronic components that possess a similar set of specifications.

## 2.1 SRAM, Process Variations, and Aging

SRAM cell, volatile memory that stores one-bit data, consists of two cross-coupled inverters and two access transistors (see Fig. 2) [15, 27]. The cross-coupled inverters are symmetrically laid out to maximize the static noise margin (SNM) [15, 27]. SNM is defined as the maximum allowable noise that can tolerate an SRAM cell without flipping its value [49]. However, the inevitable random dopant fluctuation (RDF) effect leads to threshold voltage variation and introduces asymmetry between SRAM inverters [42]. Therefore, during power-up, these two inverters race each other and settle to “1” or “0” [15, 27]. A significant difference between inverters’ strength generates a strong “0” or a strong “1”. On the other hand, a smaller difference between the two inverters generates weak “0” or weak “1”. Furthermore, the smallest difference between the two inverters creates a noisy start-up value.

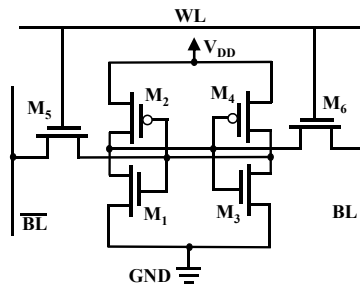


Fig. 2. SRAM cell structure.

Moreover, two well-known phenomena, negative and positive bias temperature instability (NBTI, PBTI), can also cause transistor threshold voltage to shift [26]. NBTI and PBTI are the direct consequence of transistor aging [26]. Previous research suggests that the SNM of the SRAM decreases by >9% within three years of usages [51].

## 2.2 Memory Supply Chain Vulnerabilities

Globalization of the semiconductor supply chain has allowed worldwide fabrication of authentic and counterfeit chips [7, 23]. In an established global semiconductor supply chain, several untrusted parties (foundry, assembly, third-party IPs, etc.) are involved, any of whom can pirate IP (intellectual property), insert hardware trojan, and/or include recycled, re-marked, overproduced, out-of-spec/defective, cloned, and forge-documented chips [7, 64]. In this global supply chain, the IC or memory manufacturer can (i) fabricate all memory chips or ICs in a single manufacturer-owned foundry or (ii) can send the Graphic Design System (GDSII) file (a file format that contains the final-layout information) to several foundries of their own (but in different geolocation) or third-party foundries to save on the cost per unit or to meet the target timeline [64]. A counterfeiter can sell fake memory chips as authentic ones, recycled or used memory chips as new ones through repackaging, low-quality chips as high-grade ones by mislabeling, and defective or out-of-spec chips without the manufacturer’s consent. An adversary in an untrusted foundry can insert a hardware trojan in the form of addition, deletion, or modification of memory cell, memory array, or peripheral logic [67], which changes the memory layout/architecture [67].

## 2.3 Existing Countermeasures and Limitations

There have been several techniques to detect counterfeit chips. Some existing approaches rely on generating signatures from individual chips [15, 27, 34]. One chip can not be cloned to another chip

because of the signatures' uniqueness due to the process variation. These memory signatures vary from chip to chip, even if they are fabricated in the same silicon wafer. Such signatures are well-known as physical unclonable functions (PUF). The signature from the individual chip is collected and stored in the database during the registration process. During authentication, signatures are collected from the memory under test (MUT) and compared with the database. A device is considered authentic if its signature matches with the expected stored signature. The database can store memory fingerprints from a single measurement. However, the memory signatures are noisy and can be affected by operating conditions. Recently, Guo *et al.* propose measuring memory signature at both room temperature and high temperature to compute a more robust signature [27]. However, the PUF-based method suffers from several limitations:

- **Bit-aliasing:** Bit-aliasing measures the uniqueness and correlation among signatures (PUFs) [55]. It quantifies the distribution of "0" or "1" on a specific memory cell. The bit aliasing can be quantified with Eq. 1.

$$B_i = \frac{1}{N} \sum_{p=1}^N R_p^{i,l} \quad (1)$$

Here,  $N$  is the total number of devices needed to be identified uniquely, where each device is equipped with an  $l$ -bit PUF.  $R_p^{i,l}$  is the PUF response recorded from the  $i$ th bit of the  $p$ th PUF. In an ideal case, the mean occurrence of logic "0" or "1" from a specific bit location should be 50% (i.e., bit-aliasing should be 50%). The ideal bit-aliasing of 50% minimizes the number of bits required to identify all devices uniquely. For example, in an ideal case, to identify 4 SRAM chips uniquely, we need only a 2-bit PUF response (i.e., "00", "01", "10", and "11"). In such a case, the occurrence of "1" or "0" on the first-bit position or the second-bit position is 50%. However, if the average occurrence deviates from 50%, we might need more than 2-bits to authenticate those four SRAM chips. In practice, the bit-aliasing always deviates from 50% and requires more bits than it needed theoretically.

- **Exhaustive registration process:** The signature-based chip authentication requires registering each memory chip before distributing them in the market. This extra step of registration increases both cost and lead time to market.
- **Robustness:** Device signature also may vary depending on the operating condition. A slight variation on temperature or operating voltage might alter the device characteristics and flip some bits on the device signature. Although different Error Correcting Codes (ECC) [10, 57] are proposed as a solution; however, the ECC overhead increases quadratically with the number of errors [57].

Other countermeasures such as SST, hardware metering, blockchain-based traceability, split manufacturing, IC camouflaging, Electronic Chip ID (ECID), On-chip sensor, DNA marking, etc., might be used to prevent counterfeiters [2, 3, 19, 21, 23, 25, 31, 32, 36, 38, 40, 54, 58, 59, 74, 75]; however, these techniques suffer from different drawbacks. For example, SST and hardware metering techniques provide control over post-fabrication, but it requires a change in traditional fabrication flow. Furthermore, this technique requires exhaustive communication between the foundry and the manufacturer. On the other hand, ECID tags each chip with a unique ID by adding a one-time programmable (OTP) memory. Nevertheless, this method is not suitable for all kinds of chips. For an SRAM chip, the overhead of adding an extra memory component will be very high. With an on-chip sensor, each chip is equipped with an additional hardware component, which modifies its properties due to aging. These properties can be used to detect recycled chips. However, on-chip sensor-based countermeasures need additional hardware overhead and are not feasible for inexpensive systems. In DNA marking, each memory component is marked with a unique DNA sequence. DNA marking suffers from impracticality as it requires a complex authentication scheme.

Other techniques, such as blockchain-based traceability, split manufacturing, IC camouflaging, etc., require modified fabrication flow or design techniques that are not suitable for low-cost memory chips.

Physical inspection-based schemes [1, 23, 33, 69], such as X-Ray imaging and scanning electron, can detect counterfeit/recycled chips. However, these techniques require expensive equipment and not viable for inexpensive chips. Moreover, Expensive equipment and complex authentication schemes are also not suitable for general users who want to verify their purchased products' authenticity.

This paper proposed a technique to detect counterfeit SRAM chips that do not suffer from the above limitations.

### 3 PROPOSED METHOD

By analyzing the internal signatures of the SRAM memory chips, our proposed technique will identify major types of counterfeit chips by- (i) attesting the origin of the memory chip manufacturer and the specification (i.e., the part-number) of each memory chip and (ii) detecting recycled memory chips. This section describes sources of distinguishable factors, unique features that isolate one part-number with another or identify the same part-number, and our proposed framework.

#### 3.1 Sources of Distinguishable Factors

Our proposed technique relies on the fact that SRAM chips of different specifications differ with architectural, layout, and process parameters, which leads to unique GDSII. All these factors can be used to generate a unique signature from each group of SRAMs.

- **Architectural variations:** Manufactures may optimize the SRAM structure in different ways to support the requirement [6, 12, 13, 60]. Among different structures, the symmetric 6-Transistor (6T) SRAM structure is the most common one (Fig. 2) for on-chip SRAM array (e.g., processors cache). 4T SRAM cells are also common for off-chip SRAM memory. However, 4T SRAM chips can not be implemented on-chip as they need different technology and complex process. Theoretically, the symmetric structure of SRAM cells should produce a uniform distribution of logic "0" and logic "1". On the other hand, to suppress the noise (e.g., read disturbance, half-select disturbance, etc.), other SRAM architecture such as 5T, asymmetric 6T, 7T, 8T, 9T, 10T structure is also available [6, 12, 13, 60]. However, due to these configurations' asymmetric structure, each SRAM cell on the memory array may be biased to a specific logic at start-up. Furthermore, to reduce the bitline noise, the bitlines are often twisted in different configurations [70]. The difference in bitline configuration also may affect the start-up logic locality.
- **Layout Variations:** The layout variation in SRAM cell structure may also cause a variation in start-up characteristics. For example, Apostolidis *et al.* [4] reported six different layout designs for symmetric 6T SRAM structure, and each of them has different pros and cons. For example, they have different power utilization, delay, and noise characteristics. In addition to this, some implementing and resource constrain may introduce some asymmetric nature in memory cells, leading to slight bias to a specific logic at device start-up. For example, using multiple metal layers may introduce unmatched wiring between the inverter pair. Moreover, the difference in CAD tools' configurations may also introduce variations in memory layout.
- **Process variations:** The intrinsic process variation can be either random or systematic [11, 41]. The random process variation can be considered the noise and can be varied among the chips fabricated in a single wafer. However, the systematic process variation can be introduced by the quality of the fabrication plant (foundry), microarchitectural locality, and pattern. For the symmetric layout design of the symmetric 6T SRAM cell, the layout of one inverter is the mirror to the other one. However, the fabrication plant may have different set of rules for mirrored patterns

[46]. Hence, a mirrored layout may be reffered as a different pattern when fabricated. Hence, even with the perfectly symmetric layout design, the two coupled inverters may have slightly different characteristics after fabrication. Additionally, a recent study shows that the founder-dependent channel length and threshold voltage variations impact the IC delay characteristics [69].

- **IC packaging:** Chip die is encapsulated inside a protected “package” to prevent corrosion and physical damage. The difference in IC packaging may also alter some device characteristics. Usually, manufacturers introduce different kinds of die packaging and wire bonding to trade-off among cost, noise immunity, and supporting different operating conditions [39]. The impact of die packaging is minimal compared to other factors, as the IC packaging only impacts external influences (such as noise induced by external temperature). However, the die packaging may influence some device characteristics and, therefore, may impact some of our selected features (see Sec. 3.3). For example, the chips with gold/copper wire bonding should be more robust against external temperature variation than those with aluminum wire bonding. Therefore, the noise magnitude in SRAM start-up data should be smaller with gold/copper wire bonding.
- **Aging:** Usually, the SRAM signature (PUF) can be characterized by  $PSNM_{noise}$  (PUF SNM noise) [15, 47]. The  $PSNM_{noise}$  measures how easily an SRAM cell can be initiated to logic “0” or “1”. A larger value of  $PSNM_{noise}$  ensures more robust SRAM signatures. However, the  $PSNM_{noise}$  heavily depends on SRAM transistors’ threshold voltage [15]. Hence, the SRAM  $PSNM_{noise}$  can be changed over its usages (see Sec. 2.1) due to the change in its transistors’ threshold voltage.

