ReSC: RFID-enabled Supply Chain Management and Traceability for Network Devices

Kun Yang, Domenic Forte, and Mark Tehranipoor

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

Abstract. The supply chains of today are much more complex, global, and difficult to manage than ever before. Disappearance/theft of authentic goods and appearance of counterfeit (cloned, forged, etc.) goods are two major challenges to address. As a result, owners, manufacturers, distributors, etc. are becoming more interested in approaches that facilitate greater visibility and enable traceability of products as they move through the supply chain. One promising approach is based on Radio-Frequency Identification (RFID) where each product is equipped with a unique RFID tag that can be read in a contactless fashion to track the movement of products. However, existing RFID tags are simply "wireless barcodes" that are susceptible to split attacks (i.e., separating tag from product, swapping tags, etc.) and can easily be stolen or cloned. In this paper, we propose an RFID-enabled Supply Chain (ReSC) solution specific to network devices (i.e., routers, modems, set-top boxes, video game consoles, home security devices, etc.) that addresses the security and management issues of their entire supply chain. By combining two techniques: one-to-one mapping between tag identity and control chip identity, and unique tag trace which records tag history information, ReSC is resistant to counterfeit injection, product theft, and illegal network service (e.g., Internet, TV signals, online games, etc.) access. Simulations and experimental results based on a printed circuit board (PCB) prototype demonstrate the effectiveness of ReSC.

Keywords: Radio-Frequency Identification (RFID), Supply Chain Management, Traceability, Network Device

1 Introduction

The security and management issues of today's supply chains have raised serious concerns recently for industry, governments, and consumers. Two major challenges include disappearance/theft of authentic goods and appearance of counterfeit (cloned, forged, etc.) goods. Both of these impact the profit and reputations of the owners, manufacturers, and distributors. In 2012, 117 electronic thefts were reported in the US with the average loss of $382,500 per theft incident [12]. One example is the infamous Cisco router theft problem [30, 38]. In addition, more than 12 million counterfeit parts were reported from 2007 to 2012 [6], and this number is on the rise [26]. In most cases, criminals take the risk of theft and/or counterfeiting for nothing more than the economic gain (i.e., resale values of stolen products, price discrepancy between genuine and fake goods, etc.). Such criminal activities however could later become aid in tampering and cause of other major security concerns. For example, hackers could invade the internal network of a company if they obtain the branch router using unlawful means [38], confidential data (e.g., trade secrets) could be disclosed if a counterfeit (tampered) device is installed in the information management system of a company, and so forth. Other than theft of product, theft of service draws a great deal of attention from network service providers.

For instance, Comcast, AT&T, Charter, Cox, etc. want to authenticate their devices before providing service to customers. By enhancing visibility and traceability of such devices across the entire supply chain, we may be able to overcome and mitigate many of these issues before they have even more significant consequences.

Further, the concept of the Internet of Things (IoTs) has attracted more and more attention over the past few years. The IoTs correspond to the interconnection of uniquely identifiable embedded computing devices within the existing Internet infrastructure. Cisco's Internet Business Solutions Group (IBSG) predicts there will be 25 billion devices connected to the Internet by 2015 and 50 billion by 2020 [11]. Compared with stand-alone devices, the security and management issues of networked devices have raised more concerns, not only because of the rise of the number of networked devices, but also because of the mutual dependence between networked devices. For example, if one device in a network system is tampered, the attacker could send malicious messages to its neighboring devices to obtain secret information [38].

Barcodes have traditionally been used to track and trace commodities in the supply chain [35]. Quick response (QR) codes which can include much more information have also been put into use [19]. However, both barcodes and QR codes are very easy to damage, remove, replace, forge or clone because of visibility of identity information and low technical barrier. Other shortcomings (i.e., requirement of individual scanning, need of direct line-of-sight and close proximity to reader, lack of write capability once printed, etc.) severely impact their access efficiency, thus limiting their utility. More recently, RFID technologies have been proposed to enhance the management of supply chains [10,16]. Wal-Mart and the United States Department of Defense have published requirements that their vendors place RFID tags on all shipments to improve supply chain management. Compared to barcodes and QR codes, an RFID-based scheme has much more attractive features – possess write capability, support batch scanning, exist in very small factors, and do not require direct line-of-sight for access – making them easier to be embedded in many different products and enable automatic track-and-trace. However, existing RFID tags are simply "wireless barcodes" which lack inherent connection to the objects they are attached to. As a result, they are vulnerable to split attacks (i.e., separating tag from product, swapping tags, etc.).

In this paper, we present an RFID-enabled Supply Chain (ReSC) solution that addresses the security and management issues of network devices in the supply chain. The major features of ReSC and our main contributions are as follows:

- Attack models against RFID-enabled supply chain systems are defined and analyzed. The corresponding mitigation measures have been integrated into the ReSC system.
- By binding the RFID tag and the identified network device together with a one-to-one mapping between tag identity and control chip (i.e., the host processor that is responsible for major functions and coordination between different components on the board) identity, ReSC is resistant to split attacks. Mismatch between tag and control chip identities will be detected.
- When the network device is distributed in the supply chain, a unique tag trace composed of signatures of readers on the distribution path of that device will be generated and stored in the tag memory. The tag trace is unique for each device, digitally signed by each reader on the tag's path, and thus is resistant to duplication by untrusted entities involved in the supply chain. When the network device is installed at the end-user, service requests will be rejected if the tag trace stored in the tag memory shows that the device has not passed through the valid supply chain. ReSC differs from other supply chain solutions in that: (i) the tag trace is bound to the device and cannot be duplicated to be used for another device; (ii) readers cannot repudiate their signatures;

and (iii) ReSC is the first RFID-assisted scheme to prevent fake or stolen products from being used by end-users.
– We implement major functions of ReSC system in a PCB prototype to verify that the system as a whole operates within the pre-defined specification. Our approach is also cost effective in that it takes advantage of existing parts on present network devices and requires only a few extra very low-cost components.

The rest of this paper is organized as follows: Section 2 presents previous work related to ReSC. Section 3 describes the supply chain features specific to network devices, attack models against RFID-enabled supply chain systems, and the hardware architecture of ReSC system. Section 4 elaborates on our proposed authentication procedures (i.e., tag matching with device and valid tag trace) in detail. Section 5 presents the implementation of ReSC prototype. In Section 6, we evaluate ReSC system in terms of performance and security. Finally, we conclude in Section 8.

2 Related Work

Two areas of prior work have particular relevance to our study: digital integrated circuit (IC) identification/authentication and RFID-enabled supply chain management.

