유한체를 사용한 RFID 상호인증 프로토콜 연구

안효범* · 이수연**

요 약

유비쿼터스 환경에서 개인 프라이버시를 보호하기위한 RFID 시스템 보안에 대한 많은 연구가 이루어지고 있다. RFID 시스템 보안 중 상호인증 방법으로 XOR 기반, 해쉬기반, 그리고 재암호화 기반의 프로토콜을 사용한다. 그러나 인증과 프라이버시를 보호하기위한 프로토콜은 좀 더 강화된 암호 시스템을 사용해야 한다. 공개키는 강력한 보안성을 제공하나, 비용이 많이 요구되어 RFID 시스템에서 사용하기에는 적합하지 않다. 따라서 본 논문에서는 상호 인증과 안전성을 위하여 유한체 $GF(2^n)$을 이용한 인증 프로토콜을 제안하고 RFID 시스템에서의 여러 공격에 대하여 안전성 분석을 하였다.

Study on RFID Mutual Authentication Protocol Using Finite Field

Hyo Beom Ahn* · Su Youn Lee**

ABSTRACT

There are many investigations about the security on RFID system to protect privacy. It is important to mutual authentication of the security on RFID system. The protocol for mutual authentication use light-weight operation such as XOR operation, hash function and re-encryption. However, the protocol for authentication and privacy is required more complicated cryptography system. In this paper, we propose a mutual authentication protocol using finite field $GF(2^n)$ for a authentication and are a safety analysis about various attacks.

Key words : RFID, Mutual Authentication Protocol, Finite Field

* 공주대학교 정보통신학부 교수
** 백석문화대학 컴퓨터정보학부 교수

1. 서 론

RFID 기술을 여러 응용 분야에 적용하기 위해서는 태그에 저장된 정보를 보호하고 임의의 태그에 대한 추적 방지 등과 같은 보안 문제를 해결할 수 있어야 한다. 그러나 기존의 무선 환경에서 제공하는 보안 프로토콜은 RFID 태그가 낮은 가격으로 공급되어져야하기 때문에 적합하지 않다. 이에 자원의 소모가 적으면서도 안전한 암호 알고리즘의 개발과 아울러 최소의 자원을 사용하면서도 안전한 프로토콜의 개발이 필수적이다[1].

그러나 경량 연산자를 사용한 인증 프로토콜은 단순하나 보안성부분에서는 많은 취약점을 갖고 있다. 또한, 보안성을 강화하기 위해서 공개키 또는 ECC를 사용하는 것은 비용이 많이 든다. 본 논문에서는 경량연산자의 취약점을 보완하고 공개키와 같이 비용이 많이 드는 연산을 줄이면서 보안성이 강화 된 유한체 $GF(2^n)$를 사용한 상호인증 프로토콜을 제안한다.

2. 기존연구

RFID 시스템에서는 리더를 소유한 공격자는 물리적인 접촉 없이 태그의 정보를 읽는 것이 가능하므로 사용자가 알지 못하는 사이에 태그의 정보가 유출되거나 태그의 식별 정보를 이용한 사용자 위치 추적 등이 가능하게 된다. 이러한 문제를 해결하기 위해 사용자의 프라이버시를 보호할 수 있는 RFID 인증 프로토콜이 제안되었다. 본 절에서는 지금까지 제안된 사용자 프라이버시를 해결하기 위한 인증 프로토콜을 살펴보고자 한다.

2.1 해쉬기반 인증 프로토콜

해쉬기반 인증 프로토콜은 Weis 등이 제안한 기법[3]이며 태그를 잠그고 풀기 위하여 리더가 임의의 키를 해쉬하여 데이터베이스에 저장하고 이를 태그의 메타 ID로 사용한다. 그러나 이 기법에서는 태그가 고정된 값 메타 ID를 리더에게 전송하기 때문에 위치 추적이 가능하다.

이외에서도 Dirk Henrici와 Paul Muller는 [4]에서 해쉬에 기반을 두어 ID를 갱신하므로 위치트래킹 공격을 방지하는 프로토콜을 제안하였다. 그러나 이 프로토콜은 인증이 완료될 경우 ID가 갱신되므로 위치트래킹 공격에 안전하게 보이나 태그와 데이터베이스 사이에 정상적이지 않은 인증의 경우 태그는 항상 동일한 h(ID)를 응답하므로 공격자는 태그의 위치를 트래킹 할 수 있다는 문제점을 갖는다.

