An RFID-based Technology for Electronic Component and System Counterfeit Detection and Traceability

Kun Yang, Domenic Forte, and Mohammad (Mark) Tehranipoor

ECE Dept., University of Connecticut
{kuy12001, forte, tehrani}@engr.uconn.edu

Abstract*—*The vulnerabilities in the supply chain have raised serious concerns about the security and trustworthiness of electronic components and systems. Testing for device provenance, detection of counterfeit integrated circuits/systems, and traceability mechanisms are challenging issues to address. In this paper, we develop a novel RFID-based system suitable for electronic component and system counterfeit detection and system traceability called CST. Different types of on-chip sensors and in-system structures can be connected to the CST system to provide the information needed to detect multiple counterfeit types (recycled, cloned, etc.) and to verify the authenticity of the system with some degree of confidence. Board- and chip-related information can be updated periodically on the chip and safely stored to reflect the latest hardware conditions such as the increment of chip usage time. An essential part of this system is an RFID tag employed as storage and a channel to read the information from different types of chips on the printed circuit board (PCB) in both power-off and power-on scenarios. Chip-level counterfeiting, board-level counterfeiting and board identification/tracking are supported by CST. Simulations and experimental results using Spartan 3E FPGAs demonstrate the effectiveness of this system.

I. Introduction

Today's electronic components and systems supply chain suffer from counterfeiting and lack of traceability. Counterfeiting of electronic components and systems have become more economical in recent years. More than twelve million counterfeit parts were reported from 2007 to 2012 [1], and this number is on the rise [2]. An electronic component is defined as counterfeit if its performance, provenance, age, etc. are misrepresented by the vendor, manufacturer, or distributor. Another issue is that for larger systems, integrated circuits (ICs) and subassemblies pass through many hands on multiple continents before they are ultimately installed in their final application [3]. Without proper traceability, such components could be subjected to tampering, theft, and counterfeiting. Traceability can provide device identification/tracking as it moves from one entity to another in the supply chain.

Typically an electronic device will go through a process as shown in Figure 1. Vulnerabilities are associated with each step in the supply chain. At the component level, a chip can be cloned, tampered, overproduced, etc. [4] [5] [6] [7]. At the board and system levels, similar exploitations have also been observed [8] [9] [10] [11]. Among the ones shown in Figure 1, those vulnerabilities that can be addressed by our proposed approach are highlighted with underline.

Among the various vulnerabilities, in this paper, we focus on detection of counterfeit ICs, tampered boards and their traceability. In general, counterfeit parts can be divided into the following categories: (i) lower grade parts that are "remarked" as higher grade parts; (ii) defective parts that should have been discarded or destroyed by original component manufacturers (OCMs), original equipment manufacturers (OEMs) or distributors; (iii) recycled (used) parts sold as new parts; (iv) overproduced parts generated beyond scope of the contract by foundry or assembly; (v) parts cloned using reverse engineering and intellectual property (IP) piracy; (vi) tampered parts including malicious alterations. Here, we refer to boards with unauthorized substitution of chips as tampered boards.

Since counterfeits normally do not meet the requirements of specific application risks, their inclusion could jeopardize the security and reliability of the systems that unknowingly use them. Unfortunately, the vast majority of existing physical and electrical detection solutions for counterfeit electronic parts are too complex to be used in practice, and the industry lacks simple and effective mechanisms to detect and/or prevent counterfeiting at a low cost [7]. In order to ensure the safety and reliability of critical systems, finding an effective, low-cost, reliable and universal solution to combat counterfeit systems is essential.

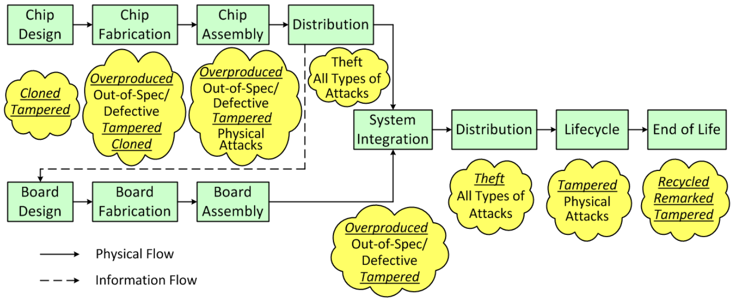

Figure 1: Electronic components and systems supply chain vulnerabilities.

So far, there has not been a one-size-fits-all solution to address these challenging problems. Various schemes have been proposed over the past decade to address counterfeit ICs. For example, physical unclonable functions (PUFs) exploit inherent process variations in silicon to provide low-cost authentication for ICs [12]. On-chip light-weight sensors are designed to effectively detect recycled ICs [13]. Hardware metering restricts the number of manufactured ICs produced by untrusted fab and thus combats overproduced and cloned parts [14]. Ending privacy of integrated circuits (EPIC) uses a novel low-overhead combinational chip-locking system and a chip-activation protocol based on public-key cryptography to render infringement impractical by making physical tampering unprofitable and attacks computationally infeasible [15]. By requiring test results to be verified by the IP owner and by requiring the IP owner to provide a "key" to unlock the correct functionalities of IPs, secure split-test (SST) allows IP owners to prevent defective parts from reaching the supply chain unnoticed [16]. Unfortunately, all the above measures are directed against one or at most two types of counterfeit ICs and none of them address counterfeit boards. In addition, test data can only be extracted when the whole system is powered on, which makes them incapable of tracking-and-tracing electronic products in the supply chain when the chips/boards are not powered.