Physical Unclonable Functions: Among different digital IC identification/authentication approaches, physical unclonable functions (PUFs) are widely considered to be one of the most promising methods [31, 37]. PUFs are more secure than conventional identity storage since they exploit the uncontrollable process variations associated with modern IC fabrication [13]. An ideal PUF produces a unique and reliable response when issued a challenge. A variety of different types of PUFs have been proposed and implemented over the past decade, including arbiter PUF [37], ring oscillator (RO) PUF [28], SRAM PUF [17], butterfly PUF [23], etc. SRAM PUF has become popular due to its convenience of using commonly available and integrated SRAM rather than include a dedicated primitive in the circuit. Comparative analysis of SRAM memories manufactured by different vendors using different technology nodes was conducted by authors in [36] and demonstrated that all of the tested SRAMs can be used as PUFs. Like other PUFs, SRAM PUF is also susceptible to reliability issues. Error Correcting Code (ECC) [8] that corrects the unreliable output bits is widely used to address the reliability issues of SRAM PUF. Neighborhood analysis based bit selection algorithms [18,39] improve the reliability of SRAM PUF by exploring the selection of stable bits through enrollment under different conditions (temperature, voltage, and aging) and exploiting interactions between neighboring SRAM cells. A soft decision helper data algorithm [27] was also presented to deal with the fuzziness of SRAM PUF's responses.

RFID-enabled Supply Chain Management: RFID technologies have been widely explored to enhance visibility and enable traceability in the supply chain over the past decade [1, 3, 14, 29]. Unidirectional key distribution across time and space [22] was proposed to address the problem of key management in RFID systems. The authors in [24,41,42] proposed a tailing mechanism to detect counterfeit goods with cloned or forged tags by writing random numbers to tags as they go through the supply chain and verifying tail (composed of random numbers) divergence between authentic and cloned or forged tags over time. However, this approach has the following limitations: (i) the tags lack inherent connection to the objects they are attached to and thus are vulnerable to split attacks; (ii) the tag trace has no necessary relation to the tag itself and thus is vulnerable to duplication attack (i.e., duplicating tag trace); (iii) readers have to be connected to the database to perform rule verification and clone detection; (iv) this approach does not consider different types of potential attacks (i.e.,

eavesdropping, denial-of-service attack, replay attack, etc.); and (v) this approach cannot prevent counterfeit or stolen products from being used by end-users.

By combining the features of these two techniques, we propose a new type of supply chain system specific to network devices that addresses most security and management issues of the supply chain.

3 ReSC Framework

Disappearance/theft of authentic goods and appearance of counterfeit (cloned, forged, etc.) goods frequently occur in the global electronics component and system supply chain. There is no effective approach to enhance product traceability, enable counterfeit detection, and prevent theft of product and service simultaneously with low cost. ReSC is the *first* supply chain system specific to network devices that enables product track-and-trace, counterfeit detection, and theft prevention. To do so, it makes use of *offline* and *online* modes (more details below).

3.1 Supply Chain with Transition Points

Figure 1(a) demonstrates our proposed RFID approach aimed at addressing different challenges/issues in the supply chain for network devices. Our proposed RFID system for network devices would consist of the following: (i) a front-end composed of RFID tags and readers; (ii) network devices equipped with RFID tags that include read-only tag identities (*tagIDs*) stored in the locked memories; (iii) locations associated with each reader; (iv) a back-end consisting of a centralized database (DB) that stores information (e.g., tag identities, control chip identities, tag traces, etc.) and authenticates network devices. We divide the supply chain for network devices into three states (S1, S2, and S3) and there are three possible state transitions (T1, T2, and T3) between states. Figure 1(b) illustrates the state transition graph of our proposed scheme.

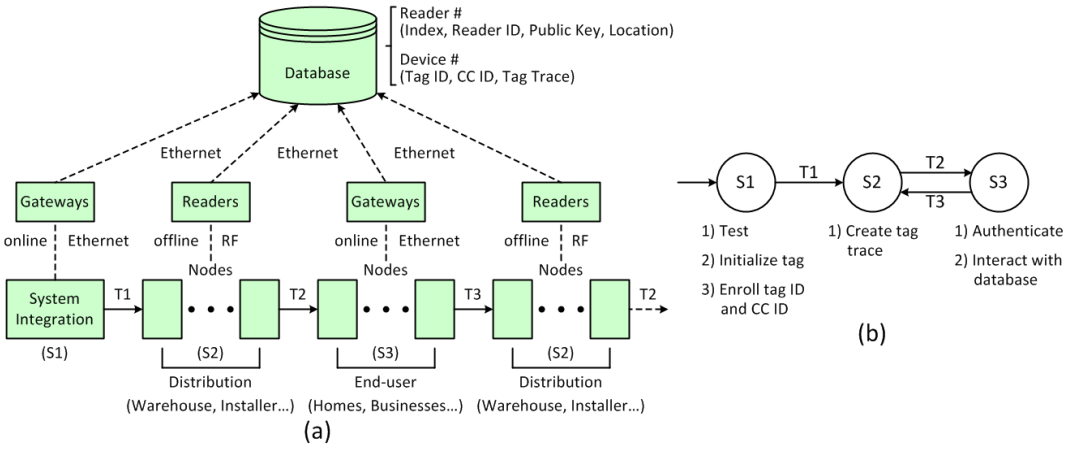

Fig. 1: (a) Supply chain with transition points and (b) State transition graph.

S1. System Integration This state is essentially the start of the network device's life and occurs in a trusted environment. The assumption that manufacturers of RFID tags or system integrators of RFID-enabled devices can be trusted is ubiquitous and has been explicitly or implicitly stated in literature [7, 25, 40]. Functional and reliability testing will be performed to ensure both hardware and software work as expected. Initialization steps are also finished and would include extracting tag identities (*tagIDs*) and control chip identities (*CC IDs*) from RFID tags and control chips separately and storing them in the centralized database. All this information will be used later to track network devices as they move through the supply chain and verify their identities. Network devices would eventually move into the next states which are untrusted (susceptible to attacks). We refer to this as transition T1.

S2. Distribution In this state, network devices are stored in inventories and transported between supply houses, distributors, retailers, and installers. In an RFID-enabled supply chain, network devices can be tracked using an *offline* (unplugged and disconnected from the network) mode. Tags are powered by the readers and communicate their authentication information (more in Section 4). RFID readers on the distribution path will jointly create a unique tag trace that is stored in the tag memory. When the RFID readers are connected to the network, they can store backups of the current tag trace in the database. Note that each reader can process many network devices almost at the same time [34]. To address the shortcomings of existing protocols as mentioned in Section 2, a more secure and practical tag trace enrollment and validation procedure will be presented in Section 4. Since the communication with RFID tag is done only by readers in the distribution and the devices are unplugged, we refer to this as *offline* mode.

