Parametric Counterfeit IC Detection via Support Vector Machines

Ke Huang
Department of Electrical Engineering
University of Texas at Dallas
Richardson, TX 75080
Email: ke.huang@utdallas.edu

John M Carulli Jr
Texas Instruments Inc.
12500 TI Boulevard, MS 8741
Dallas, TX 75243
Email: jcarulli@ti.com

Yiorgos Makris
Department of Electrical Engineering
University of Texas at Dallas
Richardson, TX 75080
Email: yiorgos.makris@utdallas.edu

***Abstract*—We present a method to detect a common type of counterfeit Integrated Circuits (ICs), namely used ones, from their brand new counterparts using Support Vector Machines (SVMs). In particular, we demonstrate that we can train a one-class SVM classifier using only a distribution of process variation-affected brand new devices, but without prior information regarding the impact of transistor aging on the IC behavior, to accurately distinguish between these two classes based on simple parametric measurements. We demonstrate effectiveness of the proposed method using a set of actual fabricated devices which have been subjected to burn-in test, in order to mimic the impact of aging degradation over time, and we discuss the limitations and the potential extensions of this approach.**

***Index Terms*—Counterfeit IC detection, one-class SVM classifier, parametric burn-in test.**

I. Introduction

Contemporary advancements in Very Large Scaled Integrated circuits have been accompanied by increasing variation in the performances of fabricated chips. 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 that 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 [1], [2].

On the other hand, ICs can also fail during their lifetimes due to aging, wear-and-tear, harsh environments, overuse, etc. This type of failures occurs when a material or component exceeds its fundamental capability, which is known as intrinsic reliability failure mechanisms [3]. Thus, it is very important to verify that a system will perform all of its required functions under its stated operating conditions for prolonged period of time, which is the role of reliability analysis.

Among a variety of intrinsic reliability failure mechanisms that can cause IC failures, the most well-known mechanisms include electromigration, Negative Bias Temperature Instability (NBTI), Hot Carrier Injection (HCI), gate oxide Time Dependent Dielectric Breakdown (TDDB), etc. Various approaches have been proposed in the literature to model the circuit performance degradation over time due to these aging mechanisms in order to predict time-dependent performance degradation and improve design if necessary to enhance yield over time [4].

One can also predict circuit performance degradation caused by aging phenomena during the production using accelerated testing such as burn-in test to shorten the time-to-failure process. During the burn-in test, higher than usual levels of stress (e.g. temperature, voltage, etc.) is applied to weed out infant mortality and speed-up the deterioration of materials caused by intrinsic reliability failure mechanisms. Once the reliability issue of an IC is properly addressed, it can be shipped to the customers with predictable life-time.

However, as the supply chain grows more complex nowadays in an electronics production flow due to globalisation, with parts coming from different suppliers, it is not always guaranteed that each part provided by the suppliers is trustworthy new brand. In other words, ICs provided by the untrustworthy suppliers could be "recycled" from used or defective circuit boards. Even if these ICs can work initially, they will have reduced lifetime and pose the reliability risks. This problem is known as IC counterfeit. IC counterfeit problem has turned up in many industrial sectors, including computers, telecommunications, automotive electronics, and even military systems. According to [5], legitimate electronics companies miss out on about $100 billion of global revenue every year because of counterfeiting. Several practices exist to identify the counterfeit devices to date, including visual inspection [6] or part authentication tools [7] which consist of providing an encrypted number for each device by an RFID tag in production. However, the time and the cost required for applying these methods are unfordable due to economic pressures in a modern electronic development and fabrication flow. To this end, there is a pressing need to develop low-cost methods to identify the counterfeit ICs to enhance reliability of the device.

In this paper, we propose a method to distinguish the counterfeit ICs from brand new ones by a one-class classifier using Support Vector Machines (SVMs). In particular, we train the classifier using only parametric measurements of brand new devices under process variations and validate it by devices through product reliability op-life tests that mimic aging degradation over time through the use of burn-in stressing at elevated temperature and voltage. The measurements used

978-1-4673-3044-2/12/$31.00 © 2012 IEEE

to build the classifier are typical test results from production Early Failure Rate (EFR) analysis required to release most products, thus no additional costs are incurred to perform identification. The proposed approach is demonstrated on an EFR data from an industrial design. The results show an excellent ability to identify counterfeit parts sold as new from previously used parts. The rest of the paper is structured as follows. In Section II, we provide a brief description of IC failure mechanisms caused by aging phenomena. In Section III, we present the proposed Counterfeit IC detection approach. In Section IV, we demonstrate the methodology on two industrial case studies. Finally, Section V concludes the paper.

