International Journal of Advanced Culture Technology Vol.3 No.2 149-160 (2015)
http://dx.doi.org/10.17703/IJACT.2015.3.2.149

IJACT 15-2-18

A Study of Security Vulnerabilities in Mobile environment

Suk-jin Kim, Hyangran Lee, Malrey Lee*

Center for Advanced Image and Information, Technology,
School of Electronics & Information Engineering, ChonBuk National University, ChonBuk, Korea
hanuri00@jbun.ac.kr, orange1469@naver.com, *mrlee@jbnu.ac.kr

Abstract

Now day's application had focus more on the security and Radio Frequency Identification (RFID) had become one of the major technologies that become important for security. RFID devices are going to be ubiquitous applications that are used in different areas especially in the business because it simplifies many business transactions. However, security and privacy issues and risks are introduced by pervasiveness of RFID systems. In RFID systems, communication between tag and reader usually takes place via wireless communication. As the nature of radio frequency signal, it can go everywhere and everyone can receive this signal, which is an insecure channel. The computational resources in RFID tag are constrained and it is a big limitation that forces researcher to apply different mitigations compared to common security solutions. At the first part of this research, RFID architecture is introduced briefly. In this paper, the researcher explains existing security challenges in RFID networks then the effects of these threats on security and privacy of RFID are discussed. After analyzing security challenges of RFID networks, different countermeasures that are proposed by other researchers are discussed. At the end of this paper, future security challenges are discussed.

Keywords: *component; RFID, Mobile RFID, Security Vulnerability, Security Challenges in RFID*

1. INTRODUCTION

Today, RFID is one of the useful applications in different areas especially in the business because it simplifies many business transactions. Many tasks in inventory systems have been simplified by RFID systems; the tasks such as keeping tracks on consumer products and managing books in the library for librarian. However, security and privacy issues and risks are introduced by pervasiveness of RFID [1].

In RFID systems, communication between tag and reader usually takes place via wireless communication. As the nature of radio frequency signal, it can go everywhere and everyone can receive this signal, which is an insecure channel. The computational resources in RFID tag are constrained and this limitation forces researcher to apply lightweight encryption algorithm but these algorithms do not have the same strength as the normal encryption algorithms such DES or AES. By considering this limitation, there is a trade-off between security and performance of lightweight algorithms and it is needed to evaluate different lightweight algorithms to propose the most fit algorithm [2].

Manuscript Received: Aug. 14, 2015 / Revised: Oct. 12, 2015 / Accepted: Nov. 22, 2015
Corresponding Author: mrlee@jbnu.ac.kr
Tel: +82-63-270-3993, Fax: +82-063-270-2394
Center for Advanced Image and Information, Technology, School of Electronics & Information Engineering, ChonBuk National University

Classical encryption algorithms that had been designed for normal computer is not appropriate for RFID tags because in order to implement these kinds of encryption, enough computational capacity, enough memory, and power should be provided. These limitations force us to design new cryptographic primitive that can provide acceptable security level in RFID system. The name of this kind of cryptography is lightweight cryptography. Deal with the trade-off among security, cost, and performance is key issue of designing lightweight cryptographic algorithm [3].

Security and privacy are important for everyone especially in the today's modern world. By considering that RFID systems can be implemented everywhere in our lives, it is so important to be a secure system. Furthermore, RFID tags contain important information such as health biomedical data, information about products or people, and their physical location in real time. According to Wang Shang-ping (2011), RFID is one of the ten important technologies developed at the end of twenty century, which is an appropriate and capable mechanism to use for identification or authentication in logistics, transportation, entrance control and retail, etc. By concerning the pervasive usage of RFID in future and the importance of security and privacy for everyone, the decision to select this topic was easy.

One of important part of electromagnetic spectrum is Radio that covers all formats of radiation. All parts such as gamma rays, cosmic-ray photons, x-rays, and visible light that were all include in term of electromagnetic spectrum. The Radio Frequency (RF) includes different bands from 30 MHz to 300 MHz. There are tree general bands that are utilized in RFID systems, the first band that it called Low Frequency (LF) at 125 kHz to 134 kHz, the second band is High Frequency (HF) at 13.56 MHz, and the third is Ultra HF at 860 to 930 MHZ. Depending on the different conditions, various types of RFID can be used. To choose an appropriate frequency band, manufactures of RFID equipment consider some criteria such as physical size of the antennas and the required power for transmission [4].

