IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received February 14, 2020, accepted March 3, 2020, date of current version March 19, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2979548

Screen Printed Security-Button for Radio Frequency Identification Tags

ALMUDENA RIVADENEYRA[1], ANDREAS ALBRECHT[2], FERNANDO MORENO-CRUZ[3], DIEGO P. MORALES[4], MARKUS BECHERER[2], AND JOSÉ F. SALMERÓN[2]

[1]Pervasive Electronics Advanced Research Laboratory (PEARL), Department of Electronics and Computer Technology, University of Granada, 18071 Granada, Spain
[2]Institute for Nanoelectronics, Technical University of Munich, 8033 München, Germany
[3]Infineon Technologies AG, 85579 Munich, Germany
[4]Biochemistry and Electronics as Sensing Technologies Group, University of Granada, 18071 Granada, Spain

Corresponding author: Almudena Rivadenerya (arivadeneyra@ugr.es)

This work was supported by the fellowship under Grant 2020-MSCA-IF-2017-794885-SELFSENS.

ABSTRACT Radio frequency identification (RFID) security is a relevant matter. The wide spread of RFID applications in the general society and the persistent attempts to safeguard it confirm it, especially since its use involves payments and the store or transmission of sensitive information. In this contribution, we present an innovative solution for improving the security of RFID passive tags through the use of a screen printed button, that allows the reception and transmission only when a certain level of physical pressure normal to its plane is applied. The materials and fabrication technology used demonstrate an easy to implement and cost-effective system, valuable in several scenarios where the user has straight contact with the tags and where its usage is direct and intentional.

INDEX TERMS Flexible, force sensor, high-frequency band, pressure, printed electronics.

I. INTRODUCTION

Radio frequency identification (RFID) tags or systems are increasingly used in day-to-day situations to provide information or handles to information stored elsewhere. In many use cases, this information stored within the tag can be sensitive; implying payments, access to restricted zones or privacy matters. Security concerns arise when not-authorized entities are able of tracking the location of tags or the person carrying it, eavesdropping on tag-to-reader communication, misuse of the information or identity theft through tag cloning [1]. In the case of users carrying RFID-tagged objects, the threat to people's privacy relies in companies, governments and crooks, tracking people without their knowledge and consent; and potentially exploiting this private information. Criminals may also fabricate fake products or duplicate identities to take advantage of its illegal use [2]. Thus, it would be desirable to add some extra control to the wireless data transfer, while maintaining it transparent to the user and not interfering in its utilization.

A lot of effort has gone into RFID privacy. To mention the most relevant solutions of the literature, Juels proposes one-time pads transmitted across multiple authentication protocols [3]. Their successful use depends on the attacker not being able to eavesdrop for a number of consecutive transmissions, appearing this as its main limitation. Garfinkel proposes a strict regulation for the customer tracking (RFID Bill of Rights) [4]. Nevertheless, this set of laws may be only viable for some use cases, since it relies entirely on legislation. Molnar and Wagner [5] for their part, propose to decrease the tag identification time with a tree-based tag scheme, even at the expense of considerably less privacy guarantees. More recently, Tu and Piramuthu [6] and Korak and Hutter [7] addressed the relay attack, consisting on the non-authorized use of the tag (identity theft) through a man in the middle attack, resending the tag communication while physically far from the target.

A common assumption in every proposed solution is that the attacker, in his pursuit of breaking the privacy of the protocol, is not capable to physically manipulate and tamper the tags. Accessing the tags' memory would mean accessing secret keys, relevant state information and hence, the ability

The associate editor coordinating the review of this manuscript and approving it for publication was Yanjiao Chen.

