유한체 위의 이변수다항식을 이용한 RFID 인증 프로토콜

정석원*

Authentication Protocol for RFID using Bivariate Polynomials over a Finite Field.

Seok Won Jung*

요 약 RFID 시스템은 공정관리, 물류관리, 고객관리, 출입통제, 환경 센싱, 개체식별 등 다양한 산업에 적용되고 있다. 그러나 무선통신을 이용하기 때문에 보안성이 매우 취약하다. 본 논문에서는 태그와 리더기 사이의 기본 보안사항인 인증에 대한 프로토콜을 제안한다. 제안 프로토콜은 유한체 위의 이변수 다항식을 이용하여 도청공격, 재전송공격, 위치추적, 트래픽분석에 대해서 안전함을 보인다.

Abstract RFID system is applied to various industry such as process control, distribution management, access control, environment sensing, entity identification, etc. Since RFID system uses wireless communication, it has more weak points for security. In this paper, an authentication protocol is suggested between tags and a reader, which is basic property for security. A suggested protocol use a bivariate polynomial over a finite field and is secure against snooping, replay attack, position tracking and traffic analysis.

Key Word : authenticaion, replay attack, bivariate polynomial, finite field

Ⅰ. 서 론

1988년 M. Weiser는 어디서나 사용자가 원할 때 필요한 정보와 서비스를 제공받을 수 있도록 컴퓨터를 모든 주변 환경에 편재시키는 유비쿼터스 컴퓨팅의 개념을 처음으로 소개하였다.[8] 이러한 개념이 소개되었을 당시에는 기술구현이 불가능할 것으로 생각되었다. 그러나 컴퓨터의 지속적인 가격 하락과 소형화가 가능하게 됨에 따라 더욱 많은 사물에 IC 칩을 내장시킬 수 있게 되었으며, 센서 기술의 향상으로 사물의 식별과 위치 확인이 용이해졌다. 또한 유무선 통신 기술의 진보에 따라 가까운 미래에 유비쿼터스 컴퓨팅 시대가 도래 할 것으로 여겨지고 있다.

RFID 시스템은 공정관리, 물류관리, 고객관리, 출입통제, 환경 센싱, 개체식별 등 다양한 산업에 적용이 가능하다.[2] 또한 개인의 이동환경에서 물품을 관리하는 것부터 휴대 단말기를 통하여 다양한 정보를 제공 받을 수 있는 매체로도 확대될 수 있다.[2] 이러한 이유로 IFID 칩이 값싸질 경우 RFID 태그는 유비쿼터스 컴퓨팅을 실현하는 핵심기술이 될 수 있을 것이다.

그러나 RFID 시스템의 핵심기술인 자동인식 기능과 물품정보 열람기능은 사용자에 대한 심각한 프라이버시 침해요소가 된다.[1] RFID 기술의 개인 프라이버시 침해는 개인에 대한 위치

* Corresponding Author: Department of Information Security Engineering Professor of Mokpo National University (jsw@mokpo.ac.kr)
Received : August 18, 2014 Revised : August 29. 2014 Accepted : September 12. 2014

추적과 개인이 소유하고 있는 물건 또는 정보가 무엇인지 알아내는 것 등이 포함된다. 따라서 이러한 역기능을 적절히 해소하지 못하면 산업에서 RFID의 적용 활성화에 많은 어려움이 있을 것으로 여겨지고 있다.

