Counterfeit Electronics: A Rising Threat in the Semiconductor Manufacturing Industry

Ke Huang*, John M. Carulli Jr†, and Yiorgos Makris*
*Department of Electrical Engineering, The University of Texas at Dallas, Richardson, TX 75080
†Texas Instruments Inc., 12500 TI Boulevard, MS 8741, Dallas, TX 75243

***Abstract*—As the supply chain of electronic circuits grows more complex, with parts coming from different suppliers scattered across the globe, counterfeit integrated circuits (ICs) are becoming a serious challenge which calls for immediate solutions. Counterfeiting includes re-labeling legitimate chips or illegitimately replicating chips and deceptively selling them as made by the legitimate manufacturer, or simply selling fake chips. Counterfeiting also includes providing defective parts or simply previously used parts recycled from scrapped assemblies. Obviously, there is a multitude of legal and financial implications involved in such activities and even if these devices initially work, they may have reduced lifetime and may pose reliability risks. In this tutorial, we provide a comprehensive review of existing techniques which seek to prevent and/or detect counterfeit integrated circuits. Various approaches are discussed and an advanced machine learning-based method employing parametric measurements is described in detail.**

I. Introduction

Contemporary advancements in Very Large Scale Integration (VLSI) have been accompanied by increasing variation in the performances of fabricated chips and concerns about correctness of their operation. Indeed, failures can occur at any stage of the lifetime of an IC. In production, devices can fail due to design weaknesses, excessive process variations, local spot defects, or due to defects which are not detected by the production tests and manifest themselves later in the field of operation. These early life failures are caused by extrinsic process defects and they are known as infant mortality. On the other hand, ICs can also fail during their lifetime due to aging, wear-and-tear, harsh environments, overuse, etc. These failures occur when a material or component exceeds its fundamental capability, and are known as intrinsic reliability failure mechanisms. Depending on the end-user application, ICs may go through burn-in tests, where they are exercised sufficiently long in stress conditions, in order to avoid early in-use system failures. Once the reliability issues of an IC are properly addressed, it can be shipped to the customers with predictable lifetime.

However, as the IC supply chain has become globalized and complex, additional sources of failure have started to become a concern. Specifically, trustworthiness of IC suppliers is much harder to assess, hence reliability of the provided parts is dubious. Indeed, ICs provided by the untrustworthy suppliers could be intentionally re-labeled, illegitimately replicated, or recycled from used or defective circuit boards. Even if these ICs initially work, they may have reduced lifetime and pose reliability risks. This problem is known as IC counterfeiting.

IC counterfeits have turned up in many industrial sectors, including computers, telecommunications, automotive electronics, and even military systems [1], [2]. The consequences can obviously be dramatic when critical systems start failing due to the use of counterfeit or lower quality components. According to [3], legitimate electronics companies miss out on about $100 billion of global revenue every year because of counterfeiting. Indeed, the hi-tech industry is heavily impacted by the counterfeiting activity. According to [4], around 1% of the semiconductor sales is estimated to be counterfeited units. The tools and technologies utilized by counterfeiting groups have become extremely sophisticated and well financed [5]. In turn, this also calls for more sophisticated methods to detect counterfeit electronic parts that enter the market. Counterfeit parts can be broadly defined in two categories [6]: 1) new parts that are misrepresented and 2) old parts that are sold as new. The first category involves activities that re-label legitimate chips at a higher grade than that offered by the original part manufacturer, in order to sell them at higher prices, or activities that illegitimately replicate chips and deceptively sell them as made by the legitimate manufacturer. The second category involves providing and selling defective parts scrapped by the original part manufacture, or previously used parts recycled from scrapped assemblies.

In this tutorial, we first review existing techniques which prevent and/or detect counterfeit electronic devices. Various approaches, from basic visual inspection, to more sophisticated methods involving hardware intrinsic security mechanisms and IC metering techniques for counterfeit IC detection are reviewed in Section II. Then, in Section III, we present a machine learning-based method for detecting counterfeit ICs based on parametric measurements which are typically taken for the purpose of Early Failure Rate (EFR) analysis. In Section IV, we demonstrate this methodology on silicon measurements form an industrial case study and in Section V we draw conclusions.

