System-Level Counterfeit Detection Using On-Chip Ring Oscillator Array

Xiaoxiao Wang, Yueying Han, and Mark Tehranipoor, *Fellow, IEEE*

***Abstract*— Counterfeiting has unfortunately become a worldwide epidemic affecting electronic systems from consumer goods to military equipment, which seriously jeopardizes system security, reliability, and electronic vendors' reputation. The counterfeit parts, e.g., integrated circuits (ICs) and printed circuit boards (PCBs), have shown a significant increase in type and number over the recent years. However, the existing counterfeit detection techniques deal with IC or PCB separately, and hence, they cannot verify the authenticity of an electronic system as a whole. In this paper, we propose concurrent IC and PCB authentication (CIPA), a novel methodology that concurrently verifies the authenticity of both IC and PCB through extracting the signature pairs generated by a ring oscillator (RO) array without/with PCB cavity resonance. With CIPA, remote authentication is allowable by transmitting the signatures between the verifier and the system vendor. The CIPA structure has shown insignificant area overhead (0.945% on average) when implemented on a number of benchmarks. Both CIPA and the benchmarks have been implemented on the authentic and counterfeit FPGA systems, and the results give 100% confidence in detecting counterfeit ones. Furthermore, the authenticity of PCB and IC (i.e., authentic or counterfeit) of the system under test can also be mined from CIPA signatures. According to the experimental results, systems composed of different authenticity states of PCB and IC are differentiated from each other with the confidence of 97.62%. The overall authentication time is 40.2 μs considering 50-MHz system clock.**

***Index Terms*— Counterfeit, sensors, supply chain security.**

I. Introduction

TODAY, most of the integrated circuit (IC) design houses provide products in a manner of the subsystem, which offers programming capacity to accelerate IC buyer's product development. The subsystem provided by design houses usually contains the IC product as well as a printed circuit board (PCB), which communicate IC with the outside world. Currently, the design houses, higher level system vendors, distributors, and end users, which are separate parts of a supply chain, are distributed all over the globe. Driven by illegal profits, the electronic subsystem is a popular target for counterfeiting [1]. As an example, the supply chain of high-end transportation and network systems has been seriously polluted [2], [3] by counterfeiting. Data show that the electronic system businesses are losing more than 250 billion each year due to counterfeiting [4].

It is obvious that, due to the unknown sources of the system components, the quality of the subsystem is not assured. Worse is that the counterfeit systems with some or all of the components replaced without design house's supervision may contain malicious firmware or hardware, which severely threatens the system security [5].

To avoid counterfeiting and preventing respective security issues in the field, counterfeit subsystem need to be detected first. However, majority of the existing detection techniques focus on the detection of individual components [i.e., field-programmable gate array (FPGA) and memory] [6]–[8] or counterfeit PCB [9]–[11], which cannot provide system-level authentication. Reference [12] proposed a system-level radio-frequency identification (RFID)-based counterfeit detection technique, which employs a PCB RFID tag to transmit the physical unclonable function (PUF; see [13]) values of all ICs on PCB. However, this technique requires to integrate both PUF and controller on each IC, as well as RFID tag and antenna on PCB, which increases an authentication cost. Furthermore, the existing system-level counterfeiting detection techniques require physical access to the suspicious system with external equipment, which causes equipment dependence and prohibits secure remote authentication.

In this paper, we present concurrent IC and PCB authentication (CIPA), a system-level authentication methodology that utilizes novel on-chip infrastructure as well as a remote authentication flow. CIPA employs an on-chip structure to extract the signature pairs of an on-chip ring oscillator (RO) array without/with PCB cavity resonance and identifies the specific process variations of both IC and PCB in the system under test, which has the following advantages.

1) CIPA concurrently verifies the authenticity of both IC and PCB, which enables system-level authentication.
2) The RO array is all-digital, with low area, power, and design overhead. No PCB modification is required.
3) It allows remote authentication with no extra equipment needed.
4) The authentication process tolerates the uncertainty of voltage supply and aging at the verifier's side.

Manuscript received February 7, 2019; revised June 15, 2019; accepted July 15, 2019. Date of publication September 30, 2019; date of current version November 22, 2019. This work was supported by the National Science Foundation of China (NSFC) under Grant 61631002 and Grant 61504007. *(Corresponding author: Xiaoxiao Wang.)*

X. Wang and Y. Han are with the School of Electronics and Information Engineering, Beihang University, Beijing 100191, China (e-mail: wangxiaoxiao@buaa.edu.cn).

M. Tehranipoor is with the Electrical and Computer Engineering (ECE) Department, University of Florida, Gainesville, FL 32611 USA (e-mail: tehranipoor@ece.ufl.edu).

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVLSI.2019.2930532

The verifier can be an original equipment manufacturer (OEM), electronic manufacturing supplier (EMS), or end user.

The rest of this paper is organized as follows. Section II presents the threats of counterfeiting. Section III analyzes PCB and IC's process variations' impacts on RO oscillation. It then proposes the CIPA-Based system-level authentication. Section IV describes the proposed system-level authentication flow. Section V shows the experimental results for the FPGA-based system. Finally, concluding remarks are given in Section VI.

II. Threat Models and Objectives

This section presents the threat models for system-level counterfeiting, which also derives the motivation behind developing CIPA.

A. Counterfeiter's Objectives

Generally, counterfeiting effort is made for illegal purposes, either illegal profits or attacks. The purposes of counterfeiters can be categorized as follows.

1) *Obtain illegal profits [2], [3]:* Most of the counterfeit systems are made for illegal purposes. Through cloning, refurbishing, or recycling, the counterfeiter either escapes the efforts of design, fabrication, system integration, or all the above. Hence, the counterfeit systems are usually sold at a much lower price and can easily infiltrate into the supply chain. However, the interest of all legal entities in the supply chain is negatively impacted due to the market and reputation losses.
2) *Attack the target system maliciously:* The safety-critical systems can be the victims of counterfeiting. Worse still, the counterfeit systems that flow into the military supply chain can cause catastrophic failures [14]. To attack the safety-critical systems, original ICs in those systems can be replaced by a counterfeit one, which might include hardware Trojans [15], [16]. Such a counterfeiting attack can take place both during manufacturing or when the system is in use. Specifically, when the system is used in the field with similar appearance, the impact of original IC replacement can be considered as a normal power off and restart. It should be noted that, since the PCB's design is visible, it is usually neglected in the threat model. However, malicious hardware can be inserted into PCB as well. For example, as reported by [17], a malicious eavesdropping and transmitting chip is suspected to be inserted into a motherboard used by the data server during fabrication.

B. Counterfeiting Methods

The counterfeit systems can be divided into the following types according to the counterfeiting methods.

1) *Recycled subsystems:* For the long-lasting subsystem in the market, counterfeiters simply clean, polish, and renew the whole used but still functional retired system and remark them as new [18]. Since the recycled systems have already been used in the field, the probability of system failure increases significantly.
2) *Refurbished subsystem:* Defective systems are identified in the process of manufacturing, distribution, acceptance test, and usage within the supply chain. These systems should be discarded or returned to the design house for diagnostic. However, these defective subsystem can be the target of the counterfeiters. As the subsystem failure is caused by the failure of components, the counterfeiters may/may not replace the failed components with the ones of similar appearance (e.g., cloned or recycled part) and then sell the refurbished systems as authentic ones in the supply chain [19]. As the refurbishing process is not supervised by the design house, the refurbished systems are likely to have low reliability.
3) *Counterfeit subsystem built from scratch:* Due to the rapid development of IC and PCB cloning techniques [20], the counterfeiting methods are not limited to remarking, repackaging, or fixing the original systems. Instead, the counterfeiters can build the cloned PCB by reverse-engineering the original PCB, purchasing all system components (i.e., ICs, FPGAs, memories, and resistors), and integrating them together. Therefore, the entire subsystem can be built from scratch [1]. It is obvious that, due to the unknown sources of the system components, the quality of this type of subsystem is not assured, and furthermore, the system may contain a malicious change that could lead to information leakage.

TABLE I
Various Categories of PCB Systems in the Market

	Type A	Type B	Type C	Type D
IC	Authentic	Authentic	Counterfeit	Counterfeit
PCB	Authentic	Counterfeit	Authentic	Counterfeit
System	Authentic	Counterfeit	Counterfeit	Counterfeit

C. Taxonomy of PCB Systems Considering Counterfeiting

Depending on the authentic/counterfeit state of IC and PCB, the systems in the market can be categorized into the following types (see Table I).

1) *Type A:* In this type, both IC and PCB in the system are authentic.
2) *Type B:* The counterfeiter replaces an original but defective PCB with a cloned one. Thus, this type of counterfeit system has authentic IC with counterfeit PCB [21].
3) *Type C:* For functional or attacking purposes, the original IC in the system is replaced by a counterfeit one with a similar appearance. Hence, in this case, the IC may be faked; however, the PCB is authentic.
4) *Type D:* For this type of counterfeit system, both IC and PCB are counterfeited by either recycling or cloning. By making a large volume of Type D systems, the counterfeiter aims at getting large illegal profit.

D. Authentication Objectives

The drawbacks of the existing anti-counterfeit methodologies were summarized in Section I. To overcome these drawbacks, CIPA should meet the following objectives.

- *Objective 1:* CIPA should be able to detect counterfeit IC from authentic ones within the supply chain. Furthermore, it should be able to identify the type (see Table I) of the counterfeit system.
- *Objective 2:* CIPA should be able to disable the counterfeit systems once detected.
- *Objective 3:* CIPA should be implemented reliably to enable the authentication by authorized entities within the supply chain whether on-site or remotely.

III. Counterfeit System Detection Using CIPA

As mentioned in Section I, CIPA utilizes novel on-chip infrastructure as well as a remote authentication flow. RO is the main component of the on-chip infrastructure.

