End-to-End Traceability of ICs in Component Supply Chain for Fighting Against Recycling

Yuqiao Zhang, *Student Member IEEE* and Ujjwal Guin, *Member IEEE*

***Abstract*—The rise of recycled ICs in the critical infrastructures causes a major concern to the government and industry because these chips exhibit lower performance and have shorter remaining useful life. The detection of these ICs becomes extremely challenging, when they are in the supply chain. It is necessary to power up a chip at a distributor's site to measure different electrical parameters for verifying whether it is used before. However, this can be challenging as many of the distributors may not be equipped with proper test infrastructures. Moreover, the reliability of authentic chips may be reduced if they have been removed from the packaging boxes for testing purposes. In this paper, we propose a robust and low-cost solution for enabling the traceability of an IC. The proposed solution builds a chain of trust among the manufacturer, distributors, and system integrator by enabling end-to-end traceability from manufacturing to system integration and provide protection against IC recycling. The proposed solution utilizes a small passive radio-frequency identification (RFID) tag, which needs to be placed on the package. Any entity in the supply chain can verify the authenticity of a chip using a commercial RFID reader.**

***Index Terms*—Electronic component supply chain, recycled ICs, RFID tag, digital signature.**

I. Introduction

The continuous growth of counterfeit integrated circuits (ICs) in electronics supply chain calls for an immediate solution as they pose serious threats to our critical infrastructures due to their inferior quality. Information Handling Services Inc. reported that counterfeit ICs represent a potential annual risk of $169 billion to the global electronics supply chain, and continues to increase in recent years [1]. These counterfeit ICs can be categorized into seven distinct types, such as, recycled, remarked, defective/out-of-spec, overproduced, cloned, forged documentation, and tampered types. Among all these different counterfeit categories, recycled ICs account for almost 80% of all reported counterfeit incidents [2]. The deployment of these recycled chips in a critical infrastructure would be catastrophic as they exhibit lower performance and shorter remaining useful lifetime than a newly manufactured IC [3]. In addition, the crude recycling process that consists of removal of the ICs from printed circuit boards (PCBs) under extremely high temperature, followed by sanding, repackaging and remarking could potentially create many defects and anomalies [2], [4]. Moreover, the recycling process may also create latent defects that can pass initial acceptance testing by original equipment manufacturers (OEM) but are susceptible to failure in the field [2].

The detection and avoidance approaches for recycled ICs are broadly classified into five different categories. First, there are several standards (e.g., AS6171, AS5553, AS6081, CCAP-101, and IDEA-STD-1010) in practice, which recommend different physical and electrical tests for the detection purpose [5]–[9]. The goal of these tests is to identify defects and anomalies present in recycled chips. However, excessive test times, test costs, low detection capability, and lack of automation make the detection of recycled ICs extremely challenging. Second, different solutions have been proposed, which are based on statistical data analysis [10]–[15]. However, these solutions provide limited accuracy when the chips are used for a short period. In addition, these schemes require authentic samples to train the model, which may be difficult to acquire from the market. Third, on-chip sensors have been proposed as an alternative to the conventional test methods [16]–[21]. Unfortunately, these solutions can provide lower accuracy when the process variations outpace aging degradation. Fourth, image processing is also used to detect recycled ICs [22], [23]. However, their effectiveness depends on the availability of authentic chips. Finally, DNA markings are commercially available to provide traceability for electronic parts [24]. However, a complex authentication process, excessive implementation, and test cost have made its application limited in practice [25].

The solution proposed in [26] is resistant to process variation, and it can detect recycled ICs very accurately even though it has been used for a very small amount of time. Due to the complex nature of the electronics supply chain, the ICs travel through many distributors (trusted and untrusted [5], [6]) before being deployed to a system. To determine a chip whether it is recycled at a distributor's site, it is required to power up a chip and measure the ring oscillator frequency. This can be challenging as the distributors may not have the proper test infrastructures. Moreover, accessing individual chip (removing it from the packaging and then place in the tester) may create additional defects. *Thus, it is a mandatory requirement for a distributor to verify the authenticity of a chip without powering it up.*

The contributions of this paper are as follows:

- The core of the proposed structure is to utilize a small radio-frequency identification (RFID) tag that contains a small non-volatile memory (NVM) to be placed on the package. The chip needs to be equipped with a ring oscillator (RO) and an electronic chip ID ($ECID$). We propose to store the registration data that consists of the

Yuqiao Zhang and Ujjwal Guin are with the Department of Electrical and Computer Engineering, Auburn University, AL, USA (e-mail: {yuqiao.zhang and ujjwal.guin}@auburn.edu).

RO frequency and the frequency measurement conditions in the tag. A digital signature, which is computed on the registration data (RD) and $ECID$, also needs to be stored in the tag to prevent tampering with the RD. Recycled ICs can be detected by comparing the RO frequencies, stored in the tag with measured values from the chip.

- The solution sets up a chain of trust among the distributors and empowers them to verify the identity of all prior distributors, who have possessed an IC. We use the concept of blockchain, which was originated from the cryptocurrency system Bitcoin [27] to develop our proposed solution. We believe this is the first approach to enable traceability for chips using RFID, while they travel through the supply chain. The end user can uniquely identify the complete route of a chip by verifying the RFID tag content. Any modification or tampering with the RFID tag data can easily be detected as they are protected using digital signatures.
- Our proposed solution enables a distributor to verify the authenticity of a chip without powering it up. This is a significant improvement compared with the traditional barcode-based tracking [28], which can easily be cloned or tampered. We believe that this is the first approach that enables verification at a distributor's site without powering up the chips.

Note that our proposed solution cannot address the detection of tampering, which may happen at a malicious distributor's site. Addressing of tampering is beyond the scope of this paper as it may require a different set of techniques.

The rest of the paper is organized as follows. Section II introduces the prior process variation resilient approach for the detection of recycled ICs. Section III introduces our proposed solution for enabling end-to-end traceability of ICs in the supply chain. Security analysis is performed in Section IV. Section V concludes the paper.