II. Aging mechanisms of ICs

Counterfeit ICs are those being "recycled" by the malicious supplier and provided to the electronic supply chain. During the lifetime of an IC, the performances are continuously degraded due to aging mechanisms. Using counterfeit ICs as brand new will significantly reduce the capability of the device to perform its required functions for prolonged period of time.

In order to properly address the counterfeit IC issue, it is important to understand the IC aging phenomena. This section provides a brief description of four most common aging phenomena: electromigration, Negative Bias Temperature Instability (NBTI), Hot carriers injection (HCI), and Time-dependent dielectric breakdown (TDDB).

A. Electromigration

This failure mechanism is due to the migration of atoms in the conduction layers caused by the electric current and it can lead to the formation of voids at some points in the metal line and hillocks or extrusions at other points. It can therefore result in either an open circuit if the void formed in the metal line becomes big enough, or a short circuit if the extrusions become long enough to serve as a bridge between the affected metal and another adjacent metal. The mean time to failure caused by electromigration depends on the cross-sectional area of the conductor, current density and the temperature.

B. Negative Bias Temperature Instability (NBTI)

The Negative Bias Temperature Instability (NBTI) occurs in PMOS devices stressed with negative gate voltages at elevated temperatures. In the reaction-diffusion model, the interface traps located near the gate oxide/silicon channel boundary are pacified with a hydrogen species. The bonds of the hydrogen species can be easily broken and allow for diffusion. This movement of charge impacts the V_{th} of the transistor. For NMOS transistors, the reliability mode is Positive Bias Temperature Instability (PBTI). For pure oxide and nitrided oxides, this has not been a dominant degradation mode. This may change with Hi-k metal gate. The degradation of V_{th} exhibits logarithmic dependence on time [8].

C. Hot carriers injection (HCI)

The Hot Carriers Injection (HCI) occurs in MOS devices where a carrier is injected from the conducting channel in the silicon substrate into the gate dielectric when it gains sufficient kinetic energy. Injected carriers that do not get trapped in the gate oxide become gate current. Over prolonged periods, the presence of such mobile carriers in the oxides can lead to deviations of device parameters such as the threshold voltage V_{th}.

D. Time-dependent dielectric breakdown (TDDB)

The Time-Dependent Dielectric Breakdown (TDDB) is a failure mechanism in MOS devices, when the gate oxide breaks down as a result of long-time application of relatively low electric field. The breakdown is caused by formation of a conducting path through the gate oxide to substrate due to electron tunneling current, when MOS devices are operated close to or beyond their specified operating voltages.

E. Impact on Integrated Circuits

To conclude this section, electromigration and TDDB are stochastic failure mechanisms. From a reliability perspective, they are modeled as time-to-fail. From a statistical perspective, this means they are non-parametric. The reliability physicist sets a parametric fail criteria for these mechanisms and then analyzes the fail fractions. Aging on these failure mechanisms generally show catastrophic failure modes at the device primary outputs. These are either hard failures or drastic performance shift at a point in time.

On the other hand, NBTI, PBTI and HCI are parametric degradations that generally drift gradually and continuously over time. The degradation impact can be captured and modeled in SPICE. As the transistor ages, one can observe the primary outputs also shift gradually over time.

As discussed in the introduction, existing practices to identify counterfeit ICs are costly and time-consuming. In the next section, we will show a novel low-cost approach to efficiently identify counterfeit ICs.

