Creative and International Competitiveness Project (CICP) 2017 result report

Project name: FPGA Reliability and Security
Project Leader: Foisal Ahmed

1. Abstract (background & aim)

An FPGA is a customizable integrated circuit used to implement many logical functions like an application specific integrated circuit (ASIC) could perform. But due to the ability of reconfigurability and updating the functionality by an end user gives FPGA more advantages over ASIC. In some modern real-time applications like Advanced driver-assistance system (ADAS), IoT, stereo vision etc. make global FPGA market rapidly increasing and is now expected to be valued at USD 9.50 Billion in 2023 [1]. The global economic market has now reduced the cost of electronics due to growing large horizontal business model who offers low-cost fabrications. As like ASIC, FPGA vendors similarly design and develop FPGA in their own lab, but fabricate them in offshore countries. This trend in the supply chain makes the back door for the illicit market who instigate to attacks like counterfeiting, malicious activities or IP stealing in real design. Specifically, the problem of counterfeiting of IC is now major concern issue which drawn much attention to not only the media, industry but also government because of global counterfeited market increasing exponentially over the past decays. Figure 1 shows the most recent data provided by IHS where shows that counterfeited component have quadruple since 2009 [2].

The impact of counterfeited IC is more vulnerable in case of some critical applications like military devices, medical Equipment, nuclear plants etc. The U.S. Department of Commerce reported that over ten thousand occurrences relating recycled ICs itself than other types of counterfeited components [3]. Also in the Department of defense of U.S. claimed about counterfeited components in the supply chain [4]. Moreover, statistical reports show that FPGA is in the top five counterfeited electronic components [5]. Before going to the supply chain, FPGAs are varied in design, functionality and tested manufacturing faults like stuck-at-faults, open/short faults or missing components but not detect any counterfeiting. There are some existing researchs in counterfeiting but most of them concentrated on IC counterfeiting. In [6, 7], researchers used some techniques at recycled ASIC detection by using electrical tests and on chip-sensors. In [8], the path delay based method has been proposed to identify recycled where they discovered the increase in path delay by aging. In [9], used early failure rate analysis data and one class SVM (Support Vector Machine) method

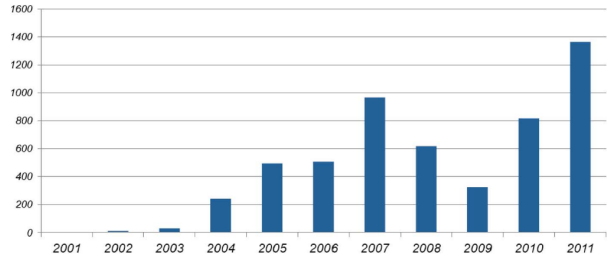

Figure 1: Counterfeit incidents reported by IHS [2].

to detect recycled data. For recycled FPGA detection, in [10] used exhaustively LUT path analysis by ring oscillator to collect an array of frequencies and using SVM and k-means clustering algorithm. But their research only concentrated on recycled FPGA detection where another counterfeiting not considered and measured value covered only part of the FPGA area. Another research [11] which has some similarity with our work used FPGA fingerprinting to identify counterfeiting in the supply chain. They have collected all FPGA fingerprint and stored it in authorized database before transferring them into the supply chain. The users compare their fingerprint using technological file provided by the company. We proposed a different technique where does not require all fingerprints of the FPGA of the same family. Instead, we have constructed a set of fingerprints using frequency distribution for an FPGA family and using machine learning technique we could classify the counterfeiting.

In this work, we proposed a non-destructive FPGA fingerprint approach to detect counterfeited FPGA. Due to intra-die process variation, each FPGA has a unique fingerprint which has some correlations with other members of FPGA fingerprint. By using this correlation, our technique requires just a few FPGA fingerprints for machine learning. The fingerprint methodology consists of the following steps:

