Heterogeneous IC Component Identification via EM Side-channels

Donald Greene
Aether Argus Inc.
Atlanta, US
don@aetherargus.com

Zahir Khan
Aether Argus Inc.
Atlanta, US
zahir@aetherargus.com

Angelos D. Keromytis
Aether Argus Inc.
Atlanta, US
angelos@aetherargus.com

Baki B. Yilmaz
Aether Argus Inc.
Atlanta, US
baki@aetherargus.com

***Abstract*—Globalization of supply chain encompasses a mix of both trusted and potentially untrusted entities, raising significant security concerns. In this paper, we introduce an electromagnetic signal-based authentication methodology for integrated circuits within heterogeneous integrated circuits, addressing the heightened security vulnerabilities emerging from the globalization of the supply chain. Our proposed method involves exciting specific components to capture their unique EM signatures, thereby generating a comprehensive dictionary of component signatures. These signatures facilitate the clustering of signals and the detection of anomalies by enabling comparisons between test signals and a reference model derived from benign samples. We achieved perfect clustering performance for the components considered in HICs. Furthermore, utilizing the same setup, we developed an anomaly detection algorithm that achieves over 95% accuracy when the loop size of the injected code exceeds 100. While our focus is on HICs, the versatility of our method allows for straightforward application to a wide range of devices, including microelectronics and Internet of Things (IoT) devices, which are equally vulnerable to the complexities and risks associated with a diversified supply chain.**

***Index Terms*—Heterogeneous IC, EM side-channels, component identification, signal processing.**

I. Introduction

Globalization, along with the geographic distribution of manufacturing, specialization, and the aggregation of production volumes, has significantly increased the complexity of the supply chain, yielding substantial cost savings for commercially available devices and components, including integrated circuits (ICs) and printed circuit boards (PCBs). However, these developments have also amplified concerns around the authentication of ICs within the semiconductor industry. This challenge has become even more pronounced with the industry's shift towards heterogeneous integration [1]. This transition introduces new threat scenarios, one of the most significant being the vulnerabilities inherent in the global supply chain. Heterogeneous ICs (HICs) and other microelectronics components pass through a supply chain that often extends beyond trusted system integrators and suppliers to include various entities responsible for fabricating, testing, and packaging the ICs; manufacturing the PCBs; assembling these PCBs with ICs and other components; loading firmware onto these boards; and, ultimately, incorporating these boards into subsystems that complete the final product. Addressing the vulnerabilities that devices encounter at each stage of this complex supply chain is crucial for enhancing system security. However, the idea of forming a supply chain comprised solely of trusted entities, while initially appealing, is not feasible due to the substantial additional costs it would involve. With the electronics market projected to reach $529.86 billion, exhibiting a compound annual growth rate of 9.2% from 2021 to 2028 [2], addressing the issue of untrusted entities within this vast supply chain becomes coercive. It is crucial to tackle this challenge in a clever and economical manner, without elevating the cost of devices. Such cost increases could significantly contribute to global inflation, making it essential to find balanced solutions that enhance security without imposing additional financial burdens.

The primary threat that emerges in the context of HICs is counterfeiting and unauthorized modifications to ICs. Counterfeiters have developed sophisticated methods, including reverse engineering, recycling, remarking, overproducing, cloning, tampering, forgery, and introducing defects to manufacture counterfeit products [3]. Such activities pose a significant threat to economic growth and innovation, adversely affecting the profits, sales, and competitive standing of legitimate companies.

To combat the issue of counterfeiting, a variety of reverse engineering methods have been developed. These techniques typically involve the use of Scanning Electron Microscopy (SEM), X-ray imaging, and Terahertz (THz) scanning to scrutinize hardware components ranging from transistors to the entire device. Additionally, the implementation of physical unclonable functions (PUFs) has been proposed [4]. PUFs leverage the inherent process variations in semiconductor manufacturing to create a unique identifier that is difficult to replicate. In a notable application of these methods, Ahmadi utilized a 3D X-ray microscope in conjunction with machine learning algorithms to identify counterfeit components at the die level [5].