II. Previous work on counterfeit detection

Several practices have been developed to identify counterfeit devices to date. Perhaps the most straightforward method is visual inspection. This method consists of observing texture, indents, labels, part codes, or even gross defects in the IC with a microscope, in order to identify counterfeit ones [7]. Hardware metering [8] attempts to uniquely tag each chip produced from a certain design by active or passive methods to facilitate tracing the chips. Similarly, part authentication tools [9] consist of providing an encrypted number for each device by an RFID tag in production. However, reverse engineering tools have become very advanced and allow an attacker to

978-1-4799-0859-2/13/$31.00

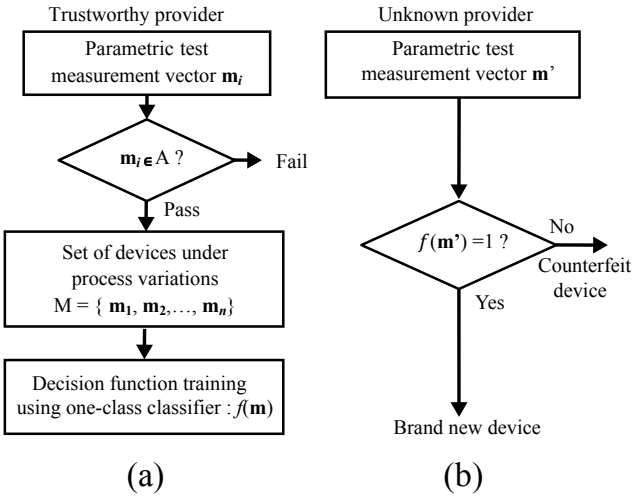

Fig. 1. Proposed flow for counterfeit IC identification: (a) training of the one-class classifier and (b) identification of devices from unknown provider.

read the stored encrypted number. To overcome this challenge, Hardware Intrinsic Security (HIS) has been proposed as a mechanism that can provide security based on inherent properties of an electronic device [10]. Physical Unclonable Functions (PUFs) [11], for example, belong to the category of such HIS mechanisms. PUFs aim to measure the responses of hardware to certain given inputs, which depend on the unique physical properties of the device, since process variations affect each device in a unique and unclonable fashion.

All of the aforementioned methods solve the problem of authentication, which aims at detecting the first category of counterfeit devices, namely misrepresented new parts. However, counterfeit devices belonging to the second category, i.e., old parts which are sold as new, are genuine from that point of view and may pass such methods. Nevertheless, they still pose reliability risks due to their aged nature.

Various on-chip aging sensors have been proposed in an effort to detect recycled counterfeit devices [12]–[15]. Of course, on-chip sensors require extra design effort, test consideration, and come with area/power overhead. In [16], a statistical approach is used to distinguish recycled counterfeit ICs by training a one-class classifier using only brand new devices. Instead of implementing on-chip sensors, the measurements used to build the classifier are typical test results from production EFR analysis required to release most products, thus no additional costs in terms of design, test and area/power overhead are incurred to perform identification, and the method is demonstrated on actual IC measurements. A similar study can be found in [17], where a method based on principal component analysis and convex hull classification, akin to the delay fingerprinting method introduced in [18], is used to detect counterfeit devices using synthetic data.

III. Proposed approach

A. Counterfeit IC identification flow

Figure 1 shows a high level description of the proposed method for identifying the counterfeit ICs. The first step involves collection of a set of parametric measurements, which can be taken from trustworthy provider across devices subject to process variations for the purpose of counterfeit IC authentication. Formally, let

$$\mathbf{m}_i = [m_1, m_2, \cdots, m_d] \tag{1}$$

denote the parametric test measurement vector of the i-th device, where d denotes the dimension of the considered measurement vector. Only devices which contain no defect or excessive process variations are used to train the one-class classifier. Let the set

$$M = \{\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_n\} \tag{2}$$

denote the devices used to train the classifier, where n is the number of considered devices under process variations. It should be noted that the value of n is not prohibitive, typically several hundred devices are sufficient to train the classifier, and the training is a one-time effort.

With our approach, only brand new devices are used to train the classifier, i.e., no prior information of counterfeit IC behavior is needed. For this purpose, we use a one-class Support Vector Machine (SVM) in order to allocate a decision function f, where $f(\mathbf{m}) = 1$ when the device is considered to belong to the group used to train the classifier, i.e., it is considered to be brand new and $f(\mathbf{m}) = -1$ when the device is considered to be counterfeit. More details of the one-class SVM are given in section III-B.

Once the classifier is trained, we can readily use it to identify devices from unknown providers, given the pattern $\mathbf{m}'$, as shown on the right-hand side of Figure 1.