1. Collect few FPGA randomly from a family of FPGA's on the same wafer after completing fabrication task.

2. After running functional test, collect frequencies from the different specific location using ring oscillator.

3. Use these frequencies to make the corresponding FPGA fingerprint.

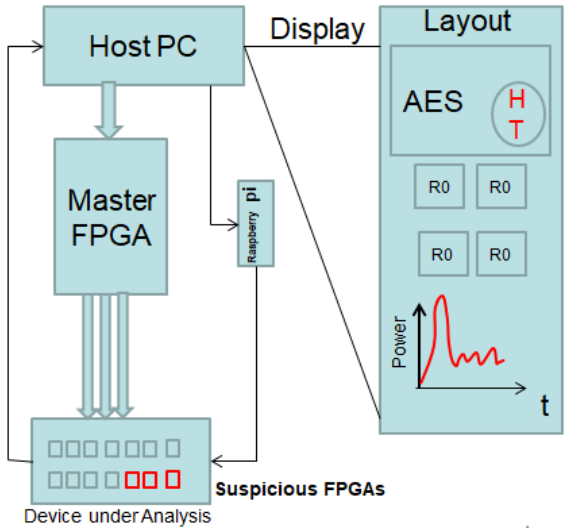

Figure 2: Initial proposed measurement environment.

4. Use machine learning approach to train using these FPGA fingerprints.

5. Select few other FPGA randomly from the same family for validation subjected to fingerprint taken from the same designated location of the FPGA.

The rest of report is organized as follows: The step by step progress of the project is described in Section II where details methodology also discussed. Experimental evaluation and result are presented in Section III. The future plan is described in Section IV and self-valuation report is given in Section V.

2. Project progress

As the progress of the project work is a continuous process, we describe it in following subsections:

1. Initial Proposal

2. Modified Proposal

3. Final Proposal

2.1. Initial Proposal

In the initial proposal, we have given a measuring environment shown in Fig. 2 for detecting recycled FPGA and Hardware Trojan. Where we have proposed Host PC, Master FPGA, Raspberry pi etc. modules for measuring system. Also machine learning technique had been proposed.

2.2. Modified Proposal

In the modified version of the proposal, we have included fingerprint concept in our design. The concept of

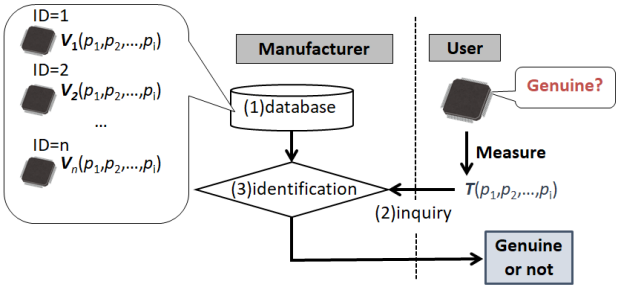

Figure 3: Modified version of the proposed technique.

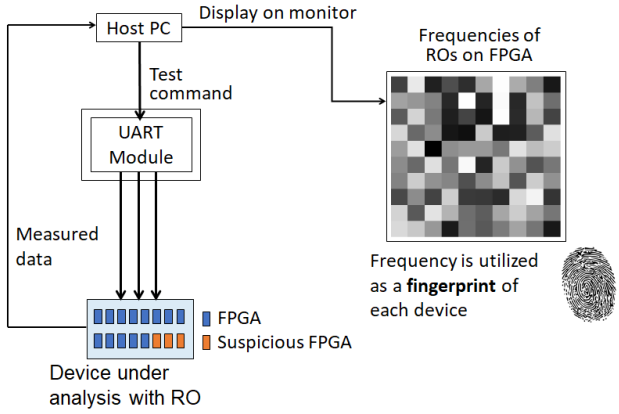

Figure 4: Final measurement system for our proposed Model.

a fingerprint is very modern and recent research [11]. We also modified our design model shown in Fig. 3 for detecting counterfeited FPGA using machine learning explicitly. Initially, we have planned in our project in detecting counterfeited FPGA where focused on reliability issue and also some part of the security issue as well. Because one of the types of counterfeiting is tempering the FPGA which is security concern also. This proposed model also able to detect tempered FPGA. Furthermore, using this same proposed model, detection of Hardware Trojan could also be possible, which is our future scope of this project work.

2.3. Final Proposal

After then, we have refined our model and completed the hardware setup. Figure 4 shown the final measuring system. In this final model, we have used UART module for transferring data from FPGA to Host PC. We used logistic regression algorithm for machine learning in our final proposed design.

