PAPER Special Section on Circuits and Systems

Cost-Efficient Recycled FPGA Detection through Statistical Performance Characterization Framework

Foisal AHMED[†a)], ***Nonmember***, **Michihiro SHINTANI**[†], ***Member***, ***and*** **Michiko INOUE**[†], ***Fellow***

SUMMARY Analyzing aging-induced delay degradations of ring oscillators (ROs) is an effective way to detect recycled field-programmable gate arrays (FPGAs). However, it requires a large number of RO measurements for all FPGAs before shipping, which increases the measurement costs. We propose a cost-efficient recycled FPGA detection method using a statistical performance characterization technique called virtual probe (VP) based on compressed sensing. The VP technique enables the accurate prediction of the spatial process variation of RO frequencies on a die by using a very small number of sample RO measurements. Using the predicted frequency variation as a supervisor, the machine-learning model classifies target FPGAs as either recycled or fresh. Through experiments conducted using 50 commercial FPGAs, we demonstrate that the proposed method achieves 90% cost reduction for RO measurements while preserving the detection accuracy. Furthermore, a one-class support vector machine algorithm was used to classify target FPGAs with around 94% detection accuracy.

key words: *field-programmable gate array (FPGA), recycled FPGA detection, compressed sensing, FPGA fingerprinting*

1. Introduction

With the continuous expansion of the IC supply chain, counterfeit electronic components are becoming a global threat owing to the influence of the global economy. Presently, in addition to causing financial losses to IC manufacturing companies, counterfeit ICs also lead to vulnerabilities in critical applications such as automobile, medical, and communication systems. Counterfeit ICs can be classified as recycled, remarks, overproduced, defective, cloned, etc. Among them, recycled components are the most prevalent ones and more than 80% of counterfeit components are recycled; that is, they have previously been used as components as reported in [1]. Field-programmable gate arrays (FPGAs) are now widely used because of their promising benefits such as low development cost and short time-to-market, thus, even recycled FPGAs are repeatedly used owing to today's complex electronics supply chain [2]. Because of their prior usage, recycled FPGAs increase reliability risks, and their performance degrades over time. It is a challenging and costly task to prevent this kind of infiltration in critical applications.

Several researche works aim to detect recycled FPGAs efficiently. Ring oscillator (RO) based delay information has been used to identify recycled FPGAs in [3]–[5]. Recycled FPGA RO frequencies are degraded owing to usage when compared to a fresh FPGA [6], [7]. A one-class support vector machine (SVM) [8] is used as a fresh/aged classifier compared to known fresh FPGAs [3], [5]. In [4], [5], the ROs are designed individually in all logic blocks. The extracted measured frequencies from the ROs represent the spatial process variation [9], [10] as a unique fingerprint (FP). In [5], machine-learning model is effectively applied to detect recycled FPGAs using the FPs through within-die process variation modeling. Although conventional methods detect recycled FPGAs effectively, many measurements of the ROs are required to exhaustively capture the aging effect, and this is unrealistic in terms of measurement time and cost.

In this paper, we propose a novel recycled FPGA detection method with a low measurement cost without losing the detection accuracy. This method exploits recent advancements in statistics [11], [12] and semiconductor characterization for the development of a low-cost silicon testing and characterization technique, called *virtual probe* (VP) [13]. In the proposed method, very few sample frequency measurements are conducted compared to the conventional FP technique. The VP technique then predicts the spatial variation of frequencies on the FPGA, i.e., the FP, based on a few sampled frequencies. The machine-learning algorithm trains a model using the predicted frequencies to detect recycled FPGAs. The VP technique utilizes the sparsity of frequency-domain components on the spatial process variation for the prediction. As the process variation on an FPGA gradually changes [14], [15], its high-frequency components are almost zero. Hence, the VP technique can be incorporated into the fingerprinting technique with remarkable affinity. Through experiments of the silicon measurements using 50 commercial FPGAs, the effectiveness of the proposed method is evaluated on the basis of various samples of measured frequencies.

The main contribution of this study is summarized as follows:

- The proposed method for detecting recycled FPGAs utilizes the VP technique to reduce the number of the RO characterizations in the fingerprinting.
- Silicon measurement results of 50 commercial FPGAs confirm that the VP technique successfully estimates the spatial variation on the FPGAs with a prediction error of 1.4% using only 10% samples.
- Based on frequencies predicted using the VP technique, the recycled FPGAs are detected using a

Manuscript received November 28, 2019.
Manuscript revised March 28, 2020.

[†]The authors are with Nara Institute of Science and Technology (NAIST), Ikoma-shi, 630-0192 Japan.
a) E-mail: ahmed.foisal.ab0@is.naist.jp

DOI: 10.1587/transfun.2019KEP0014

machine-learning algorithm with more than 94% detection accuracy using only 10% samplings while keeping the degradation of the accuracy only 2% compared to the conventional method based on the full FP measurement.

The remainder of this paper is organized as follows. In Sect. 2, preliminaries including the conventional recycled FPGA detection methods and the VP technique are introduced. Section 3 describes the VP-based recycled FPGA detection method. The experimental procedure and results of the silicon measurement are discussed in Sect. 4. Finally, we conclude our paper in Sect. 5.

2. Preliminaries

2.1 Recycled FPGA Detection

Figure 1 shows the flow of the recycled FPGA detection method proposed in [3] where the existence of golden FPGAs is assumed. It consists of the following three steps. (1) Multiple ROs are constructed on all the golden FPGAs and measured by the manufacturer. Recycled FPGA detection is formulated as an outlier detection problem to classify the FPGAs under testing (FUTs) into fresh or aged (recycled) FPGAs. Subsequently, the measured frequencies are used as feature vectors for machine learning. Here, if the feature vector size is too large to successfully converge the training, principle component analysis (PCA) [16] is conducted to reduce the feature size. (2) On the user side, before an FUT is implemented into a system, frequencies of ROs are measured in the same manner as the RO measurement of step (1). Then, the measured frequencies are sent to the manufacturer to identify whether the FUT is fresh or not. (3) The frequencies obtained in step (2) are fed to the trained model to test the FUT. If the FUT is previously used, some RO frequencies will degrade owing to the aging mechanisms including bias temperature instability (BTI) and hot carrier injection (HCI) [17], [18]. Finally, the machine-learning model returns the classification result to the user.

