

Copyright © 2010 The authors and IOS Press. Personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution to servers or lists, or to reuse any copyrighted component of this work in other works must be obtained from the authors and IOS Press.

This material is presented to ensure timely dissemination of scholarly and technical work. Copyright and all rights therein are retained by authors or by other copyright holders. All persons copying this information are expected to adhere to the terms and constraints invoked by each author's copyright. In most cases, these works may not be reposted without the explicit permission of the copyright holder.

Senthilkumar Chinnappa Gounder Periaswamy, Dale R. Thompson, Henry P. Romero, and Jia Di, "Fingerprinting radio frequency identification tags using timing characteristics," in *Proc. Workshop on RFID Security (RFIDsec'10 Asia)*, Singapore, Feb. 22-23, 2010, pp. 73-82.

Fingerprinting Radio Frequency Identification Tags Using Timing Characteristics

Senthilkumar CHINNAPPA GOUNDER PERIASWAMY ^{a,1}, Dale R. THOMPSON^a,
Henry P. ROMERO^b and Jia DI^a

^a*University of Arkansas, Fayetteville, USA*

^b*University of Colorado, Boulder, USA*

Abstract. Radio Frequency Identification (RFID) has been very actively developed as an identification technology in the last ten years. The uniqueness of RFID tag's electronic product code has made it to be used as an anti-counterfeiting feature for objects attached to it. However, currently the anti-counterfeiting properties of the tag themselves and methods to prevent counterfeiting of the tags have not been established. Here we propose a physical layer fingerprinting methodology that will improve the security of RFID tags.

Keywords. RFID, Security, Authentication, Anti-Counterfeiting

1. Introduction

Radio frequency identification (RFID) tags are devices that are used to uniquely identify objects that are attached to it. EPCglobal Class 1 Generation 2 is a widely used protocol for passive RFID systems that operates in the 860 - 960 MHz frequency (UHF) range [1]. An RFID reader identifies the tag by using the 96-bit electronic product code (EPC) of the tag. There is no method specified in the standard that prevents a duplicate tag from using the EPC of the original tag to authenticate itself as the original tag. The low cost and size that is driving the technology makes the implementation of conventional cryptographic security protocols a challenge.

In order to keep the cost low, the tags are produced with a high speed manufacturing process which introduces minor variations in the hardware components of the tag. We are using a measurement of those differences in the hardware to distinguish tags. These variations are difficult to reproduce, predict or control because this type of manufacturing focuses on mass-producing the tags at a lower cost. This method will provide an additional layer of security for authenticating RFID tags.

2. Background

The EPCglobal Class 1 Generation 2 is a reader-first-talk, half-duplex protocol. The process of a reader identifying a single tag in the system is illustrated in Fig. 1. The

¹ Corresponding Author.

reader starts the process of identifying a tag by sending a *select* command. The tag does not respond to the command but changes its state to respond to the following *query* command. The reader then sends the *query* command to which the tag responds with a random number. The reader asks the tag to send the identifying information by acknowledging the random number from that particular tag. When the tag receives the acknowledgment (*ack*), it sends the EPC, Protocol control (PC) and Cyclic redundancy check (CRC). If the reader receives the information without error, it acknowledges the receipt.

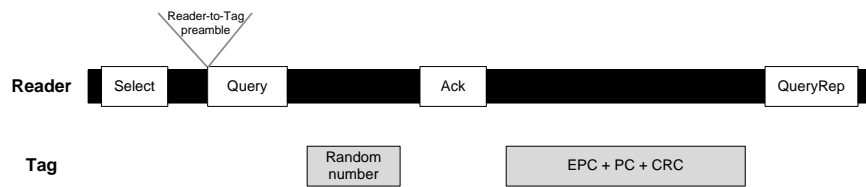


Figure 1. Reader - Tag Communication.