Depending on SRAM usage data pattern, the change in  $PSNM_{noise}$  can affect the SRAM start-up signature: (i) a noisy signature bit might get biased to “0” or “1”, (ii) a weak “0” or “1” might become strong “0” or “1”, (iii) a stable signature bit can be flipped (stable “0” to stable “1” or stable “1” to stable “0”), and (iv) a stable signature bit can become a noisy one. Hence, the change in  $PSNM_{noise}$  will affect the overall distribution of logic “0” and “1” on SRAM signature. The first three factors will increase the total number of stable signature bits; whereas, the fourth factor will produce more noisy signature bits. However, the cumulative impact of the first three factors dominates the fourth factor. Hence, the total number of noisy signature bits will reduce with device usage (which does not indicate the PUF will be more robust with aging [55]). Minimizing the mismatch between two inverters can strengthen the impact of the fourth factor, which is difficult to achieve. The equalization of transistors’ threshold voltage requires a calculative usage data pattern during the entire chip lifetime [51].

In an ideal case, the percentage of 0’s or 1’s should be identical in a new symmetric SRAM chip. One of the recent methods suggests that the skewed distribution of 0’s and 1’s at power-up state can be used to detect recycled SRAM memory [26]. With a typical usage pattern, an SRAM cell experiences more logic “0” bits than the logic “1” bits [68]. Such usages pattern creates more stress on “M4” pMOS (Fig. 2). Hence, over time, the threshold voltage difference of “M4” and “M2” PMOS increases due to the NBTI effect and causes the SRAM cell to be biased with “1” at power-up state. Note that this method of detecting recycle memory is a special case of our proposed technique.

### 3.2 Assumptions

Our proposed technique extracts a set of features from memory signatures and uses them to train a statistical model and identify manufacturer/part-number. Although our method uses a simple authentication protocol, we make the following set of assumptions which are practical for most usage scenarios.

- **Defining features:** Manufacturers/trusted third-parties are responsible for defining a set of features that defines their product best. Prior knowledge of memory architecture might enable them to define a better set of features.
- **Feature extraction:** The feature extraction process should be independent and straightforward enough to be extracted on the user's system; hence, it relaxes the requirement of any special tool or environment requirement. We also assume that the user does not have any knowledge of memory architecture; only general information available from manufacturers should enable a user to extract the features.
- **Memory Class:** Two memories are from separate classes if they have a different manufacturer and/or a different set of specifications (i.e., speed, size, temperature range, power rating, data-width, die package, die generation, etc.). A change in specification and/or manufacturer lead to different GDSII and/or packaging; hence, it will impact start-up data, as discussed in Sec. 3. Although a manufacturer may send the same GDSII to multiple fabrication facilities, we assume that fabrication plants with the same GDSII maintain the same design rule to keep uniformity. We also assume that a manufacturer may produce memories with a different specification but with the same set of fabrication plants or design memories with a slight change in specifications (for example, only change in the die package). In such a case, these memories may have two sets of features with subtle variation, which leads to a complex classification problem to identify the memory correctly.
- **Classification:** Classifying memory (authentic vs. counterfeit) can be done in either manufacturer end or consumer end, depending on the application. For example, if the manufacturer is reluctant to release the statistical model publicly, it might ask for the features from memory under test (MUT) to verify the authenticity. On the other hand, to reduce the communication overhead and complexly, the manufacturer may release the statistical model publicly, and the MUT can be verified on the user's system.

### 3.3 Feature Selection

The accuracy and efficiency of any machine learning algorithm heavily rely on the features that are used for the algorithm. Hence, in this step, we proposed a set of SRAM start-up-based features that can effectively capture the architectural, layout, and process variations. A good feature should obtain (i) the similarities of chips with the same specification and (ii) the discrepancy between chips manufactured with different specifications.

In our proposed method, we collected  $n$  sets of start-up data ( $\{D_1, D_2, \dots, D_n\}$ ) from each SRAM chip. We constructed a unified data,  $D$ , based on majority voting<sup>2</sup> cast by  $\{D_1, D_2, \dots, D_n\}$ . SRAM memory cells are generally arranged in a 2-D array of size  $r \times c$  ( $r = \text{number of rows}$  and  $c = \text{number of columns}$ ). If each word of a SRAM chip consists of  $w_l$  bit data, then, for simplicity, we can assume that there is a total of  $w_l$  2-D array of single bit contributing 1-bit data to each data word. So, the data  $D$  should be 3-D data of size  $r \times c \times w_l$ . However, to reduce the complexity, we rearrange the whole data in a 2-D array of size  $n_w \times w_l$  ( $= \text{dim}(D)$ ), where  $n_w = r \times c$  is the number of words in the memory. Now we extract the following seven features from the start-up data  $D$  [64]:

- **Feature 1 ( $\Phi_1$ ):** This feature quantifies the "cell biasness" by counting the number of logic "1" bits in the start-up data. The evaluation of  $\Phi_1$  is illustrated in Fig. 3. In this example, we presented start-up data from a  $4 \times 8$  ( $n_w \times w_l$ ) SRAM chip containing four 8-bit words. In this figure, 16 bits contain logic "1" out of 32 bits. Hence, according to our definition,  $\Phi_1 = 16/32 = 0.5$ . Cell

<sup>2</sup>In the majority voting technique, each signature bit is sampled multiple times, and the value of that signature bit is assigned as the majority of the samples [61].



bias qualitatively measures the asymmetry of the cross-coupled inverters (see Sec. 2.1). For an ideally symmetric SRAM cell structure, this value should be 0.5 (i.e., no “cell bias”). However, in practice, this value is usually deviated from 0.5 because of the different variations discussed previously (see Sec. 3.1).

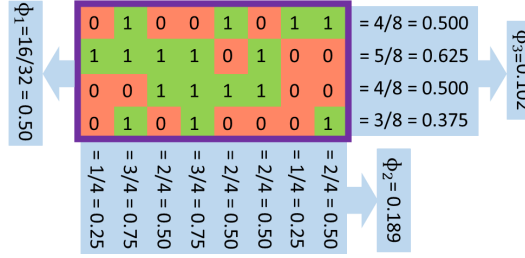


Fig. 3. Illustration of  $\Phi_1$ ,  $\Phi_2$ , and  $\Phi_3$  (4x8 SRAM).

- **Feature 2 ( $\Phi_2$ ):** An SRAM chip of word size  $w_l$  can be assumed as a series of  $w_l$  2-D SRAM arrays. We counted a fraction of “1” from each 2-D array for this feature and took the standard deviation as the feature  $\Phi_2$ . If each of the 2-D arrays follows similar data distribution, and the  $\Phi_2$  should be close to 0. In Fig. 3, each 2-D array is rearranged in a single-dimensional vector for visualization purposes and presented along each column. Now, to evaluate  $\Phi_2$ , we computed the fraction of logic “1” along each column, and then standard deviation is calculated using those values.  $\Phi_2$  can capture different physical properties of the SRAM chips. For example, if the area constraint is too tight, all 2-D memory arrays can be located in close proximity or may be fused together. In that case, they may have a smaller difference in logic distribution due to smaller process variations.
- **Feature 3 ( $\Phi_3$ ):** The fraction of logic bit “1” is counted in each word of data  $D$ ; then, the standard deviation of those values was taken as the feature  $\Phi_3$ .  $\Phi_3$  is also illustrated using Fig. 3. In this figure, we first calculated the fraction of logic “1” from each word (along the row), and then  $\Phi_3$  is estimated by computing the standard deviation of those values. In an ideal case, the distribution of logic bit “1” from each data word should be normally distributed with a mean of 50%. Our experimental results demonstrate that the mean is close to  $\Phi_1$ . However, the standard deviation of distribution may vary from chip to chip depending on memory specification (i.e., for some memory chips, the distribution can be flatter than other chips of different specifications).  $\Phi_3$  quantifies the symmetry of the SRAM cell array. For example, each SRAM cell might experience different systematic process variations due to the local layout patterns<sup>3</sup>; hence, data words from different address locations might experience different logic distribution at start-up. A larger variation on local logic distribution will result in a larger value of  $\Phi_3$ .
- **Feature 4 ( $\Phi_4$ ):** The compression ratio ( $r$ , where,  $r \geq 1$ ) of the start-up data is selected as one of the features. A start-up data with regular patterns have larger data redundancy and can be significantly compressed without any information loss. However, start-up data with randomly distributed zeros and ones can be squeezed very little and causes a smaller value of compression ratio (closer to 1).  $\Phi_4$  can capture the impact of the random process variation on SRAM chips. The compression ratio is defined as Eq. 2.

$$r = \frac{S_u}{S_c} \quad (2)$$

<sup>3</sup>Local layout patterns might be different from one cell to another, e.g., memory cells near the sense amplifier vs. memory cells at the middle of the SRAM array.

Where,

$$\begin{aligned} S_u &= \text{size of the uncompressed data} \\ S_c &= \text{size of the compressed data} \leq S_u \end{aligned}$$

For data compression, we use the standard ZLIB library [16]. ZLIB library ensures the least resource utilization during data compression.