The oscillation period of RO is determined by various parameters. According to (1) [22], [23], the delay of a CMOS or FinFET inverter, which is the fundamental element of RO, can be expressed as

$$t_d = \frac{C_L \mathrm{VDD}}{\mu C_{\mathrm{ox}} \frac{W}{L} (\mathrm{VDD} - V_{\mathrm{th}})^{\alpha}} \tag{1}$$

where C_L, μ, C_{ox}, W, L, VDD, and V_{th} are the gate load capacitance, mobility, gate oxide capacitance, gate width, gate length, RO power supply, and threshold voltage, respectively. α is a constant determined by the fabrication process. From (1), it can be seen that the inverter delay, which forms the RO oscillation period, is determined by both IC process parameters and power supply VDD. As shown in Fig. 1(a), VDD is delivered from the external power supply (V_{supply}) through PCB and IC power distribution networks (PDNs) and finally to the RO cells. According to the voltage division law [see (2)], the impedance of the PCB PDN (Z_{PCB}) is a major parameter influencing the RO VDD. As shown in Section III-A, the value of Z_{PCB} is a function of PCB process parameters. Therefore, in this section, the relationship between RO oscillation period to both IC and PCB process parameters is constructed, which generates the theoretical basis for CIPA-BASED counterfeiting system detection

$$\mathrm{VDD}(w) = V_{\mathrm{supply}} \frac{Z_{\mathrm{IC}}(w)}{Z_{\mathrm{IC}}(w) + Z_{\mathrm{PCB}}(w)}. \tag{2}$$

A. PCB Process Parameters' Impact on RO Oscillation

Fig. 1 shows the structural and lumped circuit model [24] for the PDN of PCB. From Fig. 1(a), it can be seen that the power and ground planes form cavities. The electromagnetic waveform initiated by the ac current on the power and ground planes propagates along the length and width of the cavity and reflects at the cavities' boundary wall. Hence, if the PCB dimension is an integral multiple of half of the electromagnetic wavelength, standing waveform forms in the cavity, as shown in Fig. 2. Thus, the resonance takes place in the cavity. It is obvious that, when the electromagnetic wave resonates between the PCB cavity walls, the energy is locked inside

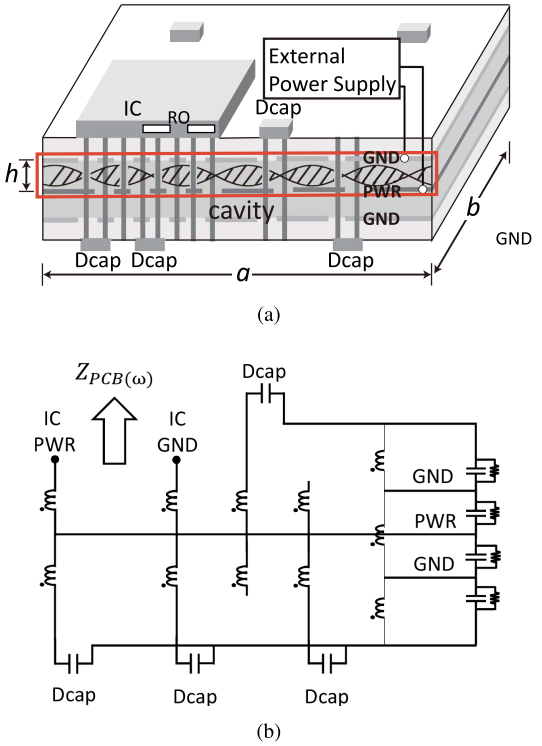


Fig. 1. (a) Structure of PCB PDN, in which the power and ground planes form the cavity. (b) Lumped circuit model of PCB PDN. Z_{PCB} is the impedance of the PCB PDN seen by the IC.

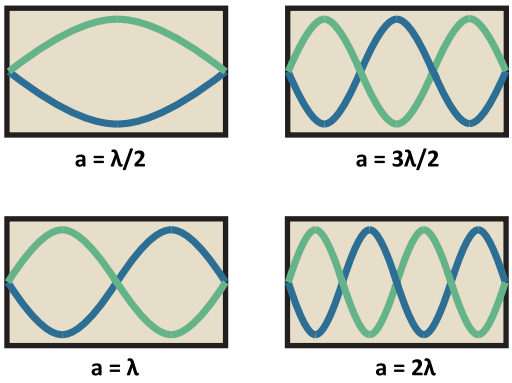


Fig. 2. Standing waveforms inside the PCB cavity.

the PCB and cannot be propagated to IC or RO. As a result, IC "sees" a significantly higher Z_{PCB} compared with the nonresonant cases.

The propagation behavior of the electromagnetic waveform of a certain frequency can also be described by the circuit model [see Fig. 1(b)], which is consisted of the interconnect parasitic capacitances, inductances, and the decoupling capacitances. It should be noted that the two models have no conflict, while the circuit model represents the higher abstraction level of the propagation behavior.

The following equation gives the value of Z_{PCB} in relation to the operation frequency, where a and b are the x- and y-dimensions of PCB, x_i and y_i are the locations of the impedance probe, d_{xi} and d_{yi} are the dimensions of the port where the probe is located, $\chi_{mn} = 1$

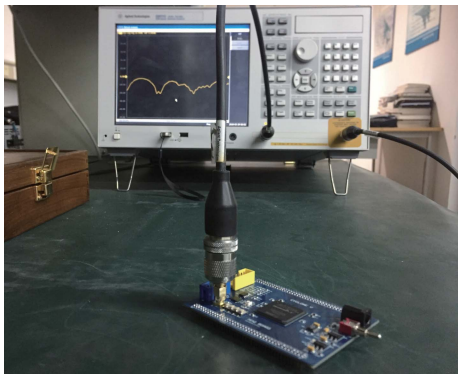


Fig. 3. Z_{PCB} measurement setup. Z_{PCB} is measured by Keysight E5071C vector network analyzer with a frequency sweeping step of 2.5 MHz.

for $m = n = 0$, $\chi_{mn} = \sqrt{2}$ for $m = 0$ or $n = 0$, $\chi_{mn} = 2$ for $m \neq 0$ or $n \neq 0$, and $k = w\sqrt{\varepsilon\mu}$ [25]:

$$Z_{\mathrm{PCB}} = jw\mu h \sum_{m=0}^{\infty}\sum_{n=0}^{\infty}\left[\frac{{\chi_{mn}}^2 \cos^2\left(\frac{n\pi}{b}y_i\right)\cos^2\left(\frac{m\pi}{a}x_i\right)}{ab\left[\left(\frac{n\pi}{b}\right)^2+\left(\frac{m\pi}{a}\right)^2-k^2\right]} \cdot \mathrm{sinc}^2\left(\frac{n\pi d_{yi}}{2b}\right)\mathrm{sinc}^2\left(\frac{m\pi d_{xi}}{2a}\right)\right]$$

$$k_{mn} = \left(\frac{n\pi}{b}\right)^2+\left(\frac{m\pi}{a}\right)^2 \quad (m = 0, 1, \ldots;\ n = 0, 1, \ldots). \tag{3}$$

When $k_{mn} = k$, the width and the length of the PCB are integral multiples of the half wavelength, and resonance takes place. At this time, according to (3), Z_{PCB} peak occurs when the denominator of the equation approaches to 0. Hence, the value of Z_{PCB} at or close to resonant frequencies is significantly larger than the value at nonresonant frequencies, which agrees with the above-discussed structural model. According to (1) and (2), the VDD drop at Z_{PCB} peaks causes an increase of inverter delay and thus the degradation of RO frequency.

In addition, according to the published data [26], the PCB fabrication process variations are unavoidable. The 3σ value of the PCB dimension variation is in the range of ($\pm 0.25 \sim \pm 1$ mil) for various high-end vendors. The following equation shows the variation rate of Z_{PCB} in accordance with dimension variation at the mode (1,0) resonant frequency.

$$Z_{\mathrm{PCB}(1,0)} = jw\mu h\left[\frac{2\cos^2\left(\frac{\pi}{a}x_i\right)}{ab\left[\frac{\pi}{a}^2-k^2\right]}\cdot \mathrm{sinc}^2\left(\frac{\pi d_{xi}}{2a}\right)\right]_{w\to\frac{\pi}{a\sqrt{\mu\varepsilon}}}$$

$$\frac{\partial Z_{\mathrm{PCB}}}{\partial h} = jw\mu\left[\frac{2\cos^2\left(\frac{\pi}{a}x_i\right)}{ab\left[\frac{\pi}{a}^2-k^2\right]}\cdot \mathrm{sinc}^2\left(\frac{\pi d_{xi}}{2a}\right)\right]_{w\to\frac{\pi}{a\sqrt{\mu\varepsilon}}}$$

$$\frac{\partial Z_{\mathrm{PCB}}}{\partial b} = \frac{jw\mu h}{b}\left[\frac{2\cos^2\left(\frac{\pi}{a}x_i\right)}{a\left[\frac{\pi}{a}^2-k^2\right]}\cdot \mathrm{sinc}^2\left(\frac{\pi d_{xi}}{2a}\right)\right]_{w\to\frac{\pi}{a\sqrt{\mu\varepsilon}}}$$

$$\frac{\partial Z_{\mathrm{PCB}}}{\partial a} = \frac{2j\mu wh}{b(\pi d x_i)^2} \times \left[\frac{3a^2\cos^2\left(\frac{\pi}{a}x_i\right)\sin^2\left(\frac{\pi}{2a}dx_i\right)+\cdots}{a^4\left(\frac{\pi}{a}^2-k^2\right)}\right]_{w\to\frac{\pi}{a\sqrt{\mu\varepsilon}}}. \tag{4}$$

It can be seen that, at the resonant frequency, when $[(\pi/a)^2 - k^2]$ approaches to 0, the impact of PCB length (a), width (b), and dioxide thickness (h) variations on Z_{PCB} is all maximized. Therefore, it can be concluded that the values of Z_{PCB} show most significant variations at the resonant frequencies. Fig. 4(a) shows the Keysight E5071C vector network analyzer [27] measured Z_{PCB} (transformed from S_{11}) for 30 four-layer PCB boards from the same lot, while Fig. 3 shows the measurement setup. According to the measurement data, at the mode (1,0) resonant frequency (847 MHz), the variation rate of Z_{PCB} is 20.5%. While at the frequencies in the middle of any two neighboring resonant frequencies, the Z_{PCB} variation rate drops to 0.003% on average, which agrees with (4). Given the stable external power supply (V_{supply}), the impact of Z_{PCB} variation on RO VDD can be expressed as

$$|\Delta \mathrm{VDD}| = V_{\mathrm{supply}}\left|\frac{Z_{\mathrm{IC}}}{(Z_{\mathrm{PCB}}+Z_{\mathrm{IC}})^2}\right|\Delta Z_{\mathrm{PCB}}. \tag{5}$$

