IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 3, 2021, accepted February 9, 2021, date of publication February 12, 2021, date of current version February 23, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3059100

A Novel Authentication Methodology to Detect Counterfeit PCB Using PCB Trace-Based Ring Oscillator

DONGRONG ZHANG, (Member, IEEE), QIANG REN, (Member, IEEE), AND DONGLIN SU, (Senior Member, IEEE)
School of Electronic and Information Engineering, Beihang University, Beijing 100191, China

Corresponding author: Qiang Ren (qiangren@buaa.edu.cn)

This work was supported by the National Natural Science Foundation of China under Grant 61631002.

ABSTRACT The existence of counterfeit products, e.g., integrated circuits (ICs) and printed circuit boards (PCBs), in the modern semiconductor supply chain has seriously jeopardized the security and reliability of electronic systems, and has also caused the loss of suppliers' profit and reputation. Most of existing research papers prevent or detect counterfeit IC and PCB substrate separately, without testing the PCB as a whole, and often require the assistance of external equipment. In this article, a novel ring oscillator-based PCB authentication (ROPA) methodology to detect counterfeit PCB through supply chain is proposed, which utilizes PCB trace-based ring oscillators (PTRO) assisted by on-chip ring oscillators, and a novel PCB signature extraction methodology. By switching the PCB to different load modes, the signature can reflect the process variations in PCB traces and overall impedance. The ROPA can provide both IC and PCB authentication independently of external equipments, and allows remote authentication for the user. The ROPA structure has shown advantageous area (0.301% on average) and power (0.355% on average) overhead when implemented on a number of benchmarks. Then the ROPA is implemented on a set of authentic and counterfeit FPGA development boards to verify the effectiveness on counterfeit detection. The results show that the proposed method provides 96.7% confidence in detecting tampered PCBs and 100% confidence in detecting overproduced, recycled, and cloned PCBs.

INDEX TERMS PCB authentication, recycle, clone, overproduction, counterfeit, tamper, supply chain security.

I. INTRODUCTION

Nowadays, the printed circuit board (PCB) is an important part of modern electronic systems, which provides a platform for the system on chip (SoC) operation. The manufactured PCB needs to go through many untrusted manufacturers and distributors (e.g., original equipment manufacturer (OEM)) before it can be used by the end user. Hence, similar to the counterfeit threat of the integrated circuit (IC) [1], the PCB is also vulnerable to counterfeiting attacks, such as replacing qualified components with recycled ones [2]. A survey from Senate Armed Services Committee in 2012 claims that there are more than one million counterfeit components in the Pentagon's supply chain [3].

The associate editor coordinating the review of this manuscript and approving it for publication was Christian Esposito.

The counterfeit PCB, sold by untrusted third parties at low prices, might cause the PCB designer endure both reputation and revenue losses. More important, the counterfeit PCB are mostly assembled with unqualified, defective, or over-aged components. These products will cause serious security and reliability risks to the electronic system [4]. In addition, malicious attackers can insert hardware Trojans into the counterfeit PCB, to steal critical information, or control the system illegally [5], [6].

Therefore, it is necessary for the PCB designer to have proper defense mechanisms so that only authentic PCBs can be integrated into electronic systems. Such an assurance is challenging and expensive. There have been several approaches in the literature, which aim at bringing trust in modern semiconductor supply chain. The most effective and popular techniques are summarized in the following.

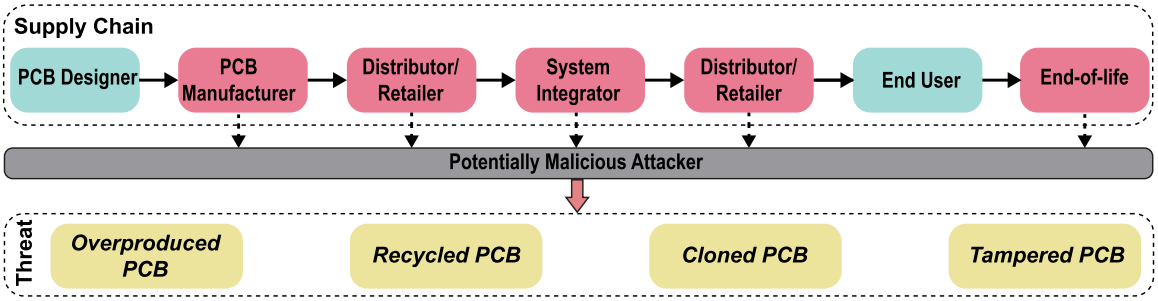


FIGURE 1. The threat models distributed along different stages of the supply chain.

Visual Inspection [7]: The tester uses their eyes, microscope or X-ray to find the footprint of the PCB and components on it being polished and refurbished. This method can only distinguish counterfeit PCBs with a relatively low level of refurbishment. And it cannot detect the cloned PCB and the overproduced PCB.

Key Components Anti-counterfeiting: This method mainly focuses on the most valuable component on the PCB or component with the greatest impact on system security and reliability, which are the main goal of counterfeiting, such as IC, memory, field programmable gate array (FPGA), etc. [8]–[13]. For example, [11] detects the recycled IC by measuring the intrinsic light emission from CMOS. If these key components are not counterfeit, then the PCB would be authentic with high probability. However, this solution cannot prevent authentic key components from being assembled on the counterfeit PCB.

PCB-level Obfuscation: To clone a PCB, an attacker must obtain the layout of the PCB through reverse engineering [14], [15], such as using X-rays to obtain information about the internal wiring of the PCB. To prevent the cloned PCB, [16] presents an PCB obfuscation approach that relies on permutation blocks to hide the interconnects among the PCB's circuit components. But this technique cannot prevent PCB recycling and malicious tampering.

PCB-level Fingerprint: Authentication service providers generate a unique fingerprint for each PCB [17]–[19] based on the unique characteristics of PCB, such as process variations of the path delay between PCB boundary scan cells [20], the intrinsic trace impedance [21], [22], and the impedance at resonance [23], [24]. [25] presents a PCB-level radio frequency identification (RFID) based counterfeit detection technique, which employs a RFID tag to collect and transmit the Physical Unclonable Function (PUF [26]) and on-chip sensors' values of all ICs on PCB. The tested PCB can be considered as counterfeit one, if its fingerprint does not match the database or the value has changed. However, most existing countermeasures require additional equipments to measure key parameters [21]–[24] or modify the PCB [25], which result in high test and area overhead. Furthermore, dependence on external equipments prevents secure remote authentication.

To overcome the limitations of the above-mentioned techniques, in this article, we propose a novel ring oscillator (RO) based PCB authentication (ROPA) methodology, which utilizes PCB trace-based ring oscillator (PTRO) assisted by on-chip ring oscillator (ORO), to remotely detect counterfeit PCBs. By measuring the frequency of PTRO and ORO in different load modes of the PCB, PCB designer can identify the specific process variations of both IC and PCB in the system under test. Our proposed technique offers the following advantages:

1) The ROPA concurrently provides authentication for both IC and PCB through novel designed PTROs.
2) The ROPA extracts the PCB signature by switching the PCB to different load modes without extra external equipment, which allows remote authentication.
3) The ROPA is all-digital, with low area and power overhead.

The rest of this article is organized as follows. The threat models are highlighted in Section II. The architecture of the proposed ROPA is introduced in Section III. Section IV presents the ROPA-based authentication methodology. The implementation and authentication flow is presented in Section V. The experimental results and analysis are discussed in Section VI. Finally, we conclude this article in Section VII.

II. THREAT MODELS AND OBJECTIVES

This section presents the threat models for PCB-level counterfeiting, and the motivation of the proposed authorization methodology.

A. THREAT MODELS

Before the manufactured PCB is used by the end users, many untrusted parties are involved, such as system integrators, distributors, etc., as shown in Figure 1. The counterfeit PCB produced by these untrusted parties can be divided into the following types:

1) *Overproduced PCB*: The PCB manufacturer can produce PCBs that beyond scope of the contract [25] for illegal profit. Since these PCBs are not monitored by the designer, their quality cannot be guaranteed.

TABLE 1. The effectiveness of existing countermeasures for the counterfeit PCB detection.

Countermeasure	Threats for PCB				PCB & IC Concurrently Detection	Additional Test Equipment	PCB Area Overhead
	Overproduced PCB	Recycled PCB	Cloned PCB	Tampered PCB			
Visual Inspection [7]	×	×	×	×	✓	Yes	N/A
Key Components Anti-counterfeiting [11]	×	×	×	×	×	No	N/A
PCB-level Obfuscation [14]	×	×	✓	×	×	No	High
PCB-level Fingerprint: Z_{Trace} [21]	✓	✓	✓	✓	×	Yes	Low
Proposed Technique	✓	✓	✓	✓	✓	No	Low

(1) ✓ indicates that the countermeasure can prevent the trust issue;
(2) × indicates that the countermeasure is ineffective.

2) *Recycled PCB*: Usually after a period of use, the PCB will be retired due to performance degradation and increased failure rate. But these PCBs still work normally in most cases. For the retired PCB but still functional well, malicious attackers can simply clean, polish, and remark the whole PCB as new product, and sell them to downstream supply chain vendors [27]. Since the recycled PCBs are over-aged, the probability of electronic system failure would be increased significantly.
3) *Cloned PCB*: Through reverse engineering [28], the attacker can obtain the layout information of the PCB, then purchase all the components (e.g., resisters, SoCs, memories, etc.) and integrate them together with the privately manufactured PCB substrate. In this process, attackers can use lower-performance or recycled components [29]–[31] to reduce costs. Since the quality of components and manufacturing processes cannot be guaranteed, the reliability of the cloned PCB is insufficient. At the same time, the cloning of PCBs violated the intellectual property rights of the PCB designer.
4) *Tampered PCB*: The attacker can perform malicious alterations, such as replacing the original chip with an illegal substitute (e.g., a counterfeit IC). Similarly, they can collect the components that can work normally on different retired PCBs, to assemble a new PCB. These tampered PCBs pose a serious threat to the security and reliability of the system.

B. COUNTERFEITER's OBJECTIVES

Most of counterfeit PCBs are made for illegal profits [3]. On the one hand, counterfeiters purchase retired PCBs at extremely low prices and sell them to downstream vendors at the original price after refurbishment, in order to obtain illegal profits. On the other hand, by cloning the PCB, the attacker (such as a system integrator) can save PCB research & development cost, which enables him to use a PCB with the same function at low cost or sell it as authentic one for extra profits.

