Analyses of Security Issues and Requirements for RFID System and Its Application

Jung-Te Kim, *Member, KIMICS*

Abstract — RFID security and privacy issues have been intensively studied in the research field, the authentication between RFID reader and tag is the fundamental them. Most of the existing authentication protocols draw assumptions on classic primitives. Since tags have small capacities, the security mechanisms which are in use in computer networks and communication are not suitable. In this paper, we compare and analyze recent technical research on the problems of privacy and security. It consists of security mechanism, threats and performance evaluation, etc.

Index Terms— Authentication, RFID, Ubiquitous system, lighted weight algorithm

I. INTRODUCTION

An emerging application is ubiquitous applications. The use of RFID tags for anti-counterfeiting by embedding them into a product is widespread. Public key cryptography (PKC) offers an attractive solution to the counterfeiting problem but whether a public key cryptosystems can be implemented on an RFID tags or not remains unclear. RFID based on identification is an example of an emerging technology which requires authentication as a cryptographic service. This property can be achieved by symmetric as well as asymmetric primitives. Previous work considered only symmetric key algorithms such as AES. It is not clear whether public key algorithms can be implemented in constrained devices, such RFID tag, and still depends on the area, performance and power requirements in typical of these applications. Many protocols have been proposed for use in RFID systems. We focus on RFID authentication protocols requiring synchronization between a tag and a back-end server, which operate under the following assumptions. The RFID tag consists of a tiny microchip and an antenna. RFID systems always consist of three major components as shown in fig.1.

1) Server or application system
2) Reader or transceiver including antenna which communicates with the tag
3) Tag or RFID label or transponder which is placed on the object to be identified

An RFID protocol consists of three flows. Typically, the first flow is a query from a server to a tag, the seconds is the reply of the tag to the server for tag authentication, and the third is the response from the server to the tag for server authentication. A server and a tag share secrets used for mutual authentication. They update the shared secrets synchronously whenever they perform a successful authentication session; a server updates tag secrets stored in its DB after receiving the second flow and having authenticated the tag, and the tag updates its stored secrets after receiving the third flow and having authenticated the server [1].

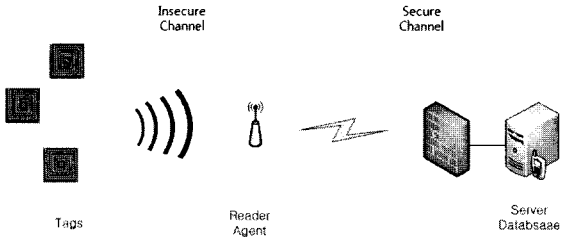


Fig. 1 Configuration of Basic RFID system

II. SECURITY ISSUES ON RFID PROTOCOL

2.1 ATTACKS ON RFID PROTOCOL

Active attacks and eavesdropping attacks may violate individual privacy as well as leak sensitive inventory data. Traffic analysis attacks also present a threat, particular to an individual's location privacy and to organizational logistics data. Denial of service

Manuscript received May 10, 2009; revised June 6, 2009.

Jung-Tae Kim is with the Department of Electronic, Mokwon University, Taejon, 302-729-123, Korea (Tel: +82-42-829-7657, Fax: +82-42-823-8506 jtkim3050@mokwon.ac.kr)

may also be a potentially expensive and disruptive attack. Active querying attacks may be addressed by limiting who is permitted to read tag data through access control. Eavesdroppers may be dealt with by ensuring that tag contents are not broadcast in the clear over the forward channel. There are several general types of adversarial attacks on RFID developments. The representative factor presented as follows.

- Tag disabling: Adversary causes tags to assume a state from which they can no longer function.
- Tag cloning: Adversary captures the identifying information of a tag.
- Tag tracking: Adversary traces tags from their protocol flows.
- Replay: Adversary uses a tag's response to a reader's challenge to impersonate the tag.
- Offline man-in-the-middle attacks: Adversary interposes between a tag and a reader and exchanges their messages.

There are also attacks that are usually excluded from the security model used, such as power analyses or side channel attacks and man-in-the-middle relay attacks [2].

2.2 VULNERABILITY OF RFID PROTOCOL

Security design of the protocol should not impede normal operations, and should prevent a malicious adversary from getting any information [2]. We consider the following measures:

A. Secrecy/Authentication

The cryptographic methods used (for example the keyed Hash function H) correspond to the state of the art in industry today, and reasonably guarantee the secrecy of the message. Thus, we assure the recipient that the messages originate from valid sources.

B. Indistinguishableness/Tracking/Passive Replay

Using a freshly generated random nonce with every message in the protocol, it is impossible to track the tag. Assume that an adversary pretends to be a genuine reader. He sends out a query, and receives a message back. Next time he sends a query, along with a fresh nonce, he receives a different message, so he cannot track the tag. Of course, with multiple tags in an area, tracking a specific tag without keys is extremely difficult if not impossible.