2. RFID ARCHITECTURE

RFID can identify objects that contain small tags in different environments without any physical contact. There are three main components in a typical RFID system: readers, back-end servers, and tags [5].

In RFID systems, transponders are normally called tags or chips; chip implies a smaller unit and tag is used for lager piece of equipment. Each RFID tag contains the following items [4]:

i. Antenna
ii. Encoding/decoding circuitry
iii. Memory
iv. Power supply
v. Communications control

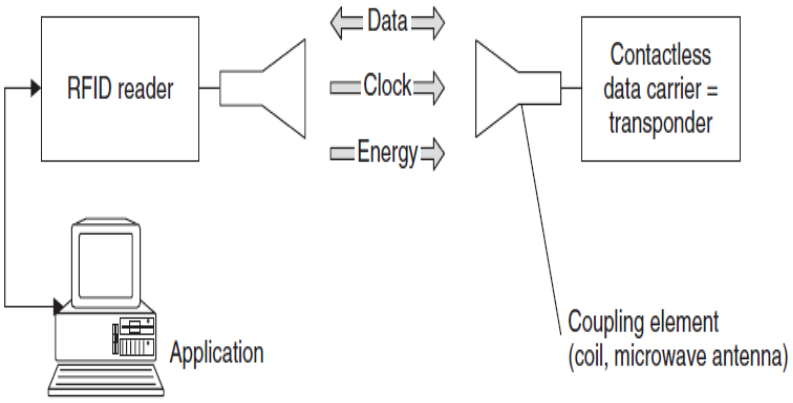

Figure 1. Connection between Readers and Tag [6]

The communication between different parts of RFID network is described in Figure 1. This figure shows RFID system that uses passive tags.

In the first step, a reader antenna transmits radio signal, after that these signals can be received by the tag. After receiving the reader's signal, tag answers with a replying radio signal (Figure 1.1). The signal that transmitted by tag can be redden by reader's receiver. The tag maybe performs some encryption functions depend on it computing power. Different kinds of tag are implemented in RFID system, some of them are read-only and the rest are able to be redden or written [7].

There are three kinds of tag: active, passive, and semi-passive. Passive RFID transponders are without an internal power source. Majority of RIFD transponders are passive. The RF field generated by the reader is a power supply for passive tag. The required supply voltage for passive tag is generated by rectifying the induced voltage which produced by RF signal of Reader. Another type of tag is an active tag that has an integrated power source. The active tag performs similar to passive tag but the speed of processor in this kind of tag is higher than passive tag. The reader signal mostly active tag by trigging [8]. A kind of tag that has a built-in power source, but it still uses the reader's radio signal to power communications that is called semi-passive tag [9].

The reader or interrogator is the second component in a RFID system. The task of the Reader or Transceiver is providing the needed energy for tag and also trigging the communication signals to the tag to do specific actions. The reader can be controlled via a computer terminal or the automatic execution of programs. There are two kinds of application, mobile applications and stationary installation. Hand held readers are used in mobile applications, while the fixed readers directly connected to communication lines and power supply in stationary installation [8].

An antenna of a reader can be integrated to reader or can be separated. The reader typically contains a system interface such as an Ethernet jack or RS-232 serial port, communications control circuits, cryptographic encoding and decoding circuitry, and a power supply or battery. For transforming the data to a LAN or other system, readers use data interface such as serial RS-232 or Ethernet. Different sizes of an antenna are available for readers, from pocket-sized to big antenna with special panel. The size of an antenna depends on a kind of tags that are used in RFID systems [10].

The third component of RFID system is back-end server. The back-end server is typically a PC-type device, hosting business applications. To implement specific business logic, including support of security functions, custom applications are also typically deployed for interfacing with the database or the middleware. The different kinds of standard commercial database are used for backend such as Oracle, Postgres, SQL, My

SQL or similar product. The backend database can run on a single PC in an office or multiple mainframes networked together depending on the application [11].

The International Organization for Standardization and EPC global has defined several protocols. These protocols are explained in Table 1.