II. Prior Process Variation Resilient Approach

The solution proposed in [26] utilizes a ring oscillator and a non-volatile memory, where – (i) the registration data (RD) that consists of the frequency (C_0) of an RO and the conditions (e.g., supply voltage (V_0), temperature (T_0), and duration (t_{D0}) for the frequency measurement), and (ii) a digital signature ($Sig(H_d)$) on data (d) that consists of RD and electronic chip ID ($ECID$) are stored. $ECID$ provides a unique identification to each chip. It generally includes the X-Y locations of a die in the wafer, lot information, wafer number, binning information, speed grade, etc. for traceability purposes [29]. This $ECID$ value can be accessed using *ECIDCODE* instruction defined in Std 1149.1 [30]. Note that $ECID$ is the unique identification for a chip, not the RFID device. The detection requires the verification of the signature to detect tampering with the NVM content and the comparison between the measured and stored frequencies. This approach helps to detect recycled ICs used as little as a day with a very low-cost measurement unit.

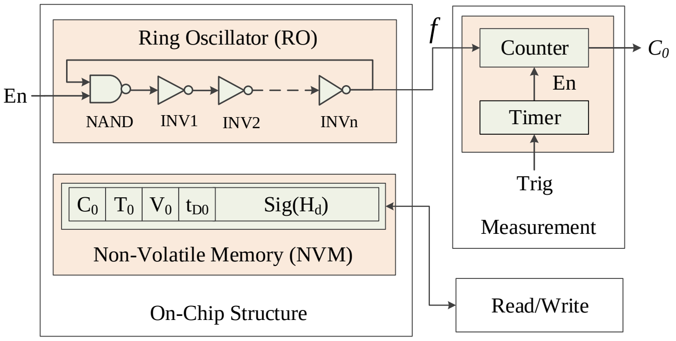


Figure 1: Prior process variation resilient on-chip structure for detecting recycled ICs [26].

Figure 1 shows the structure proposed in [26] for detecting recycled ICs. It consists of an RO and an NVM. This RO can be selected from one of the process monitors [31]–[33] currently used in modern chips. The output of this RO can be made available using an existing primary output (PO) through multiplexing primarily to reduce the pin count. A counter and a timer are required to measure the RO frequency. One can also use the existing on-chip counter and timer for the frequency measurement. Test access port and boundary-scan architecture [30] can be used to access the NVM content. The solution requires to generate the digital signature and then program it into the NVM during the registration phase. The identity of the chip is verified during the authentication phase.

A. Registration Process

The registration phase starts after the chips are manufactured and tested for defects. Only the defect-free chips go through the registration process. During this phase, the frequency of the ring oscillator is measured by using a low-cost measurement unit. Next, the digital signature is constructed on the sensor data. Finally, they are programmed into an NVM. The steps are described as follows:

1) Ring oscillator data (RD) is constructed by concatenating counter value and measurement conditions.

$$RD = \{C_0||T_0||V_0||t_{D0}\}$$

2) Data (d) is constructed by concatenating RD and $ECID$.

$$d = \{RD||ECID\}$$

3) The digital signature $(Sig(H_d))$ is constructed on the hash of d with the original component manufacturer (OCM)'s private key. This secure private key is only available to the OCM.

$$\begin{aligned} H_d &= hash(d) \\ Sig(H_d) &= K^{-}(H_d) \end{aligned}$$

where, $hash()$, K^{-}, $K^{-}()$ represent a secure hash algorithm (SHA-2/SHA-3 [34]), private key, and the encryption function (RSA or ECC [35]), respectively.

4) The oscillator data RD, and the digital signature $Sig(H_d)$ are stored in the NVM of the chip.

B. Authentication Process

The authentication process can be described as the process of verifying the authenticity of a device. It can be straightforward and performed by the system integrator or end user with a very low-cost measurement set-up, which has to be equipped with a counter and a timer (see details in [26]).

During this phase, it is necessary to read the $ECID$ and NVM content from the chip. The signature comparison is performed to verify the integrity of the NVM content. At the end of the authentication process, the age of the chip is determined by comparing the stored RO frequency with the measured RO frequency. The steps are described as follows:

1) The NVM content that consists of the ring oscillator data (RD) and digital signature ($Sig(H_d)$) of the chip under authentication, and the $ECID$ value are read. The data (d) is now constructed by concatenating RD and $ECID$.

$$d = \{RD||ECID\}$$

2) A hash (H_d) is computed on d, and another hash (H_d^*) is recovered from the signature ($Sig(H_d)$).

$$H_d^* = K^+(Sig(H_d))$$

where, K^+ represents the public key.

3) The computed hash (H_d) and the recovered hash (H_d^*) are tested for any mismatch. Any mismatch indicates the tampering of the NVM content by an adversary, and the chip will be flagged as recycled.

4) If the hashes match perfectly, the measurement parameters during registration (T_0, V_0, and t_{D0}) are extracted from the ring oscillator data (RD).

5) The RO clock cycle count (C_0^*) is measured using parameters t_{D0}, T_0, and V_0.

6) The difference between the measured clock cycle count (C_0^*) and the registration clock cycle count (C_0) is calculated. If the difference is greater than the precision of the counter (measurement error), the chip will be identified as recycled.

III. Proposed Comprehensive Approach for Combating IC Recycling

The solution proposed in Figure 1 can detect recycled ICs accurately even though they have been used for a short period of time. However, it is necessary to power up the chip when an entity in the supply chain wants to verify whether it has been used before or not. Note that a chip travels through many distributors, which some can be untrusted, before being deployed to a system. It can be challenging for many distributors to adopt the solution proposed in [26], as they may not have the proper test infrastructures. Besides, access to individual chips may be infeasible as unpackaging may create many defects and anomalies from improper handling.

Figure 2 shows our proposed design, where the chip is equipped with an RFID tag. We propose to move the on-chip NVM contents, such as, the registration data, the signature, and other information (see Section III-A) to an RFID tag. The die of a chip only contains the ring oscillator to determine the age, whereas, the RFID tag can be placed in the package during the packaging stage of the manufacturing process for enabling traceability of chips in the supply chain. Note that a similar effort to integrate RFID in the chip is ongoing by Supply Chain Hardware Integrity for Electronics Defense (SHIELD) initiative by DARPA [36].