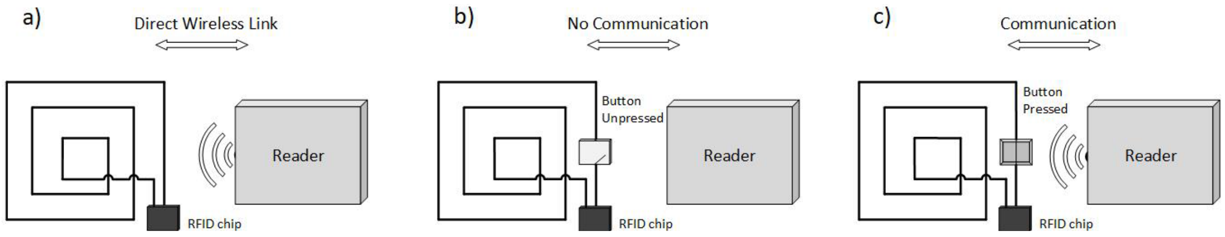


FIGURE 1. Scheme of operation: (a) Normal RFID tag; (b) Proposed Open tag; (c) Proposed Shorted tag.

of indistinguishably forge the tag. These situations are not considered, or directly assumed that physically compromised tags are out of the system. In this way, the RFID privacy concerns of these models deal only with algorithmic attacks, seeing the tag as a ''black-box''. The adversarial then has prohibited to tamper with tags' private information or to use side-channel information to break the RFID security.

On the other side, Gassend *et al.* extended the RFID privacy model to include hardware tampering attacks with minimal hardware by means of physical unclonable functions (PUFs) [8]. PUFs exploit physical characteristics of the circuit, which are difficult to model even allowing the attacker to have contact with the system.

In this paper, we focus on the high frequency (HF) band (13.56 MHz) that can be implemented in many portable devices, such as smartphones, tables or dataphones [9]. In fact, this broad use is a double-edged sword. On one side, it generalizes the use of such technology and thus, the emergence of new applications, contributing to the maturity of the technology. On the other side, it makes easier the access to the transmitted information through the wireless link, arising methods to hack the protocols and/or devices. Therefore, it is mandatory to come up with new and sophisticated strategies to cope with these potential security risks.

In this contribution, we describe an extra hardware security level for HF RFID tags. In particular, we include a force sensor between the chip and antenna, so that the tag is unreadable until it touches the reader with enough pressure normal to its surface. In this direction, Marquardt *et al.* [10] described different simple approaches to give awareness of the RFID operation to the user. Specifically, they developed three kinds of designs providing either visual, audible or vibro-tactile feedback, although the last two options needed an extra battery.

II. MATERIALS AND METHODS

A. DESCRIPTION OF OUR APPROACH

Our idea was to implement a button into the RFID antenna that is open by default and closes the loop antenna on pressure. To accomplish this, we modified the connection layer between the inductor and the RFID chip, which is normally developed by an insulator layer among the conductive traces and on top a conductive line through insulator as well, as the two points that are connected (see Figure 1a). In this work, we did not place directly a conductive line between these connections but instead, we deposited a matrix of cubes made of silicone and glued to it a silver trace printed of a polymeric foil (see Figure 1b). Therefore, once we want to activate our RFID tag we need to press on this array with a certain pressure value to create the connection between chip and antenna that allows the communication (see Figure 1c).

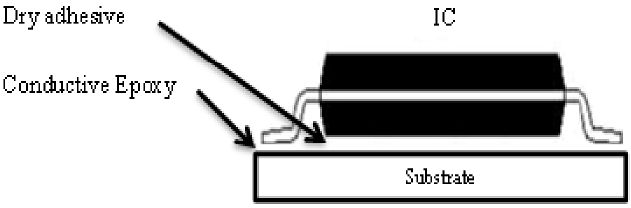


FIGURE 2. Schematics of the chip assembly process.

B. TAG FABRICATION

The silver (Ag) screen printing paste employed in this work to print the antenna was LOCTITE ECI 1010 0.2KG E&C by Henkel (Germany) used without modifications. The array of cubes was made of screen-printed polydimethylsiloxane (PDMS). The isolating paste used to isolate the bridge connecting the two ends of the inductor was TD-642 of AppliedInkSolutions (US).

All pastes were printed onto thermally pre-heated (100°C for 30 min) polyethylene terephthalate (PET) Melinex 506 of DuPont of a thickness of 100 μm. A manual screen printer (Nino from Coruna, Switzerland) was used to print with a screen with a mesh density of 120 Threads/cm. After printing, the pastes were dried at 100°C for 30 min in an oven before printing the next type of paste.