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. 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. Each measurement is characterized by its acceptable interval $m_j = (m_{jl}, m_{jh})$, $j = 1, \ldots, d$, that is, the acceptability region for all considered measurements is $A = [m_{1l}, m_{1h}] \times \cdots \times [m_{dl}, m_{dh}]$. Only devices which

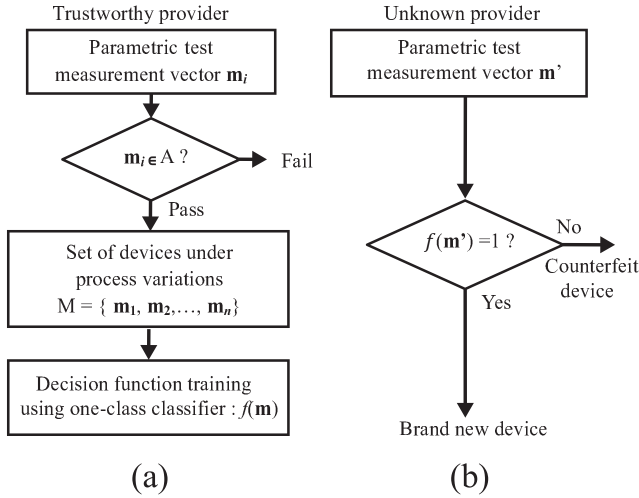

Fig. 1. Proposed flow for counterfeit IC identification: (a) training of the one-class classifier and (b) identification of devices from unknown provider.

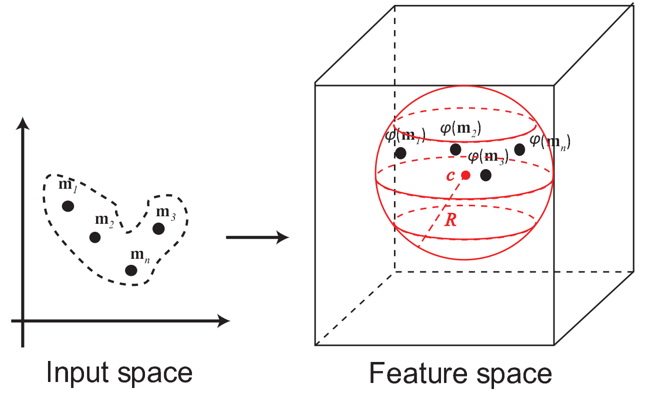

Fig. 2. One-class SVM.

contain no defect or excessive process variations, i.e., devices with $\mathbf{m} \in A$, 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) [9] 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

The 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 [9], 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:

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

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 [9]. 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 $z \geq 0$ and -1 otherwise. Via the freedom to use different types of kernel functions, this space transformation corresponds to a variety of nonlinear estimators in input space [9]. In other words, we are able to separate highly non-linear data in input space using kernel space transformation, regardless their distribution form. Intuitively, the optimization algorithm in (4) consists of finding the smallest sphere that all the training data live on.

Since it is difficult to solve the optimization problem in (4), one can also solve this problem by introducing Lagrange multipliers α, which leads to the following dual optimization problem (we omit the derivation for brevity)

$$\begin{aligned}\text{minimize} \quad & \sum_{ij} \alpha_i \alpha_j \Phi^T(\mathbf{m}_i)\Phi(\mathbf{m}_j) - \sum_i \alpha_i \Phi^T(\mathbf{m}_i)\Phi(\mathbf{m}_i) \\ \text{subject to} \quad & 0 \le \alpha_i \le \frac{1}{\nu n}, \sum_i \alpha_i = 1\end{aligned} \tag{6}$$

and the solution

$$c = \sum_i \alpha_i \Phi(\mathbf{m}_i), \tag{7}$$

can be used to compute the decision function defined in (5). By substituting (5), (7), we obtain

$$\begin{aligned}f(\mathbf{m}') = \operatorname{sgn}(R^2 - (\Phi^T(\mathbf{m}')\Phi(\mathbf{m}') - 2\sum_i \alpha_i \Phi^T(\mathbf{m}_i)\Phi(\mathbf{m}') \\ + \sum_{ij} \alpha_i \alpha_j \Phi^T(\mathbf{m}_i)\Phi(\mathbf{m}_j))\end{aligned} \tag{8}$$