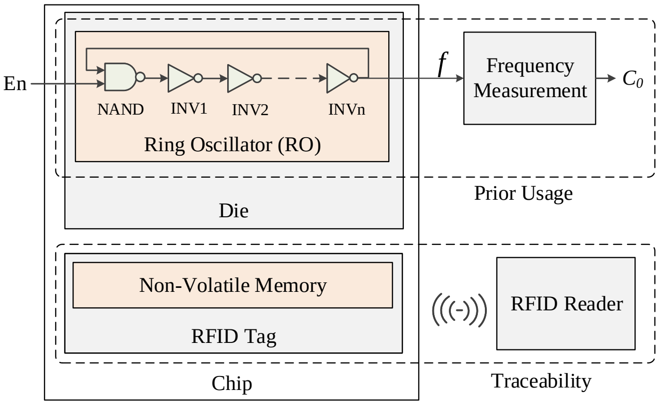


Figure 2: Proposed design for enabling traceability of ICs in the Supply Chain for combating against recycling.

In recent years, RFID tags are widely used for the traceability in the supply chain. There are two basic types of RFID tags in use: passive and active tags. For active RFID tags, the tag's lifetime may be limited by the energy stored in the integrated battery. On the other hand, passive tags are more popular due to lower size, cost, and longer lifetime. As these tags do not require a battery, they can be small enough to put into a label attached on the product. Even though the RFID solution provides flexibility for device identification, its contents are vulnerable to unwanted modifications. Our solution provides protection against it as the contents are digitally signed.

A. Proposed Approach for Enabling Traceability of ICs

The traceability of a component in the supply chain can be achieved by creating a chain of trust among the manufacturer, distributors, and the user of these chips. We use the concepts of the blockchain, which was introduced in the Bitcoin cryptocurrency system by Satoshi Nakamoto in 2008 [27]. Bitcoin uses a hash-based block structure, and a consensus algorithm denoted as Proof-of-Work (PoW) to achieve decentralization. We do not need a consensus algorithm for the traceability purposes as the endpoints of the component supply chain are trusted, and chips are the transactions. As a result, the concern for double-spending will never arise. In the supply chain, the manufacturers of chips are treated as trusted (see General Requirements of the Standard AS6171 [5]), as there is no motivation for a manufacturer to recycle chips and send them into the market as new. In addition, the end-users (e.g., Honeywell, NASA, Boeing, etc.) of the chips are also considered as trusted as they are suffered from recycled chips. Thus, our objective here is to identify a recycled (used and old) chip that enters into the supply chain through untrusted distributors.

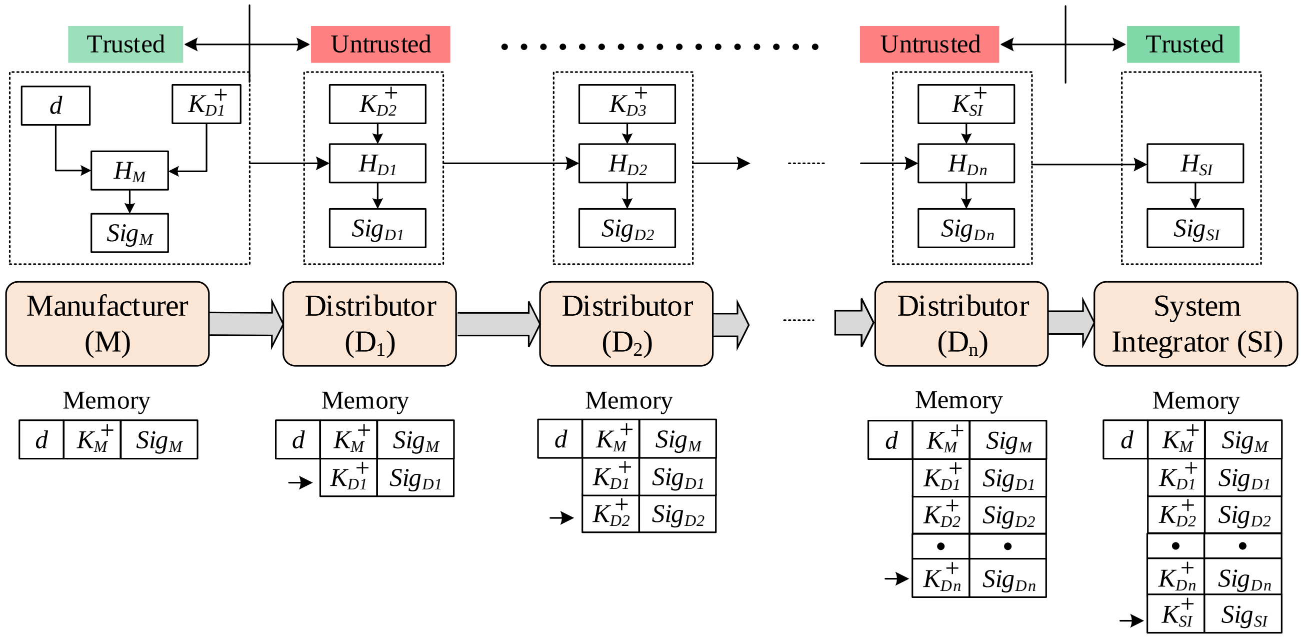


Figure 3: Proposed flow for enabling traceability of ICs in electronic component supply chain.

Figure 3 shows the proposed solution to enable traceability of chips while they travel through the electronics supply chain. First, the manufacturer reads the RO frequency (C_0) once the chip is free from manufacturing defects. The parameters during the measurement process (e.g., supply voltage (V_0), temperature (T_0), and duration (t_{D0})) are also recorded. The data (d) is constructed by concatenating these parameters with the $ECID$, where $d = \{C_0||V_0||T_0||t_{D0}||ECID\}$. A cryptographically secure hash (H_M) is computed on d and the ID of the first distributor (e.g., public key of D_1, $K^+_{D_1}$). A digital signature (Sig_M) is then computed on H_M. The manufacturer updates the RFID tag memory with $\{d, K^+_M, Sig_M\}$ using a commercial RFID reader, and later ships the chip to the distributor, D_1. Second, the distributor D_1 first reads the RFID content using a commercially available RFID reader once it receives the chips from the manufacturer. It then verifies the integrity of the RFID content. If the verification passes, D_1 creates a hash (H_{D_1}) on the previous stage's hashes and signatures, and next distributor's public ID (e.g., $K^+_{D_2}$). It then computes the signature (Sig_{D_1}) on H_{D_1}, updates the RFID with $K^+_{D_1}$, Sig_{D_1}, and sends the chip to the next distributor (D_2), which also performs the same steps as D_1. Finally, the system integrator (SI) verifies the entire RFID content and constructs the complete trace. Once the chip has been placed into a system, SI updates the RFID memory with its own signature to certify that it has been deployed.