The traditional approaches for inspecting and authenticating ICs, while effective, carry the risk of potential damage, require excessive time, and often lead to the destruction of the devices under examination. Consequently, there is a growing

This work has been supported, in part, by DARPA contract W912CG-23-C-0015. The views and findings in this paper are those of the authors and do not necessarily reflect the views of DARPA. Distribution Statement 'A' (Approved for Public Release, Distribution Unlimited)

demand for faster, more reliable, and cost-effective methods. In this context, techniques based on electromagnetic (EM) side-channels emerge as a promising solution due to their non-invasive nature, eliminating the need for device destruction. Leveraging these side-channels, several machine learning algorithms have been proposed to facilitate electronic component classification, IC authentication, and device investigation. A notable example is presented in [6], where an IC authentication method utilizes a PUF approach to generate unique EM signatures for different ICs. Unlike conventional PUF techniques that rely on complex, dedicated on-chip circuitry to produce a specific response to an input challenge, this method introduces a lightweight, variability-aware circuit. This innovation is nearly non-intrusive and carries no risk of damaging the ICs. This concept has been further extended to microcontrollers and Field-Programmable Gate Arrays (FPGAs), utilizing EM signatures as a means of authenticating the devices [4], [7].

EM signal-based identification and system analysis present substantial opportunities for enhancing supply chain security. This approach involves detailed scrutiny of software activities in IoT devices to verify that systems are uncompromised. For instance, as discussed in [8], EM signatures from a reference sample are utilized to train a neural network, which successfully classifies various programs running on an Arduino board. This demonstrates the potential of EM signals for software verification. Similarly, studies referenced in [9], [10] exploit EM emissions from motherboard components, like CPUs and memory, to differentiate hardware signatures. These distinct signatures are analyzed using deep neural networks to cluster component models, showcasing an innovative approach to hardware verification and security. In this paper, we explore HICs to develop a method for identifying individual IC components following excitation. Our approach utilizes EM side-channel signals emitted during component excitation, and employs these signals for effective clustering of the components. We achieved perfect clustering performance for the components analyzed in HICs. Additionally, we demonstrate that the same setup can be used for anomaly detection. In this regard, we have developed an anomaly detection algorithm that achieves over 95% accuracy when the loop size of the injected code exceeds 100.

The proposed method is non-invasive, as it necessitates no additional hardware circuitry within the system; it is also non-destructive, time-efficient, and significantly reduces investigation costs. By identifying components and revealing their EM signatures, our method offers a promising tool for addressing supply chain security issues, as any compromise in an IC component is likely to alter its signature. To the best of our knowledge, this is the first study to examine HICs for authentication purposes utilizing EM side-channels.

We organize the paper as follows: Section II provides information on EM side-channels, outlining our methodologies for capturing and processing signals. Section III presents our experimental setups and the findings derived from these experiments. Finally, Section IV offers a comprehensive conclusion, reflecting on both the approach taken and the results obtained.

II. Signal Processing and Characterization

For effective component classification and authentication, the initial step involves collecting signatures that uniquely define components, ensuring that any modifications result in detectable deviations in these signatures. Identifying the sources from which these signatures can be generated is crucial, followed by establishing a process pipeline for signature generation. Our proposed framework addresses this need by collecting EM signals emitted from the components of HICs. Utilizing advanced signal processing techniques, we reduce the dimensionality of the received signals while retaining the critical information necessary for clustering and authenticating components.

A. EM Side-channel Signals

EM side-channels generate emanations as a result of fluctuating current flows within a device's electronics, leading to the creation of EM waves [11]. Among the various types of side-channels, EM side-channels stand out due to their broad bandwidth and the capability to monitor devices from a distance, offering distinct advantages over other methods [12]. However, one significant challenge is that EM emanations can be exceptionally weak, occasionally making detection difficult. In contrast, power side-channels (PSCs) arise from similar principles, as they too are a consequence of current flows within a device's electronics [13]. Yet, PSCs differ notably in that they require a direct connection to the device and generally exhibit limited bandwidth [14]. This limitation is largely due to the design of mechanisms intended to stabilize supply voltage fluctuations within an IC package, which inadvertently act as low-pass filters for the current and voltage measurable at the device's external connections.