Table 1. RFID Tag Protocols [4]

Protocol	Capabilities
EPC™ Generation 1 Class 0	"Read Only," preprogrammed
EPC™ Generation 1 Class 1	"Write" Once, "Read" Many
EPC™ Generation 2.0 Class 1	"Write" Once, "Read" Many; A more globally accepted version of the Generation 1, Class 1 protocol.
ISO 18000 Standard	"Read-Only" tag identifier; may also contain rewritable memory available for user data. ISO 18000 has different subsections depending on the frequency used and the intended application.
ISO 15963	Unique Tag ID
ISO 15961	Data protocols: data encoding rules and logical memory functions
ISO 15962	Data protocols: application interface

3. SECURITY THREATS IN RFID SYSTEMS

RFID systems face the potential risk of being spied out or manipulated similar to any other telecommunication and information technology system. Different types of attack should be analyzed in order to better evaluate potential risks in RFID systems. After that, appropriate cryptographic procedures should be implemented to protect systems from common attacks [6].

RFID systems are imposed to a wide range of malicious attacks that can be categorized from passive eavesdropping to active interference. Attacks against RFID networks can target decentralized parts of the system infrastructure unlike wired networks, where computing systems typically have both host-based defenses and centralized, because RFID tags and RFID readers operate in potentially noisy and unstable environment. Additionally, as RFID technology is improving day by day and so the threats they are disposed to are in the same way evolving. Hence, having a global view of the problem is so difficult [12].

4. ATTACKS ON DIFFERENT LAYERS OF RFID NETWORK

The attacks against RFID networks are classified as follows: the physical layer, the network-transport layer, the strategic layer, and the application layer [12]. The RFID networks security problems can be listed as: tracking, spoofing attack, desynchronization, replay attack, eavesdropping, session hijacking, electromagnetic interference, etc. Each security problem belongs to one layer of different layers of RFID networks [13].

RFID systems face the potential risk of being spied out or manipulated similar to any other telecommunication and information technology system. Different types of attack should be analyzed in order to better evaluate potential risks in RFID systems. After that, appropriate cryptographic procedures should be implemented to protect systems from common attacks [6].

RFID systems are imposed to a wide range of malicious attacks that can be categorized from passive eavesdropping to active interference. Attacks against RFID networks can target decentralized parts of the system infrastructure unlike wired networks, where computing systems typically have both host-based defenses and centralized, because RFID tags and RFID readers operate in potentially noisy and unstable environment. Additionally, as RFID technology is improving day by day and so the threats they are disposed to are in the same way evolving. Hence, having a global view of the problem is so difficult [12].

The attacks against RFID networks are classified as follows: the physical layer, the network-transport layer, the strategic layer, and the application layer [12]. The RFID networks security problems can be listed as: tracking, spoofing attack, desynchronization, replay attack, eavesdropping, session hijacking, electromagnetic interference, etc. Each security problem belongs to one layer of different layers of RFID networks [13].

In this part of research, various threats that cause the security problems for RFID networks are discussed:

- **Jamming and Blocking:** Increasing the amount of tags will basically raise the likelihood of blocking and jamming. To insert the fake tags in reading zone will be much easier and increase numbers of denial of service (DNS) [14].

- **Eavesdropping:** Can be known as intercept data that are being transmitted between two system's components. By using the eavesdropping tools via an attacker, the risk of danger in RFID tags will be increased [15].

- **Tag cloning:** Make the system to read the duplicate legitimate tag. It is possible for an attacker to enter the back-end server and get or destroy the private information [16].

- **Unauthorized tag reading:** Used of unauthorized reader that duplicate from system and collecting the data by reading the tags, the risk can be solved equally between the three categories but the external elements is the factor to the risk., for an example, using an authenticating procedure [17].

- **Relay attacks:** This happen when the authenticated tag and authenticated reader were assume that they were using the right medium to transferred data which that are not true, because the attacker use an unauthenticated tag and unauthenticated reader to make the data to be leaked into the attacker hand [18].

- **Replay attack:** This attack was to attack the system where the system will be attack by the clone, this attack will happen when the interrupting device had capturing the data sent between tag and reader [12].

- **People tracking:** Tracking mobile objects (carriers) use to collect data about the carrier itself by holding a tag using many method [19].