본 논문은 RFID 시스템의 보안 기능 중 가장 기본이 되는 태그 인증에 대한 프로토콜을 제안한다. 제안 프로토콜은 기존에 제안되었던 해쉬 함수를 이용하는 프로토콜[7], 공개키 알고리즘에 기반한 프로토콜[5] 등과 달리 유한체 위에 정의된 이변수 다항식을 이용한 프로토콜이다. 이러한 이변수 다항식은 인증 프로토콜 이외에 키 분배 프로토콜에 많이 사용되고 있다.[3, 4, 6]

II. 해쉬-락(Hash-lock) RFID 인증 프로토콜

1. RFID 시스테 개요

RFID의 시스템의 구성은 보통 태그와 리더기, 그리고 백 엔드 시스템으로 분류된다. 태그는 리더기로부터 송신된 신호를 수신하여 자신이 가지고 있는 정보를 리더기로 보내는 기능을 담당한다. 리더기는 태그가 수집한 정보를 얻어올 목적으로 태그로 신호를 보낸 후 태그로부터 송신된 정보를 수신하고 그 정보를 처리하는 기능을 가지고 있는 장치이다. 백 엔드 시스템은 태그로부터 전송된 정보 또는 태그로 관리하는 물품에 대한 정보 등 RFID 시스템에 필요한 정보를 저장하는 데이터베이스를 가진 정보처리 시스템이다.

2. 해쉬-락(Hash-lock) 인증 프로토콜

백 엔드 시스템은 사용되는 태그를 물리적으로 배치시키기 전에 태그마다 유일하게 ID와 Key를 생성하여 태그에 저장한다. 그리고 해쉬 함수 H()와 키를 사용하여 metaID = H(Key)를 계산하고 metaID를 태그에 저장한다. 또한 모든 태그의 ID와 Key, metaID 값을 백 엔드 시스템의 DB에 저장한다.

태그가 배치되고 난 뒤 리더기는 태그로부터 필요한 정보를 수집하기 전에 태그가 정당한 태그인가를 확인하기 위해 요청(Query)을 보낸다. 태그는 자신이 저장하고 있던 metaID를 리더기로 전송하고, 리더기는 백 엔드 시스템의 데이터베이스에서 metaID에 맞는 ID와 Key를 찾기 위해 metaID를 보낸다. 백 엔드 시스템은 리더기로부터 받은 metaID를 가지고 DB를 찾아 metaID와 짝을 이루고 있는 Key와 ID 값을 리더기로 보낸다. 리더기는 태그로 Key를 보내고, 태그는 이를 해쉬함수로 해쉬하여 얻은 값과 자신의 metaID값이 일치하는 가를 확인한다. 일치할 경우, 리더기와의 접근이 가능하게 된다. 또한 태그가 자신의 ID 값을 리더기로 보내면 리더기는 태그로부터 받은 ID 값과 백 엔드 시스템으로부터 받은 ID 값을 비교하여 값이 같은 경우 태그를 정당한 태그로 인증한다. 아래 그림 1은 해쉬-락 기법의 동작과정을 나타낸 것이다.

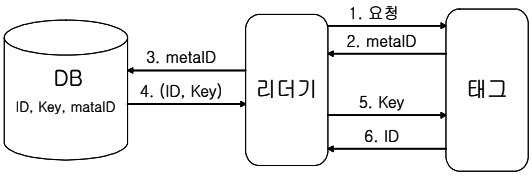

그림 1. 해쉬-락 기법

3. 해쉬락 기법의 문제점

해쉬-락 기법은 실제 ID가 노출되는 것을 방지하기 위하여 실제 ID 대신에 metaID를 이용하여 정보 전송을 하고 있다. 그러나 metaID의 값이 항상 고정되어 있기 때문에 공격자가 태그를 쉽게 추적할 수 있다. 또한 공격자가 태그와 리더기 사이의 무선구간에서 주고받는 데이터 쌍인 metaID와 ID 값을 도청한다. 리더기의 요청이 있을 때 공격자는 태그를 가장하여 metaID 값과 ID 값을 순서대로 보낸다. 이 과정에 Key 값도 얻을 수 있다. 따라서 해쉬-락 인증 프로토콜은 스푸핑 공격에 취약하다.

