공개키 암호시스템에서 RFID 보안

선동규

삼성 SDS 통합보안컨설팅그룹

Security of RFID in Public Key Cryptosystem

Dong Kyu Seon

Samsung SDS Integrated Security Consulting Group

E-mail: dk.seon@samsung.com

요 약

이 논문에서는 RFID(Radio Frequency IDentification)에 대한 여러 가지 보안위협에 대하여 간단히 알아보고 그에 대응하는 안전한 암호학적 도구(Primitive)에 대하여 알아보겠다. 공개키 암호시스템(PKC, Public Key Cryptosystem)에 사용되는 타원곡선(EC, Elliptic Curve) 암호, NTRU(N-th degree TRUncated polynomial ring) 암호, Rabin 암호 등은 초경량 하드웨어 구현에 적합한 차세대 암호시스템으로서 안전한 RFID 인증서비스 제공과 프라이버시보호를 가능케 한다. 특히, 본고에서는 초경량 키의 길이, 저전력 소모성, 고속구현 속도를 갖는 타원곡선암호의 안전성에 대한 가이드라인을 제공하겠다.

키워드: RFID, 타원곡선암호계(ECC, Elliptic Curve Cryptosystem), PKC

1. 소개

RFID(Radio Frequency IDentification)[12, 1, 10]는 바코드나 자기인식 장치의 결함을 보완하고 사용의 편리성, 물류나 재고관리, 도난방지 등에 적용할 수 있어 기술의 진보에 따라 활용범위가 비약적으로 증가되고 있는 차세대 핵심 기술이다.

그러나 RFID 기술은 원거리에서 작동이 가능하고 태그의 정보는 사용자가 알지 못하는 사이에 모든 리더에게 자동 응답되어 전송된다. 이로 인한 공격자의 ID 도청, 트래픽 분석, 재전송 공격, 스니핑(Sniffing), 서비스 거부공격(DoS), 부 채널 공격(Side Channel Attack) 등 다양한 공격[13]들이 존재하고 있어 이에 대응하는 RFID에 대한 보안대책이 우선적으로 해결이 되어야 한다.

위의 여러 가지 RFID 보안 위협에 대응하는 방법은 데이터 암호화[7], 인증프로토콜 기법[14], 접근제어[8] 등이 있고 현재 이를 위하여 각 나라마다 RFID 보안영역 표준화와 실제 구현이 가능하도록 하는 연구개발에 박차를 가하고 있다.

RFID 시스템에서 사용자의 프라이버시 보호[9, 11] 및 데이터 보안을 위한 여러 가지 기법들이 제안되었다. 그러한 기법들은 태그 무효화(kill), Faraday Cage, Blocker 태그 등 물리적 접근기법과 비트연산(XOR) 기반, 해쉬(Hash)함수 기반, 재암호화 등 암호학적 접근기법으로 분류된다.

실제, RFID 보안대응책의 대표적인 예로, 해쉬 체인방법[13], 비공개키(또는 대칭키)암호알고리즘의 초경량화 AES[15]등이 있고 공개키 암호알고리즘에 사용되는 유한체 $GF(2^m)$ 위에서 정의된 타원곡선암호(Elliptic Curve Cryptography, ECC)[3], NTRU 암호[6], Rabin 암호[16] 등은 초경량 하드웨어 구현에 적합한 차세대 암호시스템으로서 안전한 RFID 인증서비스 제공과 프라이버시보호를 가능케 한다.

이 논문에서는 RFID에 대한 여러 가지 보안위협에 대하여 알아보고 그에 대응하는 안전한 암호학적 도구(Primitive)를 이용하는 방법에 대하여 알아보겠다. 또한, 초경량 키의 길이와 고속구현 속

도를 갖도록 하는 타원곡선암호(ECC)의 안전성에 대한 가이드라인을 제공하겠다.

본 논문은 다음과 같이 구성이 된다. 2장에서는 RFID의 보안 위협 요소에 대하여 알아보고 3장에서는 기존 RFID 보안 기술의 대표적인 예로 대칭키 암호기반 RFID 보안에 대하여 간단히 설명하겠다. 4장에서는 공캐키 암호기반의 ECC의 안전성에 관련한 가이드라인을 제시하고 마지막으로 5장에서는 결론을 간단히 언급하겠다.