The assembly of the RFID chip to the foil was done in a three-step process as depicted in Figure 2. First, H20E conductive resin (Epoxy Technology Inc., Billerica, United States) was deposited to interconnect the integrated circuit (IC) and the screen printed silver pads. Double layer 50 μm-thick dry adhesive (AR Clear 8932 from Adhesives Research, Inc. Glen Rock, Pennsylvania, United States) was located on the bottom part of the IC to fix it to the substrate. Finally, a heating step was performed in an oven at 120 °C for 20 min to cure the conductive resin. Additionally, the dry film adhesion is enhanced with temperature, so the heat treatment served also to fix it better to the substrate.

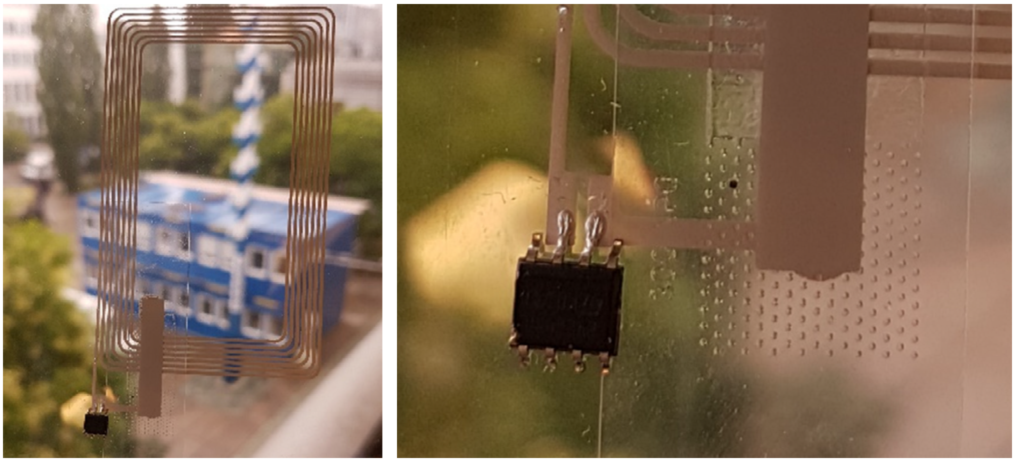


FIGURE 3. a) Screen-printed one-chip RFID tag with a pressure-activated button. b) Magnification of chip and pressure-sensing button.

C. TAG CHARACTERIZATION

A Keithley 2700 multimeter with 20 input channels was used for measuring the resistances and open-circuit voltages in the bending setup and in the thermocouple setup. A Keithley 2602B source meter was employed in the thermocouple setup. The LCR meter E4982A of Keysight was employed for all capacitance measurements at an amplitude of 1 V at a frequency of 100 kHz, if not indicated otherwise. A calibration of the wires was done after each change of the setup. The impedance analyzer E4990A was employed to measure the frequency dependent response of the wireless tags and an E5061B ENA Vector Network Analyzer of Keyight for the S_{11} parameter measurements.

Sheet resistance measurements were conducted on a printed 5 × 10 mm^2 area with a self-made linear four-point probe in combination with a Keysight B2900 source meter or a Keithley 2700 multimeter. A correction factor of 0.651 was calculated for the 5 × 10 mm^2 areas and applied to compensate the effect of limited boundaries according to Smits [11]. Profilometer studies were done with a Dektak XT of Bruker (US) with the micro-porous vacuum chuck that holds flexible samples flat.

III. RESULTS AND DISCUSSION

We investigated the use of our thin pressure sensors without a dielectric as they are pressed at a certain pressure. The implementation in a HF RFID tag is shown in Figure 3a with a magnification of the RFID chip and the sensor in Figure 3b. The latter shows the structured dielectric as dots around and between the contact areas of the bridge to the bottom contact wired to the chip, closing the circuit.

Preliminary results show that the button works as intended and changes from a capacitance of about 17.5 pF to a resistor of about 0.8 Ω at the desired frequency of 13.56 MHz (see Figure 4). The latter should not have a large influence on the antenna behavior as intended, working close to an ideal closed switch even for HF signals. The first one however, introduces a second large capacitance next to the internal one into the microcontroller and leads to a decoupling between the reader and antenna. Thus, it acts in practice as an ideal open switch, not allowing the signal to get in the microcontroller and therefore not permitting the communication.