또한, Ohkubo 등은 위치트래킹 공격에 안전하며 전방위 안정성도 보장되는 해쉬 체인 프로토콜[5]을 제안하였다. 두 개의 해쉬 함수를 이용하여 태그의 정보를 보호하는 방법으로 EPC(Electronic Product Code)에 적용하기 쉬운 기법이다.

2.2 재 암호화기반

RFID 시스템에서 리더의 질의에 태그가 매번 다른 값을 전송하여 사용자의 위치 정보가 노출되는 것을 막을 수 있다. 재 암호화 기법이란 태그의 정보를 재 암호화하여 리더의 질의에 대해서 항상 다른 값으로 응답하는 기법이다. 재 암호화 기법은 많은 연산량을 필요로 하기 때문에 제한된 자원을 가진 태그가 수행하기 어렵다. 따라서 태그를 대신하여 데이터베이스나 리더 등을 사용하여 재 암호화 과정이 이루어진다. Satio 등에 의해서 제안 기법[6]인 Universal 재 암호 기법은 재 암호화 과정이 일어날 때 공개키 없이 임의의 랜덤값을 사용하여 재 암호화가 이루어지는 기법이다. 그러나 태그의 정보에 재 암호화 과정이 여러 번 일어나더라고 단 한 번의 복호화 과정으로 원래의 메시지를 복원할 수 있다. Juels 등에 의해서 제안 기법[7]인 Privacy Protection in RFID-enabled

Banknotes는 Euro 화폐에 태그를 적용하여 불법 거래 시 화폐의 흐름을 추적하기 위해 제안되었다. 그러나 악의적인 상인이 화폐에 재 암호화 과정을 수행하지 않거나 시스템의 오류로 재 암호화 과정이 수행되기 전에 리더와 태그 사이의 통신이 끊길 경우 태그는 일정한 기간 동안 고정된 값을 리더에게 전송하게 되고 사용자의 위치 추적이 가능하다는 문제점이 있다.

2.3 XOR기반

해쉬 기반과 재 암호화 기반의 기법들은 최소한의 연산만을 수행하는 태그가 사용되는 환경에 적용하기에는 적합하지 않다. XOR 기반의 기법은 해쉬 기반의 기법보다 더 단순한 비트 연산을 사용하여 RFID의 프라이버시를 보호하는 기법으로 최저가의 RFID 태그에 적용 가능한 기법이다.

Juels는 사용자의 프라이버시를 보호하며 최소한의 암호학적 함수를 사용하는 기법을 제안 하였다[8]. 제안된 기법은 간단한 비트 연산인 XOR 연산을 사용한다. 리더로부터 임의의 값들을 받아서 그것을 이용하여 다음 세션에 사용될 값들을 갱신하므로 공격자가 태그를 추적하지 못하도록 한다. 또한, Juels에 의해 2005년에 제안된 HB 프로토콜[9]은 1비트로 상대방을 인증하는 기법이다.

이 기법은 수동적인 공격자에 대해서 안전할 수 있으나 공격자가 a값을 자신에게 유리하게 선택하여 리더에게 전송한다면 응답 값 z에서 x에 대한 값을 알아낼 수 있다. 따라서 Juels는 능동적인 공격에 안전한 HB^{+}기법을 제안하였다[10].

하지만 제안된 기법은 1비트의 값으로 태그를 인증하는 것이기 때문에 그를 관리하는 환경에서는 오류 발생의 확률이 많다. 그러므로 다수의 태그 정보를 다루는 환경에서 사용하기에는 부적합하며 이 기법은 안전성 측면에서 취약성을 갖는다[10].