Apart from embedded primitives and on-chip structures, stand-alone RFID tags have been used to identify/track electronic products. RFID tags with fingerprints based on their minimal power responses, measured at multiple frequencies, have been proposed as a way to uniquely identify the objects to which they are attached [17]. Another method of creating RF fingerprints exploits the near-field RF effects between the multiple antennas of the RFID reader and the uniquely modified substrate of the RFID tags [18]. However, all the above-mentioned RFID tags are stand-alone and lack a physical connection with the objects to which they are attached; thus, the RFID reader will make the wrong decision if, for example, an authentic tag is attached to a counterfeit system/PCB. Besides, the RFID tag data is usually static and cannot be updated to reflect the latest hardware conditions such as chip usage time, chip aging, chip grade, and the authenticity of chips on a PCB.

In this paper, we propose a universal platform for electronic component and system counterfeit detection and system traceability called CST that addresses the above-mentioned limitations of present solutions. Our main contributions are as follows:

- We propose a general infrastructure called CST that combats counterfeiting and enhances supply chain management. The CTS infrastructure is aimed at the next generation of electronic systems and requires the following: (1) sensors should be embedded inside the chips; (2) a PUF should be embedded in the RFID tag; (3) PCB antenna should be a part of the board.
- We design a module that extracts data (physical and environmental) captured by different sensors, structures, and hardware security primitives embedded inside different chips. This data is non-intrusively collected (i.e., with no impact on chip functionality, timing, and performance) by an RFID tag which can be read by an RFID reader. This eliminates the need for expensive testing, enables contactless detection from multiple different chips and boards simultaneously (thereby drastically reducing the authentication time), and can be used to retrieve chip/board information even when the chips/boards are not powered on.
- We develop new realizations and instances of several sensors/structures in the literature for our system and use each to target detection of specific counterfeit chip types.
- To enable board identification/authentication in CST, we propose a novel board ID generator that combines the tag PUF and sensor outputs from each chip on a PCB. The board ID can be used to track a PCB that is stolen and to detect illegal tampering/replacement of chips on the PCB.
- A prototype based on 90nm Xilinx Spartan-3E FPGAs is implemented and we verify that each component of CST works independently and the system as a whole operates as we expect.

The rest of this paper is organized as follows: Section II describes the basic framework of the proposed CST system; operating modes and communication flow are also introduced in this section. Section III introduces the building blocks of CST system and fully analyzes the working principles of each part. In Section IV, the performance of the CST is verified by simulation and experimental analysis. Finally, we conclude in Section V.

II. CST Architecture and Basic Operation

The proposed CST system is targeted at next generation systems to enable complete chip-level and board-level authentication and provide traceability. The focus of this paper is to develop a general infrastructure that can take advantage of existing on-chip structures/primitives for next generation electronic devices to combat counterfeiting and enhance supply chain management rather than develop new types of on-chip structures/primitives.

A. Overview of System Architecture

1) CST System: Figure 2 shows the basic framework of the proposed CST system. The analog front end and part of the digital control unit (i.e., a FM0/Miller encoder, a pulse-interval encoding (PIE) decoder, an encryption/decryption engine, a cyclic redundancy check (CRC) unit and a random number generator (RNG)) of the RFID tag are standard RFID components [19] [20]. All the remaining parts are the contributions of this paper (highlighted with light green color). CST is composed of a PCB slot antenna, an RFID tag with a board identifier generator (BIG) and a physically unclonable function (PUF), and CST sensors inside various chips on a PCB, as shown in Figure 2(a). The role of the antenna is to receive/transmit RF waves emitted from/to a reader. These RF waves will: (i) power the RFID tag when the board containing the tag is not powered on; (ii) request operations and backscatter RF responses (validation information and critical CST sensor data) from the tag to the reader. The RFID tag works as an interface between CST sensors and the RFID reader. Each chip gathers its own internal information (chip usage time, chip ID, chip grade, etc.) from the on-chip CST sensors. The RFID tag is responsible for (i) collecting and storing information from each chip and the board during operation; (ii) decoding received commands and encoding transmitted CST sensor data. The board ID is calculated based on unique information from chips and unclonable information (PUF output) from the tag.

2) Packaging and Integration: In order to ensure its functionality and security, the CST system should satisfy the following requirements in terms of packaging and interconnects for highest level of security: (1) sensors should be embedded inside the chips to provide chip-related information; (2) a BIG should be embedded in the RFID tag to provide a unique identifier; (3) PCB antenna should be a part of the board to enable communication with the RFID reader. All the above-mentioned constraints are supported by mature techniques and do not add too much of extra cost to the next-generation systems.

3) Chip Internal Structure: Figure 2(b) illustrates a chip with a number of CST sensors embedded within it ($S_1, S_2, ..., S_n$). These sensors send their measured data to the RFID tag periodically when the system is powered on or the chips are being used in the field. A light-weight controller inside the RFID tag manages the updating of CST sensors and arbitrates the bus race.

4) Internal Structure of RFID Tag: The RFID tag consists of two parts: the analog front end and the digital baseband control, as shown in Figure 2(c). The analog front end includes an internal oscillator to provide a clock signal for digital parts, a demodulator to demodulate the RF signals from the RFID reader, a voltage multiplier to boost up the power supply extracted from RF wave and drive all the other parts, and a backscattering modulator to modulate UHF wave with CST sensor data. The non-volatile memory (EEPROM) inside the RFID tag stores CST sensor data, passwords and other configuration variables. Note that while it is possible for an attacker to perform physical attacks to retrieve the information stored in the EEPROM, such attacks are expensive and protection against them are outside the scope of this paper. We are more concerned with attack capabilities of the majority of attackers rather than advanced persistent threats (APTs) [21]. By protecting the RF channel with a secure protocol [22] [23] [24] [25], it is impossible for the malicious reader to intercept data communicated by or overwrite secret data stored in the tag.