2.4. Fingerprint methodology

For our proposed model, we have used fingerprint technique described in [11]. Due to intra-die process variation (PV), each FPGA device's has its own unique

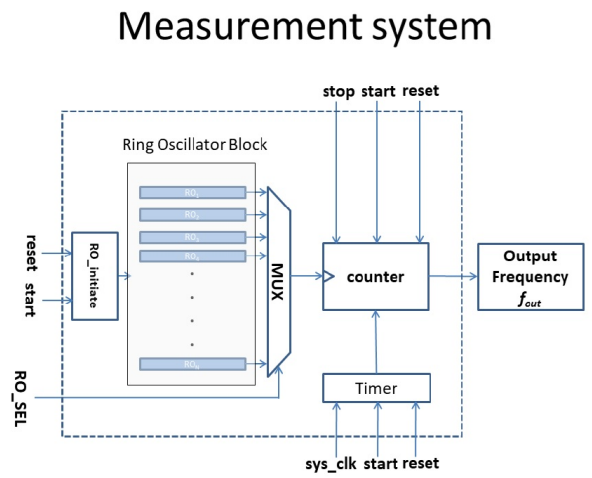

Figure 5: Frequency measurement system using RO for our proposed Model.

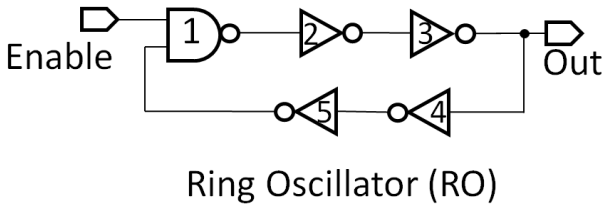

Figure 6: 5-stage Ring Oscillator (RO).

fingerprint which has some spatial correlation within the die of the various location of the FPGA. But this fingerprint has highly uncorrelated with other types of counterfeited FPGA like recycled, overproduced, tempered FPGA. In [12], Agarwal et al. presented a statistical timing analysis method to determine intra-die and inter-die variations and their spatial correlations. By motivating on that study we have assumed that the frequency of the different location of the FPGA board has the strong spatial correlation. Due to this spatial correlation, the fingerprint of the FPGA is unique than other devices of the family. As all the die within the wafer made at a time, so we can assume due to inter-die process variation they have also similar pattern but not exactly accurate fingerprint. We have incorporated this idea which is the different way of detecting counterfeiting and makes our technique faster.

2.4.1. Measurement setup

The FPGA fingerprints in this project are measured by using ring oscillators (ROs) which have been extensively used in many researchers [13]. Figure 5 shows the frequency measurement system using ROs of the different location of the FPGA. Each RO is created in one tile using two Look-up-tables (LUTs) placed in one single slice of the designated location. Only RO is moving to the various location of the FPGA such a way that total layout of the FPGA could be observed. Other routing, logic resources, and control information remains constant so that any difference in the frequency of various ROs are affected only due to manufacturing variations. The frequency of the RO is only dominated by the delays of LUTs used for RO and their interconnections between LUTs. The multiplexer is used for selecting specific RO to capture the frequency which is then transferred to counter for measuring frequency. The Timer is used for taking average frequency at specific duration. Only one RO is activated at a time for avoiding interferences. In this project work, 5-stage RO is used for frequency measurement shown in Fig. 6. After measured frequency from 200 different locations of the tile, we have made a fingerprint of the particular FPGA.

2.4.2. Counterfeited FPGA Classification

We presented in the previous section, how FPGA fingerprint is obtained from various FPGA using RO. Here, we discuss logistic regression (LR) model for detecting counterfeited FPGA. LR is a powerful machine learning algorithm for linear and binary classification problems widely used in many applications [14] [15]. In case of binary or dichotomous variables as true or false, LR is extensively used in the analysis of many problems [16]. In our work, dependent variables are genuine or counterfeited and the frequency of various locations are the features of independent variables. The goal of the LR is to estimate the probability p for linear combinations of the independent variables. The LR in a fingerprint-based counterfeited FPGA detection can be discussed as follows:

$$h_\theta(x) = \frac{1}{1+\exp(-(\theta^T x))} = \phi(z) \tag{1}$$

where $h_\theta(x)$ is the hypothesis of the decision boundary and $\phi(z)$ is logistic sigmoid function where

$$z = \theta^T x = \theta_0 x_0 + \theta_1 x_1 + \ldots\ldots + \theta_m x_m \tag{2}$$

And $p(y=1|x,\theta) = \phi(z)$ means the probability that the class $y=1$ (true) for a given input feature of x which is parameterized by θ and m is the total number of samples. For measuring cost function of LR, we used sum-squared-error cost function as follows:

$$J(\theta) = Cost(h_\theta(x^{(i)} - y^{(i)})) = \frac{1}{2}\sum_{i=1}^{m}(h_\theta(x^{(i)} - y^{(i)}))^2 \tag{3}$$