Though EM side-channels are often viewed as undesirable byproducts that may leak sensitive information, such as cryptographic keys [15], [16], it has been demonstrated that these channels can be leveraged to protect systems in air-gapped scenarios. Our framework utilizes emanated signals to generate unique signatures for IC components by running excitation programs that target specific functionalities. For example, Figure 1 displays a spectrogram captured from the Ethernet component of the Zynq UltraScale+ MPSoC ZCU102 board [17] while executing a program designed to transmit Ethernet packets to a client. The vertical and horizontal axes in the spectrograms represent time and frequency, respectively, and the excitation program repetitively carries out the same set of commands in a continuous loop. Observations from the spectrogram reveal that executing consistent code sequences generates similar signals, thereby facilitating the creation of reliable signatures. To capture the most distinctive signatures through EM side-channel analysis, we propose the following procedure:

- **Signal Acquisition:** While running the excitation code, we explore both the probe location and type to ensure the acquisition of the cleanest signal. This step aims to minimize interference from other components and environmental noise, while also maximizing signal strength.

- **Frequency Spectrum Selection:** Our investigation extends to identifying the most suitable frequency spectrum for capturing clear signals specific to a component. Following the insights provided in [18], we concentrate on frequencies modulated by the harmonic of the component's clock frequencies. The objective is to select frequency bands around the clock frequencies of the target component, ensuring they do not overlap with the clock frequencies or their harmonics of other components.
- **Verification with Spectrum Analyzer and SDR:** With the aid of a sophisticated spectrum analyzer, we finalize the choice of frequency band, probe location, and type. Subsequently, we employ a Software-Defined Radio (SDR) to test the reproducibility of the identified patterns. This step is critical for evaluating the feasibility of our measurement setup and is essential for managing the cost associated with the authentication process, considering the potential expense of spectrum analyzers.

After successfully completing these steps, we proceed to the signal processing phase, aimed at developing a model for clustering and authenticating the components.

B. Signal Processing

To achieve more reliable signature acquisition, it is essential to capture EM signals over extended periods and at higher sampling rates. This approach necessitates dealing with millions of samples for each signature and addressing potential phase differences that arise due to variations in the measurement start times. To navigate these challenges, we propose a modified version of the signal processing algorithm originally introduced in [19].

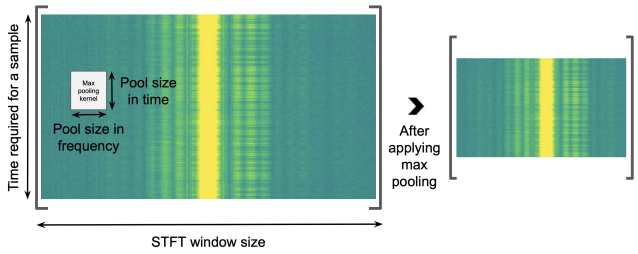


Fig. 1: The max-pooling operation applied to the spectrogram values before averaging to minimize the smearing effect.

The algorithm for processing the captured EM signals involves several key steps, aimed at generating reliable signatures with reduced computational complexity and memory storage cost. These steps can be listed as follows:

