RFID Communication: How Well Protected Against Reverse Engineering?

Artis Mednis*‡, Reinholds Zviedris†‡
*Cyber-Physical Systems Laboratory, †Digital Signal Processing Laboratory
Institute of Electronics and Computer Science
14 Dzerbenes Str., Riga, LV 1006, Latvia
‡Faculty of Computing
University of Latvia
19 Raina Blvd., Riga, LV 1586, Latvia
Email: {firstname.lastname}@edi.lv

***Abstract*—The most important advantages of RFID technology are transmitting and receiving of information wirelessly as well as low implementation and maintenance costs. Such attractive features are reason for widespread usage of RFID systems - from tracking of assets to measurement of the timing during sporting events. To ensure secure operation of such systems they should have appropriate protection against reverse engineering.**

The contribution of this paper is a method for reverse engineering of specific RFID system used for time measurements during sporting events. Selected communication protocol aspects are discussed and their replication with off-the-shelf hardware and software with the aim to simulate a non-existing RFID tag with certain self selected ID number are presented.

***Index Terms*—RFID; protected communication; reverse engineering; security**

I. Introduction

A typical RFID system consists of one or several RFID tags, one or several RFID readers as well as data processing subsystem. RFID readers transmit calling signals with the aim to activate RFID tags located nearby. RFID tags activated by RFID reader calling signals transmit response signals with the aim to declare their presence to the RFID reader. The content of the RFID tag response signals can vary from simple ID numbers to complex information stored in the RFID tag memory or computed by the RFID tag hardware and software. Data processing subsystem uses the acquired data in some useful manner [1].

Typical applications of the RFID tags are identification and tracking of several objects and subjects such as animals in rough terrain and baggage items in the airports, management of the access rights such as employee access to the restricted areas as well as additional functionality for common person documents such as passports with RFID functionality. These tags could be passive - powered by electromagnetic fields from tag readers or active - powered by internal power source. The possibility to read information from RFID tag without line of sight and even in the case it is embedded in the tracked object arises several security and privacy issues.

Significant parameter of each RFID system is its security. System considered to be secure should have certain protection against physical non-invasive and invasive attacks including such attack type as reverse engineering ([2], p. 116).

There exist more than 500 commercially available RFID tag types [3] that could be divided into three different categories:

1) tags for logistical applications with little or no routine for security i.e. asset or parcel tracking;
2) tags for consumer applications with security capability such as smart cards used for financial transactions;
3) tags for vertical applications with security tailored for specific business processes such as RFID poker chips in casinos.

RFID system investigated during this research belongs to the third above mentioned category. The choice of the particular RFID system for the reverse engineering activities was motivated by its commercial availability and relatively wide usage in sporting event time keeping domain.

Related work is discussed in Section II. Requirements and assumptions are listed in Section III. Proposed reverse engineering approach is described and analyzed in Section IV. The evaluation of the approach including successful test with developed hardware and software is described in Section V. The final section presents the conclusion that the proposed approach allows the simulation of a non-existing RFID tag with certain self selected ID number and therefore demonstrates insufficient protection of specific RFID system used for time measurements during sporting events against reverse engineering.

II. Related Work

Secure communication in RFID systems should be considered a challenging task because available hardware and software resources in low-cost RFID tags are constrained and therefore not suitable for strong cryptographic solutions. There exist proposed solutions for this task based on special lightweight algorithms and protocols [4] [5]. Weakness of authentication protocol used in low-cost RFID tags could be the result of weak pseudorandom number generator used in

©2012 IEEE, DOI: 10.1109/ICDIPC.2012.6257290

particular protocol [6]. Unfortunately such lightweight protocols can be broken by a powerful attacker. Therefore every application needs to find the best trade-off between security and performance.

Attacks to the RFID systems can be performed in several ways. First of them are eavesdropping or skimming of forward and backward channels. Other possibilities are tag cloning and physical attacks as well as relay and replay attacks ([7], p. 40). Common method to avoid tag cloning is symmetric-key cryptography [8], but physical attacks could be reduced by making tags more secure against tampering. Sequence numbers and clock synchronization are common methods against replay attacks. Specific attack method is deactivation of the tag using corresponding command. To prevent unauthorized usage of such commands they are protected by PIN code [9] therefore some typical password management and scalability issues could arise.

Another attack type to the RFID systems is RFID tag cloning. This type of attack could be prevented using security protocols based on Physical Unclonable Function (PUF) [10]. RFID with such protection are suitable in cases when the attacker can capture the example of the RFID tag and investigate it in detail.