Ⅲ. 제안 인증 프로토콜

1. 유한체 위의 일변수 다항식을 이용한 인증 프로토콜

소수 p에 대하여 유한체 $\mathbb{Z}p = \{0, 1, 2, \cdots, p-1\}$라 하고, 유한체 $\mathbb{Z}p$ 위에 정의된 다항식의 모임을 $\mathbb{Z}p[x] = \{a0 + a1x + \cdots + anxn \mid i = 0, 1, ..., n$에 대해 $ai \in \mathbb{Z}p\}$라 하자. RFID를 사용자에게 배포하기 전에 다항식 모임 $\mathbb{Z}p[x]$에서 한 다항식 f(x)를 꺼내어 리더기와 RFID에 저장한다.

가. 인증절차

다음 그림 2는 태그의 식별자 IDT 값과 난수 R 그리고 일변수 함수 f(x)를 이용한 인증프로토콜을 순서대로 그린 것이다.

단계1. 리더기는 RFID의 인증을 요청하기 위해 인증 요청 메시지와 난수 R 값을 전송한다.

단계2. 인증 요청 메시지와 R값을 받은 태그는 자신의 식별자인 IDT 값과 받은 R값을 XOR 연산(⊕)한다. 태그는 연산된 값을 저장되어있던 함수 f(x)에 대입하여 f(IDT⊕R) 값을 얻고, 얻은 f(IDT⊕R) 값과 IDT 값을 리더기에 보낸다.

단계3. $f(ID_T \oplus R)$ 값과 ID_T 값을 받은 리더기는 받은 ID_T 값과 처음에 보냈던 R값의 XOR 값을 저장되어있던 함수 f(x)에 대입하여 $f(ID_T \oplus R)$ 값을 얻고, 얻은 $f(ID_T \oplus R)$ 값이 태그에게서 받은 $f(ID_T \oplus R)$ 값과 일치하는지 확인한다.

나. 안전성분석

이 프로토콜은 태그로부터 전송되는 데이터가 리더기가 보내는 난수 R에 따라 항상 변하게 된다. 따라서 공격자가 이전에 태그로부터 전송되었던 ID_T, $f(ID_T \oplus R)$ 값을 도청하여 얻은 후 태그를 위장하여 재전송하는 공격은 가능하지 않다. 왜냐하면 리더기의 새로운 인증요청에 포함된 난수

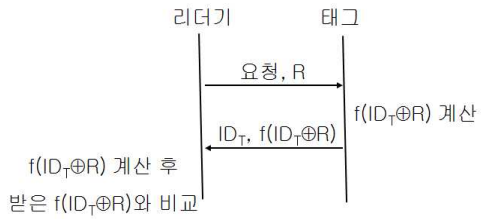

그림 2. 일변수다항식을 이용한 인증프로토콜

R′의 값이 달라 도청한 f(IDT⊕R) 값과 실제 f(IDT ⊕R')이 다르기 때문이다.

그런데 공격자가 리더기와 태그 사이의 데이터를 도청하여 n+1개의 f(IDT⊕R) 값들을 수집하였다고 가정할 수 있다. 즉, i=0, 1, ..., n+1에 대해 i번째 난수 값을 Ri라 하고 IDT⊕Ri=αi라 놓으면, β1=f(α1), β2=f(α2), ⋯, βn+1=f(αn+1)인 β1, β2, ..., βn+1 값을 수집한 것이다. 공격자는 f(x)를 찾기 위해 f(x)=a0 + a1x + ⋯ + anxn 로 놓고 x에 수집한 αi값을 넣으면

$$a0 + a1\alpha1 + \cdots + an\alpha1n = \beta1,$$
$$\vdots$$
$$a0 + a1\alpha n+1 + \cdots + an\alpha n+1n = \beta n+1$$

일차연립방정식을 얻는다. 이는 n+1개의 미지수 ai들을 포함하고 있으므로 가우스 소거법을 사용하면 해를 구할 수 있다. 따라서 공격자는 리더기의 요청에 대한 답변을 구한 f(x)를 이용하여 만들 수 있으므로 위장이 가능하다.