- For each measurement, apply Short-Time Fourier Transform (STFT) operation, specifying both the window size and the corresponding window function, along with a given overlap ratio. This process generates a matrix used to create the spectrogram, as illustrated on the left side of Figure 1. The resulting spectrogram matrix's dimensions are determined by the STFT window size (number of columns) and the number of STFT operations performed on the measured signal snippet (number of rows). Here, the time interval between consecutive STFT operations can be calculated by factoring in the sampling time and the count of non-overlapping samples.
- Apply a max-pooling operation to the matrix, utilizing predetermined pooling parameters in both frequency and time dimensions, as detailed in Figure 1. We operate under the assumption that the stride lengths match the pooling parameters. This max-pooling step effectively reduces the matrix size, thus lowering computational complexity. It also addresses the smearing effect issues, which arise from the imperfections of system clocks.
- The final step involves averaging the max-pooled matrix, either before or after converting the matrix values into decibels (dB). The outcome is a vector with a length determined by *floor* (W_S/K_F), where F_S represents the STFT window length and the K_F frequency dimension's pooling parameter. This step is crucial for efficiently condensing the signal data, especially when dealing with millions of samples, significantly reducing the memory storage requirements for the signatures.

The signal signatures generated through our process are aggregated into a feature dictionary, representing unique EM profiles of different components within a subject HIC. This repository becomes instrumental in identifying deviations that may indicate tampering or compromise. Manufacturing variations, inherent to electronic component fabrication, ensure that any alteration or substitution of components will alter the EM field around them. These changes surface in the EM signal patterns, even if the component continues to meet expected digital test outcomes. Consequently, our method provides a robust mechanism for authorizing HICs and other electronic devices, leveraging the subtle but distinct variations in EM signatures to detect unauthorized modifications.

C. Clustering with Neural Networks

The snippets generated from the signal processing algorithm are utilized not only for authentication but also for clustering the components of HICs. To achieve this, we propose the application of a deep neural network (DNN), the architecture of which is depicted in Figure 4a. Given that the processed snippets are 1D vectors, our DNN architecture starts with 1D convolutional layers. This choice is deliberate, to accommodate the nature of the snippets, in contrast to the 2D or 3D convolutional layers commonly used in image processing tasks. Following the convolutional layers, the network transitions to linear layers. The design results in the output layer comprising a number of nodes equal to the count of IC components targeted within the subject HIC.

To mitigate the risk of overfitting within our deep neural network, we incorporate dropout layers and implement early stopping mechanisms. These techniques help to regularize the model, ensuring it generalizes well to unseen data. Additionally, for purposes where visualization of the clusters is beneficial, we can adjust the architecture of the linear layer, specifically the one labeled as fc3, to align with our

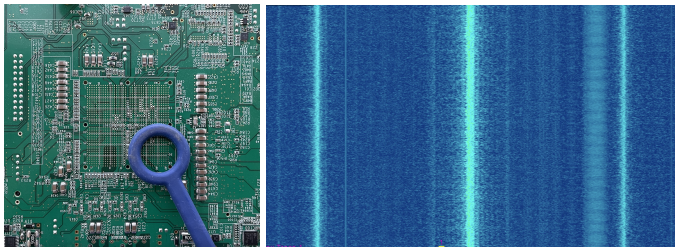
visualization goals. For instance, setting this layer to have two nodes enables the visualization of clusters within a two-dimensional space. After the network is trained, transfer learning techniques can be applied to remove all subsequent layers, allowing us to plot the outputs directly from this two-dimensional layer.

For scenarios where visualization is the primary concern, techniques like t-SNE can be utilized [20]. However, it is important to note that while t-SNE is powerful for visualizing high-dimensional data in lower dimensions, the transformation it applies is not directly extendable to new data points. Therefore, our approach, which allows for both clustering and visualization in 2D or 3D spaces, offers a more versatile solution. This adaptability is crucial, especially since the proximity of signal signature projections within these visual spaces serves as an indicator of cluster membership. Modifications to a component of a subject HIC due to supply chain discrepancies will result in a divergence from its original cluster. This feature is instrumental in detecting and addressing supply chain integrity issues.