- **Feature 5 ( $\Phi_5$ ):** All data words from each SRAM chip are split into multiple blocks to extract this feature, where each block consists of 512 consecutive data words. Then we compute the fractional value ( $P_1$ ) of each block of data that exhibits logic “1”. We, then, calculate the standard deviation of  $P_1$  calculated from each block. We select this standard deviation as feature  $\Phi_5$ . This feature captures the spatial locality of logic “0” and logic “1” of start-up data. A higher value of  $\Phi_5$  signifies a larger spatial locality. Although we select the block size of 512, the manufacture may wish to select a different size that describes the best structural granularity in memory space. A smaller value of the block size might capture more spatial details; however, the  $\Phi_5$  will also be largely influenced by the local noise if the block size is too small. We experimented with different block sizes and found that 512 provided the best result for memory classification. It is worth mentioning that  $\Phi_3$  is similar to  $\Phi_5$ , where the block size of  $\Phi_3$  is only one word. Hence,  $\Phi_3$  captures finer grain spatial information more effectively. However,  $\Phi_3$  may also capture the local noise information.
- **Feature 6 ( $\Phi_6$ ):** For each memory cell, we have collected SRAM data a total of 20 times and mark those memory cells as noisy if logic “1” is observed 8 to 12 times. We marked those cells as noisy signature bits. For this feature, we counted the percentage of noisy signature bits. In a well-designed SRAM memory cell, the coupled inverters are highly matched, and corresponding signature bits are largely affected by the external/internal noises (e.g., voltage fluctuation, thermal noise, etc.). Furthermore, we believe that this feature can contribute highly to detect recycled memory chips. Over the usage, there will be more cells with large threshold voltage mismatch in recycled memory chips [26] and will produce large  $PSNM_{noise}$  (see Sec. 3.1). Hence, a recycled SRAM chip should produce less noisy signature bits and reduce the value of  $\Phi_6$  over time.
- **Feature 7 ( $\Phi_7$ ):** In this feature, instead of accounting for the theoretical normal data distribution, we made a  $(w_l + 1)$ -bin histogram. If a data-word ( $\in D$ ) occupies a total  $t$  bit of logic “1”, and then it is placed in  $t$ th histogram bin. The standard deviation of the bin size quantifies as the feature  $\Phi_7$ . If the distribution is normal (or Gaussian), then  $\Phi_3$  and  $\Phi_7$  should be approximately the same (also well-known as *the normal approximation for probability histogram*). Hence, the  $\Phi_7$  measures the skewness on word ( $\in D$ ) distribution from the normal distribution.

We extract all these seven features from both fresh (i.e., new) and aged (i.e., recycled) SRAM chips. Then we show that these features form visually separated clusters in feature space depending on the SRAM module type (manufacturer “A” vs. Manufacturer “B”, Part-number “X” vs. Part-number “Y”, fresh vs. aged/recycled).

In addition to above features, manufacturers may choose a different feature-set that describe their chips more concisely. Furthermore, the manufacturer may prefer a different set of data (e.g., error pattern by reducing latency parameters) to extract the more appropriate features [64]. However, when the manufacturer itself does not define the features and assign the responsibility to a third-party, one or few features might not obtain the exact electrical characteristics as intended due to the special modification at the architectural or layout level (which might not be known to the third-party). For example, bit-level scrambling in the data word may limit the usefulness of feature  $\Phi_2$  [18]. Nevertheless, this problem can be avoided by using conventional feature selection and dimension reduction techniques to select the most appropriate feature-set [20, 63, 76].

It is worth mentioning that the features described above only provide qualitative information of different physical properties of the SRAM chips; however, they do not provide any quantitative information. Furthermore, each feature described above might be impacted by combined information from multiple physical properties. For example, although  $\Phi_5$  primarily varies from one memory class to another due to spatial variation,  $\Phi_5$  might also be impacted by the address scrambling caused by the architectural difference in the address decoder [66].

### 3.4 Identifying Authentic Memory Chips

Usually, memory chips with the same manufacturer and specification are labeled with a unique part-number; hence, to identify a memory authenticity, we need to identify the memory part-number. We propose a machine learning-based approach to classify the memory part-number after extracting features from the start-up data. However, the classification can be done with two different approaches- a) learning a binary classifier (positive vs. negative) for each class, and b) learning a one-class classifier for each class. In the first approach, we learn a binary classifier for each class to differentiate between positive samples and negative samples (i.e., authentic vs. counterfeit). This approach is only applicable when both positive and negative sample is available while training the classifier. Nonetheless, it is not a practical approach due to the enormous diversity in negative samples. Collecting negative samples from whole statistical distribution is not cost-effective and time-efficient. In the second approach, we do not need any samples from the negative class, and only positive samples are sufficient to learn the classifier. Recent studies show that [1, 35, 56, 62, 64], a one-class classifier is preferable for counterfeit IC detection as the statistical diversity of the counterfeit chips (negative class) is too large, and they can be introduced from a large number of sources (see Sec. 2.2). Unfortunately, one-class classification is a complex statistical problem and might reduce the accuracy. Hence, we propose a two-step approach to solve this issue:

- (1) **Identifying manufacturer:** Different vendors use different memory cell designs, design flow, and possibly fabrication facilities. Furthermore, they may integrate different peripheral inside the memory; for example, altering row-decoder may alter apparent start-up data locality seen from outside of the memory. Hence, multiple sources may contribute to start-up data variation among SRAMs manufactured by different vendors. In other words, SRAMs for different manufacturers appeared to have a larger difference in their features (large inter-manufacturer feature distance), which ease identifying the SRAM manufacturer (e.g., manufactured by vendor "A" or not). However, while training a binary-classifier, it is impossible to learn all the negative samples that the target vendor does not manufacture. Therefore, we propose a one-class learner (e.g., one-class Neural Network, one-class SVM, SVDD, etc. [1, 35, 56, 62, 64]) only to identify the manufacturer information. However, one may choose to train a binary-class classifier with all available negative samples along with a one-class classifier to improve the accuracy.
- (2) **Identifying part-number:** A manufacturer usually produces different memory chips with different specifications with different part-numbers. However, they may use the same design facility and similar peripherals for all of them, leading to a more subtle feature difference among memories. Fortunately, we can assume that a manufacturer can easily access all memories that they manufacture. Therefore, once the manufacturer is identified, the target manufacturer can easily provide a binary (target class vs. others) or a multi-class classifier to identify each memory part-number produced by them. As we mentioned earlier, the one-class classifier is a complex learning task; hence we should avoid it when we have access to the negative samples from the whole statistical distribution. In this particular scenario, one-class learning is more difficult as we have a smaller feature distance among part-numbers produced by the same manufacturer.

In summary, for manufacturer identification, we recommend using a one-class classifier as it is difficult to collect samples from all manufacturers. However, for identifying part-number, we can

safely assume that the manufacturer has access to samples from all part-number manufactured by itself. Therefore, we recommend using a binary (target class vs. others) or a multi-class classifier for identifying part-number. The one-class classifier is a complex statistical problem and requires large train samples. Unfortunately, we have only access to a limited number of samples from five major manufacturers. Therefore, for demonstration purposes, we avoid the one-class classifier for manufacturer identification and use a binary classifier for both manufacturer and part-number identification.

### 3.5 Proposed Framework

We propose a machine learning-based algorithm that uses the device signature to verify the manufacturer and the part-number. Fig. 4 represents the detailed framework of our proposed technique. Our proposed framework consists of eleven steps, and the order of the steps is numbered in Fig. 4. The steps provided in the yellow and red regions must be performed by the OEM and device owner (user/consumer), respectively. However, steps in the green region can be performed either by the user or by the manufacturer. Our proposed framework starts by defining a set of features (as explained in Sec. 3.3). Then, using a golden set<sup>4</sup> of sample memory chips, the manufacturer needs to extract the feature set and train classifiers to identify counterfeit chips. The manufacturer can train the classifier in two steps: (i) learning manufacturer-specific property ( $C_m$ ) and (ii) learning part-number-specific property ( $C_p$ ). Manufacturing-specific property can be learned by a one-class classifier (i.e., only learning the target manufacturer) and might be assisted by a binary classifier (i.e., target manufacturer vs. others). For the second step, the manufacturer can train either a multi-class classifier for all part-numbers or a multiple binary (one vs. all) classifier for each part-number. By using publicly available information provided by the manufacturer, a user should be able to collect the signature from his sample and extract the feature-set. If the classifier information is available, the user can verify the chip authenticity by himself. Otherwise, the user can send the extracted feature-set to the manufacture, and the manufacturer can verify the authenticity of the test memory chip (verify on request). The start-up data collection process can vary depending on the evaluation platform and application; therefore, we leave the detailed implementation of the start-up data collection routine to the OEM/user. Note that our proposed protocol may be adjusted to meet the evaluation platform/manufacturer requirements.

### 3.6 Identifying Recycled Memory Chips

Although identifying memory manufacturer and part-number can prevent many types of counterfeitings [64], identifying memory manufacturer and part-number does not capture the recycled memory chips. Fortunately, the features we described in Sec. 3.3 can also be used for identifying recycled memory chips. For example, the distribution of the 0's and 1's can be skewed over time due to the skewed distribution of 0's and 1's in functional memory usage, which can be easily captured by Feature 1 [26]. Additionally, we observe that the distribution of other features may

<sup>4</sup>In the presence of an untrusted foundry, it is still possible to construct a golden sample set. An untrusted foundry can cause three types of possible counterfeiting- (i) introduce defective chips as fully functional, (ii) tamper the GDSII and introduce hardware trojan or security backdoor, and (iii) sell overproduced chips. While choosing the golden samples, it is easy to avoid defective chips if the design follows standard DFT (design for testing) and memory testing (such as memory built-in self-test or MBIST) techniques. On the other hand, tempering the GDSII requires R&D effort to understand and modify the original design without altering the main chip functionality. Therefore, tampered chips can only be supplied to manufacturers (by the untrusted foundry) if the allowed GDSII to fabrication time is very long. Lastly, our proposed technique is not effective in identifying overproduced chips (see Sec. 5.1). As the feature-set extracted from the overproduced chips (with unmodified GDSII) should be the same as the authentic chip, there will be no impact on the classifier if the overproduced chips are used to train it.

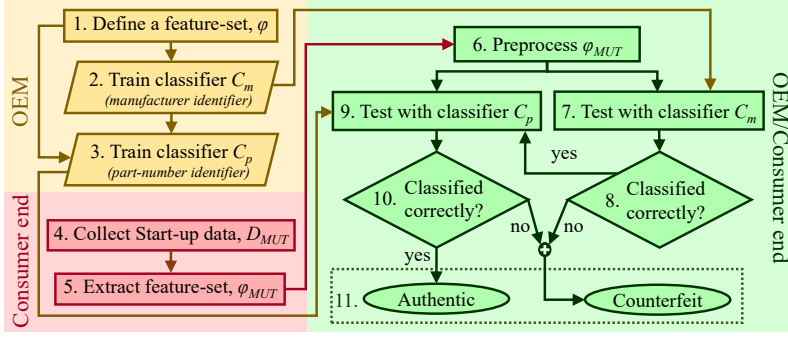


Fig. 4. Proposed protocol to identify counterfeit SRAM.

help to identify recycled SRAM chips in extreme cases, i.e., when only the symmetric data patterns are used over functional memory usage (see Sec. 4.3).