It is noted that the size of all test data is very small (36 KB for a modern commercial FPGA) and it is not costly to send test data to the manufacturer for the further verification. Furthermore, over 99% of the test data can be reduced by applying the feature engineering method proposed in [5]. Thus, the additional cost is virtually negligible for the user.

Figure 2 shows the general architecture of an FPGA. The discussion of the FPGA internal architecture is important to properly describe previous works. Basically, an FPGA is composed of an array of configurable logic blocks (CLBs) and programmable logic switches with interconnections. FPGAs can implement any logic function by appropriately configuring the look-up tables (LUTs). Figure 2 also simply shows the implementation of the i-stage RO structure as an example. By connecting multiple LUTs, multiple stage ROs can be designed in a CLB.

To enhance detection accuracy, a fingerprinting method

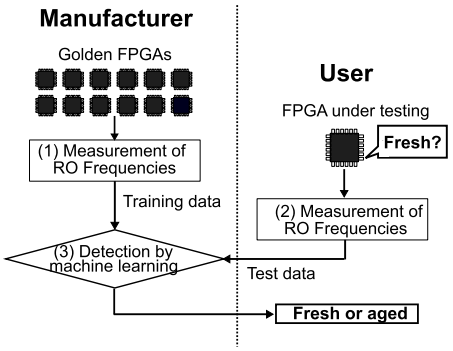


Fig. 1 Flow of the conventional recycled FPGA detection [3].

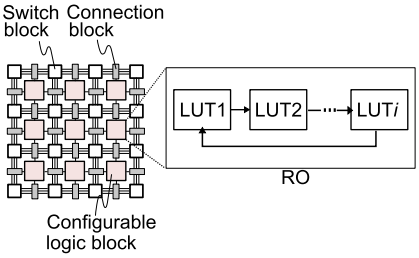


Fig. 2 Basic architecture of FPGA and LUT-based i-stage RO.

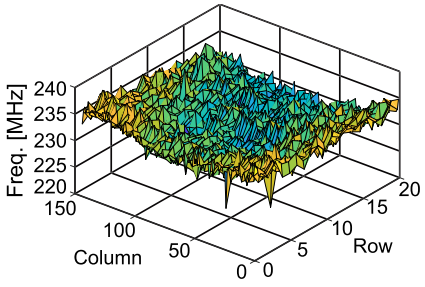


Fig. 3 Example of the FP using a commercial FPGA. The frequencies of all the CLBs are shown using the grid information in the FPGA.

has been applied in [4], [5]. The method is also based on the concept of [3] where RO-based measurements are conducted for the golden FPGAs. In [3], only a few numbers of CLBs in the FPGAs are covered in the recycled FPGA detection. As modern FPGAs consist of huge numbers of CLBs, it could fail to detect recycled FPGAs if the measured CLBs are not appropriately selected. In [4], all the CLBs were used to create the FP of each FPGA to represent a unique pattern of spatial frequency variation as shown in Fig. 3. As the FPs differ each FPGA, it can be a feature vector in the recycled FPGA classification.

Note that, in the RO characterization, each RO should be measured individually to avoid power or signal interference from other ROs. It is obvious that detection accuracy highly depends on the number and location of the ROs. Thus, either the volume of the measurement data must be sufficient or the locations of the measured ROs should be widely distributed on the FPGA for effective fresh/aged classification; however, it imposes a huge measurement cost

on the manufacturers. In this work, a statistical performance characterization framework called VP technique is used to reduce the measurement time in the RO characterization.

2.2 Virtual Probe

VP is a technique based on compressed sensing and was originally developed for a low-cost wafer-level silicon characterization [13]. In the VP technique, a subset of chips is randomly selected on a wafer and tested; then, the performances of the other chips are predicted through a statistical algorithm using the information from the tested chips.

We denote $g(x, y)$ as the two-dimensional function of the performance metric g, such as frequency, resistance, and leakage current, where x and y are the position coordinate on a wafer and are labeled as $x \in \{1, 2, \cdots, P\}$ and $y \in \{1, 2, \cdots, Q\}$. The relationship between a performance metric and its frequency-domain component can be written by a discrete cosine transform (DCT) as follows:

$$\begin{aligned} G(u, v) \quad &= \sum_{x=1}^{P} \sum_{y=1}^{Q} \alpha_u \cdot \beta_v \cdot g(x, y) \\ &\cdot \cos \tfrac{\pi(2x-1)(u-1)}{2P} \cdot \cos \tfrac{\pi(2y-1)(v-1)}{2Q}, \end{aligned} \tag{1}$$

where

$$\alpha_u = \begin{cases} \sqrt{\frac{1}{P}} & (u = 1) \\ \sqrt{\frac{2}{P}} & (2 \le u \le P) \end{cases} \tag{2}$$

$$\beta_v = \begin{cases} \sqrt{\frac{1}{Q}} & (v = 1) \\ \sqrt{\frac{2}{Q}} & (2 \le v \le Q). \end{cases} \tag{3}$$

Here, $G(u, v)$ represents a set of the DCT coefficients, where $u \in \{1, 2, \cdots, P\}$ and $v \in \{1, 2, \cdots, Q\}$. Equivalently, using an inverse discrete cosine transform (IDCT), $g(x, y)$ can be represented as a linear combination as:

$$\begin{aligned} g(x, y) \quad &= \sum_{u=1}^{P} \sum_{v=1}^{Q} \alpha_u \cdot \beta_v \cdot G(u, v) \\ &\cdot \cos \tfrac{\pi(2x-1)(u-1)}{2P} \cdot \cos \tfrac{\pi(2y-1)(v-1)}{2Q}. \end{aligned} \tag{4}$$