S3. End-user Eventually, network devices will be installed in the homes or businesses of end-users. We refer to this as transition T2. In this state, the network device will interact over encrypted Ethernet with the centralized database. Since this occurs when the network device is powered in the home or business and operates over cable or wireless WiFi, we refer to this as *online* mode. Authentication procedures (i.e., verification of the matching between tag and device, and validating tag trace) will be performed before network service is available. In more general supply chains, the track-and-trace process would end here. However, in the supply chain for many network devices, the process should continue for several reasons. First, most network devices such as set-top boxes and routers will eventually be returned to network service providers and may re-enter the distribution state. We would refer to this as transition T3 in our notation. Second, some network devices (e.g., stolen devices, expensive devices whose tags have been replaced with tags of much cheaper devices, etc.) may fail the authentication process and have to be recalled. Hence, an improved supply chain management and traceability system would include features to handle tracking at the edges and from edges back to distribution.

3.2 Attack Models

In order to evaluate the security of an RFID-enabled supply chain system, we define some practical attacks in this subsection.

1. Cloning tag ID: Rogue elements place cloned tags on fake products so as to escape inspection of RFID-based counterfeit detection systems. One main feature of this type of attack is that more than one device will carry tags with exactly the same identity, although those tag identities are indeed recorded in the centralized database.

2. Duplicating tag trace: Untrusted entities in the supply chain (e.g., installers) duplicate valid tag traces and store the copies in the tag memories of stolen products so as to spoof authentication of server when the network devices are installed in the homes or businesses of end-users. One main feature of this type of attack is that more than one device will carry tags with exactly the same trace.

3. Denial-of-service attack: Malicious readers overwrite the tag memory so that the compromised tag cannot authenticate itself to the authorized readers on its distribution path.

4. Replay attack: Rogue elements eavesdrop on the communication between the authorized reader and the legal tag, intercept the authentication code sent by the legal tag, and replay the authentication code to the authorized reader to obtain copies of reader updates.

5. Man-in-the-middle attack: Rogue elements intercept the authentication code sent by the legal tag to the authorized reader, change the tag identity contained in the authentication code to any other wanted tag identity, and send the forged authentication code to the authorized reader to obtain reader update associated with that specific tag identity.

3.3 ReSC Hardware Architecture and Constraints

Figure 2 illustrates the hardware architecture of ReSC, including the entities involved and their connections. Central to our approach are two new features: i) the RFID tag and the control chip are bound together with a one-to-one mapping to prevent potential split attacks; ii) tag identity, control chip identity, and tag trace can be sent to the database for authentication over encrypted Ethernet. The constraints of the entities are described as follows:

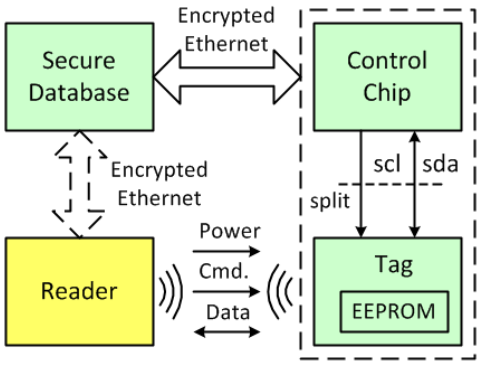

Fig. 2: ReSC hardware architecture.

Database: One centralized database stores reader information (i.e., index, identity, public key, location, etc.), tag information (i.e., identity, tag trace, etc.), and device information (i.e., control chip identity, one-to-one mapping between tag and device, etc.). Database can authenticate readers based on their secret identities (would not be transmitted in plaintext). Database can also authenticate devices based on authentication procedures to be discussed in Section 4. We assume that the database could inform the readers of their preceding readers for each tag in the supply chain, which is also assumed in other literature [24, 41, 42]. This is a fair assumption especially for the supply chain of network devices since its topology is relatively fixed and there are usually limited number of owners, manufacturers, and distributors involved.

RFID Reader: Readers are dispersed at different stages of the supply chain. Readers can jointly create a unique tag trace and store that trace in the tag memory in a secure fashion. To be specific, readers at different locations will write their own signatures (protected by cryptographic hash functions) to the tag memory to make up a unique tag trace. If necessary, the RFID reader could communicate with the database via Ethernet channel to store or retrieve the backup of tag trace. It is a fair and popular assumption that the readers are networked in the RFID-based supply chain solutions [7, 24, 40]. We assume the communication between database and readers is secure and protected by a strong protocol (e.g., transport layer security (TLS) protocol [2, 9]).

RFID Tag: Every tag has a tag memory storing tag identity and tag trace. The size of tag memory is typically several kilo bits. Generally speaking, low-cost RFID tags are not equipped to resist physical tampering. The RFID tag communicates with the RFID reader via RF channel.

Control Chip: The start-up signature (SRAM PUF) of embedded SRAM inside the control chip will be captured and used as its identity. Each SRAM cell consists of two cross-coupled CMOS inverters and two access transistors. Depending on the mismatch between the transistors, each SRAM cell produces a zero or a one after powering up the circuit. Larger mismatch leads to a more stable zero/one output for some SRAM cells. A number of such stable SRAM cells defines the output of the SRAM PUF. The SRAM PUF will be used to authenticate the control chip when the network device is installed at the end-user. The control chip communicates with the RFID tag via I2C channel [32] on board. The connection between the RFID tag and the control chip allows the control chip to read out tag trace and transmit the trace to the database for authentication in *online* mode (plugged and connected to the network). We also assume the communication between database and network devices is secure and protected by a strong protocol (e.g., transport layer security (TLS) protocol [2, 9]).

4 Authentication

Overall, the authentication procedure of ReSC can be split into two phases: (i) verification of the matching between the tag identity (*tagID*) and the control chip identity (*CC ID*); and (ii) verification of the integrity of tag trace to make sure that the network device has passed through the valid supply chain before arriving at the end-user.

4.1 ReSC I: Tag Matching with Device

At the system integration stage, the control chip identity (*CC ID*) will be generated from the start-up signature (SRAM PUF) of embedded SRAM inside the control chip. The control chip identity together with the tag identity will compose a 2-tuple (*CC ID*, *tagID*) and is stored in the centralized database in *online* mode for future device authentication. The communication between the control chip and the database is assumed protected by cryptographic protocols such as TLS [9]. Potential split attacks can be detected since we bind the RFID tag and the network device together with the one-to-one mapping between the tag identity and the control chip identity. Even if the attacker could probe the I2C channel [32], intercept the packets being transmitted between the tag and the control chip, and program them into the cloned tag, we can still detect this type of eavesdropping since the tag identity stored in the tag memory only matches one specific control chip identity (which is never communicated in plaintext). The tag memory includes two parts: one unique, read-only tag identity and one unique tag trace composed of the signatures of readers on the distribution path of that tag.