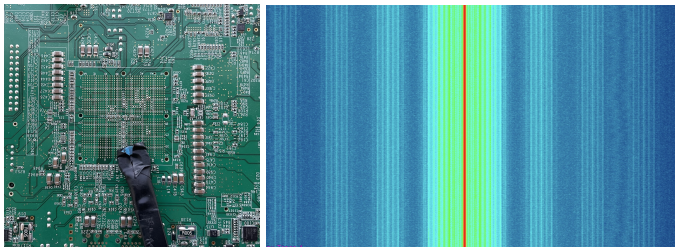
III. Experimental Setup and Results

In this section, we detail the experimental results obtained from testing on the Zynq UltraScale+ MPSoC ZCU102 board. Our experiments focused on three key components: the CPU, UART, and Ethernet. The initial step is to follow the procedures outlined in Section II-A for EM side-channel analysis. For our probes, we selected two near-field probe sets, one from Aaronia and another from Tekbox, complemented by a Siglent spectrum analyzer (SA) and an Ettus USRP SDR. Through extensive and meticulous experimentation, we identified the optimal probe placement as depicted in Figure 2. Additionally, the specific probe types utilized in our experiments, along with their corresponding center frequencies, can be listed as follows: 1) AAronia near-field magnetic-field probe at 1.108 GHz for CPU, 2) Tekbox near-field magnetic-field probe at 125 MHz for UART, and 3) AAronia near-field electric-field probe at 1.24 GHz for Ethernet.

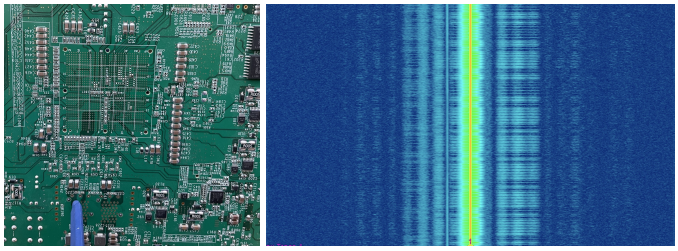
As depicted in Figure 2, we opted to capture signals from the rear of the board, a decision influenced by the presence of a heat-sink attached to the core components. This strategic positioning of probes, along with their specific locations and center frequencies, was determined after thorough investigation, ensuring minimal interference and sufficient signal strength for the clustering algorithm to perform effectively. It is important to note that while we do not assert this setup as the definitive best for maximizing the Signal-to-Interference-plus-Noise Ratio (SINR), given the vast array of possible experimental configurations, it proved adequate for achieving our algorithm's desired performance levels. The spectrograms illustrated in this figure highlight the distinctiveness of each component's signal, both in terms of pattern and center frequency. This distinction is particularly valuable, enabling us to generate unique signatures for each component. These signatures are pivotal for subsequent clustering or detecting deviations, emphasizing the efficacy of our experimental approach.



(a) CPU (Spectrogram Center Frequency: 1.108 GHz)



(b) UART (Spectrogram Center Frequency: 125 MHz)



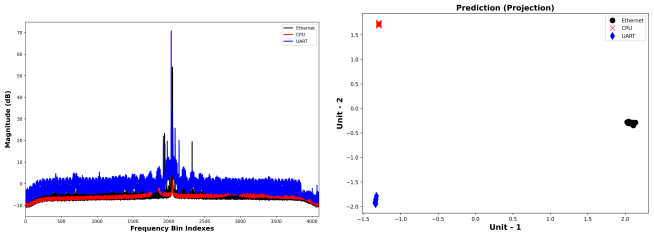
(c) Ethernet (Spectrogram Center Frequency: 1.24 GHz)

Fig. 2: Experimental setups and corresponding spectrograms. The vertical axis represents time, covering approximately 5 seconds, while the horizontal axis corresponds to frequency. The spans for the spectrograms around the given centers are 8 MHz, 2 MHz, and 1 MHz, respectively, for clearer illustration.

As the next step, we proceeded to collect signals using the USRP SDR, adhering to the experimental setup and center frequencies determined previously. For each component under investigation, signals were captured for a duration of 3 seconds at a sampling rate of 8 MSPS. This approach resulted in each signature being derived from a signal comprising 24 million complex numbers, reflecting the baseband signals returned by the SDR. In our analysis, we intentionally disregarded the knowledge of center frequencies to increase the processing algorithm's challenge, essentially simulating a scenario where all component signals are presumed to be informative within the same frequency band. This decision adds an extra layer of complexity to the signal processing task. Despite these constraints, the processed EM signals representing the signatures for the three components we examined are illustrated in Figure 3a. To achieve the desired outcomes, we configured the STFT window size to 40960, with pooling parameters set at 10 in frequency and 8 in time. This configuration effectively reduced

the dimensionality of the signal from 24 million to 4096. This significant reduction in signal size not only simplifies the computational demands of our analysis but also retains the essential characteristics necessary for accurate component identification and anomaly detection.