Note that the IDs of different manufacturers, distributors, and system integrators (users) are required to be stored in a secure database and can be accessed through a trusted website such that one cannot tamper these IDs. One can also store the certificates [37] in the RFID, however, it may require larger tag memory space.

Figure 4 shows our proposed approach for enabling traceability in the supply chain. The proposed approach consists of three stages - (1) read RFID content, (2) verify RFID content, and (3) update RFID content. Note that the manufacturer only performs the update operation, as there are no prior entities in the supply chain and it is not required to verify RFID content.

1) **Read RFID Content:** The first step is to extract the information stored in the RFID tag. This can be performed through a commercial RFID reader without powering a chip.

2) **Verify RFID Content:** The distributor needs to perform signature verification for all prior stages starting from the OCM. Note that each row in the memory contains the public key (K^+_i) of the manufacturer (first row), the system integrator (last row), or the distributor (other rows), and the signature (Sig_i). The verification can be performed as follows:

- Step 1: The content in the 1^{st} row of the RFID memory needs to be read first by i^{th} distributor (D_i), which was created by the OCM. A hash H_M is computed based on d and the public key of distributor 1.

$$H_M = hash(d||K^+_{D1}) \tag{1}$$

where, $hash(.)$ represents a secure hash function (e.g., SHA-2 or SHA-3 [34]). Similarly, a hash (H^*_M) will be recovered from the signature by using the following equation:

$$H^*_M = K^+_M(Sig_M) \tag{2}$$

where, K^+_M is the public key from the OCM. The integrity is verified by comparing H_M with H^*_M.

- Step 2: Once the previous verification is passed, D_i reads the next row j of the RFID content. A hash is now

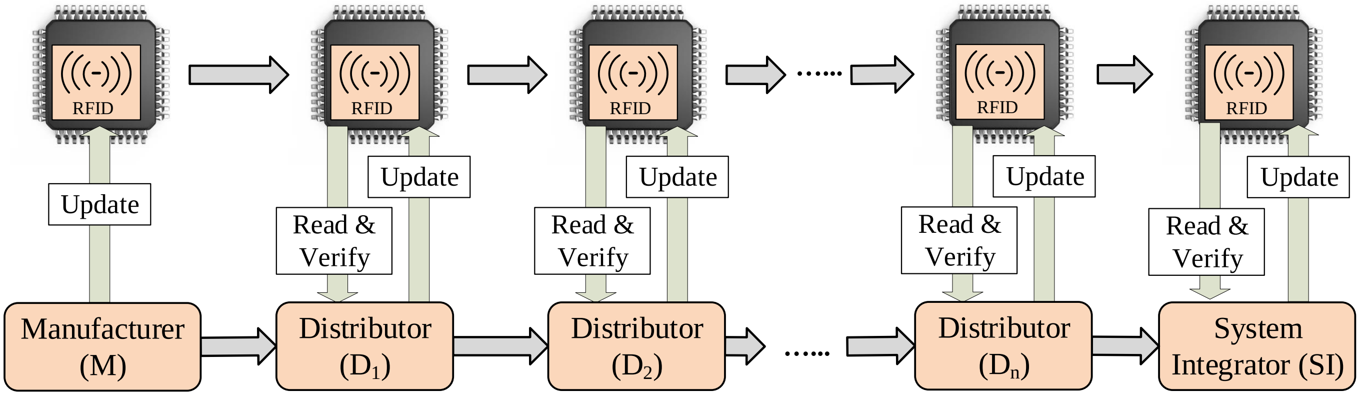


Figure 4: Verification and update process for the contents of an RFID tag placed in the package of a chip.

computed on previous stage hash value H_{j-1}, signature Sig_{j-1}, and the public key K_{j+1}^{+} using Equation 3.

$$H_j = hash(H_{j-1}||Sig_{j-1}||K_{j+1}^{+}) \tag{3}$$

Similarly, another hash value H_j^* is recovered from the signature by using following equation.

$$H_j^* = K_j^{+}(Sig_j) \tag{4}$$

The verification will pass if $H_j = H_j^*$, j will be increased by 1, and stay at Step 2. Any mismatch of the computed hash value and recovered hash value will give an indication that RFID content is tampered and the chip will be flagged as recycled, and the corresponding distributor will be identified. In addition, distributor, D_{i-1} can also be charged for promoting recycled ICs, as either it does not perform the verification when it acquired the chips from D_{i-2} or deliberately falsified the authentication results. Note that the end-user or the system integrator will also follow the same verification process as D_i.

The authenticity of a device can be ensured by verifying its identity. At every stage (different distributors and the SI), the verification of a device ID is performed. The data d contains an electronic chip ID (See Equation 5), which is unique to every device. The manufacturer (considered trusted in our threat model) provides its digital signature to certify $ECID$. Any tampering of d can be detected at any stages (D_1 through SI).

3) **Update RFID Content:** In this phase, all entities in the supply chain write data into the RFID memory. As the manufacturer is the first entity in the supply chain and trusted, the content directly written by the OCM should be authentic and verified. On the other hand, the distributors and system integrator only update the RFID memory, once the chip passes the verification as described above. The manufacturer writes the data d, its public key (K_M^{+}), and signature (Sig_M) into the RFID tag memory.

The update process for the manufacturers can be described as follows:

- Step 1: The data (d) is constructed by concatenating the RO cycle count (C_0) with measurement conditions (e.g., temperature (T_0), supply voltage (V_0) and duration (t_{D0}), and electronic chip ID ($ECID$).

$$d = \{C_0||T_0||V_0||t_{D0}||ECID\} \tag{5}$$

- Step 2: A secure hash is computed based on d and the public key of the first distributor (K_{D1}^{+}).

$$H_M = hash(d||K_{D1}^{+}) \tag{6}$$

- Step 3: The signature of the manufacturer is computed on H_M.

$$Sig_M = K_M^{-}(H_M) \tag{7}$$

where, K_M^{-} is the private key of the manufacturer.

- Step 4: Finally, the manufacturer writes the data $\{d$, K_M^{+}, $Sig_M\}$ into the RFID and distributes the chip into the supply chain.