2. RFID의 보안 위협

본장은 RFID 시스템의 구성요소에서 침해를 유발하는 공격 기법 및 보안 취약점에 대해 살펴보겠다. 일반적으로 많이 알려진 RFID에 대한 일반적인 공격기법[13]을 살펴보면 다음과 같다.

도청 공격 RFID의 태그와 리더사이에 공격자가 중간에 데이터를 도청하는 것을 말한다. 도청공격의 형태로는 공격자가 리더를 갖고 태그를 스캐닝(scanning)하는 적극적 공격과 리더와 태그 간 통신을 무선으로 수신하는 수동적 공격이 있다.

트래픽 분석 리더와 태그 간 통신 중 트래픽 분석을 통한 위협이 존재한다. 공격자가 어떤 특정 지역 내지 특정 태그에서 리더와 태그간의 트래픽 분석에 의한 통계 기반의 식별정보를 추적할 수 있다면 공격자는 그 지역에서 어느 정도의 트래픽이 존재하는지, 어느 정도의 물품이 존재하고 빠져나가는지에 대해서 알 수 있다.

재전송 공격(Replay Attack) RFID 시스템은 공격자가 도청으로 획득한 정보를 이용하여 정당한 태그로 가장하여 공격할 수 있다.

스니핑(Spoofing) 공격자가 정당한 리더로 가장하여 태그에 질의함으로써 태그로부터 인증정보를 획득할 수 있거나 공격자가 상품의 태그를 이용하여 유인 태그를 만든 후 실제 제품과 바꾸는 공격이다.

태그 복제 공격자는 도청한 데이터의 해독, 부채널 공격(Side channel Attack) 등을 통해 태그의 정보를 복제할 수 있다.

서비스 거부(DoS, Denial of Service) 공격 서비스 거부(DoS) 공격이란 공격자가 여러 대의 장비 또는 시스템을 이용해 표적 시스템이 처리하지 못할 정도의 엄청난 데이터를 집중적으로 전송함으로써 표적 시스템의 정상적인 기능을 방해하는 것을 말한다. 공격자는 태그의 수를 급격히 늘리거나 전파방해 등을 통해 서비스 거부 공격을 시도할 수 있다.

부 채널 공격 방법(Side Channel Attack)[2] 암호화에 사용된 키를 찾기 위해서 암호 알고리즘의 이론적인 취약점이 아닌 암호화 과정에서 누설되는 타이밍 정보, 전력소모, 전자파 신호등을 이용하는 물리적인 공격방법이다.

3. 기존 RFID 보안기술

RFID 시스템에서 사용자의 프라이버시 보호 및 데이터 보안을 위한 여러 가지 기법들이 제안되었다. 이런 기법들은 크게 태그 무효화(Kill), Faraday Cage, Blocker 태그 등 물리적 접근기법과 비트연산(XOR) 기반, 해쉬함수 기반, 재암호화 등 암호학적 접근기법으로 분류된다.

프라이버시 보호 뿐 아니라 인증 및 데이터 보호까지 고려하기 위해서는 암호학적 접근 기법을 이용하여야 한다. XOR 기반의 기법은 단순한 로직 연산으로 RFID와 같이 하드웨어 제약이 많은 시스템에 적절한 것으로 고려되고 있다. 실제로 ISO/IEC 18000-6 타입C 표준에서도 데이터를 비밀키 값과 XOR하여 전송하는 방식으로 데이터를 암호화 할 수 있도록 하고 있다. 하지만 이러한 단순 XOR 방식은 태그와 리더 사이에서 수동 공격(Passive attack)으로도 비밀 정보를 알아낼 수 있다.[2]

대칭키 기반의 암호 알고리즘은 하드웨어 구현의 복잡성으로 인해 RFID와 같은 환경에 적합하지 않은 것으로 간주되었으나 Feldhofer, Dominikus, Wolkerstorfer[15] 등에 의하여 AES의 저면적 구현이 RFID 시스템의 인증 및 암호 프로토콜로 사용가능함으로 보임으로써 점차 RFID 시스템으로의 활용에 대한 연구가 활발히 진행되고 있다. 하지만 이러한 보안 프로토콜을 이용하여 구현하더라도 부 채널 공격과 같이 태그에 대한 물리적 공격으로 인한 암호화 키 추출이 가능하다.