To measure RO VDD at resonance, an RO period-VDD lookup table is built for each board at various static VDD values. Then, the operating clocks of the ICs on the 30 PCB boards are set to 847 MHz, which initiates the (1,0) mode resonance. Through recording RO periods at resonance, RO VDD can be identified according to the period-VDD lookup table. Fig. 4(b) shows the average RO VDD values of the same 30 PCB boards as shown in Fig. 4(a), with the system operating at/not at resonance. As shown in Fig. 4(b), the average RO VDD ranges from 2.1211 to 2.9651 V and from 3.2707 to 3.3287 V, with/without resonance, respectively. Hence, the variation rate of RO VDD at resonance is 39.8%, which is much larger than the nonresonant case (1.8%). The measured data confirms that the unique PCB fabrication variations introduce significant variations to Z_{PCB} during resonance among the systems. Furthermore, according to (5), Z_{PCB} variation (ΔZ_{PCB}) causes RO VDD variation, which can be sensed by the RO and cause oscillation frequency variation. It should be noted that we use a relatively simple four-layer PCB model to show an intuitive understanding of PCB resonance and PDN structure and deduce the equation of input impedance and operation frequency explicitly to display quantitative analysis. However, the qualitative result of resonant that comes from the quantitative analysis is universal to all the PCBs, such as flexible PCB (FPC) and SiP. In a word, the scheme can be applied to every kind of PCB structure.

B. IC Process Variations' Impact on RO Oscillation

As shown in (1), the variations of the parameters, including gate oxide thickness (t_{ox}), threshold voltage (v_{th}), gate length (L), and width (W), affect the delay of an inverter cell and thus the oscillation frequency of an RO. For 55-nm

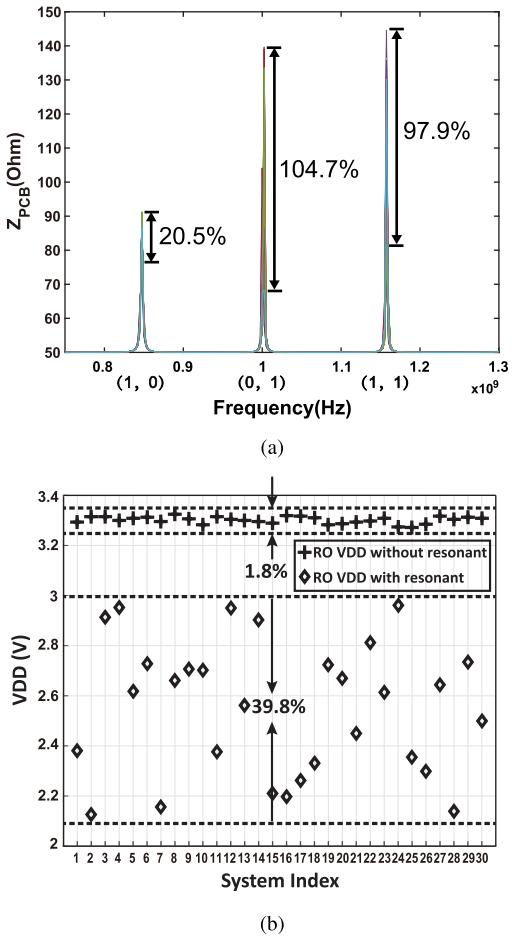


Fig. 4. PDN impedance (Z_{PCB}) and RO VDD of the 30 same-type fabricated boards. (a) Variation rates of PCB PDN impedance (Z_{PCB}) are 20.5%, 104.7%, and 97.9% at mode (1,0), (0,1), and (1,1) cavity resonant frequencies, respectively. At the nonresonant frequencies, the Z_{PCB} variation rate is significantly lower. (b) RO VDD values of the same 30 PCB boards as shown in Fig. 4(a), with the system operating with and without resonant at 847 and 50 MHz, respectively. The variation rate of RO VDD at resonant is 39.8%, which is much larger than the nonresonant case (1.8%).

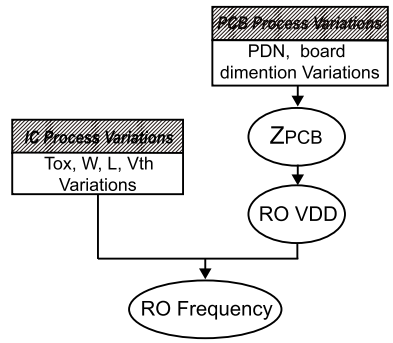


Fig. 5. RO frequency is affected by both the PCB and IC process parameters. When the system clock frequency is not equal to the resonant frequency, the IC process variations are dominant. When the system clock frequency equals to the resonant frequency, the PCB process parameters introduce significant impact on RO oscillation by impacting Z_{PCB} and RO VDD.

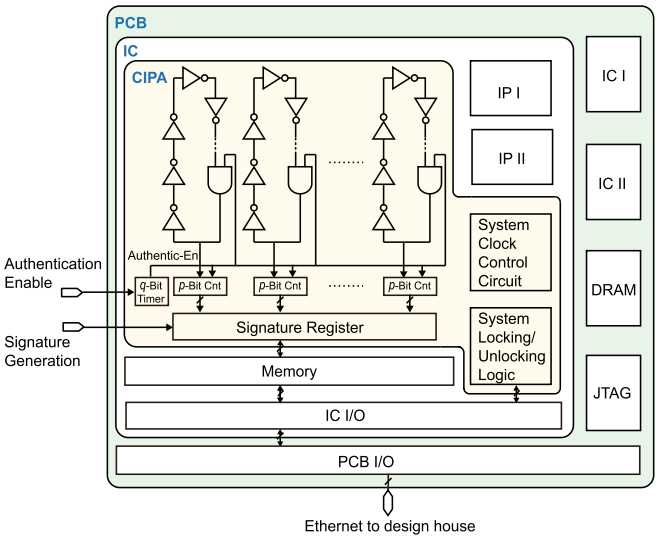


Fig. 6. Architecture of CIPA.

and below technologies, the inter-die and intra-die variation percentage of v_{th} and L can reach as high as 30% and 15%, respectively [28]. The significant process variations make a manufactured gate's delay quite random. As a result, it makes the period of a manufactured RO, which is a sum of a series of gates' delay [29] randomly. Several existing works [30], [31] have proved the effectiveness of employing multiple ROs on the same die to build a PUF and using the PUF to generate a unique signature as the identity of the IC.

C. Concurrent Counterfeit PCB and IC Detection With CIPA

According to the discussions in Sections III-A and III-B, the RO frequency is affected by both PCB and IC process variations, as shown in Fig. 5. Especially, at the nonresonant frequencies, the process variations of RO cells are dominant. While at or close to the resonant frequencies, the PCB process variations introduce significant impact additionally. Therefore, the RO array can be used as PUF to authenticate both IC and PCB. In this section, the theory of employing RO-based array for system-level CIPA is presented.

CIPA, as shown in Fig. 6, is composed of an n-RO array with n p-bit counters, a central q-bit timer, signature register, system clock control circuit, and system locking/unlocking logic. When the authentication enable signal goes high, the timer enables all ROs to oscillate and terminates the oscillation after a predefined number of system clock cycles. Then, the system clock control circuit configures the on-chip PLL to output a system clock frequency at or close to a resonant frequency. The CIPA signatures, which are the counter values without/with resonance, are registered into the signature register and communicated to the design house through IC, PCB I/O, and Ethernet. Through checking CIPA signatures with/without resonance, the system can be locked or unlocked. Locking/unlocking circuits [32]–[35] can be applied with CIPA decisions. It should be noted that the security of the communication channel is outside the scope of this paper. In other words, we assume the communication to be secure, which means that the CIPA signatures will not be extracted by attackers. In addition, if attackers tamper, remove, or disable ROs in the system, regardless of bypassing the verification

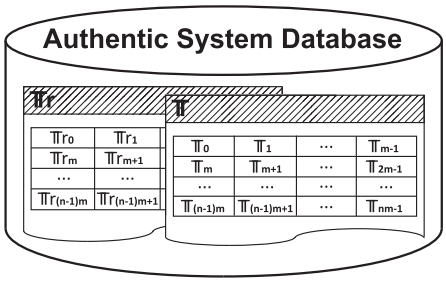


Fig. 7. Architecture of ASDB is consisted of RO periods $\mathbb{T}$ and $\mathbb{T}_r$.

process, or the malicious attack, the verification will fail, and the system will be detected as counterfeit, even if other components are untouched and genuine. In this case, we do not have to verify the authenticity of other components but try to prevent the system from continuing to flow in the supply chain, because we consider the system as counterfeit, and no longer belongs to a secure supply chain.

To provide system-level authentication, CIPA needs to be integrated into an IC, which can be either an application-specific IC (ASIC) or a reconfigurable device (e.g., FPGA). It should be noted that, if the system is FPGA based, CIPA can be part of a bitstream and loaded into it after fabrication. However, if the IC in the system is ASIC, then CIPA should be integrated into the IC during the design stage. In addition, as the resonant frequency may not be known during the design stage, the system clock control circuit is designed to be configurable during authentication.

1) System Enrollment by Authentic System Database Construction: After system fabrication, the CIPA signature is collected by the design house either remotely or with physical access to the system with minimum IC functional activities. The minimum activities (low noise) generate minimum RO VDD fluctuation, which makes that the IC or RO process variations dominate RO frequency. Array $\mathbb{T} = \{T_0, T_1, T_2, \ldots, T_{n-1}\}$ represents the measured periods of n ROs in a low-noise IC. It should be noted that $\mathbb{T}$ can also be collected by the system vendor and shared with the design house.

In the next step, the system clock of IC is set to a frequency at or close to a PCB resonant frequency, and CIPA's signature is collected again. As the PCB resonates at various frequencies, a resonant frequency within the range of on-chip PLL configuration should be selected. $\mathbb{T}_r = \{T_{0r}, T_{1r}, T_{2r}, \ldots, T_{(n-1)r}\}$ represents the measured periods of n ROs at PCB resonance.