B. One-class SVM

Support Vector Machines (SVMs) were originally designed to solve binary classification problem, in which the SVM is trained with samples of two classes and maps a new sample to one of the two classes in the feature space. In [19], a one-class SVM is presented using kernels to compute inner products in feature space to the domain of unsupervised learning. Formally, we consider the training data

$$\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_n \in O \tag{3}$$

where n is the number of brand new devices under process variations used to train the SVM, and O is the original input space. Let Φ be a feature map $O \mapsto F$, that is, a map into an inner product feature space F such that a simple separation boundary can be drawn in F to separate training samples and other samples from a foreign distribution. The separation boundary can be considered as a d'-dimensional sphere with radius R and center point c, as shown on the right side of Figure 2, where d' is the dimension of the transformed feature space F.

Then one-class SVM training is equivalent to solve the following optimization problem:

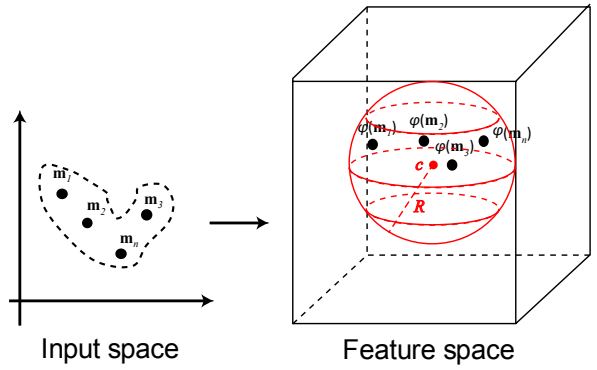

Fig. 2. One-class SVM.

$$\begin{aligned} \underset{R\in\Re,\xi\in\Re^n,c\in F}{\text{minimize}} \quad & R^2+\frac{1}{\nu n}\sum_i \xi_i \\ \text{subject to} \quad & |\Phi(\mathbf{m}_i)-c|^2 \le R^2+\xi_i, \\ & \xi_i \ge 0 \; for \; i\in\{1,\ldots,n\} \end{aligned} \tag{4}$$

where the slack variables ξ_i are penalization parameters in the objective function, ν is a characterization parameter which can be tuned during the training of the SVM, and c can be considered as the center point of the sphere [19]. The goal of the training is to develop an algorithm that returns a function f that takes the value $+1$ in a small region capturing most of the training data points and -1 elsewhere.

For a new point $\mathbf{m}'$, the value $f(\mathbf{m}')$ is determined by evaluating if the point is inside or outside the separation sphere in the feature space:

$$f(\mathbf{m}') = \text{sgn}(R^2 - |\Phi(\mathbf{m}') - c|^2) \tag{5}$$

Here, we use the convention that sgn(z) = 1 for $z \ge 0$ and -1 otherwise.

C. Group classification

Our objective is to identify a set of counterfeit ICs that a malicious supplier provided to the electronic supply chain. Thus, it is worthwhile to generalize the individual decision function $f(\mathbf{m}')$ in (5) to a group decision function $f(M')$, where M' denotes a set of devices under authentication:

$$M' = \{\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_{n'}\} \tag{6}$$

where n' is the number of devices under authentication. In this work, we derive the group decision function $f(M')$ by applying a voting technique. In particular, let I_1 denote the individual classification indicator where $I_1 = 1$ when the individual device is classified as brand new, i.e., $f(\mathbf{m}') = 1$ and $I_1 = -1$ when it is classified as counterfeit, i.e., $f(\mathbf{m}') = -1$. Then the group decision function $f(M')$ can be computed as

$$f(M') = \text{sgn}(\sum_{i=1}^{n'} I_1^i) \tag{7}$$

where I_1^i denotes the individual classification indicator for i-th device under authentication. As before, $f(M') = 1$ indicates the group under authentication is brand new, and $f(M') = -1$ indicates the group is counterfeit. This approach is inspired by the well-known "one-against-one" voting strategy when the SVM is used to solve multi-class classification problems.

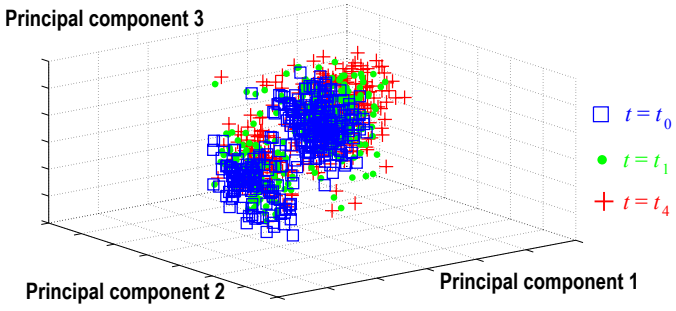

Fig. 3. Projection of the first three principal components of devices at $t = t_0, t_1, t_4$, shown by the squares, solid circles and plus signs, respectively.