- **Tag content change:** Altering the data – authentication data- Reader will recognize tag as unauthenticated tag and denied access after had false the identity [20].

- **Physical tag destruction:** In this case, a tag cannot send a signal to the reader because a tag is destroyed physically by an attacker [21].

- **Denial/Disruption of Service:** If there are too many fake tags and malicious reader had been deployed, disruption of service may happen if the computer resources had been abused [22].

- **Location-based Attacks (Mafia Fraud/Terrorist Attacks):** There messages from the attacker that will make the two honest side that are involved in protocol to believe that they are very close proximity [10] [23]. Dishonest party that involved in protocol was collaborating with the attacker, which is call terrorist attack [24].

- **Side Channel Analysis:** In the near future, side channel analysis potentially is the most serious threat to RFID tags, which implement cryptographic functions. Several typical side channel information such as computation fault, power consumption, timing information and electromagnetic radiation that can expose RFID secret information for the analysis [25].

Unauthorized tag reading, Replay attacks, tag content, People tracking, and Tag cloning changes can be happened in relay attacks. In this research, threats as a general security problem are considered and these threat are not calculated as RFID architectural problems [14].

5. RELATED WORK AND CURRENT COUNTERMEASURES FOR SECURE RFID

To counter the above threats, the following security properties are required: mutual authentication between tag and reader/back-end server, anonymous/privacy-preserving transaction, forward security, secure key exchange, and secure tag location. In field of RFID networks, a lot of studies have been done to address the security and privacy problems about these systems. Most of previous RFID protocols tried to solve both security and privacy issues but the final solution has always been a security solution and not privacy. It is established that around 70 to 80 percent of related RFID security research works focused on security, 10-15 percent on privacy and only a few works on trust and trusted computing. It means that security and privacy have always been the main focus for every RFID systems and protocols [1]. We now summarize some of countermeasures designed for secure RFID [22]:

- **Hash-based Protocols:** Weis *et al.* (2003) introduced two hash-lock based authentication schemes. But they suffer from secret key disclosure problem, impersonation attack and violation of tag anonymity [26]. Yeo and Kim (2005) proposed hash-chain based protocol providing privacy-protection, tag-to-server authentication and forward security but server-to-tag authentication cannot be provided in this case. Furthermore, the hash chains should be computed by the server to identify a tag [27].

- **LPN-based Protocols:** Juels *et al.* proposed HB+, which employs binary-inner product and based on the learning parity with noise (LPN) problem. HB+ repeats a basic authentication protocol with a noise bit,

and accepts the tag only if a very limited number of responses are invalid. HB+ is weak against some attacks such as man-in-the-middle attacks and does not achieve anonymity and forward security [28]. Extensions and improvements of HB protocol like [29], HB++ [30], HB-MP [31] have been proposed but these protocols only consider the authentication of tags and not readers, and suffer from tracking problem and violation of tag anonymity.

- **Ultra-lightweight Protocols:** The main idea of proposing these protocols is providing RFID security using different ultra-lightweight primitives that are suitable for RFID systems. The trade-off among security, cost, and performance is the key issue of designing lightweight cryptographic algorithms is to deal with the [3]. RFID tags are resource-constrained smart devices, and the processing power of tags is usually low. By considering the limitation of resources in RFID tags, it should be necessary to focus on lightweight symmetric ciphers in this paper. The previous proposals in field of RFID security can be divided into the three categories. In the first category, highly optimized and compact hardware implementations are available and block ciphers such as AES and IDEA can be implemented easily [32], while in the second category, for lightweight applications a classical block cipher like DES can be used [33]. Finally, in the third category, new low-cost designs are considered. There are a lot of previous studies that tried to improve security in resource-constrained especially RFID tags such as mCrypton [34], PRESENT [35], lightweight block ciphers HIGHT [36], SEA [37], KTANTAN [38] , TEA [39], and Hummingbird [40], as well as lightweight stream ciphers Grain [41] and Trivium [13]. These primitives that are used include MULTIPLY, EXOR, NOT, ROTATE, AND, OR, random number generator, CRC, and ADD. To achieve this purpose, there are some protocols: Peris- Lopez et al. (2009), Han and Kwon (2009), Hung-Yu (2007), and Karthikeyan et al. (2005). These protocols are highly desirable for low-cost RFID tags, but do have drawbacks like key disclosure, and de-synchronization attacks. Therefore they need further strengthening and research. Various schemes have been proposed to solve security issues of RFID systems. There are two gereral groups of provided solutions. Using jamming, blocking and physical solutions is the first group. Cryptographic concepts and privacy preserving protocols are used in other groups. Cryptographic solutions that have proposed for RFID security issues can be divided into two main groups, complex cryptographic and lightweight solutions. It is not impossible to use complex cryptographic protocols in future RFID tags but most RFID researchers, believe that the industry needs low cost and simple RFID tags with limited number of logical gates. Many solutions have been suggested for this case that are based on the lightweight cryptographic solutions and protocols. In case of that the price of RFID tags should be very low, lightweight protocols are useful because of keeping the very low computational demand. The researcher performs a security analysis of five lightweight protocols, and show that they are vulnerable to some simple security attacks, in this article [42].