C. AUTHENTICATION OBJECTIVES

The objective of this article is to propose a robust solution to detect the counterfeit PCBs listed in Section II-A. Table 1 summarizes the limitations and major challenges of the existing countermeasures for counterfeit PCB prevention and detection. Hence, the proposed solution to ensure the trust in the modern supply chain must have the following criteria:

1) The proposed technique must be able to concurrently verifies the authenticity of both PCB and IC.
2) It can detect the above four types of counterfeit PCBs.
3) The proposed technique does not rely on external equipment for data measurement and collection.
4) The proposed technique enable the PCB designer or trusted manufacturer to perform authentication remotely.
5) The proposed technique should be able to protect the legitimate rights and interests of the PCB designer and the end user.

III. STRUCTURE

A. PTRO

As mentioned in Section I, ROPA mainly utilizes PCB trace-based ring oscillator (PTRO), to remotely detect counterfeit PCBs. By transmitting the oscillating signal from the IC to the PCB trace, the oscillation period of proposed PTRO can reflect PCB traces, overall PCB impedance, I/O and IC process variations. Testers can switch PCBs between high and low load modes to extract the digital signature of the PCB using PTRO, which varies due to the process variations for different PCBs.

The structure of PTRO is shown in Figure 2, which is composed of PCB traces, complementary metal oxide semiconductor (CMOS) based gates, and input/output (I/O) pins. The oscillation period of the PTRO can be expressed by Equation (1):

$$T_{PTRO} = 2 * (t_{PCB\_trace} + t_{IC} + \sum_{i=0}^{1} t_{I/O_i}) \tag{1}$$

where t_{PCB_trace}, t_{IC}, and $t_{I/O}$ are the delay of the PCB trace used by the PTRO, CMOS based path in the IC, and I/O cell, respectively. And t_{IC} can be expressed by Equation (2):

$$t_{IC} = \sum_{i=0}^{k} t_{gate_i} \tag{2}$$

where k is the total number of gates that constituting the CMOS based path in the IC, and t_{gate_i} is the delay of the ith gate.

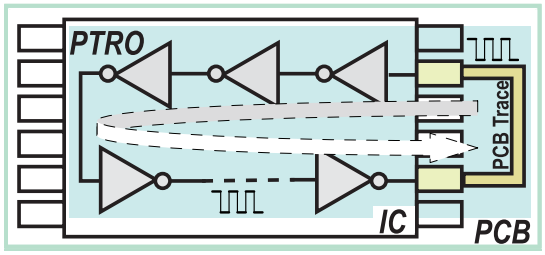


FIGURE 2. The overview of the proposed PCB trace-based ring oscillator (PTRO).

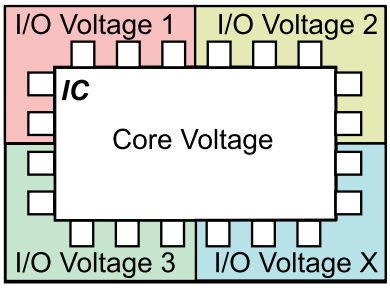


FIGURE 3. Different power supply voltages required by IC.

Hence, the process variations of PCB, IC, and I/O cell would impact the oscillation period of the PTRO.

1) T_{PTRO} IMPACTED BY PCB TRACE PROCESS VARIATION

According to [32], the propagation delay of the PCB trace can be expressed as:

$$t_p = \sqrt{\varepsilon_{re}}/c \tag{3}$$

where c is the velocity of light, and ε_{re} is the effective dielectric constant of the substrate material. The effective dielectric constant is lower than the relative dielectric constant (ε_r) of the substrate. And the ε_{re} can be expressed as [33]:

For $W/H \leq 1$,

$$\varepsilon_{re} = \frac{\varepsilon_r + 1}{2} + \frac{\varepsilon_r - 1}{2}\left[\frac{1}{\sqrt{(1 + 12\frac{H}{W})}} + \frac{(1 - \frac{W}{H})^2}{25}\right] \tag{4}$$

For $W/H \geq 1$,

$$\varepsilon_{re} = \frac{\varepsilon_r + 1}{2} + \frac{\varepsilon_r - 1}{2}\frac{1}{\sqrt{(1 + 12\frac{H}{W})}} \tag{5}$$

where H is the height of the trace above the ground plane, and W is the width of trace, both of which can be effected by the process variation.

For a PCB trace of length L, the delay is:

$$t_{PCB\_trace} = t_p * L \tag{6}$$

In addition, if the trace passes through the via, the delay of the via (t_{via}) must be added to the delay of the PCB trace (t_{PCB_trace}). And t_{via} is determined by the parasitic capacitance and inductance of the via [34].

According to [35], after the PCB is used for a long time, the characteristics of its traces and vias will change due to oxidation, corrosion, etc., resulting in t_{PCB_trace} changed. Hence, process variations and aging will affect T_{PTRO}.

2) T_{PTRO} IMPACTED BY PCB IMPEDANCE PROCESS VARIATION

As shown in Figure 3, an IC usually has multiple power supply voltages, such as core voltage, at which the internal logic operate, and I/O voltage, which drive the I/O buffers. According to the connected peripherals, the I/Os are grouped in banks, each of which can operate at different voltages. When an I/O bank works in high load mode (all I/Os in this bank switch at a relatively high frequency), the impedance of this I/O bank will decrease. According to the law of voltage division (Equation (7)), the actual supply voltage of this I/O bank ($VDD_{I/O}$) will also decreases.

$$VDD_{I/O} = VDD_{supply}\frac{Z_{I/O}}{Z_{I/O} + Z_{PCB}} \tag{7}$$

where VDD_{supply} is the recommended power supply voltage of the I/O bank delivered from the external power supply, $Z_{I/O}$ is the impedance of the I/O bank, and Z_{PCB} is the impedance of the PCB part connected to the IO bank.

Hence, the delay of I/Os in this bank will increase, resulting in the T_{PTRO} in this I/O bank changed (ΔT_{PTRO}), where

$$\Delta T_{PTRO} = (T_{PTRO})_{high\_load} - (T_{PTRO})_{low\_load} \tag{8}$$

Due to process variations, the impedance of PCBs various, resulting in various ΔT_{PTRO} for different PCBs. Similarly, aging will cause the PCB impedance to change [35], so it will also cause a difference of ΔT_{PTRO} before/after PCB aging.

Hence, through the PCB signature extraction methodology, which switches PCB from low load mode to high load mode, the difference in PCB overall impedance can be reflected by the ΔT_{PTRO}. The PCB signature extraction method through PTRO will be discussed in detail in Section IV.A.

3) T_{PTRO} IMPACTED BY IC PROCESS VARIATION

The delay of a CMOS based inverter (t_d) can be expressed by Equation (9) [36], [37]:

$$t_d = \frac{C_L VDD}{\mu C_{ox}\frac{W}{L}(VDD - V_{th})^{\alpha}} \tag{9}$$

where C_L, μ, C_{ox}, W, L, VDD, V_{th} are gate load capacitance, mobility, gate oxide capacitance, gate width, gate length, ORO power supply, and threshold voltage, respectively. α is a constant determined by process variation. According to Equation (9), fluctuations of parameters C_L, C_{ox}, W, L, V_{th} and α, which are caused by process variation during IC fabrication, would make the delay of the CMOS randomly change in different ICs.

And t_d is also effected by the aging degradation. Several aging mechanisms can greatly affect reliability during the lifetime of an IC, including negative bias temperature

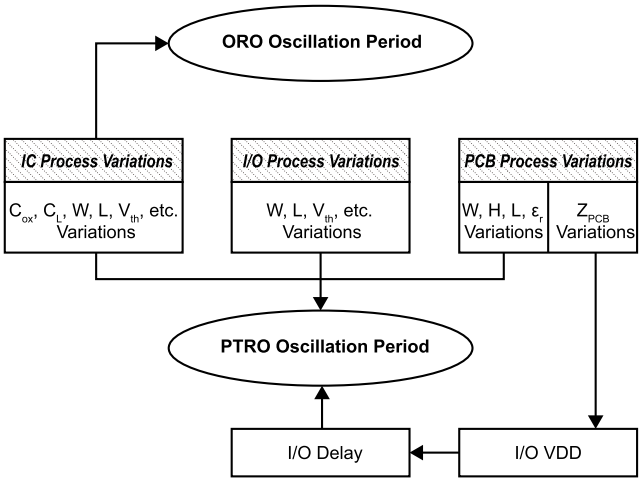


FIGURE 4. The oscillation periods of on-chip ring oscillator (ORO) and PCB trace-based ring oscillator (PTRO) effected by various process parameters.

instability (NBTI) [38], [39] and hot carrier injection (HCI) [40]. Both NBTI and HCI increase the threshold voltage (V_{th}) and the t_d. Similarly, other CMOS based gates will also be affected by the above mentioned process variation and aging.

4) T_{PTRO} IMPACTED BY I/O PROCESS VARIATION

There are various I/O standard, such as CMOS and Transistor Transistor Logic (TTL) I/O standards [41], [42]. Similar to the CMOS based gates, the delay of IO cells ($t_{I/O}$) using these standards is also affected by factors such as power supply, transistor length/width, oxide thickness, poly resistivity, etc. [43]. This means that process variations will affect the delay of I/O cell ($t_{I/O}$).

As discussed above, the oscillation periods of PTRO effected by various process parameters, as shown in Figure 4. The process variations of these parameters lead to differences in the oscillation periods of PTRO on different PCBs, which can be used to detect counterfeit PCBs.

5) COMPARED WITH THE ON-CHIP RO

Compared with the on-chip RO, PTRO has two advantages: 1) according to the structure of PTRO, the process variations of I/Os and PCB traces are introduced; 2) through the novel PCB signature extraction method, which extracts signatures at different load modes of PCB, the overall impedance variations of the PCB would be further reflected. Hence, PTRO can be used to generate a PCB fingerprint.

In detail, the proposed PTRO is composed of PCB traces, CMOS based gates and I/O pins. Hence, PTRO would have some characteristics of the traditional on-chip ring oscillator (RO) PUF, which can generate a fingerprint for IC authentication. However, only using the on-chip RO is difficult to reflect the process variations of the PCB, which means it is suitable for identifying whether the IC rather than the PCB is counterfeit. For the proposed PTRO, by transmitting the oscillating signal from the IC to the PCB trace through I/O pins, the process variations of PCB traces and I/O pins are introduced, as shown in Figure 4. And through the novel PCB signature extraction method, which extracts signatures at different load modes of PCB, the overall impedance variations of the PCB would be further reflected. Therefore, the PTRO can generate a fingerprint that is applicable for both IC and PCB.