4.2 ReSC II: Valid Tag Trace

We define a tag trace as valid when it carries all the necessary signatures of authorized readers on its distribution path. When the network device is distributed in the supply chain, the RFID readers dispersed at different locations will join up to compose a unique tag trace and store that trace in the tag memory. The contents of tag memory include a static read-only tag identity and a unique tag trace composed of the signatures of readers on the tag's distribution path. We assume that the system integrator can be trusted and will perform the tag initialization (i.e., assigning an initial signature ($SIGN_0$)). We also assume that each reader (R_i) knows the public key (pk_{i-1}) of the reader (R_{i-1}) at the previous stage. This is a fair assumption since all the public keys of readers could be uploaded to the cloud and shared among them. The centralized database can also look up the public key (pk_i) of each reader (R_i) using the index ($Index_i$) of that reader. Public key cryptography based digital signature technique (e.g., Merkle signatures [5], Rabin signatures [33], GMR signatures [15], etc.) is used to generate reader's signature. Figure 3 illustrates our proposed light-weight RFID protocol with cyclic redundancy check (CRC) and XORing with random numbers omitted for brevity of expression. The entire communication flow between RFID reader and RFID tag can be divided into the following three steps:

Step 1: When the network device arrives at the next intermediate stage, the reader R_i at that stage will first issue a *Query* command to the tag.

Step 2: After receiving the *Query* command, the tag will reply with its identity (*tagID*) and current authentication code

$$SIGN_{i-1} = H_{sk_{i-1}}(tagID||Index_{i-1}||timestamp_{i-1}) \tag{1}$$

where $Index_{i-1}$ is the index associated with the $(i-1)_{th}$ reader, $timestamp_{i-1}$ denotes the specific time when reader R_{i-1} updated the tag, $||$ indicates the concatenation operation, and $H_{sk_{i-1}}(X)$ indicates encrypted hash value of input argument X using sk_{i-1} as private key of reader R_{i-1}. Note that $timestamp_{i-1}$ and $Index_{i-1}$ which are contained in the tag's memory will also be sent to verify the hash in the next step.

Step 3: After receiving the quad ($SIGN_{i-1}$, $tagID$, $Index_{i-1}$, $timestamp_{i-1}$), the reader R_i will decrypt $SIGN_{i-1}$ with the public key pk_{i-1} of reader R_{i-1}, and recover the hash value of $tagID||Index_{i-1}||timestamp_{i-1}$. Simultaneously, the reader R_i will generate the hash value of $tagID||Index_{i-1}||timestamp_{i-1}$ locally. By comparing these two hash values, the reader R_i can authenticate the tag. If these two match, the reader R_i will generate its own signature $SIGN_i$ by encrypting the hash value of $tagID||Index_i||timestamp_i$ with its private key sk_i and send the triple ($SIGN_i$, $Index_i$, $timestamp_i$) to the tag to update the tag trace. However, if the old signature fails the verification or there is no old signature stored in the tag memory, the tag may be impersonated or compromised by a rogue reader. The reader R_i will then communicate with the centralized database to determine whether the tag with that specific tag identity has been authenticated at the previous stage. If yes, the reader R_i will extract backup from the centralized database and send the backup to the tag to recover the compromised tag memory contents; otherwise, the reader R_i will simply flag that device as suspicious and report an event to the centralized database. Note that if the old signature passes the verification, the reader R_i does not need to communicate with the centralized database in real-time. Instead, the reader R_i can let the centralized database know that the tag carrying one specific tag identity has passed its authentication when the reader is not busy. The reader signature update process will utilize a wraparound fashion and the tag memory will be regarded as a circular buffer storing 10 reader signatures, which can prevent the tag memory from overflowing.

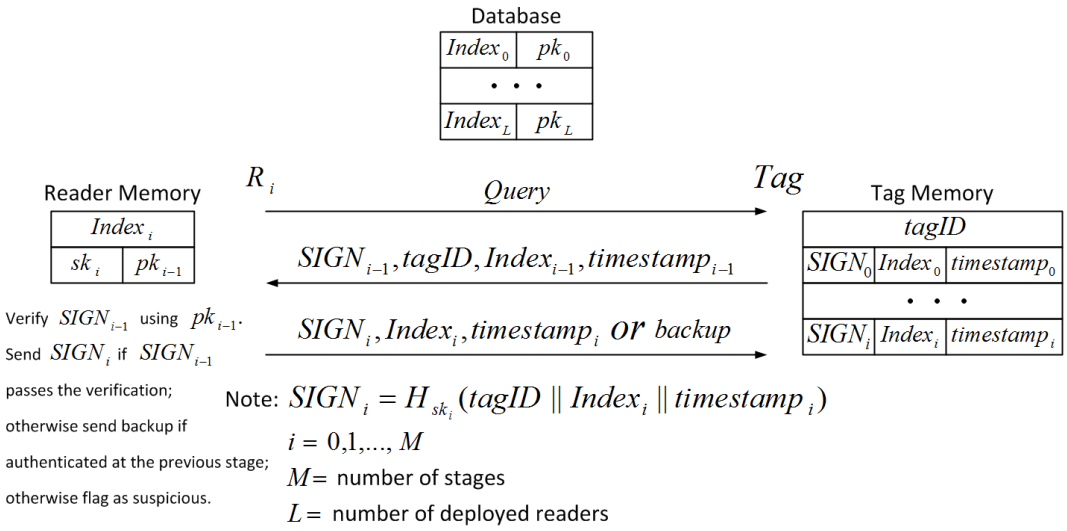

Fig. 3: Light-weight RFID protocol.

The above process of updating tag traces has several useful features. The *timestamp* can prevent attackers from replaying a proper supply chain trace in a stolen device's tag. It can also be useful for forensics. For example, if a rogue employee uses an authorized reader to update a stolen device, we can catch him or her since the *timestamp* embedded in the reader's signature could indicate who is on duty at that time. The reader R_i can read out the incomplete tag trace from the tag memory and send the tag identity (*tagID*) associated with its trace to the centralized database for backup. The reader R_i can also retrieve the backup of tag trace from the centralized database to recover the compromised tag trace in the tag memory.