4. 공개키 암호기반 RFID 보안기술

최근 RFID 보안 기술에 ECC, NTRU 암호, Rabin 암호와 같은 공개키 암호알고리즘을 사용하는 논문들이 발표되고 복잡성과 초경량문제를 극복하고자 많은 연구가 활발히 진행되고 있다. 그 중 타원곡선암호는 암호화와 서명생성 및 검증 측면에서 **[표 1]**에서와 같이 저전력 소모, 안전성과 효율성이 검증이 되었다.

Encryption/Decryption		Rabin	NtruEncrypt	NtruEncrypt parallel	ECMV
- Message Payload		< 512 bits	< 265 bits	< 265 bits	< 200 bits
- Ciphertext (Packets of 30 bytes)		512 bits (3)	1,169 bits (5)	1,169 bits (5)	400 bits (2)
Encryption	Time per Message	2.88 ms	58.45 ms	0.87 ms	817.7 ms
	Avg. Power	148.18 μW	19.13 μW	118.7 μW	394.4 μW
	Energy per Message	426.76 nJ	1,118.15 nJ	102.79 nJ	322.5 μJ
Decryption	Time per Message	1.089 s	116.9 ms	1.732 ms	411.54 ms
	Avg. Power	191.5 μW	58.73 μW	158.3 μW	394.4 μW
	Energy per Message	208.64 μJ	6,865.54 nJ	274.18 nJ	162.31 μJ
Sign / Verify		Rabin	NtruSign	NtruSign parallel	ECDSA
- Signature Length (Packets of 30 bytes)		512 bits (3)	1,169 bits (5)	1,169 bits (5)	200 bits (1)
Sign	Time per Message	1.089 s	233.8 ms	3.464 ms	410.45 ms
	Avg. Power	191.5 μW	58.73 μW	158.3 μW	394.4 μW
	Energy per Message	208.64 μJ	13.73 μJ	548.35 nJ	161.88 μJ
Verify	Time per Message	2.88 ms	58.45 ms	0.87 ms	822.5 ms
	Avg. Power	148.18 μW	19.13 μW	118.7 μW	394.4 μW
	Energy per Message	426.76 nJ	1,118.15 nJ	102.79 nJ	324.39 μJ

표 1. PKC 기반 RFID 암호와 서명구현 결과[14]

RFID/USN의 초경량 암호방식에 사용될 수 있는 타원곡선(Elliptic Curve)은 160 비트의 작은 비트 수의 연산으로 1024 비트를 사용하는 RSA암호방식[7]과 같은 안전성을 보장하고 부 채널 공격에 강하며 다양한 유한체(Finite Field)에서 정의되어 여러 시스템 환경에 적용될 수 있다.

RFID 보안에서 관심을 보이고 있는 이진유한확장체(Binary Finite Extension Field)[3]는 $GF(2^m)$(단, m은 양의 정수)의 형태로서 효율적인 계산단위(Arithmetic Unit)를 구성하여 빠른 연산할 수 있고 그로 인하여 고성능의 태그인식을 할 수 있도록 구현 및 설계를 가능케 한다.

이진확장유한체는 $GF(2^m) := GF(2)[z]/ < f(z) >$와 같이 정의되고 $f(z)$는 $\{0, 1\}$을 갖는 $GF(2)$ 위에서 정의된 m(단, m은 양의 정수)차 기약다항식(Irreducible Polynomial)이다. 유한체 $GF(2^m)$는 $m-1$차수 이하의 다항식들의 집합으로서 2^m개의 원소를 갖는다. 이 유한체에서는 RFID에서 사칙연산, XOR, Modular 연산 등과 같은 비트연산 수행 시 고속 구현을 가능케 한다. 다음으로 유한체 $GF(2^m)$ 위에서 정의된 타원곡선 $E := E(GF(2^m))$의 정의는 다음과 같다.

$$E(GF(2^m)) := \{(x,y) | y^2 + xy = x^3 + ax^2 + b\} \bigcup O$$

(단, $x, y, a, b \in GF(2^m), O$는 무한원점)

