RFID 프라이버시를 위한 ECC기반의 익명인증기법

정회원 김 석 매*, 이 영 진**°, 이 상 호***, 이 충 세***

A Anonymous Authorization Scheme Based on ECC for RFID Privacy

Shi-Mei Jin*, Yong-Zhen Li**°, Sang-Ho Lee***, Chung-Sei Rhee*** ***Regular Members***

요 약

최근 이동통신기술의 발달과 사용편리성을 위한 최근에 모바일 RFID리더기에 대한 연구 개발도 활발하게 진행되고 있다. 특히 현재 RFID 시스템에서는 리더와 백-엔드 DB 구간은 유선구간으로 간주하여 안전한 채널로 가정하고 있다. 그러나 모바일 RFID 리더기 사용으로 시스템에는 무선 환경의 보안 취약성과 프라이버시 침해 등 문제점이 발생하고 있다. 이 논문에서는 초특이 타원 곡선 Weil-pairing 유한군을 적용한 타원 곡선 암호 알고리즘을 사용하여 은닉서명을 설계하고 그 은닉서명을 기반으로 사용자 익명성이 보장되는 모바일 RFID리더 인증 기법을 제안한다.

Key Words : RFID, Privacy, Anonymous, Authorization, ECC

ABSTRACT

Recently, with the development of mobile techniques and the consideration to conveniency of using, the research on Mobile RFID Reader technique is getting more and more attentions. Until now, all security authentication algorithms of RFID are algorithms about range between Tag and Reader. The range between Reader and backend DB is composed by wired networks, so it's supposed to be secure range. But it must be taken account of the problem of information security and privacy in wireless range during the design of Mobile REID Reader. In this paper we design an blind signature scheme based on weil-paring finite group's ECC encryption scheme, and by using this blind signature we propose the anonymous authorization scheme to Mobile RFID Reader's users.

Ⅰ. 서 론

최근 들어 RFID 기술은 단순한 바코드의 대체 수준을 넘어서 통신, 물류, 국방, 소방, 금융, 의료, 환경, 교육, 정보가전, 도로, 건설 등 다양한 인간의 생활 전반에 활용되어 무한한 부가가치의 창출이 가능하여, 향후 전 세계적인 산업구조, 시장구조의 변화뿐만 아니라 인간의 삶의 형태까지 변화시키게 될 유비쿼터스 컴퓨팅의 기반 기술로서 인식되고 있다. 그러나 기존 RFID 시스템은 비용문제, 무선 환경의 보안 취약성 및 프라이버시 침해와 같은 새로운 보안문제점이 발생하고 있다[1].

RFID시스템의 보안문제의 연구에서는 실제 RFID 시스템을 태그, 리더 및 백-엔드 DB 등 3개

* 충북대학교 전자계산학과 알고리즘 연구실(kimsm@chungbuk.ac.kr),
** 중국연변대학교 컴퓨터과학 및 기술학과(lyz2008@ybu.edu.cn) (° : 교신저자)
*** 충북대학교 전기전자컴퓨터공학부(shlee@chungbuk.ac.kr), (cscrhee@chungbuk.ac.kr)
논문번호 : KICS2007-10-441, 접수일자 : 2007년 10월 4일, 최종논문접수일자 : 2008년 2월 20일

요소로 구성하고 통신 구간을 태그와 리더 구간 리더와 백-엔드 DB 구간으로 구분한다. 태그와 리더 구간은 태그의 자원의 제한으로 그리고 무선 특성 때문에 안전하지 않은 채널로, 리더와 백-엔드 DB 구간은 유선구간으로 간주하여 기존 보안기법들을 그대로 적용할 수 있어 안전한 채널로 가정하고 있다[1]. 그러나 이동통신기술의 발달과 사용편리성을 위하여 최근에 모바일 RFID리더 연구가 활발하게 진행되고 있다[2].

현재 대부분 분야에서는 RSA나 ElGamal 공개키 암호화 알고리즘을 이용한 전자서명을 사용하고 있다. 이런 전자서명 기법들은 계산량이 많고 암호화/복호화 속도가 느리기 때문에 자원의 제약을 받는 모바일 RFID 리더에 적용할 수 없다. 따라서 이 논문에서는 초특이 타원 곡선 Weil-pairing 유한군을 적용한 타원 곡선 암호 알고리즘을 사용하여 은닉 서명을 설계하고 그 은닉 서명을 기반으로 리더를 인증하는 기법을 제안한다. 즉, 모바일 RFID 리더 장치의 연산 능력을 고려하고 사용자 익명성이 보장되는 보다 효율적인 RFID리더 인증 기법을 제안한다.