For example, if the PCB is tampered with by replacing the PCB substrate with a counterfeit one, the PCB traces and overall impendence would be changed, because it is not able for an attacker to replicate the exact manufacturing process. Then, the frequency of PTRO would be significantly affected, while the on-chip RO is not very sensitive to changes in the overall impedance and traces of the PCB. For PTRO, even if the overall impedance and traces change of the PCB is relatively small, the tampered PCB can be detected with high accuracy. Since most of components on the PCB have the same operating voltage as the connected I/Os of the IC with the authentication function, by switching the PCB to the high load mode, voltage fluctuations caused by changes in the overall impedance of the PCB would be amplified, as shown in Equation 7.

In conclusion, the frequency of PTRO is sensitive to the process variations of IC, I/Os, PCB traces and PCB overall impedance, so the signature generated by it is suitable as the fingerprint of both IC and PCB for simultaneous authentication. Compared with the IC fingerprint generated by on-chip RO PUF, it has a wider range of counterfeit PCB detection, e.g., the detection of authentic IC with recycled PCB substrate.

B. ROPA

The overview of the proposed ROPA structure in IC is shown in Figure 5, which is composed of several RO pairs, Counter, Timer, Controller, Signature Register and Physical Unclonable Function (PUF). And Figure 6 shows the proposed ROPA at PCB level.

1) RO PAIR

Each RO pair contains an ORO and a PTRO, which have the similar structure but different signal connections. The ORO is completely inside the IC, which is used to assist PTRO to reflect the IC process variation, aging degradation, power supply fluctuation, etc. The PTRO frequency fluctuation can additionally reflect the process variation and aging degradation of the PCB. The layout of ORO and PTRO on the chip are exactly the same.

As shown in Figure 5, the ORO is mainly composed of n inverters, where n is an odd number. The *RO_en* is used to control the ORO oscillation through an AND gate. And remaining two MUXs in ORO and an AND gate are used to maintain the same structure as the PTRO, so that the ORO can provide the PTRO with a reference frequency. The output of ORO is connected to a counter to measure its period.

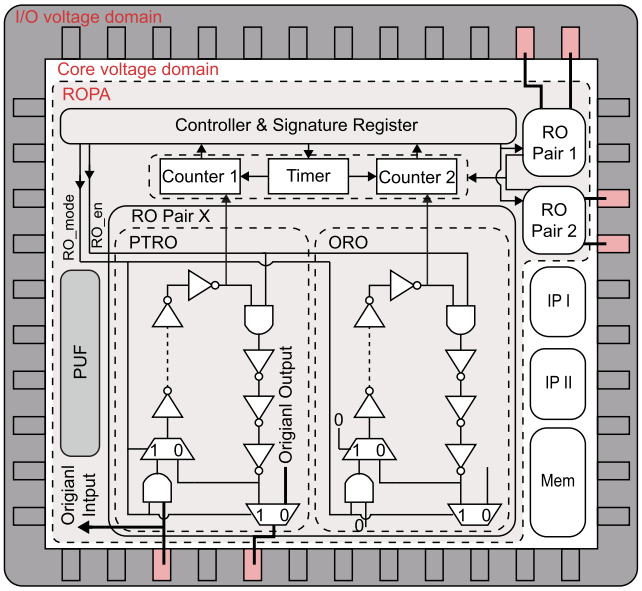


FIGURE 5. The overview of the proposed RO-based PCB authentication (ROPA) structure in IC.

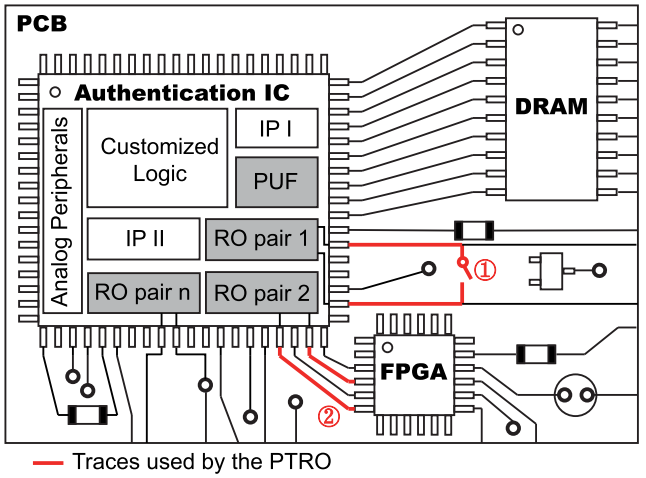


FIGURE 6. The proposed ROPA structure at PCB level. Three types of PCB traces marked by red lines, can be used to construct PTRO.

The oscillation period of the ORO can be expressed by Equation (10):

$$T_{ORO} = 2 * (\sum_{i=0}^{n} t_{INV_i} + t_{AND} + t_{MUX}) \tag{10}$$

where t_{INV_i}, t_{AND}, t_{MUX} are the delay of the ith inverter, AND gate and MUX gate in the ORO, respectively. By measuring the period variation of the ORO between different ICs and at different time, the tester can know the process variation between ICs and aging degradation of ICs.

As shown in Figure 5 and Figure 6, the PTRO is composed of CMOS based gates, input/output (I/O) pins, and PCB traces. And the structure of PTRO in the IC is the same as that of the ORO, except that the signal connection is different.

PTRO multiplexes the original I/Os of the IC. When $RO\_mode = 1$, the PTRO signal is output from the multiplexed output pin and returns to the IC through the PCB trace and the multiplexed input pin; when $RO\_mode = 0$, the multiplexed I/Os input/output normal signals.

As shown in Figure 6, there are two types of PCB traces can be used to construct PTRO:

- Type 1): The PCB designer can select a pair of existing PCB traces and connect them with switching devices, such as a transistor. And the PCB traces can pass through some capacitors, resistors or vias, etc. to introduce more process variations.
- Type 2): When an IC with authentication function is connected to a configurable IC, such as a FPGA, the I/Os of the configurable IC corresponding to PTRO can be configured to connect directly to form a loop. This type of PCB traces does not add additional area overhead and is difficult to be found by the attacker, which is the recommended type.

When $RO\_mode = 1$ and $RO\_en = 1$, the oscillation period of the PTRO can be expressed by Equation (1), where

$$t_{IC} = \sum_{i=0}^{n} t_{INV_i} + t_{AND} + t_{MUX} \tag{11}$$

When $RO\_mode = 0$ and $RO\_en = 1$, the signal propagation path of PTRO is exactly the same as that of ORO, at this time $T_{PTRO} = T_{ORO}$.

2) RO PAIR OPERATION MODE

There are two operation modes for the RO pair, which are the detection mode and aging mode.

For the RO pair, when $RO\_mode = 1$ and $RO\_en = 1$, both PRTO and ORO work in the detection mode. In this mode, the PTRO signal goes through the I/O pins and PCB traces, while the ORO oscillates on chip. The oscillation period of two types of RO is measured by counters and timer. By measuring the period when the PTRO and ORO run under different load modes of the PCB, the designer may authenticate whether the PCB under test is counterfeit. The detailed load modes of the PCB and authentication method will be described in Section IV.

And when $RO\_mode = 0$ and $RO\_en = 1$, PRTO and ORO work in aging mode. In this mode, the PTRO and ORO only oscillate within the IC, while the IC works normally. And the periodic signals they generate follow the same path, because the PTRO and ORO have the same layout on the chip. Hence, the RO pair ages simultaneously with the IC, while PTRO and ORO age at the same rate. By comparing the difference between the ORO oscillation period tested by the end user and the period at the PCB manufacturer, the designer can get the aging degree of the IC, thereby detecting whether the end user has used an over-aged IC. Since the PTRO and ORO have the same aging rate, the ORO can be used as a reference for PTRO to eliminate the aging factors of the IC, so that designers can obtain the overall aging state of the PCB.

Both ORO and PTRO are recommended to use aging-sensitive gates to construct.

3) COUNTER AND TIMER

The proposed technique requires two p-bit counters and one q-bit timer. Two counters are driven by the periodic pulses of PTRO and ORO, respectively. The count value of the counter is stored in the Signature Register for calculating the attached RO oscillation period. The timer, controlled by the Controller, is used to enable two counters. If the count value is P, with the timer enabling the counter Q reference clock cycles (T_{ref_clk}), the period under test (T_{RO}) is:

$$T_{RO} = \frac{T_{ref\_clk} Q}{P} \tag{12}$$

4) CONTROLLER AND SIGNATURE REGISTER

The Controller is designed to control RO pairs working mode through *RO_mode* and *RO_en* signals. And when RO pair is in detection mode, the Controller enables timer to measure the oscillation period of PTRO and ORO. The Signature Register is used to store the count values, which would be delivered to the PCB designer as the PCB's signature for authentic PCB database construing and counterfeit PCB detecting. The Signature Register can directly reuse the IC's existing memory, such as static random-access memory (SRAM).

5) PUF

PUF is utilized to give each IC a unique identification (ID). When the PCB is manufactured by the factory, the IC's ID and the signature of the PCB are delivered to the PCB designer to construct an authentic product database. When detecting counterfeit PCBs, the designer compares the signatures collected by the end user with the signatures in the authentic product database based on the ID of the IC. If it does not match, the PCB tested is considered as a counterfeit product.

For the proposed ROPA, PUF can be replaced by any other instance that can generate a unique ID for each IC. For security, the signature of the fresh manufactured PCB would not be stored locally. Hence, the designer needs an ID to index the PCB from the authentic product database, then the designer can get the corresponding fresh signature of the PCB to be authenticated.

For the proposed ROPA, the authentication is divided into two steps: 1) determine whether the ID of the PCB to be authenticated is in the database; 2) the signature of the PCB to be authenticated matches the signature in the database. The ID found in the database can only indicate that the IC on the PCB to be authenticated is registered, while other components on the PCB may not be authentic. If only ID is used to identify counterfeit PCBs, just unregistered PCBs can be identified, such as overproduced and cloned PCBs. And there is a risk of ID being modified. Therefore, it is necessary to introduce PTRO and ORO to further identify the recycled and tampered PCBs, and these two types of counterfeiting are more complicated.

