AFRL-RY-WP-TR-2022-0174

ROBUST, LOW-COST, AND ACCURATE DETECTION OF RECYCLED INTEGRATED CIRCUITS (ICs) USING DIGITAL SIGNATURES

Ujjwal Guin
Auburn University

JULY 2022
Final Report

AIR FORCE RESEARCH LABORATORY
SENSORS DIRECTORATE
WRIGHT-PATTERSON AIR FORCE BASE, OH 45433-7320
AIR FORCE MATERIEL COMMAND
UNITED STATES AIR FORCE

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with The Under Secretary of Defense memorandum dated 24 May 2010 and AFRL/DSO policy clarification email dated 13 January 2020. This report is available to the general public, including foreign nationals.

Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RY-WP-TR-2022-0174 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

//Signature//

GLEN D. VIA
Program Manager
Aerospace Components & Subsystems Technology Division

//Signature//

LAVERN A. STARMAN (Acting)
Deputy Chief, Aerospace Components & Subsystems Technology Division
Sensors Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

*Disseminated copies will show "//Signature//" stamped or typed above the signature blocks.

REPORT DOCUMENTATION PAGE

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED	
		START DATE	END DATE
July 2022	Final	21 February 2019	21 February 2022

4. TITLE AND SUBTITLE

ROBUST, LOW-COST, AND ACCURATE DETECTION OF RECYCLED INTEGRATED CIRCUITS (ICs) USING DIGITAL SIGNATURES

5a. CONTRACT NUMBER	5b. GRANT NUMBER	5c. PROGRAM ELEMENT NUMBER
FA8650-19-1-1707	N/A	N/A
5d. PROJECT NUMBER	**5e. TASK NUMBER**	**5f. WORK UNIT NUMBER**
N/A	N/A	Y1YW

6. AUTHOR(S)

Ujjwal Guin

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Auburn University 107
Samford Hall,
Auburn, Alabama 368479

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)	11. SPONSOR/MONITOR'SREPORT NUMBER(S)
Air Force Research Laboratory, Sensors Directorate Wright-Patterson Air Force Base, OH 45433-7320 Air Force Materiel Command, United States Air Forces	Defense Advanced Research Projects Agency (DARPA) 675 North Randolph Street Arlington, VA 22203	AFRL/RYD	AFRL-RY-WP-TR-2022-0174

12. DISTRIBUTION/AVAILABILITY STATEMENT

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

Report contains color. This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with The Under Secretary of Defense memorandum dated 24 May 2010 and AFRL/DSO policy clarification email dated 13 January 2020. This report is available to the general public, including foreign nationals. This material is based on research sponsored by Air Force Research Lab (AFRL) and the Defense Advanced Research Projects Agency (DARPA) under agreement number FA8650-19-1-1707. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of Air Force Research Lab (AFRL) and the Defense Advanced Research Projects Agency (DARPA) or the U.S. Government.

14. ABSTRACT

The continuous growth of counterfeit integrated circuits (ICs) in the electronic components supply chain calls for an immediate solution. This project addresses trustworthy electronics by developing an efficient method for the detection of recycled ICs, thereby enhancing the safety and security of US cyber infrastructure. The core of the proposed on-chip structure utilizes a ring oscillator and a small non-volatile memory (NVM). The on-chip structure stores the RO frequency, the measurement conditions, and a digital signature in the NVM.

15. SUBJECT TERMS

design assurance, counterfeit integrated circuit (IC), electronic

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES
a. REPORT	b. ABSTRACT	C. THIS PAGE		
Unclassified	Unclassified	Unclassified	SAR	44

19a. NAME OF RESPONSIBLE PERSON	19b. PHONE NUMBER *(Include area code)*
Glen Via	

PREVIOUS EDITION IS OBSOLETE.

STANDARD FORM 298 (REV. 5/2020)
Prescribed by ANSI Std. Z39.18

Table of Contents

Section **Page**

List of Figures

Figure **Page**

List of Tables

Table **Page**

1 PROBLEM STATEMENT

The continuous growth of counterfeit integrated circuits (ICs) poses a serious threat to our critical infrastructures because they can potentially impact the security and reliability of a wide variety of electronic systems. These ICs are cause for major concerns to governments and industries due to the counterfeit ICs' inferior quality. The microelectronics supply chain is corrupted by different counterfeit ICs and can fall under different categories of counterfeit. These categories are recycled, remarked, out-of-spec/defective, overproduced, cloned, forged documentation, and tampered. Among all these different counterfeit ICs, recycled ICs account for almost 80% of all the reported counterfeiting incidents. Recycled ICs pose a significant challenge to the global electronic components supply chain due to the lack of efficient, robust, and low-cost detection and avoidance technologies. The objective of this project is to design a solution that can effectively detect recycled ICs and fulfills the requirements of being – (i) low-cost, as the solution needs to be implemented into a wide variety of ICs. Moreover, a distributor in the electronic components supply can verify the authenticity of an IC using a hand-held device without performing costly and time-consuming test methods, (ii) robust, as it is necessary to eliminate the effect of measurement errors and manufacturing process variations during the detection process, and (iii) accurate, as to reduce the probability of identifying a recycled IC as new and vice versa. This proposed solution will also enable a distributor to perform the verification without powering up a chip by using a commercial hand-held radio-frequency identification (RFID) reader.

2 BACKGROUND

The rise of counterfeit ICs in electronics supply chain calls for immediate solution. 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]. Recycled, remarked, defective/outof-spec, overproduced, cloned, forged documentation and tampered ICs pose a serious threat to our critical infrastructures. Among all these different counterfeit ICs, recycled ICs account for almost 80% of all the reported counterfeiting incidents [2]. The deployment of these recycled chips in a critical infrastructure will be catastrophic as they exhibit lower performance and less remaining useful lifetime [3].

Recycled ICs are those that are reclaimed or recovered from a used system and are then misrepresented as new components produced by an original component manufacturer (OCM). Recycled ICs generally exhibit lower performance and have shorter lifespan compared to the authentic ones, due to the effects of aging during their prior usage and mishandling during the recycling process. The recycling process consists of aggressively removing components from printed circuits boards (PCBs) under very high temperatures [4]. The components are then subjected to washing, sanding, repackaging, and remarking, all of which could damage the ICs and introduce many defects and anomalies [2, 5]. The recycling process may also introduce latent defects that pass initial testing but are prone to failure in later stages. The electrical defects could be resistive open/short, negative-bias temperature instability (NBTI), time-dependent dielectric breakdown (TDDB), out-of-spec leakage current and out-of-spec dynamic current [2]. These defects could even make the components completely non-functional because of the components' exposure to extreme conditions.

The detection and avoidance approaches for recycled ICs are broadly classified into four different categories. First, there are several standards (e.g., AS6171 [6], AS5553 [7], CCAP-101 [8], and IDEA-STD1010 [9]) in practice, which recommend different physical and electrical tests for the detection purpose. The goal of these methods is to identify the defects and anomalies present in those recycled ICs, which are not typically found in authentic ones. Since we assume that foundries and assemblies have a fairly consistent manufacturing process and comprehensively test their components, one should not expect to see many defective parts. A counterfeit part often contains one or more different anomalies and deviations from the normal/usual form and/or functionality of a genuine component. These anomalies may be physical (i.e., related to the leads, package, etc.) or electrical (e.g., degradation in its performance or a change in its specifications). The PI was actively involved in developing a comprehensive assessment process for these test methods [2, 10]. The major limitation and challenges of implementing these test methods are the excessive test time, high cost, and low confidence of identifying recycled ICs.

Second, different solutions have been proposed based on statistical data analysis [11, 12, 12–16]. In [11], path-delay fingerprinting was used to differentiate recycled digital ICs from genuine ones through changes in their path delay distribution caused by prior usage. However, this technique requires data from genuine ICs, which can make its implementation impractical. In [12], a statistical approach was presented to distinguish recycled ICs by measuring electrical parameters and using a one-class support vector machine (SVM). This technique can be applied

to all types of ICs (analog and digital) but requires data from genuine samples for SVM training. In [13], the authors presented a scan-based characterization technique to detect recycled ICs. The access to the scan chains may not be always possible when the chips are already in the market, thus making it difficult to implement because of burnt fuses commonly practiced in industry. In [14], the authors utilized dynamic current analysis to determine the aging difference between high-activity and low-activity portions of symmetric structures. However, this approach requires at least a year of aging for reliable detection of recycled ICs. The authors in [15] proposed a two-phase detection approach that utilizes one-class SVM classifier to detect only recycled Field (Programmable Gate Arrays) FPGAs.

Third, on-chip sensors, which uses aging degradation, have been proposed as an alternative to the conventional test methods [17–21]. Note that extensive research has been carried out by the solid-state circuits community to analyze aging degradation in ICs. The authors in [22] proposed two separate structures to monitor NBTI and TDDB. A silicon odometer using on-chip ring oscillators has been first proposed in [23] to monitor NBTI induced degradation by measuring the beat frequency between the reference and stressed ROs. An improved version of the odometer was presented in [24] to separately monitor NBTI and HCI induced degradation. In [25], the authors presented a measurement system with an array of ROs that utilized statistical aging measurements to monitor the degradation. In [26] the authors described a product-level aging monitoring system which consists of a performance critical ARM1176 path. The authors in [27] presented a hybrid on-chip aging monitor consisting of a ring-oscillator and a delay-line. The objective of these sensors was to improve the reliability of ICs by accurately measuring the aging degradation, not to accelerate the degradation to its maximum value to identify recycled ICs. To address the shortcomings in these technologies, low-cost structures have been proposed to detect recycled ICs with greater ease [17, 18]. The technique introduced in [17] inserts a lightweight ring oscillator (RO)-based sensor (similar to one proposed in [23]) in the chip to capture the usage of the chip in the field. All these sensors will be ineffective for detecting recycled ICs when they have been used for a very short duration with high process variation.

Finally, DNA markings are commercially available to provide traceability for electronic parts. DNA marks are created using plant DNA, and then integrated with inks. This ink is then applied on the packages of the IC for enabling traceability. The authentication includes first checking whether the ink fluoresces under specific light, and second, sending a sample of the ink to a lab to verify that the DNA is in the database of valid sequences [28]. Note that DoD mandated DNA marking be placed on the components in order to track them throughout the supply chain [29]. DNA markings have several limitations that introduce some serious concerns of their applicability in counterfeit avoidance. The fast authentication achieved by observing the fluorescence of the marking under specific light can be imitated by counterfeiters, either with invalid DNA or other materials. But detailed DNA validation is extremely time-consuming and costly [30]. As a result of complex authentication process, excessive implementation, and test cost have made its application limited in practice.

3 SOLUTION STATEMENT

Recycled ICs pose a great threat to our critical infrastructure, as the counterfeiters source these parts to the supply chain due to the unavailability of low-cost test methods that can accurately detect them. The lack of proper detection approaches motivates us to develop an on-chip structure that can detect recycled ICs effectively. The core of the proposed on-chip structure is utilizing a ring oscillator and a small non-volatile memory (NVM). The on-chip structure stores the RO frequency, the measurement conditions, and a digital signature in the NVM. Although the emphasis of this project and our experimental analysis is on detection of recycled ICs, we acknowledge that our proposed solution can also be utilized to detect cloned and remarked ICs. An IC becomes an attractive target for the cloners when there is a high demand, and when original component manufacturers (OCM) stop manufacturing as they move to a new technology node and design. The RO frequency will give an indication of a cloned IC if the cloners use a pirated design file (layout/GDSII) to produce a clone. Moreover, the detection of remarked ICs can be ensured by signature verification. A digital signature is computed on the data, which consists of electronic chip ID (ECID) and RO frequency. Any tampering of the data will be detected by signature verification.