Ⅱ. 관련 연구

익명성 기술은 프라이버시 보호가 전 세계적인 이슈로 등장하면서 이론적 연구가 크게 부각되고 있다. 주요 기술로는 Mix-Network, 전자서명, 익명 신임장 등 기술들이 있다.

2.1 Mix-Network기반 익명기술

Mix network는 1981년 Chaum에 의해 제안되었으며, 네트워크에서 익명성을 유지하도록 해준다[3]. Mix network는 암호화된 메시지를 입력받아 재 암호화한 후 랜덤한 순서로 출력하는 방식으로 입력 메시지와 출력 메시지간의 대응 관계를 알 수 없게 한다. 이것은 anonymous 전자 우편, 웹 브라우징, 익명화 지불 시스템 등에 응용된다[4].

1) Anonymizer

웹 사용자의 인터넷 이용에 관련된 정보를 숨기는 기술이다. 이 기술은 웹 사이트를 통해 제공하는 IP 주소와 같은 사용자의 인터넷 이용 정보를 숨긴다.

2) Onion Routing

Mix-network를 통하여 데이터 트래픽의 내용을 숨기는 기술이다. 네트워크상에서 패킷(packet)의 익명성을 유지하는 것을 목표로 개발한 안전한 통신 제공 시스템 구조로서 자동적으로 사용자의 통신 내용에 대한 익명성을 보장한다.

3) Crowds

라우팅 되는 HTTP 트래픽의 내용을 숨기는 기술이다. 인터넷에서 사용자의 익명성을 보호하기 위해 암호화를 사용하여 통신하는 데이터 트래픽이 어떤 전달 과정을 거쳐 서버까지 오게 되었는지의 라우팅 경로 정보를 은닉시켜 송신자의 익명성을 제공한다.

4) Janus

URL을 암호화하여 클라이언트와 서버의 익명성을 동시에 제공하는 proxy 서버 기술이다. 이 기술은 IP 주소와 호스트 이름을 숨겨 익명성을 제공한다.

5) TAZ

URL과 데이터 스트림까지 암호화하여, 데이터의 무결성 및 보안을 동시에 제공하는 기술이다. 이 기술은 Janus기술의 문제점을 데이터 트래픽의 암호화로 해결하였다.

2.2 전자서명기반 익명기술

1) 그룹 서명

그룹 서명은 1991년 D. Chaum과 Van Heyst에 의해 처음으로 제안되었다[5]. 그룹 서명은 그룹의 구성원이 그룹을 대표하여 서명하고, 서명자의 익명성이 보장된다. 미국 Department of Transportation이 제안한 Vehicle Safety Communications 시스템은 그룹 서명을 이용하여 사용자의 익명을 제공한다. 효율적인 그룹 서명을 위해 서명의 길이가 짧아야 하며 현재 가장 짧은 그룹 서명은 대략 200비트 정도이다[6,7].

2) 링(Ring) 서명

링 서명은 2001년 Rivest, Shamir와 Tauman에 의해 제안되었으며 그룹 서명과 거의 유사하다. 다만 그룹 관리자가 없다는 점이 그룹 서명과 다르다. 그룹서명은 그룹 관리자에 의해 누가 서명하였는지 알 수 있지만 링 서명은 사용자에 대한 무조건적인 익명성이 보장된다[8,9].

3) 은닉(Blind) 서명

은닉 서명은 프라이버시 보호를 위한 기본 프리

미티브로서 전자 화폐를 위한 인증 기법이며, 1981년에 Chaum이 RSA을 이용한 인증기법을 제안하였다. 은닉 서명은 사용자에게 완벽한 익명성을 주기 때문에 전자 투표에 이용되기도 한다[10, 11].

2.3 기타

1) 익명 신임장

익명 신임장(Anonymous credential)시스템은 가명(pseudonym)시스템이라고도 불리며, 1985년 Chaum에 의해 제안되었다[12]. 이 시스템은 기관과 사용자로 구성되며 기관은 사용자의 가명만을 알고 그에 대한 신임장(credential)을 발급할 뿐 사용자의 신원에 대해선 알 수 없으므로 사용자의 프라이버시를 보호된다. 익명 신임장 시스템은 최근에 Camenisch와 Lysyanskaya가 은닉 사상을 이용한 기법을 제안하였다[13].