When the network device is installed at the end-user, the control chip will read out the chain of readers' signatures from the tag memory and transfer it to the centralized database for validation in *online* mode. The database has stored the correct supply chain trace (associated with each tag). It will use the index $Index_i$ of each reader to look up its public key pk_i and then validate the signature $SIGN_i$ using that public key pk_i. If the chain of readers' signatures is incomplete or does not match the expected trace (stored in the database), the service request from the suspicious network device will be rejected by the server.

4.3 Authentication at the End-user

The authentication at the end-user involves the following two steps: (i) the control chip authenticates itself to the centralized database based on its identity; and (ii) the control chip reads out the contents of tag memory (i.e., tag identity and tag trace), encrypts them, and transmits them to the centralized database for validation. Both steps are performed in *online* mode. This second step can ensure not only that the device has passed through the legal supply chain (as described above) but also that the tag is genuine and bound to that specific device. Service is only available to the end-user after all the authentication procedures (i.e., tag matching with device, valid tag trace including all the necessary signatures of authorized readers on the distribution path, etc.) are passed. This shall prevent stolen

and/or counterfeit products from being used; making them worthless. The authentication procedures can also be performed in retail stores before purchase.

5 Implementation

A PCB prototype has been designed and fabricated to prove the concept of ReSC. In this section, we will briefly introduce the implementation of ReSC prototype. First, we introduce the ICs contained on ReSC prototype and the connections between them. Next, we discuss the PCB slot antenna design to ensure that: (i) it can generate enough bandwidth at the operating frequency specified by the EPC C1G2 standard [21] to guarantee proper communication between the RFID reader and tag; (ii) it can transfer enough power from the RFID reader's RF waves to finish read/write operations towards the RFID tag.

5.1 ICs and Connections between Them

Texas Instruments' (TI's) microcontroller (MCU) MSP430F247 is used as the control chip in the ReSC prototype. We choose one of TI's MSP430 family of microcontrollers because of their popularity, small footprint area, and low power consumption. ReSC itself does not have any special requirements towards the control chip being used so long as it has a large enough embedded SRAM and supports communication with RFID tag. The start-up signature of $4KB$ SRAM embedded inside MSP430F247 is utilized to generate control chip identity. NXP Semiconductors' UCODE I2C SL3S4021 is used as the RFID tag in the ReSC prototype. A 96-*bit* tag identity ($tagID$) including a 48-*bit* unique serial number is used to uniquely identify each tag. It is stored in the locked memory and cannot be tampered by the attacker. The 3328-*bit* user memory is used to store tag trace. I2C channel (serial clock and serial data) [32] is used to connect the control chip and the RFID tag. TI's TPS77601 is used as the voltage regulator to provide stable 3.3V power supply to the control chip and RFID tag in *online* mode. π section filters composed of capacitors and ferrite beads are used to suppress power supply noise in the ReSC prototype. GMR signature scheme [15] is used to generate reader's signature. We assign 20 $bits$ for each index which could mark 1 $million$ readers. We assign 40 $bits$ for each timestamp in the format of yymmddhhmm (i.e., year:month:day:hour:minute). The bit-width of signature depends on the selected signature scheme. For GMR signatures, 10 readers can be visited before the tag's memory is full. To overcome this limitation, the reader signature update process will utilize a wraparound fashion and the tag memory will be regarded as a circular buffer storing 10 reader signatures. Figure 4(a) shows the PCB prototype layout.

5.2 PCB Antenna Design

For the sake of reducing cost and saving assembly space, a PCB slot antenna instead of a discrete antenna component is used in the ReSC prototype. The impedance of the PCB antenna should be matched conjugately to the input impedance of RFID tag chip in order to eliminate the need for matching network and sustain the power supply for RFID tag. Figure 4(b) shows our PCB antenna design and its return loss obtained using the simulation tool Ansoft HFSS 14.0. The PCB antenna arms should be symmetrical to achieve prime performance. FR4 is the dielectric material employed and its thickness is set to $0.5mm$. The PCB antenna impedance is designed to be $12.7 + j199Ohm$ in our prototype. The resonance frequency and $-10dB$ bandwidth are $910MHz$ and $522MHz$ respectively. Simulation results demonstrate that the PCB slot antenna is sufficient to provide enough

$-10dB$ bandwidth at the operating frequency. Further, at the wave valley point ($910MHz$) the vast majority of input power is absorbed by the antenna and only a tiny part is reflected back. Therefore, there will be enough power provided to the tag when the ReSC system is in *offline* mode.

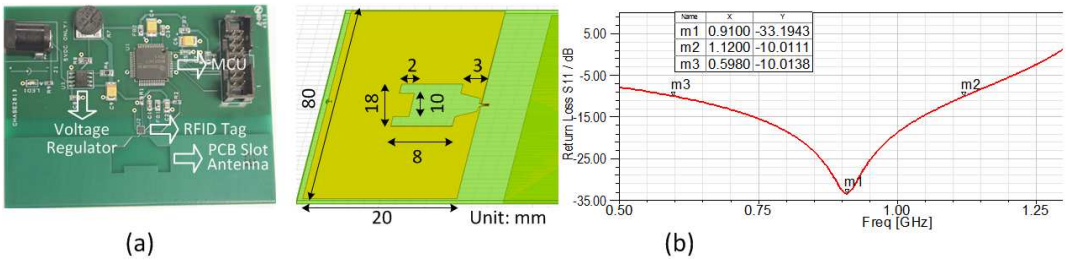

Fig. 4: (a) PCB prototype layout and (b) PCB antenna design and its return loss.

6 Evaluation

In this section, we evaluate the performance and security of ReSC via experiments and theoretical analysis. Experimental results are based on a PCB prototype implementation. Afterwards, we compare ReSC with prior work in terms of overhead and security.

6.1 Performance Evaluation

In this subsection, we evaluate the performance of ReSC in two phases (ReSC I and ReSC II as discussed in Section 4). For ReSC I, we verify the quality of control chip identity (SRAM PUF) in terms of uniqueness. Since tag identity is nothing more than a bitstream stored in the read-only memory block, the issue of uniqueness will not occur and thus there is no need to verify its quality. Discussion on reliability issue is out of the scope of this paper. For ReSC II, we evaluate the performance of ReSC in terms of RF communication efficiency.

Performance of ReSC I The essence of ReSC I is the matching between tag identity and control chip identity. Since tag identity is not faced with the issue of uniqueness, we only consider the quality of control chip identity here. The start-up signature (SRAM PUF) of embedded SRAM inside the control chip is used as its identity. Two bit selection algorithms, random bit selection and neighborhood analysis based bit selection [18, 39], are respectively employed to pick up the candidate bits for control chip identity from all the stable bits at enrollment phase.