As resonance causes Z_{PCB} to increase dramatically, which causes RO power supply (VDD) to drop significantly, the RO oscillation period drops at resonance. At the same time, the increase in Z_{PCB} is significantly impacted by PCB process variations. Hence, the RO period increase is unique for each system, which generates unique $\mathbb{T}_r$. Finally, $\mathbb{T}$ and $\mathbb{T}_r$ are registered into the authentic system database (ASDB), and the system is ready to be shipped to the customer. The architecture of ASDB is shown in Fig. 7. It should be noted that each chip in ASDB is also equipped with electronic chip identification (ECID) that is used as a public ID and identifier.

2) Counterfeit-Type Detection: During authentication, the design house can remotely initiate CIPA without/with resonance at the verifier's side. The CIPA signatures are collected and transmitted to the design house from the verifier via Ethernet. Then, $\mathbb{T}'$ and $\mathbb{T}'_r$, which are the reported RO periods without/with resonance, are calculated by the system vendor from CIPA signature and compared with ASDB.

To tolerate external power supply fluctuation and aging effects, which increase/decrease the RO period, during ASDB comparison, as long as there exists $System_k$ ($0 \le k \le K-1$, K is the authentic system count) in ASDB satisfying

$$\exists \left| \frac{\mathbb{T}'_i}{\mathbb{T}_i} - c \right| \le \varepsilon \quad (0 \le i \le n-1) \tag{6}$$

the IC can be determined as authentic. In (6), $c = Avg[(\mathbb{T}'_i/\mathbb{T}_i)](0 \le i \le n-1)$ is the scaling constant to tolerate universal supply voltage shifting and aging, and ε is the deviation used to tolerate the imbalanced power distribution as well as aging variations among n ROs within CIPA. Otherwise, the IC is considered as counterfeit. It should be noted that, with the fabrication date logged in ASDB, the age of the authentic IC can also be determined, which helps to identify recycled systems.

In addition, if the same system under test and $System_k$ in ASDB also satisfy

$$\exists \left| \frac{\mathbb{T}'_{ri}}{\mathbb{T}_{ri}} - c_r \right| \le \varepsilon_r \quad (0 \le i \le n-1) \tag{7}$$

where again $c_r = Avg[(\mathbb{T}'_{ri}/\mathbb{T}_{ri})](0 \le i \le n-1)$ is the scaling constant and ε_r is the maximum allowable deviation, the PCB can be considered as authentic. Otherwise, the PCB is counterfeit. Therefore, if (6) and (7) are all satisfied, a Type A system in Table I is detected. However, if (6) is satisfied, while (7) is not, it means that the IC must have been detached from its original system and soldered on a cloned PCB, and then, a Type B system in Table I is also detected. The counterfeit decision flow is shown in Fig. 8.

A counterfeit IC can disturb the detection of PCB. In this case, regardless of PCB being authentic or not, the CIPA signature $\mathbb{T}'_{ri}$ that represents the identity of PCB cannot be matched to any signature in ASDB. But, according to (5), the RO period degradation reflects the resonant Z_{PCB} increase, which is determined by PCB variations. Hence, a new feature is introduced as follows:

$$\exists \left| \frac{(\mathbb{T}'_{ri} - \mathbb{T}'_i)/\mathbb{T}'_i}{(\mathbb{T}_{ri} - \mathbb{T})/\mathbb{T}} - c_{r2} \right| \le \varepsilon_{r2} \quad (0 \le i \le n-1). \tag{8}$$

As a result, all four counterfeiting types shown in Table I can be accurately identified. It should be noted that the constants c, c_r, and c_{r2} are fitted for each system during ASDB matching to obtain the minimum ε, while ε, ε_r, and ε_{r2} are defined as counterfeit detection thresholds, which are determined by the clustering of authentic systems during training.

3) CIPA's Resilience to Aging and VDD Fluctuation: The employments of c and ε are to tolerate the systematic and stochastic RO supply and aging variations, respectively, which enhance the reliability of CIPA. With systematic RO supply and aging degradation across the die, $\mathbb{T}'$ and $\mathbb{T}'_r$ in (6) and (7)

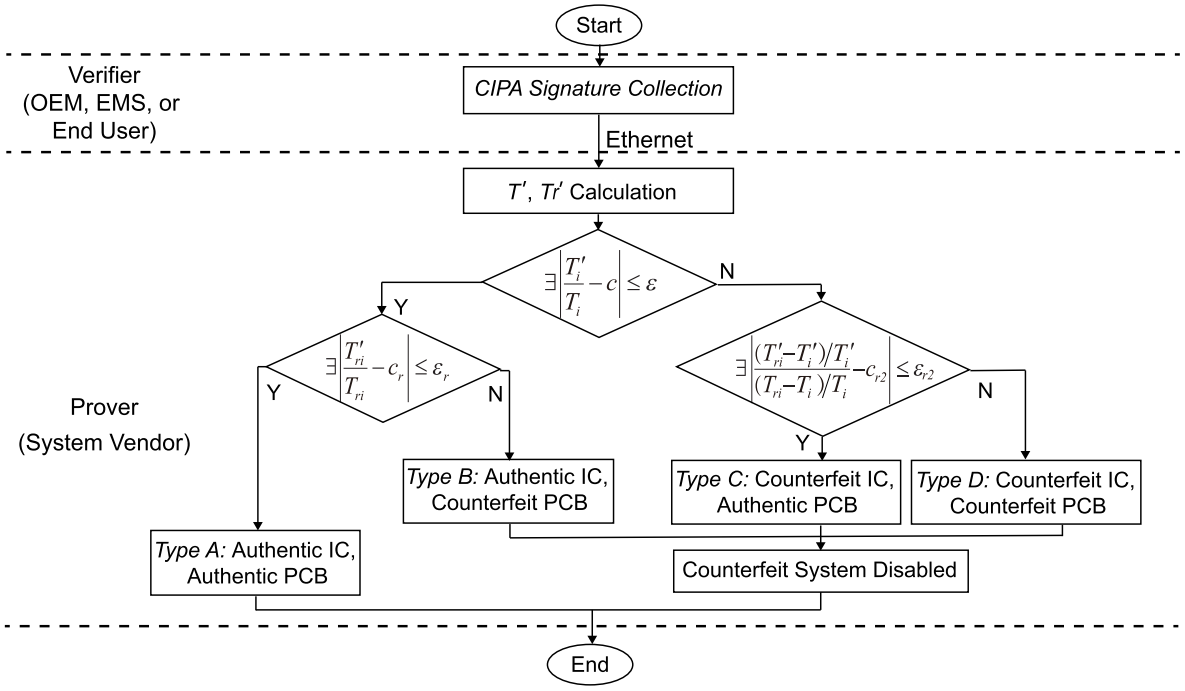


Fig. 8. Decision flow of CIPA-based counterfeit system detection.

may scale to $\mathbb{T}''$ and $\mathbb{T}''_r$. Suppose that k and k_r are the scale factors, there are

$$\begin{aligned} \mathbb{T}'' &= (1+k)\mathbb{T}' \\ \mathbb{T}''_r &= (1+k_r)\mathbb{T}'_r. \end{aligned} \tag{9}$$

Hence

$$\begin{aligned} \left|\frac{\mathbb{T}''}{\mathbb{T}}\right| &= c(1+k)+e \\ \left|\frac{\mathbb{T}''_r}{\mathbb{T}_r}\right| &= c_r(1+k_r)+e_r \\ \left|\frac{\mathbb{T}''_r/\mathbb{T}''}{\mathbb{T}_r/\mathbb{T}}\right| &= c_{r2}\frac{(1+k_r)}{1+k}+e_{r2}. \end{aligned} \tag{10}$$

According to (10), it can be seen that the scale factors representing VDD fluctuation and aging across the die only impact the constants c, c_r, and c_{r2} without impacting ε, ε_r, and ε_{r2}. Hence, the counterfeit-type detection accuracy is not impacted.

IV. CIPA-Based System Authentication Flow

The flow for the CIPA-based system authentication is shown in Fig. 9. Three entities within the supply chain: design house, system fabricator, and verifier, which can be any role in the supply chain adopting the IC-centered system, are involved in the authentication process.

Step 1 (CIPA Instantiation): In this step, the structure of CIPA, including RO array, counter, timer, signature register, system clock control circuit, and locking/unlocking logic, is synthesized as a stand-alone block by the design house.

Step 2 (CIPA Insertion): As CIPA is stand alone, which requires no cross timing constraint in relation to the principle circuit. Hence, for the ASIC-based system, CIPA can be integrated into the IC any time before layout generation. For the FPGA-based system, CIPA can either be integrated as a fixed peripheral during the FPGA design stage or be loaded into the programmable logic after FPGA fabrication. It should be noted that CIPA can be inserted into multiple chips in a system, and the implementation and measurement of RO arrays in different chips do not conflict with the current authentication flow.

Step 3 (IC Tapeout, System Fabrication, and Test): This step includes all industrial IC tapeout, PCB fabrication, and system integration procedures. CIPA authentication gives no impact on these industrial procedures.

Step 4 (PCB Resonant Frequency Identification and ASDB Construction): In this step, the design house determines the nonresonant and resonant frequencies for CIPA signature collection. It should be noted that the resonant frequencies of a batch of PCB boards are basically the same, and the design house just needs to test the resonant frequency once for each batch of PCB boards. As the test process costs little time, the testing time will not be a problem. Then, the design house initiates CIPA at both frequencies in sequence and collects the CIPA signatures of all authentic systems as ASDB.

Step 5 (System Delivery): After ASDB is constructed, the IC-centered systems are ready to be delivered to consumers.

Step 6 (CIPA-Based System Authentication): During system usage, either the design house or a role in the supply chain can request the system authentication. Upon receiving the request, the design house initiates CIPA remotely and collects CIPA signatures. Through comparing the CIPA signatures with ASDB, the system authenticity can be determined. If the counterfeiting type is detected, system locking can be applied to disable the counterfeit system.