The update process for the distributors is described as follows:

- Step 1: D_i reads the entire RFID memory to construct the data (d_i) for hash computation.

$$d_i = \{H(...(H(H(d||K_{D1}^{+})||Sig_M||K_{D2}^{+})||Sig_{D1}|| \\ ...)||K_{Di}^{+})||Sig_{Di-1}\} \tag{8}$$

- Step 2: A secure hash is computed on d_i and the public key of the $(i+1)^{th}$ distributor (K_{Di+1}^{+}).

$$H_{Di} = hash(d_i||K_{Di+1}^{+}) \tag{9}$$

- Step 3: The signature of D_i is computed on H_{Di}.

$$Sig_{Di} = K_{Di}^{-}(H_{Di}) \tag{10}$$

- Step 4: Finally, the distributor appends $\{K_{Di}^{+}$, $Sig_{Di}\}$ to the RFID and sends the chips to the next distributor or system integrator.

Finally, the update process for the SI can be described as follows:

- Step 1: SI reads the entire RFID memory to construct the data (d_{SI}) for hash computation.

$$d_{SI} = \{H(...(H(H(d||K_{D1}^{+})||Sig_M||K_{D2}^{+})||Sig_{D1}|| \\ ...)||K_{SI}^{+})||Sig_{Di}\} \tag{11}$$

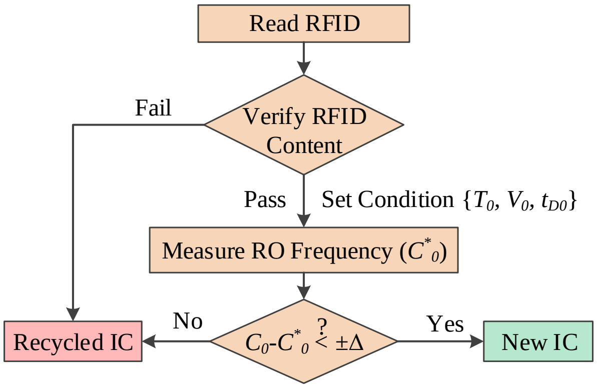

Read RFID
Verify RFID Content
Fail
Pass
Set Condition {T_0, V_0, t_{D0}}
Measure RO Frequency (C^*_0)
Recycled IC
No
C_0-$C^*_0 \overset{?}{<} \pm\Delta$
Yes
New IC

Figure 5: Flow for detecting Recycled ICs.

- Step 2: A secure hash is computed on d_{SI}.

$$H_{SI} = hash(d_{SI}) \tag{12}$$

- Step 3: The signature of SI is computed on H_{SI}.

$$Sig_{SI} = K^{-}_{SI}(H_{SI}) \tag{13}$$

- Step 4: Finally, SI appends $\{K^{+}_{SI}, Sig_{SI}\}$ to the RFID after deploying it into a system.

B. Approach for Verification of the Prior Usage of an IC

This proposed solution enables a chain of trust among the distributors. Anyone in the supply chain can verify the identity of chips without powering them on. However, the final verification, whether a chip is used before or not, is performed at the system integrator's site. Figure 5 shows the verification of the prior usage of an IC by the SI. Once the complete route of an IC in the supply chain is verified, the SI powers up the chip to measure the RO frequency.

The measurement conditions (T_0, V_0) are first set up to measure the RO clock cycle count (C^*_0) with the fixed time interval (t_{D0}). These measurement parameters are reconstructed from the data ($d = \{C_0||T_0||V_0||t_{D0}||ECID\}$), which is present at the 1^{st} row of the RFID memory. The difference between the measured clock cycle count (C^*_0) and the registration clock cycle count (C_0) is calculated. If the difference is greater than the precision of the counter (measurement error, Δ), the chip is identified as recycled, otherwise, as new. The same setup (e.g., a timer and a counter) presented in Figure 1 can be used for the measurement, and the details can be found in [26].

IV. Analysis

This section focuses on the implementation details and the attack analysis of our proposed solution for providing traceability of chips in the supply chain.

A. Implementation Details

We have implemented our proposed scheme using a commercial off-the-shelf RFID tag (MIFARE Classic [38]). Figure 6 shows the experimental setup for implementing our proposed solution. We choose a very low-cost RFID reader (MFRC522 RFID module [39]) to read and update the RFID tag memory. A Raspberry Pi 3 with 1.2 GHz quad-core CPU and 1GB RAM, which controls the read/write data, is used to interface the RFID reader. Here the SRAM chip is treated as the circuit under test. Furthermore in the future, we plan to fabricate chips with RFID tags placed in the package. We use M2Crypto [40], crypto, and SSL toolkit for Python, to compute and then verify Elliptic Curve Digital Signatures. The distributor IDs and digital signatures are loaded into the MIFARE RFID tag using the MFRC522 RFID module. Note that the Laundry MIFARE Classic RFID tag has an electrically erasable programmable read-only memory (EEPROM) of 1K Bytes, where we store the trace for different distributors. In the MIFARE Laundry Classic 1K RFID tag, there are 16 sectors, and each sector consists of 4 blocks of 16 bytes each.

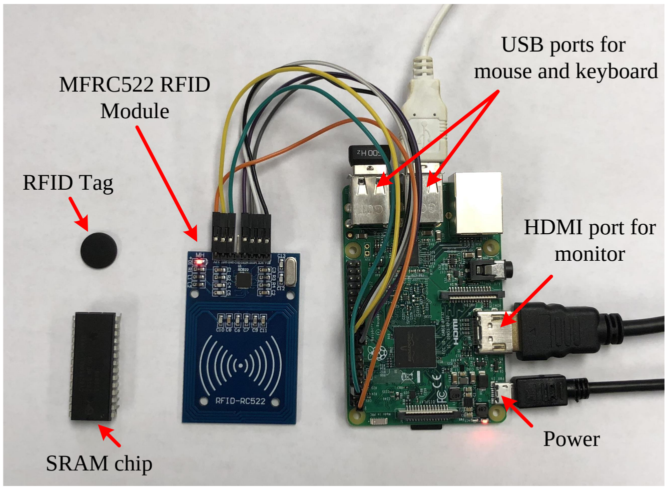


Figure 6: Setup for implementing our proposed approach.