The reader sets the data rate of the tag-to-reader communication during the reader-to-tag preamble that precedes all *query* commands from the reader. The data rate remains the same for the entire session. The reader-to-tag preamble shown in Fig. 2 consists of a fixed-length start delimiter, a data '0' symbol, a reader-to-tag calibration symbol (*TRcal*) and a tag-to-reader calibration symbol (*TRcal*). The tag measures the length of the *TRcal* and uses it as the basis to determine the data rate of the tag-to-reader communication. The data rate for the FM0 encoding is calculated by dividing the *divide ratio* by the *TRcal*. The *divide ratio* is sent to the tag as a part of the query command based on the data rate required.

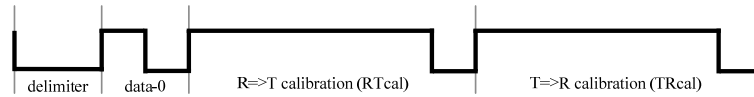


Figure 2. Reader-to-Tag preamble.

In this paper, we are using the differences in the measurement, storage, and usage of the *TRcal* value between tags to distinguish them. The differences are represented in the time required to transmit the EPC, PC and CRC.

3. Measurement

The communication signals between the RFID reader and RFID tags were captured using a Tektronix DPO70604 oscilloscope in our lab, which was a non-controlled radio frequency (RF) environment. The oscilloscope had a bandwidth of 6 GHz with a sampling rate of 25 Giga samples per second with maximum capture duration of 4 milliseconds at the highest resolution. A TagSense Micro-UHF reader was used to communicate with the tag. The reader was connected to a PC through an USB interface. This reader shown in Fig. 3 had a small form factor. A linear patch antenna

was connected to the reader to communicate with the tag. The antenna had a gain of 8 dBi.

We used this oscilloscope because the sampling rate will allow us to capture information at high resolution which was required for frequency features we were planning to analyze. However, we found that the timing feature discussed in this paper does not require such high resolution. Signals captured at a sampling rate of 25 Mega samples per second will provide enough resolution to extract the timing based features discussed in this paper.

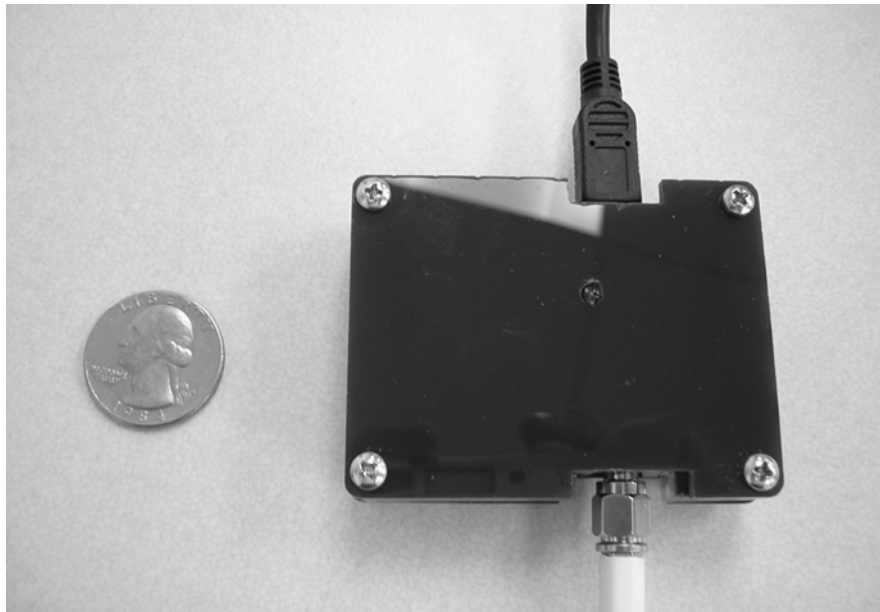


Figure 3. TagSense Micro-UHF RFID reader.