Generally, it is trivial to uniquely determine $g(x, y)$, once the DCT coefficients $G(u, v)$ are known and vice versa. This problem can be mathematically constructed by a linear equation as follows:

$$\boldsymbol{A} \cdot \boldsymbol{s} = \boldsymbol{b}, \tag{5}$$

where

$$\boldsymbol{A} = \begin{bmatrix} A_{1,1,1} & A_{1,1,2} & A_{1,1,3} & \cdots & A_{1,P,Q} \\ A_{2,1,1} & A_{2,1,2} & A_{2,1,3} & \cdots & A_{2,P,Q} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ A_{M,1,1} & A_{M,1,2} & A_{M,1,3} & \cdots & A_{M,P,Q} \end{bmatrix}, \tag{6}$$

$$\begin{aligned} A_{m,u,v} &= \alpha_u \cdot \beta_v \cdot \cos \frac{\pi(2x_m - 1)(u - 1)}{2P} \\ &\cdot \cos \frac{\pi(2y_m - 1)(v - 1)}{2Q}, \end{aligned} \tag{7}$$

$$\boldsymbol{s} = [G(1,1) \quad G(1,2) \quad \cdots \quad G(P,Q)]^T, \tag{8}$$

and

$$\boldsymbol{b} = [g(x_1, y_1) \quad g(x_2, y_2) \quad \cdots \quad g(x_M, y_M)]^T. \tag{9}$$

To derive $g(x, y)$, the DCT coefficients $\boldsymbol{s}$ need to be determined using Eqs. (5) to (9). However, we are now considering the situation where the number of samples M, taken at some locations $\{(x_m, y_m);\ m = 1, 2, \cdots, M\}$, is much smaller than PQ, i.e., $M \ll PQ$. Hence, the determination of $\boldsymbol{s}$ is not easy, as Eq. (5) is an under-determined linear equation.

The VP technique determines $\boldsymbol{s}$ by assuming that it is sparse. As the systematic component of the process variation gradually changes over a wafer, the high-frequency components of the DCT coefficients approach zero [19]. Thus, the sparse representation assumption is reasonably supported in the wafer-level characterization. To find the sparse solution of $\boldsymbol{s}$, the optimization problem is formulated as:

$$\begin{aligned} &\underset{\boldsymbol{s}}{\text{minimize}} \quad \|\boldsymbol{s}\|_1 \\ &\text{subject to} \quad \boldsymbol{A} \cdot \boldsymbol{s} = \boldsymbol{b}, \end{aligned} \tag{10}$$

where $\|\boldsymbol{s}\|_1$ is the L_1-norm of the vector $\boldsymbol{s}$. Using convex optimization and linear programming, the feasible sparse solution can be obtained from Eq. (10). Although, the L_0-norm provides a more accurate solution than the L_1-norm, the optimization problem for the L_0-norm is NP-hard; hence, the L_1-norm is used to solve it practically using the VP technique. Finally, once the DCT coefficients $\boldsymbol{s}$ are obtained, the $\hat{g}(x, y)$, the prediction of g at (x, y), can be calculated by the IDCT as in Eq. (4).

Perfect recovery of the unknown coefficients s depends on the orthonormality of $\boldsymbol{A}$ and the sparsity of s. A sufficient condition to find the exact solution s is known as a RIP condition (the condition based on restricted isometric properties) [13]. Since the RIP condition has some computational difficulty to be directly applied, as a practical solution, it is also known that if s contains at most K ($K \ll PQ$) non-zeros and M measurements are randomly chosen where M is in the order of $O(K \cdot \log(PQ))$, the RIP condition is almost guaranteed. See [20] for more details.

3. Recycled FPGA Detection Using the Virtual Probe Technique

The proposed recycled FPGA detection method is still based on the conventional method shown in Fig. 1, and its flow is summarized in Fig. 4. Our aim is to reduce measurement costs for golden FPGAs while preventing the degradation of detection accuracy. For this purpose, we incorporate the VP technique into the recycled FPGA detection flow. As the performances of neighboring CLBs in FPGA are very similar [14], [15], the sparse assumption is strongly supported, and our expectations are high that the VP technique will work very well in our recycled FPGA detection process.

With this method, the fingerprinting measurement is assumed as with [4] to represent $g(x, y)$ using the grid information in the FPGA die, where the target performance g is

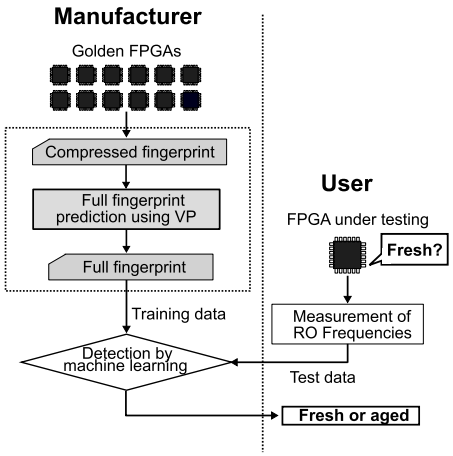


Fig. 4 Flow of the proposed recycled FPGA detection.