타원곡선 E는 가환군으로서 위수 $\#(E) = n$을 갖으며 Hasse의 정리[3]에 의하여 타원곡선의 위수는 $n = 2^m + 1 - t$(단, $-2\sqrt{2^m} \le t \le 2\sqrt{2^m}$)을 만족한다. 타원곡선암호는 기본적으로 타원곡선이산대수 문제(ECDLP, Elliptic Curve Discrete Logarithm Problem)와 타원곡선디피헬만문제(ECDHP, Elliptic Curve Diffie-Hellman Problem)의 어려움을 가정으로 하여 다양한 암호알고리즘 및 프로토콜을 구현한다. 타원곡선이산대수문제와 타원곡선디피헬만문제의 정의는 다음과 같다.

정의 1. 타원곡선이산대수문제(ECDLP): E의 원소 P와 αP이 주어졌을 때 α를 찾는 문제

정의 2. 타원곡선디피헬만문제(ECDHP): E의 원소 P와 αP, βP가 주어졌을 때 $\alpha\beta P$를 찾는 문제

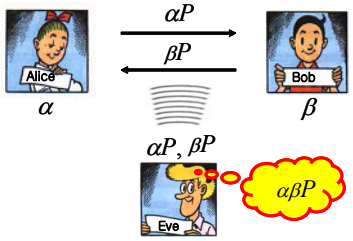

그림 1. ECDHP를 이용한 키 공유와 도청공격

ECDLP와 ECDHP은 통신하는 데이터를 제 3자가 도청하여도 알지 못하는 기능을 제공한다. [**그림 1**](Alice를 리더로 Bob을 태그로 가정해도 좋다.)

그러나 이들 문제들은 수학적으로 안전하다고(어렵다고) 증명이 되었지만 최근에 ECDLP와 ECDHP에 대한 많은 공격방법들이 발표되고 있다. 기본 공격조건들은 도청만 가능하면 적용될 수 있는 공격으로서 4가지로 BSGS 방법[7], Pollig-Hellman 공격[7], Diem 공격[5], Cheon의 알고리즘[4]이 있다. 이들 중 Cheon의 알고리즘은 타원곡선의 위수가 취약할 때 매우 막강한 공격으로서 상대적으로 적은 데이터의 도청으로 비밀키를 알아 낼 수 있다. 다음 [**표 2**]는 각 공

격에 대하여 안전한 변수의 조건을 보여준다.

공격방법	안전한 변수 조건
BSGS	그룹의 위수 r이 160비트 이상이 되어야 함
Pollig-Hellman	$r-1$의 인수가 작은 인수와 매우 큰 소수 인수의 곱의 형태를 가져야 함
Diem	m은 160 이상의 소수가 되어야 함
Cheon	$r-1$과 $r+1$의 작은 인수가 $(\log r)^2$ 보다 크지 않아야 함
NIST 권고사항	$m=163$ 또는 $m=191$
	$f(z)=z^{163}+z^7+z^6+z^3+1$

표 2. RFID에서 ECC의 안전한 변수 조건

다음의 타원곡선의 예는 Pollig-Hellman 공격과 Cheon의 알고리즘에 취약함을 보여준다. 즉, $p-1$의 인수들이 작은 소수의 곱으로 표현이 됨을 알 수 있다.

$m=163,\ f(z)=z^{163}+z^7+z^6+z^3+1$

$E: y^2+xy=x^3+x^2+9354108838529314164470685187060716566985388984531$

(단, 계수는 $GF(2^{163})$의 원소를 의미한다. 예를 들어 $10=z^3+z^2$으로 표현가능)

$n=2\cdot 5846006549323611672814739077079481794380048524409=2\cdot p$ (p는 162비트)

$p-1=2^3\cdot 3\cdot 709\cdot 467237\cdot 71926663\cdot 16115487924011\cdot 6343533284169558523$

다음으로 타원곡선을 이용한 RFID 태그 아키텍처를 간단히 소개하겠다. 이 구조는 ECU(Elliptic Curve Unit)가 핵심이며 주된 연산(다항식 모듈러 사칙연산, 제곱, 타원곡선 상수 곱 kP 등)을 처리한다. ECU기반 아키텍처는 기존의 구현된 보안기능의 RFID 아키텍처 보다 다소 복잡하지만 여러 가지 구현 방법[14]으로 현실성 있는 칩 구성이 개발 중이며 표준화에 진행 중이다.