C. Forward Security

This means that the current key of a tag has been found, and can be used to extract previous messages (assuming that all its past conversations are recorded). Let's say the adversary somehow finds keys. The tag always communicates using a hash function. The adversary cannot use the key to decode any of the tag's messages because the one-way hash function H is considered computationally un-invertible. In other words, the adversary needs to have access to the hash digest table for lookups. So, he cannot decipher/recreate any past messages sent with previously used keys. There are a number of solutions proposed so far to solve the security problems and threats associated with the use of RFID systems.

III. REQUIREMENTS OF SECURITY SOLUTIONS

Some of authentication protocols use hash algorithm and symmetry key algorithms due to their simplicity compared to public key algorithms. However, they fail to satisfy the mentioned basic requirements of RFID systems. It is shown that a public key cryptographic algorithm is necessary to satisfy the required properties. We evaluate the two primitives.

3.1 Symmetric key primitives

Symmetric key cryptographic primitives for privacy or authentication are efficient and focus on implementation of these primitives. Not many papers show primitives specifically at the tightly constrained environments of RFID tags. Vajda and Buttyan proposed a medley of lightweight cryptographic primitives for RFID tags authentication [3]. Feldhofer, Dominikus, and Wolkerstorfer propose lightweight hardware implementation of a symmetric key cipher, namely, 1 128 bit version of the Advanced Encryption Standard (AES). Their design requires just over 3500 gate equivalents, considerably more than appropriate for basic RFID tags, but suitable for higher cost RFID tags [4].

3.2 Asymmetry key primitives

The task of an RFID tag is to provide information over the radio channel using minimal hardware components. This work can be supported by ECC processor for RFID tags which implements an ECDSA signature generation device. ECC is utilized to gain strong resistance against cryptographic attacks and to reduce the storage requirements. The RFID tag will provide cryptographic authentication and copy protection with the help of the digital signature. The Elliptic Curve Digital Signature Algorithm (ECDSA) provides authentication utilizing the elliptic curve discrete logarithm problem as underlying intractable

operation. ECC promises the same security level for a 160 bit key as with the RSA method using 1,000 bit key [5]. This makes ECDSA attractive for small devices like RFID tags, where the die size is the major cost factor. Recently, a few papers discussed feasibility of ECC based PKI on RFID tags [6]. Gaubatz et al showed that RSA is not a feasible solution while encryption can be implemented in about 3,000 gates [7]. Recent work of Wolkerstorfer is the first to claim possible to have low power and compact implementation of ECC that meets the constraints imposed by the EPC standard [8]. We analyzed various standardized cryptographic algorithms which have a high level of security, optimized the implementation for application in passively powered RFID tags. This helps protocol designers to estimate costs more accurately. Table I explains the main features of the realized crypto modules SHA-256, SHA-1, MD5, AES-128, and ECC-192. Table I shows that public key computation (ECC-192) take much longer. Moreover, ECC is in terms of power consumption and chip area more cost intensive. The implementation in a modern process technology could solve in future. The comparison of the other algorithms shows that AES-128 is best suitable for implementation in passive RFID tags because it requires by far the smallest chip area. AES-128 also features the lowest power consumption. Additionally, the higher level of security (128 bits) in comparison to competing algorithm MD5 puts the slightly higher 1,032 clock cycles into perspective. The comparison gives strong arguments for favoring AES. Some focus on ultra low cost AES design which can be used in RFID, which can be found in [5].

Table 1 Comparison of performance of algorithm

Algorithm	Security [bits]	I_{mean} (uA@ 100kHz)	Chip area	Clock [cycles]
SHA-256	128	5.86	10,868	1,128
SHA-1	80	3.93	8,120	1,274
MD5	80	3.16	8,001	712
AES-128	128	3.0	3,400	1,032
ECC-192	96	18.85	23,600	502,000

To satisfy RFID security and system requirements, it is proven that a public key cryptosystem is necessary. An Elliptic Curve (EC) based cryptosystem would be one of the best candidates for the RFID systems due to its small key size and efficient computation [9]. The comparison of the SGD (Signature generation device) to other ECDSA devices involves chip area, cycle count for signature generation and consideration about side channel resistance. SPA means simple power analyses and DPA shows differential power analyses.