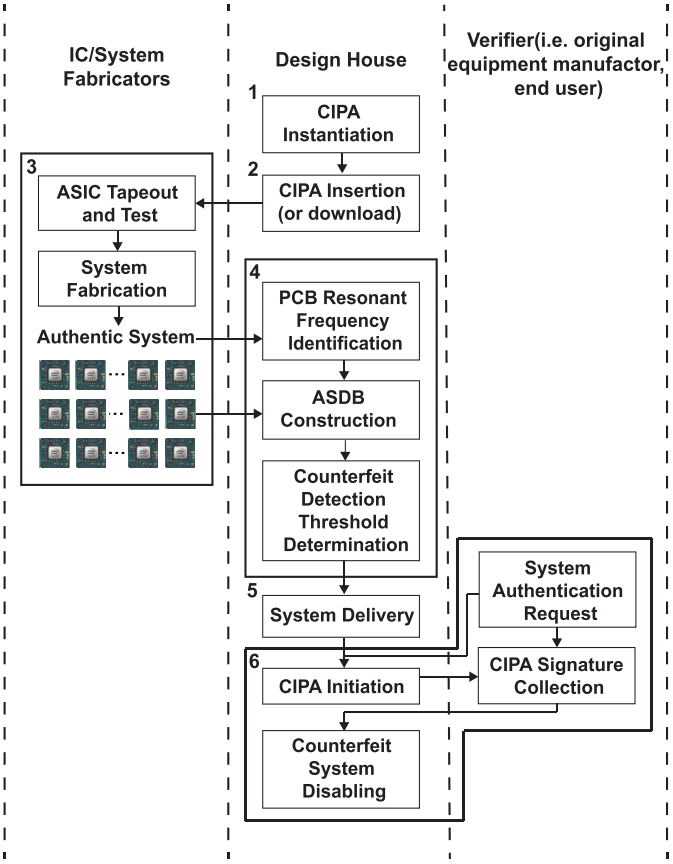


Fig. 9. Flow for CIPA-based system authentication.

TABLE II
AREA OVERHEAD OF CIPA

Benchmark	ITC'b19	VGA_LCD	FGU	Leon3s
# FF	6042	17058	27931	17495
Area Overhead	1.98%	0.70%	0.42%	0.68%

V. EXPERIMENTAL RESULTS AND ANALYSIS

In this paper, CIPA is implemented with eight ROs, eight 8-bit counters, a single 8-bit timer, and a 128-bit signature register. The area overhead of CIPA locating on several benchmark circuits, from Gaisler, OPENCORE, ITC'99, to OpenSPARCT2, is shown in Table II.

A set of 120 28-nm FPGA development boards are used to verify the effectiveness of CIPA on system-level counterfeit detection. Overall, the 120 FPGA systems are divided into four groups, which include all counterfeiting scenarios, as discussed in Section I. The setups of the four groups are described in Table III and Fig. 10, in which Type A originally includes 60 authentic FPGA systems, with FPGAs from a trusted source and PCBs manufactured by fabricator 1. The CIPA signatures for the 60 Type A systems without/with resonance ($\mathbb{T}_A/\mathbb{T}_{Ar}$) are collected as ASDB.

While Fig. 11 shows the distribution of $\mathbb{T}/\mathbb{T}_r$ in ASDB, the relative Hamming distance distribution of $\mathbb{T}$ and $\mathbb{T}_r$ is shown in Fig. 12. Inter$D_{T\text{avg}}$ and Inter$D_{T_r\text{avg}}$, the average

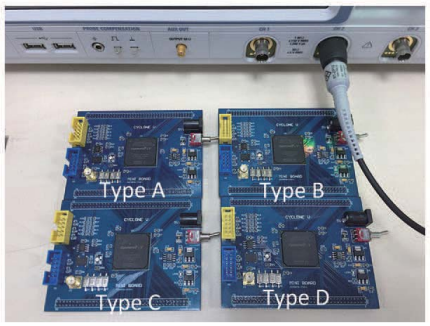


Fig. 10. Four types of system representing different counterfeit scenarios.

TABLE III
SETUP OF THE FOUR TYPES OF SYSTEMS REPRESENTING DIFFERENT COUNTERFEIT SCENARIOS

	IC	PCB	Count
Type A	Authentic	Authentic (*Fabricator 1*)	60 (30 reused)
Type B	Authentic	Counterfeit (*Fabricator 2*)	30
Type C	Counterfeit	Authentic (*Fabricator 1*)	30
Type D	Counterfeit	Counterfeit (*Fabricator 2*)	30

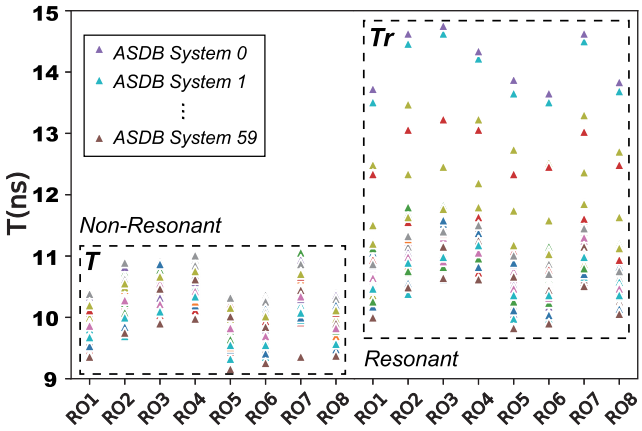


Fig. 11. CIPA signatures of the 60 authentic systems logged in ASDB.

value of the relative hamming distance, can be expressed as

$$\text{Inter}D_{T\text{avg}} = \frac{2}{n(n-1)} \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} D_{T_{ij}}$$
$$\text{Inter}D_{T_r\text{avg}} = \frac{2}{n(n-1)} \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} D_{T_{rij}} \quad (11)$$

where n is the size of ASDB, and $D_{T_{ij}}$ and $D_{T_{rij}}$ are the relative hamming distance between any two RO period vectors logged in ASDB

$$D_{T_{ij}} = \frac{1}{m} \sum_{k=1}^{m} \frac{|T_{jk} - T_{ik}|}{\Delta \mathbb{T}_i}$$
$$D_{T_{rij}} = \frac{1}{m} \sum_{k=1}^{m} \frac{|T_{rjk} - T_{rik}|}{\Delta \mathbb{T}_{ri}} \quad (12)$$

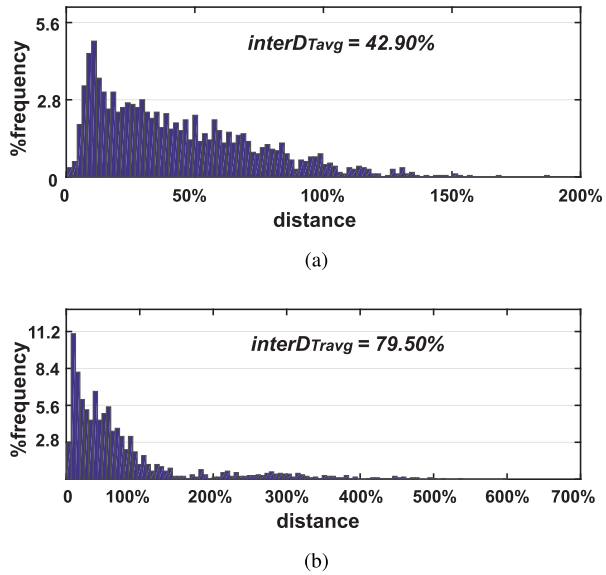


Fig. 12. Relative Hamming distance distribution of $\mathbb{T}$ and $\mathbb{T}_r$. (a) Average relative Hamming distance distribution of $\mathbb{T}$ is 42.9%. (b) Average relative Hamming distance distribution of $\mathbb{T}_r$ is 79.5%.

where m is the number of ROs in each system and $\Delta\mathbb{T}_i$ and $\Delta\mathbb{T}_{ri}$ are the range of RO periods $\mathbb{T}_i$ and $\mathbb{T}_{ri}$. In this paper, n is 60 and m is 8.

As Inter$D_{T\text{avg}}$ and Inter$D_{T_r\text{avg}}$ reach 42.90% and 79.50%, it can be seen that all of the authentic systems have differentiable unique CIPA signatures.

Type B represents the first refurbishing scenario, in which the counterfeiter replaces the failing PCB of an original system by a cloned one. Hence, for Type B, we detach 30 authentic FPGAs from Type A systems and re-solder them on cloned PCBs from another PCB manufacturer (fabricator 2). Type C represents the other refurbishing scenario, in which the counterfeiter replaces the failing IC of an original system by a counterfeit one. Hence, for Type C, we reuse the 30 authentic PCBs from Type A systems whose FPGAs are detached to construct Type B systems, and solder counterfeit FPGA from unknown sources on them. Finally, 30 systems representing the Type D counterfeit system built from bottom to top are made with cloned PCBs from fabricator 2 and counterfeit FPGAs.

A. Counterfeiting-type Detection

Fig. 13 shows the measured ε and ε_r values for the 30 Type A authentic circuits. For each system i ($1 \leq i \leq 30$) belonging to Type A, by compared with all of the slots in ASDB, the slot that gives minimum deviation ($\min|(\mathbb{T}_{Ai}/\mathbb{T}_j) - c_i|$ and $\min|(\mathbb{T}_{Ari}/\mathbb{T}_{rj}) - c_{ri}|$) is shown in Fig. 13. From Fig. 13, the counterfeit detection thresholds ε and ε_r are determined as 0.0022 and 0.0025.

Fig. 14 shows the measured ε and ε_r values for the 30 Type B counterfeiting circuits. It can be seen that the values of $\min|(\mathbb{T}_{Bi}/\mathbb{T}_j) - c_i|$ ($1 \leq i \leq 30$) all fall in the range of ε. According to the measurement results presented in Fig. 4(a), the mode (1,0) resonant frequency of the system is close to 847 MHz, which is an available internal PLL frequency. Hence, the functional clock is set as 847 MHz to initiate resonance.