We used an optimization algorithm for minimizing cost function $J(\theta)$, called gradient descent algorithm.

$$J(\theta) = \frac{1}{m}[\sum_{i=1}^{m} y^{(i)} log h_\theta(x^{(i)}) + (1-y^{(i)}) log(1-h_\theta(x^{(i)}))] \tag{4}$$

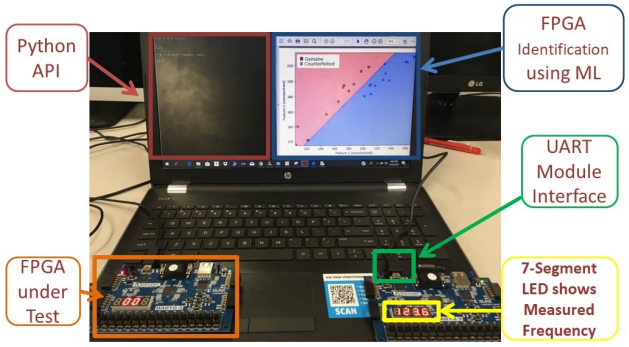

Figure 7: Demonstration of measurement system.

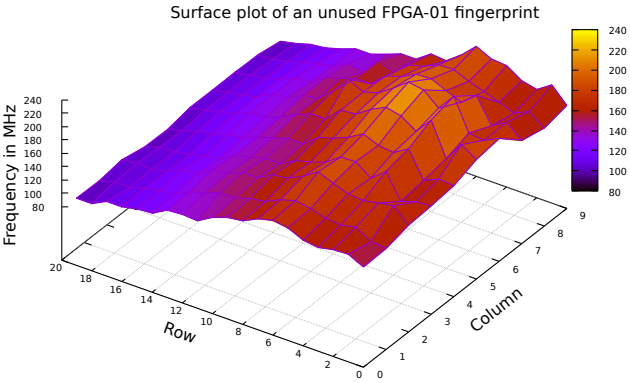

Figure 8: 3D surface plot showing measured frequency response (unused FPGA-1).

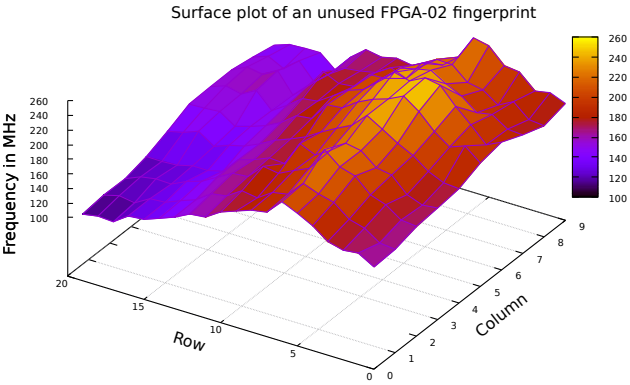

Figure 9: 3D surface plot showing measured frequency res-pose (unused FPGA-2).

3. Results

3.1. Experimental setup

In this project work, we have used NAND-INVERTER-NOR based RO of 5-stage in FPGA board. The Xilinx BASYS 3 board was used as unused and ZIBO board as counterfeited for this experiment [17]. Initially, for prototype design, we have implemented 200 ROs in each Xilinx Artix-7 FPGA chip of 28nm technology. Each RO is placed in one CLB unit. To avoid interference, only one RO is activated at a time. We have taken frequency from RO about the 10s period of time for getting an average value. The location of the RO was changed using Xilinx Design Constraint (XDC) file. All measurements were taken at the nominal supply voltage, room temperature and using on-board 100 MHz clock. Figure 7 shows the entire fingerprint measurement system. After collecting all frequency from ROs, we made fingerprint for each FPGA respectively. We used same techniques and approaches for all three unused FPGAs and one counterfeited FPGAs. Figure 8, Fig. 9 and Fig. 10 show two genuine (unused) and one counterfeited FPGAs respectively.