- **Universal Composability (UC) Protocols:** O-FRAP Protocol [43], Optimistic Forward Secure RFID Authentication Protocol is the first full-fledged protocol, which is proven secure in a UC-based security framework [44]. The mutual authentication, privacy-preserving, a mechanism to prevent de-synchronization of secret key attack, and forward security can be achieved by this protocol. To get better results, O-FRAP can be improved to be key exchanger. To protect privacy of a tag, this protocol uses pseudonym approach But it is shown to be susceptible to tracing attack and violation of forward security in [45].

- **Multi Tag Scanning Protocols:** Juels et al. (2005) proposed yoking-proof that was the first protocol to identify the multiple tag scanning issues. A reader can make a co-existence proof of two tags by using this protocol. Allowing two tags sign each other's random number is the basic idea in the yoking-proof protocol. The signing algorithm can be a message authentication code scheme. Recently, Saito et. al. (2005), Piramuthu (2006), and Burmester et al. (2009) extended yoking-proof to support multiple scanning of several tags, called the grouping-proof.

- **Distance-bounding Protocols:** Hancke et al. (2005) proposed kind of protocol that can identify mafia-fraud attack on RFID. Repeating a simple authentication step multiple times is the main idea in this protocol so that each step can be complete in a very short time. Recently, Chong Hee (2011) proposed a more secure protocol based on binary mixed challenges.

- **Side channel analysis and protection on RFID:** The electromagnetic analysis of high frequency (HF) RFID tag operating at 13.56 MHz, was performed by Kim et al. (2010), etc. Clavier et al. (2010) introduced power analysis and electromagnetic attack on their own RFID prototype with AES implementation under artificially generated passive HF RFID settings, but did not describe any countermeasures. Recently, side channel analysis on targeted RFID tag shifted to ultra-high frequency (UHF) RFID tag, which normally works at 900 MHz. Oren and Shamir (2007) showed a successful analysis result which can be used to extract kill password remotely from a UHF EPC tag. The authors suggested common countermeasures to prevent the analysis with some examples.

6. CONCLUSION

This article presents fundamental observations about the vulnerability of commonly-used passive RFID tags. It is the first work that provides concrete results of practical experiments in the context of fault analysis on RFID devices. Global fault-injection methods on HF and UHF tags are described as well as local methods. The difference between Global fault-induction methods affect and local-fault induction methods is that Global fault-induction analyzes the entire chip at once, but local-fault induction analyzes special parts of entire chip. The effects of electromagnetic interferences are analyzed in this study. Optional inductions can counted as a very convenient fault-injection method because of effective manner of this method. Investigation the susceptibility of faults on RFID gadgets and identification weaknesses in RFID devices is the main purpose of this study. As a result, only the tags are examined by the researcher that excludes other countermeasures against fault-analysis attacks at this stage. In this study, the researcher has focused on various operations that which are critical when execution time and power consumption are important for us. It is shown that fault-injection methods can prevent modification of tag's content and also the writing of faulty values. There is a trade-off between cost, security, and performance in RFID systems because as the nature of RFID tags, there is limitation in resources such as computational capacity, memory, and power capacity [46]. Potential weaknesses of RFID tags is described to provide a basis for future researches like analysis of the susceptibility of cryptographic-enabled RFID tags to faults, in this research. It is concluded that countermeasures against fault analysis have to be considered especially in applications where security is of increasing interest.