Our proposed solution also enables a distributor to perform authentication without powering up a chip. We believe, this is a significant improvement compared to the traditional tracking based on QR codes, which can easily be cloned. The solution sets up a chain of trust among the distributors, and empowers them to verify all prior distributors. Any modification or tampering with the RFID tag data can preciously be detected. The end user can uniquely identify the complete route of a chip in the supply chain by verifying the RFID tag content. The proposed research activity will make a significant contribution for developing innovative techniques to improve detection capabilities, and reduce test time. The electronic components supply chain will be secure as we can detect recycled ICs with high confidence levels. We believe that we can finally ensure our critical infrastructure free from counterfeit parts. The following tasks are intended to address the counterfeiting problem with a systematic and holistic way. These tasks will be undertaken during the entire duration of this project:

3.1 Task 1- Design of a Robust, Low-cost, and Accurate On-chip Sensor

This project proposes the design and implementation of a robust, low-cost, and accurate on-chip sensor. The design and implementation requires a ring oscillator (RO) and an on-chip non-volatile memory (NVM). The frequency of the RO needs to be measured with a specified operating condition. A digital signature is created using the measurement data which consists of the RO frequency and the operating conditions. These values will then need to be stored in the NVM for future authentication.

3.2 Task 2- Performance Evaluation of the Proposed On-chip Sensor

The system is required to be implemented using different field programmable gate array (FPGA) boards, each of which are manufactured with different technologies (28nm, 45nm, and 90nm) to evaluate the effectiveness of the proposed on-chip sensor. Our preliminary results indicate that we are able to detect recycled ICs that have been used for as little as a single day.

3.3 Task 3- Integration of the Proposed Sensor with the RFID

To reduce chip overhead, the PI plans to incorporate RFID infrastructure into the proposed method. RFID tags can store data into their memory and transmit the data when any RFID reader tries to read the content. Saving the data (d) in an RFID tag and attaching it to the chip will eliminate the need for an on-chip NVM. The PI plans to set up the RFID read/write infrastructure in his System Engineering and Security (SES) Laboratory. He also has access to the RFID Lab at Auburn University that will help prototype an RFID that is capable of performing read/write operations on the data and the digital signature for enabling traceability.

3.4 Task 4- Enabling End-to-End Trust in the Component Supply Chain

The PI proposes to implement an end-to-end security model for the global microelectronics supply chain against recycling. One of the greatest benefits of using RFID technology is that any distributor in the supply chain will be able to authenticate the chip purchased from either the manufacturer or other distributors. The user can uniquely identify the complete route of a chip in the supply chain by scanning the RFID tag. Another advantage of using RFID is that a distributor does not need to power up the chip. This is one of the major requirements of the proposed system, since a distributor may not have the necessary expertise to power up the chip to perform authentication. The PI plans to demonstrate the end-to-end protection for the fabricated chips using a commercial RFID tag.

4 DESIGN OF A ROBUST, LOW-COST, AND ACCURATE ON-CHIP SENSOR

This section presents the on-chip structure that can detect recycled ICs effectively. The core of the proposed on-chip structure is utilizing a ring oscillator and a small non-volatile memory. The on-chip structure stores the RO frequency, the measurement conditions, and a digital signature [31] in the NVM.

The proposed solution is robust as the process variations do not affect the accuracy of the authentication process. Unlike previous approaches [17-20]. No comparison is performed between different ROs to determine the usage of an IC. Our solution can detect recycled ICs accurately even if a chip was used for a very short period of time (e.g. aging due to manufacturing tests, burn-in and system tests).

Move over, the integrity of NVM content is ensured by verification through digital signatures. Any tampering with the NVM content will be detected during the signature verification process. This solution is also low-cost as the on-chip structure consists of a single RO and a small NVM. We do not require any additional overhead as ROs are commonly used in modern ICs to monitor process variation [33–35]. Note that no additional pin is required for frequency measurement as the same resource is available for process monitoring [33]. On the other hand, the measurement device only requires a counter and a timer. One can also use this resource from process monitor circuit [35] to measure the RO frequency. Finally, this solution is accurate for measuring RO frequency as the measurement error is much less than the degradation.

Figure 1 shows the structure proposed in [32] for detecting recycled ICs. It consists of an RO and an NVM. The output of the 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 [36] can be used to access the NVM content. The following information are necessary to be updated in the NVM: (*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*). *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 [37]. This *ECID* value can be accessed using *ECIDCODE* instruction defined in Std 1149.1 [36]. 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.

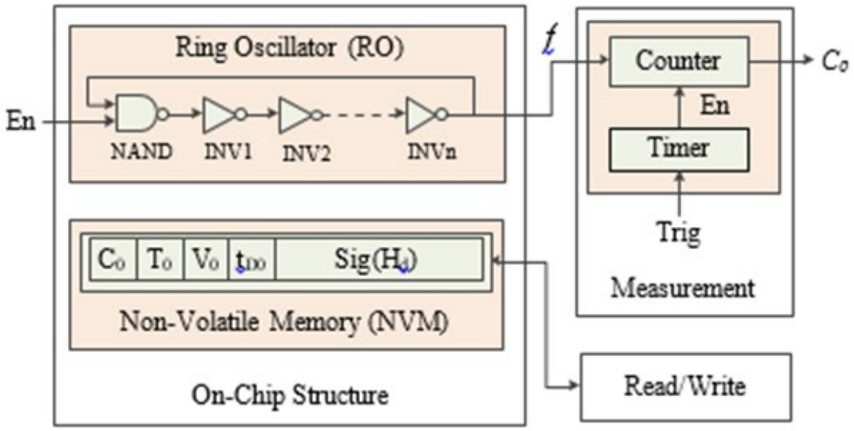


Figure 1: Prior Process Variation Resilient On-chip Structure for Detecting Recycled ICs [32]

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.

4.1 Registration Phase

The registration phase starts after the chips are manufactured and tested for defects. Only the defect-free chips can 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 based on the collected 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.

$$H_d = hash(d)$$

$$Sig(H_d) = K^-(H_d)$$

where, $hash()$, K^-, $K^-()$ represent a secure hash algorithm (SHA-2/SHA-3 [38]), private key, and the encryption function (RSA or ECC [31]), respectively.

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

4.2 Authentication Phase

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. During this phase, it is necessary to extract 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 status of the chip is determined by comparing the stored RO frequency in the meomory with the measured RO frequency performed by the end user(system integrator). 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.

Note that the authentication process consists of two distinct phases. First, a signature matching is performed in order to ensure that none of the NVM content has been modified by an adversary. Second, the current oscillator frequency is compared with the value of the registered frequency in order to identify the aging or usage of the chip.

5 PERFORMANCE EVALUATION OF THE ON-CHIP SENSOR

We have implemented an on-chip sensor to detect recycled ICs. To demonstrate the effectiveness of our on-chip sensor, we perform accelerated aging experiments on different FPGA technologies, *i.e.*, 28nm, 45nm, and 90nm, and use the sensors to verify the detection accuracy.

Figure 2 shows accelerated aging for evaluation of aging degradation. We age the FPGA using a Tempeteronic Thermospot DCP-201 system [39], which is a thermal inducing system designed to control a device's operating temperature over a wide range. The RO frequency data from the brand new FPGA boards need to be collected first. The board will then be aged for two hours at a nominal supply voltage and an elevated temperature of 85°C. Accelerated aging of two hours under the conditions mentioned above corresponds to approximately one day of in-field aging [32]. The data are collected after 2hrs, 4hrs, and 6hrs of accelerated aging, representing approximately 1, 2, and 3 days of normal usage in the field.

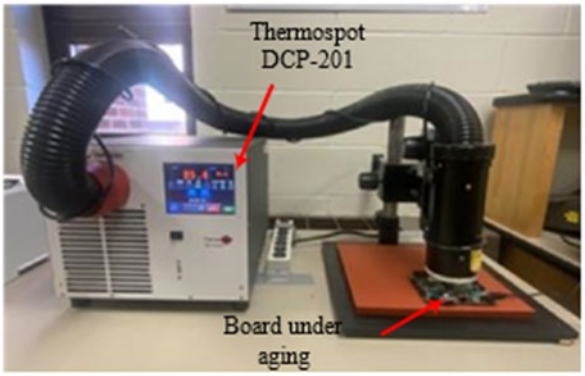


Figure 2: Experimental Setup for Accelerated Aging

A computer is required to interface with the board in order to collect the RO frequency. The tool RealTerm is used to control and monitor the UART communication and display the results transmitted from the FGPA board. A MUX-based selection is constructed in the design and reads the RO data. A 0.1-second timer is set up to capture the counter value. Figure 3 shows the setup for collecting the frequencies of different ROs implemented in 28nm, 45nm, and 90nm technology nodes. The Artix-7 FPGA (Nexys 4) shown in Figure 3(a) is fabricated in a 28nm High-Performance Low-power (HPL) process. The micro-USB port supports the UART data transmission, in addition to powering the FPGA board. ROs with four variable stages, *e.g.* 21, 31, 51, and 81 stages, are implemented to evaluate the aging performance. The RTL schematic of our RO sensor implementation and measurement is shown in Figure 4. Each type of RO setup (*i.e.*, 21, 31, 51, 81 stages) has 300 instances, with a total of 1200 ring oscillators implemented on the Artix-7 FPGA board. The data for each RO is readout serially through the UART interface. The Spartan-6 FPGAs are manufactured with a 45 nm low-power copper process (LPC) technology. Four different ROs with 3, 5, 7, and 9 inverter stages are created to evaluate the performance. An extra PmodUSBUART module is required to interface the FPGA with the PC for UART protocol. Similarly, we activate the counter for 1/10 second and then calculate the RO frequency. Figure 3(b) shows the measurement setup for Spartan-6 (CMOD S6), whereas Figure 3(c) shows the same for Spartan-3E100 (Basys 2) FPGAs.