또한, Lopez에 의해서 LMAP와 M2AP이 제안되었는데, 이 방법은 비트연산인 XOR와 AND 그리고 덧셈($\mathrm{mod} 2^n$)을 사용한다[11, 12]. 이 제안된 방법은 상호인증을 제공하고 위치추적공격을 막을 수 있고, 여러 가지의 복잡한 계산방식에 의해 nonce를 키의 갱신에서 사용하도록 함으로써 키의 복잡도를 높였다. 그러나 복잡한 계산방식을 사용함에도 불구하고 Li와 Wang는 [13]에서 이 두 프로토콜이 비동기화 공격(de-synchronization attack)과 완전노출공격(full Disclosure attack)에 취약점이 있다는 것을 분석하였고, 이에 대한 대안으로 재동기화(re-synchronization)를 제시하였다. 그러나 하나의 태그에 대한 많은 상태 정보를 저장해야하는 문제를 갖게 된다. 그러한 이유로 유비쿼터스 환경에서는 이러한 상태저장 프로토콜(stateful protocol)이 적당치 않음을 보여준다.

2.4 공개키 기반

이제까지 RFID 상호인증은 태그의 제약조건으로 인하여 경량화 된 연산자를 사용한 방법이 제안되었다. 그러나 최근에 태그의 설계기술의 발전으로 인해 공개키 기반의 RFID 인증 알고리즘을 제안하고 있다. [17]에서는 ECC 기반 태그 식별(identification) 프로토콜을 제안하였다.

3. 제안된 인증프로토콜

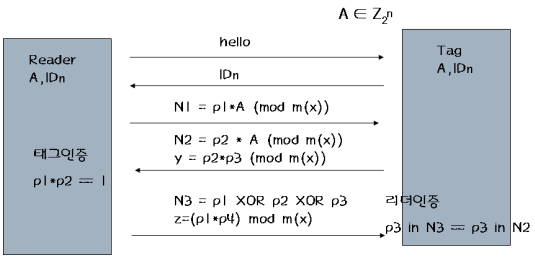
제안된 방법을 사용하기 위해서는 유한체 $GF(2^n)$를 구하는 곱셈회로와 이를 대체할 수 있는 곱셈 검색테이블이 요구된다. 이 두 구현 방법은 서로 trade-off관계에 있다. 즉, 회로로 구성을 하면 유한체를 계산하기 위하여 많은 회로가 요구되는 반면 저장장치를 많이 요구하지 않는다. 그러나 테이블로 구성을 하게 되면 테이블을 저장하기 위한 많은 저장공간이 요구된다.

유한체의 고속계산은 [15]에서 최소회로를 제시하고 있어 이를 이용한다면 RFID 태그에서 구현

할 수 있다. 본 논문에서 제안한 인증 프로토콜은 RFID에서 유한체의 차수을 일반화한 n차수를 사용한다.

3.1 제안된 프로토콜과 상호인증

본 논문에서 제안된 상호인증 프로토콜은 (그림 1)과 같다. 태그와 리더는 비밀정보로 A와 $m(x)$를 비트로 저장하고 있다. A는 2^n비트 크기를 갖는 비트 스트림이고, 이진 다항식 $m(x)$는 나누어질 수 없는 특성을 갖는 다항식이다. 예를 들면, 프로토콜에서 사용되는 정보의 크기가 2^8이라면, 이에 대응하는 이진 다항식 $m(x)$는 $x^8+x^4+x^3+x+1$을 사용한다.



(그림 1) 제안된 상호인증 프로토콜

제안된 프로토콜은 태그와 리더의 상호인증을 위해 다음과 같은 단계를 수행한다.

단계 1 : 리더는 태그에게 hello 메시지를 보낸다.

단계 2 : 태그는 자신의 ID_n을 보낸다.

단계 3 : 리더는 ID_n을 받고 비밀정보 A를 얻을 수 있고, 임의의 랜덤 값($<2^n$)인 N1을 생성하여 태그에게 보낸다.

$$N1 = p1*A \bmod m(x) \quad (1)$$

단계 4 : 태그는 리더로부터 받은 N1의 연산결과를 갖는 A에 대응되는 값, 즉 p1을 테이블로부터 찾고 곱셈에 대한 역(inverse)인 p2($1=p1*p2$)를 테이블에서 찾은 후, N2와 y를 리더에게 보낸다.

$$N2 = (p2*A) \bmod m(x) \quad (2)$$

$$y = (p2*p3) \bmod m(x) \quad (3)$$

단계 5 : 리더는 N1 으로부터 p1을 유도할 수 있고, N2로부터 p2를 유도할 수 있으므로 만약 $(p1*p2) \bmod m(x) = 1$이면 태그를 정당한 태그라고 인정할 수 있다. 인증 작업이 끝난 후, 리더는 x로부터 p3를 유도하여 N3와 z를 보낸다.

$$N3 = p1 \oplus p2 \oplus p3 \quad (4)$$

$$z = (p1*p4) \bmod m(x) \quad (5)$$

단계 6 : 태그는 N3로부터 자신이 보낸 p3를 확인할 수 있고, 이를 통해 리더를 인증할 수 있다. 또한 z를 통해 p4를 유도해 내는데 p3와 p4는 통신에서 사용될 세션키와 ID 추적을 피할 수 있는 ID갱신을 하는데 사용된다.