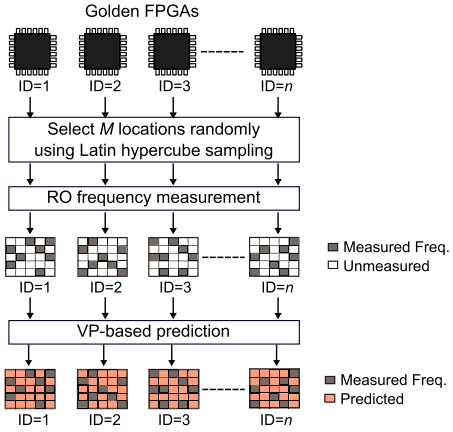


Fig. 5 Flow of the fingerprint generation through the VP technique.

the RO frequency. A single RO is designed in each CLB and placed in an array (x, y) using hardware macro modeling to keep the same internal routing and logic resources [21]. Unlike the conventional fingerprinting technique, small sampled, that is, *compressed*, RO measurements are conducted for M ROs, and the compressed measurement corresponds to $\boldsymbol{b}$ in Eq. (5). Before training the machine-learning algorithm, the FP is fully reconstructed, i.e., $\hat{g}(x, y)$ for all (x, y), and then the recycled FPGA classification is determined based on the fully reconstructed FPs.

The detailed flow of a portion of the VP technique in our recycled FPGA detection is illustrated in Fig. 5. Note that RO measurement and prediction are conducted independently in each golden FPGA. First, the VP technique starts to randomly select the M sampling locations for the small measurement. To accurately predict full FPs, matrix $\boldsymbol{A}$ needs to satisfy the RIP condition [13]. This means all the columns of $\boldsymbol{A}$ should be orthonormal. As matrix $\boldsymbol{A}$ is determined by the sampling locations shown in Eq. (6), if a set of bad samples is selected, $\boldsymbol{A}$ does not meet the RIP condition, and hence, a large prediction error occurs. For better random selection, we adopt Latin hypercube sampling [22] in this method, as was the case in [13]. In addition, since the most suitable $\boldsymbol{A}$ is different for each golden FPGA, the sampling locations should be adaptively determined for each one as shown in Fig. 5. Based on the discussion above, Eq. (5) can be rewritten as follows:

$$\boldsymbol{A}_n \cdot \boldsymbol{s}_n = \boldsymbol{b}_n, \tag{11}$$

where the subscript of each matrix and vector stands for n-th FPGA in the golden FPGA set. Next, the selected ROs are measured and the compressed FPs are constructed and stored in the database for further recycled FPGA detection. The full FP is predicted through the VP technique based on Eq. (11) as with Eq. (5). The reconstructed FPs $\hat{g}(x, y)$ are then fed to a machine-learning algorithm as training data.

Note that the VP technique is not applied to the FUTs on the user side. Though the golden FPGAs are thoroughly assumed to be fresh, the FUTs may contain recycled FPGAs. In recycled devices, all the CLBs are not always fully utilized. In that case, only the used LUTs will degrade, and the smooth change of the process variation on the die will not be observed. As a result, the sparse representation assumption is not satisfied, and the VP technique will fail to reconstruct, resulting in a large prediction error. Accordingly, the proposed method applies the VP technique only for the golden FPGAs.

We would like to note that the proposed method is to be applicable for a large number of FPGAs since the total measurement time is linearly changed as increasing the number of FPGAs. Also, the VP-based prediction can be conducted on a personal computer. Thus, the predictions for FPGAs can be performed parallelly by personal computers. Furthermore, our work utilizes the ML algorithm where a large number of training samples can be easily managed.

4. Experiments

To quantitatively evaluate the effectiveness of the methodology, we conducted experiments using 50 Xilinx Artix-7 FPGAs [23].

4.1 Measurement Setup

In the experiments using the FPGA devices, 7-stage ROs were designed using an XNOR based logic gate. We placed 3,964 ROs with the exception of the empty space in the layout through hardware macro modeling using the Xilinx CAD tool, Vivado [23], as shown in Fig. 6. Thus, a measured FP contains 3,964 RO frequencies. Figure 7 shows the frequency measurement system to make an FP that represents the spatial variation of the frequencies. Each CLB is configured by a single RO. A host computer controls to start the measurement through a joint test action group (JTAG) circuit. Each RO is activated by the selector and the counter circuit measures their frequencies individually. The measured frequency is then transferred to the computer. A universal asynchronous receiver-transmitter (UART) module is implemented as an interface between the FPGA and

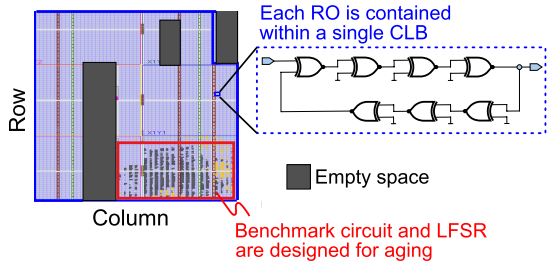


Fig. 6 An array of ROs in the Xilinx Artix-7 FPGA. A single RO is designed in a single CLB. For the aged FPGA, the benchmark and LFSR circuits are placed at the right-bottom corner.

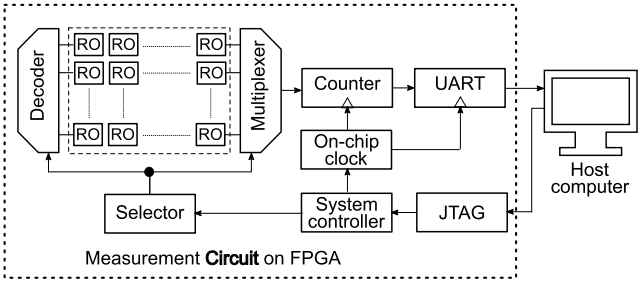


Fig. 7 Block diagram of a frequency measurement circuit for FPGA fingerprinting.