Despite the intentional analytical challenges and the difficulty in discerning signal differences directly from the figures, our analysis reveals distinct signal patterns for different components, coupled with a notable consistency within signals of the same class. This demonstrates our method's ability to effectively differentiate and cluster component signals, affirming its potential for reliable authentication and anomaly detection.



(a) Before projection. (b) After projection.

Fig. 3: Processed baseband signals.

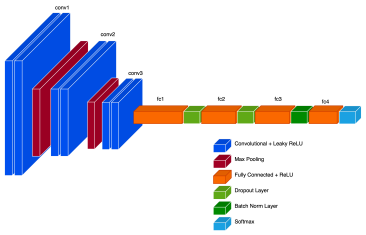
A. Clustering Components

After acquiring the signatures, we proceed to train the neural network as detailed in Figure 4a. The network is configured with output channels set at 5, 20, and 1 for the convolutional layers, each employing a kernel size of 2. For the linear layers, we establish the number of nodes at 60, 20, 2, and 3, respectively, incorporating a dropout rate of 30% to mitigate over-fitting.

After completing the training phase, we modified the network by removing all extraneous layers, focusing on visualizing the outputs of the adjusted network as depicted in Figure 3b. The visualization clearly shows that each class is densely populated and distinctly separated from the signals of other components. This separation underscores the uniqueness of the signal patterns for each component, effectively demonstrating the proposed framework's capability to distinguish between different component signals. We need to note here that the excitation codes used in our experiments are not the only or optimal codes for conducting these tests and achieving the observed performances. We believe there are countless possibilities for excitation codes that could be utilized. For our experiments, we employed simple codes, such as sending Ethernet packets to stimulate Ethernet components or executing basic algorithmic operations on the CPU to activate it. Even with these simple codes, we were able to successfully identify different components.

B. Anomaly Detection

In this section, we demonstrate how the experimental setups used for identifying different IC components can also be employed to detect anomalous activities. To evaluate the robustness of our framework against modifications, we conducted a controlled experiment where the size of the injected code could be precisely adjusted. This method allowed us to investigate the relationship between the size of the injected code and its impact on signal patterns. Our analysis was confined to CPU activities to facilitate the implementation of targeted tests. Specifically, we injected a for-loop containing simple algorithmic operations with varying numbers of iterations, as illustrated in Fig. 4b. This variation in loop size enabled us to systematically assess the framework's sensitivity to changes in code size. While we have not conducted experiments on other components due to space constraints, similar methodologies could be applied to them. For instance, an anomalous packet could be sent through Ethernet and UART communications to identify unexpected traffic.



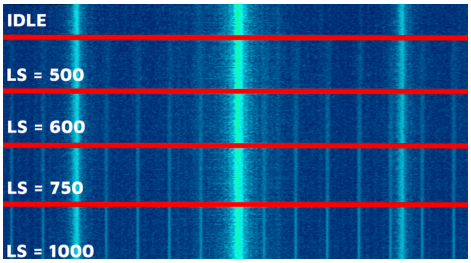

```
void main() {
    // Some functionality
    ...

    // Injected code
    if (trojan is active) {
        for (number_of_iteration)
            (*a_pointer)++;
    }

    // Some functionality
    ...
}
```

(a) (b)

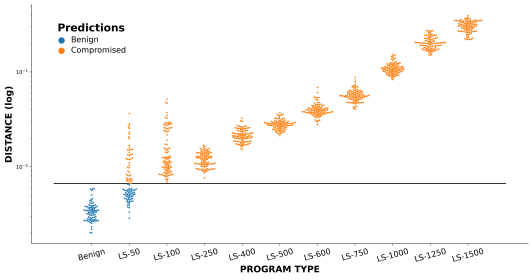
Fig. 4: a) The neural network structure used to cluster the ICs. b) An example of the pseudo-code used to obtain the results.