The antennas and tag were mounted to plastic stands such that they were at an elevation of 180 cm from the ground; this elevation from the ground reduced the interference caused by the reflection of RF signals. The setup had a free space of 0.5 meter around it. The frequency hopping of the reader was disabled and it was made to communicate with the tag at 915 MHz. RFID tags from three major manufacturers were used. They were entry-level passive tags with a cost of about six cents per tag. Tags from each manufacturer were taken from the same roll, which shows that they were manufactured at the same time. These models have already been deployed in both case level and item level RFID applications. We programmed all the tags with the same EPC, which was 300833b2ddd9048035050000. There was no specific reason in choosing this EPC; we just wanted all the tags to have the same EPC.

The captured communication between a reader and a single tag is shown in Fig. 3. We wanted to capture the communication between the tag and the reader such that the reader and the tag parts of the communication can be differentiated by their power level. This difference in tag to reader power was used as trigger to capture the tag communication. This enabled capturing tag communication without using a setup that

captures communication using the synchronization between the communicating reader and the capturing oscilloscope.

Each tag was measured six times initially. The tags were measured again six times after one week. The two sets were labeled *time1* and *time2* respectively. The tags were removed from the test fixture after *time1* measurements and stored. The tags were mounted again in the test fixture for the *time2* measurements. In all the measurements, the reader used double-sideband amplitude-shift keying (DSB-ASK) modulation with pulse-interval encoding (PIE) Type C encoding. The tags used ASK modulation with FM0 (bi-phase space) encoding.

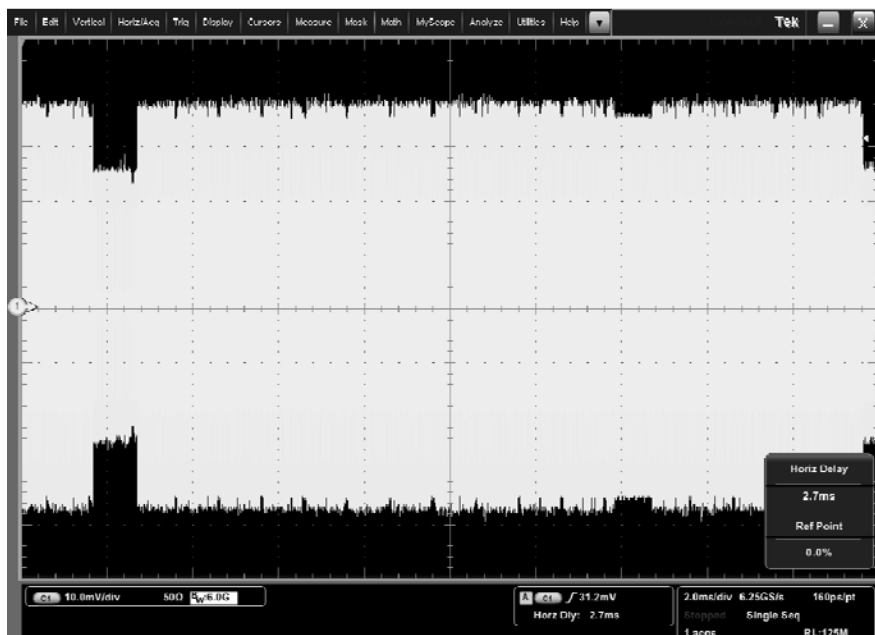


Figure 4. Reader to Tag Communication.

4. Tag Timing Response

The time required for the tag to send the EPC, PC and CRC to the reader was measured. This information was extracted from the captured signals using a MATLAB script. The script used the difference in the power level of the tag and reader communication to extract the information. The transmission time of the tags are shown in Fig. 5, Fig. 6 and Fig. 7.