#### 4 RESULT AND ANALYSIS

In our experiment, we have collected SRAM start-up signatures to demonstrate our proposed technique<sup>5</sup>. Typically, the success of any machine learning (ML) model relies on the sample quality and sample size. However, it is difficult to collect data from a large set of sample chips in a lab environment and imitate all possible operating conditions. Therefore, we divide the data collection process into the following tasks:

- (1) We used Arduino Due board [5] for collecting start-up data from SRAM chips. We have used 345 4-Mbit (256K×16) SRAM chips from 5 different manufacturers and 23 different part-numbers (i.e., 23 memory classes). All of these 23 part-numbers are tabulated in Table 2. From now on, we will use the “tag” (specified in Table 2) to recall a specific memory part-number/class. We have used 230 SRAM chips to train ML models (10 chips from each class) and 115 chips to test the model (5 chips from each class).
- (2) We have collected data from both test chips and train chips at a nominal voltage (3.3V) and room temperature (25°C). We used two different Arduino boards to emulate the platform variation among different embedded systems and utilized them to collect start-up signatures from test samples<sup>6</sup>.
- (3) We have used a one-vs-all binary classifier (positive vs. negative) for both manufacturer identification and part-number identification. As we explained in Sec. 3.4, the one-classifier would be the best for the manufacturer identification. However, the one-class classification task is a complex statistical problem and might require a large number of samples to train the model.
- (4) Data noise can impact the classification models severely. To reduce noise, we collected start-up data from the same SRAM chips 20 times. We maintained a constant sampling interval of 2 minutes. We have shorted the power pin ( $V_{CC}$ ) and other control pins of the SRAM chip with the ground within this time interval. We maintained such settings using relay circuits (also controlled by the same Arduino Due board). This experimental setup should be sufficient to

<sup>5</sup>We have made our data publicly available at: <https://sourceforge.net/projects/authentimem/files/>

<sup>6</sup>We have not observed any visible impact from platform variation. Such observation is expected as the two testing platforms only differed by operating voltage (within  $3.3 \pm 35\text{mV}$ ), which is within the range of SRAM normal operating voltage (3.0 to 3.6 mV). Most modern chips are equipped with a voltage clamp circuit and can control the internal voltage as long as the external voltage is within the range [45].

avoid the potential discharge inversion effect on the SRAM start-up state [44]. We combined those 20 sets of data in a single set using the majority voting technique [61].

Table 2. List of SRAM chips in experiment.

Manufacturer <sup>7</sup>	CY					IDT						ISSI				AMI		REA					
Part-number	CY7C1041G30-10ZSXI	CY7C1041CV33-20ZSXA	CY7C1041G18-15ZSXI	CY62147G30-55ZSXE	CY62146EV30LL-45ZSXIT	IDT71V416S10PHG8	IDT71V416S12PHG8	IDT71V416L15PHG8	IDT71V416S10PHGI	IDT71V416S12PHG	IDT71V416L15PHG	ISS61LV25616AL-10TL	ISS1WV25616BLL-10TL	ISS61WV25616BLL-10TLI-TR	ISS4LV25616AL-10TLI	ISS1C25616AS-25TLI	AMI1AS7C34098A-10TCN	AMI2AS7C34098A-10TIN	AMI3AS6C4016-55ZIN	REA1RMLV0414ECGB-4S2#AA1	REA2RMLV0414FCGB-4S2#HA1	REA3RMLV0416FCGB-4S2#AA1	REA4RMLV0416FCGB-4S2#H1
Tag	CY1	CY2	CY3	CY4	CY5	IDT1	IDT2	IDT3	IDT4	IDT5	IDT6	ISS1	ISS2	ISS3	ISS4	ISS5	AMI1	AMI2	AMI3	REA1	REA2	REA3	REA4

- (5) The variance error is expected when the sample size is too small [53]. A model with high variance provides too much attention to the data that are trained with and prone to overfitting. Hence, to reduce the variance error in the trained model, we segmented the SRAM signature data in 16 chunks and virtually increased the sample count by treating each segment as an individual memory chip (i.e., extracting an individual set of features from each segment). However, in the inference phase, the class of a test sample is determined by the majority voting method using all 16 segments. If the same number of votes supports multiple class labels, the tie is broken by comparing the cumulative posterior probabilities<sup>8</sup> of all 16 segments.
- (6) To examine the temperature sensitivity of our proposed technique, we collected data from test samples at high temperatures ( $\sim 45^\circ\text{C}$ ) and validated the same trained model learned in task 3.

#### 4.1 Visualizing Features

The accuracy and efficiency of an ML algorithm largely depend on the quality of the features. Hence, to demonstrate the feature-merit (explained in Sec. 3.3), we have presented the feature distribution of train chip across different manufacturers and different part-numbers in Fig.5. The figure shows that most features are normally distributed (median is centered), and in many cases, at least one feature distribution of a particular class produces a clear visible separation with other classes (i.e., manufacturer "A" vs. all and part-number "X" vs. all). For example, in Fig. 5a, the SRAM chips manufactured by Renesas Electronics are readily separable by the distribution of feature  $\Phi_5$ . Similarly, Fig. 5b demonstrates that SRAM chips from CY4 are easily distinguishable from the distribution of feature  $\Phi_2$ . Unfortunately, in our case, many of the classes can not be separated from other classes based on their feature distribution due to the complex interaction among those features. For example, feature  $\Phi_1$  (number of 1's) and  $\Phi_4$  (compression ratio) might have a close relation; for instance, if the signature data is highly random, the  $\Phi_1$  should be close to 0.5, and  $\Phi_4$  should be close to 1.

For such cases, the class separability can still be visualized if the current feature-space ( $\Phi$ -space) is transferred to a new feature-space ( $\varphi$ -space), where the  $\varphi_i = f(\Phi_1, \Phi_2, \dots, \Phi_n)$ . In our

<sup>7</sup>CY: Cypress Semiconductor; IDT: Integrated Device Technology; ISSI: Integrated Silicon Solution, Inc.; AMI: Alliance Memory, Inc.; REA: Renesas Electronics.

<sup>8</sup>The posterior probability quantifies the confidence level of inferencing a sample to a particular class [30].

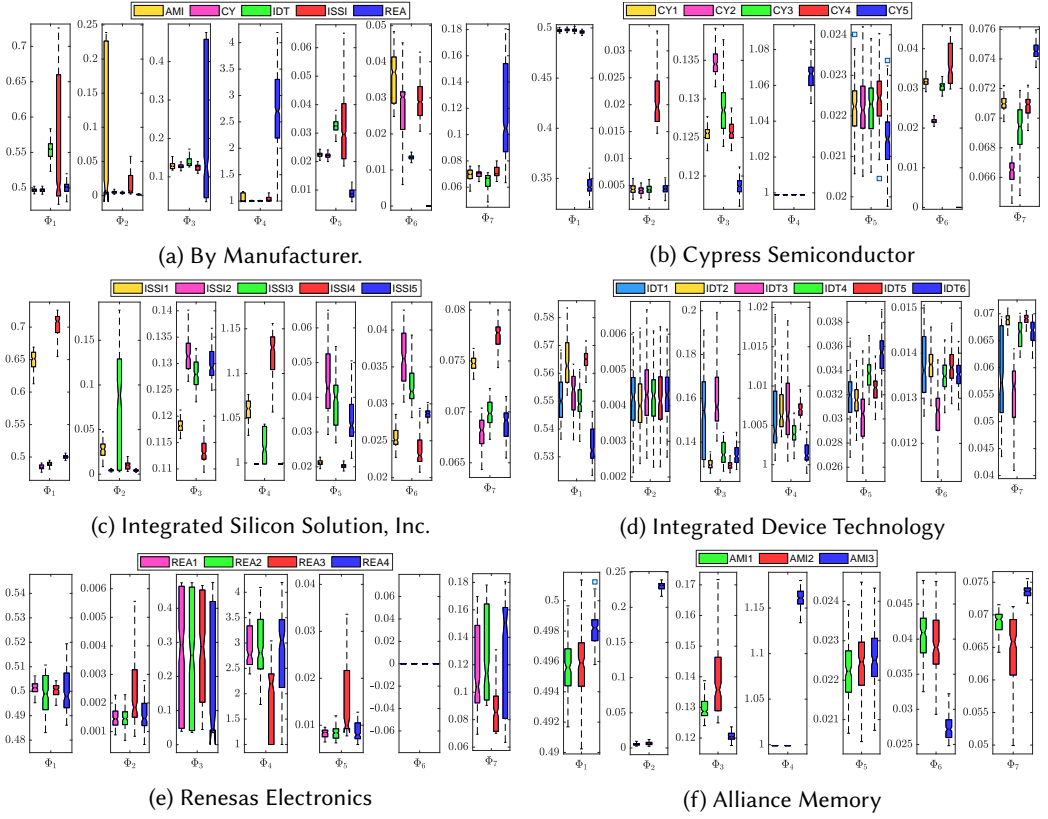


Fig. 5. Visualizing feature distribution by- (a) vendor, and (b)-(f) part-number.

experiment, we have used generalized discriminant analysis (GDA) [8] to transform the  $\Phi$ -space to  $\varphi$ -space, where data points are linearly separable at  $\varphi$ -space. GDA<sup>9</sup> is a supervised machine learning technique to find a reduced set of features that preserves the maximum separability among the classes. This reduced set of features is related to the old feature space by a non-linear kernel function. In our experiment, we have used an *RBF* kernel function [64]. The *RBF* functions' parameter ( $\gamma$ ) is determined by the 10-fold cross-validation method and ensured minimum Euclidean distance between samples and corresponding centroids [9]. Fig. 6 represents the test memory chips in  $\varphi$ -space (in 2D projection) and demonstrates the manufacturer and part-number separability. Each dot in Fig. 6 represents each memory segment as explained in task-5. Those two figures demonstrate that memory classes (manufacturer "A" vs. "B" and part-number "X" vs. "Y") are fairly distinguishable in at least one 2D projection of the  $\varphi$ -space. While transforming the feature-space of a  $K$ -class problem, it is worth mentioning that at most  $K - 1$  dimensions are required in the new feature-space without losing any information of class separability [30]. However, for IDT, adding more than three dimensions (Fig. 6d) only adds very small details on class separability (which is not recognizable from visual appearance). However, we have used  $K - 1$  dimensional new space for a  $K$ -class problem for other cases in Fig. 6.