3.2 ID 갱신과 세션키 생성

위와 같은 프로토콜로 상호인증을 한 후 얻어지는 p3와 p4를 이용하여 다음과 같이 ID(ID_{n+1})와 세션키(k_s^{n+1})를 갱신할 수 있다.

$$ID_{n+1} = ID_n \oplus (p2 \cdot p4) \quad (6)$$

$$K_s^{n+1} = k_s^n \oplus (p1 \cdot p3) \quad (7)$$

ID의 갱신은 제 3자에 의해서 ID를 추적하는 것을 막기 위해 갱신된다. 즉, 제 3자가 ID를 갖고 있다하더라도 다음번에 사용되는 ID가 다르기 때문에 태그의 사용을 추적할 수 없다. 제 3자는 ID를 추적하기 위해서는 $(p2 \cdot p4)$를 알아내야 하는데 프로토콜 과정 중에 노출이 된 적이 없는 값이기 때문에 이 값들을 유도하기가 힘들다. 그러나, 최근 들어 비동기화공격에 의해서 태그와 DB에 저장된 정보가 서로 같지 않은 현상이 나타날 수

있다. 이를 해결하기 위해서 이전에 사용된 ID들을 저장하여 유지하는 방법을 [13]에서 제시하였다. 만약 비동기화 공격에 의해서 태그와 DB가 저장된 내용이 다르다면, 제안된 프로토콜은 고정된 비밀정보 A와 바로 전 세션에 사용된 p2와 p4를 알고 있다면 이전 ID를 복구할 수 있다.

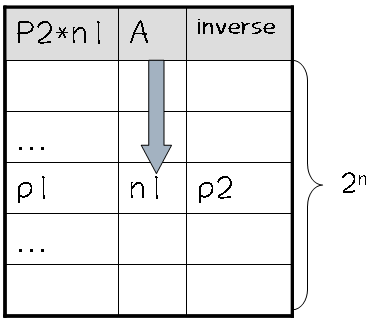
$$ID_n = ID_{n+1} \oplus (p2 \bullet p4) \quad (8)$$

복구된 ID와 비밀정보 A를 사용하여 서로 저장하고 있는 정보에 대한 동기화 작업을 진행할 수 있다.

세션키의 갱신은 RFID에서 단순 인증만을 요구하는 어플리케이션이 아니라, 중요한 비밀정보가 요구된다면 이를 안전하게 리더에게 전달해줄 세션키가 요구된다. 이때 사용되는 비밀 키로서 매 세션마다 변경되기 때문에 공격자는 이를 추적해서 알아내기가 힘들다.

3.3 제안된 인증프로토콜의 구현

제안된 인증 프로토콜은 GF(2^n)를 이용한 프로토콜로 n의 차수가 적을 때와 많은 때 구현하는 방법이 달라질 수 있다. 즉 차수가 적을 경우에는 검색테이블(look-up table)을 이용하는 것이 효율적이고, 차수가 클 경우에는 계산을 수행하는 것이 더 효율적이 된다. 계산을 수행하기 위해서는 유한체의 곱셈이 요구되는데 [15]에서처럼 구현될 수 있다. 이때, p1을 얻기 위해서는 $N1 * A^{-1} \bmod m(x)$를 하면 된다. 또한 p2를 구하는 방법은 $p1 * p2 = 1$이라는 것을 이용하여 p1의 역을 구하면 된다.