5) Internal Structure of the Digital Control Unit in the RFID Tag: Figure 2(d) illustrates the internal structure of the digital control unit in the RFID tag, which is composed of a controller (FSM), a FM0/Miller encoder, a PIE decoder, an encryption/decryption engine, a sequencer, a CRC unit, a RNG and a BIG. The controller is responsible for the coordination and management of each individual unit. The PIE decoder translates the commands and control parameters from the RFID reader, which is made up of a command parser and a packet parser. The FM0/Miller encoder encodes the backscattered CST sensor data. The sequencer sorts different CST sensor data bits and check bits. The CRC unit will generate 16-bit cyclic-redundancy checks (CRC16s) to ensure the integrity of transmitted data. The RNG unit will generate 16-bit random numbers (RN16s) to be XORed with transmitted data. The encryption/decryption engine is responsible for encrypting/decrypting CST sensor data with advanced encryption standard (AES) or some other cryptographic algorithms.

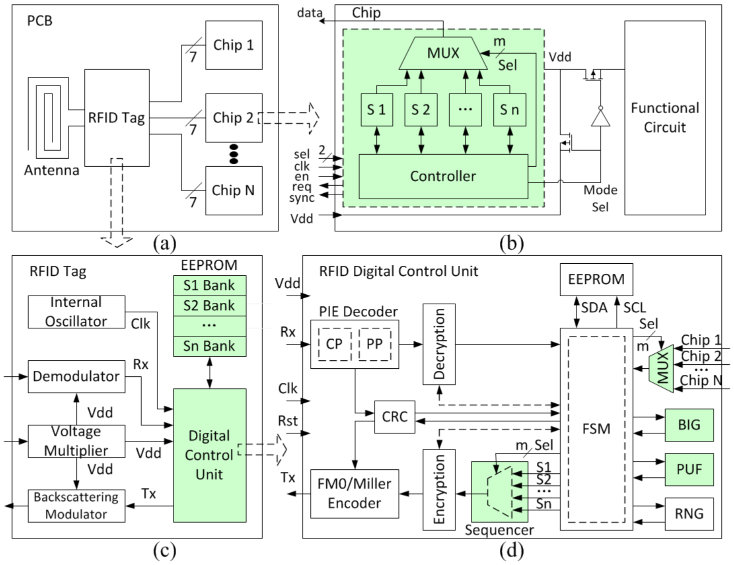

Figure 2: CST system: (a) A PCB with an RFID tag connected to different chips, (b) Internal structure of a chip with various sensors, (c) Internal structure of an RFID tag, and (d) Internal structure of the digital control unit in an RFID tag.

B. Operating Modes

There are two operating modes for the proposed CST system: Tag Access mode and System Operation mode. In System Operation mode, as shown in Figure 3(b), the system is conducting regular functional operations. *$Chip_i$* represents an arbitrary chip on the board. $(S_1, S_2, ..., S_n)$ denote n different sensors inside $Chip_i$. (S_1 Bank, S_2 Bank,...,S_n Bank) are n memory blocks allocated to n sensors in the non-volatile memory of the RFID tag. Different types of CST sensors $(S_1, S_2, ..., S_n)$ in different chips on the board can individually update their data to the memory inside the RFID tag according to predefined priorities. The entire system is powered on by the power supply on the board. As shown in Figure 3(c), all the sensors can be divided into three categories: (a) sensors that need to be updated only once over the life cycle (e.g., Electronic Chip ID [26]); (b) sensors that need to be updated once each time the system is powered on (e.g., PUF [12] [27]); and (c) sensors that need to be frequently updated when the system is powered on (e.g., the counter-based combating die/IC recycling sensor). $(1)-(3)$ denote the CST sensor priorities. Sensors of type (a) will be updated the first time the system is powered on. Sensors of type (b) are of a higher priority than sensors of type (c). When updating condition is satisfied, updating requests are sent to the RFID tag by the sensors of type (c). If the bus is not busy, the sample clock will be transmitted to sensors of type (c) to synchronize data transmission. In Tag Access mode, as illustrated in Figure 3(a), the RFID tag will be powered by the RF electromagnetic waves emitted by the RFID reader. Everything except the RFID tag is powered down. After verifying the identities and states of both sides, the RFID reader will issue commands to the RFID tag on the board, and the RFID tag will send corresponding CST sensor data back to the RFID reader.

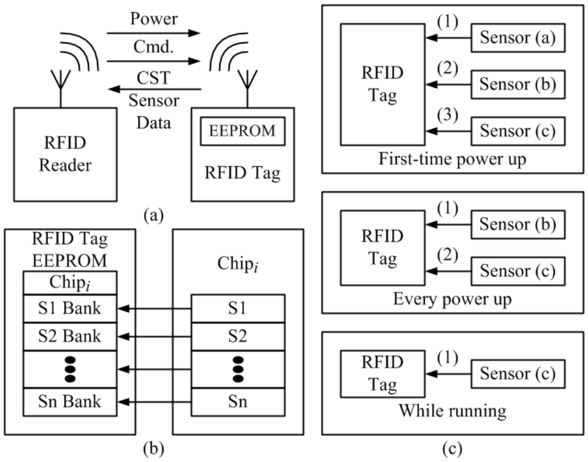

Figure 3: (a) Tag Access mode, (b) System Operation mode, and (c) CST sensor update priority.

C. Communication Flow

Mutual authentication between the reader and the tag is needed during communication. The communication flow between the RFID reader and the RFID tag (during Tag Access mode) is fully compatible with EPC Class-1 Generation-2 UHF RFID protocol [28]. Note that here we just implement the basic pseudo random number and password based authentication protocol for the purpose of simplicity. More secure AES based protocols [23] and hash-based protocols [22] [24] [25] are also supported by our proposed CST system. The focus of this paper is hardware architecture design. Designing more secure RFID protocol is out of the scope of this paper.

III. CST System Sensors

Different types of sensor data will be stored in different places of tag's non-volatile memory and updated periodically when the CST system is powered on. In the following, we briefly describe four sensors commonly mentioned in the literature and one new sensor which are used by CST. Table I lists each sensor and its purpose. We limit ourselves to these for brevity but many other sensors and on-chip structures can be used by the CST system as well depending on the applications the PCB is used in.