Four prototype boards are employed to analyze the uniqueness of control chip identity. For each board, the entire $4KB$ embedded SRAM is divided into 9 blocks. Each block has the same size (416 *bytes*) and will be used to work as a 128-*bit* identity. Thus, 36 128-*bit* identities will be generated to evaluate the uniqueness of control chip identity. Figure 5 illustrates the hamming distance (HD) distributions of control chip identities based on random bit selection and neighborhood analysis based bit selection respectively. Hamming distance distributions based on both bit selection algorithms appear Gaussian. Both distributions pass the Chi-square goodness-of-fit test at the 5% significance

level. The mean values of hamming distances for both bit selection algorithms are 63.8317 (49.87%) and 63.8381 (49.87%) respectively. Both average inter-die HDs are quite close to the ideal value 64 (50%) out of 128. Experimental results demonstrate that the embedded SRAM PUF is effective at identifying boards.

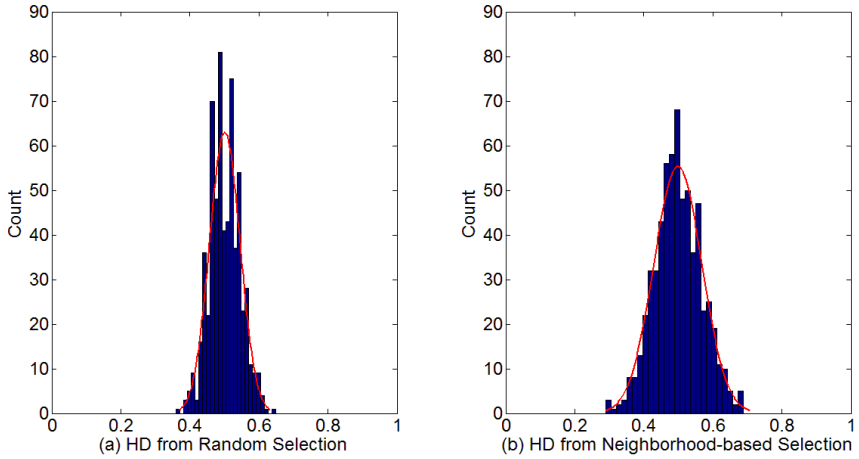

Fig. 5: Hamming distance distributions of control chip identities.

Performance of ReSC II The essence of ReSC II is the composition process of unique tag trace based on the signatures of readers at different locations. We evaluate the RF communication efficiency by performing tag access using an actual RFID reader to ensure that the tags can be updated promptly in the supply chain and the tag trace composition process can function correctly. Our experimental platform is set up as shown in Figure 6(a). Figure 6(b) shows the RF communication efficiency. When the reading distance is smaller than 4 meters, the reading rate is larger than $50 reads/sec$, which indicates that the RFID reader can finish reading 50 boards per second. No bit error occurs throughout our experiments. Experimental results demonstrate that the RF communication between the RFID reader and the RFID tag is effective and efficient for implementing track-and-trace in the supply chain.

6.2 Security Evaluation

In addition to the attack models discussed in Section 3.2, several other attacks/risks are also considered in this subsection to perform a comprehensive security evaluation. Table 1 lists the potential system-level attacks/risks associated with general RFID-based systems (including ReSC) and corresponding mitigation methods. We divide all the potential attacks/risks into five categories in terms of attack targets and discuss them respectively. We don't consider sophisticated physical attacks [20] here.

RFID tag: By binding the RFID tag and the identified network device together with a one-to-one mapping between tag identity (*tagID*) and control chip identity (*CC ID*), cloning tag ID can

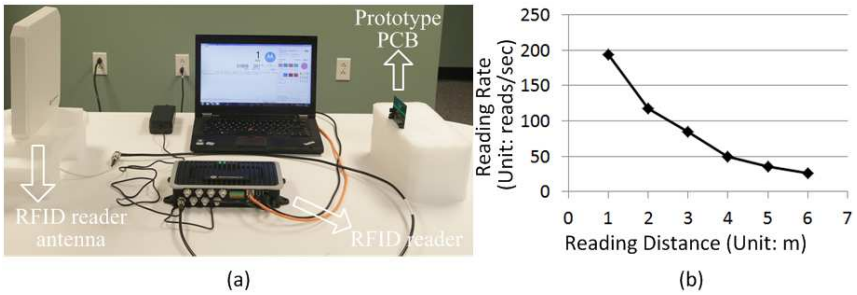

Fig. 6: (a) Experimental setup for evaluating RF performance and (b) RF communication efficiency.

be detected and service request will be rejected by the server when the cloned network device is installed at the end-user. Since the tag trace of ReSC depends on both reader information (i.e., reader's index and private key), tag information (i.e., tag identity), and the specific time (i.e., *timestamp*) when the tag trace is updated, it is unique for each device and thus is resistant to duplication attack (duplicating tag trace by untrusted entities involved in the supply chain). When a rogue employee uses an authorized reader to update a stolen device, we can catch him or her since the *timestamp* embedded in the reader's signature could indicate who is on duty at that time. Although spoofed reader could overwrite or compromise tag trace stored in the tag memory to perform denial-of-service attack, this type of tampering can be detected by the reader at the next stage. We can restore the compromised tag trace by retrieving backup from the database when the reader is connected to the network. Protecting tag privacy [4] is out of the scope of this paper.

Control chip: Illegal substitute of control chip (i.e., replacing original control chip with a counterfeit/tampered IC) can be detected with unclonable control chip identity (SRAM PUF).

Network device: Stolen network devices can be detected since their tag traces are either incomplete or fake and will fail the tag trace validation procedure.

RF channel: Sensitive information (e.g., reader's private key) is never transmitted in clear and thus is resistant to eavesdropping. Replay attack described in Section 3.2 can be prevented since reader update (i.e., new signature generated by current reader) is generated based on one specific tag identity and cannot be simply duplicated to be used for another tag. To be specific, even if the adversary could eavesdrop on the RF channel, intercept the tag authentication codes (see Section 4.2) sent by legal tags, and replay the tag authentication codes to authorized readers to obtain copies of reader updates. The freshly generated readers' signatures are computed based on the identities of tags under attack and cannot be simply used for counterfeit tags with different identities. In the worst case, even if the adversary performs replay attack and tag ID cloning simultaneously, the copies of reader updates obtained by replay attack could match the cloned tag identities. Those cloned tag identities would not match the control chip identities. ReSC is also resistant to man-in-the-middle attack described in Section 3.2 since the tag authentication code is bound to one specific tag identity and would not match another tag identity. Specifically, when the adversary intercepts the authentication code sent by the legal tag to the authorized reader, changes the tag identity contained in the authentication code to any other wanted tag identity, and sends the forged authentication code to the authorized reader to swindle reader update associated with that wanted tag identity, the forged authentication code will fail the verification by the authorized reader since it does not match the provided tag identity.