There are previous attempts to use reverse engineering against RFID systems [11] [12] as well as attempts to create technical or non-technical methods to prevent reverse engineering [13]. Both reverse engineering attempts include hardware analysis with the aim to investigate silicon implementations. Unlike them proposed reverse engineering approach is based mainly on black box analysis of communication signals transmitted by RFID reader and RFID tags.

III. Requirements

The following requirements were chosen as a basis for reverse engineering of the specific RFID system used for time measurements during sporting events:

1) Reverse engineering of the specific RFID system should be performed using relatively simple reverse engineering techniques. Usage of specific software tools as well as pool of computing devices is not intended.
2) The black box approach should be used for exploration of the RFID communication protocol physical and logical layers. Dismantling or physically damaging hardware items as well as social engineering for acquiring of classified information are not intended.
3) Additional hardware and software necessary for reverse engineering activities should be freely available, relatively inexpensive and characterized by steep learning curve.
4) Communication of specific RFID system should be considered as insufficiently protected against reverse engineering if there is a possibility to simulate a non-existing RFID tag with certain self selected ID number using above mentioned relatively simple tools and methods.

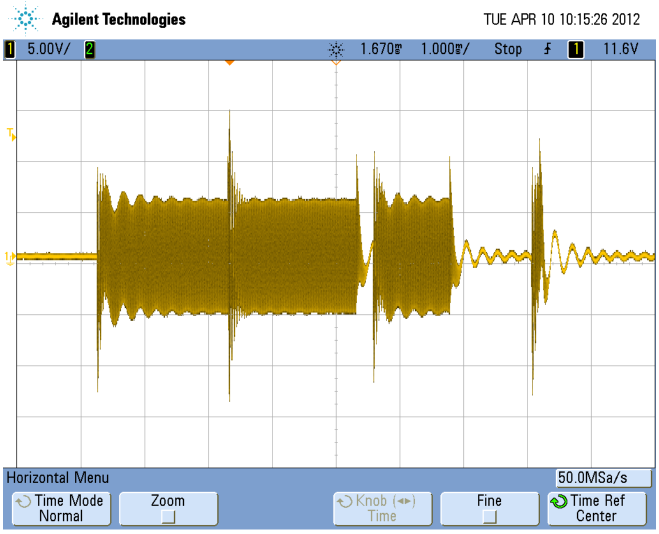

Fig. 1. RFID reader calling message - a sequence of OOK modulated 125 kHz oscillations.

IV. Approach

All activities performed for reverse engineering of specific RFID system were divided into several consecutive steps:

1) Investigation of the physical layer of RFID system communication protocol.
2) Development of the toolset consisting of off-the-shelf hardware and software with the aim to simulate corresponding RFID system components.
3) Investigation of the logical layer of RFID system communication protocol.
4) Development of the method to simulate a non-existing RFID tag with certain self selected ID number.

A. Communication protocol physical layer

Investigation of RFID system communication protocol physical layer was performed using RFID reader, two RFID tags with known ID numbers as well as digital oscilloscope with the functionality to store measurement data for further analysis.

First experiment was aimed at determination of RFID reader calling message performed by analyzing signals on terminals of RFID reader antenna coil. The calling message consists of a sequence of OOK modulated 125 kHz oscillations (Fig. 1):

1) ON for 2.05 ms;
2) OFF for 0.02 ms;
3) ON for 2.00 ms;
4) OFF for 0.25 ms;
5) ON for 1.20 ms;
6) OFF for 1.30 ms;
7) ON for 0.15 ms.

RFID calling message is transmitted 80 times per second.

Second experiment was aimed at determination of RFID tag response message performed by analyzing signals on terminals of probe coiled around RFID tag. The entire response message consists of 36 sequential single response messages transmitted