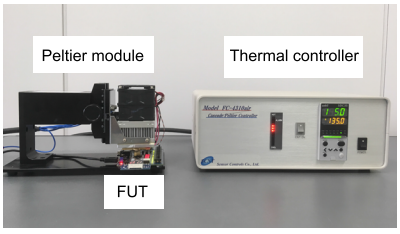


Fig. 8 Experimental setup for accelerating the aging process.

the computer with the Python programming language to collect measured frequencies and store them. After completing the measurements of all ROs, a unique FP is obtained representing the spatial correlation of the manufacturing process variation. We implemented this same measurement system on the 50 FPGAs, labeled as FPGA-01 to FPGA-50. All measurements are taken by the generated on-chip clock frequency with the help of the system clock frequency of 100 MHz.

A MATLAB software running in the same computer was used to apply the VP technique on the measured frequencies of the various sampling rates. In the machine learning-based recycled FPGA detection, a Python Scikit-learn library [24] was used to implement the machine learning algorithm.

Among the 50 FPGAs, only two FPGAs, FPGA-01 and FPGA-02, were aged and were used as recycled FPGAs. To accelerate the aging process, a Peltier module with a thermal controller was used as shown in Fig. 8 while running the s9234 benchmark circuit from the ISCAS'89 benchmark circuit [25]. Random workloads were fed to the circuit by

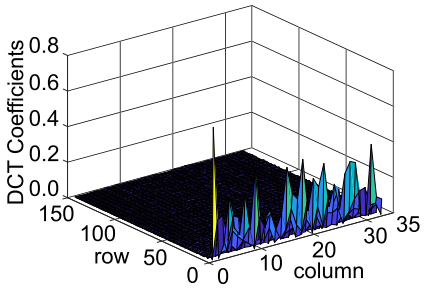


Fig. 9 DCT coefficients of frequency of the 3,964 ROs showing sparse representation. The coefficients values are normalized by L_1-norm.

a 16-bit linear feedback shift register (LFSR) at 100 MHz. The benchmark circuit and LFSR are placed at the bottom-right area as shown in Fig. 6. Both the FPGAs were heated up to 135 °C using the Peltier module and the random workload was used to achieve dynamic stress. We applied the aging stress to the two FPGAs for two days, after which all stresses were removed, and then FP measurements were conducted at room temperature. We applied the aging stress only for two days, after which all stresses were removed. Once the temperature of FPGA returns to a room temperature, measurements were conducted. It took approximately 10 minutes from removing the stresses to the FP measurement.

4.2 Results

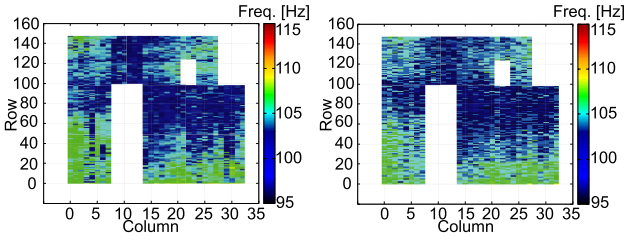
4.2.1 VP-Based Prediction

Figure 9 shows the frequency-domain components $G(u, v)$ obtained from $g(x, y)$ of fresh FPGA-01 by a DCT. It can be observed that a large number of DCT coefficients are close to zero. Thus, we can confirm that the sparsity of $G(u, v)$ is also observed in the FPGAs. This sparsity is the important condition for successfully applying the VP technique.

Figures 10 and 11 show the heat maps of the FPs of FPGA-01 and FPGA-02, respectively, when they are fresh. Though we show only the FPGA-01 and FPGA-02 results owing to page limitations, a similar trend was observed in the other FPGAs. Figures 10(a) and 11(a) show the heat maps of the fully-measured FP, i.e., when the VP technique is not applied. From the figures, we can see that the frequency distributions have a smooth change along the coordinates. The correlation coefficient (r) between the fully-measured of two FPs is found 0.66, where r is calculated using Pearson correlation coefficient as:

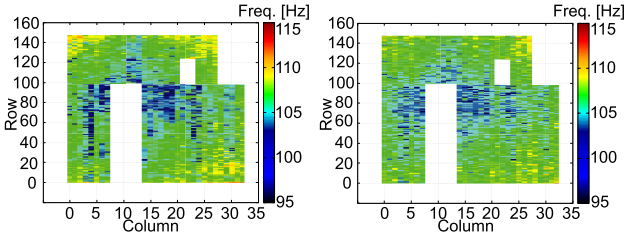
$$r = \frac{\sum_{x,y}(g_1(x,y) - \overline{g_1(x,y)})(g_2(x,y) - \overline{g_2(x,y)})}{\sqrt{\sum_{x,y}(g_1(x,y) - \overline{g_1(x,y)})^2 \sum_{x,y}(g_2(x,y) - \overline{g_2(x,y)})^2}}, \tag{12}$$

where $g_1(x, y)$ and $\overline{g_1(x, y)}$ are the frequency and mean of the frequency of FPGA-01 and $g_2(x, y)$ and $\overline{g_2(x, y)}$ are the



(a) Full measurement (b) Predicted by VP with 30% samples

Fig. 10 Heat maps of measured FP of fresh FPGA-01.



(a) Full measurement (b) Predicted by VP with 30% samples

Fig. 11 Heat maps of measured FP of fresh FPGA-02.

frequency and mean of the frequency of FPGA-02. From the correlation value, we can say that they are not highly correlated and can be used as FPs to identify them, as proposed in [4].

We applied the VP technique to the two FPs shown in Figs. 10(a) and 11(a). Figures 10(b) and 11(b) show the two predicted heat maps of the FPs of FPGA-01 and FPGA-02, respectively, where 30% sampling frequencies were used. Comparing Figs. 10 and 11, the relative error is found less than 1.2% between the fully-measured and predicted FPs. In the experiment, the relative error E between the correct frequencies $g(x, y)$ and the predicted $\hat{g}(x, y)$ is defined by:

$$E = \sqrt{\frac{\sum_{x,y}(g(x,y) - \hat{g}(x,y))^2}{\sum_{x,y}(g(x,y))^2}}. \tag{13}$$

Thus, it can be seen a good similarity between the fully-measured and predicted FPs. Using the VP technique, Fig. 12 similarly shows the same DCT sparsity with only 30% sampling of the frequencies for FPGA-01 shown in Fig. 10(a). Comparing Figs. 9 and 12, we notice that both the low-frequency and the high-frequency of the DCT coefficients are successfully captured even when the FP is reconstructed by the VP technique using only 30% frequency samplings.