The memory space required to store one distributor (and the manufacturer) is determined as follows:

- The data (d) can be of 174 bits (T_0 of 10 bits, V_0 of 10 bits, C_0 of 32 bits, t_{D0} of 10 bits, and $ECID$ of 112 bits [29]).
- A distributor (manufacturer) ID can be of 20 bits, which can represent 2^{20} distinct entities. Note that it is not necessary to store the public keys (K^{+}) in the RFID due to its resource (low memory) constraints. We can store unique public IDs of the manufacturer and the distributors instead. It is necessary to maintain a website from which one can find the public keys for different manufacturers, distributors, and system integrators using this public ID.
- ECDSA signature (SECP-256R1 ECDSA [41]) can be of 512-bits. We chose SHA256 to hash the data. We used the M2Crypto library [40] in python to create the hash and digital signature. Here the signature is combined with 10 bytes of cyclic redundancy check (CRC) to protect the integrity of the signature from unintended modification, such as, noise.

Combining all these bits, we need 5 blocks in the RFID tag memory to store the trace for one distributor or the system integrator. For the manufacturer, we need to store the data (d) along with its ID and signature, which requires 7 blocks.

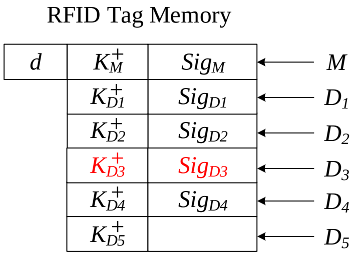
We can store relevant information for one manufacturer, one system integrator, and seven distributors, when we use this RFID tag.

Note that we do not need to add one tag per chip, and it is not necessary to attach this tag into the package as long as they travel together in the supply chain. One can add only one RFID tag for a small batch of chips. One only needs to measure all the frequencies and then construct the data ($d = \{C_0^{(1)}||C_0^{(2)}||...||C_0^{(n)}||V_0||T_0||t_{D0}||ECID^{(1)}||ECID^{(2)}||...|| ECID^{(n)}\}$) and then store the signature (Sig_M) into the RFID tag. Here, $C_0^{(i)}$ and $ECID^{(i)}$ are the RO frequency and $ECID$ of the i^{th} chip, respectively.

B. Attack analysis

In this section, we present different attack scenarios against our proposed solution and assess the resistivity of the proposed architecture under such attacks.

1) Tampering with the RFID Content: In this attack, an adversary tampers with the RFID content using an RFID reader. To break the traceability of a component in the supply chain, the attacker can remove one or more entries from the RFID memory to eliminate the trace for few distributors. For example, an adversary (D_4) removes the 4^{th} entry (i.e., public key and signature from the D_3) of the RFID tag memory, and then sells the chip to D_5. Figure 7 shows an example of removing attack, where the row highlighted in red was removed by the distributor D_4. Note that M and D_i represents the manufacturer, and i^{th} distributor, respectively.



RFID Tag Memory

d	K_M^+	Sig_M	← M
	K_{D1}^+	Sig_{D1}	← D_1
	K_{D2}^+	Sig_{D2}	← D_2
	K_{D3}^+	Sig_{D3}	← D_3
	K_{D4}^+	Sig_{D4}	← D_4
	K_{D5}^+		← D_5

Figure 7: Tampering with the RFID content to modify trace.

This attack can be detected by a distributor (in this example, distributor D_5) or the system integrator (SI) while they perform the signature verification. When doing authentication described in Section III, the first two verifications for the manufacturer (M) and distributor (D_1) will be passed. However, the third verification will fail as there will be a mismatch of the computed hash value H_2 and recovered value H_2^* from the signature because of the involvement with different public keys. The authentication can be performed as follows:

- D_5 reads the entire memory, constructs data for each stages, and then compute the hashes.

  $d_M = \{d\}, H_M = hash(d_M||K_{D_1}^+)$

  $d_{D1} = \{H_M||Sig_M\}, H_{D1} = hash(d_{D1}||K_{D2}^+)$

  $d_{D2} = \{H_{D1}||Sig_{D1}\}, H_{D2} = hash(d_{D2}||K_{D4}^+)$
- It recovers the hashes from the signatures.

  $H_M^* = K_M^+(Sig_M); H_{D1}^* = K_{D1}^+(Sig_{D1})$

  $H_{D2}^* = K_{D2}^+(Sig_{D2})$
- Finally, it performs signature verification.

  $ver(H_M, H_M^*) = pass;\ ver(H_{D1}, H_{D1}^*) = pass$

  $ver(H_{D2}, H_{D2}^*) = fail$, as

  $H_{D2}^* = hash(H_{D1}||Sig_{D1}||K_{D3}^+)$ where the $ver()$ function can be described as follows:

$$ver(x_1, x_2) = \begin{cases} pass & \text{if } x_1 = x_2; \\ fail & \text{otherwise;} \end{cases} \quad (14)$$

2) Impersonation of a Distributor: In this attack, an untrusted distributor (D_j) try to sneak into stage $(i+1)^{th}$ distribution stage using the identity of a trusted distributor (D_{i+1}). However, this attack is infeasible as the entries of the RFID memory is protected by the digital signature. It is infeasible for D_j to create a signature of D_{i+1}. As a result, D_j cannot pass the chip to D_{i+2} as the signature verification will fail. In addition, we do not see any motivation for D_j to sneak into the supply chain. However, it can perform tampering with an authentic chip received from D_i and send to D_{i+1}, which is beyond the scope of this paper.

3) Dictionary Attack: In this attack scenario, a recycler (untrusted distributor) constructs a dictionary of RO frequencies from many new chips. Each entry of the dictionary consists of the data (d), manufacturer's public key (K_M^+), and its signature (Sig_M) from new chips. After recycling an old chip, the adversary measures the frequency of that RO. If a match (or close enough) is found in the dictionary, he/she can update the RFID content with the respective content from the dictionary. Note that the RO frequencies of the new chips vary significantly (generally Gaussian in nature [19]) due to process variation. It can be possible that two RO frequencies of new and recycled chips are of the same value. Thus, it seems that a recycler can impersonate an old chip with a new one. However, one can easily detect this attack by verifying the signature (Sig_M). The verification process can be performed as follows:

- Read $ECID^*$ value, and RFID contents from the chip.
- *First Authentication:* This fails if $ECID$, which is present in the data (d) from the RFID, does not match with $ECID^*$ of the chip. This authentication can only be performed by the SI as it is necessary to power up the chip to read $ECID^*$.
- *Second Authentication:* If the *First Authentication* passes, a second authentication is necessary to verify the signature, which can be done as follows: (i) compute hash on data (d), $H_d = hash(d)$, (ii) recover the hash from the signature (Sig_M), $H_d^* = K_M^+(Sig_M)$, and (iii) verify both these hashes using $ver(H_d, H_d^*)$ function (see Equation 14).