A. CST Sensors

Multiple types of counterfeits can be detected and combatted using different types of CST sensors/primitives. Note that we use the terms sensors and primitives interchangeably. This section will discuss our implementations of the sensors shown in Table I. Since many of the original implementations [12] [13] [27] of these sensors were imagined for different platforms than ours, we have

Table I: Functions of different types of CST sensors

Sensor Type	Function
CDIR_CTR	Tracks chip usage time (fine granularity) and detects recycled ICs.
CDIR_RO	Tracks chip usage time (coarse granularity) and detects recycled ICs.
PUF	1. Uniquely identifies silicon chips. 2. Detects cloned and overproduced ICs.
ECID	Protects the chip against remarking and over-grading.
Board ID	1. Identifies and tracks boards in the supply chain. 2. Detects board cloning and overproduction. 3. Detects unauthorized substitution of chips on the board. (e.g., mod-chips in video game consoles)

developed new practical realizations for each sensor making them suitable for meeting the CST system's objectives. We also propose a novel board ID generator in this section.

1) Counter-based CDIR: The first two sensors we discuss are called combating die/IC recycling (CDIR) sensors. The counter-based CDIR sensor (CDIR_CTR) [13], which belongs to sensors of type (c), can be used to track chip usage time and detect recycling of ICs. Even an extremely short chip usage time can be detected by this sensor. Figure 4 shows our implementation. The contribution of this paper is highlighted with light green color. The four *most active* nets of the functional circuit, marked as $sw[0-3]$, are selected as the trigger signal of the CDIR_CTR sensor. If and only if all four nets are transitioned to high level, a positive edge pulse will be generated by the AND gate to drive counter1. In order not to update the CDIR_CTR memory bank inside the RFID tag too frequently, the minimum four bits of counter1 will be filtered by a bit-wise AND operation with $16'hFFF0$ to produce a value for $flag$, which is a new design of this paper. The benefit of this modification is that we do not need to request updates too frequently and thus avoid bus race. A timer triggered by the system clock will periodically check whether $flag$ is larger than zero or not. If the value of $flag$ is larger than zero, the value of counter1 will be sent to a shift register. Simultaneously, a request update (*requpdate*) signal will be sent to the RFID tag control logic. If the RFID tag is not busy, sample clocks will be sent to CDIR_CTR. Subsequently the CDIR_CTR data will be shifted out bit by bit by the sample clock. The CDIR_CTR data associated with $Chip_i$ can indicate whether the chip is new or used.

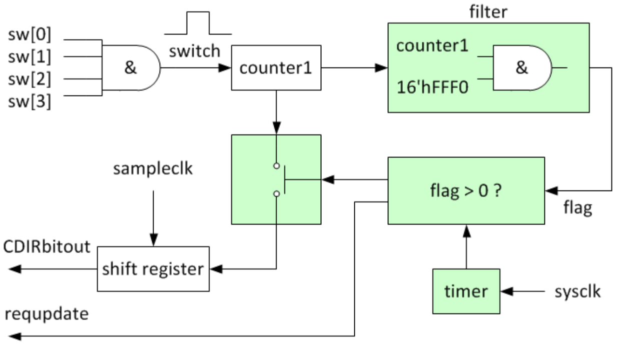

Figure 4: A counter-based CDIR sensor: this sensor captures circuit usage time in the field.

2) RO-based CDIR: Figure 5 shows the structure of the RO-based combating die/IC recycling sensor (CDIR_RO) [13], which consists of a Reference ring oscillator (RO), a Stressed RO, two counters, a timer, a subtractor and a shift register. The contribution of this paper is highlighted with light green color. CDIR_RO belongs to sensors of type (b). Unlike CDIR_CTR, CDIR_RO does not require any memory element to store the chip usage time, since it is solidified in the frequency difference between two ROs. However, the granularity of detection for CDIR_RO is larger than CDIR_CTR, which means CDIR_RO is not as sensitive to extremely short chip usage time. The Stressed RO will be under DC stress when the chip is powered on. The Reference RO will be disconnected from power using the sleep transistors, and thus will experience minimal aging effects. The Reference RO will oscillate only when the RFID tag is reading CDIR_RO data from the specific chip. As the Stressed RO has gone through aging effects, the time delay of the inverters composing RO will increase. As a result, the oscillating period of the Stressed RO will be larger than that of the Reference RO. Therefore, the value of counter_ref will be larger than that of counter_str. In the original design, a multiplexer is exploited to select one of the two ROs and a counter is responsible for measuring the oscillating cycles of the selected one. In this paper, two identical counters measure the oscillating cycles of the two ROs simultaneously during a pre-specified time period, which is controlled by the timer. CDIR_RO data will be obtained by subtracting the value of counter_str from the value of counter_ref, which is a new design of this paper. By comparing CDIR_RO data at time t with initial CDIR_RO data, one can determine whether the chip of interest is recycled or not. The benefit of this modification is that we do not need any external postprocessing anymore.

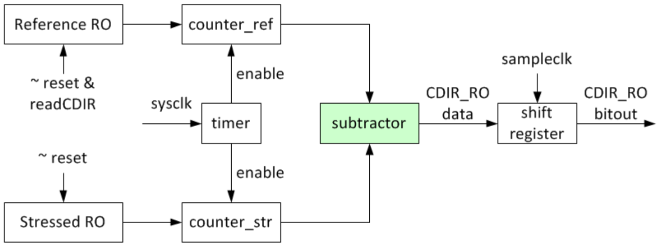

Figure 5: A RO-based CDIR sensor.