<sup>9</sup>The reference implementation of GDA is available at: <https://github.com/mhaghghat/gda>

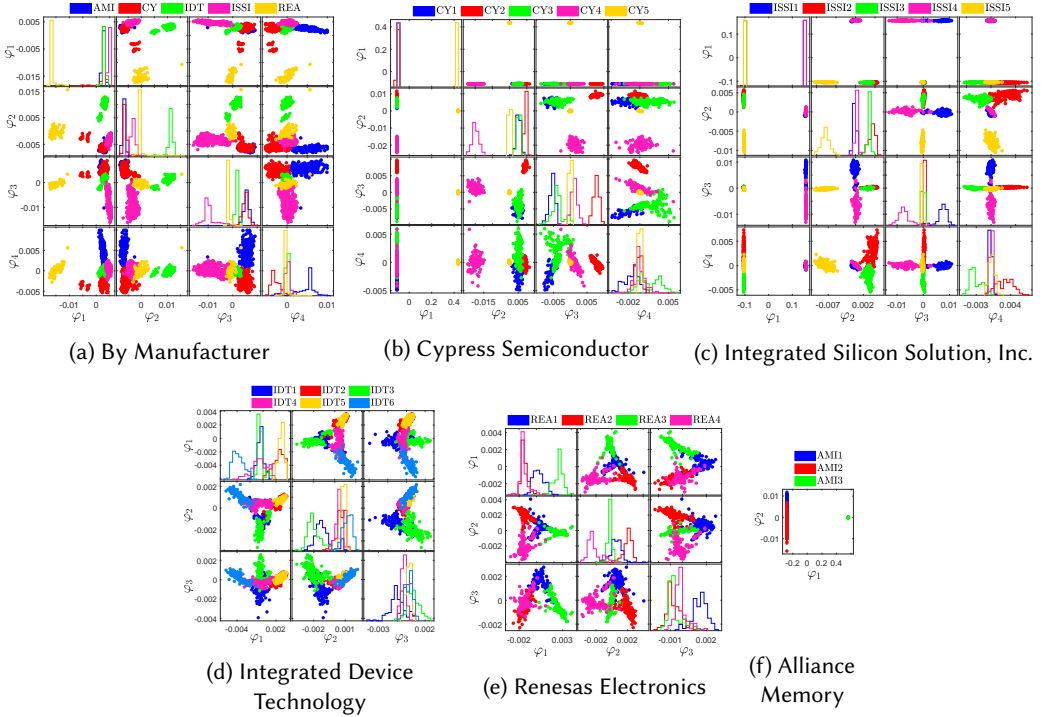


Fig. 6. Representation of SRAM memory in feature-space, clustered by- (a) vendor, and (b)-(f) part-number.

Note that some overlapping between multiple classes is still visible in the  $\varphi$ -space due to the random process variation. However, such overlapping can be reduced by further optimizing the RBF parameters, given that more train samples are available (we have only ten samples from each part-number). While classifying the test memory chips, the impact of such overlap is minimized by assigning equal weight on all 16 segments of the chip and casting a “vote” from each segment.

## 4.2 Labeling Test Memory Chips

Although the GDA can be used for both visualization and classification tasks, GDA is not ideal for a small sample size. Fortunately, the ensemble learning technique can still perform reasonably better even with a small set of samples [17]. In the ensemble technique, multiple base models are learned with different configurations, and then the output label of the test sample is determined based on the vote cast by each model. Although several ensemble algorithms are available, we have used the bagging (**bootstrap aggregating**) method in our experiment. The bagging method is similar to other ensemble methods, except the base model is trained with a different set of train data (sampled with replacement). The bagging method has the inherent ability to reduce the variance error of the trained model and can out-perform other ML algorithms when the train sample size is small [73]. The detailed construction of the algorithm is out of the scope of this paper.

In our experiment, we have trained multiple ensemble models using different base classifiers (e.g., SVM, Decision Tree, Naive Bayes, Discriminant Analysis, Kernel, etc.), and the best model is chosen based on the 10-fold cross-validation score. Then we generated the test score based on our test samples. We represented the test score in Table 3 and 4. The table presents four types of test scores: *Precision* ( $P$ ), *Recall* ( $R$ ),  $F_1$  score, and accuracy, which are defined by Eq. 3, 4, 5, and



6, respectively.  $P$  quantifies the trained model's accuracy out of all predicted positives, and the  $R$  computes the fraction of positives that the model captures correctly. On the other hand,  $F_1$  score is the harmonic mean of the  $P$  and  $R$ . For an ideal case, all of these test scores should be close to 1. Note that, the accuracy is not a very useful metric when the test samples from the positive and negative classes are not equal (unbalanced data). In our experimental setup, the number of test samples for binary (one vs. all) classifiers is unbalanced; hence, we emphasize the  $P$ ,  $R$ , and  $F_1$  score in our discussion.

$$\text{Precision } (P) = \frac{tp}{tp + fp} \quad (3)$$

$$\text{Recall } (R) = \frac{tp}{tp + fn} \quad (4)$$

$$F_1 = \frac{2}{(P)^{-1} + (R)^{-1}} \quad (5)$$

$$A = \frac{tp + tn}{tp + tn + fp + fn} \quad (6)$$

Where,

$tp$  = True positive;  $tn$  = True negative;  $fp$  = False positive;  $fn$  = False negative

We have trained our binary model by utilizing the samples from the target class and the samples from the outlier class (i.e., not belong to the target class). Target class implies manufacturer (or part-number), which is targeted to separate from other manufacturers (or part-numbers). Note that we can either consider the target class as the positive class or the outlier class as the positive class in Eq. 3, 4, 5, and 6. Depending on the definition of positive class, the  $P$ ,  $R$ , and  $F_1$  score can be different for unbalanced test samples. We focus on the test scores produced by considering the target class as the positive class as it delivers the worse set of test scores.

Table 3 and 4 presents a single accuracy score and two sets of  $P$ ,  $R$ , and  $F_1$  score for manufacturer and part-number identification considering both objectives as discussed above. In Table 3, the 1<sup>st</sup> row represents the target manufacturer, and the 2<sup>nd</sup> row represents the corresponding accuracy score. Row 3, 4, and 5 represent the  $P$ ,  $R$ , and  $F_1$  score considering the target class as the positive class. Similarly, row 6, 7, and 8 represent the  $P$ ,  $R$ , and  $F_1$  score considering the outlier class as the positive class. Column 2–6 represents the classifier score for each manufacturer, and column 7 ( $\mu^V$ ) represents the average classification score considering all manufacturers. The table shows that the average test scores are  $\geq 0.92\%$  (positive class = target class), which is promising considering such a small number of samples. However, the classification score is a little lower for CY and AMI than the other manufacturers, resulting from the fact that CY and AMI slightly overlap in feature space (blue and red dots in 6a). However, the classification scores can be improved by adding more samples and further optimization of the classifiers.

Table 3. Classification scores (at nominal temperature) for SRAM manufacturer identification.

Manufacturer		CY	IDT	ISSI	AMI	REA	$\mu^V$
A		0.93	1.00	0.99	0.97	0.99	0.98
Target Class	$P$	0.87	1.00	1.00	0.87	1.00	0.95
	$R$	0.80	1.00	0.96	0.87	0.95	0.92
	$F_1$	0.83	1.00	0.98	0.87	0.97	0.93
Outlier	$P$	0.98	1.00	0.99	0.98	0.99	0.98
	$R$	0.98	1.00	1.00	0.98	1.00	0.99
	$F_1$	0.98	1.00	0.99	0.98	0.99	0.99

Table 4. Classification scores (at nominal temperature) for SRAM part-number identification.

Manufacturer		CY					IDT							ISSI					AMI			REA				$\bar{y}_{\mu^M}$				
Tag		CY1	CY2	CY3	CY4	CY5	$\mu^M$	IDT1	IDT2	IDT3	IDT4	IDT5	IDT6	$\mu^M$	ISSI1	ISSI2	ISSI3	ISSI4	ISSI5	$\mu^M$	AMI1	AMI2	AMI3	$\mu^M$	REA1	REA2	REA3	REA4	$\mu^M$	—
A		0.88	1.00	0.88	1.00	1.00	0.95	0.87	0.87	1.00	0.77	0.90	0.77	0.86	1.00	0.92	0.92	1.00	1.00	0.97	0.73	0.73	1.00	0.82	0.65	0.65	0.85	0.76	0.88	
Target Class	P	0.75	1.00	0.67	1.00	1.00	0.88	0.33	0.20	1.00	0.33	0.20	0.42	0.53	0.79	1.00	0.80	0.80	1.00	0.92	0.92	1.00	0.85	0.33	0.40	0.33	1.00	0.71	0.81	
	R	0.60	1.00	0.80	1.00	1.00	0.88	0.33	0.20	1.00	0.36	0.40	0.40	0.53	0.79	1.00	0.80	0.80	1.00	0.92	0.92	1.00	0.73	0.40	0.33	1.00	0.60	0.72	0.81	
	F <sub>1</sub>	0.67	1.00	0.73	1.00	1.00	0.88	0.33	0.20	1.00	0.36	0.57	0.59	0.53	0.79	1.00	0.80	0.80	1.00	0.92	0.92	0.71	0.33	0.68	0.36	0.40	0.57	0.83	0.71	
Outlier	P	0.90	1.00	0.95	1.00	1.00	0.97	0.86	0.86	1.00	0.88	0.89	1.00	0.92	1.00	0.95	0.95	1.00	1.00	0.98	0.75	0.83	1.00	0.86	0.76	0.73	0.83	0.85	0.93	
	R	0.95	1.00	0.90	1.00	1.00	0.97	1.00	1.00	1.00	0.84	0.84	0.72	0.93	1.00	0.95	0.95	1.00	1.00	0.98	0.60	1.00	1.00	0.87	0.73	0.79	0.83	0.85	0.92	
	F <sub>1</sub>	0.95	1.00	0.92	1.00	1.00	0.97	0.93	0.93	1.00	0.86	0.89	0.84	0.91	1.00	0.95	0.95	1.00	1.00	0.98	0.83	1.00	1.00	0.86	0.76	0.73	0.83	0.85	0.92	

In Table 4, we have presented the classification score for the part number identification, where the 2<sup>nd</sup> row represents the target part-number. Note that,  $\mu^M$  represents the average classification score over the corresponding manufacturer, and the  $\mu^V$  columns represents the average classification score over all manufacturers. Similar to Table 3, rows 4–9 of table 4 represent two sets of  $P$ ,  $R$ , and  $F_1$  scores. Unlike manufacturer identification, the part-number classification score for some manufactures is not up to the mark; especially, the  $P$  or the  $R$  (and corresponding  $F_1$  score) scores to identify a few part-numbers of IDT, REA, and AMI are unacceptably low (shown in red). Nevertheless, such low test scores can be explained from multiple perspectives. For example, the model used to classify manufacturers trained based on 40–60 samples per class; however, due to the extremely limited number of samples from each part-number (10 from each), it is harder to learn part-number classifiers. Besides, the differences among a few memory part-numbers, especially from IDT, REA, and AMI, are not well-understood from their electrical characteristics mentioned in the datasheets. For example, the only noticeable difference between IDT2 and IDT5 is how they are packed during shipping (tube/tray vs. tape/reel). Hence, these two part-numbers might be equivalent based on their electrical characteristics. Similarly, the following pair of the part-numbers- (IDT3, IDT6), (REA1, REA2), and (REA3, REA4) do not have any recognisable difference other than their packing method. Hence, to extract the perfect set of features to differentiate those chips (IDT2 vs. IDT5, IDT3 vs. IDT6, REA1 vs. REA2, and REA3 vs. REA4), we might require more detailed information about the chip characteristics. On the other hand, the IDT1 and IDT4 memory chips are only differed by the temperature grade, and possibly have only difference in their die packaging along with some minor fabrication imperfections [48]. Hence IDT1 and IDT4 may have very subtle differences due to the possible similarity in die architectural, layout, and systematic process variation. We found the similar problem for AMI1 and AMI2, which are also only differed by the temperature grade<sup>10</sup>. Note that, the difference between IDT1 and IDT4 (or, between AMI1 and AMI2) might still be captured by using more train samples. Additionally, if we have more detailed information on chip design, we may be able to identify the subtle difference due to die packaging. For example, the die packaging and wire bonding should impact the characteristics of chips IOs; therefore, the peripheral circuitry of memory chips communicating with IOs should have more impact due to the difference in die

<sup>10</sup>IDT1 and AMI1 are commercial grade (supports 0° to +70°C operating temperature); whereas, the IDT4 and AMI2 are industrial grade (supports –40° to +85°C operating temperature).

packaging. Hence, a feature that captures the memory peripheral characteristics should be more suitable to capture the subtle variation due to die package variation. Unfortunately, understanding the memory peripheral characteristics requires detailed design information on peripheral design, which is only available to memory manufacturers.