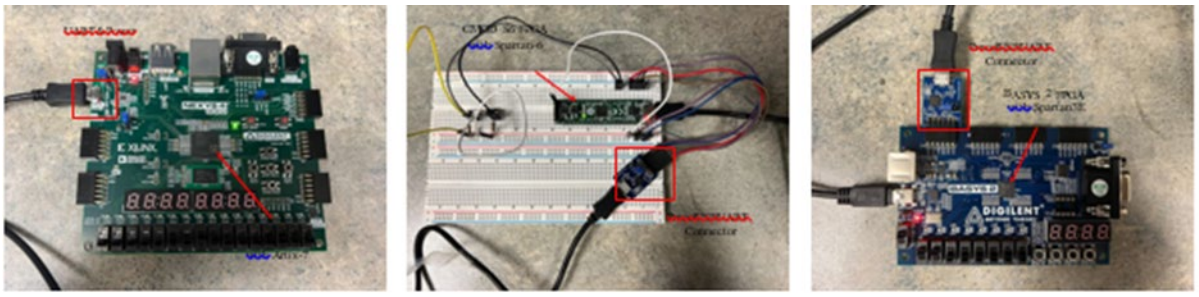


Figure 3: Setup for Measuring the Frequencies of Different ROs Implemented
Artix-7 (NEXYS 4) with 28nm HPL process [40] (a), (b) Spartan-6 (CMOD S6) with 45nm LPC technology [41], and (c) Spartan-3E100 (Basys 2) with 90nm process [42]

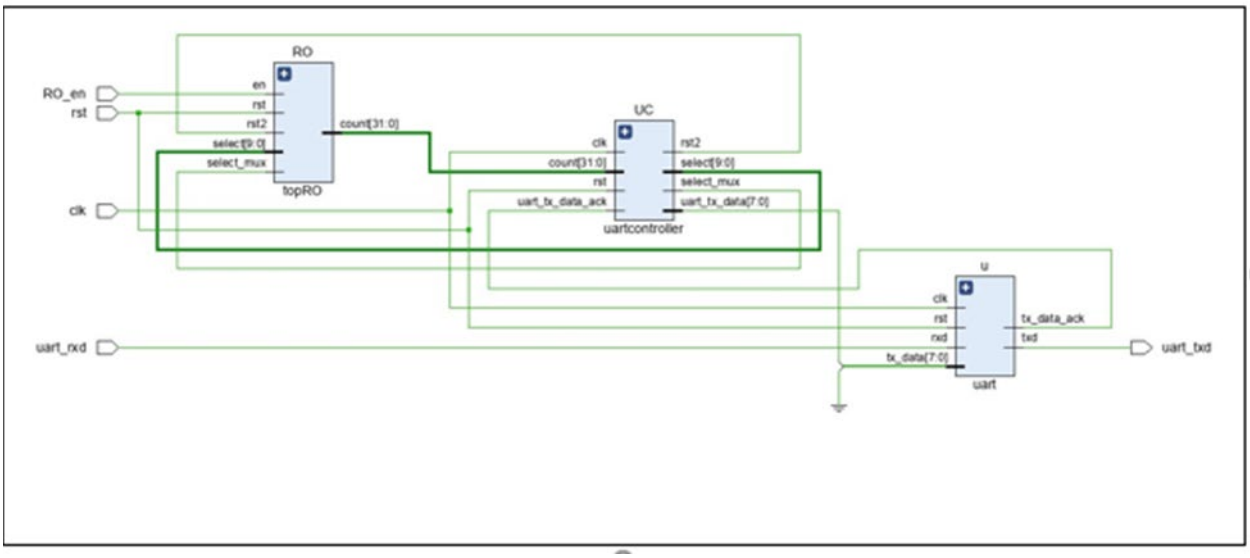


Figure 4:RTL Schematic of RO Implementation and Measurement
The top RO contains 1200 ring oscillators (for Artix-7 FGPA). The uart is used to readout all these ROs serially.

Figure 5 shows the Vivado layout of implemented design on the 28nm Artix-7 FPGA board, Figure 5 (a) shows the overall layout, and the highlighted LUTs are assigned for the implementation of multiple ROs with different stages (21, 31,51, and 81) using hard macros. Figure Figure 5 (b) illustrates the part layout. Each red box represents a 51-stage RO.

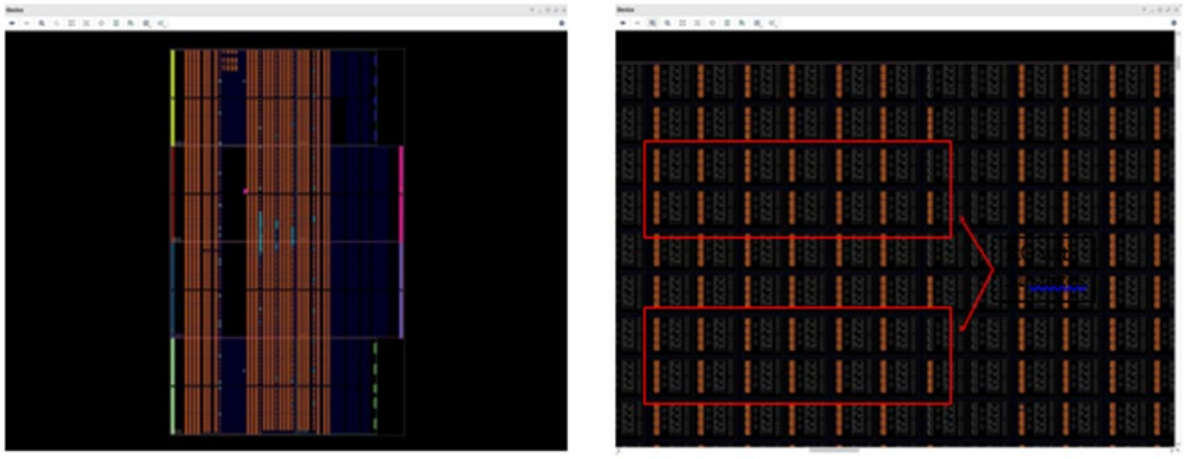


Figure 5: Implemented Design on Vivado for Artix-7 FPGA Board
Overall layout design (a) and (b) Partial with 51 stages.

The histogram of percentage degradation for RO frequencies on different chips and technology nodes is shown in Figure 6. The samples are taken from the implemented 21-stage ROs on 28nm and 3-stage ROs on 45nm and 90nm, respectively. Then, we performed accelerated aging for 2 hours, 4 hours, and 6 hours. The distributions are shown in different colors. We observe a Gaussian distribution for the percentage of degradation for these ROs on different technology processes and different chips. The mean (μ) value of the percentage (%) degradation and 3-times standard deviations 3σ are also labeled for each histogram. For example, one can observe a mean (μ) value of 0.155% with a 3σ of 0.128 for 2hrs of accelerated aging, as shown in Figure 6(a). When considering the 4 hours of accelerated aging, the average percentage degradation μ is increased to 0.203 with a 3σ of 0.095. It can be concluded from the figure that the distribution will move towards the right further when a chip has been aged more. The same trend can be observed in other technologies, *i.e.*, 45nm and 90nm in Figure 6(c)-(f), which indicates the feasibility of our proposed on-chip sensor.

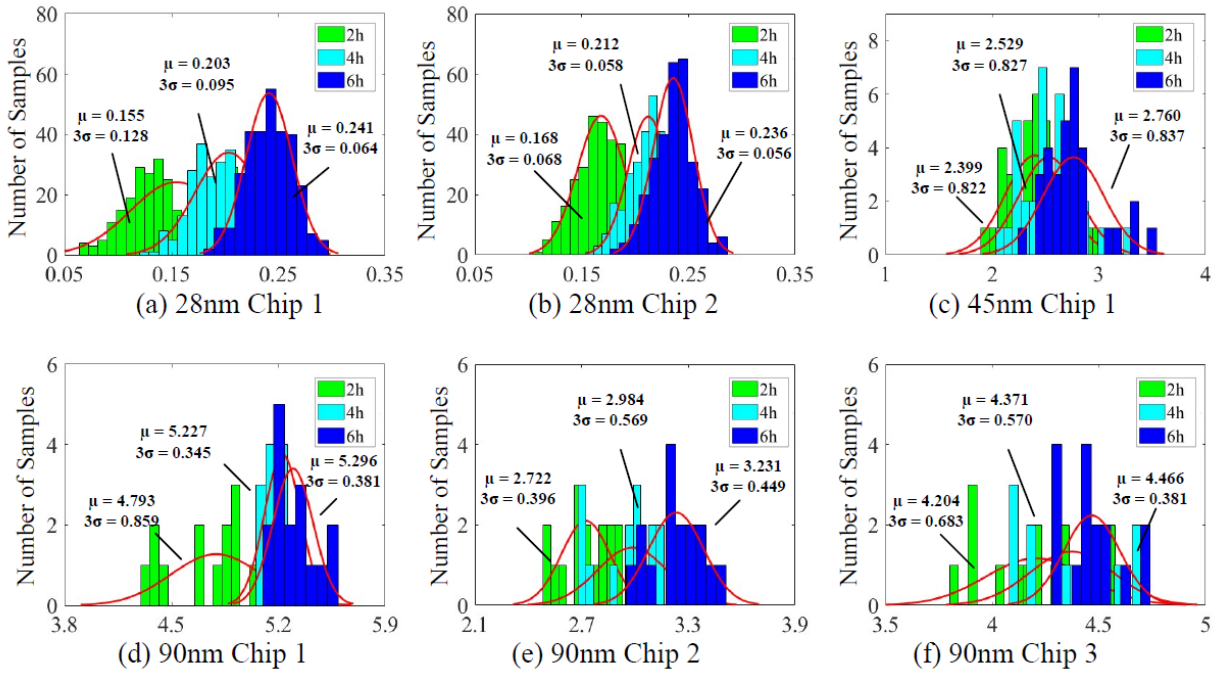


Figure 6: Percentage Degradation of RO (implemented in 28 nm, 45 nm, and 90 nm technology) Frequency under Accelerated Aging

In Table 1, we have summarized the experiment results from three different technologies. The temperature used for accelerated aging is set to a constant of 85°C. Column 1 shows the aging duration. We perform 2, 4, and 6 hours of accelerated aging for each FPGA board, which represents approximately 1 day, 2 days, and 3 days of usage in the field. Columns 2 and 7 represent the number of stages for each technology. The mean value (μ) and three times the standard deviation (3σ) are provided for each chip. The frequency percentage degradation evaluation for the 28nm HPL process is performed on two chips with 300 ROs each and shown in Columns 3-6. For example, we observe a mean value μ of 0.263 with a 3-times standard deviation value 3σ of 0.139 for 6-hour-aged 81 stages ROs. Columns 8-9 shows the results on CMOD S6 FPGA with 45nm LPC process, and each stage has 32 samples. Columns 10-15 show the experimental results on 90nm with three different boards. Even though the different boards with the different technologies may have different frequency change, we observe more degradation with the increased aging time.