Note that this second authentication can be performed by any entity in the supply chain.

4) Tampering the ring oscillator: For this attack scenario, an attacker tampers the physical structure of the RO of a counterfeit chip. An RO becomes faster if the number of inverter stages becomes smaller. An attacker can reduce the number of inverter stages using FIB circuit edit [42]. To perform this attack, the chip needs to be decapsulated to remove old package and then perform the edit. After the modification, the chip needs to be repackaged again and remarked to its original specification. Note that this attack needs to be performed to every chip. As a result, the circuit edit, repackaging, and remarking may not be cost-effective to the counterfeiters. Hence, it is unlikely to be used in practice by an adversary.

5) Improper Registration: In this attack scenario, an untrusted entity at the production site can update the RFID content with a false oscillation count which is significantly less than the actual measured value. As a result, the oscillation frequency can still be found very close to the registration value, even though a chip has been used in the field for a long time. However, there will not be any financial motivation behind such an act from a foundry's perspective as it will only help the counterfeiters. Moreover, we generally consider the foundry as trusted for IC recycling. Thus, manipulating the frequency value in the registration phase does not make any financial motivation to the foundries.

6) Key Breach: If a breach happens for distributor D_j, it is required to update its keys and put its new signature in forthcoming chips. However, the public key remains unchanged (old key) in the RFID memory of chips with previous signatures. Practically an adversary can put a signature at the $(j+1)^{th}$ location of the RFID memory (first location is reserved for the manufacturer) with modifying next stage distributor ID, and thus, make the authentication fail for an authentic chip. At this point, the system integrator (SI) can contact distributor D_j for more information regarding the key breach. It is then up to the SI to decide the acceptance of this chip. If a breach happens, the distributor must report it to all the participating entities in the supply chain. Note that if the manufacturer's database is breached, no authentication can be performed for chips with old keys as the RO frequency value can be updated in the RFID memory.

V. Conclusion

In this paper, we proposed a robust and low-cost solution for detecting recycled ICs, which are reclaimed from old electronic systems. Our solution enables traceability by ensuring a chain of trust among the manufacturer, the distributors, and the system integrator. It utilizes a small passive RFID tag, which needs to be placed on the package of a chip. Any entity in the supply chain can verify the authenticity of a chip using a hand-held commercial RFID reader. It is not necessary for a distributor to power up a chip during the verification process. However, the final verification needs to be performed at the system integrator's site and requires powering up the chip for RO frequency measurement. As an RFID tag can be placed in the package of a chip, our proposed solution can practically be applied to all the chips.

Acknowledgment

This material is based upon a work supported by the United States Air Force/Air Force Materiel Command (USAF/AFMC) under grant AF-FA8650-19-1-1707. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the USAF/AFMC.

References

[1] IHS iSuppli, "Top 5 Most Counterfeited Parts Represent a $169 Billion Potential Challenge for Global Semiconductor Market," 2011.

[2] M. M. Tehranipoor, U. Guin, and D. Forte, *Counterfeit Integrated Circuits: Detection and Avoidance*. Springer, 2015.

[3] U. Guin, K. Huang, D. DiMase, J. Carulli, M. Tehranipoor, and Y. Makris, "Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain," *Proceedings of the IEEE*, pp. 1207–1228, 2014.

[4] U. Guin, D. DiMase, and M. Tehranipoor, "Counterfeit Integrated Circuits: Detection, Avoidance, and the Challenges Ahead," *Journal of Electronic Testing*, 2014.

[5] G-19A Test Laboratory Standards Development Committee, "AS6171: Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts," 2016.

[6] G-19CI Continuous Improvement, "AS5553: Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition," 2009.

[7] G-19D Distributor, "AS6081: Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition - Distributors," 2012.

[8] CTI, "Certification for Counterfeit Components Avoidance Program," 2011, http://www.cti-us.com/pdf/CCAP101Certification.pdf.

[9] IDEA, "Acceptability of Electronic Components Distributed in the Open Market," 2017, http://www.idofea.org/products/118-idea-std-1010b.

[10] X. Zhang, K. Xiao, and M. Tehranipoor, "Path-Delay Fingerprinting for Identification of Recovered ICs," in *Proc. International Symposium on Fault and Defect Tolerance in VLSI Systems*, 2012.

[11] K. Huang, J. Carulli, and Y. Makris, "Parametric counterfeit IC detection via Support Vector Machines," in *Proc. International Symposium on Fault and Defect Tolerance in VLSI Systems*, pp. 7–12, 2012.

[12] Y. Zheng, A. Basak, and S. Bhunia, "CACI: Dynamic current analysis towards robust recycled chip identification," in *Design Automation Conference (DAC)*, pp. 1–6, 2014.

[13] H. Dogan, D. Forte, and M. Tehranipoor, "Aging analysis for recycled FPGA detection," in *IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, 2014.

[14] Y. Zheng, X. Wang, and S. Bhunia, "SACCI: Scan-Based Characterization Through Clock Phase Sweep for Counterfeit Chip Detection," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 2014.

[15] Z. Guo, M. T. Rahman, M. M. Tehranipoor, and D. Forte, "A zero-cost approach to detect recycled SoC chips using embedded SRAM," in *IEEE Int. Symp. on Hardware Oriented Security and Trust*, 2016.

[16] T.-H. Kim, R. Persaud, and C. Kim, "Silicon Odometer: An On-Chip Reliability Monitor for Measuring Frequency Degradation of Digital Circuits," *IEEE Journal of Solid-State Circuits*, pp. 874–880, 2008.

[17] X. Zhang, N. Tuzzio, and M. Tehranipoor, "Identification of recovered ICs using fingerprints from a light-weight on-chip sensor," in *Proc. IEEE-ACM Design Automation Conference*, 2012.