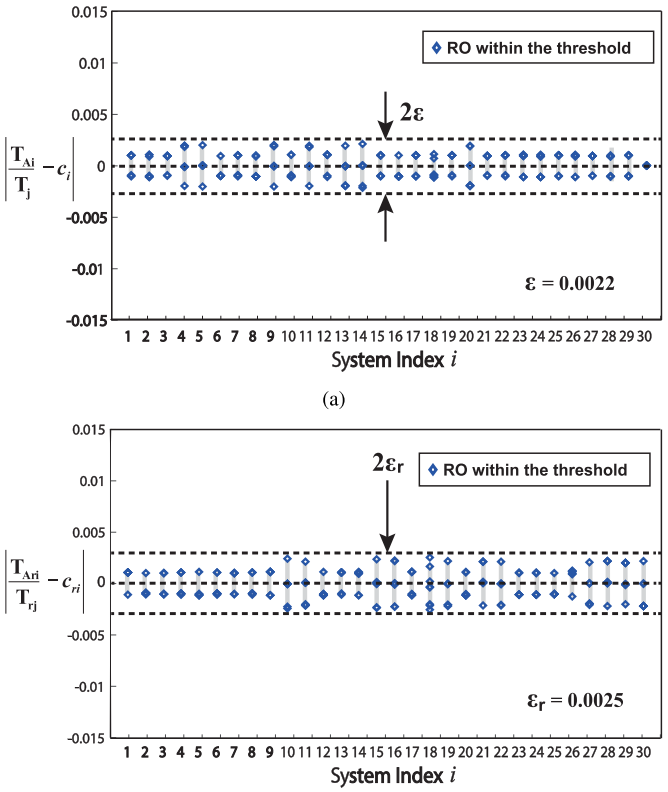


Fig. 13. RO periods of Type A systems in comparison with ASDB. (a) Deviation of Type A systems without resonance is within the counterfeit detection threshold ε. (b) Deviation of Type A systems with resonance is within the counterfeit detection threshold ε_r.

Again, for each system i belonging to Type B, by compared with all of the slots in ASDB, the slot giving minimum deviation ($\min|(\mathbb{T}_{Bri}/\mathbb{T}_{rj}) - c_r|$) is shown in Fig. 14(b). From Fig. 14(b), it can be seen that all of $\min|(\mathbb{T}_{rBi}/\mathbb{T}_{rj}) - c_r|$ exit ε_r. Hence, the PCBs are all detected as counterfeiting, while the ICs are authentic.

Fig. 15 shows the measured ε values for the 30 Type C and 30 Type D systems. It can be seen that the values of $\min|(\mathbb{T}_{Ci}/\mathbb{T}_j) - c_i|$ and $\min|(\mathbb{T}_{Di}/\mathbb{T}_j) - c_i|$ ($1 \leq i \leq 30$) all exit ε. Hence, the ICs are all detected as counterfeiting. Since the value of $\mathbb{T}_r$ is derived from the value of $\mathbb{T}$ of an authentic IC, there is no need to measure ε_r values for Type C and Type D systems.

According to the aforementioned analysis, the minimum oscillation period deviations without/with resonance represent the counterfeiting types. Thus, it can be used as features to classify different counterfeiting types. A simple two-feature four-class support vector machine (SVM) classifier, adopting the features of $[\min|(\mathbb{T}/\mathbb{T}_A) - c|\ \min|(\mathbb{T}_r/\mathbb{T}_{rA}) - c_r|]$, is trained by randomly pick 30% samples of each counterfeit type. The left 70% of each counterfeit type is used for the test. Fig. 16 shows the result of classification. It can be seen that first 100% of the 90 counterfeit systems are differentiated from the 30 authentic systems. Then, all 30 counterfeit Type B systems are differentiated from other counterfeit types. However, as the value of $\mathbb{T}_r$ in ASDB is derived from the value of $\mathbb{T}$ of an authentic IC, for counterfeit Type C and Type D, the IC is

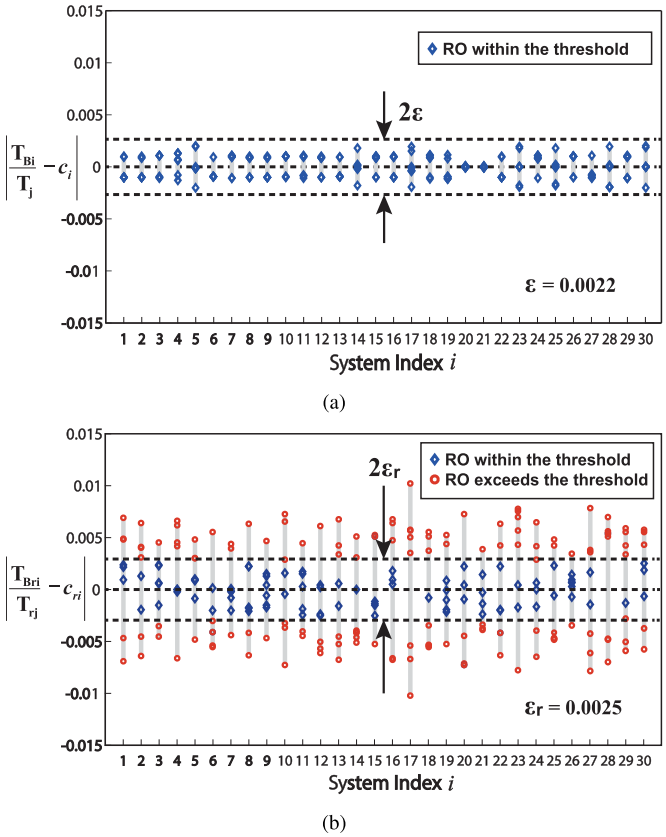


Fig. 14. RO periods of counterfeit Type B systems in comparison with ASDB. (a) Deviation of counterfeit Type B systems without resonance is within the counterfeit detection threshold ε. (b) Deviation of counterfeit Type B systems with resonance falls out of the counterfeit detection threshold ε_r.

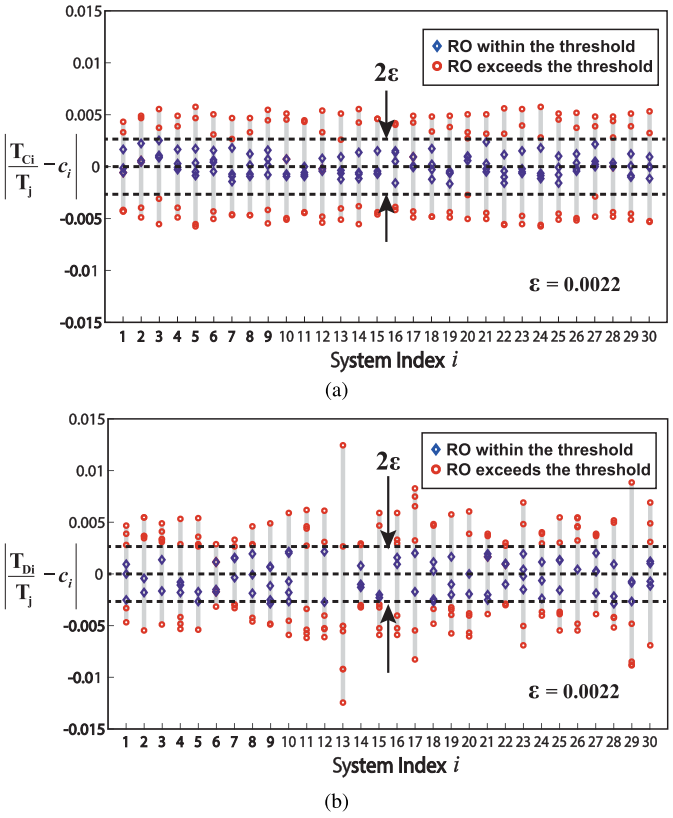


Fig. 15. RO periods of counterfeit Type C and Type D systems in comparison with ASDB. (a) RO periods without the resonance of counterfeit Type C systems in comparison with ASDB. The deviation of all the systems falls out of the counterfeit detection threshold ε. (b) RO periods without the resonance of counterfeit Type D systems in comparison with ASDB. The deviation of all the systems falls out of the counterfeit detection threshold ε.

not authentic, and $\mathbb{T}'_r$ cannot match any slot in ASDB. Hence, as shown in Fig. 16, Type C and Type D cannot be effectively differentiated.

To further separate Type C and Type D counterfeiting types, the drop from T to T_r reflects the RO VDD drop caused by PCB PDN impedance Z_{PCB} increasing due to resonance. The third feature $\min|((\mathbb{T}_r - \mathbb{T})/\mathbb{T}/(\mathbb{T}_{rA} - \mathbb{T}_A)/\mathbb{T}_A) - c_{r2}|$ introduced in Section III-C2 is added for PCB authentication determination. According to Fig. 17, Type C and Type D counterfeit systems are successfully differentiated by this new three-feature SVM classifier, and the improved three-feature SVM classifier successfully separates all four types of systems from each other with a confidence of 97.62%, while Type C and Type D are classified with each other with a 95.24% confidence level in this case.

In summary, CIPA successfully detects the four categories of counterfeiting types shown in Table I.