Crucially, Equation (6) and (8) are formed as a function of inner product $\Phi^T(\mathbf{m}_i) \cdot \Phi(\mathbf{m}_j)$, permitting us to leverage the kernel trick and express (6) and (8) as a function of kernel function $k(\mathbf{m}_i, \mathbf{m}_j)$

$$k(\mathbf{m}_i, \mathbf{m}_j) = (\Phi^T(\mathbf{m}_i) \cdot \Phi(\mathbf{m}_j)) \tag{9}$$

In other words, the optimization algorithm for training and the decision function for a new point $\mathbf{m}'$ in feature space can be expressed as a function of points in input space using the kernel function. Among a variety of kernels, the most prevalent is the squared exponential, also known as the radial basis function kernel. In this work, we employed a radial basis function kernel

$$k(\mathbf{m}_i, \mathbf{m}_j) = \exp(-\gamma |\mathbf{m}_i - \mathbf{m}_j|^2) \tag{10}$$

where γ is some characteristic length-scale of the radial basis function kernel. Employing this kernel is equivalent to training a classifier with an infinite-dimensional feature space.

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 (8) to a group decision function $f(M')$, where M' denotes a set of devices under authentication:

$$M' = \{\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_{n'}\} \tag{11}$$

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

$$f(M') = \operatorname{sgn}(\sum_{i=1}^{n'} I_1^i) \tag{12}$$

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 [10].

D. Data normalization

It should be noted that two different measurements can take ranges of values that differ by many orders of magnitude. Thus, in the training and validation stage of the classifier, the measurement vector $\mathbf{m}$ should be normalized to have similar mean and variance for $m_i, i = 1, \ldots, d$, such that we avoid having the classification result being dominated by a few measurements while being practically insensitive to variations in the rest of the measurements. In this work, we chose to scale each measurement in $\mathbf{m}$ to have 0 mean and 1 variance. In the rest of paper, we keep the notation of (1), however the reader should be aware that the measurement pattern is assumed to be normalized.

IV. CASE STUDY

In this section, we demonstrate our approach on two industrial case studies produced in high-volume.

A. Case study 1

The first case study involves two parametric test measurements, namely $\mathbf{m} = [m_1, m_2]$, considered for 35 devices randomly chosen from different lots to train and validate the classifier. The same devices are then passed through the burn-in test in which we applied higher voltage and temperature values to accelerate the aging mechanisms. It should be noted again that these test measurements are 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 7 different time points: $t = t_0, t_1, \ldots, t_6$ [1]. Time points are approximately log time based since aging degradations such as NBTI exhibit logarithmic dependence on time [3]. The measurements taken from time point $t = t_0$ are served as brand new devices to train the classifier, and devices at $t \neq t_0$ are served as counterfeit IC patterns to be identified.

Figure 3 shows the projection the devices at $t = t_0, t_1, t_6$ onto the 2-dimensional normalized measurement space, shown by squares, solid dots and plus signs, respectively. It can be observed from Figure 3 an obvious measurement shift when t increases. Despite of the overlap between groups of measurements with different t, the mode/median are statistically different and follow the aging degradation physics. The test set-up has the resolution to about 10mV in the flows. So, the data is not convoluted by gauge repeatability and reproducibility issues.

[1]Exact hours are not shown here due to industrial confidentiality

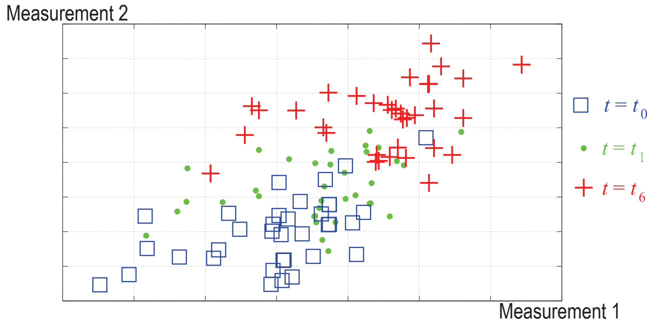

Fig. 3. Projection of devices at $t = t_0, t_1, t_6$, shown by squares, solid dots and plus signs,.

TABLE I
CLASSIFICATION RATE FOR CASE STUDY 1 AT DIFFERENT TIME POINTS.