Assuming that the PCB designer does not index by ID, but directly uses the signature value of the PCB to be authenticated to match the signatures in the authentic database. If a signature with a high degree of similarity can be found, then the PCB to be authenticated can be considered as an authentic one. However, the counterfeit coverage and detection accuracy of this method is insufficient. For example, if the performance of a fresh IC is at the fast-fast corner, and after aging, it might close to the slow-slow corner. The signatures extracted under both conditions may be found in the database, which means that some over-aged PCBs would not be identified as a counterfeit one. The accuracy of detecting recycled PCBs would decrease. Hence, it is necessary to introduce an ID to assist counterfeit detection.

Therefore, the proposed authentication methodology uses both ID and signature extracted by ROPA to detect counterfeit PCBs.

C. SECURITY ENHANCEMENT AND ANALYSIS

To ensure security, four countermeasures are adopted by the proposed ROPA methodology, including 1) the IC does not store the signature value extracted by ROPA, hence for the recycled, already tampered, or unregistered PCB, the attacker cannot extract the correct signature from them; 2) only at the given low load mode and high load mode, ROPA would be enabled for signature extraction; 3) the value of timer is determined by the PCB designer and stored in secure read-only memory, which is only accessed by the timer, and 4) the extracted signatures are firstly reordered and obfuscated together with IC's ID, and then encrypted before being sent to the designer.

With a counterfeit PCB, the main goal of the attacker is to predict or steal the correct signature value, which can pass the authentication of the PCB designer and deceive the end user. With countermeasure 1), there is no correct signature can be extracted from the recycled PCB, already tampered PCB, and unregistered PCB (overproduced and cloned PCB), and the attacker cannot disguise these counterfeit PCBs as authentic products.

The only way for the attacker is to use a fresh authentic PCB, try to obtain its correct signature, then replace the PCB substrate with a counterfeit one, and modify the signature of counterfeit PCB to the correct one. The fresh authentic PCB substrate is sold in other ways to obtain illegal profits. Modeling attack [44] is a common way to obtain signatures. The attacker can collect a subset of challenge-response pairs (CRPs) from signature generation instance (e.g. PUF) and using machine learning algorithms to predict more CRPs. However, with countermeasure 2), there are only two CRPs for the proposed ROPA, which is not suitable to implement modeling attack. And responses are encrypted making it hard for the attacker to obtain CRPs.

During ROPA extracting signatures, the attacker may directly measure the frequency of PTRO through PCB traces. But with countermeasure 3), the attacker cannot predict the

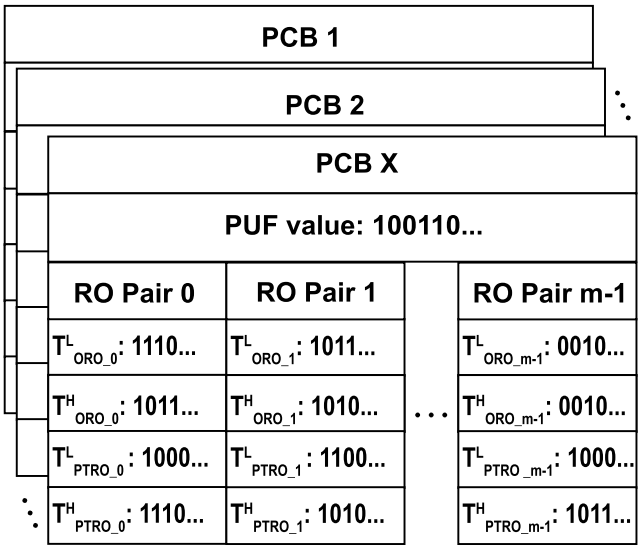


FIGURE 7. The signature of each PCB stored in authentic PCB database (APDB).

counter values without the timer value. In addition, it is hard for the attacker to obtain the frequency of ORO.

Furthermore, countermeasure 4) ensures that the signature is obfuscated and encrypted before being sent to the designer, and the attacker cannot read and tamper with the signature, which prevents the attacker from counterfeiting a PCB with the correct signature.

IV. PCB AUTHENTICATION METHODOLOGY

Through the proposed ROPA structure as discussed in Section III, the tester can extract the unique signature of each PCB, which can be used to construct authentic PCB database and detect counterfeit PCB.

A. AUTHENTIC PCB DATABASE CONSTRUCTION

After PCB is manufactured, the signature of each PCB is extracted by the PCB manufacturer during factory test. The detailed signature extraction method is as follows:

First, the tester sets the PCB into a low load mode. In this mode, only the designed ROPA structure and necessary circuits operate, which generates minimal voltage and temperature noise. Hence, the IC and PCB trace process variations dominate the oscillation period of ORO and PTRO.

Suppose there are m RO pairs in the PCB under test. The tester sequentially sets each pair of ROs in the detection mode to obtain two sets of data, $\mathbb{T}^L_{ORO}$ and $\mathbb{T}^L_{PTRO}$ (Equation (13)), which represent the count value of counters to m OROs and m PTROs, respectively. The PCB designer can calculate the oscillation period of RO through Equation (12) with the count value.

$$\mathbb{T}^L_{ORO} = \left\{T^L_{ORO\_0}, T^L_{ORO\_1}, \cdots T^L_{ORO\_m-1}\right\} \quad (13a)$$

$$\mathbb{T}^L_{PTRO} = \left\{T^L_{PTRO\_0}, T^L_{PTRO\_1}, \cdots T^L_{PTRO\_m-1}\right\} \quad (13b)$$

The $\mathbb{T}^L_{ORO}$ and $\mathbb{T}^L_{PTRO}$ mainly reflect the process variations of IC, I/Os, and part of PCB traces, which are unique on different PCBs.

Then, the tester sets the PCB into a high load mode. In this mode, the tester sequentially sets the RO pairs to work in the detection mode, while the I/Os in the I/O voltage domain where the activated RO pair is located are flipped at a relatively high speed, and the remaining circuits on the PCB are kept in a low active state. Similarly, the tester can obtain the period data of RO pairs in the high-load mode, which are $\mathbb{T}^H_{ORO}$ and $\mathbb{T}^H_{PTRO}$ (Equation (14)).

$$\mathbb{T}^H_{ORO} = \left\{T^H_{ORO\_0}, T^H_{ORO\_1}, \cdots T^H_{ORO\_m-1}\right\} \quad (14a)$$

$$\mathbb{T}^H_{PTRO} = \left\{T^H_{PTRO\_0}, T^H_{PTRO\_1}, \cdots T^H_{PTRO\_m-1}\right\} \quad (14b)$$

As high-speed I/Os flipping causes the corresponding I/O voltage to decrease significantly, the oscillation periods of PTRO increase. Due to process variations in the impedance of the PCB, the increase of the PTRO oscillation periods (ΔT_{PTRO}) on each PCB varies. For the tampered or over-aged PCB, the impedance is different from the original one, resulting in a mismatch between the ΔT_{PTRO} and data in the database.

All oscillation periods of RO pairs at different work load with the corresponding PUF value are used as a signature of PCB, which will be delivered to the PCB designer to construct the authentic PCB database (APDB). The architecture of APDB is illustrated in Figure 7.

B. COUNTERFEIT PCB DETECTION

In the supply chain, to prevent buying counterfeit PCBs from upstream suppliers, the verifier (such as system integrator, the end user, etc.) need to apply to the PCB designer/manufacture for PCBs authentication.

During authentication, the verifier first sets the PCB under test to low load mode and collects period data of OROs and PTROs, which are $u\mathbb{T}^L_{ORO}$ and $u\mathbb{T}^L_{PTRO}$, respectively. Then, the PCB under test is set to high load mode, the period data of OROs and PTROs are collected, which are $u\mathbb{T}^H_{ORO}$ and $u\mathbb{T}^H_{PTRO}$, respectively. These period data and the corresponding PUF value are delivered to the PCB designer/manufacturer, who owns the APDB, for signature matching. The PCB with mismatched signatures is considered as a counterfeit product. Figure 8 shows the PCB signature matching flow for counterfeit PCB detection.

PCB designer/manufacturer first looks up the PUF value of the PCB to be detected in the APDB. If it is not found, then the PCB to be detected is considered to be overproduced by the PCB manufacturer privately or cloned by an attacker in the supply chain through reverse engineering.

If the PUF value of PCB in APDB, then the PCB designer compares $u\mathbb{T}^L_{ORO}$ with $\mathbb{T}^L_{ORO}$. When $\left|u\mathbb{T}^L_{ORO} - \mathbb{T}^L_{ORO}\right| > \varepsilon^L_{ORO}$, where ε^L_{ORO} is the over-aged threshold of IC, the PCB under test is considered to be a tampered or recycled one. The

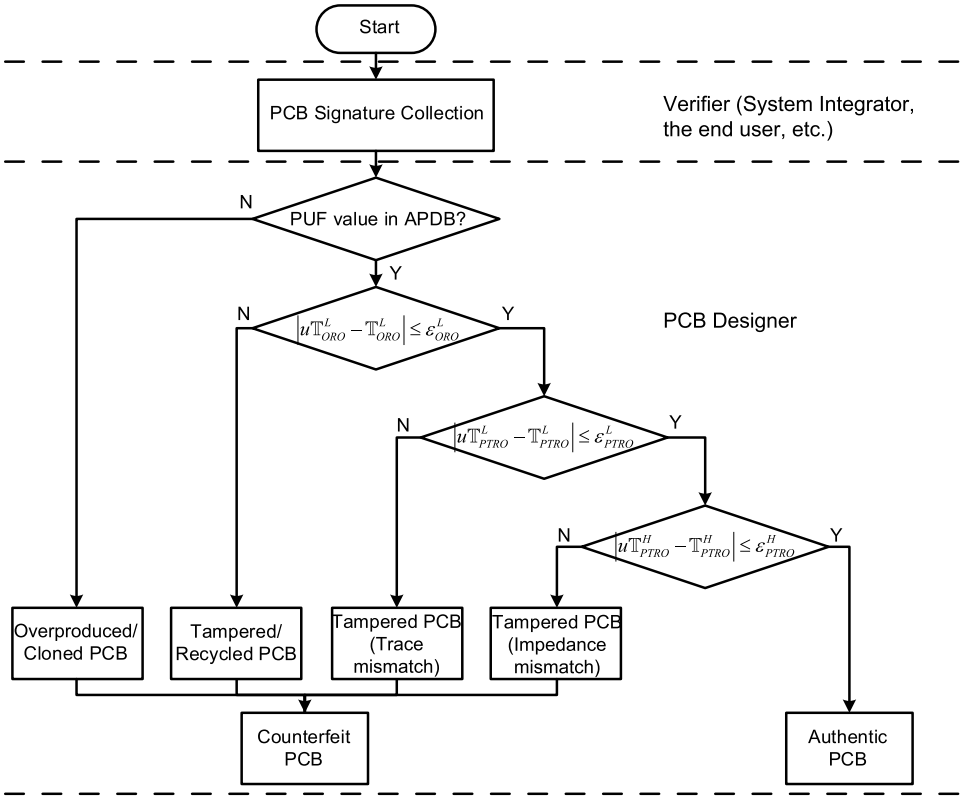


FIGURE 8. The PCB signature matching flow for counterfeit PCB detection based on the proposed technology.

attacker may maliciously alternative the IC with an over-aged IC or the whole PCB is recycled.