3) PUF: PUF is a security primitive that exploits IC manufacturing process variations to uniquely identify and authenticate each chip. Cloned and overproduced ICs can be detected using PUFs. Typical PUFs include delay-based PUF [12], butterfly PUF [29] and bi-stable ring PUF [30]. The CST system can adopt all different types of PUFs. Here we present the popular RO-PUF as a sensor/primitive of type (b). Figure 6 shows the structure of the PUF implemented in the CST system, which consists of a linear feedback shift register (LFSR), 64 identical ROs, 2 multiplexers, and 2 counters. The contribution of this paper is highlighted with light green color. A 10-bit seed will be injected into the LFSR to generate a 10-bit challenge. The most-significant 5 bits of the challenge will be used to select one RO from the upper 32 ROs, and the least-significant 5 bits of the challenge will be used to select a second RO from the lower 32 ROs. Two identical counters will count the clock cycles of the two selected ROs. A pre-specified value (PV) is stored in the two counters, which is generated by connecting certain input bits of a latch array to power and the other input bits to ground with *tiehi* and *tielo* cells. These cells act as one-time programmable (OTP) cells. When one of the two counters reaches the pre-specified value more quickly, it will disable the other counter immediately, which is a new design of this paper. If the upper RO arrives the pre-specified value first, 0 will be output as the response to the challenge; otherwise, 1 will be output as the response to the challenge. Compared with traditional RO-PUF [27], which compares the number of oscillations of two selected ROs in a fixed time interval (comparison time), this new implementation eliminates the need for a comparator and a timer (recording the comparison time), and thus saves area overhead and harvest time. Once a one bit output is generated, the challenge request signal will be activated, requiring that the LFSR generate a new challenge. The responses for all subsequent challenges are concatenated to form a large unique chip response which is sent to the RFID tag and stored. In this paper, we assume an implementation of a reliable RO-PUF. The reliability analysis of such PUFs are outside the scope of this paper.

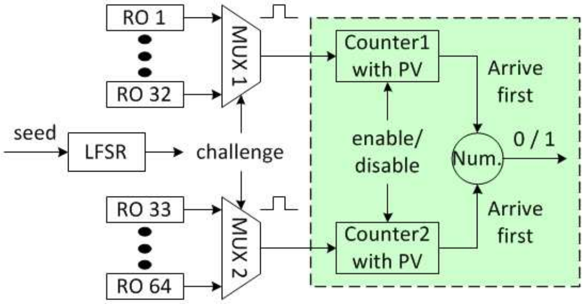

Figure 6: An implementation of RO-PUF.

4) Electronic Chip ID (ECID): The ECID, which belongs to sensors of type (a), will provide general information about chips, including chip grade, classification and manufacturer, to protect the chip against remarking, especially combatting over-grading. An ECID is generated by connecting certain bits of a latch array to power and the other bits to ground with *tiehi* and *tielo* cells. The ECID is solidified within the hardware and thus cannot be easily modified to remark a chip. When the sample clock from RFID tag arrives, the ECID will be shifted out bit by bit. Additional information including temperature limits, noise, etc. can also be included in an ECID. The ECID is public and there is no negative impact even if it is cloned.

5) Board ID: The board ID we design here is primarily targeted for board identification and tracking in the supply chain. In addition, the board ID can be used to detect unauthorized substitution of original chips on board, which we refer to as board tampering. Figure 7 shows the structure of our proposed board ID generator, which is integrated inside the RFID tag. The board ID in our CST system is generated by combining the tag PUF and each individual chip's PUF with a special function. The function should be such that (i) the ID generated for each board is unique for all the boards in the population and (ii) it is very sensitive to any changes to the chips on the board (e.g., replacing one chip with a counterfeit or modified chip). In the worst case, even if the attacker could intercept the communication between the tag and chips and figure out the chip PUFs, it is still impossible for the attacker to clone the board ID since the tag PUF never leaves the tag.

We propose two functions in this paper. In both cases, we choose the bit width of the board ID to be equal to the bit width of the tag and chip PUFs but other functions could work differently. Our first function is as follows. We perform a bitwise exclusive OR on the tag PUF and all chip PUFs. Assuming there are one tag PUF (PUF_0) and L different chip PUFs ($PUF_1, PUF_2, ..., PUF_L$), the board ID based on the first option can be calculated as:

$$BoardID = bitxor(PUF_0, PUF_1, PUF_2, ..., PUF_L) \tag{1}$$

Our second function is as follows. We count the number of ones and zeroes at the same bit location for the tag PUF and all chip PUFs. If the number of ones exceeds the number of zeroes, the corresponding bit of board ID will be one; otherwise it will be zero. For this method, the number of chip PUFs should be even given that there is one more tag PUF. Assuming there are one $N-bit$ tag PUF (PUF_0) and L different $N-bit$ chip PUFs, the i_{th} bit of the board ID based on the second option can be calculated as:

$$BoardID(i) = \begin{cases} 1, & \text{if } \sum_{j=0}^{L} PUF_j(i) > \frac{L+1}{2} \\ 0, & \text{if } \sum_{j=0}^{L} PUF_j(i) < \frac{L+1}{2} \end{cases}, \ i = 1, 2, ..., N \tag{2}$$

We compare the uniqueness and sensitivity to changes of both proposed functions using a CST prototype in the results section.

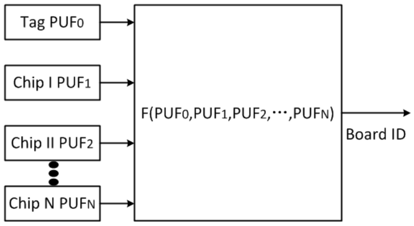

Figure 7: Board ID generator.

B. Updating of Each Sensor Type

Since the ECID is static, it will be written to the memory only once for each chip. The PUF will be updated only once every time when the system is powered on. For CDIR_RO, an initial difference between Reference RO and Stressed RO (present due to process variation) will be stored during system startup. When the system is used in the field, the difference between Reference RO and Stressed RO will periodically be stored. The chip usage time can thus be calculated as:

$$T_{chip\_usage} = CDIR\_RO_t - CDIR\_RO_0 \tag{3}$$

where $CDID\_RO_0$ denotes the initial difference between Reference RO and Stressed RO, and $CDID\_RO_t$ represents their difference at time t.