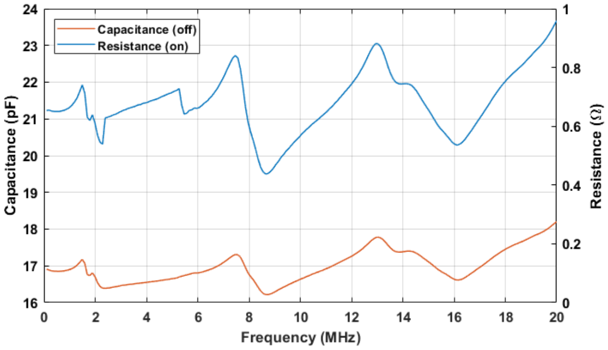


FIGURE 4. Capacitance (when the button is OFF) and resistance (when the button is pressed at 10 mN), over the frequency range from 100 Hz to 20 MHz.

We used a FR4 antenna as reader, resonating at approximately 13.56 MHz, and brought the safe tag close to it, pressing the button with a plastic clamp at two different distances (as shown in Figure 5). We tested two copper antennas as well as reference, whose responses with the reader can be seen in Figure 5 (copper1 and copper2) with a resonance frequency in both cases about 14 MHz.

When the HF tag is placed in the reader surroundings, the antiresonance of the reader antenna disappears. In particular, when the button was pressed, the matching of the characteristic impedance was achieved at resonance frequency of 13.56 MHz. On the other side, if the clamp was removed and the button was not pressed, a shift in the resonance frequency of the circuit appeared of more than 1 MHz. This should reliably inhibit the coupling of the reader and the tag and not permit non-intended communications, since the RFID chip would not be able to operate.

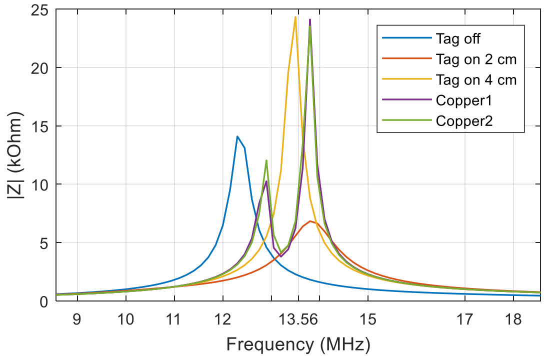


FIGURE 5. Coupling of a copper HF reader with two reference copper antennas and the printed tag. Tag without (off) and with (on) pressure in the button at distances of 2 and 4 cm.

Apart from providing extra hardware security to the RFID communication, our developed switch gives a threshold pressure value of around 10 mN. New use-cases emerge from tags that only activate when certain pressure is applied to the objective, security aside. Goods differentiation or energy savings in case of battery-assisted tags can be as well achieved.

IV. CONCLUSION

We demonstrated how a pressure-sensitive button implemented in an RFID tag can increase its security by inhibiting unwanted readings. In other words, through the combination of a NFC tag with an imperceptible printed security button, we allow data transfers only when the button is pressed with a certain level of pressure. This merges the comfort of a wireless tag like a credit card or an access batch, with additional security against tracking, relay attack or eavesdropping. The inclusion on current solutions as the mentioned ones would be indubitably straightforward. Besides, adding that antenna, circuitry and button are screen printed, results in a greatly convenient and inexpensive solution for a security boost in several use cases, not implying changes in the firmware or communication protocols, nor the inclusion of more components to the system.

To conclude, we enhanced the security and, in last term privacy, of RFID tags. Although still assuming that the attacker is not able to physically manipulate the tag as most of the literature; we went further than most of the current solutions not considering only the protocol algorithmic, but as well its physical nature and interaction in realistic scenarios, without compromising the energetic autonomy of the tag.

REFERENCES

[1] N. Marquardt, A. S. Taylor, N. Villar, and S. Greenberg, "Rethinking RFID: Awareness and control for interaction with RFID systems," in *Proc. SIGCHI Conf. Hum. Factors Comput. Syst.*, 2010, pp. 2307–2316.

[2] P. Kitsos, *Security in RFID and Sensor Networks*. New York, NY, USA: Auerbach, 2016.

[3] A. Juels, "Minimalist cryptography for low-cost RFID tags," in *Proc. Int. Conf. Secur. Commun. Netw.*, 2004, pp. 149–164.