If the PCB under test meets the above two conditions, $u\mathbb{T}^L_{PTRO}$ is compared with $\mathbb{T}^L_{PTRO}$. When $\left|u\mathbb{T}^L_{PTRO}-\mathbb{T}^L_{PTRO}\right| > \varepsilon^L_{PTRO}$, where ε^L_{PTRO} is the PCB trace matching threshold, it means that the IC is authentic but the traces corresponding to PTROs do not match. Hence, this type of PCB may be caused by the attacker placing the authentic IC on the counterfeit PCB substrate (e.g. over-aged or cloned PCB substrate).

PCB traces matching cannot fully indicate that the PCB is authentic, and it is necessary to verify whether the overall impedance of the PCB matches. Therefore, when the PCB does not exceed the above two thresholds, the PCB designer calculates $\left|u\mathbb{T}^H_{PTRO}-\mathbb{T}^H_{PTRO}\right|$. If $\left|u\mathbb{T}^H_{PTRO}-\mathbb{T}^H_{PTRO}\right| > \varepsilon^H_{PTRO}$, where ε^H_{PTRO} is the PCB overall impedance mismatch threshold, the PCB is considered to be counterfeit except the IC with ROPA. The attacker can assemble the authentic IC on the recycled or cloned PCB to manufacture such counterfeit products.

$u\mathbb{T}^H_{ORO}$ is used to detect whether the power supply of the PCB under test is abnormal. If there is a big difference between $u\mathbb{T}^H_{ORO}$ and $\mathbb{T}^H_{ORO}$ in the high load mode, it is considered that the power supply used by the user is insufficient and the recommended power supply is required. This mechanism can avoid misjudgment of $u\mathbb{T}^H_{PTRO}$ in high load mode, which leads to the identification of authentic PCB as cloned or tampered PCB.

Finally, if the PCB meets all the above conditions, it can be regarded as an authentic product, otherwise it is a counterfeit product.

V. IMPLEMENTATION AND AUTHENTICATION FLOW

The implementation of the proposed ROPA and the authentication flow based on the ROPA, shown in Figure 9, is divided into the following steps.

Step 1 (PUF Integration): During IC design stage, the IC designer needs to integrate a PUF module into the original design. Generally, most of ICs contain a PUF, and the IC designer does not need to design a new PUF, additionally. The PUF value can be used to generate a unique ID for each IC.

Step 2 (ROPA Insertion): According to the I/O voltage domain of IC, the IC designer insert ROPA to ensure that each I/O voltage domain has at least one RO pair. Then, the modified IC design would be re-placed & routed to meet the timing requirement. It should be noted that if the target IC is FPGA, ROPA can either be integrated as a fixed peripheral during the FPGA design stage or be loaded into the programmable logic after FPGA fabrication. The designed IC will be delivered to the foundry for tape-out, and then sold to the downstream supply chain manufacturers.

Step 3 (PTRO Construction): If the PCB designer wants to enable ROPA to detect counterfeit PCBs, he/she needs to select PCB traces to construct PTROs during design stage. The detailed construction method of PTRO is shown in Section III.A. Type 2 PTRO is recommended.

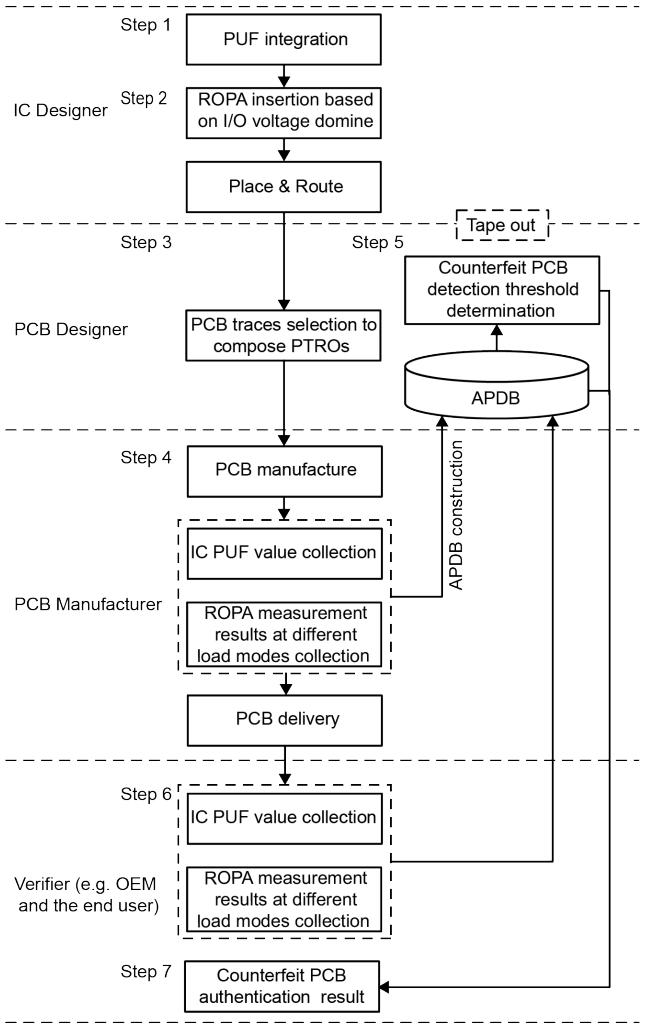


FIGURE 9. The implementation of the proposed ROPA and authentication flow based on the ROPA.

Step 4 (PCB Manufacture and Signature Collection): After the PCB design is completed, the PCB designer would deliver its layout to the PCB manufacturer for manufacturing. During the factory test of the PCB, the manufacturer needs to collect the signature of each PCB, which includes IC PUF value and ROPA measurement results at different load modes. These signatures would be sent to the PCB designer to construct APDB. PCBs that pass the factory test would be delivered to downstream manufacturers, such as OEM and system integrator, or the end user.

Step 5 (APDB Construction and Detection Threshold Determination): The PCB designer would construct APDB using PCB signatures as shown in Section IV.A. Then, the PCB designer can determine the counterfeit PCB detection threshold based on the APDB.

Step 6 (Signature Collection of PCB to be Authenticated): When users, such as OEMs and end users, purchase PCBs, they can apply for PCB authentication to prevent counterfeit PCB mixed into the system. To complete the authentication, the verifier need to set the ROPA to the detection mode and collect the signature of the PCB, including IC PUF value and ROPA measurement results at different load modes. The signature would be delivered to the PCB designer online.

Step 7 (ROPA Based Authentication): When receiving the signature of the PCB to be authenticated, the PCB designer compares it with the data in the APDB. If the signature exceeds the counterfeit PCB detection threshold, the PCB is considered to be a counterfeit product. The detailed methodology is shown in Section IV.B.

VI. EXPERIMENTAL RESULTS AND ANALYSIS

In this article, the ROPA is implemented with five RO pairs, two 16-bit counters, one 16-bit timer, and one controller. It should be noted that PUF is used to generate a unique ID, ROPA can directly use the existing PUF in IC without additional design. The ROPA is simulated in the benchmark circuit to estimate the overhead and tested on the FPGA development board for functional verification, respectively.

A. OVERHEAD

First, ROPA is integrated into several benchmark circuits from OpenSPARCT2, Gaisler, and OPENCORE, in a 32-nm technology node [45], for area and power overhead evaluation. The circuits were synthesized with 100MHz functional clock frequency and 10MHz scan clock.

As shown in Figure 5, the area and power overhead on IC level mainly from the RO pairs, counters and timer. From Table 2, it can be seen that the area overhead for ROPA on different benchmarks is limited to 0.160% - 0.428%. And the power overhead for ROPA on different benchmarks is limited to 0.219% - 0.673%. With a 100MHz functional clock, the signature extracting time is 20.5μs, which is negligible.

TABLE 2. The area and power overheads of ROPA.

IP Benchmark	VGA-LCD	FGU	Leon3s	b19
# SFF	17058	27931	17495	6042
Area Overhead	0.319%	0.160%	0.295%	0.428%
Power Overhead	0.270%	0.219%	0.258%	0.673%

B. APDB CONSTRUCTION AND COUNTERFEIT PCB MANUFACTURING

Then, a set of 28nm Altera 5CEFA4F23I7N FPGA development board is used to verify the effectiveness of ROPA on counterfeit detection. The I/O of this FPGA has only one reference voltage, which is 3.3V. All FPGA development boards are divided into 5 types, which includes authentic PCBs and all counterfeiting scenarios. The setup of PCB types are described in Table 3 and Figure 10.

Type 1 represents authentic PCB that the PCB designer authorizes the PCB manufacturer to manufacture, and its signature is stored in APDB. Type 2 represents the recycled PCB, on which ICs and other components are over-aged. Type 3 represents the tampered PCB, which means that the attacker replaces the faulty PCB substrate of an original system with

TABLE 3. The setup of PCB types including authentic PCBs and all counterfeiting scenarios.