CDIR_CTR data will be accumulated once the request update signal is active and the RFID tag is not busy. CDIR_CTR data may be updated multiple times once the system is powered on. In order to save the number of bits for CDIR_CTR data, each time when the CDIR_CTR data increment is sent to the RFID tag, it will be shifted to the right by 8 bits to generate a Δ. If Δ is not equal to zero, it will be added to the old CDIR_CTR data to produce new CDIR_CTR data, which will override the old data. If Δ is equal to zero, $16'd1$ will be added to the old CDIR_CTR data to produce new CDIR_CTR data.

IV. Results and Analysis

In this section, we evaluate CST operation via both simulations and a prototype implementation with 90nm Xilinx Spartan-3E FPGAs. All the results are used to verify that each function of the CST system is performed correctly. First, we estimate the sensor overheads via design tools to show that the system is non-intrusive (i.e., little impact of area, power, timing, etc.). Next, the prototype was used to verify the digital parts of the system, and compare the uniqueness and sensitivity to changes of the proposed board ID functions. Note that we do not include results for most of the sensors since they are available in prior work. Finally, we evaluate the system robustness to different types of potential attacks.

A. Simulation Results

Synopsys Design Compiler (DC) is used to synthesize the CST sensors embedded inside various chips. Table II shows the area and power overhead based on IBM 130nm CMOS 8RF-DM technology. Taking into consideration the large quantity of information these sensors can provide, an overhead of this order is acceptable. In order to reflect the latest hardware conditions, the updating periods should not be too long (please refer to Table III for exact quantifications) for those sensors which need frequent updates. At the same time, the processing time of each sensor should be as short as possible to be sensitive to extremely short power-on time. After placement and routing, the Synopsys Verilog Compiler Simulator (VCS) is used to analyze the timing of the CST sensors. Table III shows the updating periods and processing time of the CST sensors. When sampling clocks from the RFID tag arrive, CDIR_CTR and ECID are already ready, so CDIR_CTR and ECID need less processing time. In contrast, CDIR_RO and PUF have to generate sensor data in real time and thus consume more processing time.

Table II: Overhead analysis of CST sensors

Sensor	Area Overhead		Power Overhead	
	# of cells	Area (μm^2)	Dynamic Power (μW)	Leakage Power (nW)
CDIR_CTR	186	2828	127.27	37.57
CDIR_RO	255	3433	123.53	43.11
PUF	432	4894	166.34	48.67
ECID	28	342	17.68	4.55
Four Sensors + Ctl. Unit	1026	21235	519.28	220.94

Table III: Updating periods and processing time of CST sensors

Sensor	Updating Period (μs)	Processing Time (μs)
CDIR_CTR	6554	3
CDIR_RO	Once each time powered on	5007
PUF	Once each time powered on	9926
ECID	Once	3

B. *Experimental Analysis*

The digital part of the CST system was implemented on 90nm Xilinx Spartan-3E FPGAs, in order to verify its effectiveness in working as a channel to collect board- and chip-related ID and usage information. Two Spartan 3E FPGAs were used to work as the RFID reader and the RFID tag respectively. Flash M25P16 on board was employed to store the CST sensor data. An SPI bus was utilized to connect the FPGA chip and the Flash M25P16. The test and measurement setup is shown in Figure 8 (a). Figure 8 (b) shows the FPGA layout of the RFID tag digital part with ring oscillators highlighted. For CDIR_RO, Reference RO and Stressed RO should be placed at symmetrical locations and next to each other to reduce the influence of process and environmental variations. Similarly, the upper and lower 32 ROs of PUF should be also symmetrically placed and close to each other.

15 Spartan 3E FPGA boards were employed to generate 15 128-bit board IDs, with 17 PUFs implemented on each board. Figure 9 illustrates the hamming distance distributions of board IDs based on Equation 1 and Equation 2 respectively. The mean values of hamming distances for both board IDs are 63.3714(49.51% out of 128) and 53.3143(41.65% out of 128) respectively. Hamming distance mean value of the first board ID is closer to the half of board ID bit-width 128 which is ideal. Hamming distance distributions based on both equations approximate normal distribution. Experimental results demonstrate that the first board ID is more effective at identifying boards. Table IV shows the board ID variance when replacing one of 17 PUFs that constitute the board ID with another irrelevant PUF. The board ID based on Equation 1 is more sensitive to PUF replacement. With the first board ID implemented in the CST system, we can find abnormity of board ID even when only one counterfeit chip is located on the board.

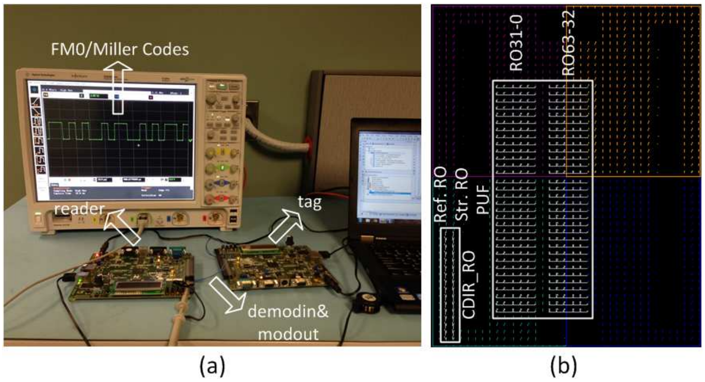

Figure 8: (a) Experimental Setup and (b) FPGA Layout of the RFID Tag Digital Part.