Table 2 Comparison of Various ECDSA devices

ECDSA Devices	Gates.	Cycles	SCA Considered	Field
SGD-192	22.6K	502K	SPA & DPA	$GP_{(p192)}$
ECC P(*)	23.8K	677K	SPA & DPA	$GP_{(p192)}$
		426K		$GP_{(2^{192})}$
ECC P(**)	19K	527K	SPA & DPA	$GP_{(2^{193})}$
8051+ECAU (***)	29K	1416K	No	$GP_{(2^{192})}$
SGD-160	19K	362K	SPA & DPA	$GP_{(p160)}$
PACS(****)	46K	134K	No	$GP_{(2^{163})}$
MALU(*****)	5.3K	353K	SPA & DPA	$GP_{(2^{163})}$

J. Wolkerstorfer presented a dual field arithmetic unit in for GF(p) and GF(2m). Paar and Kumar showed that a way to calculate the scalar multiplication kP over GF(2m) with their ECC processor. M. Koschuch, et al, showed that an approach for an ECC crypto extension using a 8051 processors was shown. The PACS for medical applications gives a very fast processor using windowing techniques on EC layer, but utilizing the most gates. The MALU is a very small circuit for scalar point multiplication over GF(2m) but will need another microcontroller to finish the digital signature like all GF(2m) approaches [10].

ECC is based on discrete logarithms that are more computationally expensive to invert at equivalent key length than other algorithm. Even though ECC offers greater per key bit, its complex elliptic curve algorithm makes it computationally intensive and thus generally less suitable in small, lightweight, low power application environments. Computation cost and communication cost are the most important aspects of password authentication protocols which affect the overall performance. They include number of steps, exponentiations, large blocks, symmetric encryption and decryption, hash functions and random numbers. We compare the EC-SAKA (Elliptic Curve Secure Authentication Key Agreement), Leakage Resilient Authenticated Key Exchange (LR-AKE) protocol, Simple Key Agreement (SKA) protocol, Secure Remote Password (SRP) protocol, EC-SRP, Simple Password Exponential Key Exchange (BSPEKE) protocol, Password Authenticated Key Exchange (PAK) protocol and Authentication Memorable Password (AMP) protocol [11]. The comparison is done in terms of number of steps, random numbers, exponentiations and hash functions.

Table 4 shows the compared result for random numbers and hash functions. From table 3, EC-SAKA protocol has the minimal cost in term of number steps and exponentiations compared with these above protocols. Its computational load is also improved using EC-SAKA protocol as shown in table 3. From the table 2, we can easily notice that EC-SAKA protocol requires 2 random numbers and 5 hash functions while all the other protocols require more [11].

Table 3 Comparison of computational load

Protocol	Rounds	Exponentiations		
		Client	Server	Total
B-SPEKE	4	3	4	7
SRP	4	3	3	6
AMP	4	2	3	5
PAK-RY	3	5	4	9
PAK-X	3	5	4	9
SKA	3	2	3	5
LR-AKE	3	3	4	5
AKEECC	4	2	4	4
EC-SRP	3	2	4	4
EC-SAKA	3	1	0	1

Table 4 Comparison of random number and hash function number

Protocol	Random N.	Hash Function N.
SRP	2	6
AMP	2	9
PAK-RY	3	8
AK-X	3	10
SKA	2	7
LR-AKE	2/4	6
AKEECC	2	6
EC-SRP	3	5
EC-SAKA	2	5

IV. COMPARISON OF PERFORMANCE

Some of the security properties of protocols are listed as below.

A. Security analyses

▪ Confidentiality:

This is a mechanism to guarantee a tag's privacy. In real design, a tag's secret values will never be disclosed in clear during the protocol execution.

▪ Tag anonymity:

As the ID of the tag is static, we should send it, and all other interchanged messages, in random wraps (i.e., to an eavesdropper, random numbers are sent).

▪ Tag/reader authenticity:

We can design the protocol with both reader-to-tag authentication (due to messages A and B) and tag-to-reader authentication (due to message C). These are achieved via the shared and synchronized secrets at both sides, and the permanent hidden value (ID) as well.

B. Performance Analysis

We can estimate and make a close comparison of protocol to compare performance in terms of computational, storage and communication overhead.

- Computational overhead:
- Storage overhead:
- Communication overhead:

As mentioned earlier, the primary objective of ECC is to provide a ready-to-use, publicly available software package for ECC based PKC operations that can be flexibly configures and integrated into sensor network application. To achieve this goal, we follow several principles in the design and development of ECC.

1. Security
2. Portability
3. Resource awareness and configurability
4. Efficiency
5. Functionality

The security protocol has lots of issues that can be continued for future study.

1) Backend system loading issue
2) Strong hash function software simulation issue
3) Whole scheme hardware simulation issue
4) RFID offline mode operation

C. Comparison of current technology

We analyze the performance of some current compact algorithm where block ciphers are ordered by block and key size while hash functions are ordered by the size of the output. Table 5 shows that the hash functions available are unsuitable in practice. When we consider what we need from a hash function in an RFID tag based application, we can consider issues. In tag based application, we do not need the property of collision resistance. Most often the security of the protocol depends on the one way property. It is safe to use hash functions with smaller hash outputs. Applications will typically require moderate levels. Consequently 80 bit security, or even less, may be adequate [12].