#	Tpye	IC	PCB Substrate	Count
Type 1	Authentic	Authentic	Authentic	60
Type 2	Recycled	Counterfeit	Counterfeit	10
Type 3	Tampered	Authentic	Counterfeit	20
Type 4	Tampered	Counterfeit	Authentic	10
Type 5	Cloned	Counterfeit	Counterfeit	10

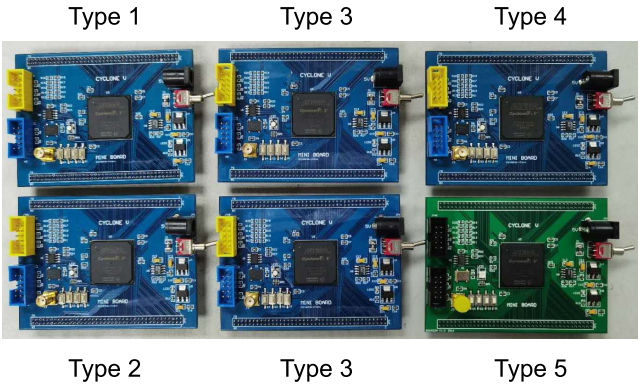


FIGURE 10. Authentic PCB and 4 types of counterfeit PCB.

a recycled one or other manufacturer produced one, each with 10 examples. Another type of tampered PCB, Type 4, represents that the attacker replacing failing IC with a counterfeit IC. Finally, Type 5 refers to the cloned PCB that the attacker obtains the PCB layout through reverse engineering and purchases counterfeit components to assemble.

The ROPA signatures for 60 authentic PCBs (Type 1) are collected to construct the APDB, as shown in Figure 11. It can be seen that the cycle of PTRO changes significantly under different load modes, and the cycle increment ($T^H_{PTRO\_i} - T^L_{PTRO\_i}$) is shown in the lower right corner of Figure 11.

If the signatures of different PCBs have a high degree of similarity, it is easy for an attacker to produce counterfeit products whose signatures are close to the authentic PCBs. Figure 12 shows the Euclidean distance distribution of $\mathbb{T}^L_{ORO}$, $\mathbb{T}^L_{PTRO}$, and $\mathbb{T}^H_{PTRO}$. The Euclidean distance is used to measure the similarity between two samples, which is calculated as follows:

$$d_{ij} = \sqrt{\sum_{k=0}^{m-1} \left| \mathbb{T}_{ik} - \mathbb{T}_{jk} \right|^2} \tag{15}$$

where m is the number of RO pairs in ROPA, and $\mathbb{T}_i$ and $\mathbb{T}_j$ are the ith and jth data set of ORO or PTRO's cycle, respectively. Hence, the average Euclidean distance can be expressed as:

$$D_{avg} = \frac{1}{n(n-1)} \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} d_{ij} (i \neq j) \tag{16}$$

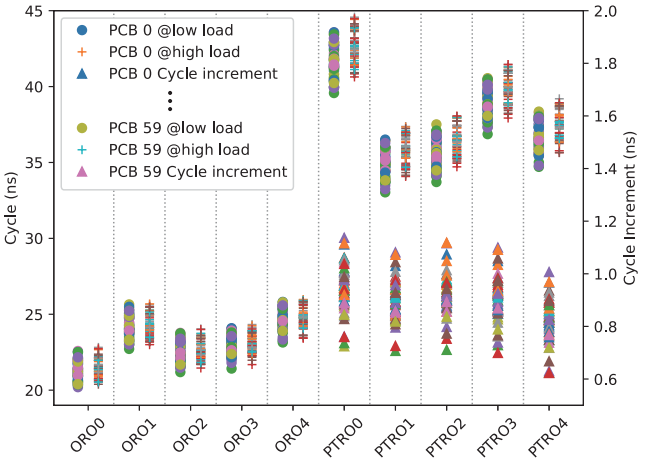


FIGURE 11. The ROPA signatures for 60 authentic PCBs (Type 1) in APDB, and the cycle increment of PTRO under different load modes.

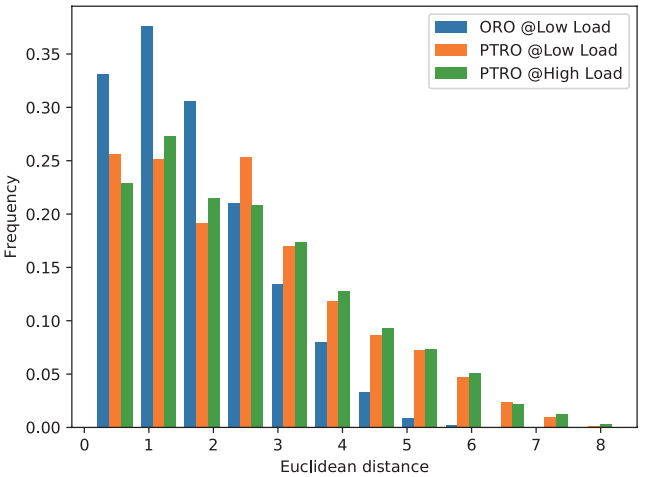


FIGURE 12. Euclidean distance distribution of $\mathbb{T}^L_{ORO}$, $\mathbb{T}^L_{PTRO}$, and $\mathbb{T}^H_{PTRO}$.

where n is the number of authentic PCBs in APDB. In this article, m and n are 5 and 60, respectively.

D_{avg} for $\mathbb{T}^L_{ORO}$, $\mathbb{T}^L_{PTRO}$, and $\mathbb{T}^H_{PTRO}$ are 1.761, 2.252. and 2.482, respectively, which demonstrates that the signatures in the APDB are unique and distinguishable.

C. OVERPRODUCED PCB DETECTION

An untrusted PCB manufacturer can produce more than the licensed number of PCBs. However, with ROPA, the PUF values of all PCBs shipped from the manufacturer are registered to the PCB designer, while the overproduced PCBs are not. When a user applies for authentication with an overproduced PCB, the PCB designer can directly determine it as a counterfeit product because it is not registered. Hence, the ROPA-based authentication flow can prevent overproduced PCBs.

D. RECYCLED PCB DETECTION

Ten authentic PCBs are burned-in under 85°C for 24 hours to mimic recycled PCBs (Type 2). The burn-in test equipment is

FIGURE 13. Burn-in test equipment to mimic recycled PCB (Type 2).

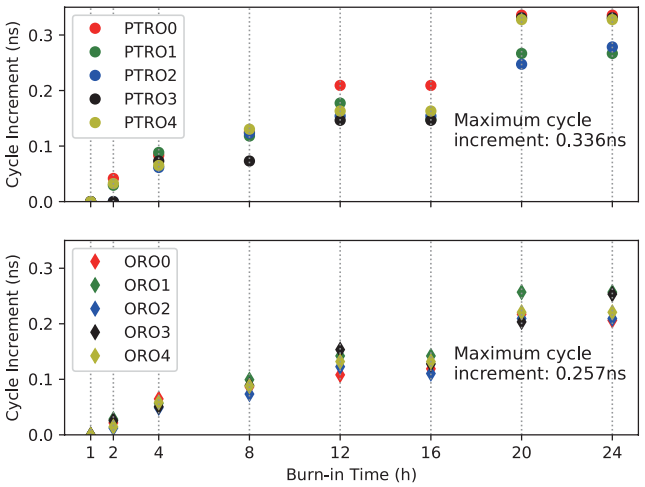


FIGURE 14. The cycle increment of OROs and PTROs during the 24-hour burn-in test of a single authentic PCB. The maximal cycle increment of OROs and PTROs are 0.257ns and 0.336ns, respectively.

shown in Figure 13. Figure 14 exhibits the cycle increment of OROs and PTROs during the 24-hour burn-in test of a single authentic PCB. The maximum cycle increment of OROs and PTROs are 0.257ns and 0.336ns, respectively. And the change of the cycle increment of PTROs (ΔT_{PTRO}) under different load modes during the 24-hour burn-in process is shown in Figure 15, the average value of which decreases from 1.025ns to 0.589ns. It can be seen that the aging rate of FPGA and other components on the PCB are different, which causes the change of ΔT_{PTRO}.

Figure 16 shows OROs cycle increment and Euclidean distance between 10 recycled PCBs and PCBs with the same PUF value in APDB. The IC aging threshold (ε^L_{ORO}) is set when the Euclidean distance is 0.224. It can be seen that all recycled PCBs fall above ε^L_{ORO}.

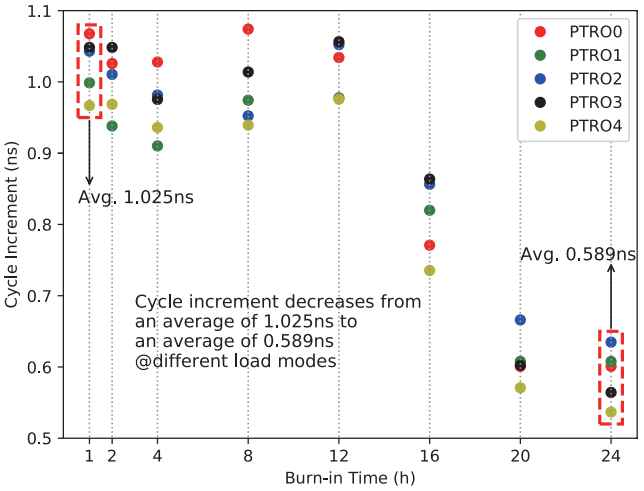


FIGURE 15. During the 24-hour burn-in process of a single authentic PCB, the change of the cycle increment of PTROs under different load modes, the average value of which decreases from 1.025ns to 0.589ns.

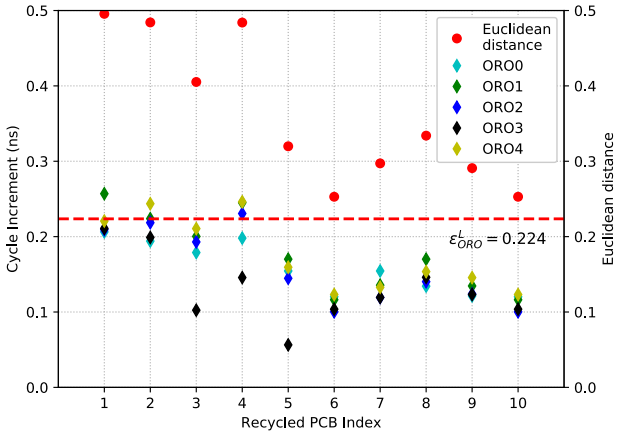


FIGURE 16. OROs cycle increment and Euclidean distance between 10 recycled PCBs and PCBs with the same PUF value in APDB. For all recycled PCBs, the Euclidean distance is greater than the IC aging threshold ($\varepsilon^L_{ORO} = 0.224$).