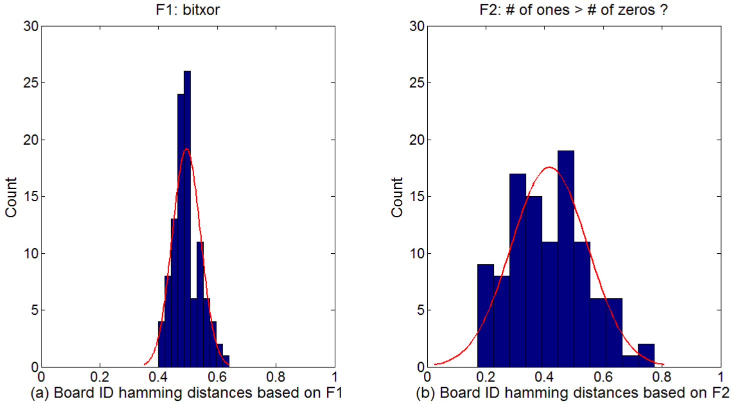

Figure 9: Hamming distance distribution of board IDs.

C. *Security Evaluation*

Table V lists the potential system-level attacks towards general board-level system (including our proposed CST system) associated with their attack cost before/after mitigation and mitigation methods. The board ID can be used to detect unauthorized chip replacement. The tag clone can be prevented by embedding a PUF in the tag. By placing the transmission lines linking the tag and chips on the internal layers of PCB, using chip package with hidden pins/leads (e.g., ball grid array package) and an embedded EEPROM, we can reduce the vulnerability to basic probing attacks. Further protection towards the communication between the tag and chips is available by encryption. By encrypting the memory data bus and hiding the secret data in a random location, we can ensure the security and integrity of the secret data stored in the EEPROM (but this is admittedly quite expensive). We are not interested in addressing expensive physical attacks. The RF channel will be safe so long as the communication between the reader and the tag follows secure protocols. One limitation of the proposed system is that we cannot address board tampering with extra malicious circuitry. Taking into account that this type of attack requires redesigning the board, which is expensive, our proposed CST system is secure in the vast majority of application areas.

V. Conclusion

This paper presents the first RFID-based system suitable for electronic component and system counterfeit detection and system traceability called CST. The effectiveness of this system has been

Table IV: Board ID sensitivity towards PUF replacement

Function	Board ID (128 bits) variance														
	Board I	Board II	Board III	Board IV	Board V	Board VI	Board VII	Board VIII	Board IX	Board X	Board XI	Board XII	Board XIII	Board XIV	Board XV
F1: bitxor	45.66%	46.29%	45.23%	44.37%	50.27%	43.28%	47.38%	48.83%	46.48%	47.7%	49.88%	55.16%	48.67%	51.84%	48.28%
F2: # of ones > # of zeros ?	4.61%	10.94%	3.48%	9.1%	6.99%	2.07%	4.49%	11.68%	6.45%	0.78%	8.59%	4.41%	4.65%	6.29%	5.43%

Table V: System level security evaluation

Attack target	**Attack approach**	**Attack cost before mitigation**	**Attack cost after mitigation**	**Mitigation**
Chip	Replace the original chip with an illegal substitute (e.g., a counterfeit IC).	Low	Extremely High	Detect malicious chip replacement via board IDs generated over tag PUF and all chip PUFs.
Chip interconnection	Intercept the communication between the tag and chips to obtain the chip-related information.	Low	High	1. Place the transmission lines, linking the tag and chips, on the internal layers of PCB. 2. Use chip package with hidden pins/leads. 3. Encrypt the communication between the tag and chips.
RFID tag	Clone the tag to evade counterfeit detection.	Medium	Extremely High	Embed a PUF in the tag.
EEPROM	1. Decap EEPROM and microprobe the data bus to gain secret data (e.g., password and board ID). 2. Decap EEPROM and use expensive equipment (e.g., an electro-optical probe) to sense the value of EEPROM bit cells.	High	Extremely High	1. Encrypt memory data bus. 2. Hide the secret data in a random location.
RF channel	Use a malicious reader to access the tag and steal secret data.	Low	Extremely High	1. Access is protected through password. 2. Data transmission is XORed with random numbers. 3. Apply AES encryption. 4. Apply hash-based secure protocol.

verified through simulations and experimental results. Compared with existing approaches, the CST system has the following merits: (1) CST is the first platform to detect multiple types of counterfeits by collecting, storing, and communicating the measurements and chip-related information from multiple sensors; (2) Board identification and tracking in the supply chain are supported; (3) Board- and chip-related information can be updated periodically and extracted even when the system is powered off; (4) The test overhead is much lower than existing tests because an RFID reader can extract the information from multiple boards simultaneously and in a contactless fashion. In future work, we aim to build on this concept to address more well-funded attackers with greater capabilities.

References

[1] J. Carbone, "Most counterfeit parts involve obsolete semiconductors and other EOL components," *The Source*, Aug. 2012.

[2] H. Livingston, "COUNTERFEIT INCIDENT REPORTING TRENDS C OBSERVATIONS IN ANTICIPATION OF FORTHCOMING REGULATIONS," Aug. 2013, http://counterfeitparts.wordpress.com/2013/08/06/counterfeit-incident-reporting-trends-observations-in-anticipation-of-forthcoming-regulations/.

[3] S. C. H. I. for Electronics Defense (SHIELD) Microsystems Technology Office, "Broad Agency Announcement," March 2014, DARPA-BAA-14-16.

[4] P. Subramanyan, N. Tsiskaridze, K. Pasricha, D. Reisman, A. Susnea, and S. Malik, "Reverse engineering digital circuits using functional analysis," in *Design, Automation Test in Europe Conference Exhibition (DATE), 2013*, March 2013, pp. 1277–1280.

[5] R. Chakraborty, S. Narasimhan, and S. Bhunia, "Hardware trojan: Threats and emerging solutions," in *High Level Design Validation and Test Workshop, 2009. HLDVT 2009. IEEE International*, Nov 2009, pp. 166–171.