K Nearest Neighbor algorithm (KNN) was used to classify the data. KNN is an instance-based classifier that classifies the current instance to the closest enrolled group by using a distance metric [2]. The classifier was trained on *time1* data which became the enrolled group. Then the classifier was used to classify the *time2* data which became the instance being classified. Tags from Manufacturer-1 were classified with a success rate of 98.44%. Manufacturer-2 tags were classified with a success rate of 96.25%. The success rate of Manufacturer-3 tags was 31.54%.

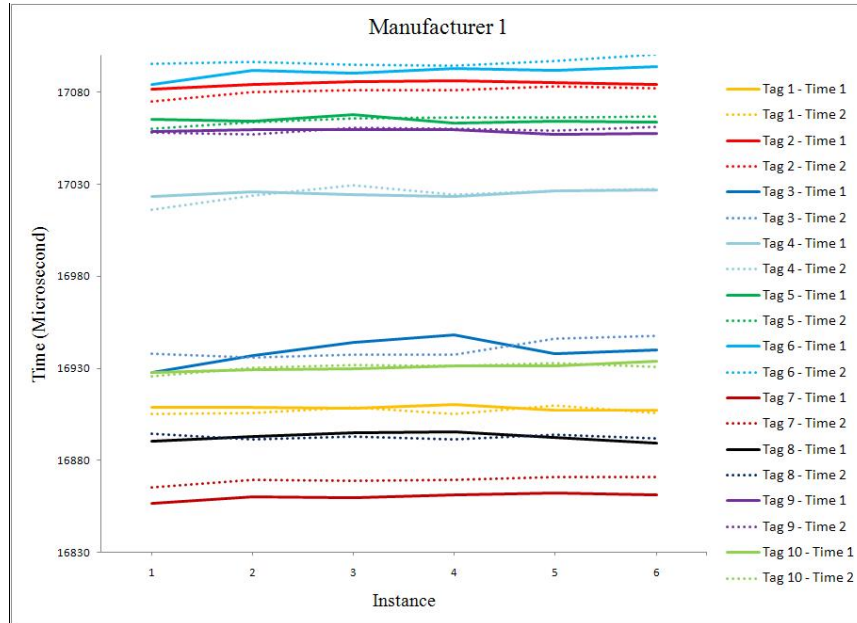


Figure 5. Tag timing response – Manufacturer 1.

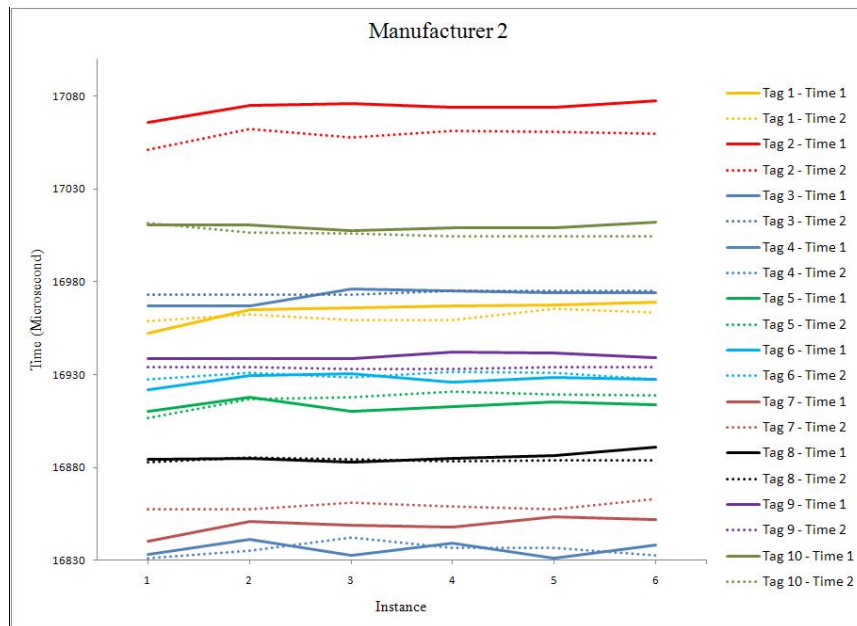


Figure 6. Tag timing response – Manufacturer 2.