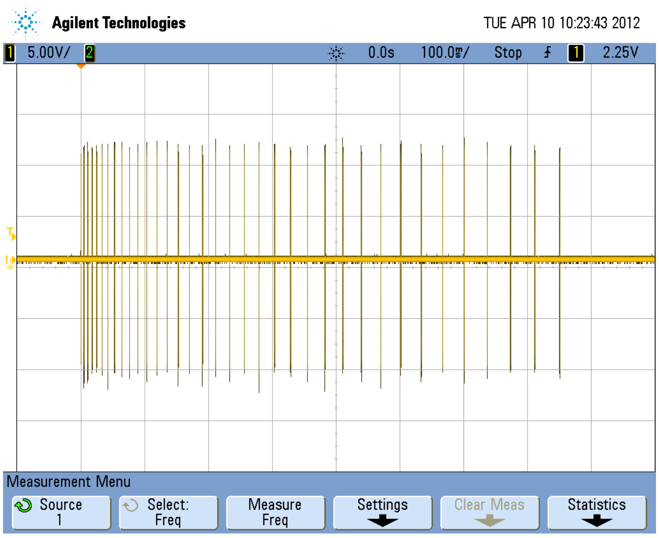

Fig. 2. Entire RFID tag response message - a sequence of 36 single response messages with incrementing time intervals between them.

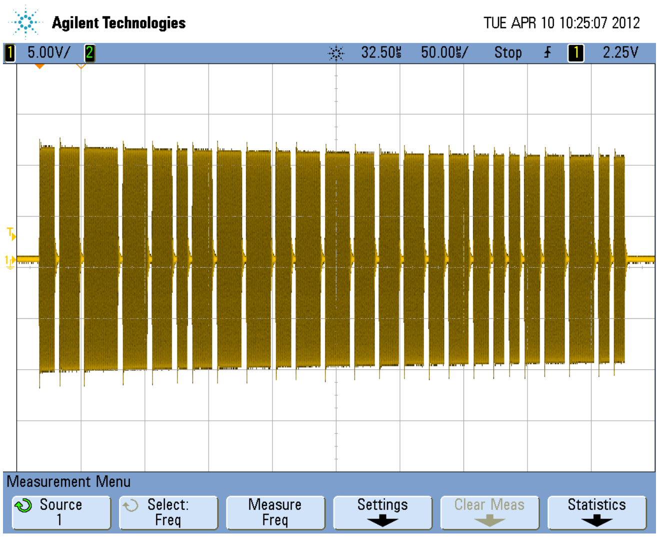

Fig. 3. Single RFID tag response message - a sequence of 25 variable length ON items with 24 fixed length OFF items between them.

with time interval between sequential messages incrementing from 4 ms to 39 ms (Fig. 2).

Each single response message consists of a sequence of OOK modulated 3 MHz oscillations (Fig. 3):

1) 25 ON items with the length from 9 to 28 μs;
2) 24 OFF items with a fixed length of 3 μs.

The time of the transmission of the entire RFID tag response message is about 0.8 seconds.

B. Hardware and software

Development of the toolset consisting of off-the-shelf hardware and software with the aim to simulate corresponding RFID system components was carried out using open source electronics prototyping platform Arduino [14] and specifically its board - Arduino Duemilanove [15].

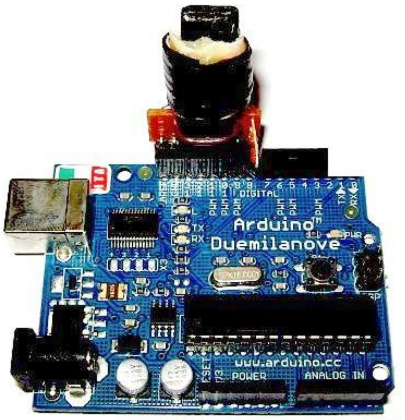

Fig. 4. Arduino Duemilanove board expanded with RFID reader simulation circuit.

To ensure Arduino board's functionality - acting as simulated RFID reader and transmitting of calling message, the board was expanded with the circuit consisting of a magnetic antenna in series with appropriate resistor to limit output current of the boards MCU (Fig. 4). Due to relatively low main oscillations frequency (125 kHz) software was used not only for OOK modulation but also for generation of the main oscillations. Developed hardware and software system was tested with both available RFID tags and both of them showed reliable detection of transmitted calling message.

To ensure Arduino board's functionality - acting as simulated RFID tag and transmitting of entire response message, the board was expanded with the circuit consisting of 3 MHz oscillator (Fig. 5). Due to relatively high main oscillations frequency (3 MHz) software could be used only for OOK modulation. Developed hardware and software system was tested with available RFID reader and it showed reliable detection and decoding of transmitted response message.

C. Communication protocol logical layer

Investigation of RFID system communication protocol logical layer was performed using two RFID tags with known ID numbers as well as some additional information about potential content of the message.