[6] R. Maes, D. Schellekens, P. Tuyls, and I. Verbauwhede, "Analysis and design of active IC metering schemes," in *Hardware-Oriented Security and Trust, 2009. HOST '09. IEEE International Workshop on*, July 2009, pp. 74–81.

[7] U. Guin, D. DiMase, and M. Tehranipoor, "Counterfeit Integrated Circuits: Detection, Avoidance, and the Challenges Ahead," *Journal of Electronic Testing: Theory and Applications (JETTA)*, 2014.

[8] W. Cobb, E. Garcia, M. A. Temple, R. Baldwin, and Y. Kim, "Physical layer identification of embedded devices using rf-dna fingerprinting," in *MILITARY COMMUNICATIONS CONFERENCE, 2010 - MILCOM 2010*, Oct 2010, pp. 2168–2173.

[9] S. Sathyanarayana, W. Robinson, and R. Beyah, "A network-based approach to counterfeit detection," in *Technologies for Homeland Security (HST), 2013 IEEE International Conference on*, Nov 2013, pp. 473–479.

[10] B. Mitchell, "Network Engineer Charged in Multi-Million Dollar Cisco Equipment Theft," Dec. 2011, http://compnetworking.about.com/b/2011/12/10/network-engineer-charged-in-multimillion-dollar-cisco-equipment-thef.htm.

[11] A. Waters, "The Case of the Great Router Robbery," May 2011, http://resources.infosecinstitute.com/router-robbery/.

[12] G. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Design Automation Conference, 2007. DAC '07. 44th ACM/IEEE*, 2007, pp. 9–14.

[13] X. Zhang and M. Tehranipoor, "Design of on-chip lightweight sensors for effective detection of recycled ICs," *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on*, vol. PP, no. 99, pp. 1–1, 2013.

[14] F. Koushanfar and G. Qu, "Hardware metering," in *Design Automation Conference, 2001. Proceedings*, 2001, pp. 490–493.

[15] J. Roy, F. Koushanfar, and I. Markov, "Ending piracy of integrated circuits," *Computer*, vol. 43, no. 10, pp. 30–38, Oct 2010.

[16] G. Contreras, M. Rahman, and M. Tehranipoor, "Secure split-test for preventing IC piracy by untrusted foundry and assembly," in *Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), 2013 IEEE International Symposium on*, 2013, pp. 196–203.

[17] S. Periaswamy, D. Thompson, and J. Di, "Fingerprinting RFID tags," *Dependable and Secure Computing, IEEE Transactions on*, vol. 8, no. 6, pp. 938–943, 2011.

[18] V. Lakafosis, A. Traille, H. Lee, G. Orecchini, E. Gebara, M. Tentzeris, J. Laskar, G. DeJean, and D. Kirovski, "An RFID system with enhanced hardware-enabled authentication and anti-counterfeiting capabilities," in *Microwave Symposium Digest (MTT), 2010 IEEE MTT-S International*, 2010, pp. 840–843.

[19] U. Karthaus and M. Fischer, "Fully integrated passive UHF RFID transponder ic with 16.7- mu;w minimum RF input power," *Solid-State Circuits, IEEE Journal of*, vol. 38, no. 10, pp. 1602–1608, Oct 2003.

[20] D. Yeager, F. Zhang, A. Zarrasvand, N. George, T. Daniel, and B. Otis, "A 9 μA, addressable gen2 sensor tag for biosignal acquisition," *Solid-State Circuits, IEEE Journal of*, vol. 45, no. 10, pp. 2198–2209, Oct 2010.

[21] T. Mustafa, "Malicious data leak prevention and purposeful evasion attacks: An approach to advanced persistent threat (apt) management," in *Electronics, Communications and Photonics Conference (SIECPC), 2013 Saudi International*, April 2013, pp. 1–5.

[22] K. Yüksel, J.-P. Kaps, and B. Sunar, "Universal hash functions for emerging ultra-low-power networks," in *Proceeding of The Communications Networks and Distributed Systems Modeling and Simulation Conference (CNDS)*, January 2004.

[23] M. Feldhofer, "Securing passive RFID tags using strong cryptographic algorithms," in *RFID Systems and Technologies (RFID SysTech), 2008 4th European Workshop on*, June 2008, pp. 1–2.

[24] G. Avoine and P. Oechslin, “A scalable and provably secure hash-based RFID protocol,” in *Pervasive Computing and Communications Workshops, 2005. PerCom 2005 Workshops. Third IEEE International Conference on*, March 2005, pp. 110–114.

[25] D. Henrici and P. Muller, “Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers,” in *Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second IEEE Annual Conference on*, March 2004, pp. 149–153.

[26] Y. Su, J. Holleman, and B. Otis, “A digital 1.6 pj/bit chip identification circuit using process variations,” *Solid-State Circuits, IEEE Journal of*, vol. 43, no. 1, pp. 69–77, Jan 2008.

[27] S. Mansouri and E. Dubrova, “Ring oscillator physical unclonable function with multi level supply voltages,” in *Computer Design (ICCD), 2012 IEEE 30th International Conference on*, Sept 2012, pp. 520–521.

[28] E. Inc., “EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz C 960 MHz Version 1.2.0,” May 2008.

[29] S. Kumar, J. Guajardo, R. Maes, G.-J. Schrijen, and P. Tuyls, “Extended abstract: The butterfly PUF protecting IP on every FPGA,” in *Hardware-Oriented Security and Trust, 2008. HOST 2008. IEEE International Workshop on*, 2008, pp. 67–70.

[30] M. Bhargava, C. Cakir, and K. Mai, “Reliability enhancement of bi-stable PUFs in 65nm bulk CMOS,” in *Hardware-Oriented Security and Trust (HOST), 2012 IEEE International Symposium on*, 2012, pp. 25–30.