Group\ Validation size	t_0	t_1	t_2	t_3	t_4	t_5	t_6
17	100%	0%	100%	100%	100%	100%	100%
8	100%	20%	50%	80%	100%	100%	100%
4	100%	20%	50%	70%	80%	100%	100%
2	90%	10%	50%	70%	80%	90%	100%
1	80%	30%	90%	80%	40%	80%	100%

The following data sets are used to train and validate the one-class SVM:

- The set S_t contains 18 devices randomly chosen from the 35 devices at $t = t_0$. S_t is used to train the classifier.
- The set S_v contains 7 subsets $\{S_{v0}, S_{v1}, \ldots, s_{v6}\}$, corresponding to 35-18=17 other devices at $t = t_0, \ldots, t_6$, respectively. Thus, S_v contains $17 \times 7 = 119$ devices and is used to validate the classifier.

In this experiment, we used the $LIBSVM$ [11] as classification tool to implement the one-class SVM proposed in [9]. We assigned the default values $\nu = 0.1$ and $\xi = 0.001$. The second line of Table I shows the classification rate computed using the group decision function defined in (12) for all subsets of S_v: $\{S_{v0}, \ldots, S_{v6}\}$, where 100% denotes a correct classification and 0% denotes an erroneous classification. It can be observed that the only misclassification occurs at $t = t_1$, where the group S_{v1} is classified as brand new group at $t = t_0$. This is mainly due to the large overlap region between groups S_{v0} and S_{v1}, as can be seen in Fig. 3. More measurements are needed to further distinguish S_{v0} and S_{v1}.

It is also worthwhile to compute the classification results while the size of validation set decreases. The question that arises is: how small a group of devices under authentication can be, to be correctly identified by the classifier? We have evaluated the classification results for reduced validation size to address this question. The following data are generated:

Step 1 s samples (s <17) are randomly chosen from each of the validation sets S_{vi}, $i = 0, \ldots, 6$ and let I_2 denote the classification accuracy indicator where 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}, $i = 0, \ldots, 6$ is computed as

$$C_{vi} = \sum_{k=1}^{r} I_2^k \tag{13}$$

where C_{vi} denotes the classification rate of the i-th time point. The 3rd to 6th lines in Table I show the classification results computed by (13) with the validation size s = 8, 4, 2, 1, respectively, and r=10. It can be observed from Table I that 1) as we reduce the validation set size, the classification rate degrades, 2) when the validation time point $t \neq t_0$, the classification rate is better for larger t, e.g., all devices at $t = t_6$ are distinguishable from $t = t_0$. These observations can be further justified by observing Fig. 3, the performance degradations are more pronounced as we increase the burning-in test time, which makes the validation set more distinguishable from the brand new devices at $t = t_0$. As a consequence, the devices at $t = t_6$ are totally separable from brand new devices at $t = t_0$ and 3) the classification rate turned out not to be satisfactory for some cases such as $t = t_1$. The main reason for these poor results is the tested time-points for these devices are very close to t_0. As a consequence, these devices are not distinguishable from the brand new devices using the actual measurements. We chose nevertheless to include them in the analysis, in order to show the limitations of the approach, and demonstrate the potential extensions for classification improvement, as will be shown in the next case study.

B. Case study 2

The second case study involves 49 parametric test measurements considered for 313 devices randomly chosen from different lots, i.e. , $\mathbf{m} = [m_1, \ldots, m_{49}]$. The same measurements are taken for 5 different time points: $t_0, \ldots, t_4$, corresponding to the first 5 time points in the previous case study.

Since we have a high data dimensionality d for this case study (d = 49), 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 4 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. As before, performance degradation caused by aging mechanisms is accelerated during the burn-in test and it can be readily observed in Figure 4.

As before, 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 $t = t_0, \ldots, t_4$,

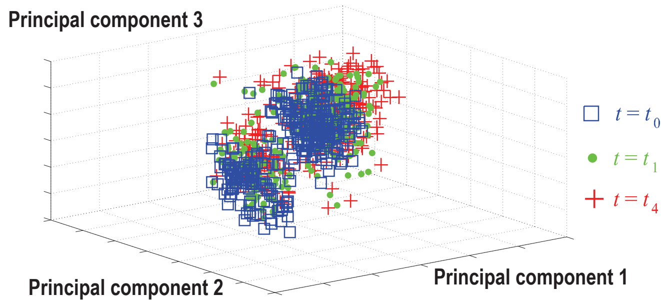

Fig. 4. Projection of the first three principal components of devices at $t = t_0, t_1, t_4$, shown by the squares, solid circles and plus signs, respectively.