E. TAMPERED PCB DETECTION

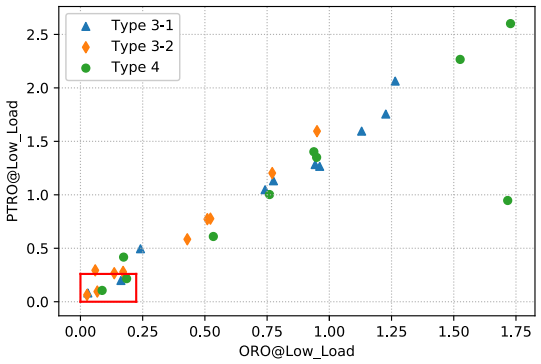
Thirty tampered PCBs are used to verify ROPA's ability to detect tampered PCBs, including using recycled PCB substrates (Type 3-1), non-factory original PCB substrates (Type 3-2) and recycled ICs (Type 4) to replace the corresponding parts of the authentic PCBs, each with 10 examples.

As shown in Figure 8, three Euclidean distance features can be used to detect counterfeit PCBs. Both the PCB trace mismatch threshold (ε^L_{PTRO}) and the PCB overall impedance mismatch threshold (ε^H_{PTRO}) are set to be 0.260. Figure 17(a) shows that only the Euclidean distance feature of ORO and PTRO at low load mode are used to detect tampered PCBs. And 80.0% of tampered PCBs are identified as counterfeit. Then all three Euclidean distance features are used to detect tampered PCBs, as shown in 17(b). The result shows that 29 tampered PCBs have at least one feature greater than the corresponding threshold, which means that 96.7% of tampered PCBs can be detected. Hence, introducing the

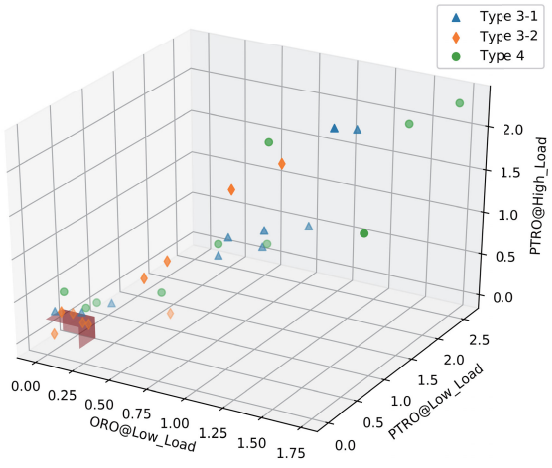
TABLE 4. The Comparison among ROPA, EMFORCED [46], secure physical enclosures (SPE) [47], and CIPA [23] .

Metrics	ROPA	EMFORCED [46]	SPE [47]	CIPA [23]
IC and PCB Co-authentication	Yes	No (only IC)	Yes	Yes
Allow Remote Authentication	Yes	No (need near-field EM probe)	Yes	Yes
Require PCB Modification	Yes (Low)*	No	Yes (High)	No
Design Effort	RO pairs and measurement circuits insertion, and PCB traces modification (Low) *	No	PCB covers, capacitive sensors, and evaluation unit (high)	RO array and measurement circuits (Low)
Overproduced PCB Detection	Yes	No	No	No
Recycled PCB Detection	Yes	Yes	No	No
Tampered PCB Detection	Yes	No (part of tampered PCB)	Yes	Yes
Cloned PCB Detection	Yes	No	No	No

* Without PCB traces modification when employs the Type 2 PTRO



(a) Only the Euclidean distance feature of ORO and PTRO at low load mode are used to detect tampered PCBs. The red box is the authentic area, and 80.0% of tampered PCBs are identified as counterfeit.



(b) All three Euclidean distance features are used to detect tampered PCBs. The red planes represent three thresholds. 96.7% of tampered PCBs can be detected.

FIGURE 17. The result of detecting tampered PCBs, using different number of Euclidean distance features. It can be seen that introducing the Euclidean distance of PTRO at high load mode can significantly improve the detection accuracy.

Euclidean distance of PTRO at high load mode significantly improves the detection accuracy.

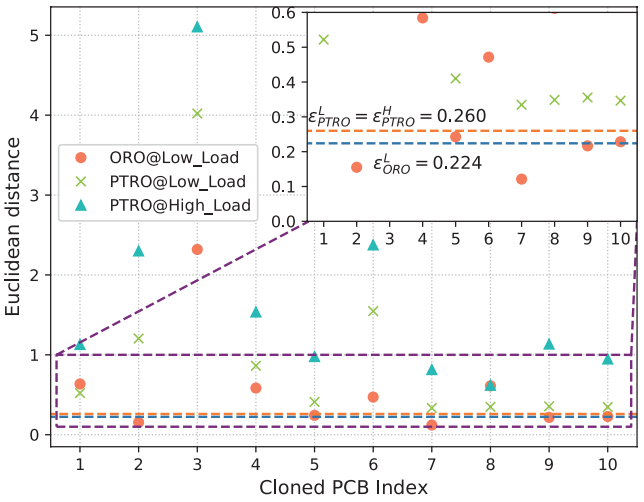


FIGURE 18. The Euclidean distance distributions between the cloned PCBs and the PCBs in APDB in the worst case.

F. CLONED PCB DETECTION

In this experiment, 10 cloned PCBs were manufactured through reverse engineering attacks. Because the PUF values of cloned PCBs are not in APDB, designers can directly determine that these PCBs are counterfeit. But if the PUF value is stored unencrypted, an attacker can read and modify the PUF value to the PUF value existing in APDB. In the worst case, the attacker happens to find the one in APDB with the smallest Euclidean distance from the cloned PCB. Figure 18 shows the Euclidean distance distributions between the cloned PCBs and the PCBs in APDB in the worst case. It can be seen that at least one feature of each cloned PCB is greater than the corresponding threshold, so all cloned PCBs can be regarded as counterfeit.

G. COMPARING WITH EXISTING TECHNIQUES

The comparisons of ROPA with major anti-counterfeit techniques, including EMFORCED [46], secure physical

enclosures (SPE) [47], and CIPA [23] are listed in Table 4. The results and analyses show that ROPA can detect overproduced, recycled, tampered and cloned PCBs with low design effort, and allows IC and PCB co-authentication remotely.

VII. CONCLUSION

In this article, a novel authentication methodology to detect counterfeit PCB through supply chain is proposed, which utilizes PCB trace-based ring oscillators assisted by on-chip ring oscillators to extract the signature of PCB. By switching the PCB to different load modes, the signature can reflect the difference in PCB traces and overall impedance. The ROPA can provide both IC and PCB authentication independently of external equipment, and allows remotely authentication for the user. The experiment results shows that the ROPA has insignificant area (0.301% on average) and power (0.355% on average) overhead. And the proposed method gives 96.7% confidence in detecting tampered PCBs and 100% confidence in detecting overproduced, recycled, and cloned PCBs.

REFERENCES

[1] R. A. McCormack, "Boeing's planes are riddled with chinese counterfeit electronic components," *Manuf. Technol. News*, vol. 19, p. 1, Jun. 2012. [Online]. Available: http://www.manufacturingnews.com/news/counterfeits615121.html

[2] X. Zhang, K. Xiao, and M. Tehranipoor, "Path-delay fingerprinting for identification of recovered ICs," in *Proc. IEEE Int. Symp. Defect Fault Tolerance VLSI Nanotechnol. Syst. (DFT)*, Oct. 2012, pp. 13–18.

[3] *Senate Armed Services Committee Releases Report on Counterfeit Electronic Parts*. Accessed: Mar. 18, 2020. [Online]. Available: https://www.armed-services.senate.gov/press-releases/senate-armed-services-committee-releases-report-on-counterfeit-electronic-parts

[4] M. M. Tehranipoor, U. Guin, and S. Bhunia, "Invasion of the hardware snatchers," *IEEE Spectr.*, vol. 54, no. 5, pp. 36–41, May 2017.

[5] A. Greenberg. *Planting tiny spy chips in hardware can cost as little as $200*. Accessed: Mar. 19, 2020. [Online]. Available: https://www.wired.com/story/plant-spy-chips-hardware-supermicro-cheap-proof-of-concept/

[6] A. Iyengar and S. Ghosh, "Hardware trojans and piracy of PCBS," in *The Hardware Trojan War*. Cham, Switzerland: Springer, 2018, pp. 125–145.

[7] *How to Protect Your PCB Designs From Counterfeit Electronic Components*. Accessed: Mar. 19, 2020. [Online]. Available: https://resources.altium.com/pcb-design-blog/how-to-protect-your-pcb-designs-from-counterfeit-electronic-components

[8] K. Huang, J. M. Carulli, and Y. Makris, "Parametric counterfeit IC detection via support vector machines," in *Proc. IEEE Int. Symp. Defect Fault Tolerance VLSI Nanotechnol. Syst. (DFT)*, Oct. 2012, pp. 7–12.

[9] H. Dogan, D. Forte, and M. M. Tehranipoor, "Aging analysis for recycled FPGA detection," in *Proc. IEEE Int. Symp. Defect Fault Tolerance VLSI Nanotechnol. Syst. (DFT)*, Oct. 2014, pp. 171–176.

[10] Z. Guo, X. Xu, M. M. Tehranipoor, and D. Forte, "FFD: A framework for fake flash detection," in *Proc. 54th Annu. Design Autom. Conf.*, Jun. 2017, pp. 1–6.

[11] P. Song, F. Stellari, and A. Weger, "Counterfeit IC detection using light emission," in *Proc. Int. Test Conf.*, Oct. 2014, pp. 1–8.

[12] X. Wang, D. Tran, S. George, L. Winemberg, N. Ahmed, S. Palosh, A. Dobin, and M. Tehranipoor, "Radic: A standard-cell-based sensor for on-chip aging and flip-flop metastability measurements," in *Proc. IEEE Int. Test Conf.*, Nov. 2012, pp. 1–9.

[13] J. Couch and J. Arkoian, "An investigation into a circuit based supply chain analyzer for FPGAs," in *Proc. 26th Int. Conf. Field Program. Log. Appl. (FPL)*, Aug. 2016, pp. 1–9.

[14] S. E. Quadir, J. Chen, D. Forte, N. Asadizanjani, S. Shahbazmohamadi, L. Wang, J. Chandy, and M. Tehranipoor, "A survey on chip to system reverse engineering," *ACM J. Emerg. Technol. Comput. Syst.*, vol. 13, no. 1, pp. 1–34, Dec. 2016.

[15] N. Asadizanjani, S. Shahbazmohamadi, M. Tehranipoor, and D. Forte, "Non-destructive PCB reverse engineering using X-ray micro computed tomography," in *Proc. 41st Int. Symp. Test. Failure Anal.*, Nov. 2015, pp. 1–5.