Figure 13 shows the relative errors as a function of the spatial sampling rate of the 50 fresh FPGAs. The sampling results of the Latin hypercube sampling change at each trial owing to its randomness [22]; thus, the relative error E varies. In Fig. 13, the sampling results of 150 VP trials for each FPGA are shown, where FPGA-01 and others are shown separately. Here, note that the VP technique is not applied when the spatial sampling rate is 100%. In

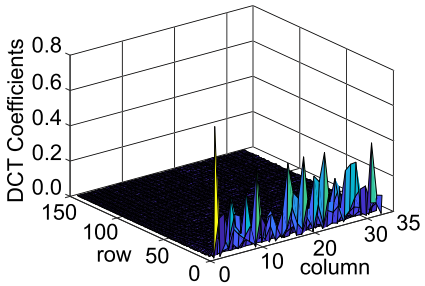


Fig. 12 Predicted DCT coefficients using 30% sampling frequencies of FPGA-01 also showing sparse representation.

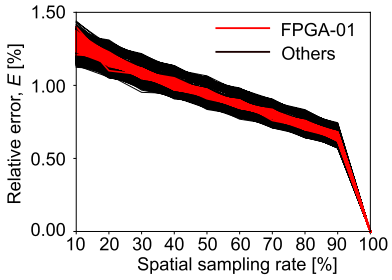


Fig. 13 Relative errors of the 50 fresh FPGAs for various sampling rates estimated by 150 trials.

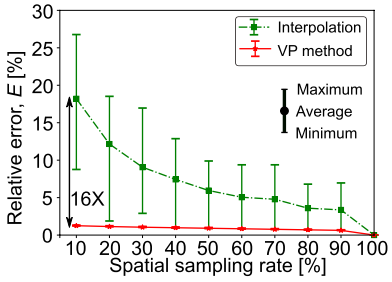


Fig. 14 Relative errors of different algorithm estimated by 150 trials to compare VP method.

Fig. 13, as spatial sampling rate increases, the relative errors decrease. It should also be noted that the variation in a single device, FPGA-01, is relatively small compared to the device-to-device variation of the relative errors. We also found that the relative error is less than 1.4% for all the fresh FPGAs and the entire spatial sampling rate. To compare VP with other method for estimating the FP, we applied a curve fitting based linear interpolation using similar sampling rate as our proposed work. Figure 14 shows the relative error calculated by Eq. (13) for both VP and curve fitting based linear interpolation repeated 150 trials. It is noted that VP achieves up to 16× error reduction than the curve fitting based linear interpolation. Based on the results, it is confirmed that the VP technique can efficiently and accurately recover the spatial variations of the fully measured FP using an extremely small data measurement sample.

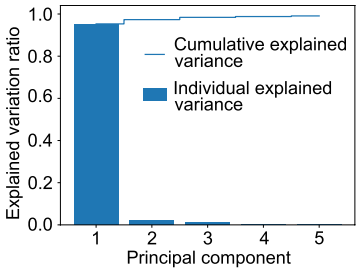


Fig. 15 Significant variations curve of PCA.

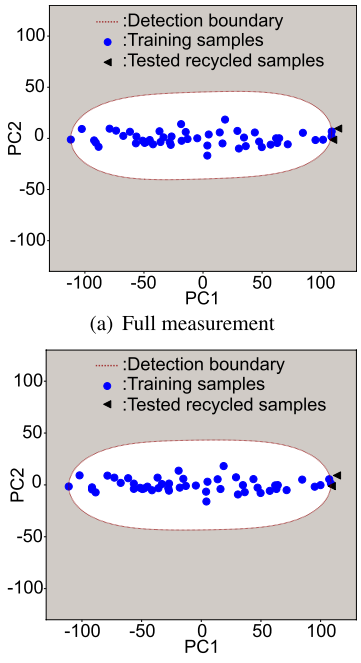
4.2.2 Recycled FPGA Detection

Next, we conducted recycled FPGA detection. The standard deviation of the frequencies of ROs of fresh FPGA-01 and FPGA-02 are 1.644 MHz and 1.664 MHz, respectively. The mean and standard deviation of the degradations of oscillation frequency for FPGA-01 are 0.78 MHz and 0.098 MHz and for FPGA-02 are 0.59 MHz and 0.078 MHz, respectively. That is, the level of degradation is within the variation of fresh FPGAs, and it is difficult to detect recycled FPGA only from such statistics. Therefore, we used one-class SVM as ML-based classification.

Before learning, we apply PCA to reduce the size of the feature vector as the 3,964 vectors are too numerous to efficiently train the model. PCA has also been used effectively in conventional recycled FPGA detection [3]. In this experiment, we use two principal components (PCs), PC1 and PC2, as a 98% significance variation is achieved using only the two PCs as shown in Fig. 15.

Then, we form the one-class decision boundary using the SVM on the basis of the two PCs in the recycled FPGA detection. Using a brute-force search, the hyper-parameters of the one-class SVM were selected to obtain better accuracy in the machine learning algorithm. We used 50 FPGAs, fresh FPGA-01 to FPGA-50, for training samples and 52 FPGAs, fresh FPGA-01 to FPGA-50 and two-day aged FPGA-01 and FPGA-02, for testing. Note that the measurements of fresh FPGA-01 to FPGA-50 for training and testing were separately conducted in order to consider the actual situation. Thus, the training and testing data are slightly different due to measurement error.