RFID reader: Spoofed tags usually originate from an illegal channel and cannot include valid signatures of previous readers. We can detect spoofed tags by verifying the old signatures stored in the tag memory.

Table 1: System level security evaluation

Attack target	Attack approach	Mitigation
RFID tag	1. Cloning tag ID 2. Duplicating tag trace 3. Denial-of-service attack	1. One-to-one mapping between tag identity and control chip identity. 2. Tag trace is unique to each device and generated based on the tag identity. 3. i) The compromised tag trace can be detected by the reader at the next stage. ii) Backup the tag trace when the reader is connected to the network.
Control chip	Replacing the original chip with an illegal substitute (e.g., a counterfeit IC).	Unclonable control chip identity (SRAM PUF).
Network device	Stealing devices from inventories or shelves.	Verification of the integrity of tag trace.
RF channel	1. Eavesdropping 2. Replay attack 3. Man-in-the-middle attack	1. Sensitive information (e.g., reader's private key) is never transmitted in clear. 2. Reader update is generated based on one specific tag identity and cannot be simply duplicated to be used for another tag. 3. The tag authentication code is bound to one specific tag identity.
RFID reader	Spoofed tag	Authenticate tag by verifying the old signatures stored in the tag memory.

6.3 Comparison with Prior Work

In this subsection, we compare ReSC with prior work in terms of overhead and security. Table 2 compares ReSC with several famous RFID-based techniques in terms of overhead. Table 3 compares ReSC with those techniques in terms of anti-attack capability. Different from tailing mechanism [24, 41, 42], ReSC can verify tag trace without requiring that reader be connected to the database. As a tradeoff, ReSC has to store more authentication information in the tag memory. For ReSC, the tag traces are mostly validated at the end-user. Different from the other three techniques, ReSC prevents tag cloning by binding the tag identity to the unclonable control chip identity. ReSC can address more attacks with a relatively smaller overhead. Among these four approaches under comparison, ReSC is the only one that can prevent counterfeit or stolen products from being used by end-users.

Table 2: Overhead comparison

Metrics	Tailing [41]	Jeongkyn et al. [40]	Hung-Yu et al. [7]	ReSC
# of Hash Operations	0	$2N+2$	0	1
# of Keyed Hash Operations	0	2	0	1
# of RNG Operations	1	1	6	0
# of Encryptions	0	1	0	1
# of Decryptions	0	1	0	1
# of Messages	4	5	5	3
Required Tag Memory Size	$M \times symbol + pointer + tagID$	*SN+ID+2 keys*	*EPC + 2 keys*	$M \times (SIGN + Index + TS) + tagID$
Extra Tag Circuit	*No*	*Yes*	*No*	*No*
Real-time Interaction with DB	*Yes*	*Yes*	*Yes*	*No*
Exhaustive Search in DB	*No*	*Yes*	*Yes*	*No*

Note: 1. M stands for the number of stages on the distribution path.
2. N stands for the number of issued tags.
3. Extra tag circuit indicates the primitive not supported by EPC C1G2.
4. SN: serial number, EPC: electronic product code, and TS: timestamp.

Table 3: Security comparison

Attacks	Tailing [41]	Jeongkyn et al. [40]	Hung-Yu et al. [7]	ReSC
Removing tag	√	√	√	√
Swapping tags	×	×	×	√
Cloning tag ID	√	√	×	√
Forging tag	√	√	√	√
Cloning tag ID + Duplicating tag trace	×	−	−	√
Tracking tag location	×	√	√	×
Spoofed reader	×	√	√	√
Illegal chip replacement	×	×	×	√
Product theft	×	×	×	√
Eavesdropping	×	√	×	√
Replay attack	×	√	√	√
Denial-of-service attack	×	√	√	√
Spoofed tag	×	√	√	√

7 Conclusion

In this paper, we have presented an RFID-enabled Supply Chain (ReSC) solution that addresses the security and management issues of network devices in the supply chain. The practical effectiveness of ReSC system has been verified through simulations, theoretical analysis, and experimental results. Compared with existing approaches, ReSC has the following merits: (1) By binding the RFID tag and the identified device together with a one-to-one mapping, potential split attacks (i.e., separating tag from product, swapping tags, etc.) can be detected; (2) By combining two techniques (i.e., one-to-one mapping between tag identity and control chip identity, and unique tag trace composed of signatures of readers on the distribution path) together, this system is resistant to counterfeit injection, product theft, and illegal network service access; (3) The fabrication cost is quite low since the vast majority of components (e.g., voltage regulator, control chip with embedded SRAM, etc.) in this design already exist in many modern network devices.

References

1. ANGELES, R. RFID Technologies: Supply-chain Applications and Implementation Issues. *Information Systems Management 22*, 1 (2005), 51–65.
2. ARMKNECHT, F., GASMI, Y., SADEGHI, A.-R., STEWIN, P., UNGER, M., RAMUNNO, G., AND VERNIZZI, D. An Efficient Implementation of Trusted Channels based on OpenSSL. In *Proceedings of the 3rd ACM workshop on Scalable trusted computing* (New York, NY, USA, 2008), STC '08, ACM, pp. 41–50.
3. ASIF, Z. Integrating the Supply Chain with RFID: a Technical and Business Analysis. *Communications of the Association for Information Systems 15*, 1 (2005), 24.
4. AVOINE, G. Privacy Challenges in RFID. In *Data Privacy Management and Autonomous Spontaneus Security*. Springer, 2012, pp. 1–8.
5. BUCHMANN, J., GARCÍA, L. C. C., DAHMEN, E., DÖRING, M., AND KLINTSEVICH, E. CMSS–an Improved Merkle Signature Scheme. In *Progress in Cryptology-INDOCRYPT 2006*. Springer, 2006, pp. 349–363.
6. CARBONE, J. Most Counterfeit Parts Involve Obsolete Semiconductors and Other EOL Components. *The Source* (Aug. 2012).
7. CHIEN, H.-Y., AND CHEN, C.-H. Mutual Authentication Protocol for RFID Conforming to EPC Class 1 Generation 2 Standards. *Computer Standards & Interfaces 29*, 2 (2007), 254–259.
8. DEVADAS, S., AND YU, M. Secure and Robust Error Correction for Physical Unclonable Functions.