[4] S. Garfinkel, "An RFID bill of rights," *Technol. Rev.*, vol. 105, no. 8, p. 35, 2002.

[5] D. Molnar and D. Wagner, "Privacy and security in library RFID: Issues, practices, and architectures," in *Proc. 11th ACM Conf. Comput. Commun. Secur. (CCS)*, 2004, pp. 210–219.

[6] Y.-J. Tu and S. Piramuthu, "On addressing RFID/NFC-based relay attacks: An overview," *Decis. Support Syst.*, vol. 129, Feb. 2020, Art. no. 113194.

[7] T. Korak and M. Hutter, "On the power of active relay attacks using custom-made proxies," in *Proc. IEEE Int. Conf. RFID (IEEE RFID)*, Apr. 2014, pp. 126–133.

[8] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," in *Proc. 9th ACM Conf. Comput. Commun. Secur. (CCS)*, 2002, pp. 148–160.

[9] N. Chhabra, "Comparative analysis of different wireless technologies," *Int. J. Sci. Res. Netw. Secur. Commun.*, vol. 1, no. 5, pp. 3–4, 2013.

[10] N. Marquardt, A. S. Taylor, N. Villar, and S. Greenberg, "Visible and controllable RFID tags," in *Proc. 28th Int. Conf. Extended Abstr. Hum. Factors Comput. Syst.*, 2010, pp. 3057–3062.

[11] F. Smits, "Measurement of sheet resistivities with the four-point probe," *Bell Syst. Tech. J.*, vol. 37, no. 3, pp. 711–718, 1958.

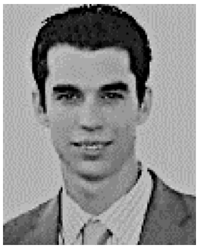
ALMUDENA RIVADENEYRA received the master's degrees in telecommunication engineering, environmental sciences, and electronics engineering from the University of Granada, Spain, in 2009, 2009, and 2012, respectively, and the Ph.D. degree in design and development of environmental sensors from the University of Granada, in 2014. Since 2015, she has been with the Institute for Nanoelectronics, Technical University of Munich, where her work is centered in printed and flexible electronics with a special focus on sensors and RFID technology.

ANDREAS ALBRECHT received the master's degree in electrical engineering and information technology and the Ph.D. degree in printed electronics and printed sensors for the Internet of Things from the Technical University of Munich, in 2014 and 2018, respectively. He is currently with Cicor Technologies in the industrialization of aerosol jet printed electronics for mass and niches markets.

FERNANDO MORENO-CRUZ received the M.S. degree in telecommunications engineering from the University of Granada, Spain, in 2013, with the maximum grade obtained on his senior thesis. After two years in development and test in the automotive sector and two years in research and development in the IoT field, he is currently pursuing the Ph.D. degree with Infineon Technologies AG and Grupo de Investigación en Dispositivos Electrónicos,Granada. He has been rewarded with first prizes in the contests; Intel IoT Solutions 2017 and Embedded Wireless Systems and Networks 2018. His research interests include wireless power for sensor nodes, energy harvesting, antennas, and low-power network protocols.

DIEGO P. MORALES received the M.Sc. degree in electronic engineering and the Ph.D. degree in electronic engineering from the University of Granada, Spain, in 2001 and 2011, respectively. He was an Associate Professor with the Department of Computer Architecture and Electronics, University of Almería, Spain. He joined the Department of Electronics and Computer Technology, University of Granada, where he currently serves as a Tenured Professor. His current research interest includes developing reconfigurable applications.

MARKUS BECHERER was born in Bühl, Germany. He received the Diploma and Ph.D. degrees from the Technical University of Munich (TUM), Germany, in 2005 and 2010, respectively. He is currently a Full Professor with the Chair of Nanoelectronics, TUM.



JOSÉ F. SALMERÓN received the degrees in telecommunication engineering and electronics engineering from the University of Granada, Granada, Spain, in 2009 and 2011, respectively, and the master's degree in computer and network engineering and the Ph.D. degree in development of sensing capabilities in RFID technologies from the University of Granada, in 2012 and 2014, respectively. He is currently a Postdoctoral Researcher with the Institute for Nanoelectronics, Technical University of Munich, Germany, where he is involved in the design and development of smart RFID labels with sensing capabilities.