(그림 2) 비밀정보 A에 대한 곱셈의 역과 p1을 저장한 테이블

제안된 인증 프로토콜에서 구현은 이 두 가지 방법을 사용하여 구현할 수 있다. 고정된 비밀정보 A를 사용하는 식 (1)과 식 (2)부분에서는 계산보다는 (그림 2)와 같은 구조의 검색테이블을 사용하여 구현하는 것이 더 효율적인데 그것은 A는 고정된 비밀정보로 미리 계산된 테이블을 만들 수 있다. 식 (3)과 식 (5)는 값이 임의로 변하는 값에 대하여 곱셈을 수행함으로 테이블 보다는 회로를 구성하는 것이 효율적이다.

4. 안정성 분석

GF(2^n)은 곱셈과 덧셈에서 동일한 연산결과의 수가 2^n개이기 때문에 연산결과를 이용해서 곱셈과 덧셈의 대상이 되는 두 피연산자를 추측하는 것이 어렵다. 즉, GF(2^8)일 경우에 $(p1 \cdot p3)$와 $(p2 \cdot p4)$는 각각 2^8개가 같은 결과가 존재한다.

그러므로 식 (1)에서 비밀정보 A를 알지 못하는 한 p1을 알기위해서는 2^n번의 시도가 있어야 된다. 또한, 식 (2)에서도 A를 알지 못하면 공격자는 식 (1)에서와 동일한 시도를 해야 한다.

또한, 공격자가 p1 * p2 = 1이라는 성질을 이용하여 n1 * n2를 하더라도 A * A(mod m(x))가 되어 A를 추측하는 것 또한 2^n개가 A의 대상이 된다. 그러므로 비밀정보 A를 N1과 N2에서 유도해 내는 것은 어렵게 된다. 또한, x와 y에서 각각의 정보를 유도한다는 것은 어렵다.

제안된 프로토콜은 트래픽공격시 세션키를 사용하여 전달되는 데이터를 암호화 할 수 있기 때문에 도청을 통한 공격으로부터 보호할 수 있다. 또한 위치트래킹 공격을 방지하기 위해 매 세션마

다 사용되는 ID를 변경하도록 설계되어 있다.

재전송공격은 정당한 태그로 인증을 받기위한 공격으로 제안된 프로토콜에서는 비밀정보 A를 알 수 없고, 또한 매번 통신할 때 마다 인증과정에서 사용되는 값이 리더와 태크로부터 변경되기 때문에 재전송공격을 상호인증을 통해 방지할 수 있다. 스프핑 공격 또한 상호인증을 수행하기 때문에 방지할 수 있다.

최근의 태그와 DB에 대한 공격으로서 비동기 공격이 있다. 이 때 비동기 공격은 상호인증 후에 이루어지기 때문에 서로 상호인증과정을 수행하지 않는다면 변경된 정보를 저장하지 않는다. 비동기 공격을 허용했다하더라도 앞 절에서 설명한 것처럼, 한번에 한하여 비-동기된 정보를 동기화시키기 위한 이전 ID복구가 가능하기 때문에 동기화 프로토콜을 이용하여(동기화 프로토콜은 이 논문에서는 제시하지 않음) 서로의 비동기 정보를 동기화 시킬 수 있다.

5. 결 론

RFID 인증 프로토콜로서 제시된 기존의 방법은 경량화에 초점을 맞추어 제안되었다. 그러나 최근들어 경량 연산자(Lighted-weight operation)에 대한 연구와 더블어 보안성이 강조된 공개키 암호체계와 ECC를 사용한 상호인증 프로토콜이 제시되고 있으나 아직까지는 현실성이 결여되어 있다. 본 논문에서 제안된 유한체를 이용하는 방법은 보안성은 강조되면서 공개키나 ECC를 사용하는 것보다 경량화된 방법으로써 제안되었다. 제안된 프로토콜은 현재까지 제안된 프로토콜보다는 많은 연산을 수행하지만 보안성을 강화하면서 상호인증을 하는 프로토콜이다. 그러나 제안된 유한체를 이용하는 경우 구현 복잡도는 유한체의 구현논문[15]을 볼 때 적은 회로로 구현이 가능하다.

추후 연구과제로는 유한체 $GF(2^n)$를 사용하였을 경우의 수학적 분석이 요구되며, 또한 비동기공격에 대한 프로토콜의 구현이 요구된다.

참 고 문 헌

[1] S. E. Sarma, “Towards the fivecent tag”, MIT Auto ID Center, Technical Report MIT-AUTOID-WH-006.2001(http://autoidcenter.org).