The predicted fresh FPs obtained from 30% sampling of frequencies were used to train the one-class SVM model to classify the testing samples. The detection boundary is formed to check only two recycled FPGAs as tested samples in Fig. 16, where the circle and triangle indicate training and testing samples, respectively. Figures 16(a) and 16(b) show the results of the conventional method and proposed method, respectively. As shown in Fig. 16(b), the decision boundary obtained from estimated training samples successfully classifies the recycled FPGAs the same as conventional methods using full measurement shown in Fig. 16(a). This shows the effectiveness of this method, which uses only a few measurements to correctly differentiate the recycled FPGAs from fresh ones.



(a) Full measurement

(b) Predicted by VP with 30% sampling

Fig. 16 Recycled FPGA detection boundary using one-class SVM. The PC1 and PC2 are used as a feature vector.

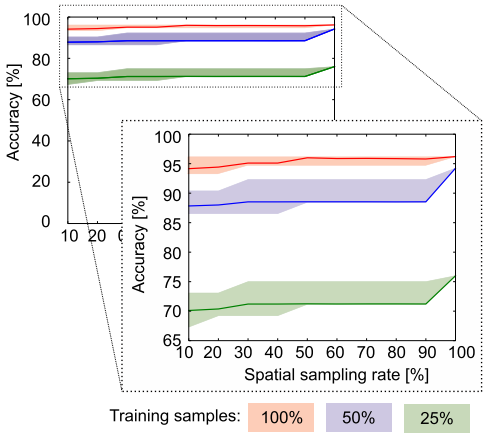


Fig. 17 Detection accuracy from different samples of the frequency estimated by 150 trials. Each line shows the detection results of different training samples.

Figure 17 shows the detection accuracy where the SVM model is trained by the predicted fresh FP using various samples of frequencies. We also change the training sample ratio to 100%, 50%, and 25%. In the figure, the detection accuracy score is calculated as follows:

$$\text{Accuracy} = \frac{\text{Number of correct predictions}}{\text{Total number of testing samples}}. \quad (14)$$

As the relative error changes based on sample locations, the detection accuracy varies owing to the randomness of the Latin hypercube sampling. In Fig. 17, the detection accuracies are shown as the functions of the spatial

sampling rate at various training sample ratios. The shaded regions stand for the variations when each experiment runs 150 times repeatedly to properly estimate accuracy. The upper and lower bounds of the shaded region represent the maximum and minimum accuracy of each sampling rate, respectively, and each line shows the average accuracy of the corresponding training sample. The figure shows detection accuracy improves as the number of training samples increases. At 100% training samples, we found a maximum of 96.15% accuracy in all of the sampling frequencies where at least 92.30% of the accuracy was achieved in only 10% of the samples. On average of 94.15% accuracy was obtained using only 10% samples frequencies at the 100% training samples which are nearly equal to accuracy using 100% sampling frequency. Detection accuracy higher than 90% is obtained when using more than 50% training samples. Thus, the proposed method can well recover full FP and detect recycled FPGAs using ML-based classification.

The most important observation from Fig. 17 is the small difference in detection accuracies for all training samples between the spatial sampling rates of 10% and 100%. More specifically, the detection accuracies at 10% and 100% spatial sampling rates are 94.15% and 96.15%, respectively, for 100% training samples, and although the RO measurement time was reduced by 90%, the decrease in detection accuracy is a negligibly small 2%. The total measurement time for each FPGA is reduced from 75 seconds to only 7.5 seconds at the 10% sampling rate. From the practical viewpoint of recycled FPGA detection using estimated FPs, both measurement cost and detection accuracy should be considered in choosing the sampling rate. From Fig. 17, it is observed that using 10% sampling rate although the measurement cost is very small but accuracy is less than the sampling rate 30%. As a final note, we can conclude that the proposed recycled FPGA detection method based on the VP technique reduces measurement time for FPGA manufacturing companies while maintaining high detection accuracy.

5. Conclusion

In this paper, we proposed a cost-effective recycled FPGA detection technique to efficiently estimate the spatial process variation from a very small frequency measurement sample. To achieve the small measurement, we utilized the VP technique originally proposed for low-cost wafer-level silicon characterization. This method can drastically minimize the cost of the measurements for golden FPGAs without losing the recycled FPGA detection accuracy. The results of the experiments, in which 50 commercially available FPGAs were used, demonstrate that the reconstruction error was smaller than 1.4% even though only 10% of the total sample frequencies were used in the VP technique for the reconstruction. Furthermore, based on the reconstructed frequencies, it was found that the one-class SVM successfully detects the recycled FPGAs with more than 94% detection accuracy, which is nearly equivalent to conventional methods, but utilizing only 10% sampled frequencies.

Acknowledgments

This work was partly supported by Telecommunications Advancement Foundation and JSPS KAKENHI Grant No. 18K18025.