Entire response message from RFID tag to RFID reader is transmitted as soon as RFID tag detects a valid calling message. After each approximately 7 ms long calling message there is approximately 5 ms long pause. There could be also other RFID tags detecting calling messages and responding to them and each individual entire response message is about 0.8 seconds long and contains 36 single response messages. Taking into account all these aspects the hypothesis about uniformity of all 36 single response messages during one entire response message and subsequently - the inclusion of all transmitted information into each single response message was taken. This hypothesis was successfully proven using simulated RFID tag transmitting single response message.

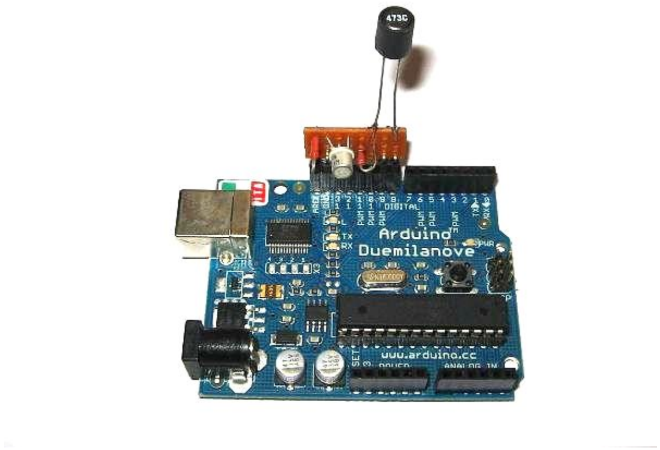

Fig. 5. Arduino Duemilanove board expanded with RFID tag simulation circuit.

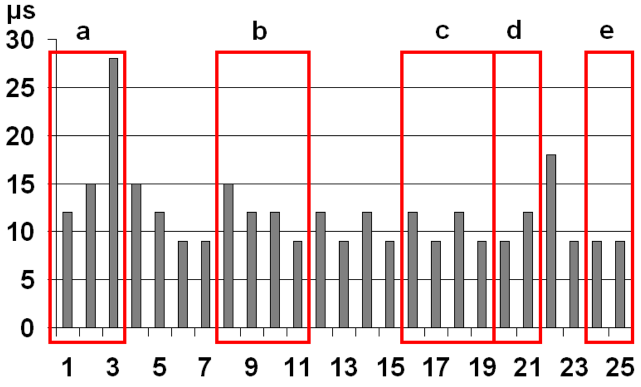

Fig. 6. Single RFID tag response message in detail: a - preamble, b - quaternary ID digits #6-#9, c - quaternary ID digits #2-#5, d - quaternary ID digit #1 with the leading zero, e - postamble.

During previous activities - investigation of RFID system communication protocol physical layer - single response messages from two RFID tags with known ID numbers were recorded. These messages were analyzed and compared with the aim to determine potential meaning of the different message parts. The first 3 and the last 2 ON items in both single response messages were completely identical. This aspect allowed making assumption about adherence of these items to respectively preamble and postamble parts of the single response message (Fig. 6 - a and e). Stronger confirmation of this assumption could be acquired after analysis of a larger number of corresponding RFID tags, as well further work on investigation of RFID system communication protocol logical layer could be performed based on this assumption.

More detailed analysis of the single response message ON items revealed that their lengths, except the #3 which length was 28 μs, are strictly one from the following list:

1) 9 μs;
2) 12 μs;
3) 15 μs;
4) 18 μs.

This distribution allowed making assumption about the usage of the quaternary numeral system. To prove this assumption following steps were carried out:

1) Both original ID numbers consisting of 5 decimal digits were converted to quaternary numeral system.
2) Both obtained ID numbers consisting of 9 quaternary digits were compared to corresponding single response messages.

Analysis of the comparison revealed that ON item with length of 9 μs means quaternary digit 0 and other ON items with lengths of 12, 15 and 18 μs means respectively quaternary digits 1, 2 and 3. Single response message ON items #8-#11 corresponds to quaternary ID digits #6-#9, ON items #16-#19 corresponds to quaternary ID digits #2-#5, but ON items #20-#21 with a certain probability corresponds to quaternary ID digit #1 with leading zero (Fig. 6 - b, c and d). Complete coincidence in the case of at least 8 digits allows making assumption that ID number is transmitted in exactly described way.

According to information available about features of the corresponding RFID system, RFID tags transmit not only their ID number, but also the charge level of the internal battery measured in whole percents. This information could be submitted using 4 additional quaternary digits. In the context of a short term usage information about charge level could be considered as static data. As described reverse engineering activities are related to the simulation of a non-existing RFID tag with certain self selected ID number, exact determination of the meaning of other message parts is left for future work and by that time other 10 ON items are considered as checksum.