9. DIERKS, T. The Transport Layer Security (TLS) Protocol Version 1.2.
10. EKINCI, Y., EKINCI, O., AND GIINAYDIN, U. The Application of UHF Passive RFID Technology for the Effectiveness of Retail/Consumer Goods Supply Chain Management. In *RFID Eurasia, 2007 1st Annual* (Sep. 2007), pp. 1–6.
11. EVANS, D. The Internet of Things: How the Next Evolution of the Internet Is Changing Everything. *CISCO white paper 1* (2011).
12. FREIGHTWATCH INTERNATIONAL SUPPLY CHAIN INTELLIGENCE CENTER. 2013 Global Cargo Theft Threat Assessment, 2013.
13. GASSEND, B., CLARKE, D., VAN DIJK, M., AND DEVADAS, S. Silicon Physical Random Functions. In *Proceedings of the 9th ACM conference on Computer and communications security* (2002), ACM, pp. 148–160.
14. GAUKLER, G. M., SEIFERT, R. W., AND HAUSMAN, W. H. Item-Level RFID in the Retail Supply Chain. *Production and Operations Management 16*, 1 (2007), 65–76.
15. GOLDWASSER, S., MICALI, S., AND RIVEST, R. L. A Digital Signature Scheme Secure Against Adaptive Chosen-message Attacks. *SIAM Journal on Computing 17*, 2 (1988), 281–308.
16. HANCKE, G. P. RFID and Contactless Technology. In *Smart Cards, Tokens, Security and Applications*. Springer, 2008, pp. 295–322.
17. HOLCOMB, D., BURLESON, W., AND FU, K. Power-Up SRAM State as an Identifying Fingerprint and Source of True Random Numbers. *Computers, IEEE Transactions on 58*, 9 (Sept 2009), 1198–1210.
18. HOSEY, A., RAHMAN, M., XIAO, K., FORTE, D., TEHRANIPOOR, M., ET AL. Advanced Analysis of Cell Stability for Reliable SRAM PUFs. In *Test Symposium (ATS), 2014 IEEE 23rd Asian* (2014), IEEE, pp. 348–353.
19. HUANG, H.-C., CHANG, F.-C., AND FANG, W.-C. Reversible Data Hiding with Histogram-based Difference Expansion for QR Code Applications. vol. 57, pp. 779–787.
20. HUTTER, M., MANGARD, S., AND FELDHOFER, M. *Power and EM Attacks on Passive 13.56 MHz RFID Devices*. Springer, 2007.
21. INC., E. EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz-960 MHz Version 1.2.0, May 2008.
22. JUELS, A., PAPPU, R., AND PARNO, B. Unidirectional key distribution across time and space with applications to rfid security. In *USENIX Security Symposium* (2008), pp. 75–90.
23. KUMAR, S. S., GUAJARDO, J., MAES, R., SCHRIJEN, G.-J., AND TUYLS, P. The Butterfly PUF Protecting IP on Every FPGA. In *Hardware-Oriented Security and Trust, 2008. HOST 2008. IEEE International Workshop on* (2008), IEEE, pp. 67–70.
24. LEHTONEN, M., OSTOJIC, D., ILIC, A., AND MICHAHELLES, F. Securing RFID Systems by Detecting Tag Cloning. In *Pervasive Computing*. Springer, 2009, pp. 291–308.
25. LEHTONEN, M. O., MICHAHELLES, F., AND FLEISCH, E. Trust and Security in RFID-based Product Authentication Systems. *Systems Journal, IEEE 1*, 2 (2007), 129–144.
26. LIVINGSTON, H. Couterfeit Incident Reporting Trends – 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/.
27. MAES, R., TUYLS, P., AND VERBAUWHEDE, I. Low-overhead Implementation of a Soft Decision Helper Data Algorithm for SRAM PUFs. In *Cryptographic Hardware and Embedded Systems-CHES 2009*. Springer, 2009, pp. 332–347.
28. MAITI, A., AND SCHAUMONT, P. Improved Ring Oscillator PUF: an FPGA-friendly Secure Primitive. *Journal of cryptology 24*, 2 (2011), 375–397.
29. MICHAEL, K., AND MCCATHIE, L. The Pros and Cons of RFID in Supply Chain Management. In *Mobile Business, 2005. ICMB 2005. International Conference on* (2005), IEEE, pp. 623–629.
30. MITCHELL, B. 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.

31. MUKHOPADHYAY, D., CHAKRABORTY, R. S., NGUYEN, P. H., AND SAHOO, D. P. Tutorial T7: Physically Unclonable Function: A Promising Security Primitive for Internet of Things. In *VLSI Design (VLSID), 2015 28th International Conference on* (2015), IEEE, pp. 14–15.
32. NXP SEMICONDUCTORS. I2C Bus Specification and User Manual, Apr. 2014.
33. RABIN, M. O. Digitalized Signatures and Public-key Functions as Intractable as Factorization. Tech. rep., DTIC Document, 1979.
34. ROBERTI, M. How Can an RFID Reader Interrogate Multiple Tags Simultaneously?, Sep. 2010. http://www.rfidjournal.com/blogs/experts/entry?7853.
35. ROCHOLL, J., KLENK, S., AND HEIDEMANN, G. Robust 1D Barcode Recognition on Mobile Devices. In *Pattern Recognition (ICPR), 2010 20th International Conference on* (Aug. 2010), pp. 2712–2715.
36. SCHRIJEN, G.-J., AND VAN DER LEEST, V. Comparative Analysis of SRAM Memories Used as PUF Primitives. In *Proceedings of the Conference on Design, Automation and Test in Europe* (2012), EDA Consortium, pp. 1319–1324.
37. TARIGULIYEV, Z., AND ORS, B. Reliability and Security of Arbiter-based Physical Unclonable Function Circuits. *International Journal of Communication Systems 26*, 6 (2013), 757–769.
38. WATERS, A. The Case of the Great Router Robbery, May 2011. http://resources.infosecinstitute.com/router-robbery/.
39. XIAO, K., RAHMAN, T., FORTE, D., TEHRANIPOOR, M., HUANG, Y., AND SU, M. Bit Selection Algorithm Suitable for High-Volumn Production of SRAM PUF. In *Hardware-Oriented Security and Trust (HOST), 2014 IEEE International Symposium on* (2014).
40. YANG, J., PARK, J., LEE, H., REN, K., AND KIM, K. Mutual Authentication Protocol. In *Workshop on RFID and Lightweight Crypto* (2005).
41. ZANETTI, D., CAPKUN, S., AND JUELS, A. Tailing RFID Tags for Clone Detection. In *Network and Distributed System Security Symposium* (2013).
42. ZANETTI, D., FELLMANN, L., AND CAPKUN, S. Privacy-preserving Clone Detection for RFID-enabled Supply Chains. In *RFID, 2010 IEEE International Conference on* (2010), IEEE, pp. 37–44.