[18] X. Zhang and M. Tehranipoor, "Design of On-Chip Lightweight Sensors for Effective Detection of Recycled ICs," *IEEE Transactions on Very Large Scale Integration Systems*, pp. 1016–1029, 2014.

[19] U. Guin, X. Zhang, D. Forte, and M. Tehranipoor, "Low-cost On-Chip Structures for Combating Die and IC Recycling," in *Proc. of ACM/IEEE on Design Automation Conference*, 2014.

[20] U. Guin, D. Forte, and M. Tehranipoor, "Design of Accurate Low-Cost On-Chip Structures for Protecting Integrated Circuits Against Recycling," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, pp. 1233–1246, 2016.

[21] K. He, X. Huang, and S. X. D. Tan, "EM-based on-chip aging sensor for detection and prevention of counterfeit and recycled ICs," in *IEEE/ACM International Conf. on Computer-Aided Design*, pp. 146–151, 2015.

[22] N. Asadizanjani, M. Tehranipoor, and D. Forte, "Counterfeit electronics detection using image processing and machine learning," in *Journal of Physics: Conference Series*, 2017.

[23] S. Shahbazmohamadi, D. Forte, and M. Tehranipoor, “Advanced physical inspection methods for counterfeit ic detection,” in *40th International Symposium for Testing and Failure Analysis*, pp. 55–64, 2014.

[24] M. Miller, J. Meraglia, and J. Hayward, “Traceability in the Age of Globalization: A Proposal for a Marking Protocol to Assure Authenticity of Electronic Parts,” in *SAE Aerospace Electronics and Avionics Systems Conference*, 2012.

[25] Semiconductor Industry Association (SIA), “Public Comments - DNA Authentication Marking on Items in FSC5962,” 2012.

[26] M. Alam, S. Chowdhury, M. Tehranipoor, and U. Guin, “Robust, Low-Cost, and Accurate Detection of Recycled ICs using Digital Signatures,” in *IEEE Int. Symposium on Hardware Oriented Security and Trust (HOST)*, 2018.

[27] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” http://bitcoin.org/bitcoin.pdf,” 2008.

[28] ISO/IEC JTC 1/SC 31, “Information technology automatic identification and data capture techniques QR code bar code symbology specification,” *International Organization for Standardization*, ISO/IEC 18004:2015.

[29] Bill Eklow, “ECID vs Device ID,” 2006, btw.tttc-events.org/material/BTW10/Presentations/Session%205.2.pptx.

[30] IEEE 1149.1-2013 - IEEE Standard for Test Access Port and Boundary-Scan Architecture, https://standards.ieee.org/standard/1149_1-2013.html.

[31] T.-K. Lee, “Process monitor for CMOS integrated circuits,” Jan. 23 1996, US Patent 5,486,786.

[32] E. O. Sugasawara, “Process monitor circuitry for integrated circuits,” 2000, US Patent 6,124,143.

[33] R. Bach, “Process monitor with statistically selected ring oscillator,” 2003, US Patent 6,544,807.

[34] National Institute of Standards and Technology, “FIPS 180-4: Secure Hash Standard (SHS),” 2015.

[35] Elaine Barker, “FIPS 186-4: Digital Signature Standard (DSS),” 2013.

[36] K. Bernstein, “Supply chain hardware integrity for electronics defense (SHIELD),” *Defense Advanced Research Projects Agency, Microsystems Technology Office/MTO Broad Agency Announcement*, 2014.

[37] D. R. Kuhn, V. C. Hu, W. T. Polk, and S.-J. Chang, “Introduction to public key technology and the federal PKI infrastructure,” National Inst of Standards and Technology, Tech. Rep., 2001.

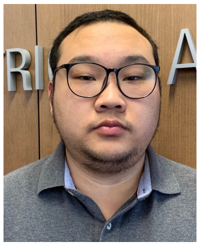
[38] NXP, “MIFARE Classic EV1 1K - Mainstream contactless smart card IC for fast and easy solution development,” 2018, https://www.nxp.com/docs/en/data-sheet/MF1S50YYX_V1.pdf.

[39] NXP, “MFRC522: Standard performance MIFARE and NTAG frontend,” 2016, https://www.nxp.com/docs/en/data-sheet/MFRC522.pdf.

[40] M2Crypto, https://gitlab.com/m2crypto/m2crypto.

[41] ECDSA_AllPrime-Elliptic Curve Digital Signature Algorithm, https://csrc.nist.gov/csrc/media/projects/cryptographic-standards-and-guidelines/documents/examples/ecdsa_prime.pdf.

[42] C. Helfmeier, D. Nedospasov, C. Tarnovsky, J. S. Krissler, C. Boit, and J.-P. Seifert, “Breaking and entering through the silicon,” in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pp. 733–744, 2013.



Yuqiao Zhang (S’18) received the M.S. degree in Electrical and Computer Engineering from Auburn University, Auburn, AL, USA in 2018. He is pursuing the Ph.D. degree from the Department of Electrical and Computer Engineering, Auburn University, Auburn, AL, USA. His current area of research includes hardware security, designing of RFID systems, implementation of blockchain-based frameworks, and supply chain security.

Ujjwal Guin (S’10–M’16) received his PhD degree from the Electrical and Computer Engineering Department, University of Connecticut, in 2016. He is currently an Assistant Professor in the Electrical and Computer Engineering Department of Auburn University, Auburn, AL, USA. He received his B.E.degree from the Department of Electronics and Telecommunication Engineering, Bengal Engineering and Science University, Howrah, India, in 2004 and his M.S.degree from the Department of Electrical and Computer Engineering, Temple University, Philadelphia, PA, USA, in 2010. Dr.Guin has developed several on-chip structures and techniques to improve the security, trustworthiness, and reliability of integrated circuits. His current research interests include Hardware Security & Trust, Blockchain, Supply Chain Security, Cybersecurity, and VLSI Design & Test. He is a co-author of the book *Counterfeit Integrated Circuits: Detection and Avoidance*. He has authored several journal articles and refereed conference papers. He was actively involved in developing a web-based tool, Counterfeit Defect Coverage Tool (CDC Tool), *http://www.sae.org/standardsdev/cdctool/*, to evaluate the effectiveness of different test methods used for counterfeit IC detection. SAE International has acquired this tool from the University of Connecticut. He is an active participant in SAE International’s G-19A and G-32 Standard Development Committees. He is a member of both the IEEE and ACM.