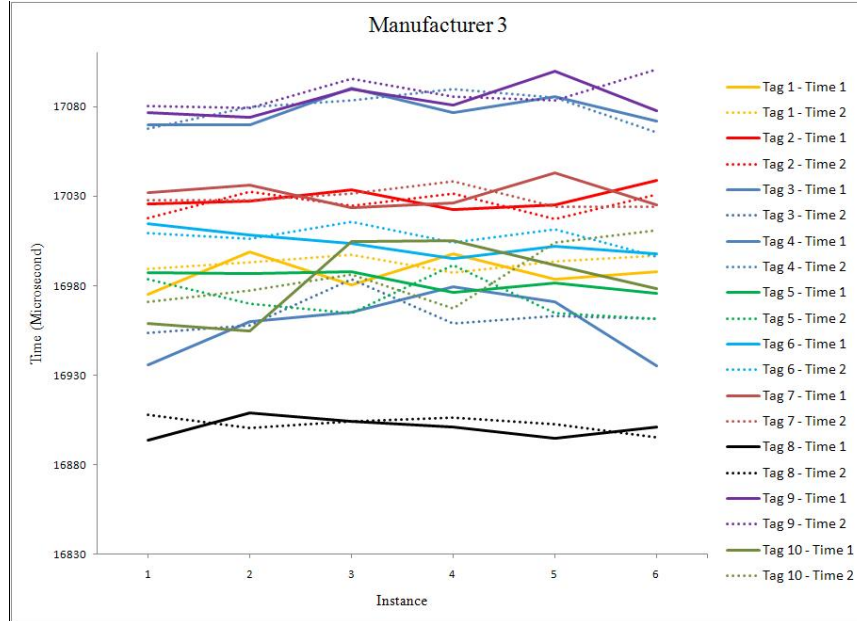


Figure 7. Tag timing response – Manufacturer 3.

Two of the tag manufacturers were repeatable and reproducible, and one manufacturer was not completely repeatable and reproducible. Investigating the behavior of manufacturer 3 tag is part of the future work. Having one manufacturer that was not repeatable leads us to believe that the final fingerprint will need multiple features, not just timing, and be ranked based on their reliability and performance.

The differences that occur during the measurement storage and the use of the TR_{cal} value by the tag leads to the differences in the length of the EPC, PC and CRC transmission. It can also be observed that the reader is using the same TR_{cal} and $divide\ ratio$ by observing that the measurements are reproducible for the same tag. Therefore, it is the differences in the interpretation and implementation of the TR_{cal} by the tag that produces the differences in length of the transmission.

The measurements show that the transmission time is between 16.8 milliseconds and 17.1 milliseconds which will lead to a small bandwidth and resolution when there are a larger number of tags in the system. The bandwidth and resolution can be increased when the length of the data sent from the tag is increased. Transmission of longer lengths like repeatedly sending the EPC multiple times could be done by using custom commands.

There is a possibility of adversaries building tags or circuits that can mimic the hardware feature but the feasibility of such an approach is an open research question.

5. Related Work

Several light weight cryptographic models [3-9] have been proposed to prevent unauthorized reading or cloning of tags. Although they may improve security and provide resistance to cloning after sufficient peer review [10], they face the possibilities

of attack through improper implementation, reverse-engineering [11], relay [12-14] and side-channel [15] attacks. Building a secure cryptographic protocol for a RFID tags which has only a couple of thousand gates dedicated for security is a challenge by itself, so providing an additional layer of security through hardware fingerprinting increases the reliability of the security mechanism.