ACKNOWLEDGEMENTS

This work (Grants No: 1401001175) was supported by Business for Academic-industrial Cooperative establishments funded Korea Small and Medium Business Administration in 2015.

REFERENCES

[1] M. F. Mubarak, *et al.*, "A critical review on RFID system towards security, trust, and privacy (STP)," in *2011 IEEE 7th International Colloquium on Signal Processing and Its Applications, CSPA 2011, March 4, 2011 - March 6, 2011*, Penang, Malaysia, 2011, pp. 39-44.

[2] W. Shang-Ping, *et al.*, "An Authentication Protocol for RFID Tag and its Simulation," *Journal of Networks*, vol. 6, pp. 446-453, 2011.

[3] A. Poschmann, *et al.*, "Lightweight Cryptography and RFID: Tackling the Hidden Overheads Information, Security and Cryptology – ICISC 2009." vol. 5984, D. Lee and S. Hong, Eds., ed: Springer Berlin / Heidelberg, 2010, pp. 129-145.

[4] F. Thornton, *et al.*, *RFID Security*: Syngress, 2005.

[5] I. Erguler and E. Anarim, "Security flaws in a recent RFID delegation protocol," pp. 1-13, 2011.

[6] K. Finkenzeller, *et al.*, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication*: John Wiley & Sons, 2010.

[7] P. H. Cole, *Networked RFID systems and lightweight cryptography : raising barriers to product counterfeiting*. Berlin [u.a.: Springer, 2008.

[8] P. Kitsos and Y. Zhang, *RFID security: techniques, protocols and system-on-chip design*: Springer, 2008.

[9] B. Glover and H. Bhatt, *RFID essentials*: O'Reilly, 2006.

[10] W.-J. Yoon, *et al.*, "Implementation and performance evaluation of an active RFID system for fast tag collection," *Computer Communications*, vol. 31, pp. 4107-4116, 2008.

[11] S. Ahson and M. Ilyas, *RFID handbook: applications, technology, security, and privacy*: CRC Press, 2008.

[12] A. Mitrokotsa, *et al.*, "Classifying RFID attacks and defenses," *Information Systems Frontiers*, vol. 12, pp. 491-505, 2010.

[13] G. Jiezhong, *et al.*, "A secure authentication protocol for RFID based on Trivium," in *Computer Science and Service System (CSSS), 2011 International Conference on*, 2011, pp. 107-109.

[14] M. a. Naser, *et al.*, "A framework for RFID systems' security for human identification based on three-tier categorization model," in *2009 International Conference on Signal Acquisition and Processing, ICSAP 2009, April 3, 2009 - April 5, 2009*, Kuala Lumpur, Malaysia, 2009, pp. 103-107.

[15] R. K. Pateriya and S. Sharma, "The Evolution of RFID Security and Privacy: A Research Survey," in *Communication Systems and Network Technologies (CSNT), 2011 International Conference on*, 2011, pp. 115-119.

[16] G. Kapoor and S. Piramuthu, "Vulnerabilities in Chen and Deng's RFID mutual authentication and privacy protection protocol," *Engineering Applications of Artificial Intelligence*, vol. 24, pp. 1300-1302, 2011.

[17] C. Bae-Ling, *et al.*, "Security on the Design of RFID Access Control Protocol Using the Strategy of Indefinite-Index and Challenge-Response," in *Genetic and Evolutionary Computing (ICGEC), 2011 Fifth International Conference on*, 2011, pp. 9-12.

[18] Z. Yanjun, "Survivable RFID Systems: Issues, Challenges, and Techniques," *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, vol. 40, pp. 406-418, 2010.

[19] F. Xiaoxing, *et al.*, "An UHF RFID transponder with novel demodulator and security algorithm," in *2009 3rd International Conference on Anti-counterfeiting, Security, and Identification in Communication, ASID 2009, August 20, 2009 - August 22, 2009*, Hong Kong, China, 2009, p. Guizhou Normal University; Xiamen University; City University of HK; CAS/COM Chapter IEEE HK.

[20] T. Good and M. Benaissa, "A low-frequency RFID to challenge security and privacy concerns," in *Mobile Adhoc and Sensor Systems, 2009. MASS '09. IEEE 6th International Conference on*, 2009, pp. 856-863.