TABLE II
CLASSIFICATION RATE FOR CASE STUDY 2 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%	100%	100%	100%	100%
10	100%	100%	100%	100%	100%
1	80%	60%	80%	100%	80%

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

The second line of Table II shows the classification rate computed using the group decision function defined in (12) 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 II that all subsets of S_v are correctly classified with a 100% classification rate. This shows that by adding more measurements sensitive to aging degradation and considering more devices to train the classifier, we can efficiently improve the classification capability of the classifier.

We generate similarly as in the previous case study 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 as in the previous case study.

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 by (13)

The 3rd to 6th lines in Table II show the classification results computed by (13) when the validation size s = 80, 20, 10,1, respectively, and r=10. Based on the classification rate shown in Table II, our observations are the following: 1) By adding more measurements in training the classifier, we can further improve the classification capability. 2) 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 to assign a group of devices under authentication to the class $t = t_0$ or to $t \neq t_0$. 3) The size of validation group can be as small as 10 devices. However, we cannot distinguish individual devices (see the last line of Table II). 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. CONCLUSIONS

In this paper, we presented a low-cost method to detect counterfeit ICs from brand new ones by employing a one-class SVM classifier. The classifier is trained using only parametric measurements of brand new devices in production, and is validated through industrial data from burn-in test analysis that is performed in a typical production EFR evaluation to mimic aging degradation over time. No additional costs are incurred for identification. The experimental results show an excellent ability to identify counterfeit parts sold as new from previously used parts. In particular, with several parametric measurements, we are able to identify a group of potential counterfeit ICs as small as 10.

VI. ACKNOWLEDGEMENTS

This work is partially supported by the National Science Foundation (NSF 1149465) and the Army Research Office (ARO W911NF-12-1-0091). The authors would also like to thank Texas Instruments Inc. for providing the data on which this study was performed.

REFERENCES

[1] J. M. Carulli and T. J. Anderson, "Test connections - trying application to process," in *IEEE International Test Conference*, 2005, pp. 679–686.
[2] J. M. Carulli and T. J. Anderson, "The impact of multiple failure modes on estimating product field reliability," *IEEE International Test Conference*, vol. 23, no. 2, pp. 118–126, 2006.
[3] A. Krishnan W. Bosch V. Reddy, J. M. Carulli and B. Burgess, "Impact of negative bias temperature instability on product parametric drift," in *IEEE International Test Conference*, 2004, pp. 148 – 155.
[4] C. Hu, "IC reliability simulation," *IEEE Journal of Solid-State Circuits*, vol. 27, no. 3, pp. 241–246, 1992.
[5] 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.
[6] "Detection of counterfeit electronic components," *http://www.aeri.com/detection-of-counterfeit.asp*.
[7] K. Chatterjee and D. Das, "Semiconductor manufacturers' efforts to improve trust in the electronic part supply chain," *IEEE Trans. Compon. Packag. Technol.*, vol. 30, no. 3, pp. 547–549, 2007.
[8] A.T. Krishnan, C. Chancellor, S. Chakravarthi, P.E. Nicollian, V. Reddy, A. Varghese, R.B. Khamankar, and S. Krishnan, "Material dependence of hydrogen diffusion: implications for NBTI degradation," in *IEEE International Electron Devices Meeting, Technical Digest*, 2005, pp. 691–694.
[9] 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.
[10] C.W. Hsu and C.J. Lin, "A comparison of methods for multi-class support vector machines," *IEEE Transactions on Neural Networks*, vol. 13, no. 2, pp. 415–425, 2002.
[11] C. C. Chang and C.J. Lin, "LIBSVM: A library for support vector machines," *ACM Transactions on Intelligent Systems and Technology*, vol. 2, pp. 1–27, 2011, Software available at http://www.csie.ntu.edu.tw/ cjlin/libsvm.