Some manufacturers provide security using a unique Transponder ID (TID) for a controlled group of tags. TID is a number that is present in an Integrated Chip (IC) to identify their model and locate custom/optional commands they support. They are written in a Read Only Memory (ROM) when the tag is manufactured. Their purpose of identifying the manufacturing and specification details of the IC has been extended to identifying the RFID tag itself [16]. The TID was not created as a security feature but it is currently being used as one. This feature does not prevent an attacker from programming a non-programmed RFID tag or building a RFID tag emulator with the same TID information. Non-programmed RFID tags are currently not available in the market which may not be the case in the future [16]. Therefore, TID cannot be a reliable standalone anti-counterfeiting feature but can be used as one of the time buying and inexpensive options to prevent counterfeiting

A proposal to create a physical fingerprint of RFID tags using the initialization state of SRAM's in them was proposed in [17]. They used data from virtual tags to show that a SRAM can be used to uniquely identify tags. This research is closest to our work although it was done independently and simultaneously. The fingerprinting mechanism proposed in this paper is also based on variations that are caused due to the manufacturing process of the RFID tags. A difference between the work in [17] and our work is that their fingerprinting methodology has only been demonstrated in virtual tags and not in real tags. All of our features are measured from commonly used RFID tags without using any invasive methods.

The work in [18] investigates how RFID tags can be made unclonable by linking it to a Physical Unclonable Function (PUF). PUFs are physical structures that respond to challenges that are easy to measure but are hard to predict. In addition, PUFs are difficult to copy or clone. They are embedded in the tag such that any attempt to remove them will either destroy them or modify the values of the responses to challenges. The PUF only communicates with the chip of the tag and is inaccessible to the reader. Security protocols based on PUFs are used in [19]. PUF based security requires special circuits that needs to be built into tags when they are manufactured while our method can work on any existing tag.

Different models of high frequency (HF) RFID tags were distinguished using the differences of the waveform in [20] and [21]. The process of fingerprinting HF tag is very different from process of fingerprinting UHF tags. HF tags use inductive coupling (magnetic field) for communication while the main form of UHF tags communicate in the radiative field (electric field). In HF RFID, communication is almost instantaneous because the transmission time is a fraction of a cycle of a RF voltage. There is no separation between reader and tag communication; changes in the reader antenna induce change in the tag antenna and vice versa. This is further explained by the work done in [20] where they used changes in the reader antenna when different tags were used to fingerprint the tag. The changes in the reader were more pronounced than the changes to the tag because of the greater modulation depth. In contrast, there is distinct channel of communication between reader transmission and tag communication in UHF RFID. The longer length of the transmission path makes the signals susceptible to more loss and interference.

6. Conclusion

We have used the transmission time of EPC, PC and CRC to distinguish individual UHF passive RFID tags from two major manufacturers, with the measurements being repeatable and reproducible. This feature is appropriate to be part of a hardware-based fingerprinting system which can be used against counterfeiting of RFID tags. The hardware-based fingerprinting system when combined with other application layer security protocols will provide robust security for RFID tags. This fingerprinting method is independent of the computational capabilities and resources of the tag which enables its implementation with any tag already in the system.

All the above measurements were taken by measuring the tag by itself. There will be more variation in the hardware based electronic features when the tag is part of a product due to the dielectric, reflective and constructive properties of the product. When the tag is fingerprinted along with the product, we will create a fingerprint of the tag-product combo. This combo fingerprint can be used to prevent tag swapping on products for malicious purposes.