D. Simulation of non-existing RFID tag

Development of the method to simulate a non-existing RFID tag with certain self selected ID number was performed using brute force attack principles. This approach conforms to the requirement about relatively simple reverse engineering techniques and in case of success could be considered as demonstration of the insufficient protection against reverse engineering.

As it was mentioned in the previous subsection, there are 10 ON items that could be considered as checksum. Each of these items represents one quaternary digit and there are 1 048 576 possible combinations. Additional aspects that should be taken into account during development of brute force attack are minimal time interval between two single response messages - 4 ms as well as duty cycle of the RFID reader - approximately 7 ms for the calling message and approximately 5 ms for the listening to the response messages. Taking into consideration all these aspects the following algorithm for the brute force attack was selected:

1) All 1 048 576 possible single response messages for particular ID number are transmitted to the RFID reader in sequential order.

2) Each individual single response message is repeated 12 times.
3) Time intervals between subsequent transmitted single response messages are 4 ms long.

According to calculations, the time necessary for the transmitting of one of the 1 048 576 possible single response messages 12 times is about 54 ms and therefore corresponds to 4.5 cycles of RFID reader's duty cycle. That means there are at least 4 possibilities for RFID reader to detect valid single response message. Total time of the transmission of all 1 048 576 possible single response messages 12 times is about 15.6 hours and subsequently could not be considered as relatively simple reverse engineering technique. Therefore additional assumptions about potential meaning of different message parts were taken.

Quaternary digits representing ID number digits are grouped in 3 sequences - 2 sequences containing 4 digits and one sequence containing 2 digits. Quaternary digits representing checksum (and the charge level of the internal battery) are grouped identically - 2 sequences containing 4 digits and one sequence containing 2 digits. Most significant ID number digits are stored in the shortest sequence and it is supposed that this short sequence in most cases is invariable therefore potentially not so significant for checksum calculation. Shortest sequence of the checksum (and the charge level of the internal battery) allows transmitting 16 different levels of charge level and similarly to shortest sequence of the ID number digits, in this case could be relatively invariable. Based on analysis of before mentioned aspects it was considered to try a simplified version of previously described algorithm that uses only 8 ON items for potential checksum, 65 536 possible single response messages and therefore just 1 hour for transmission of all possible single response messages 12 times.

V. Evaluation and Performance Results

To evaluate the described reverse engineering method the following set of the activities were performed:

1) Selection of a non-existing ID number which differed from one of the real ID numbers by two quaternary digits.
2) Development of the Arduino software for subsequent transmission of 65 536 possible single response messages 12 times.
3) Test with developed hardware and software with the aim to determine a valid single response message containing self selected ID number.

Whereas the test was carried out just for proof of the concept of previously described method several features such as automatic detection of a valid single response message and extraction of corresponding checksum were not implemented in the software but performed by test operator manually. Nevertheless full test with successful determination of a valid checksum for the particular self selected ID number took just about 1.2 hours what could be considered as demonstration of the insufficient protection against reverse engineering. Performance of the described method allows acquiring up to 20 valid checksums per 24 hours for self selected ID numbers using one RFID reader device and one simulated RFID tag device. Further decreasing of the time for the acquiring of a valid single response message could be achieved by automatization of manually performed actions as well as optimization of transmitting sequence of 65 536 possible single response message. There is also a possibility to use more than one simulated RFID tag device with the aim to distribute the sequence of 65 536 possible single response messages between them.

VI. Conclusion and Future Work

This paper describes a method for reverse engineering of specific RFID system used for time measurements during sporting events and its evaluation on a particular task - the simulation of a non-existing RFID tag with certain self selected ID number. The evaluation tests resulted in successful accept of RFID communication message, transmitted by developed off-the-shelf hardware and software and the performance analysis showing that generation of a valid RFID communication message with certain self selected ID number takes just about one hour.

The future work includes experiments in generation of RFID communication message with the aim to decrease the time for acquiring of a valid message exchange as well as further exploration of the communication protocol's logical layer.

VII. Acknowledgment

This work has been supported by the European Social Fund within the project "Support for Doctoral Studies at University of Latvia - 2". Special thanks to our IECS colleague Gatis Supols for his help during signal measurements.