[21] K. Hyun-Seok, *et al.*, "The Vulnerabilities Analysis and Design of the Security Protocol for RFID System," in *Computer and Information Technology, 2006. CIT '06. The Sixth IEEE International Conference on*, 2006, pp. 152-152.

[22] D. Dang Nguyen, *et al.*, "Open issues in RFID security," in *Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for*, 2009, pp. 1-5.

[23] K. Chong Hee and G. Avoine, "RFID Distance Bounding Protocols with Mixed Challenges," *Wireless Communications, IEEE Transactions on*, vol. 10, pp. 1618-1626, 2011.

[24] M. Soini, *et al.*, "- The challenges on the development of mobile controlled rfid system," in *Mechatronics for Safety, Security and Dependability in a New Era*, A. Eiji and A. Tatsuo, Eds., ed Oxford: Elsevier, 2006, pp. 301-304.

[25] T. Hollstein, *et al.*, "Security challenges for RFID key applications," *RFID Systems and Technologies (RFID SysTech), 2007 3rd European Workshop on*, pp. 1-12, 2007.

[26] C. Hung-Yu, "Secure Access Control Schemes for RFID Systems with Anonymity," in *Mobile Data Management, 2006. MDM 2006. 7th International Conference on*, 2006, pp. 96-96.

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

[28] A. Juels and S. Weis, "Authenticating Pervasive Devices with Human Protocols," in *Advances in Cryptology ??{CRYPTO} 2005*, 2005, pp. 293-308.

[29] J. Katz and J. Shin, "Parallel and Concurrent Security of the HB and HB⁺ Protocols Advances in Cryptology - EUROCRYPT 2006." vol. 4004, S. Vaudenay, Ed., ed: Springer Berlin / Heidelberg, 2006, pp. 73-87.

[30] J. Bringer, *et al.*, "HB^+^+: a Lightweight Authentication Protocol Secure against Some Attacks," in *Security, Privacy and Trust in Pervasive and Ubiquitous Computing, 2006. SecPerU 2006. Second International Workshop on*, 2006, pp. 28-33.

[31] J. Munilla and A. Peinado, "HB-MP: A further step in the HB-family of lightweight authentication protocols," *Computer Networks*, vol. 51, pp. 2262-2267, 2007.

[32] D. Engels, *et al.*, "Hummingbird: ultra-lightweight cryptography for resource-constrained devices," presented at the Proceedings of the 14th international conference on Financial cryptograpy and data security, Tenerife, Canary Islands, Spain, 2010.

[33] C. Paar, *et al.*, "New Designs in Lightweight Symmetric Encryption RFID Security," P. Kitsos and Y. Zhang, Eds., ed: Springer US, 2009, pp. 349-371.

[34] C. H. Lim and T. Korkishko, "MCrypton - A lightweight block cipher for security of low-cost RFID tags and sensors," in *6th International Workshop on Information Security Applications, WISA 2005, August 22, 2005 - August 24, 2005*, Jeju Island, Korea, Republic of, 2005, pp. 243-258.

[35] A. Bogdanov, *et al.*, "PRESENT: An ultra-lightweight block cipher," in *9th International Workshop on Cryptographic Hardware and Embedded Systems, CHES 2007, September 10, 2007 - September 13, 2007*, Vienna, Austria, 2007, pp. 450-466.

[36] D. Hong, *et al.*, "HIGHT: A new block cipher suitable for low-resource device," in *8th International Workshop on Cryptographic Hardware and Embedded Systems, CHES 2006, October 10, 2006 - October 13, 2006*, Yokohama, Japan, 2006, pp. 46-59.

[37] F. Mace, *et al.*, "FPGA Implementation(s) of a Scalable Encryption Algorithm," *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on*, vol. 16, pp. 212-216, 2008.

[38] C. De Cannière, *et al.*, "KATAN and KTANTAN — A Family of Small and Efficient Hardware-Oriented Block Ciphers Cryptographic Hardware and Embedded Systems - CHES 2009." vol. 5747, C. Clavier and K. Gaj, Eds., ed: Springer Berlin / Heidelberg, 2009, pp. 272-288.