The spectrograms captured for different versions of the injected code, as shown in Figure 5a, reveal that code injection results in certain frequencies becoming prominently active, appearing as vertical lines in the spectrogram. Also, the intensity of these active frequencies escalates with an increase in the size of the injected code, while the smearing around these frequencies diminishes. To analyze the system's performance, we initially collect benign EM signals to generate the training model, as detailed in Section II. These signals are processed to produce what we refer to as 'golden samples.' We allocate 20% of these golden samples to obtain hyperparameters like a threshold, which is subsequently excluded from the training model. The training model thus comprises the remaining 80% of the golden samples, along with hyper-parameters like the threshold derived from the initial 20% of the data. The subsequent step involves comparing test signals to the golden samples by calculating their Euclidean distances, as shown in Figure 5b. This figure displays the divergence of test signals from the established baseline, where each dot represents multiple test samples, and the black horizontal line indicates the threshold distinguishing between valid and anomalous samples. It is crucial to note that our method employs a one-class classification strategy, recognizing the challenge of predicting all potential malicious activities.

Our findings demonstrate that the proposed method achieves a remarkable accuracy rate of 95% for detecting anomalies, provided the loop size exceeds 100 iterations. This underscores



(a) The changes in spectrogram.



(b) Distance distribution.

Fig. 5: Experimental results for anomaly detection.

the efficacy of our framework in identifying modifications through dynamic code changes, demonstrating its potential as a reliable tool for enhancing system security. It is important to note that altering the code within the loop affects the number of instructions executed. However, variations in the number of instructions do not linearly impact the emanated EM signals due to the specifics of their hardware implementations. While increasing the number of instructions tends to enhance the quality of the received EM signals, it also extends the execution time. Consequently, the performance of our algorithm in terms of loop size changes as the instructions change within the loop.

IV. Conclusion

In this work, we have developed an authentication method for HICs by analyzing the unique EM signals emitted from their components. Our approach not only facilitates the clustering of EM signals but also enables the detection of anomalies, leveraging a signature-based methodology assuming the use of golden samples during the training phase. By creating a comprehensive dictionary of component signatures, modifications to components become detectable through deviations from the established model. Through rigorous experimentation, we have demonstrated the utility of our method in clustering component signals within an HIC, as well as in identifying modifications using the same technique. A neural network model further aids in clustering, with the capability to visualize the data in two or three dimensions, enhancing interpretability. Given its non-invasive nature and vendor neutrality, our method holds promise for widespread application across various systems, including microelectronics and IoT devices, addressing critical security concerns in the face of the increasingly complex global supply chain.

References

[1] C. Xi, A. A. Khan, N. Jessurun, N. Vashisthan, M. M. Tehranipoor, and N. Asadizanjani, "Physical assurance for heterogeneous integration: Challenges and opportunities," in *2022 IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA)*. IEEE, 2022, pp. 1–6.

[2] Grand View Research. Active Electronic Components Market Worth $529.86 Billion By 2028, Published: April 2021. [Online]. Available: https://www.grandviewresearch.com/press-release/global-active-electronic-components-market

[3] E. Oriero and S. R. Hasan, "Survey on recent counterfeit ic detection techniques and future research directions," *Integration*, vol. 66, pp. 135–152, 2019.

[4] M. M. Ahmed, D. Hely, E. Perret, N. Barbot, R. Siragusa, M. Bernier, and F. Garet, "Robust and noninvasive ic authentication using radiated electromagnetic emissions," *Journal of Hardware and Systems Security*, vol. 3, pp. 273–288, 2019.