References

[1] S. E. Sarma, S. A. Weis, and D. W. Engels, "Rfid systems and security and privacy implications," in *Revised Papers from the 4th International Workshop on Cryptographic Hardware and Embedded Systems*, ser. CHES '02. London, UK, UK: Springer-Verlag, 2003, pp. 454–469. [Online]. Available: http://dl.acm.org/citation.cfm?id=648255.752715

[2] P. Cole and D. Ranasinghe, *Networked RFID Systems and Lightweight Cryptography: Raising Barriers to Product Counterfeiting*, ser. Computer Science. Springer, 2008. [Online]. Available: http://books.google.lv/books?id=_QjPM5G_r0cC

[3] T. Phillips, T. Karygiannis, and R. Huhn, "Security standards for the rfid market," *IEEE Security and Privacy*, vol. 3, no. 6, pp. 85–89, Nov. 2005. [Online]. Available: http://dx.doi.org/DB27D663-87D5-47E9-9CD2-8B12AC62B325

[4] I. Vajda and L. Buttyn, "Lightweight authentication protocols for low-cost rfid tags," in *Second Workshop on Security in Ubiquitous Computing Ubicomp 2003*, 2003.

[5] A. Juels, "Minimalist cryptography for low-cost rfid tags (extended abstract)," in *Security in Communication Networks*, ser. Lecture Notes in Computer Science, C. Blundo and S. Cimato, Eds. Springer Berlin / Heidelberg, 2005, vol. 3352, pp. 149–164, 10.1007/978-3-540-30598-9_11. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-30598-9_11

[6] M. Merhi, J. C. H. Castro, and P. Peris-Lopez, "Studying the pseudo random number generator of a low-cost rfid tag," in *RFID-TA*. IEEE, 2011, pp. 381–385.

[7] Y. Zhang and P. Kitsos, *Security in RFID and Sensor Networks*, ser. Wireless Networks and Mobile Communications Series. CRC Press, 2009. [Online]. Available: http://books.google.lv/books?id=lPEwic6W1RgC

[8] A. Juels, “Rfid security and privacy: A research survey,” *JOURNAL OF SELECTED AREAS IN COMMUNICATION (J-SAC)*, vol. 24, no. 2, pp. 381–395, 2006.

[9] P. Peris-Lopez, J. C. H. Castro, J. M. Estévez-Tapiador, and A. Ribagorda, “Rfid systems: A survey on security threats and proposed solutions,” in *PWC*, ser. Lecture Notes in Computer Science, P. Cuenca and L. Orozco-Barbosa, Eds., vol. 4217. Springer, 2006, pp. 159–170.

[10] P. Tuyls and L. Batina, “Rfid-tags for anti-counterfeiting,” in *Topics in Cryptology CT-RSA 2006*, ser. Lecture Notes in Computer Science, D. Pointcheval, Ed. Springer Berlin / Heidelberg, 2006, vol. 3860, pp. 115–131, 10.1007/11605805_8. [Online]. Available: http://dx.doi.org/10.1007/11605805_8

[11] H. Plötz and K. Nohl, “Peeling away layers of an rfid security system,” in *Financial Cryptography and Data Security*, ser. Lecture Notes in Computer Science, G. Danezis, Ed. Springer Berlin / Heidelberg, 2012, vol. 7035, pp. 205–219, 10.1007/978-3-642-27576-0_17. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-27576-0_17

[12] K. Nohl, D. Evans, S. Starbug, and H. Plötz, “Reverse-engineering a cryptographic rfid tag,” in *Proceedings of the 17th conference on Security symposium*, ser. SS’08. Berkeley, CA, USA: USENIX Association, 2008, pp. 185–193. [Online]. Available: http://dl.acm.org/citation.cfm?id=1496711.1496724

[13] S. Guilley, J.-L. Danger, R. Nguyen, and P. Nguyen, “System-level methods to prevent reverse-engineering, cloning, and trojan insertion,” in *Information Systems, Technology and Management*, ser. Communications in Computer and Information Science, S. Dua, A. Gangopadhyay, P. Thulasiraman, U. Straccia, M. Shepherd, and B. Stein, Eds. Springer Berlin Heidelberg, 2012, vol. 285, pp. 433–438, 10.1007/978-3-642-29166-1_41. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-29166-1_41

[14] Arduino - homepage. [Online]. Available: http://arduino.cc/en/

[15] Arduino - arduinoboardduemilanove. [Online]. Available: http://arduino.cc/en/Main/arduinoBoardDuemilanove