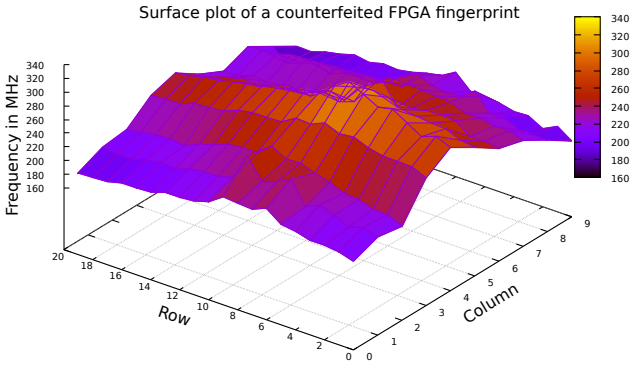

Figure 10: 3D surface plot showing measured frequency res-pose (counterfeited FPGA).

3.2. Discussion

As we discussed initially in the previous section, we have taken three unused FPGA fingerprint and one counterfeited FPGA fingerprint in our experiment. The two unused fingerprint in Fig. 8 and Fig. 9 look very similar pattern due to same manufacturing process variation. Although they have different intra-die process variation but the measured frequencies are within the range from 100 MHz to 260 MHz. Also, other unused FPGA have similar ranges of frequencies 100 MHZ to 280 MHz. Thus, from these observations, it can be said that it is not necessarily important to take all FPGAs fingerprint for a single wafer. Instead, few amounts of FPGA fingerprint within a wafer may potentially detect counterfeiting. Machine learning algorithms help in this regard efficiently. Our preliminary experiment shows very encouraging results in detection of counterfeited FPGA. Figure 10 shows the counterfeited fingerprint, the pattern is totally different than the unused fingerprint. The cause for this different pattern is mainly due to recycled or used or tempering or other counterfeited FPGA. For detecting unused or used FPGA, we have used logistic regression (LR) which we have discussed in preceding section. We used python tools for the detection mechanism and also selected another popular machine learning workbench

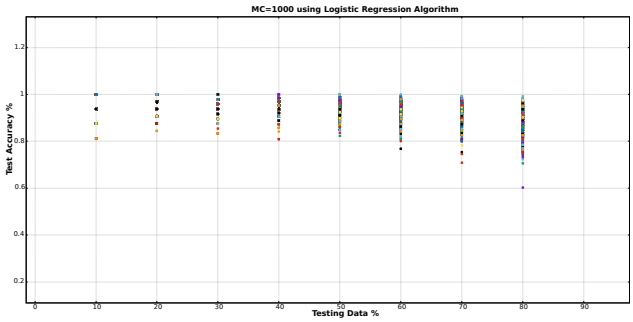

Figure 11: Accuracy of testing is changing as varying the percentages of testing data.

called WEKA [18] for training and testing our proposed technique.

For this prototype design, our number of FPGAs are very little. So, for analyzing the accuracy of our proposed method, we have arranged our total 200 locations data in such a way that each 5 locations data have assumed one single FPGA. Using this such arrangement, we have plotted accuracy of all data in terms of percentage of testing data. The 1000 Monte Carlo (MC) simulation results of using logistic regression algorithm is shown fig. 11 where we observe that most of the testing case our accuracy is more than 90%. The range of testing is from 0% to 80%. As the percentages of testing data increases, the variation of accuracy also increases because of decreasing training percentages. The average accuracy is more than 94%. Although, the number of tested FPGAs are very little but the obtained results are very promising. Because, in the manufacture, this technique not only detect the counterfeiting but also it makes detection very faster and efficient as well. The summery of statistical report and confusion matrix using WEKA tool are given in Table 1 and Table 2. The total number of the classified instance is 4 and the rate of correct classification is 100%. This ML report is only for counterfeited FPGA detection.

4. Future plans

In this research, we have done focused only counterfeited FPGA detection but what types of counterfeited it, we do not consider. But our preliminary results encourage us to extend this research work. The future scopes and plans are given followings:

- In Xilinx Artix-7 FPGA device, the total number of LUTs are more than thousand so the number of location for making FPGA fingerprint can be increased. Then the result will be more accurate and observed smooth spatial correlation as well.

- The aging effect will be highlighted in order to detect recycled FPGA more accurately. Also, there will be necessary to analyze and differentiate between aging effect and process variation. It will be important to explicitly define the reason of variations whether it is due to process variations or aging effect.

- The further aging effect can be analyzed to specifically in case of NBTI, HCI, and Electromigration.

- There will be carried out another research, where LUT path analysis can be considered in counterfeited detection. We know LUT have different path automatically connected to the aging effect is different in different LUT path.

- One of the important limitations of our present research is that it will not apparently classify the counterfeited types. In future, the types counterfeited FPGA can be distinguished whether it is recycled, cloned, tempered, or overproduced FPGA.