In Table 5, we have also presented the summary result (only average test score) by changing the operating temperature of the test samples to  $\sim 45^\circ\text{C}$ . The 2<sup>nd</sup> and last row of Table 5 represents the average score for the manufacturer and part-number detection (respectively) from all manufacturers. On the other hand, rows 3–7 represent the average score for part-number detection from the corresponding manufacturer and the row 8 represents the average score for part-number detection over all manufacturers. From Table 3, 4 and 5, it is apparent that our proposed technique is not very sensitive to temperature. The temperature insensitivity of our selected features is reasonable; previous work shows that varying  $+60^\circ\text{C}$  only changes the SRAM start-up data by  $\sim 12\%$  [52].

Table 5. Arithmetic mean of classification scores (at high temperature)

Classification goal		A	Target Class			Outlier		
			P	R	F <sub>1</sub>	P	R	F <sub>1</sub>
Manufacturer ( $\mu^V$ )		0.97	0.93	0.94	0.93	0.99	0.98	0.98
Part-number	CY ( $\mu^M$ )	0.97	0.93	0.96	0.93	0.99	0.97	0.98
	IDT ( $\mu^M$ )	0.81	<b>0.54</b>	<b>0.47</b>	<b>0.43</b>	0.90	0.88	0.88
	ISSI ( $\mu^M$ )	0.95	0.93	0.88	0.87	0.97	0.97	0.97
	AMI ( $\mu^M$ )	0.82	0.76	0.73	0.72	0.89	0.87	0.86
	REA ( $\mu^M$ )	0.73	<b>0.58</b>	<b>0.55</b>	<b>0.48</b>	0.85	0.78	0.81
	$\mu^V$	<b>0.86</b>	<b>0.74</b>	0.71	<b>0.68</b>	0.92	0.90	0.91

With the temperature increase, the average test score for manufacturer identification almost retain the same score as of the nominal temperature. However, the average part-number identification across all manufacturers is slightly degraded (presented in red in Table 5); for example, the  $F_1$  score to identify the target class reduced from 0.71 to 0.68 (presented in red in Table 5). Especially, the SRAM chips from IDT and REA are affected most while we have increased the temperature. For IDT, the average  $F_1$  score for part-number identification is reduced by 19% (0.53 to 0.43), and for REA, the  $F_1$  score is degraded by 9%. For IDT and REA, we expected such results as the features associated with those part-numbers are very closely distributed (as explained in the previously). Hence, a slight thermal noise on start-up data impacted the corresponding classifiers heavily. Interestingly, the classification score improved by a little margin for AMI, although chips from AMI1 and AMI2 are closely located in feature-space (Fig. 6f). With closer observation, we have found that the features from AMI1 impacted heavily at higher temperatures and shifted away from the AMI2, which provided a relatively better separation between AMI1 and AMI2. The temperature sensitivity of AMI1 is not surprising as AMI1 possesses a lower temperature grade than AMI2.

In Table 3, 4 and 5, we trained the classifier using only one entropy source (i.e., all features are extracted from start-up data at nominal voltage). Our proposed technique can be further improved if more features can be extracted from different entropy sources. For example, we collected three sets of start-up data at low voltage (3.0V), nominal voltage (3.3V), and high voltage (3.6V) from all IDT chips. Then, we only extracted feature  $\Phi_1$ ,  $\Phi_4$ ,  $\Phi_6$ , and  $\Phi_7$  from all of those three datasets and concatenated them in a single feature set (total 12 features). We trained ML models from train samples as we have done earlier and used the model to identify part-numbers from IDT. The outcome of the experiment was aligned with our expectation; The average  $F_1$  score of part-number identification is improved to 0.6 from 0.53 (presented in cyan in Table 4).

### 4.3 Identifying Recycled Memory Chips

As we explained in Sec. 3, the recycled (aged) and fresh (aged) SRAM chip can be distinguished by only observing the number of 1's in start-up data [26]. As our method also uses the number of 1's as a feature ( $\Phi_1$ ), our method is more generalized. Moreover, identifying the recycled chips by observing the number of 1's is only possible if the SRAM chips experience more logic "1" than the logic "0" (skewed data distribution). Although such a scenario is practical over the natural usage of the SRAM chips, we conducted an experiment without making the assumption of skewed data distribution.

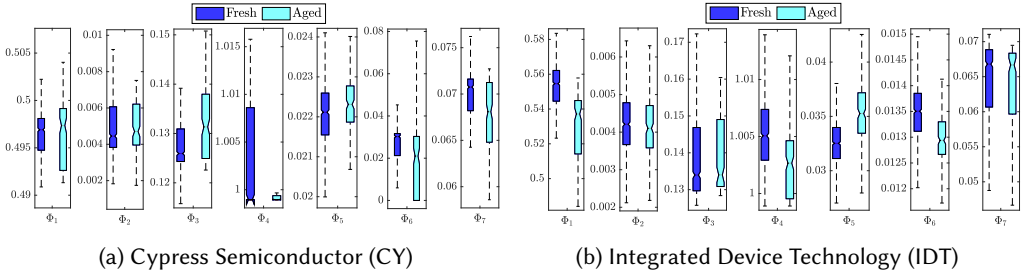


Fig. 7. Visualizing feature distribution: fresh vs. aged.

Our experiment used the "accelerated aging" [27] method by continuously writing random bits on SRAM chips. In accelerated aging, we exposed the memory chips in high voltage (3.6V) and high temperature (80°C) for 1 hour and continuously wrote different random numbers (with the normal distribution of 0's and 1's). The temperature of the chip was controlled by a thermostream system [65]. We collected start-up data before and after the aging process and extracted features from them. The aging process is time-consuming, and we had limited access to the thermostream system; hence, we were only able to experiment with a limited number of chips. Our experiment used 2 SRAM chips from each part-number of CY and IDT (10 CY chips and 12 from IDT). Although this small number of chips is not sufficient for the ML algorithm, our experiment demonstrates the impact of the aging process on features that are selected in Sec. 3.3.

We presented the distribution of the features from fresh chips and aged chips in Fig. 7. Fig. 7a and 7b represent feature distribution for CY and IDT, respectively. Because of using random numbers (uniform distribution of 0's and 1's) to age the device, we have an unpredictable shift on the  $\Phi_1$  (number of 1's) distribution, which is used in previously proposed method to identify recycled SRAM chips [26]. However, we observed some other features might be extremely useful even with the presence of the uniform data pattern. For example, the distribution of  $\Phi_6$  (number of noisy signature bits) always tends to shift towards 0. With sufficient aging, the distribution of  $\Phi_6$  from the fresh and aged chips will be completely separable. During the aging process with the random data pattern, the number of 0's or 1's experienced by each memory cell will be a normal distribution. Hence, some of the noisy signature bits (located at distribution tail) will experience more 0's or 1's than others. With the same argument presented in [26], we can argue that this will bias those noisy signature bits either toward "1" or "0" and reduce the total number of noisy signature bits (see Sec. 3.1 for details). Note that, even with the biased data pattern (dominate by "0" or "1"), the number of the noisy signature bits will also be reduced (noisy signature bits will achieve either stable "1" or "0").

We also observe a shift in the distribution of other features. For example, now the compression ratio is closer to 1 (distribution of  $\Phi_4$ ). This is also understandable as the random distribution on

the data pattern biased the SRAM cells randomly and randomizes the start-up data. However, this distribution might shift upward if the usage data pattern is biased towards either “0” or “1” (i.e., start-up data will have more “1” or “0” after usages). Hence, imposing a boundary condition on  $\Phi_4$  distribution might also be helpful to identify recycled SRAMs.

#### 4.4 Evaluation Time

Our proposed method is aimed to identify counterfeit memory chips from the consumer end (or at least start-up signature should be collected at consumers’ end (See Fig. 4)). Nevertheless, our proposed method can also be scaled up for bulk testing. A single FPGA or high-speed embedded system can be used to collect and analyze data for bulk testing purposes. The average access time for a Commercial off-the-shelf (COTS) SRAM is  $<15\text{ns/word}$ . Hence the total access time for a 4Mb ( $256\text{K} \times 16$ ) SRAM is  $<4\text{ms}$  ( $\approx 15\text{ns} \times 256\text{K}$ ). In our experiment, we have collected start-up data 20 times. Additionally, to avoid the discharge inversion effect, the sampling interval of 10s should be more than sufficient [44]. The inference time of the machine learning model is very negligible compared to the data collection process (order of  $\mu\text{s}$ ). Hence, the total time required to test an SRAM chips’ authenticity is  $\sim 3\text{min}$  ( $\approx 19 \times 10\text{s} + 20 \times 4\text{ms}$ ), which is the time required for collecting the SRAM start-up data.