References

[1] U. Guin, K. Huang, D. DiMase, M. Tehranipoor, and Y. Makris, "Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain," Proc. IEEE, vol.102, no.8, pp.1207–1228, 2014.
[2] M.M. Tehranipoor, U. Guin, and D. Forte, Counterfeit Integrated Circuits, Springer, 2015.
[3] H. Dogan, D. Forte, and M.M. Tehranipoor, "Aging analysis for recycled FPGA detection," Proc. IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems, pp.171–176, 2014.
[4] V. Jyothi, A. Poojari, R. Stern, and R. Karri, "Fingerprinting field programmable gate arrays," Proc. International Conference on Computer Design, pp.337–340, 2017.
[5] F. Ahmed, M. Shintani, and M. Inoue, "Feature engineering for recycled FPGA detection based on WID variation modeling," Proc. IEEE European Test Symposium, 2019.
[6] A. Amouri, F. Bruguier, S. Kiamehr, P. Benoit, L. Torres, and M. Tahoori, "Aging effects in FPGAs: An experimental analysis," Proc. International Conference on Field Programmable Logic and Applications, 2014.
[7] M. Slimani, K. Benkalaia, and L. Naviner, "Analysis of ageing effects on ARTIX7 XILINX FPGA," Microelectron. Reliab., vol.76, pp.168–173, 2017.
[8] B. Schölkopf, R. Williamson, A. Smola, J. Shawe-Taylor, and J. Platt, "Support vector method for novelty detection," Proc. Conference and Workshop on Neural Information Processing Systems, pp.582–588, 1999.
[9] Y. Pino, V. Jyothi, and M. French, "Intra-die process variation aware anomaly detection in FPGAs," Proc. IEEE International Test Conference, pp.1–6, 2014.
[10] H.Y. Wong, L. Cheng, Y. Lin, and L. He, "FPGA device and architecture evaluation considering process variations," Proc. IEEE/ACM International Conference on Computer-Aided Design, 2005.
[11] D.L. Donoho, "Compressed sensing," IEEE Trans. Inf. Theory, vol.52, no.4, pp.1289–1306, 2006.
[12] E.J. Candes and M.B. Wakin, "An introduction to compressive sampling," IEEE Signal Process. Mag., vol.25, no.2, pp.21–30, 2008.
[13] W. Zhang, X. Li, F. Liu, E. Acar, R.A. Rutenbar, and R.D. Blanton, "Virtual probe: A statistical framework for low-cost silicon characterization of nanoscale integrated circuits," IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol.30, no.7, pp.1814–1827, 2011.
[14] H. Yu, Q. Xu, and P.H. Leong, "Fine-grained characterization of process variation in FPGAs," Proc. International Conference on Field Programmable Technology, pp.138–145, 2010.
[15] T. Tuan, A. Lesea, C. Kingsley, and S. Trimberger, "Analysis of within-die process variation in 65 nm FPGAs," Proc. IEEE International Symposium on Quality Electronic Design, 2011.
[16] I.T. Jolliffe, Principal Component Analysis, Springer-Verlag, 1986.
[17] D. Lorenz, G. Georgakos, and U. Schlichtmann, "Aging analysis of circuit timing considering NBTI and HCI," Proc. IEEE International Symposium on On-Line Testing and Robust System Design, 2009.
[18] S. Kiamehr, A. Amouri, and M.B. Tahoori, "Investigation of NBTI and PBTI induced aging in different LUT implementations," Proc. International Conference on Field Programmable Technology, 2011.
[19] S. Ohkawa, M. Aoki, and H. Masuda, "Analysis and characterization of device variations in an LSI chip using an integrated device matrix array," IEEE Trans. Semicond. Manuf., vol.17, no.2, pp.155–165,

2004.
[20] E. Candes and J. Romberg, "Sparsity and incoherence in compressive sampling," Inverse Probl., vol.23, no.3, pp.969–985, 2007.
[21] D.P. Sahoo, R.S. Chakraborty, and D. Mukhopadhyay, "Towards ideal arbiter PUF design on Xilinx FPGA: A practitioner's perspectivequantitative and statistical performance evaluation," Proc. Euromicro Conference on Digital System Design, pp.559–562, 2015.
[22] B. Tang, "Orthogonal array-based latin hypercubes," J. Am. Stat. Assoc., vol.88, no.424, pp.1392–1397, 1991.
[23] Xilinx, Inc., 7 Series FPGAs Data Sheet: Overview. [Online: https://www.xilinx.com/support/documentation/data_sheets/ds180_7Series_Overview.pdf].
[24] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, D. Cournapeau, M. Brucher, M. Perrot, and E. Duchesnay, "Scikit-learn: Machine learning in Python," J. Machine Learning Research, vol.12, pp.2825–2830, 2011.
[25] F. Brglez, D. Bryan, and K. Koiminski, "Combinational profiles of sequential benchmark circuits," Proc. IEEE International Symposium on Circuits and Systems, pp.1930–1934, 1998.

Foisal Ahmed received B.E. degree from Prime University, Dhaka, in 2008; P.G.D. degree from Bangladesh University of Engineering and Technology (BUET), Dhaka, in 2014 and M.E. degree from Islamic University of Technology (IUT), Dhaka, Bangladesh, in 2016. Currently, he is pursuing a Ph.D. degree at the Graduate School of Information Science, Nara Institute of Science and Technology (NAIST), Japan. His research interests include counterfeit field programmable gate array (FPGA) detection, hardware security and reliability, very large scale integration (VLSI) testing, signal processing, and communications systems. He is a student member of IEEE.

Michihiro Shintani received B.E. and M.E. degrees from Hiroshima City University, Hiroshima, Japan, and a Ph.D. degree from Kyoto University, Kyoto, Japan, in 2003, 2005 and 2014, respectively. He was with Panasonic Corporation, Osaka, Japan, from 2005 to 2014, with Semiconductor Technology Academic Research Center (STARC), Yokohama, Japan, from 2008 to 2010, and with Kyoto University, Kyoto, Japan. In 2017, he joined the Graduate School of Information Science, Nara Institute of Science and Technology (NAIST), where he is currently an assistant professor. His research interests include reliability-aware LSI design, device modeling, and circuit simulation. He is a senior member of IEEE and member of the Institute of Electronics, Information and Communication Engineers (IEICE).

Michiko Inoue received her B.E., M.E., and Ph.D. degrees in Computer Science from Osaka University, Japan in 1987, 1989, and 1995 respectively. She worked at Fujitsu Laboratories Ltd. from 1989 to 1991. She is a Professor of Graduate School of Science and Technology, Nara institute of Science and Technology (NAIST). Her research interests include distributed algorithms, graph theory and dependability of digital systems. She is a member of Science Council of Japan, the Information Processing Society of Japan (IPSJ), and Japanese Society for Artificial Intelligence, a senior member of IEEE, and a fellow of the Institute of Electronics, Information and Communication Engineers (IEICE).