Table 1: Summery of Statistical Cross-validation report of LR for Counterfeited detection

No:	Parameters	Value
1	Correctly Classified Instances	100%
2	Incorrectly Classified Instances	0%
3	Mean absolute error	0
4	Root mean squared error	0
5	Relative squared error	0.0001%
6	Root Relative squared error	0.0002%
7	Total number of Instances	4

Table 2: Confusion Matrix of LR for Counterfeited detection

		True Test		
		Genuine	Counterfeited	Total
Screening	Genuine	3	0	3
	Counterfeited	0	1	1
	Total	3	1	4

5. Self-valuations

To evaluate our project we would like to discuss following two issues:

1. There are two deviations from the project proposal what we submitted and finally what we have done. One of the major issue is that although we focused HT detection in our proposal but finally we do not focus on it and keep it as future work and another is Raspberry-pi and master FPGA was included in the initially designed method to collect testing FPGA frequency but we have used UART interface using python coding which served the same purpose.

2. To evaluate our project in terms of successful-ness, it is almost 100% successful. But in terms of completeness, we still have some work to do.

References

[1] "Field-Programmable Gate Array (FPGA) Market Is Expected to Reach USD 9.50 Billion in 2013." [Online]. Available: https://transparencymarketresearch.com/field-programmable-gate-array.html].

[2] IHS, "Reports of counterfeit parts quadruple since 2009, challenging U.S. Defence Industry and National Security, Apr. 2012." [Online]. Available: http://www.ihs.com/images/IHS-iSuppli-Reports-Counterfeit-Parts-Quadruple-Since-2009.pdf.].

[3] "Defense Industrial base Assessment: Counterfeit Electronics, Bureau of Industry and Security, U.S. Department of Commence, Jan. 2010." [Online]. Available: http://www.bis.doc.gov/defenseindustrialbase program/osies/defmarketresearchrpts/final _counterfeit_electronics_report.pdf].

[4] Defenseone, "Counterfeits Can Kill U.S. Troops. So Why Isnt Congress and DoD Doing More to Stop it?" [Online]. Available: http://tiny.cc/7xd6gy.].

[5] ICC, "Estimating the global economic and social impacts of counter- feiting and piracy," 2011.

[6] K. Huang, Y. Liu, N. Korolija, J. M. Carulli, and Y. Makris, "Recycled ic detection based on statistical methods," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 34, no. 6, pp. 947–960, 2015.

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

[8] S. Kiamehr, A. Amouri, and M. B. Tahoori, "Investigation of NBTI and PBTI induced aging in different LUT implementations," in *Proceedings of International Conference on Field Programmable Technology*, 2011, pp. 1–8.

[9] K. Huang, J. M. Carulli, and Y. Makris, "Parametric counterfeit ic detection via support vector machines," in *Proceedings of IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems*, 2012, pp. 7–12.

[10] M. M. Alam, M. Tehranipoor, and D. Forte, "Recycled FPGA Detection Using Exhaustive LUT Path Delay Characterization," in *Proceedings of IEEE International Test Conference*, 2016, p. 12.3.

[11] V. Jyothi, A. Poojari, R. Stern, and R. Karri, "Fingerprinting Field Programmable Gate Arrays," in *Proceedings of International Conference on Computer Design*, 2017, pp. 337–340.

[12] A. Agarwal and et al., "Statistical timing analysis for intra-die process variations with spatial correlations," 2003, pp. 900–907.

[13] U. Guin and et al., "Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain," *Proceedings of IEEE*, vol. 102, no. 8, pp. 1207–1228, 2014.

[14] Q. Lei, H. Zhang, H. Sun, and L. Tang, "Fingerprint-based device-free localization in changing environments using enhanced channel selection and logistic regression," *IEEE Access*, vol. 6, no. 8, pp. 2569–2577, 2018.

[15] Y. Zhou and J. Yan, "A Logistic Regression Based Approach for Software Test Management," in *Proceedings of International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, 2016, pp. 268–271.

[16] D. Hosmer and S. lemeshow, "Applied logistic regression," wiley, 2000.

[17] "Xilinx," [Online]. Available: https://www.xilinx.com/].

[18] G. Homless, A. Donkin, and I. Witten, "Weka: A machine learning workbench," in *Proceedings of Second Australia and New Zealand Conference on Intelligent Information System, Brisbane, Australia*, 1994.