Table 5 Comparison of different ciphers

	Model	Key size	Block size	Cycles Per block	Throughput at 100KHz	Logic Process(um)	Area (GE)
Block ciphers	PRESENT-80[1]	80	64	32	200	0.18	1
	PRESENT-80[2]	80	64	563	11.4	0.18	0.68
	DES	56	64	144	44.4	0.18	1.47
	mCrypton	96	64	13	492.3	0.13	1.71
	PRESENT-128	128	64	32	200	0.18	1.20
	TEA	128	64	64	100	0.18	1.50
	HIGHT	128	64	34	188.2	0.25	1.65
	DESXL	184	64	144	44.4	0.18	1.38
	AES-128	128	128	1032	12.4	0.35	2.17
Stream ciphers	Grain	1	1	1	100	0.13	0.82
	Trivium	1	1	1	100	0.13	1.66

V. CONCLUSIONS

RFID is a widely adopted identification technology in recently. In this paper, we analyses security schemes and vulnerability, etc, in RFID application. Taking this RFID-system issue, we can categorize the security threats related to issues by means of information security and privacy. Neither a symmetric nor an asymmetric cryptographic deployment is necessarily with light weighted algorithm. Both have advantages and disadvantages and their relative suitability will depend on the application. We carefully analyzed the current issues so that it is pretty secure against a variety of advanced attacks and compact architectures.

ACKNOWLEDGMENT

This work was supported in part of my work in ISI at Queensland University of Technology.

REFERENCES

[1] S. A. Weis, S. E. Sarma, R. Rivest, and D. W. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," in Proc. 1st Security Pervasive Comput., 2003, vol. 2802, Lecture Notes in Computer Science. Berlin, Germany: Springer-Verlag, pp. 201–212.

[2] P. Ekdahl, and T. Johansson, "Another attack on A5/1", IEEE Transactions on Information Theory, V.49, N.1, pp.284-289, 2003.

[3] I. Vajda and L. Buttyan, "Lightweight authentication protocols for low cost RFID tags," in Proc, 2nd Workshop on Security in Ubiquitous Computer, 2003, pp.76-82

[4] M. Feldhofer, etcs, "Strong authentication for RFID systems using the AES algorithm," Cryptographic hardware and embedded systems", CHES 2004, v.3156, pp.357-370, 2004.

[5] Martin Feldhofer, "Strong crypto for RFID Tag, - A comparison of low power hardware implementation", 2007 IEEE, pp.1839-1842.

[6] Mangard,S, et al, "Power analyses attacks-revealing the secrets of smartcards", Springer-ISBN: 0-387-30857-1,2007

[7] G.Gaubatz, et.al, "Public key Cryptography in sensor network", 1st European workshop on security in Ad Hoc and sensor networks", ESAS 2004, Aug.2004

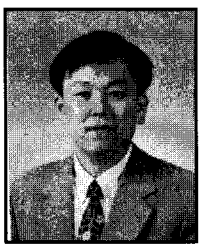
[8] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong authentication for RFID systems using the AES algorithm," in Proc. WorkshopCryptographic Hardware Embedded Syst. (CHES 2004), Lecture Notes in Computer Science. Berlin, Germany: Springer-Verlag, vol. 3156, pp. 357–370.

[9] Yong Ki Lee, etcs, "Elliptic Curve Based Security Processor for RFID", IEEE Transactions on Computers, v.57. n.11, pp. 1514-1526, NOV. 2008.

[10] Pieer E, etcs, "A Fast Secure Elliptic Curve Based Authenticated Key Agreement Protocol For Low Power Mobile Communications", The 2007 International Conference on Next Generation Mobile Applications, Services and Technologies, pp.33.-38, 2007.

[11] Pieer E, etcs, "A Fast Secure Elliptic Curve Based Authenticated Key Agreement Protocol For Low Power Mobile Communications", The 2007 International Conference on Next Generation Mobile Applications, Services and Technologies, pp.33.-38, 2007.

[12] Andrey B,etcs, "Hash functions and RFID tags: Mind the Gap:, CHES 2008, LNCS, pp.283-299, 2008



Jung-Tae Kim
received his Ph.D. degrees in Electrical and Electronic Engineering from the Yonsei University in 2001. From 1991 to 1996, he joined at ETRI, where he worked as senior member of technical staff. In 2002, he joined the department of electronic engineering, Mokwon University, Korea, where he is presently professor. His research interest is in the area of information security system technology that includes network security system design, USN and RFID security protocol.