Table 1. Percentage Frequency Degradation under Accelerated Aging for Different ROs Based on 28 nm, 45 nm, and 90 nm Technology

Aging Times (Hrs)	Stages	28nm				Stages	45nm		90 nm					
		Chip 1		Chip 2			Chip 1		Chip 1		Chip 2		Chip 3	
		μ	3σ	μ	3σ		μ	3σ	μ	3σ	μ	3σ	μ	3σ
2	21	0.155	0.128	0.168	0.068	3	2.399	0.822	4.793	0.859	2.722	0.396	4.204	0.683
4		0.203	0.095	0.212	0.058		2.529	0.827	5.227	0.345	2.984	0.569	4.371	0.570
6		0.241	0.064	0.236	0.056		2.760	0.837	5.296	0.381	3.231	0.449	4.466	0.381
2	31	0.155	0.095	0.170	0.061	5	2.507	1.162	4.987	0.229	2.874	0.203	4.409	0.192
4		0.210	0.066	0.219	0.054		2.617	1.145	5.157	0.241	3.210	0.202	4.537	0.191
6		0.239	0.064	0.241	0.056		2.832	1.151	5.258	0.241	3.394	0.187	4.543	0.193
2	51	0.171	0.150	0.177	0.080	7	2.539	0.952	5.012	0.192	2.914	0.154	4.411	0.168
4		0.223	0.124	0.224	0.064		2.745	0.974	5.157	0.211	3.255	0.162	4.533	0.172
6		0.255	0.136	0.248	0.068		3.136	1.181	5.266	0.201	3.426	0.152	4.534	0.174
2	81	0.158	0.107	0.185	0.125	9	2.267	1.293	5.026	0.158	2.930	0.092	4.398	0.211
4		0.226	0.105	0.233	0.065		2.479	1.283	5.167	0.152	3.272	0.099	4.516	0.199
6		0.263	0.139	0.252	0.074		2.734	1.539	5.272	0.166	3.444	0.105	4.517	0.206

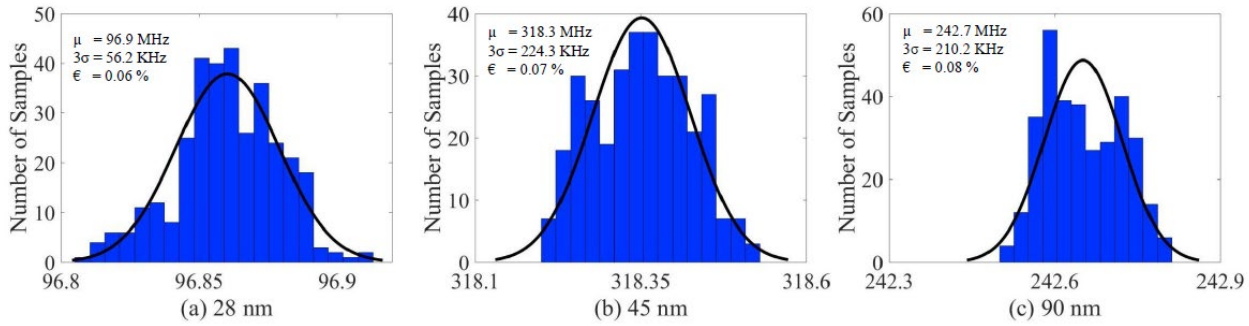


Figure 7: Measurement Error Evaluation during Frequency Measurement for Single RO Based on 28, 45and 90 nm Technology

To evaluate the measurement accuracy, we have also recorded the same RO 330 times for all different HPL processes, and the plots of measurement errors are shown in Figure 7. In Figure 7(a), we have observed a Gaussian distribution with a mean (μ) value of 96.9 MHz with a three standard deviation (3σ) of 56.2 kHz for 28 nm technology. The calculated measurement error (ε) for the first RO is 0.06%. Similar trends of distribution can also be observed on 45 and 90 nm technology, which are shown in Figure 7(b) and Figure 7(c), respectively. Note that the measurement error ε for each technology is less than 0.1% and much lower than the percentage degradation of frequency after two hours of accelerated aging, which indicates that our proposed solution can detect the recycled IC efficiently and accurately.

6 INTEGRATION OF THE PROPOSED SENSOR WITH THE RFID

The solution proposed and developed in Task 1 (and 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. It can be challenging for many distributors to adopt the solution proposed in [32], 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.

Our proposed design is shown in Figure 8, where each 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 to the 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 the traceability of chips in the supply chain. In recent years, RFID tags are widely used for traceability in the supply chain. There are two basic types of RFID tags in use: passive and active tags. Passive tags are more popular due to their 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 to 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.

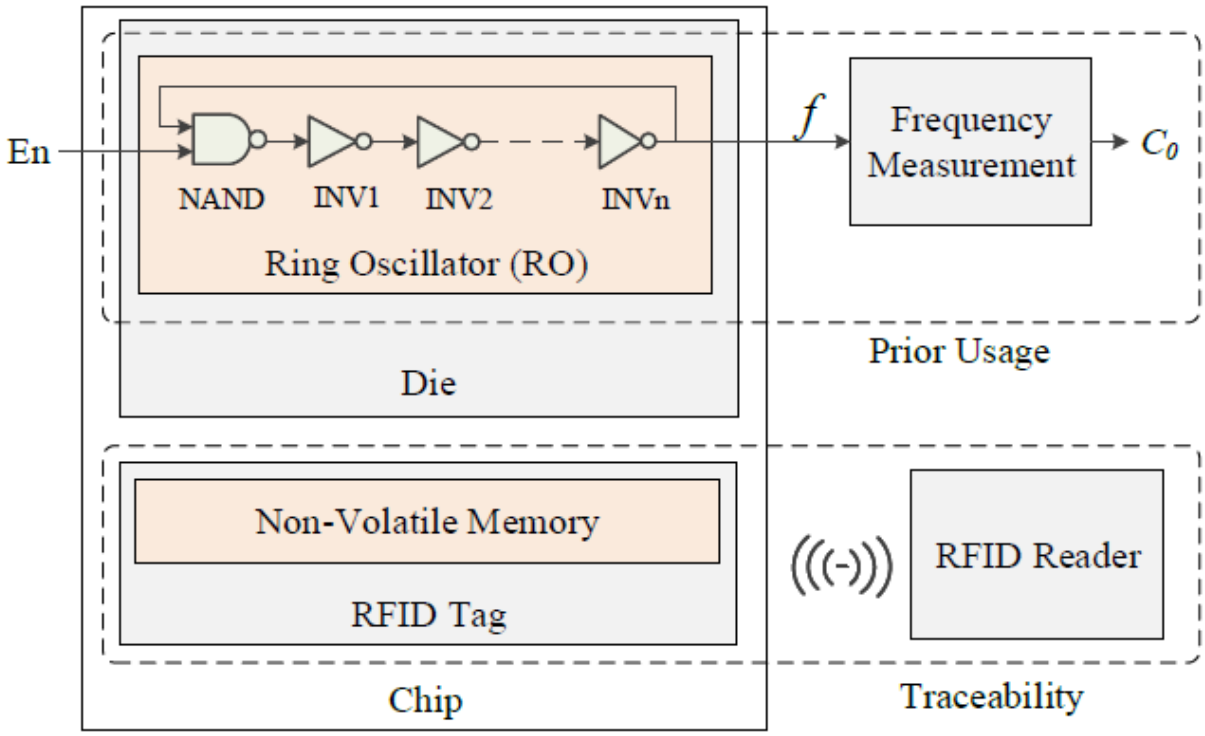


Figure 8: Proposed design for enabling traceability of ICs in the Supply Chain for combating against recycling

Figure 9(a) shows the integration of an RFID into the package of an SRAM chip. We selected a high frequency (HF) RFID tag, LXMS33HCNG-134 [43], so that a mobile phone (e.g., iPhone 12) can be used as an RFID reader. To evaluate the feasibility of integrating the tag in the chip package, we drill a small hole, place the RFID tag into it and apply adhesive. The chip remains fictional after the RFID integration. Note that this tag can easily be integrated during the packaging step of IC manufacturing. Due to the small size of the RFID tag, it can be placed in the majority of the chip packages.

Figure 9(b) shows how the read and write can be performed using an iPhone. Near Field Communication (NFC) enables devices within a few centimeters of each other to exchange information wirelessly [44]. The operating frequency of the NFC tag is the same as the HF technology, which is at 13.56 MHz. An iOS app running on the supported device (iPhone 12 in Figure 9(b)) could help the designer read/write content from/into the RFID tag. Different NFC applications from the Apple Store can be used to perform the operations. When performing a writing process, the manufacturer needs to create the initial data and calculated signatures and put them into the text box. Once the NFC area of the phone is close enough to the tag and the write button is pressed, the phone will scan the available NFC tag nearby and update the tag memory. In the case of a read operation, the NFC function can be recalled by pressing the Scan/Read button. Next, the distributor/end-user can extract the data and perform the signature verification with other tools. Since the apps in the store are only designed with NFC function support only, we are also going to design and demonstrate our application, which combines the NFC function and cryptographical computation together for enabling IC protection in the supply chain.

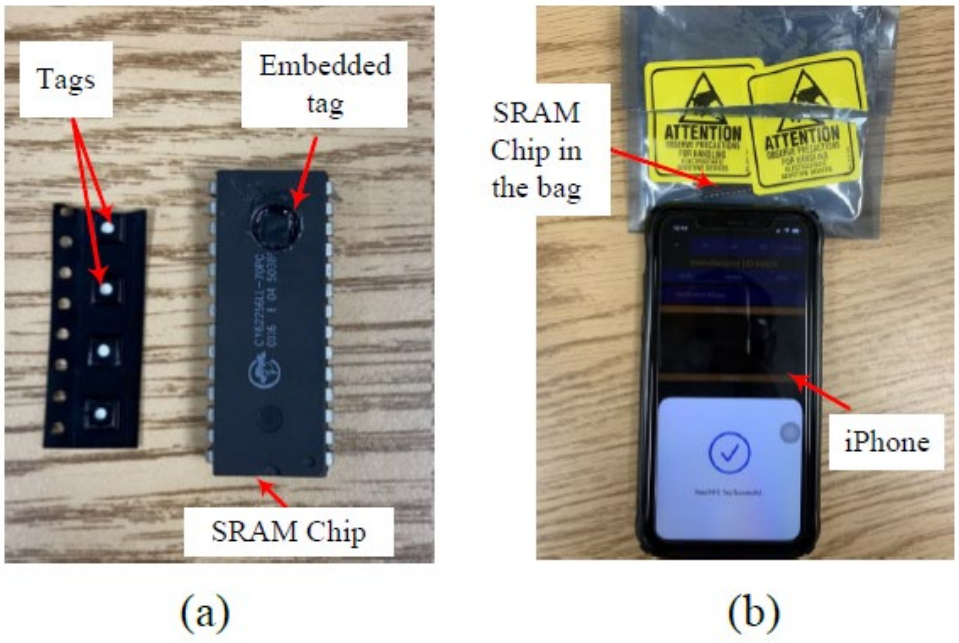


Figure 9: RFID and SRAM Chip as a Product in the Supply Chain
Left: and SRAM chip as a product in the supply chain. Left: multiple RFID tags on a rail. Right: an RFID tag is embedded into the package of the SRAM chip (b)The chip with RFID tag inside the packing can be read successfully.

7 ENABLING END-TO-END TRACEABILITY IN THE COMPONENT SUPPLY CHAIN

The traceability of a component in the supply chain can be achieved by creating a chain of trust among the manufacturer, distributors, and users. We use the concepts of the blockchain, which was introduced in the Bitcoin cryptocurrency system by Satoshi Nakamoto in 2008 [45]. Bitcoin uses a hash-based block structure, and a consensus algorithm denoted as Proof-of-Work (PoW) to achieve decentralization. A consensus algorithm is unnecessary for traceability purposes as the endpoints of the component supply chain are trusted, and chips can be considered the transactions. In the supply chain, the manufacturers of chips are treated as trusted (see General Requirements of the Standard AS6171 [6]), as there is no motivation for a manufacturer to recycle chips and send them into the market as new. In addition, the end-users of the chips are also considered trusted as they are suffered from recycled chips. Thus, our objective here is to identify a recycled (used and old) chip that enters the supply chain through untrusted distributors.

7.1 Approach for End-to-End Traceability

Figure 10 shows the solution for enabling the traceability of chips while they travel through the 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_{D1}) 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_{D1}) on H_{D1}, updates the RFID with $K_D{}^+{}_1$, Sig_{D1}, 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.