IV. Case Study

Our case study is a DSP device with 49 parametric test measurements performed for 313 devices randomly chosen from different lots, i.e. , $\mathbf{m} = [m_1, \ldots, m_{49}]$. The same devices are then passed through burn-in test, in which high voltage and temperature are applied to accelerate the aging mechanisms. It should be stressed that unlike previous methods that aim to detect counterfeit devices by on-chip aging sensors [12]–[15], the proposed approach uses measurements taken from typical production EFR evaluations required to release most products. Thus, no additional costs are incurred to perform identification. During the burn-in test, devices are re-tested with the same measurements $\mathbf{m}$ at 5 different time points: t = $t_0, \ldots, t_4$, with exact hours omitted here due to industrial confidentiality reasons. Time points are approximately log time based since aging degradations such as NBTI exhibit logarithmic dependency on time. The measurements taken from time point $t = t_0$ are considered from brand new devices to train the classifier, and devices at $t \ne t_0$ are considered as counterfeit IC patterns to be identified.

We have performed a Principal Component Analysis (PCA) in order to map the original 49 measurements onto vectors in a lower dimensional space with cardinality $d' < 49$. We maintained the structure of the data while keeping only 9 principal components, i.e. d' = 9. Figure 3 shows the projection of devices at $t = t_0, t_1, t_4$, onto the first three principal components, shown by the squares, solid circles and plus signs, respectively. Performance degradation caused by aging mechanisms is accelerated during the burn-in test and it can be readily observed in Figure 3.

We have generated the following data sets to train and validate the one-class SVM:

- The set S_t contains 157 devices randomly chosen from the 313 devices at $t = t_0$. S_t is used to train the classifier.
- The set S_v contains 5 subsets $\{S_{v0}, \ldots, S_{v4}\}$, corresponding to 313-157=156 other devices at $t = t_0, \ldots, t_4$,

TABLE I
CLASSIFICATION RATE AT DIFFERENT TIME POINTS.

Group \ Validation size	t_0	t_1	t_2	t_3	t_4
156	100%	100%	100%	100%	100%
80	100%	100%	100%	100%	100%
20	100%	96.2%	99.4%	100%	100%
10	100%	95.6%	98.4%	100%	100%
1	82.2%	69.2%	75.5%	87.6%	92.2%

respectively. Thus, S_v contains $156 \times 5 = 780$ devices and is used to validate the classifier.

The second line of Table I shows the classification rate computed using the group decision function defined in (7) for all subsets of S_v: $\{S_{v0}, \ldots, S_{v4}\}$, where 100% denotes a correct classification and 0% denotes an erroneous classification. It can be observed from the second line of Table I that all subsets of S_v are correctly classified with a 100% classification rate.

We generate the following data sets to evaluate the classification capability with reduced validation size:

Step 1 s (s <156) samples are randomly chosen from each of the validation subsets S_{vi}, $i = 0, \ldots, 4$ and let I_2 denote the classification accuracy indicator such that $I_2 = 1$ when the classification is correct and $I_2 = 0$ when the classification is erroneous.

Step 2 The $step1$ is repeated r times in order to consider random effects. The classification accuracy indicator function for the j-th time is denoted by I_2^j.

Step 3 The final classification rate for each of the reduced validation subset S_{vi}, $i = 0, \ldots, 4$ is computed as

$$C_{vi} = \sum_{k=1}^{r} I_2^k \tag{8}$$

The 3^{rd} to 6^{th} lines in Table I show the classification results computed by (8) when the validation size s = 80, 20, 10,1, respectively, and $r = 10$. Based on the classification rate shown in Table I, our observations are the following: 1) Between $t = t_0$ and $t \neq t_0$, the burn-in impact is very pronounced and distinguishable from the process variations impact. We are able to train the classifier to correctly assign a group of devices under authentication to the class $t = t_0$ or to $t \neq t_0$. 2) Misclassification is very low, even with a validation group of as small as 10 devices. However, we cannot distinguish individual devices (see the last line of Table I). In other words, if we have a batch of devices and we know that all of them are either brand new or counterfeit, we can correctly identify them as a group, even if only devices at $t = t_0$ are used for training.