2. 유한체 위의 이변수 다항식을 이용한 인증 프로토콜

소수 p에 대하여 유한체 $\mathbb{Z}p$ 위에 정의된 이변수다항식의 모임을 $\mathbb{Z}p[x, y] = \{f(x, y) = \sum_i \sum_j aijxiyj \mid aij \in \mathbb{Z}p\}$라 하자.

태그를 물리적으로 배포하기 전에 이변수 다항식 모임인 $\mathbb{Z}p[x, y]$에서 한 다항식 f(x, y)를 꺼내어 리더기와 태그에 저장한다. 그리고 태그의 식별자 IDT 값과 리더기의 식별자 IDR을 저장해두고, 태그들의 식별자 IDT 값들은 데이

터베이스에 저장해 둔다.

가. 인증절차

리더기가 보내는 난수를 R이라 하고, 태그가 보내는 난수를 r로 표시하자.

단계1. 리더기는 태그의 인증을 요청하기 위해 인증 요청 메시지와 난수 R 값을 방송한다.

단계2. 요청 메시지와 R 값을 받은 태그는 저장되어있던 IDR 값과 받은 R 값, 자신의 식별자인 IDT 값과 난수 r 값을 가지고 IDR⊕R 값과 IDT⊕r⊕R 값을 얻는다. 태그는 계산한 IDR⊕R 값과 IDT⊕r⊕R 값을 이변수다항식 f(x, y)에 대입하여 f(IDR⊕R, IDT⊕r⊕R) 값을 계산하고, f(IDR⊕R, IDT⊕r⊕R) 값과 IDT⊕r 값을 리더기에 보낸다.

단계3. f(IDR⊕R, IDT⊕r⊕R) 값과 IDT⊕r 값을 받은 리더기는 저장되어있던IDR 값과 R 값을 XOR 연산하고, 받은 IDT⊕r 값에 R 값을 XOR 연산하여 IDT⊕r⊕R 값을 얻는다. 리더기는 연산한 IDR⊕R 값과 IDT⊕r⊕R 값을 이변수다항식 f(x)에 대입하여 f(IDR⊕R, IDT⊕r⊕R) 값을 얻고, 얻은 f(IDR⊕R, IDT⊕r⊕R) 값이 태그에게서 받은 f(IDR⊕R, IDT⊕r⊕R) 값이 일치하는지 확인한다.

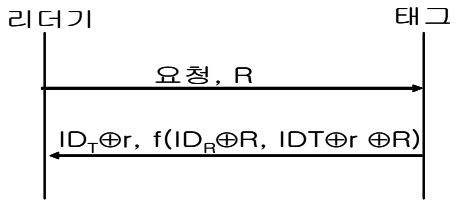

그림 3. 이변수다항식을 이용한 인증프로토콜

나. 안전성 분석

이 프로토콜은 태그로부터 전송되는 데이터가 리더기가 보내는 난수 R과 태그가 보내는 난수 r에 따라 항상 변하게 된다. 따라서 이전에 태그로부터 전송되는 IDT⊕r, f(IDR⊕R, IDT⊕r⊕R) 값을 도청하여 저장하고 있다고 하여도 리더기의 새로운 인증요청에 전송되는 난수 R′이 달라 재전송 공격에 안전함을 알 수 있다.

리더기와의 통신 때마다 태그의 응답 값이 달라 트래픽 분석이 가능하지 않으며, RFID의 식별자가 그대로 전송되지 않고 매번 난수 r과 XOR 되어 전송되기 때문에 위치추적에도 안전하다.

공격자가 리더기와 태그 사이에 오고가는 데이터를 도청하여 R 값과 IDT⊕r 값, f(IDR⊕R, IDT⊕r⊕R) 값을 여러 쌍 수집할 수 있다. 공격자는 $f(x, y) = \sum_i \sum_j aijxiyj$로 가정하고 수집한 값들로 일차연립방정식을 만들어 aij 값을 알아내려 할 것이다. 그러나 이 경우 공격자는 aijxiyj에서 x와 y의 값인 IDT⊕r와 IDT⊕r⊕R을 알 수 없으므로 aij 값도 알아낼 수 없다. 그러므로 제안 인증 프로토콜이 도청 공격에 안전함을 알 수 있다.