### 5 DISCUSSION

#### 5.1 Scope and Limitations

Identifying memory manufacturer and part-number are useful for identifying many counterfeitings, which might be introduced at a different supply chain stage. In our proposed method, we extracted a set of features to capture the architectural, layout, and process variations among the memory chips manufactured by different manufacturers with different specification sets. Although identifying manufacturer/part-number does not identify recycled chips directly, our proposed feature-set can differentiate between new and recycled chips, as the device properties are changed over time (explained in Sec 3.1 and 4.3). The tampered and out-of-spec/defective memory chips usually have some fundamental differences at the silicon level, either intentionally introduced by the untrusted facility center or due to the fabrication imperfection. Therefore, feature-set extracted from these types of counterfeit chips should have different characteristics from the authentic chips. For reverse-engineered chips, the counterfeiter usually recovers the functional netlist by depackaging the chip by some electrochemical process and inspecting the chip die by some imaging techniques [21, 23]. Once the netlist is constructed, the counterfeiter can use it for layout design and fabricating new chips without incurring any R&D cost on developing the netlist. The reverse-engineered memory chips are usually differed by layout design and process variation. Therefore, our proposed feature set should be able to capture this type of counterfeiting. In cloned counterfeit type, the counterfeit chips are at least differed by the process variation, i.e., the final GDSII is cloned by the counterfeiter but fabricated in a different fabrication facility. Therefore, the cloned chips can also be identified by our proposed technique. Finally, the remarked chips are completely different from the authentic chips, where the manufacturer name and the part-number are altered; therefore, our proposed method can also identify the cloned chips. Unfortunately, our proposed method might not be able to identify the forged documented and overproduced chips as they are usually designed and fabricated with the same entity; hence, they usually have similar architectural, layout, and process variations.

#### 5.2 Future Work

In our future work, we aim to explore more robust entropy sources across the temperature and voltage variation but are sensitive to usage. Additionally, ML model accuracy largely depends on

feature selection/extraction techniques; hence, we emphasize exploring more features to improve our algorithm. For instance, many well-known features that work well with the binary image classification [37] might also be used to extract features from binary memory signature. We also like to explore the correlation between the feature-set and the technology node, which might provide some deeper insight into features that can add value to our feature selection technique.

## 6 CONCLUSION

This article presents a non-invasive and low-cost technique to (i) identify the memory manufacturer and part-number and (ii) recycled SRAM chips without requiring any additional hardware. This proposed framework has potential to use for other volatile and nonvolatile memory chips and help stop spreading them in the supply chain. Finally, to train a more practical and accurate ML model, we need more train samples which might require an industry scale setup and crowd-sourcing.

## ACKNOWLEDGMENTS

This work was supported in part by the National Science Foundation under Grant Number CNS-1850241.

## REFERENCES

- [1] Ali Ahmadi et al. 2016. A machine learning approach to fab-of-origin attestation. In *2016 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. 1–6. <https://doi.org/10.1145/2966986.2966992>
- [2] Nail Etkin Can Akkaya, Burak Erbagci, and Ken Mai. 2018. Secure chip odometers using intentional controlled aging. In *2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. 111–117. <https://doi.org/10.1109/HST.2018.8383898>
- [3] Yousra M. Alkabani and Farinaz Koushanfar. 2007. Active Hardware Metering for Intellectual Property Protection and Security. In *16th USENIX Security Symposium (USENIX Security 07)*. USENIX Association, Boston, MA.
- [4] G Apostolidis, Dimitrios Balobas, and Nikos Konofaos. 2016. Design and simulation of 6T SRAM cell architectures in 32nm technology. *Journal of Engineering Science and Technology Review* 9, 5 (2016), 145–149.
- [5] Arduino [n.d.]. *Arduino Due*. Arduino. [store.arduino.cc/usa/due](https://store.arduino.cc/usa/due)
- [6] Vivek Asthana et al. 2013. Circuit optimization of 4T, 6T, 8T, 10T SRAM bitcells in 28nm UTBB FD-SOI technology using back-gate bias control. In *2013 Proceedings of the ESSCIRC (ESSCIRC)*. 415–418. <https://doi.org/10.1109/ESSCIRC.2013.6649161>
- [7] Abhishek Basak and Swarup Bhunia. 2016. P-Val: Antifuse-Based Package-Level Defense Against Counterfeit ICs. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 35, 7 (2016), 1067–1078. <https://doi.org/10.1109/TCAD.2015.2501311>
- [8] Gaston Baudat and Fatiha Anouar. 2000. Generalized discriminant analysis using a kernel approach. *Neural computation* 12, 10 (2000), 2385–2404.
- [9] Daniel Berrar. 2019. Cross-Validation. In *Encyclopedia of Bioinformatics and Computational Biology*, Shoba Ranganathan, Michael Gribskov, Kenta Nakai, and Christian Schönbach (Eds.). Academic Press, Oxford, 542–545. <https://doi.org/10.1016/B978-0-12-809633-8.20349-X>
- [10] Mudit Bhargava, Cagla Kaker, and Ken Mai. 2010. Attack resistant sense amplifier based PUFs (SA-PUF) with deterministic and controllable reliability of PUF responses. In *2010 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*. 106–111. <https://doi.org/10.1109/HST.2010.5513106>
- [11] Y. Cao et al. 2002. Design sensitivities to variability: extrapolations and assessments in nanometer VLSI. In *15th Annual IEEE International ASIC/SOC Conference*. 411–415. <https://doi.org/10.1109/ASIC.2002.1158094>
- [12] Leland Chang et al. 2008. An 8T-SRAM for Variability Tolerance and Low-Voltage Operation in High-Performance Caches. *IEEE Journal of Solid-State Circuits* 43, 4 (2008), 956–963. <https://doi.org/10.1109/JSSC.2007.917509>
- [13] Ching-Te Chuang et al. 2007. High-performance SRAM in nanoscale CMOS: Design challenges and techniques. In *2007 IEEE International Workshop on Memory Technology, Design and Testing*. 4–12. <https://doi.org/10.1109/MTDT.2007.4547603>
- [14] US Congress. 2018. HR 5515–John S. McCain National Defense Authorization Act for Fiscal Year 2019. In *115th Congress, August*, Vol. 13. [www.congress.gov/bill/115th-congress/house-bill/5515/text](http://www.congress.gov/bill/115th-congress/house-bill/5515/text)
- [15] Mafalda Cortez et al. 2012. Modeling SRAM start-up behavior for Physical Unclonable Functions. In *2012 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*. 1–6. <https://doi.org/10.1109/DFT.2012.6378190>

- [16] Peter Deutsch and Jean-Loup Gailly. 1996. *Zlib compressed data format specification version 3.3*. Technical Report. RFC 1950, May. [www.ietf.org/rfc/rfc1950.txt](http://www.ietf.org/rfc/rfc1950.txt)
- [17] Thomas G. Dietterich. 2002. Ensemble Learning. In *The Handbook of Brain Theory and Neural Networks*, M. Arbib (Ed.). MIT Press, 405–408.
- [18] P. Ehlig and S. Pezzino. 2017. Error Detection in SRAM. [www.ti.com/lit/an/spracc0a/spracc0a.pdf](http://www.ti.com/lit/an/spracc0a/spracc0a.pdf)
- [19] Kaoutar Elkhyaoui, Erik-Oliver Blass, and Refik Molva. 2012. CHECKER: On-site checking in RFID-based supply chains. In *Proceedings of the fifth ACM conference on security and privacy in wireless and mobile networks*. 173–184.
- [20] Antonio Jesús Fernández-García, Luis Iribarne, Antonio Corral, and Javier Criado. 2018. A comparison of feature selection methods to optimize predictive models based on decision forest algorithms for academic data analysis. In *World Conference on Information Systems and Technologies*. Springer, 338–347.
- [21] DJ Forte and RS Chakraborty. 2018. Counterfeit Integrated Circuits: Threats, Detection, and Avoidance. In *Conference on Cryptographic Hardware and Embedded Systems*.
- [22] Martin Goetz and Ramesh Varma. 2017. Counterfeit Electronic Components Identification: A Case Study. *I-Connect007* (2017). [smt.icconnect007.com/article/105495](http://smt.icconnect007.com/article/105495)
- [23] Ujjwal Guin et al. 2014. Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain. *Proc. IEEE* 102, 8 (2014), 1207–1228. <https://doi.org/10.1109/JPROC.2014.2332291>
- [24] Ujjwal Guin, Daniel DiMase, and Mohammad Tehranipoor. 2014. Counterfeit integrated circuits: Detection, avoidance, and the challenges ahead. *Journal of Electronic Testing* 30, 1 (2014), 9–23.
- [25] U. Guin, D. Forte, and M. Tehranipoor. 2016. Design of Accurate Low-Cost On-Chip Structures for Protecting Integrated Circuits Against Recycling. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 24, 4 (2016), 1233–1246. <https://doi.org/10.1109/TVLSI.2015.2466551>
- [26] Ujjwal Guin, Wendong Wang, Charles Harper, and Adit D. Singh. 2019. Detecting Recycled SoCs by Exploiting Aging Induced Biases in Memory Cells. In *2019 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. 72–80. <https://doi.org/10.1109/HST.2019.8741032>
- [27] Zimu Guo et al. 2018. SCARe: An SRAM-Based Countermeasure Against IC Recycling. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 26, 4 (2018), 744–755. <https://doi.org/10.1109/TVLSI.2017.2777262>
- [28] Zimu Guo, Md. Tauhidur Rahman, Mark M. Tehranipoor, and Domenic Forte. 2016. A zero-cost approach to detect recycled SoC chips using embedded SRAM. In *2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. 191–196. <https://doi.org/10.1109/HST.2016.7495581>
- [29] Matt Hartzell. 2012. Counterfeit parts have real consequences. *COMPUTERWORLD* (2012). [www.computerworld.com/article/2473854](http://www.computerworld.com/article/2473854)
- [30] Trevor Hastie, Robert Tibshirani, and Jerome Friedman. 2009. *The elements of statistical learning: data mining, inference, and prediction*. Springer Science & Business Media.
- [31] James A Hayward and Janice Meraglia. 2011. DNA Marking and Authentication: A unique, secure anti-counterfeiting program for the electronics industry. In *International Symposium on Microelectronics*, Vol. 2011. International Microelectronics Assembly and Packaging Society, 000.
- [32] Kai He, Xin Huang, and Sheldon X.-D. Tan. 2015. EM-based on-chip aging sensor for detection and prevention of counterfeit and recycled ICs. In *2015 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. 146–151. <https://doi.org/10.1109/ICCAD.2015.7372562>
- [33] Ryan L. Helinski et al. 2016. Electronic forensic techniques for manufacturer attribution. In *2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. 139–144. <https://doi.org/10.1109/HST.2016.7495572>
- [34] Daniel E. Holcomb, Wayne P. Burlison, and Kevin Fu. 2009. Power-Up SRAM State as an Identifying Fingerprint and Source of True Random Numbers. *IEEE Trans. Comput.* 58, 9 (2009), 1198–1210. <https://doi.org/10.1109/TC.2008.212>
- [35] Ke Huang, John M Carulli, and Yiorgos Makris. 2012. Parametric counterfeit IC detection via Support Vector Machines. In *2012 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*. 7–12. <https://doi.org/10.1109/DFT.2012.6378191>
- [36] Ke Huang, John M. Carulli, and Yiorgos Makris. 2013. Counterfeit electronics: A rising threat in the semiconductor manufacturing industry. In *2013 IEEE International Test Conference (ITC)*. 1–4. <https://doi.org/10.1109/TEST.2013.6651880>
- [37] Anne Humeau-Heurtier. 2019. Texture Feature Extraction Methods: A Survey. *IEEE Access* 7 (2019), 8975–9000. <https://doi.org/10.1109/ACCESS.2018.2890743>
- [38] Md Nazmul Islam, Vinay C Patil, and Sandip Kundu. 2018. On IC traceability via blockchain. In *2018 International Symposium on VLSI Design, Automation and Test (VLSI-DAT)*. 1–4. <https://doi.org/10.1109/VLSI-DAT.2018.8373269>
- [39] R. Khazaka, L. Mendizabal, D. Henry, and R. Hanna. 2015. Survey of High-Temperature Reliability of Power Electronics Packaging Components. *IEEE Transactions on Power Electronics* 30, 5 (2015), 2456–2464. <https://doi.org/10.1109/TPEL.2014.2357836>