References

- [1] *EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz*, ver. 1.2.0, EPCglobal Inc., Oct. 23, 2008. Available: <http://www.epcglobalinc.org>.
- [2] D. W. Aha, D. Kibler and M. K. Albert, "Instance-Based Learning Algorithms," *Machine Learning*, vol. 6, pp. 37-66, 1991.
- [3] A. Juels, "RFID security and privacy: a research survey," *Selected Areas in Communications, IEEE Journal on*, vol. 24, pp. 381-394, 2006.
- [4] A. Juels, "Minimalist cryptography for low-cost RFID tags," in *International Conference on Security in Communication Networks -- SCN 2004; Lecture Notes in Computer Science*, 2004, pp. 149-164.
- [5] A. Juels, "'Yoking-proofs' for RFID tags," in *International Workshop on Pervasive Computing and Communication Security -- PerSec 2004*, 2004, pp. 138-143.
- [6] F. Kerschbaum and A. Sorniotti, "RFID-based supply chain partner authentication and key agreement," in *Proceedings of the Second ACM Conference on Wireless Network Security -- WiSec'09*, 2009.
- [7] M. Lehtonen, F. Michahelles and E. Fleisch, "How to detect cloned tags in a reliable way from incomplete RFID traces," in *IEEE International Conference on RFID -- RFID 2009*, 2009.
- [8] T. Dimitriou, "A lightweight RFID protocol to protect against traceability and cloning attacks," in *First International Conference on Security and Privacy for Emerging Areas in Communication Networks -- SecureComm 2005*, Athens, Greece, September 2005.
- [9] A. Juels, "Strengthening EPC tags against cloning," in *WiSe '05: Proceedings of the 4th ACM Workshop on Wireless Security*, 2005, pp. 67-76.
- [10] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, T. Li and J. C. A. van der Lubbe, "Weaknesses in two recent lightweight RFID authentication protocols," in *Workshop on RFID Security -- RFIDSec'09*, 2009.
- [11] S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin and M. Szydlo, "Security analysis of a cryptographically-enabled RFID device," in *USENIX Security Symposium*, 2005, pp. 1-16.
- [12] Z. Kfir and A. Wool, "Picking virtual pockets using relay attacks on contactless smartcard systems," in *First International Conference on Security and Privacy for Emerging Areas in Communication Networks -- SecureComm 2005*, Athens, Greece, September 2005.
- [13] G. Hancke, "A Practical Relay Attack on ISO 14443 Proximity Cards," February. 2005. Available <http://www.cl.cam.ac.uk/gh275/relay.pdf>
- [14] G. Hancke and M. Kuhn, "An RFID distance bounding protocol," in *First International Conference on Security and Privacy for Emerging Areas in Communication Networks -- SecureComm 2005*, Athens, Greece, September 2005.
- [15] D. Carluccio, K. Lemke and C. Paar, "Electromagnetic side channel analysis of a contactless smart card: first results," in *ECRYPT Workshop on RFID and Lightweight Crypto*, Graz, Austria, July 2005, pp. 44-51.

- [16] M. Lehtonen, A. Ruhanen, F. Michahelles and E. Fleisch, "Serialized TID numbers - A headache or a blessing for RFID crackers?" in *IEEE International Conference on RFID -- RFID 2009*.
- [17] D. Holcom, W. Burleson and K. Fu, "Initial SRAM state as a fingerprint and source of true random numbers for RFID tags," in *Workshop on RFID Security -- RFIDSec'07, 2007*.
- [18] P. Tuyls and L. Batina, "RFID-tags for anti-counterfeiting," in *Topics in Cryptology - CT-RSA 2006, the Cryptographers' Track at the RSA Conference 2006; Lecture Notes in Computer Science, 2006*.
- [19] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola and V. Khandelwal, "Design and Implementation of PUF-Based Unclonable RFID ICs for Anti-Counterfeiting and Security Applications," *IEEE International Conference on RFID*, pp. 58-64.
- [20] H. P. Romero, K. A. Remley, D. F. Williams and Chih-Ming Wang, "Electromagnetic Measurements for Counterfeit Detection of Radio Frequency Identification Cards," *Microwave Theory and Techniques, IEEE Transactions on*, vol. 57, pp. 1383-1387.
- [21] B. Danev, T. S. Heydt-Benjamin and S. Capkun, "Physical-layer identification of RFID devices," in *Proceedings of the 18th USENIX Security Symposium USENIX'09, 2009*.