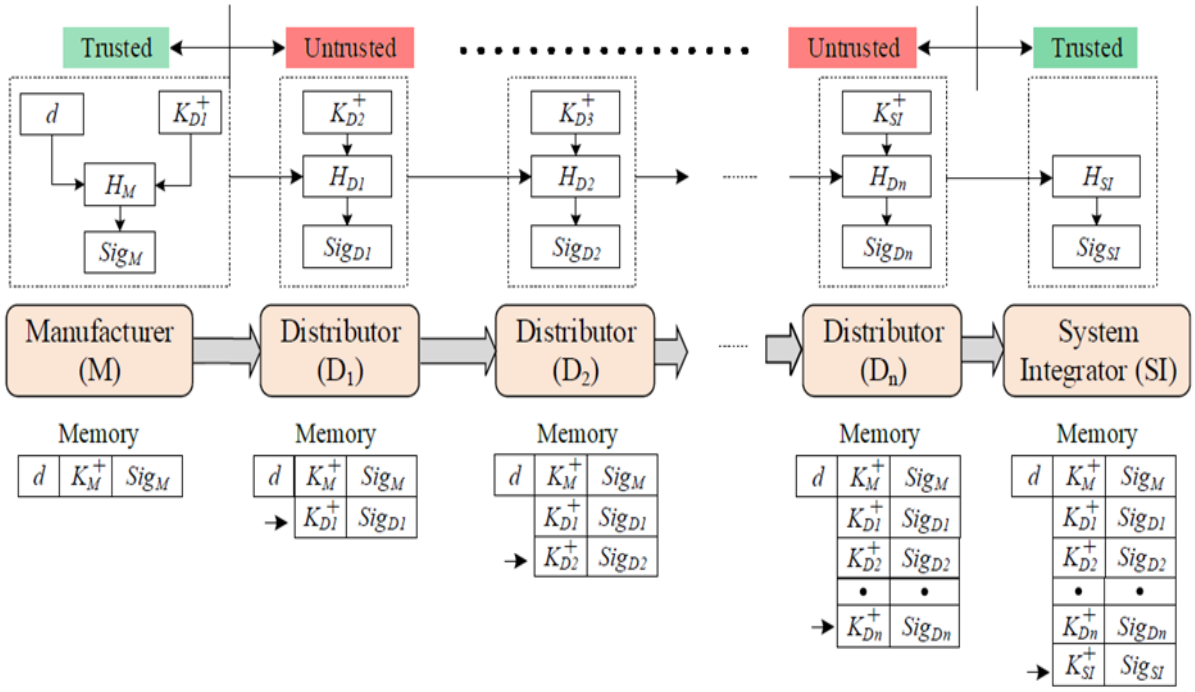


Figure 10: Proposed Flow for Enabling Traceability of ICs in Electronic Component Supply Chain

Figure 11 shows the approach for enabling traceability in the supply chain. It 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 the RFID content.

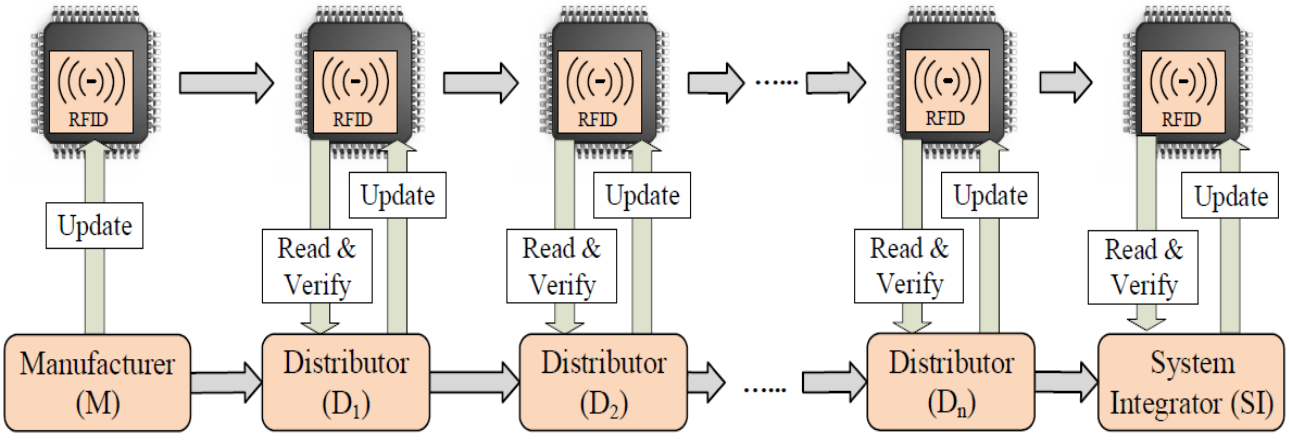


Figure 11: Verification and Update Process for the Contents of an RFID Tag Placed in the Package of a Chip

7.1.1 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.

7.1.2 Verify RFID Content:

The distributor needs to perform signature verification for all prior stages starting from the manufacturer. 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 [38]). 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 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 indicate 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 (e.g., 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*).

7.1.3 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_{D^+1}).

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

- 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.

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

- 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.

7.2 Final Verification for Detecting Recycled ICs:

This proposed solution enables a chain of trust among manufacturers, distributors, and system integrators. As a result, 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 12 shows the final 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 with the same experimental parameters. If a mismatch of RO frequency over measurement error is detected, it indicates that the IC under test is recycled, otherwise, it is brand new. Note that this operation will only be performed at the end-user side since the distributor may not have the proper test infrastructure. In the case of a successful brand new qualification, the system integrator is also required to update their own information into the RFID tag memory. Thus, the entire protection of IC in the supply chain from manufacturer to system integrator is achieved.

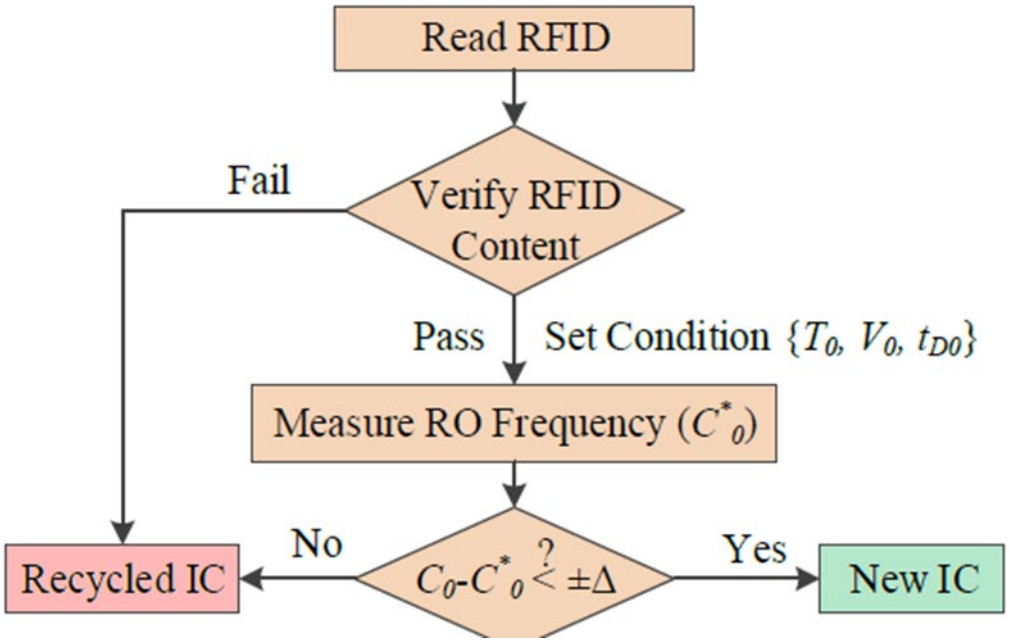


Figure 12: Final Verification Flow for Detecting Recycled ICs

7.3 Prototype for Supply Chain Protection

The need to develop an authentication app that can seamlessly integrate with a low-cost and hand-held device can enable both distributors and end-users to verify the authenticity of ICs, which is crucial for supply chain provenance. We implemented our supply chain traceability solution on multiple platforms. We created one application in the *Windows* platform so that a permanent measurement platform can be developed for large-scale IC testing. We also developed one for the platform so that an individual at the testing facility can authenticate ICs using a commercial mobile phone (e.g., iPhone). Both implementations support the function of *read*, *verify* and *update* the entity-specific data on the commercial RFID tags. Thus, an entity in the supply chain can verify all data stored in the passive RFID tag written by the manufacturer and prior distributors, thus the complete route of a chip in the supply chain.

7.3.1 Windows Application for supply chain protection:

In order to implement this technique efficiently at a large scale it is critical to be able to make use of high speed RFID readers. In order to show that this can be done we have developed a windows application that can pair with a high speed RFID reader and perform all necessary operations for reading from the RFID tags, verifying that the contents of the tags is correct, and writing updated data back to the tag. This app can be used by the manufacturer, distributors, and the end-user.

The prototype verification system with our Windows application is shown in Figure 13.
In addition to the Windows interface, an ultra-high frequency (UHF) RFID reader gun (Zebra RFD8500) is used to read data from an RFID tag. The reader gun can read and write data on a commercial UHF RFID tag. The RFID tags used are attached to ICs such as those that this technique aims to help protect. The RFID reader gun will be used to read the data from the RFID

tag to the windows app where the data will be verified and updated and then the reader gun will be used again to write the updated information from the windows app to the RFID tag. This process is repeated several times from the perspective of sequential members of the supply chain in order to simulate the full path of an IC through the supply chain from the manufacturer to the end-user.