Ⅳ. 결 론

유비쿼터스 컴퓨팅은 사용자에게 정보 서비스를 할 때 '언제, 어디에서든지 컴퓨터에 엑세스할 수 있도록 하는 상태'를 말한다. 이런 유비쿼터스 컴퓨팅이 이루어지는 사회가 바로 유비쿼터스 사회이고, 유비쿼터스 사회는 이미 우리 생활 속에 깊숙이 파고들어와 있다.

그러나 RFID 시스템은 개방화된 통신망인 무선통신을 해야 하기 때문에 유선망을 이용할 때보다 훨씬 더 보안에 있어서 심각한 문제를 일으킬 수 있다. 공격자가 정보들을 도청하여 악의적인 목적으로 사용할 수도 있으며 보안이 취약함에 따라 구매자의 위치정보, 구매이력 등이 유출 될 수도 있다. 그러므로 RFID 시스템에서의 보안문제를 해결하는 것은 유비쿼터스 사회의 구축을 위해 매우 시급한 일이다.

본 논문에서는 RFID 시스템에 대한 보안에서 가장 기본이 되는 사항인 태그와 리더기의 인증에 대한 프로토콜을 제안하였다. 가장 처음으로

제안되었던 해쉬-락 기법은 도청으로 얻은 정보를 이용한 재전송 공격에 취약하며, 사용자의 위치정보 노출과 같은 취약점이 있었다. 본 논문에서 제안된 인증프로토콜은 공격자가 도청하여 얻은 정보로 재전송 공격이 가능하지 않으며, 트래픽 분석을 어렵게 만들고 태그의 식별자 노출이 없으므로 태그의 위치정보를 제공하지 않는 장점이 있다. 이를 요약하면 [표 1]과 같다.

표 1. 해쉬락 기법과 제안 프로토콜의 비교

	해쉬-락 기법	제안 프로토콜
재전송 공격	가능	불가능
트래픽분석	가능	불가능
위치정보	노출	노출 안 됨
안전성 근거	해쉬함수	이변수 다항식

향후 이변수 다항식을 태그 내의 하드웨어 암호모듈로 구현할 때 기존의 해쉬함수와 비교했을 때 어느 정도 효율성을 갖는가에 대한 연구가 필요하다. 또한 이변수 다항식 자체의 암호학적 특성이나 요구사항에 대한 연구가 필요하다.

References

[1] 강전일, 박주성, 양대헌, “RFID 시스템에서의 프라이버시 보호기술”, 정보보호학회지 제14권 제6호, pp.28-36, 2004.

[2] 유승화, 유비쿼터스 사회의 RFID, 전자신문사, 2005년.

[3] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks", In IEEE Symposium on Security and Privacy, pp.197-213, 2003.

[4] W. Du, J. Deng, Y. S. Han, S. Chen, and P. K. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge", Technical Report, 2003. Available from http://www.cis.syr.edu/~wedu/Research/paper/ddhcv03.pdf

[5] A. Juels, R. L. Rivest, and M. Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy", The 8th ACM Conference on Computer and Communications Security, 2003.

[6] D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks", In 10th ACM Conference on Computer and Communications Security, 2003.

[7] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, "Security and Privacy Aspects of Low-cost Radio Freqency Identification Systems", First International Conference on Security in Pervasive Computing, LNCS 2802, pp.201-212, 2003.

[8] M. Weiser, "The Computer for the 21 Centry, Scientific American", Vol. 256, No. 3, pp.94-104, 1991.

저자약력

정석원 (Seok-won Jung) **정회원**

현재 - 목포대학교 정보보호학과 교수

<관심분야> 신호처리, 영상처리, 암호화, 컴퓨터 보안