[16] Z. Guo, M. Tehranipoor, D. Forte, and J. Di, "Investigation of obfuscation-based anti-reverse engineering for printed circuit boards," in *Proc. 52nd Annu. Design Autom. Conf.*, Jun. 2015, pp. 1–6.

[17] K. Chatterjee and D. Das, "Semiconductor Manufacturers' efforts to improve trust in the electronic part supply chain," *IEEE Trans. Compon. Packag. Technol.*, vol. 30, no. 3, pp. 547–549, Sep. 2007.

[18] L. Wei, C. Song, Y. Liu, J. Zhang, F. Yuan, and Q. Xu, "BoardPUF: Physical unclonable functions for printed circuit board authentication," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design (ICCAD)*, Nov. 2015, pp. 152–158.

[19] U. Guin, S. Bhunia, D. Forte, and M. M. Tehranipoor, "SMA: A system-level mutual authentication for protecting electronic hardware and firmware," *IEEE Trans. Dependable Secure Comput.*, vol. 14, no. 3, pp. 265–278, Jun. 2017.

[20] A. Hennessy, Y. Zheng, and S. Bhunia, "JTAG-based robust PCB authentication for protection against counterfeiting attacks," in *Proc. 21st Asia South Pacific Design Autom. Conf. (ASP-DAC)*, Jan. 2016, pp. 56–61.

[21] F. Zhang, A. Hennessy, and S. Bhunia, "Robust counterfeit PCB detection exploiting intrinsic trace impedance variations," in *Proc. IEEE 33rd VLSI Test Symp. (VTS)*, Apr. 2015, pp. 1–6.

[22] J. R. Hamlet, M. T. Martin, and N. J. Edwards, "Unique signatures from printed circuit board design patterns and surface mount passives," in *Proc. Int. Carnahan Conf. Secur. Technol. (ICCST)*, Oct. 2017, pp. 1–6.

[23] X. Wang, Y. Han, and M. Tehranipoor, "System-level counterfeit detection using on-chip ring oscillator array," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 27, no. 12, pp. 2884–2896, Dec. 2019.

[24] Y. Han, X. Wang, and M. Tehranipoor, "CIPA: Concurrent IC and PCB authentication using on-chip ring oscillator array," in *Proc. IEEE 27th Asian Test Symp. (ATS)*, Oct. 2018, pp. 109–114.

[25] K. Yang, D. Forte, and M. Tehranipoor, "An RFID-based technology for electronic component and system counterfeit detection and traceability," in *Proc. IEEE Int. Symp. Technol. for Homeland Secur. (HST)*, Apr. 2015, pp. 1–6.

[26] J.-L. Zhang, G. Qu, Y.-Q. Lv, and Q. Zhou, "A survey on silicon PUFs and recent advances in ring oscillator PUFs," *J. Comput. Sci. Technol.*, vol. 29, no. 4, pp. 664–678, Jul. 2014.

[27] J. Villasenor and M. Tehranipoor, "Chop shop electronics," *IEEE Spectr.*, vol. 50, no. 10, pp. 41–45, Oct. 2013.

[28] N. Asadizanjani, M. Tehranipoor, and D. Forte, "PCB reverse engineering using nondestructive X-ray tomography and advanced image processing," *IEEE Trans. Compon., Packag., Manuf. Technol.*, vol. 7, no. 2, pp. 292–299, Feb. 2017.

[29] P. Ghosh and R. S. Chakraborty, "Recycled and remarked counterfeit integrated circuit detection by image-processing-based package texture and indent analysis," *IEEE Trans. Ind. Informat.*, vol. 15, no. 4, pp. 1966–1974, Apr. 2019.

[30] U. Guin, K. Huang, D. DiMase, J. M. Carulli, 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, Aug. 2014.

[31] R. S. Chain, "Counterfeit parts DOD needs to improve reporting and oversight to," U.S. Government Accountability Office, Washington, DC, USA, Tech. Rep. GAO-16-236, 2016.

[32] H. Johnson, H. Johnson, and M. Graham, *High-speed Signal Propagation: Advanced Black Magic* (PTR Signal Integrity Library). Upper Saddle River, NJ, USA: Prentice-Hall, 2003.

[33] I. J. Bahl and D. K. Trivedi, "A designer's guide to microstrip line," *Microwave*, vol. 16, pp. 174–182, May 1977.

[34] J.-H. Kim, S.-W. Han, and O.-K. Kwon, "Analysis of via in multilayer printed circuit boards for high-speed digital systems," in *Proc. Adv. Electron. Mater. Packag.*, 2001, pp. 382–387.

[35] G. W. Hannaman and C. D. Wilkinson, "Evaluating the effects of aging on electronic instrument and control circuit boards and components in nuclear power plants," Electr. Power Res. Inst. (US), Washington, DC, USA, Tech. Rep. 000000000001011709, 2005.

[36] J. M. Rabaey, A. P. Chandrakasan, and B. Nikoli, *Digital Integrated Circuits: A Design Perspective*, vol. 7. Upper Saddle River, NJ, USA: Pearson, 2003.

[37] K. Yang, D. Forte, and M. Tehranipoor, "Analytical model to estimate FinFET's i_{ON}, i_{OFF}, SS, and v_T distribution due to FER," in *Proc. IEEE Int. Symp. Technol. Homeland Secur.*, Dec. 2015, pp. 1–6.
[38] W. Abadeer, W. Tonti, W. Hansch, and U. Schwalke, "Bias temperature reliability of n^+ and p^+ polysilicon gated NMOSFETs and PMOSFETs," in *Proc. 31st Annu. Proc. Rel. Phys.*, 1993, pp. 147–149.
[39] M. A. Alam and S. Mahapatra, "A comprehensive model of PMOS NBTI degradation," *Microelectron. Rel.*, vol. 45, no. 1, pp. 71–81, Jan. 2005.
[40] E. Takeda, Y. Nakagome, H. Kume, and S. Asai, "New hot-carrier injection and device degradation in submicron MOSFETs," *IEE Proc. I-Solid-State Electron Devices*, vol. 130, no. 3, pp. 144–150, Jun. 1983.
[41] B. Pandey and G. Singh, "Simulation of CMOS IO standard based energy efficient gurmukhi unicode reader on FPGA," in *Proc. Int. Conf. Comput. Intell. Commun. Netw.*, Nov. 2014, pp. 917–920.
[42] M. Mergens, G. Wybo, B. Van Camp, B. Keppens, F. De Ranter, K. Verhaege, P. Jozwiak, J. Armer, and C. Russ, "ESD protection circuit design for ultra-sensitive IO applications in advanced sub-90 nm CMOS technologies," in *Proc. IEEE Int. Symp. Circuits Syst.*, May 2005, pp. 1194–1197.
[43] G. Esch and T. Chen, "Design of CMOS IO drivers with less sensitivity to process, voltage, and temperature variations," in *Proc. 2nd IEEE Int. Workshop Electron. Design, Test Appl.*, Jan. 2004, pp. 312–317.
[44] J. Shi, Y. Lu, and J. Zhang, "Approximation attacks on strong PUFs," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 39, no. 10, pp. 2138–2151, Oct. 2020.
[45] (2016). *Synopsys 32/28nm Generic Library*. [Online]. Available: http://www.synopsys.com/Community/UniversityProgram/Pages/genericlibraries.aspx
[46] A. Stern, U. Botero, F. Rahman, D. Forte, and M. Tehranipoor, "EMFORCED: EM-based fingerprinting framework for remarked and cloned counterfeit IC detection using machine learning classification," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 28, no. 2, pp. 363–375, Feb. 2020.
[47] V. Immler, J. Obermaier, K. K. Ng, F. X. Ke, J. Lee, Y. P. Lim, W. K. Oh, K. H. Wee, and G. Sigl, "Secure physical enclosures from covers with tamper-resistance," *IACR Trans. Cryptograph. Hardw. Embedded Syst.*, vol. 7, pp. 51–96, Nov. 2018.

DONGRONG ZHANG (Member, IEEE) received the B.S. degree in electrical engineering from Beihang University, Beijing, China, in 2016, where he is currently pursuing the Ph.D. degree in electronic science and technology. His current research interests include hardware security and reliability, which include on-chip monitoring, physical design, on-chip dynamic adaptation methodologies, and counterfeit IC/PCB detection.

QIANG REN (Member, IEEE) received the B.S. degree in electrical engineering from Beihang University, Beijing, China, in 2008, the M.S. degree in electrical engineering from the Institute of Acoustics, Chinese Academy of Sciences, Beijing, in 2011, and the Ph.D. degree in electrical engineering from Duke University, Durham, NC, USA, in 2015. From 2016 to 2017, he was a Postdoctoral Researcher with the Computational Electromagnetics and Antennas Research Laboratory (CEARL), The Pennsylvania State University, University Park, PA, USA. In September 2017, he joined the School of Electronics and Information Engineering, Beihang University, as an "Excellent Hundred" Associate Professor. His current research interests include numerical methods for multiscale and multiphysics modeling, metasurfaces, inverse scattering, and parallel computing. He was a recipient of the Young Scientist Award of the 2018 International Applied Computational Electromagnetics Society (ACES) Symposium in China. He serves as a Reviewer for 30 journals. He serves as an Associate Editor for *ACES Journal* and *Microwave and Optical Technology Letters (MOTL)*.

DONGLIN SU (Senior Member, IEEE) received the B.S., M.S., and Ph.D. degrees in electrical engineering from Beihang University (BUAA), Beijing, China, in 1983, 1986, and 1999, respectively. In 1986, she joined the Faculty of the School of Electronics and Information Engineering, BUAA, where she was first an Assistant, then a Lecturer, and later an Associate Professor, and is currently a Full Professor. From 1996 to 1998, she was a Visiting Scholar with the Department of Electrical Engineering, University of California at Los Angeles (UCLA), Los Angeles, CA, USA, under the BUAA-UCLA Joint Ph.D. Program. She has authored more than 100 articles and coauthored several books. Her research interests include the numerical methods for microwave and millimeter-wave integrated circuits and systematic electromagnetic compatibility design of various aircrafts. She is a member of the Chinese Academy of Engineering. She is a Fellow of the Chinese Institute of Electronics. She received the National Science and Technology Advancement Award of China in 2007 and 2012 and the National Technology Invention Award of China in 2018. She is also the Chair of the Beijing Chapter of the IEEE Antennas and Propagation Society and the Deputy Chair of the Antennas Society and the Chinese Institute of Electronics.