V. CONCLUSION

In this tutorial, we provided a comprehensive review of existing techniques which prevent and/or detect counterfeit electronic devices. Various approaches, from basic visual inspection to more sophisticated methods based on machine-learning are discussed. We also introduced a low-cost approach to identifying recycled counterfeit devices by training a one-class classifier using only brand-new devices. The measurements used to train the classifier are typical tests from production Early Failure Rate analysis, which is required to release most products; thus, no additional cost in terms of design, test and area/power overhead is incurred. Experimental results with actual IC measurements show an excellent ability in identifying counterfeit parts, namely used ICs sold as new.

REFERENCES

[1] "Inquiry into counterfeit electronic parts in the department of defense supply chain," Senate Report of the Committee on Armed Services, 112th congress, 2nd session, 2012.

[2] "Defense industrial base assessment: counterfeit electronics," U.S. Department of Commerce report, 2010.

[3] M. Pecht and S. Tiku, "Bogus: electronic manufacturing and consumers confront a rising tide of counterfeit electronics," *IEEE Spectrum*, vol. 43, no. 5, pp. 37–46, 2006.

[4] N. Kae-Nune and S. Pesseguier, "Qualification and testing process to implement anti-counterfeiting technologies into IC packages," in *Design, Automation & Test in Europe Conference (DATE)*, 2013, pp. 1131–1136.

[5] S. Bastia, "Next generation technologies to combat counterfeiting of electronic components," *IEEE Transactions on Components and Packaging Technologies*, vol. 25, no. 1, pp. 175–176, 2006.

[6] F. Koushanfar, S. Fazzari, C. McCants, W. Bryson, P. Song, M. Sale, and M. Potkonjak, "Can EDA combat the rise of electronic counterfeiting?," in *Design Automation Conference (DAC)*, 2012, pp. 133–138.

[7] "Detection of counterfeit electronic components," *http://www.aeri.com/detection-of-counterfeit.asp*.

[8] F. Koushanfar and Q. Gang, "Hardware metering," in *Design Automation Conference (DAC)*, 2001, pp. 490–493.

[9] K. Chatterjee and D. Das, "Semiconductor manufacturers' efforts to improve trust in the electronic part supply chain," *IEEE Transactions on Components and Packaging Technologies*, vol. 30, no. 3, pp. 547–549, 2007.

[10] V. Van de Leest and P. Tuyls, "Anti-counterfeiting with hardware intrinsic security," in *Design, Automation & Test in Europe Conference (DATE)*, 2013, pp. 1137–1142.

[11] R. Pappu, "Physical one-way functions," *Ph.D Thesis*, Massachusetts Institute of Technology, 2001.

[12] T.H. Kim, R. Persaud, and C.H. Kim, "Silicon odometer: an on-chip reliability monitor for measuring frequency degradation of digital circuits," *IEEE Journal of Solid-State Circuits*, vol. 43, no. 4, pp. 874–880, 2008.

[13] K.K Kim, W. Wang, and K. Choi, "On-chip aging sensor circuits for reliable nanometer MOSFET digital circuits," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 57, no. 10, pp. 798–802, 2010.

[14] J. Keane, X. Wang, D. Persaud, and C.H. Kim, "An all-in-one silicon odometer for separately monitoring HCI, BTI, and TDDB," *IEEE Journal of Solid-State Circuits*, vol. 45, no. 4, pp. 817–829, 2010.

[15] X. Zhang, N. Tuzzio, and M. Tehranipoor, "Identification of recovered ICs using fingerprints from a light-weight on-chip sensor," in *Design Automation Conference (DAC)*, 2012, pp. 703–708.

[16] K. Huang, J.M. Carulli, and Y. Makris, "Parametric counterfeit IC detection via support vector machines," in *IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, 2012, pp. 7–12.

[17] X. Zhang, K. Xiao, and M. Tehranipoor, "Path-delay fingerprinting for identification of recovered ICs," in *IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, 2012, pp. 13–18.

[18] Y. Jin and Y. Makris, "Hardware Trojan detection using path delay fingerprint," in *IEEE International Workshop on Hardware-Oriented Security and Trust*, 2008, pp. 51–57.

[19] B. Schölkopf, J. Platt, J. Shawe-Taylor, A. J. Smola, and R. C. Williamson, "Estimating the support of a high-dimensional distribution," *Neural Computation*, vol. 13, no. 7, pp. 1443–1471, 2001.