[2] 정병호, “RFID/USN 환경에서의 정보보호”, 제9회 정보보호심포지움, pp. 447-463, 2004.

[3] S. A. Weis, S. E. Sarma and D. W. Engels, “Security and privacy Aspects of Low Cost Radio Frequency Identification System”, First International Conference on Security in Pervasive Computing, 2003(http://theory.lcs.mit.edu/sweis/spc-rfid.pdf).

[4] D. Herinici and P. Muller, “Hash based enhancement of location privacy for radio frequency identification devices using varying identifiers”, Per-Sec, pp. 149-153, March 2004.

[5] M. Ohkubo, K. Suxuki, and S. Kinoshita, “Efficient Hash-Chain Based RFID Privacy Protection Scheme”, Ubcomp 2004 workshop.

[6] S. Junichiro, R. Jae-Chelo, and S. Kouichi, “Enhancing privacy of Universal Re-encryption scheme for RFID Tags”, EUC 2004, Vol. 3207 LNCS, pp. 879-890, Dec. 2004.

[7] A. Jule, “Minimalost cryptography for Low Cost RFID Tag”, The Fourth International Conference on Security in Communication Networks SCN, Vol. 3352 LNCS, pp. 149-164, Sep. 2004.

[8] A. Jule, “Authentication Pervasive Devices

with Human Protocols", To appear Crypto 2005, Aug. 2005.

[9] A. Jule and R. Pappu, "Squealing euros : Privacy protection in RFID-enable banknote", In proceedings of Financial Cryptography-FC '03, Vol. 2742 LNCS, pp. 103-121, Sep. 2003.

[10] A. Juels and Stephen A. Weis, "Authenticating Pervasive Device with Human Protocols", Advances in Cryptology-CRYPTO 2005, LNCS, Vol. 3621, pp. 293-308, 2005.

[11] P. Peris-Lopez, J. C. Hernandes-Castro, J. M. Estevez-Tapiador, and A. Ribagorda, LMAP : A Real Lightweight Mutual Authentication Protocol for Lowcost RFID tags, In : Proc. of 2nd Workshop on RFID Security, July 2006. http://events.iaik.tugraz.at/RFIDec06/.

[12] P. Peris-Lopez, J. C. Hernandes-Castro, J. M. Estevez-Tapiador, and A. Ribagorda. M2AP : A Minimalist Mutual-Authentication Protocol for Low-cost RFID Tags. In : Proc. of International Conference on Ubiquitous Intelligence and Computing UIC'06, LNCS 4159, pp. 912-923. Springer-Verlag, 2006.

[13] TieyanLi and Guilin Wang, Security Analysis of Two Ultra-Lightweight RFID Authentication Protocols, IFIP SEC 2007, 14-16 May 2007, Sandton, Gauteng, South Africa, 2007.

[14] A. Poschmann, G. Leander, K. Schramm, and C. Paar, "A Family of Light-Weight Block Ciphers Based on DES Suited for RFID Applications", Workshop on RFID Security, Graz, Austria, July 2006.

[15] 조용석, "유한체상에서 고속연산을 위한 직렬곱셈기의 병렬화구조", 정보보호학회논문집, 제17권, 제1호, pp. 33-40, 2007.

[16] J. Daemen and V. Rijmen, The Design of Rijndael : The Wide Trail Strategy Explained. New York, Springer-Verlag, 2000.

[17] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede, "Public-Key Cryptography for RFID-Tags", In Proceedings of IEEE International Workshop on Pervasive Computing and Communication Security, p. 6, 2007.

안 효 범

1992년 단국대학교 전자계산학과 (이학사)
1994년 단국대학교 전산통계학과 대학원 석사(이학석사)
2002년 단국대학교 전산통계학과 대학원 박사(이학박사)
1997년~2005년 천안 공업대학 정보통신과 부교수
2005년~현재 공주대학교 정보통신학부 부교수

이 수 연

1990년 단국대학교 전산학과 학사(이학사)
1993년 단국대학교 전산통계학과 대학원 석사(이학석사)
2003년 성균관대학교 전기전자 및 컴퓨터공학부 대학원 박사(공학박사)
1997년~현재 백석문화대학 컴퓨터정보학부 교수