[5] B. Ahmadi, B. Javidi, and S. Shahbazmohamadi, "Automated detection of counterfeit ics using machine learning," *Microelectronics Reliability*, vol. 88, pp. 371–377, 2018.

[6] M. M. Ahmed, D. Hely, N. Barbot, R. Siragusa, E. Perret, M. Bernier, and F. Garet, "Radiated electromagnetic emission for integrated circuit authentication," *IEEE Microwave and Wireless Components Letters*, vol. 27, no. 11, pp. 1028–1030, 2017.

[7] M. M. Ahmed, D. Hely, E. Perret, N. Barbot, R. Siragusa, M. Bernier, and F. Garet, "Authentication of microcontroller board using non-invasive em emission technique," in *2018 IEEE 3rd International Verification and Security Workshop (IVSW)*. IEEE, 2018, pp. 25–30.

[8] A. Sayakkara, N.-A. Le-Khac, and M. Scanlon, "Leveraging electromagnetic side-channel analysis for the investigation of iot devices," *Digital Investigation*, vol. 29, pp. S94–S103, 2019.

[9] E. J. Jorgensen, F. T. Werner, M. Prvulovic, and A. Zajić, "Deep learning classification of motherboard components by leveraging em side-channel signals," *Journal of Hardware and Systems Security*, vol. 5, no. 2, pp. 114–126, 2021.

[10] F. T. Werner, B. B. Yilmaz, M. Prvulovic, and A. Zajić, "Leveraging em side-channels for recognizing components on a motherboard," *IEEE Transactions on Electromagnetic Compatibility*, vol. 63, no. 2, pp. 502–515, 2020.

[11] A. Zajic and M. Prvulovic, "Experimental demonstration of electromagnetic information leakage from modern processor-memory systems," *Electromagnetic Compatibility, IEEE Transactions on*, vol. 56, no. 4, pp. 885–893, Aug 2014.

[12] S. Sangodoyin, F. Werner, B. B. Yilmaz, C. L. Cheng, E. M. Ugurlu, N. Sehatbakhsh, M. Prvulovic, and A. Zajić, "Side-channel propagation measurements and modeling for hardware security in iot devices," *IEEE Transactions on Antennas and Propagation*, pp. 1–1, 2020.

[13] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Annual International Cryptology Conference*. Springer, 1999, pp. 388–397.

[14] X. T. Ngo, Z. Najm, S. Bhasin, S. Guilley, and J.-L. Danger, "Method taking into account process dispersion to detect hardware trojan horse by side-channel analysis," *Journal of Cryptographic Engineering*, vol. 6, no. 3, pp. 239–247, 2016.

[15] D. Genkin, L. Pachmanov, I. Pipman, and E. Tromer, "Stealing keys from pcs using a radio: Cheap electromagnetic attacks on windowed exponentiation," in *International workshop on cryptographic hardware and embedded systems*. Springer, 2015, pp. 207–228.

[16] M. Alam, H. A. Khan, M. Dey, N. Sinha, R. Callan, A. Zajic, and M. Prvulovic, "One&done: A single-decryption em-based attack on openssl's constant-time blinded rsa," in *Proceedings of the 27th USENIX Conference on Security Symposium*. USENIX Association, 2018, pp. 585–602.

[17] Xilinx, "Zynq ultrascale+ mpsoc zcu102," https://www.xilinx.com/products/boards-and-kits/ek-u1-zcu102-g.html.

[18] R. Callan, A. Zajic, and M. Prvulovic, "A Practical Methodology for Measuring the Side-Channel Signal Available to the Attacker for Instruction-Level Events," in *Proceedings of the 47th International Symposium on Microarchitecture (MICRO)*, 2014.

[19] B. B. Yilmaz, E. M. Ugurlu, F. Werner, M. Prvulovic, and A. Zajic, "Program profiling based on markov models and em emanations," in *Cyber Sensing 2020*, vol. 11417. SPIE, 2020, pp. 69–83.

[20] L. Van der Maaten and G. Hinton, "Visualizing data using t-sne." *Journal of machine learning research*, vol. 9, no. 11, 2008.