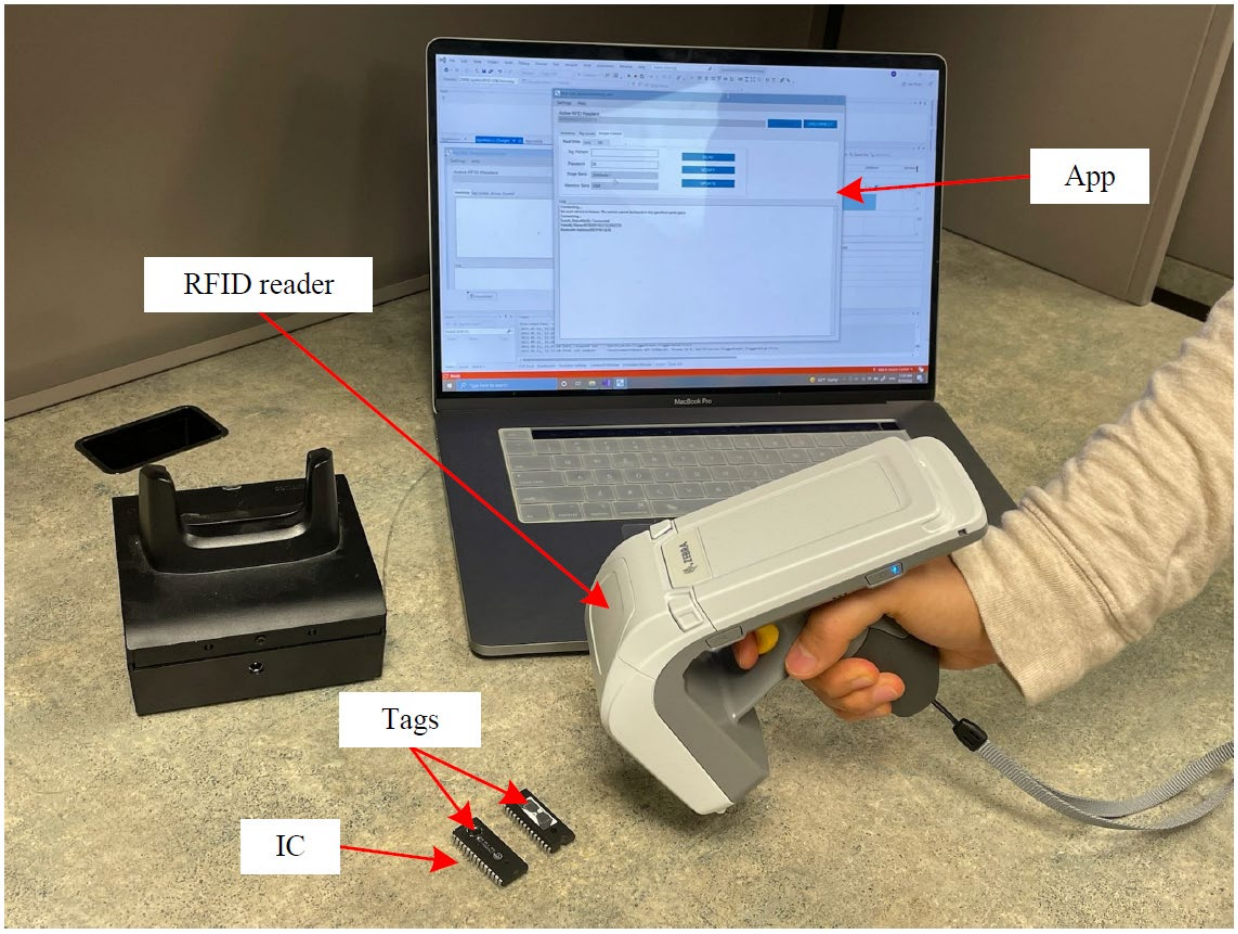


Figure 13: Experimental Setup for End to End Authentication with Windows Application

We have developed an in-house user interface (GUI) to enable end-to-end traceability described in Figures 10-11. Figure 14 shows the different interfacing buttons and a drop-down list for stage selection.

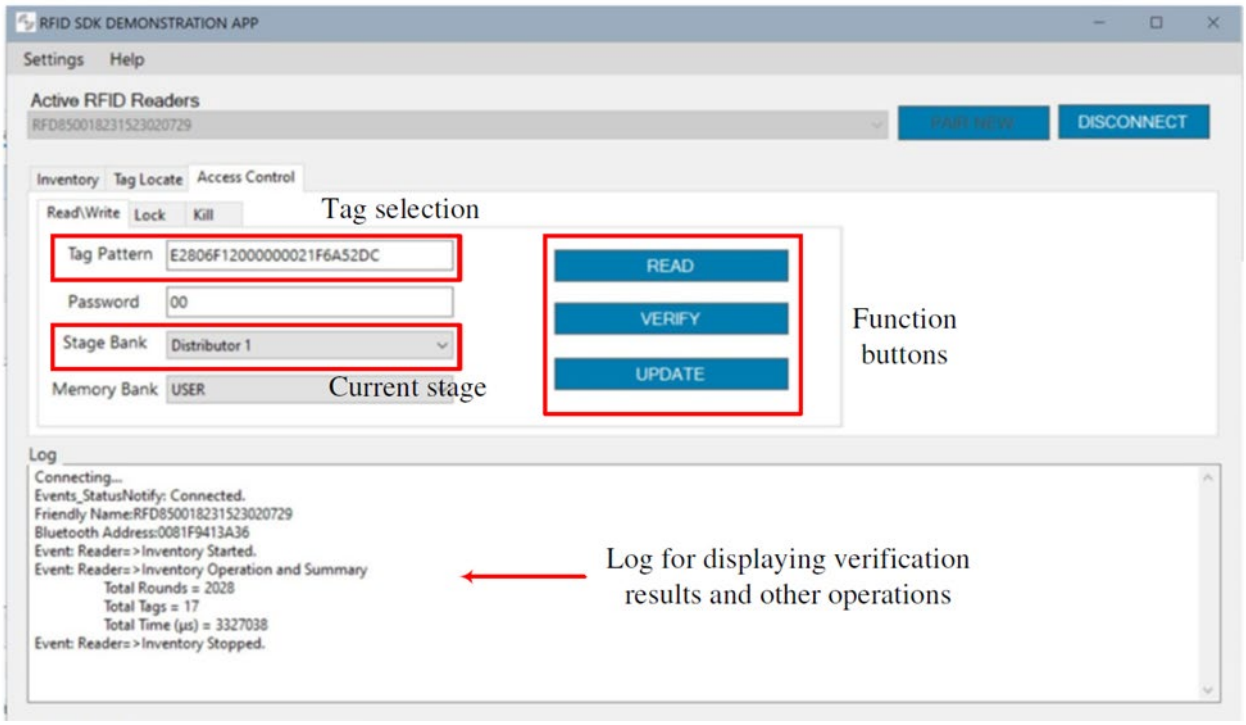
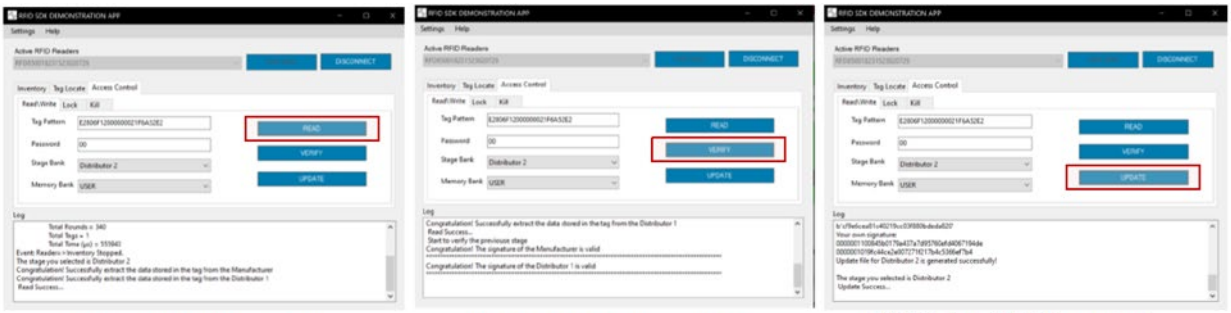


Figure 14: Layout Design for Windows Application

Depending on the different stages in the supply chain, one can configure the app as either "Manufacturer","Distributor", or "End User". The computer can be treated like a wallet with unique public-private key pair, where the private key will never leave the system. The authorized personnel with proper login credentials can use this platform to authenticate chips and upload signatures in the RFID tag. The GUI includes buttons in the top right corner for pairing a new RFID reader with the application and for disconnecting the currently paired reader. There are three function buttons in the GUI: "*read*", "*verify*", and "*update*." The read button is used to read the data from the RFID tag, the verify function is used to verify the signatures of all previous entities in the supply chain where the chip traveled, and the update button is used to update the RFID tag with the signature of current entity (e.g., i^{th} distributor). As the supply chain entity needs to perform "read", "verify", and "update" on every the chip within the same batch, the entity selects the tag on the target chip using the "tag pattern" box to avoid the reader gun inadvertently picking the wrong RFID signal. The log window displays the possible content stored in the RFID tag along with the appropriate "read", "verify", and "update" status results.

Let us consider Distributor 2, D_2, as an example. When it receives a shipment of ICs, each chip is authenticated individually. The "read", "verify", and "update" operations performed by D_2 on a single chip is shown in Figure 15. First, D_2 readout the content already stored in the tag, that is data d, the public keys and digital signatures for both Manufacturer (M) and D_1, as shown in Figure 15(a). Second, it verifies whether the digital signatures from both M and D_1 are valid or not, as shown in Figure 15(b). If verification is successful, it means that all signatures are computed correctly and the RFID content has not been tampered with. D_2 then knows that the chip is authentic and can proceed with the last step by updating its own public key and the corresponding digital signature into the RFID memory, as depicted in Figure 15(c). If the stored

digital signatures from either M or D_1 do not match with the computed value, D_2 knows that the chip must be counterfeit and there is no need to save its own information into the RFID tag.



(a) Read RFID content. (b) Verify RFID content. (c) Update RFID content.

Figure 15: Read, Verify and Update Operations are performed on RFID Tag

7.3.2 iOS Application for Supply Chain Provenance:

We have also designed the end-to-end supply chain traceability app on *iOS*. For the demonstration purpose, we have implemented one manufacturer, three distributors, and an end-user on the same phone. Note that when this app will be deployed, one needs to create a wallet with unique public-private key pairs. While registering, the entity (manufacturer, distributor, or end-user) needs to create an account (like any other app) so that the appropriate functions can be enabled. We did not include this feature as it is out of the scope of this project.

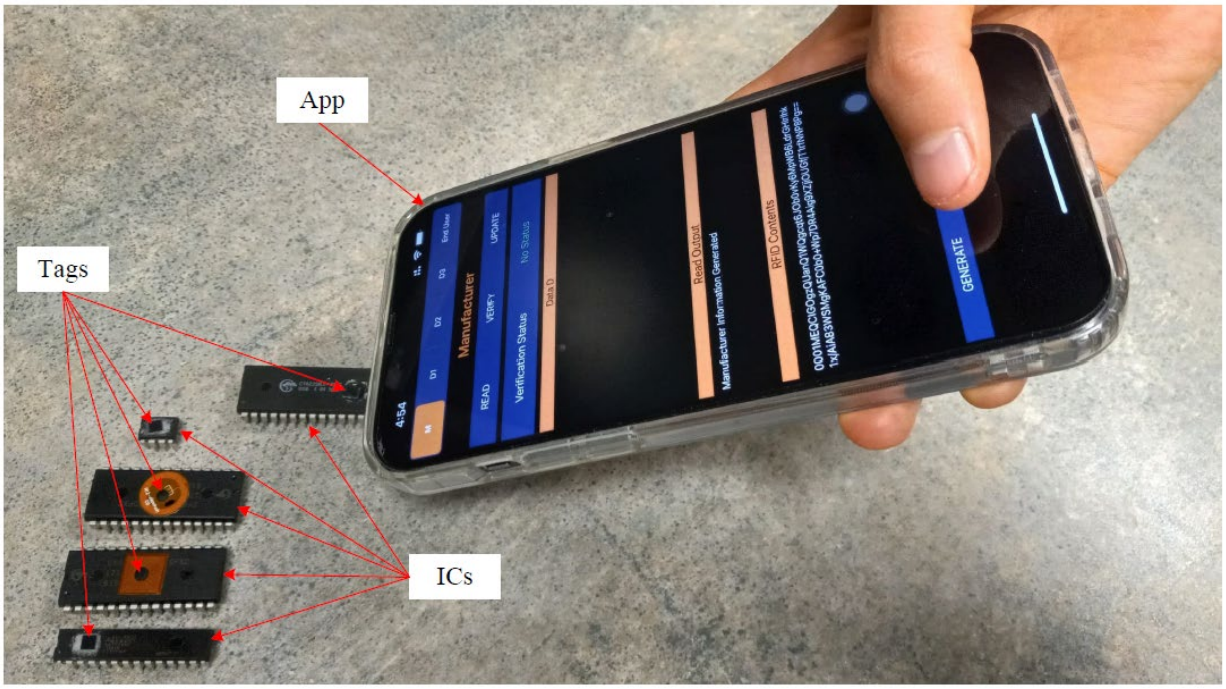


Figure 16: Experiemtnal Setup for End-to-End Authentication with iOS Application

Like the Windows application, the same “read”, “verify”, and “update” functions are implemented. Any entity in the supply chain (with proper authorization) can read, verify, and update the RFID tag memory. All three operations are performed by simply using a commercial iPhone.