[39] P. Israsena, "Securing ubiquitous and low-cost RFID using tiny encryption algorithm," in *Wireless Pervasive Computing, 2006 1st International Symposium on*, 2006, p. 4 pp.

[40] X. Meng-Qin, *et al.*, "Low power implementation of hummingbird cryptographic algorithm for RFID tag," in *Solid-State and Integrated Circuit Technology (ICSICT), 2010 10th IEEE International Conference on*, 2010, pp. 581-583.

[41] M. Hell, *et al.*, "A Stream Cipher Proposal: Grain-128," in *Information Theory, 2006 IEEE International Symposium on*, 2006, pp. 1614-1618.

[42] E. Vahedi, *et al.*, "Security Analysis and Complexity Comparison of Some Recent Lightweight RFID Protocols Computational Intelligence in Security for Information Systems." vol. 6694, Á. Herrero and E. Corchado, Eds., ed: Springer Berlin / Heidelberg, 2011, pp. 92-99.

[43] T. V. Le, *et al.*, "Universally composable and forward-secure RFID authentication and authenticated key exchange," presented at the Proceedings of the 2nd ACM symposium on Information, computer and communications security, Singapore, 2007.

[44] M. Burmester, *et al.*, "Universally Composable RFID Identification and Authentication Protocols," *ACM Trans. Inf. Syst. Secur.*, vol. 12, pp. 1-33, 2009.

[45] K. Ouafi and R. Phan, "Traceable Privacy of Recent Provably-Secure RFID Protocols Applied Cryptography and Network Security." vol. 5037, S. Bellovin, *et al.*, Eds., ed: Springer Berlin / Heidelberg, 2008, pp. 479-489.

[46] Y. Oren and A. Shamir, "Remote Password Extraction from RFID Tags," *Computers, IEEE Transactions on*, vol. 56, pp. 1292-1296, 2007.

[47] C. Clavier, *et al.*, "Passive and Active Combined Attacks on AES Combining Fault Attacks and Side Channel Analysis," in *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2010 Workshop on*, 2010, pp. 10-19.

[48] P. Peris-Lopez, *et al.*, "LAMED - A PRNG for EPC Class-1 Generation-2 RFID specification," *Comput. Stand. Interfaces*, vol. 31, pp. 88-97, 2009.

[49] A. Juels, ""Yoking-proofs" for RFID tags," in *Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second IEEE Annual Conference on*, 2004, pp. 138-143.

[50] G. P. Hancke and M. G. Kuhn, "An RFID Distance Bounding Protocol," in *Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on*, 2005, pp. 67-73.

[51] Y. C. Kim, *et al.*, "Side channel analysis countermeasures using obfuscated instructions," in *Security Technology (ICCST), 2010 IEEE International Carnahan Conference on*, 2010, pp. 42-51.

[52] P. Peris-Lopez, *et al.*, "Vulnerability analysis of RFID protocols for tag ownership transfer," *Computer Networks*, vol. 54, pp. 1502-1508, 2010.

[53] S. Weis, *et al.*, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems," 2003.

[54] S.-S. Yeo and S. Kim, "Scalable and Flexible Privacy Protection Scheme for RFID Systems Security and Privacy in Ad-hoc and Sensor Networks." vol. 3813, R. Molva, *et al.*, Eds., ed: Springer Berlin / Heidelberg, 2005, pp. 153-163.

[55] A. Juels, "Power games in RFID security," in *Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for*, 2009, pp. 1-1.

[56] S. Vaudenay, "On Privacy Models for RFID Advances in Cryptology – ASIACRYPT 2007." vol. 4833, K. Kurosawa, Ed., ed: Springer Berlin / Heidelberg, 2007, pp. 68-87.

[57] S. Karthikeyan and M. Nesterenko, "RFID security without extensive cryptography," presented at the Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks, Alexandria, VA, USA, 2005.

[58] J. Saito and K. Sakurai, "Grouping proof for RFID tags," in *Advanced Information Networking and Applications, 2005. AINA 2005. 19th International Conference on*, 2005, pp. 621-624 vol.2.

[59] S. Piramuthu, "On Existence Proofs for Multiple RFID Tags," in *Pervasive Services, 2006 ACS/IEEE International Conference on*, 2006, pp. 317-320.