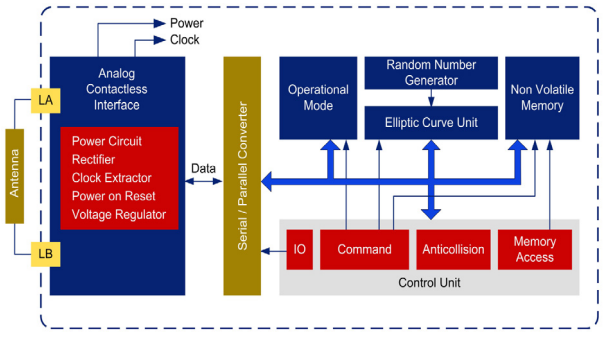

그림 2. ECC 기반 RFID 태그 아키텍처

5. 결론

타원곡선은 상대적으로 작은 키를 사용하여 안전한 인증 프로토콜을 구현할 수 있고 빠른 구현 속도와 저전력 소모성를 자랑한다. 그러나 RFID 관련 보안위협과 여러 가지 타원곡선에 대한 공격이 존재한다. 본고에서는 그에 대한 대응책으로 공개키 암호시스템의 하나인 타원곡선을 이용하는 RFID 보안기술에 대한 안전한 변수를 선택할 수 있는 가이드라인을 제공하였다. 이 결과는 차세대 RFID 보안기술에 영향을 줄 것으로 사료된다.

[참고자료]

[1] Universit´e catholique de Louvain Louvain-la-Neuve, “Bibliography on Security and Privacy in RFID Systems”, Information Security Group, 2009.

[2] 최두호,“RFID/USN 하드웨어 보안 대책”, 정보보호21c, 2009.4.

[3] I. Blake, G. Seroussi, N. Smart,“Elliptic Curves in Cryptography”London Mathematical Society, LNS 265, Cambridge University Pree, 1999.

[4] J. H. Cheon,“Security Analysis of the Strong Diffie-Hellman Problem”, Eurocrypt 2006, LNCS 4004 Springer-Verlag, pp. 1-11, 2006.

[5] C. Diem,“The GHS attack in odd characteristic”, Journal of the Ramanujan Mathematical Society 18, pp. 1-32, 2003, http://www.math.uni-leipzig.de/~diem

[6] J. Hoffstein, J. Pipher, and J. H. Silverman. “NTRU: a ring based public key cryptosystem”. In Proceedings of the 3rd Algorithmic Number Theory Symposium (ANTS 1998), 1998.

[7] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone,“Handbook of Applied Cryptography”,CRCPress, 1996.

[8] R.L. Rivest,“Approaches to RFID Privacy”, RSA Japan Conference 2003.

[9] K. Romer, T. Schoch, F. Mattern, and T. Dubendorfer, “Smart Identification Frameworks for Ubiquitous Computing Applications”, PerCom03, pp.253-262, 2003. 3.

[10] S. Sarma, S. Weis, and D. Engels,“RFID: Security Risks and Challenges”, CryptoBytes, 2003.

[11] Sarah Spiekermann and Sergei Evdokimov. “Privacy Enhancing Technologies for RFID”A Critical Investigation of State of the Art Research IEEE Privacy and Security 2009, 2009.

[12] S. Weis, “Security and Privacy in Radio Frequency Identification Devices”, Master’s thesis, MIT. 2003.

[13] 김광조, “RFID/USN 정보보호 기술”, TTA 저널, 95호

[14] G. Gaubatz, “State of the Art in Ultra-LowPower Public Key Cryptography for Wireless Sensor Networks”. In 2nd IEEE International Workshop on Pervasive Computing and Communication Security, 2005.

[15] M. Feldhofer, S. Dominikus, J. Wolkerstorfer, "Strong Authentication for RFID Systems using the AES Algorithm", CHES, 2004.

[16] M. O. Rabin. “Digitalized signatures and public key functions as intractable as factorization”. MIT/LCS/TR-212, Massachusetts Institute of Technology, 1979.