B. CIPA's Robustness Against Aging and Power Supply Noise

Eight Type A systems are burned-in under 80 °C to reflect the aging's impact on CIPA. The burn-in setup is shown in Fig. 18(a). To represent the different lengths of usage, the burn-in time length varies for each system, which is 1, 2, 4, 8, 16, 24, 32, and 40 h, respectively. Fig. 19(a) and (b) shows the delay degradation of a

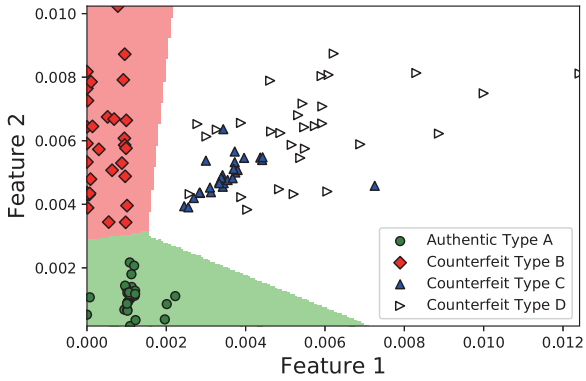


Fig. 16. Two-feature SVM classifier employing the features of $[\min|(\mathbb{T}/\mathbb{T}_A)-c|, \min|(\mathbb{T}_r/\mathbb{T}_{rA})-c_r|]$ separates authentic systems (Type A) from all counterfeit systems with a confidence of 100%. Counterfeit Type C and Type D cannot be separated.

specific RO in these eight systems with/without PCB resonance. The delay degradation rate r is calculated by comparing the RO oscillation period difference between the aged system $\mathbb{T}_a$ and the fresh system $\mathbb{T}_f$ as follows:

$$r = (\mathbb{T}_a - \mathbb{T}_f/\mathbb{T}_f) \times 100\%. \tag{13}$$

From Fig. 19(a) and (b), it can be seen that the delay degradation follows the power-law trend as the fitting curve shows. During aging, degradation rate r increases, and

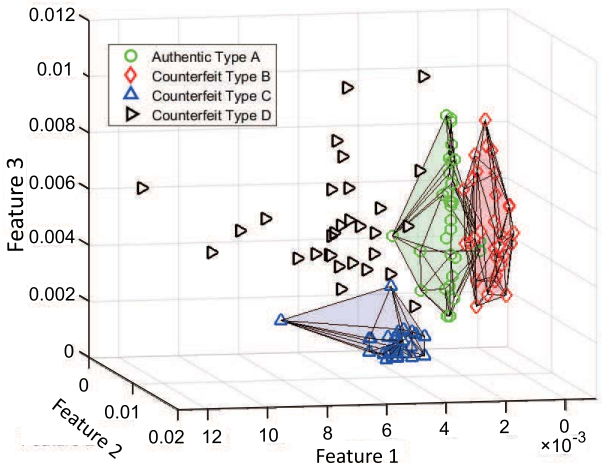
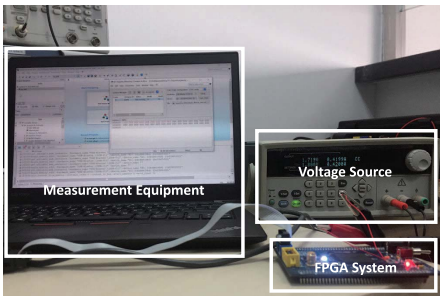


Fig. 17. Improved three-feature SVM classifier employing the features of $[\min|(\mathbb{T}/\mathbb{T}_A) - c|,\ \min|(\mathbb{T}_r/\mathbb{T}_{rA}) - c_{r1}|,\ \min|((\mathbb{T}_r - \mathbb{T})/\mathbb{T}/(\mathbb{T}_{rA} - \mathbb{T}_A)/\mathbb{T}_A) - c_{r2}|]$ successfully separates all four types of systems from each other with a confidence of 97.62%.

(a)

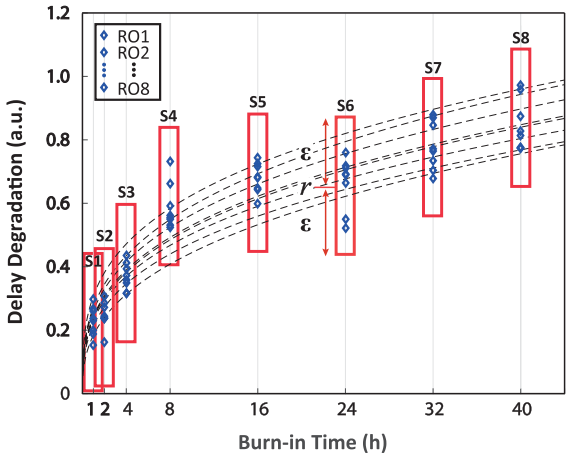


(b)

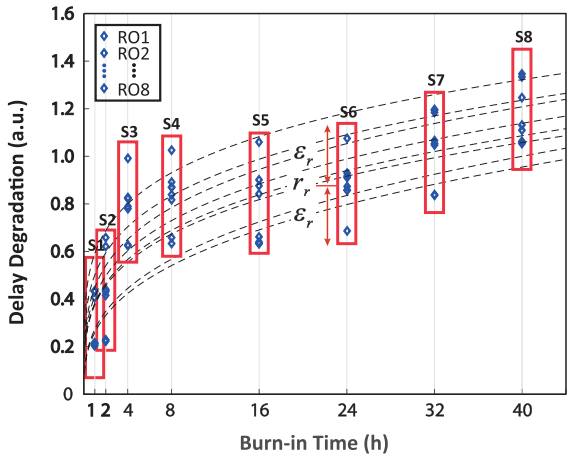
Fig. 18. Experimental setup for aging and power supply voltage shifting. (a) Burn-in equipment used for aging Type A systems. (b) Power supply shifts the VDD of FPGA under test.

however, the variation of r stays within the thresholds of $\varepsilon = 0.0022$ and $\varepsilon_r = 0.0025$, which are determined at time-zero. Hence, it is proved that the chip-level aging degradation r can be tolerated by adjusting the scaling constants c and c_r, and appropriate ε and ε_r can be predefined to encompass aging variations. It should be noted that in addition, the aging status of an authentic IC in ASDB can be investigated during the scaling of c and c_r, which helps to identify the recycled over-aging ICs.

As the power supply instability also impacts RO frequency, we remove the regulator chip LT3021 in the FPGA system and directly connect the power supply to an external voltage source



(a)



(b)

Fig. 19. Measurement results of RO periods under aging. Agreeing with the analysis in Section III-C3, the resilience of CIPA-based counterfeit detection to aging is verified. (a) Aging degradation of ROs in eight Type A systems (S1–S8) without resonance. The deviations of the degradation rate are within ε. (b) Delay degradation of ROs in eight Type A systems (S1–S8) with resonance. The deviations of degradation rate are within ε_r.

(Tektronix PWS4205 programmable dc power supply [36]), as shown in Fig. 18(b). Since the regulated output voltage of LT3021 is in the range of 1.737–1.854 V, the input voltage is between 2.1 and 10 V [37]. We set the external source to 1.737, 1.800, and 1.854 V, respectively, and the scalings of RO periods under different power supplies are shown in Fig. 20. From Fig. 20, it can be seen that, again, the chip-level external power supply shifting can be tolerated by scaling the constants c and c_r. And the deviations for all supply voltage cases are all within the counterfeit detection thresholds $\varepsilon = 0.0022$ and $\varepsilon_r = 0.0025$, when the PCB is quiet/resonant, which means that the SVM trained under normal supply voltage still can differentiate all counterfeiting types. Therefore, CIPA is robust against systematic aging and power supply shifting.

C. Comparing With Existing Solutions on Counterfeit Systems Detection

Three existing component- or system-level counterfeit detection methods [7], [10], [12], which have been described

TABLE IV
COMPARISON OF CIPA WITH EXISTING COMPONENT- OR SYSTEM-LEVEL COUNTERFEIT DETECTION METHODS

	IC PUF[7][30] [31]	**PCB PUF[10]**	**CST [12]**	**CIPA**
Allow System-Level Authentication	No (Only IC)	No (Only PCB)	Yes	Yes
Require PCB Modification	NA	Yes	Yes	No
All-digital	Yes	No (Trace impedance is measured by probe)	Yes	Yes
Allow Remote Authentication	Yes	No (Verifier needs physical access the PCB under test)	No (Verifier needs physical access to the system)	Yes
Robust Against Environmental Variations	No (VDD variation is not considered; Chips under different aging times are uniformly identified as used)	No (VDD and aging variations are not considered)	No (VDD and aging variations are not considered)	Yes
Sources of Area Overhead	RO and Measurement Circuit on IC	Traces on PCB	CST Sensors on IC and PCB	RO and Measurement Circuit on IC
Design Effort	RO and Measurement Circuit Insertion	PCB Traces Insertion	CST Sensors, RFID Tag and Antenna Insertion	CIPA Insertion

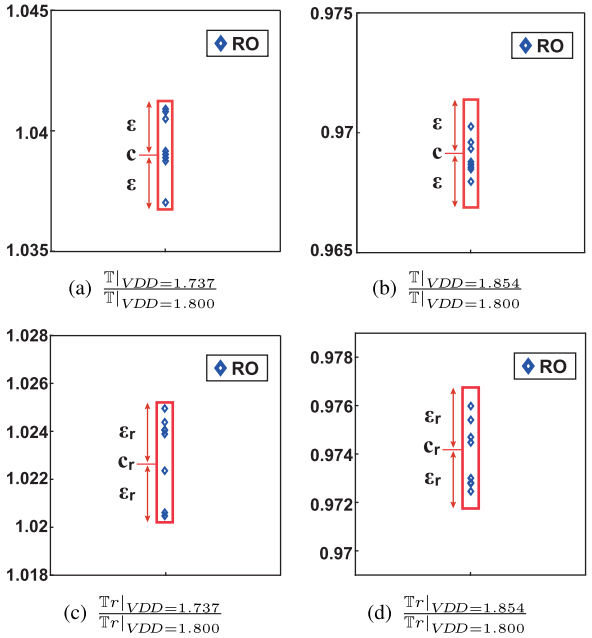


Fig. 20. Ratio of RO periods between different power supplies when the main circuit is quiet/resonant. The deviations of scalings are within the counterfeit detection thresholds ε and ε_r. As discussed in Section III-C3, the resilience of CIPA-based counterfeit detection to systematic VDD fluctuation is verified. (a) $(\mathbb{T}|_{\text{VDD}=1.737}/\mathbb{T}|_{\text{VDD}=1.800})$. (b) $(\mathbb{T}|_{\text{VDD}=1.854}/\mathbb{T}|_{\text{VDD}=1.800})$. (c) $(\mathbb{T}r|_{\text{VDD}=1.737}/\mathbb{T}r|_{\text{VDD}=1.800})$. (d) $(\mathbb{T}r|_{\text{VDD}=1.854}/\mathbb{T}r|_{\text{VDD}=1.800})$.

in Section I, are selected for comparison with CIPA. The characteristics of the four solutions are shown in Table IV. As demonstrated earlier, the proposed methodology offers the following advantages: system-level authentication, no PCB modification needed, all-digital, remote detection allowable, and robust against IC VDD shifting and aging degradation.