The demonstration setup with our iOS application is shown in Figure 16. As the current mobile devices are NFC-enabled, one only needs to install the app on the phone without the need for any external RFID reader. An authorized entity in the supply chain can perform “read”, “verify”, and “update” functions for the on-chip RFID tag when it is within the read/write distance from the mobile device.

The layout of our developed *iOS* app is shown in Figure 17. The top row indicates the possible supply chain entities, where M denotes the Manufacturer, D_1, D_2, and D_3 are the three Distributors, and the End-User is the last entity in the supply chain. It supports the same functions “read”, “verify”, and “update” as in the Windows application. The verification status bar displays whether or not the data already stored in the tag memory is valid. The status can be either three of the following: (*i*) “No Status” is the default status before an entity presses the “verify” button; (*ii*) “Pass” if the verification is successful; or (*iii*) “Failed” if one or more mismatch is found between the computed signatures and stored valued during the signature verification. The complete content in the RFID tag is shown in the “Read Data” section once the “read” function is invoked. For the Manufacturer, it can input the measured ring-oscillator frequency, its associated parameters, and ECID under the “Data D” box. But, for other entities, the “Data D” cannot be modified. Once all the signatures of prior stages have been verified with the status “PASS”, the entity can press the “Generate” button to append its own public key along with its corresponding digital signature, where the public-private key pair is entity-specific and stored in the mobile device. Both public key and signature are displayed in the “RFID Content” box. Once the entity presses the “update” button, the new data is saved to the tag. A pop-up window will show “Write NFC Successfully” to confirm that the desired data is stored in the RFID tag.

When the chips are delivered to Distributor 1 (D_1), it first needs to verify the RFID tag’s memory contents before updating its own stage ID and signature. Figure 18(a) shows a successful read from D_1. Once the tag is successfully read, the entire data stored in the RFID tag memory will be shown in the bottom text box. It can be verified that in our demonstration, extracted data is identical to the stored data provided by the Manufacturer. Figure 18(b) shows the verification status when clicking the Verify button. A “PASS” means that the initial data, stage ID, and signature computed by the manufacturer are valid and authentic. After that, D_1 can generate the updated information by simply pressing the “generate” then “update” buttons, as shown in Figure 18(c), where information will be written into the RFID tag through the NFC function. Thus, a complete group of operations from D_1 is executed successfully. Similarly, Distributor 2 (D_2) and Distributor 3 (D_3) perform identical steps of transactions. After distributor 3 updates the RFID tag, the chip will be sent to the end-user for final verification. The end-user will validate all the previous signatures first. Then, a final IC verification will be performed to identify whether the chip is brand new or recycled, as illustrated in Figure 12. The chip is considered genuine and ready for deployment once the RO measurement agrees with the value saved in the tag.

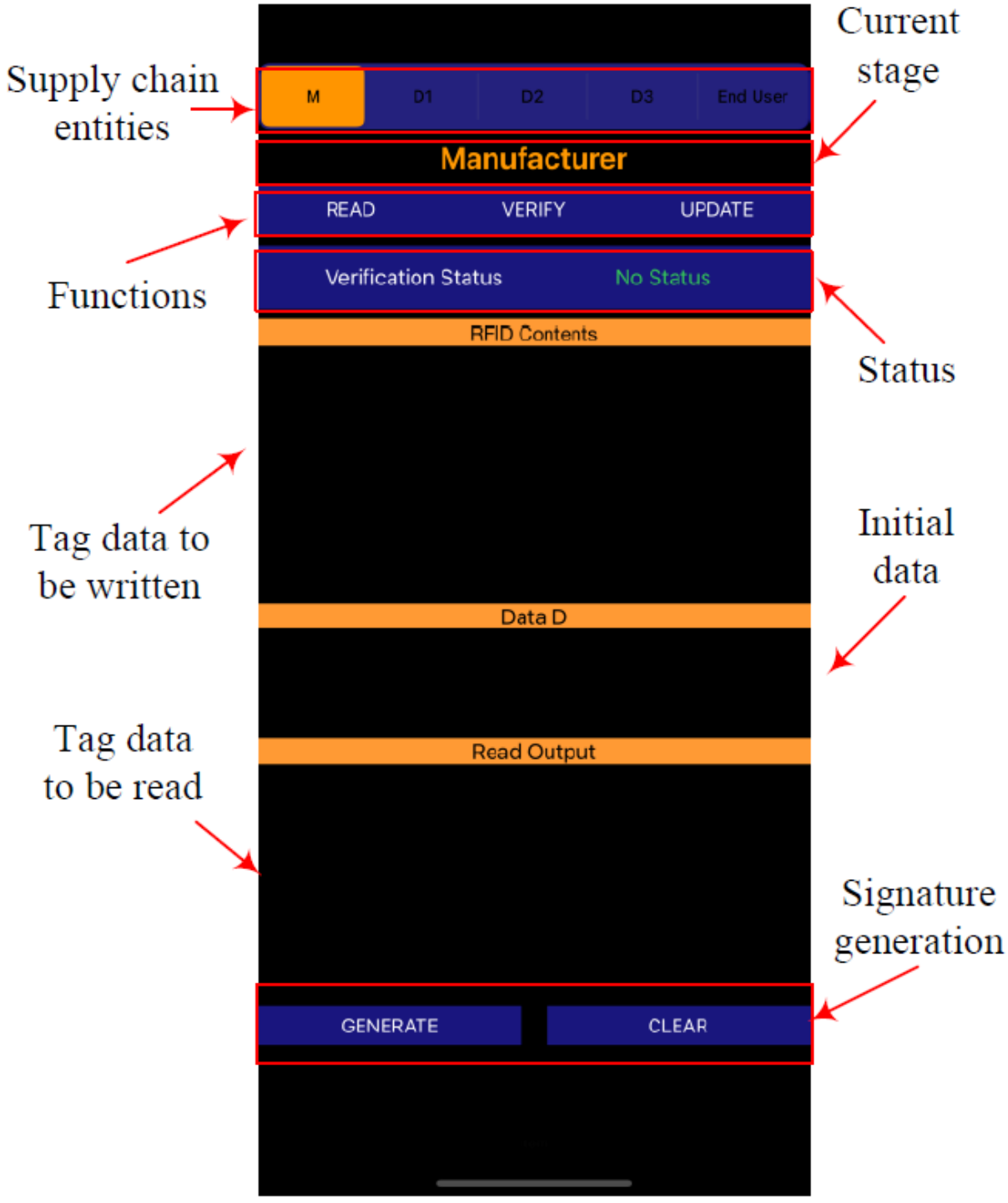
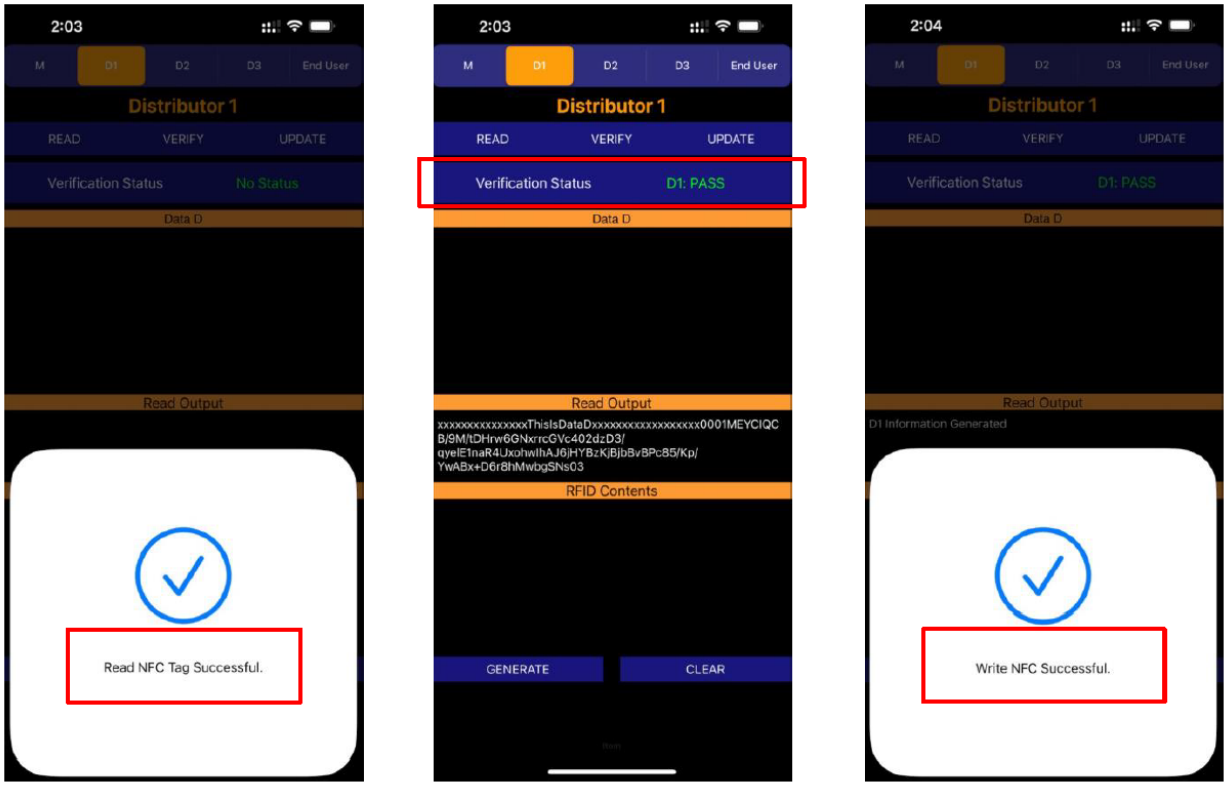


Figure 17: Application Layout Overview



(a) Read RFID content (b) Verify RFID content (c) Update RFID content

Figure 18: Read, Verify and Update Operations Performed by Distributor 1

8 SECURITY ANALYSIS

In this section, we present different scenarios where our proposed solution is under attack. Under the adversarial settings, it is possible for attackers to maliciously alter the contents stored in the RFID tag, masquerade as an authentic distributor, clone tag data from new chips to recycled ones, or tamper with the on-chip sensors, *etc*. The robustness of our proposed architecture under these attacks is thoroughly assessed.

8.1 Tampering with the RFID Content

In this attack, an adversary is going to use a commercial RFID reader to tamper with the RFID content. 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 a few distributors.