- [40] Farinaz Koushanfar, Gang Qu, and Miodrag Potkonjak. 2001. Intellectual property metering. In *International Workshop on Information Hiding*. Springer, 81–95.
- [41] Kelin J. Kuhn et al. 2011. Process Technology Variation. *IEEE Transactions on Electron Devices* 58, 8 (2011), 2197–2208. <https://doi.org/10.1109/TED.2011.2121913>
- [42] Jinmo Kwon et al. 2012. Heterogeneous SRAM Cell Sizing for Low-Power H.264 Applications. *IEEE Transactions on Circuits and Systems I: Regular Papers* 59, 10 (2012), 2275–2284. <https://doi.org/10.1109/TCSI.2012.2185335>
- [43] Carl Levin and John McCain. 2012. Senate Armed Services Committee Releases Report on Counterfeit Electronic Parts. *Senate Committee On Armed Services* (2012). [www.armed-services.senate.gov/press-releases/senate-armed-services-committee-releases-report-on-counterfeit-electronic-parts](http://www.armed-services.senate.gov/press-releases/senate-armed-services-committee-releases-report-on-counterfeit-electronic-parts)
- [44] Zhonghao Liao, George T. Amariuca, Raymond K. W. Wong, and Yong Guan. 2017. The impact of discharge inversion effect on learning SRAM power-up statistics. In *2017 Asian Hardware Oriented Security and Trust Symposium (AsianHOST)*. 31–36. <https://doi.org/10.1109/AsianHOST.2017.8353991>
- [45] T.J. Maloney and S. Dabral. 1996. Novel clamp circuits for IC power supply protection. *IEEE Transactions on Components, Packaging, and Manufacturing Technology: Part C* 19, 3 (1996), 150–161. <https://doi.org/10.1109/3476.558861>
- [46] Michail Maniatakis, Ibrahim Abe M Elfadel, Matteo Sonza Reorda, H Fatih Ugurdag, José Monteiro, and Ricardo Reis. 2019. *VLSI-SoC: Opportunities and Challenges Beyond the Internet of Things*. Springer. [www.springer.com/gp/book/9783030156626](http://www.springer.com/gp/book/9783030156626)
- [47] Shayesteh Masoumian et al. 2020. Modeling Static Noise Margin for FinFET based SRAM PUFs. In *2020 IEEE European Test Symposium (ETS)*. 1–6. <https://doi.org/10.1109/ETS48528.2020.9131583>
- [48] R Mishra, M Keimasi, and D Das. 2004. The temperature ratings of electronic parts. *Electronics Cooling* 10, 1 (2004), 20.
- [49] Debasis Mukherjee, Hemanta Kr Mondal, and BVR Reddy. 2010. Static noise margin analysis of SRAM cell for high speed application. *International Journal of Computer Science Issues (IJCSI)* 7, 5 (2010), 175.
- [50] J Oberg. 2012. Did Bad Memory Chips Down Russia's Mars Probe? *IEEE Spectrum* (2012). [nssdc.gsfc.nasa.gov/nmc/spaceraft/display.action?id=2011-065A](http://nssdc.gsfc.nasa.gov/nmc/spaceraft/display.action?id=2011-065A)
- [51] Sang Phill Park, Kunhyuk Kang, and Kaushik Roy. 2009. Reliability Implications of Bias-Temperature Instability in Digital ICs. *IEEE Design Test of Computers* 26, 6 (2009), 8–17. <https://doi.org/10.1109/MDT.2009.154>
- [52] C. Premalatha, K. Sarika, and P. Mahesh Kannan. 2015. A comparative analysis of 6T, 7T, 8T and 9T SRAM cells in 90nm technology. In *2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*. 1–5. <https://doi.org/10.1109/ICECCT.2015.7226147>
- [53] Peter Van Der Putten and Maarten Van Someren. 2004. A bias-variance analysis of a real world learning problem: The CoIL challenge 2000. *Machine learning* 57, 1 (2004), 177–195.
- [54] Md. Tauhidur Rahman et al. 2014. CSST: Preventing distribution of unlicensed and rejected ICs by untrusted foundry and assembly. In *2014 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*. 46–51. <https://doi.org/10.1109/DFT.2014.6962096>
- [55] M Tauhidur Rahman et al. 2017. Systematic correlation and cell neighborhood analysis of SRAM PUF for robust and unique key generation. *Journal of Hardware and Systems Security* 1, 2 (2017), 137–155.
- [56] Md. Tauhidur Rahman and B. M. S. Bahar Talukder. 2021. Systems and methods for identifying counterfeit memory. <https://patents.google.com/patent/US11139043B2/en> US Patent 11,139,043.
- [57] Md. Tauhidur Rahman, Domenic Forte, Jim Fahrny, and Mohammad Tehranipoor. 2014. ARO-PUF: An aging-resistant ring oscillator PUF design. In *2014 Design, Automation Test in Europe Conference Exhibition (DATE)*. 1–6. <https://doi.org/10.7873/DATE.2014.082>
- [58] Jeyavijayan Rajendran, Michael Sam, Ozgur Sinanoglu, and Ramesh Karri. 2013. Security analysis of integrated circuit camouflaging. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. 709–720.
- [59] Jeyavijayan Rajendran, Ozgur Sinanoglu, and Ramesh Karri. 2013. Is split manufacturing secure?. In *2013 Design, Automation Test in Europe Conference Exhibition (DATE)*. 1259–1264. <https://doi.org/10.7873/DATE.2013.261>
- [60] R. Rollini, Jenyfal Sampson, and P. Sivakumar. 2017. Comparison on 6T, 5T and 4T SRAM cell using 22nm technology. In *2017 IEEE International Conference on Electrical, Instrumentation and Communication Engineering (ICEICE)*. 1–4. <https://doi.org/10.1109/ICEICE.2017.8191924>
- [61] Yizhak Shifman et al. 2018. A Method to Improve Reliability in a 65-nm SRAM PUF Array. *IEEE Solid-State Circuits Letters* 1, 6 (2018), 138–141.
- [62] O. Sinanoglu et al. 2013. Reconciling the IC test and security dichotomy. In *2013 18th IEEE European Test Symposium (ETS)*. 1–6. <https://doi.org/10.1109/ETS.2013.6569368>
- [63] Li Song, Hongbin Ma, Mei Wu, Zilong Zhou, and Mengyin Fu. 2018. A Brief Survey of Dimension Reduction. In *Intelligence Science and Big Data Engineering*, Yuxin Peng, Kai Yu, Jiwen Lu, and Xingpeng Jiang (Eds.). Springer International Publishing, Cham, 189–200.
- [64] B. M. S. Bahar Talukder et al. 2020. Towards the Avoidance of Counterfeit Memory: Identifying the DRAM Origin. In *2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. 111–121. <https://doi.org/10.1109/>



HOST45689.2020.9300125

- [65] Temptronic ThermoStream [n. d.]. *ATS-605 Thermostream*. Temptronic ThermoStream. [www.intestthermal.com/temptronic/thermostream](http://www.intestthermal.com/temptronic/thermostream)
- [66] A. J. van de Goor and I. Schanstra. 2002. Address and data scrambling: causes and impact on memory tests. In *Proceedings First IEEE International Workshop on Electronic Design, Test and Applications '2002*. 128–136.
- [67] Xinmu Wang et al. 2021. Hardware Trojan Attack in Embedded Memory. *ACM Journal on Emerging Technologies in Computing Systems (JETC)* 17, 1 (2021), 1–28.
- [68] Debao Wei et al. 2016. NRC: A Nibble Remapping Coding Strategy for NAND Flash Reliability Extension. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 35, 11 (2016), 1942–1946. <https://doi.org/10.1109/TCAD.2016.2533861>
- [69] James B. Wendt, Farinaz Koushanfar, and Miodrag Potkonjak. 2014. Techniques for foundry identification. In *2014 51st ACM/EDAC/IEEE Design Automation Conference (DAC)*. 1–6. <https://doi.org/10.1145/2593069.2593228>
- [70] Neil HE Weste and David Harris. 2015. *CMOS VLSI design: a circuits and systems perspective*. Pearson Education India.
- [71] Kan Xiao et al. 2014. Bit selection algorithm suitable for high-volume production of SRAM-PUF. In *2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*. 101–106. <https://doi.org/10.1109/HST.2014.6855578>
- [72] Xiaolin Xu et al. 2015. Reliable Physical Unclonable Functions Using Data Retention Voltage of SRAM Cells. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 34, 6 (2015), 903–914. <https://doi.org/10.1109/TCAD.2015.2418288>
- [73] Selen Yilmaz Isikhan, Erdem Karabulut, and Celal Reha Alpar. 2016. Determining cutoff point of ensemble trees based on sample size in predicting clinical dose with DNA microarray data. *Computational and mathematical methods in medicine* (2016).
- [74] Xuehui Zhang and Mohammad Tehranipoor. 2014. Design of On-Chip Lightweight Sensors for Effective Detection of Recycled ICs. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 22, 5 (2014), 1016–1029. <https://doi.org/10.1109/TVLSI.2013.2264063>
- [75] Xuehui Zhang, Nicholas Tuzzio, and Mohammad Tehranipoor. 2012. Identification of recovered ICs using fingerprints from a light-weight on-chip sensor. In *DAC Design Automation Conference 2012*. 703–708.
- [76] Xiaobo Zhang, Jianzhou Wang, and Yuyang Gao. 2019. A hybrid short-term electricity price forecasting framework: Cuckoo search-based feature selection with singular spectrum analysis and SVM. *Energy Economics* 81 (2019), 899–913.