VI. CONCLUSION

In this paper, we proposed a methodology, which concurrently verifies the authenticity of both IC and PCB. The authentication is based on the structure named CIPA, which extracts the signature pairs of the RO array without/with PCB cavity resonance. Remote authentication is allowable by transmitting the CIPA signatures between any verifier and system vendor within the supply chain. According to the experimental results, the proposed methodology successfully differentiates 90 counterfeit systems belonging to different counterfeit types from the 30 authentic ones considering aging variations and nonideal power supply conditions. Furthermore, the PCB and IC authenticity status (i.e., authentic or counterfeit) have been successfully detected, which helps to determine the source of the counterfeit systems and the vulnerability of the supply chain.

REFERENCES

[1] M. M. Tehranipoor, U. Guin, and S. Bhunia, "Invasion of the hardware snatchers," *IEEE Spectr.*, vol. 54, no. 5, pp. 36–41, May 2017.
[2] R. A. McCormack, "Boeing's planes are riddled with chinese counterfeit electronic components," *Manuf. Technol. News*, vol. 19, no. 10, Jun. 2012.
[3] (Apr. 2012). *Top 5 Most Counterfeited Parts Represent a $169 Billion Potential Challenge for Global Semiconductor Market*. [Online]. Available: https://technology.ihs.com/405654/
[4] M. Shindell *et al.* (Jul. 2013). *The Ticking Time Bomb of Counterfeit Electronic Parts*. [Online]. Available: http://www.industryweek.com/
[5] 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.
[6] K. Huang, J. M. Carulli, and Y. Makris, "Parametric counterfeit IC detection via support vector machines," in *Proc. IEEE Int. Symp. Fault Defect Tolerance VLSI Syst.*, Oct. 2012, pp. 7–12.
[7] 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.
[8] Z. Guo, X. Xu, M. Tehranipoor, and D. Forte, "FFD: A framework for fake flash detection," in *Proc. Design Autom. Conf.*, 2017, Art. no. 8.
[9] *Printed Circuit Board Identification (PCB ID) and Authentication*. (2015). [Online]. Available: http://www.maximintegrated.com/en/products/comms/onewire
[10] F. Zhang, A. Hennessy, and S. Bhunia, "Robust counterfeit PCB detection exploiting intrinsic trace impedance variations," in *Proc. IEEE 33rd VLSI Test Symp.*, Apr. 2015, pp. 1–6.
[11] A. Hennessy, Y. Zheng, and S. Bhunia, "JTAG-based robust PCB authentication for protection against counterfeiting attacks," in *Proc. 21st Asia South Pacific Design Automat. Conf.*, Jan. 2016, pp. 56–61.

[12] 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. Homeland Secur.*, Apr. 2015, pp. 1–6.

[13] J.-L. Zhang, G. Qu, Y.-Q. Lyu, 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.

[14] *Counterfeit IC Threat Evolves With Spread of Clone Parts*. Accessed: Mar. 2018. [Online]. Available: http://mil-embedded.com/articles/counterfeit-threat-evolves-spread-clone-parts/

[15] M. Tehranipoor and F. Koushanfar, "A survey of hardware Trojan taxonomy and detection," *IEEE Design Test Comput.*, vol. 27, no. 1, pp. 10–25, Jan. 2010.

[16] S. Paley, T. Hoque, and S. Bhunia, "Active protection against PCB physical tampering," in *Proc. 17th Int. Symp. Quality Electron. Design (ISQED)*, Mar. 2016, pp. 356–361.

[17] (2018). *The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies*. [Online]. Available: https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

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

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

[20] 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.

[21] *Guide for Spotting Counterfeit Cisco Equipment*. Accessed: Jul. 2018. [Online]. Available: https://www.eetimes.com/document.asp?doc_id=1241472

[22] J. Rabaey, A. Chandarkasan, and B. Nikoic, *Digital Integrated Circuits: A Design Perspective*. 2nd ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2003.

[23] S. Mittal, Amita, A. S. Shekhawat, S. Ganguly, and U. Ganguly, "Analytical model to estimate FinFET's I_{ON}, I_{OFF}, SS, and V_T distribution due to FER," *IEEE Trans. Electron Devices*, vol. 64, no. 8, pp. 3489–3493, Aug. 2017.

[24] K. Shringarpure *et al.*, "Formulation and network model reduction for analysis of the power distribution network in a production-level multilayered printed circuit board," *IEEE Trans. Electromagn. Compat.*, vol. 58, no. 3, pp. 849–858, Jun. 2016.

[25] M. Xu, T. Hubing, J. Drewniak, T. Van Doren, and R. DuBroff, "Modeling printed circuit boards with embedded decoupling capacitance," *Measurement*, vol. 30, no. 35, p. 40, 2001.

[26] *Design Optimization of Single-Ended and Differential Impedance PCB Transmission Lines*. Accessed: Jul. 2018. [Online]. Available: https://www.jlab.org/eng/eecad/pdf/053designop.pdf

[27] *E5071c ENA Vector Network Analyzer*. Accessed: Mar. 2018. [Online]. Available: https://www.keysight.com/

[28] X. Wang *et al.*, "Radic: A standard-cell-based sensor for on-chip aging and flip-flop metastability measurements," in *Proc. IEEE Int. Test Conf.*, Nov. 2013, pp. 1–9.

[29] M. Bhushan, A. Gattiker, M. B. Ketchen, and K. K. Das, "Ring oscillators for CMOS process tuning and variability control," *IEEE Trans. Semicond. Manuf.*, vol. 19, no. 1, pp. 10–18, Feb. 2006.

[30] X. Zhang and M. Tehranipoor, "Design of on-chip lightweight sensors for effective detection of recycled ICs," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 22, no. 5, pp. 1016–1029, May 2014.

[31] X. Wang and M. Tehranipoor, "Novel physical unclonable function with process and environmental variations," in *Proc. Design, Automat. Test Eur. Conf. Exhib. (DATE)*, Mar. 2010, pp. 1065–1070.

[32] M. T. Rahman, D. Forte, Q. Shi, G. K. Contreras, and M. Tehranipoor, "CSST: Preventing distribution of unlicensed and rejected ICs by untrusted foundry and assembly," in *Proc. IEEE Int. Symp. Defect Fault Tolerance VLSI Nanotechnol. Syst.*, Oct. 2014, pp. 46–51.

[33] Y. M. Alkabani and F. Koushanfar, "Active hardware metering for intellectual property protection and security," in *Proc. USENIX Secur. Symp.*, 2008, pp. 291–306.

[34] X. Wang, Y. Guo, T. Ramhan, D. Zhang, and M. Tehranipoor, "DOST: Dynamically obfuscated wrapper for split test against ic piracy," in *Proc. AsianHOST*, Oct. 2017, pp. 1–6.

[35] A. C. Baumgarten, "Preventing integrated circuit piracy using reconfigurable logic barriers," Ph.D. dissertation, Dept. Elect. Comput. Eng., Iowa State Univ., Ames, IA, USA, 2009, vol. 8, no. 2.

[36] *PWS4205 Programmable DC Power Supply*. Accessed: Aug. 2018. [Online]. Available: https://www.tek.com/dc-power-supply/pws4205-manual/pws4205pws4305pws4602pws4721

[37] *LT3021/LT3021-1.2/LT3021-1.5/LT3021-1.8 500 mA, Low Voltage, Very Low Dropout Linear Regulator*. Accessed: Aug. 2018. [Online]. Available: http://www.analog.com/media/en/technical-documentation/data-sheets/3021fc.pdf?domain=www.linear.com

Xiaoxiao Wang received the B.S. and M.S. degrees in electrical engineering from Beihang University, Beijing, China, in 2005 and 2007, respectively, and the Ph.D. degree in electrical and computer engineering from the University of Connecticut, Storrs, CT, USA.

She joined the design for test (DFT) Team, Microcontroller Solutions Group, Freescale Semiconductor, Austin, TX, USA, in 2010. She joined the faculty of Beihang University in 2014, where she is currently a Professor. Her current research interests include on-chip measurement architecture design, reliability, and DFT.

Yueying Han received the B.S. degree in electrical engineering from Beihang University, Beijing, China, in 2017, where she is currently working toward the M.S. degree under the supervision of Dr. X. Wang.

Her current research interests include on-chip measurement architecture design, hardware counterfeit detection, and reliability.

Mark Tehranipoor (S'02–M'04–SM'07–F'18) received the Ph.D. degree from The University of Texas at Dallas, Richardson, TX, USA, in 2004.

He served as the Founding Director for the Center for Hardware Assurance, Security, and Engineering (CHASE) and Comcast Center of Excellence in Security Innovation (CSI) Centers, University of Connecticut, Storrs, CT, USA. He is currently the Intel Charles E. Young Preeminence Endowed Chair Professor in Cybersecurity with the University of Florida, Gainesville, FL, USA, where he is also a Founding Director of the Florida Institute for Cybersecurity Research (FICS). He has published over 400 journal articles and refereed conference papers and has given more than 175 invited talks and keynote addresses. He has published 10 books and more than 20 book chapters. His current research interests include hardware security and trust, supply chain security, IoT security, VLSI design, test, and reliability.

Dr. Tehranipoor is a Golden Core Member of the IEEE Computer Society (CS) and a member of the ACM and the ACM Special Interest Group on Design Automation (SIGDA). He was a recipient of a dozen best paper awards and nominations, as well as the 2008 IEEE CS Meritorious Service Award, the 2012 IEEE CS Outstanding Contribution, the 2009 NSF CAREER Award, and the 2014 AFOSR MURI Award. He serves on the program committee of more than a dozen leading conferences and workshops. He has also served as the Program Chair for a number of IEEE and ACM sponsored conferences and workshops, such as Hardware-Oriented Security and Trust (HOST), design for test (DFT), the IEEE Defect and Data Driven Testing Workshop (D3T), the IEEE Defect-Based Testing Workshop (DBT), and the IEEE North Atlantic Test Workshop (NATW). He co-founded the IEEE International Symposium on HOST and served as the HOST-2008 and HOST-2009 General Chair. He is currently serving as a Founding the Editor-in-Chief (EIC) for the *Journal on Hardware and Systems Security* (HaSS) and an Associate Editor for the *Journal of Electronic Testing: Theory and Applications* (JETTA), the *Journal of Low Power Electronics* (JOLPE), the IEEE TRANSACTIONS ON VERY LARGE-SCALE INTEGRATION SYSTEMS (TVLSI), and ACM the *ACM Transactions on Design Automation of Electronic Systems* (TODAES).