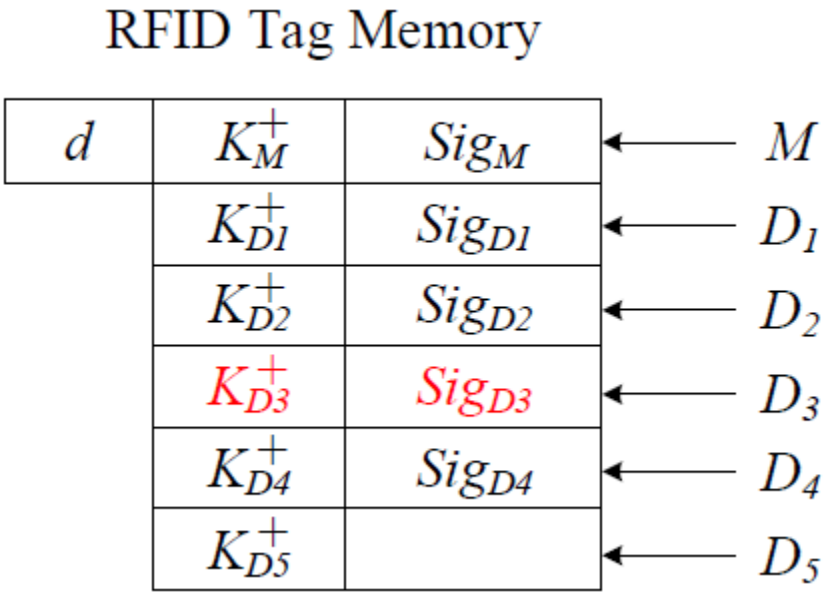


Figure 19: Tampering with RFID Content to Modify Trace

For example, an adversary (D_4) removes the 4^{th} entry (i.e., public key and signature from D_3) of the RFID tag memory, and then sell the chip to D_5. Figure 19 shows an example of the removal 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.

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, 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: • *Step-1:* D_5 reads the entire memory, constructs data for each stages, and then compute the hashes.

$d_M = \{d\}$, $H_M = hash^{(d_M||K_{D_1}^+)}$
$d_{D1} = \{H_M||Sig_M\}$, $H_{D1} = hash^{(d_{D1}||K_{D2}^+)} d_{D2} = \{H_{D1}||Sig_{D1}\}$, $H_{D2} = hash^{(d_{D2}||K_{D4}^+)}$

- *Step-2:* It recovers the hashes from the signatures.

$$H_M^* = K_M^+(Sig_M);$$
$$H_{D1}^* = K_{D+1}(Sig_{D1}); H_{D2}^* = K_{D+2}(Sig_{D2}).$$

- *Step-3:* Finally, it performs signature verification.

$$ver(H_M, H_M^*) = pass; ver(H_{D1}, H_{D1}^*) = pass; ver(H_{D2}, H_{D2}^*) = fail,$$

since

$$H_{D2}^* = hash(H_{D1}||Sig_{D^1}||K_{D3}^+) \neq H_{D2} = hash(H_{D1}||Sig_{D^1}||K_{D4}^+);$$

where the *ver*() function can be described as follows:

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

8.2 Impersonation of a Distributor

In this attack, an untrusted distributor (D_j) tries 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.

8.3 Dictionary Attack

In this attack scenario, an illegal recycler (untrusted distributor) constructs a dictionary of RO frequencies from fresh new chips. Each entry of the dictionary consists of the data (d), the 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 (SigM). 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 8.1).

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

8.4 Tampering the Ring oscillator

For this attack scenario, an attacker tampers with 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 [46]. To perform this attack, the chip needs to be decapsulated to remove the old package and then perform the edit. After the modification, the chip needs to be repackaged and remarked to its original specification. Note that this attack needs to be performed on 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.

8.5 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 at the registration phase has limited financial motivation for foundries.

8.6 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) by modifying the 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.

9 LIST OF PUBLICATIONS

The following work and papers are published during the implementation of this project:

1. Y. Zhang and U. Guin, “End-to-End Traceability of ICs in Component Supply Chain for Fighting Against Recycling,” Transactions on Information Forensics & Security (TIFS), pp. 767-775, 2019.
2. A. Jain, M. T. Rahman and U. Guin, “ATPG-Guided Fault Injection Attacks on Logic Locking,” in IEEE Physical Assurance and Inspection of Electronics (PAINE), pp. 1-6, 2020.
3. A. Jain, and U. Guin, ”A Novel Tampering Attack on AES Cores with Hardware Trojans,” in ITC-Asia, pp. 77-82, 2020.
4. A. Jain, Z. Zhou and U. Guin, ”TAAL: Tampering Attack on Any Key-based Logic Locked Circuits,” in ACM Transactions on Design Automation of Electronic Systems (TODAES), pp. 1-22, 2021.
5. A. Jain, Z. Zhou, and U. Guin, ”Survey of Recent Developments for Hardware Trojan Detection,” in IEEE International Symposium on Circuits & Systems (ISCAS), pp. 1-5, 2021.
6. Y. Zhang, C. Tang, P. Li, and U. Guin ,“CamSkyGate: Camouflaged Skyrmion Gates for Protecting ICs,” in Design Automation Conference (DAC), pp. 1-6, 2022.

10 STUDENTS SUPPORTED

- Graduate Students
  1. Yuqiao Zhang, PhD
  2. Ayush Jain, MS
  3. Austin Walthall, MS
  4. Caleb McCarley, MS
- Undergraduate Students
  1. Paschal Onyeka, BS
  2. Craig Manes, BS

11 FUND

The summary of the project spending is given below:

287,854	Beginning Total
265,671	Bal end of May 2019
22,183	Total Spent Q1
227,614	Balance end of Aug 2019
38,057	Total Spent Q2
207,406	Balance end of Nov 2019
20,208	Total Spent Q3
179,263	Balance end of Feb 2020
28,143	Total Spent Q4
149,759	Balance end of May 2020
29,504	Total Spent Q5
112,877	Balance end of Aug 2020
36,882	Total Spent Q6
103,997	Balance end of Nov 2020
8,880	Total Spent Q7
90,035	Balance end of Feb 2021
13,962	Total Spent Q8
66,280	Balance end of May 2021
23,755	Total Spent Q9
42,426	Balance end of Aug 2021
23,854	Total Spent Q10
34,419	Balance end of Nov 2021
8,007	Total Spent Q11
27,883	Balance end of Feb 2022
6,536	Total Spent Q12

12 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] B. Hughitt, "Counterfeit Electronic Parts," *NEPP Electronics Technology Workshop*, June 2010.

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

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

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

[8] CTI, "Certification for Counterfeit Components Avoidance Program," 2011, http://www.ctius.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] U. Guin, D. DiMase, and M. Tehranipoor, "A Comprehensive Framework for Counterfeit Defect Coverage Analysis and Detection Assessment," *Journal of Electronic Testing*, vol. 30, no. 1, pp. 25–40, 2014.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[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] E. Karl, P. Singh, D. Blaauw, and D. Sylvester, "Compact in-situ sensors for monitoring negative-biastemperature-instability effect and oxide degradation," in *Solid-State Circuits Conference, 2008. ISSCC 2008. Digest of Technical Papers. IEEE International*, pp. 410–623, Feb 2008.
[23] T.-H. Kim, R. Persaud, and C. Kim, "Silicon odometer: An on-chip reliability monitor for measuring frequency degradation of digital circuits," *Solid-State Circuits, IEEE Journal of*, vol. 43, no. 4, pp. 874–880, April 2008.
[24] J. Keane, X. Wang, D. Persaud, and C. Kim, "An all-in-one silicon odometer for separately monitoring hci, bti, and tddb," *Solid-State Circuits, IEEE Journal of*, vol. 45, no. 4, pp. 817–829, April 2010.
[25] J. Keane, W. Zhang, and C. Kim, "An array-based odometer system for statistically significant circuit aging characterization," *Solid-State Circuits, IEEE Journal of*, vol. 46, no. 10, pp. 2374–2385, Oct 2011.
[26] K. Hofmann, H. Reisinger, K. Ermisch, C. Schlunder, W. Gustin, T. Pompl, G. Georgakos, K. Arnim,
J. Hatsch, T. Kodytek, T. Baumann, and C. Pacha, "Highly accurate product-level aging monitoring in 40nm cmos," in *VLSI Technology (VLSIT), 2010 Symposium on*, pp. 27–28, June 2010.
[27] E. Saneyoshi, K. Nose, and M. Mizuno, "A precise-tracking nbti-degradation monitor independent of nbti recovery effect," in *Solid-State Circuits Conference Digest of Technical Papers (ISSCC), 2010 IEEE International*, pp. 192–193, Feb 2010.
[28] 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.
[29] U.S. Defense Logistics Agency, "Dna authentication marking on items in fsc 5962," August 2012. [Online]. Available:
https://www.dibbs.bsm.dla.mil/notices/msgdspl.aspx?msgid=685
[30] Semiconductor Industry Association (SIA), "Public Comments - DNA Authentication Marking on Items in FSC5962," 2012.

[31] Elaine Barker,"FIPS 186-4: Digital Signature Standard (DSS)," 2013, https://csrc.nist.gov/publications/detail/fips/186/4/final.
[32] 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.
[33] T.-K. Lee, "Process monitor for CMOS integrated circuits," Jan. 23 1996, US Patent 5,486,786.
[34] E. O. Sugasawara, "Process monitor circuitry for integrated circuits," 2000, US Patent 6,124,143.
[35] R. Bach, "Process monitor with statistically selected ring oscillator," 2003, US Patent 6,544,807.
[36] IEEE 1149.1-2013 - IEEE Standard for Test Access Port and Boundary-Scan Architecture, https://standards.ieee.org/standard/1149 1-2013.html.
[37] Bill Eklow, "ECID vs Device ID," 2006, btw.tttc-events.org/material/BTW10/Presentations/Session%205.2.pptx.
[38] National Institute of Standards and Technology, "FIPS 180-4: Secure Hash Standard (SHS)," 2015, https://csrc.nist.gov/publications/detail/fips/180/4/final.
[39] Temptronic ThermoSpot DCP-201 Bench Top Temperature Forcing System, https://www.intestthermal.com/temptronic/thermospot.
[40] 7 Series FPGAs Data Sheet: Overview (DS180), Xilinx, https://docs.xilinx.com/v/u/en-US/ds180 7Series Overview.
[41] Spartan-6 Family Overview (DS160), Xilinx, https://docs.xilinx.com/v/u/en-US/ds160.
[42] Spartan-3E FPGA Family Data Sheet (DS312), Xilinx, https://docs.xilinx.com/v/u/en-US/ds312.
[43] LXMS33HCNG-134 Datasheet, muRata, https://www.murata.com/-/media/webrenewal/products/rfid/rfid/pdf/lxms33hcng-134-datasheet-200803.ashx.
[44] Near Field Communication, https://developer.apple.com/design/human-interface-guidelines/ios/userinteraction/near-field-communication/.
[45] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," http://bitcoin.org/bitcoin.pdf," 2008.
[46] 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.

LIST OF SYMBOLS, ABBREVIATION, AND ACRONYMS

ACRONYM	DESCRIPTION
DNA	Deoxyribonucleic Acid
ECID	Electronic Chip ID
FPGA	Field Programmable Gate Arrays
HF	High Frequency
HPL	High-Performance Low-power
ICs	Integrated Circuits
LPC	Low-Power Copper
NBTI	Negative-Bias Temperature Instability
NVM	Non-Volatile Memory
OCM	Original Component Manufacturer
PCBs	Printed Circuits Boards
RFID	Radio Frequency Identification
RO	Ring Oscillator
SES	System Engineering and Security
SVM	Support Vector Machine
TDDB	Time-Dependent dielectric
UART	Universal Asynchronous Receiver-Transmitter