2) 분산암호기법

분산암호기법은 1979년 Shamir가 최초로 마스터 키에 대한 비밀 공유 문제에 대하여 연구하였다. 마스터 키를 한 사람에게 맡겨 놓는 것은 키가 유출되었을 경우나 키를 맡은 사람이 배신을 할 경우 대책이 없기 때문이다. 그러므로 키에 대한 정보를 모두에게 나누어서 위험을 줄이려는 것이다. 분산암호기법은 n명의 구성원이 있다면 적어도 k명 이상이 모여야 키를 복구할 수 있고, k명 이하일 경우는 키에 대한 어떤 정보도 얻을 수 없는 (n, k)-threshold 기법을 말한다[14].

Ⅲ. 제안 기법

3.1 Weil-Pairing을 적용한 은닉 서명

은닉 서명은 서명 의뢰자가 서명자에게 메시지의 내용을 보여주지 않고 메시지에 대한 유효한 서명값을 얻는 서명 방식이다. 은닉 서명은 사용자의 완전한 익명성과 불추적성을 제공하므로 개인 프라이버시를 보장할 수 있다. 이 연구에서는 초특이 타원곡선인 Weil Pairing 적용한 ID 기반 공개키 암호기법을 사용하여 은닉 서명 방법을 다음과 같이 제안한다. 서명 과정은 보통 초기화 단계, 서명 생성 단계 및 서명 검증 단계 등 3개 단계로 나뉜다.

1) 초기화 단계

초기화 단계는 표 1에서와 같이 서명에 필요한 객체들에 대한 정의, 파라메타 생성 및 등록하는 단계이다.

표 1. 은닉 서명을 위한 초기화 정보

초기화 정보	설 명
G	소수l을 위수로 하는 GDH군
P	G의 생성원
$\hat{e}$	bilinear 함수 Weil-Pairing
H_1, H_2	충돌회피 해쉬 함수
id_X	서명자의 ID
$t, r \in Z/l$	난수
$W_X = H_2(ID_X)$	서명자의 공개키
$w_X = t \cdot W_X$	서명자의 개인키
$P_X = tP$	공개
M	서명될 메시지

2) 서명 생성 단계

이 단계는 서명 의뢰자가 메시지 교환을 통하여 서명을 획득하는 과정으로 구체적으로는 다음과 같다

(1) 서명자는 난수 $r \in Z/l$를 선택하고 난수 r과 자신의 공개키 W_X를 이용하여 $A = r\,W_X$,를 계산하고 그 값을 서명 의뢰자한테 전송한다.
(2) 서명 의뢰자는 서명자로부터 받은 A값과 서명메시지 M을 해쉬 함수 H_1에 통과시켜 해쉬 값 $h = H_1(M.A)$을 계산하고 그 값을 서명자한테 전송한다.
(3) 서명자는 서명 의뢰자로부터 받은 은닉 메시지 $h = H_1(M.A)$를 이용하여 $B = (r+h)w_X$를 계산하여 서명 의뢰자에게 B를 보낸다.
(4) 서명 의뢰자는 서명자로부터 받은 A와 B를 받음으로서 메시지 M에 서명 $Sign_X(A, B)$를 획득하게 된다.

3) 서명검증단계

서명의뢰자의 서명검증은 bilinear 함수 $\hat{e}$를 사용하여 $\hat{e}(P_X, A + h\,W_X)$값과 $\hat{e}(P, B)$값을 계산하여 동일 여부를 확인한다. 즉, $\hat{e}(P_X, A + h\,W_X)$ $=\hat{e}(P, B)$임을 증명하면 된다.

[증명]

$$\hat{e}(P_X, A + h W_X)z \quad (1)$$

$\because\ P_X = tP,\ A = r W_X$ 이것을 식(4)에 대입

$\therefore\ \hat{e}(P_X, A + h W_X)$

$= \hat{e}(tP, r W_X + h W_X)$ (2)

Weil Pairing은 $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$라는 특성이 있으므로 식(2)를 다음과 같이 변화할 수 있다.

$$\hat{e}(tP, r W_X + h W_X) = \hat{e}(P, (r+h) W_X)^t$$
$$= \hat{e}(P, (r+h)t W_X) \quad (3)$$

$\because$ 서명자의 개인키와 공개키 상관관계는 $w_x = t W_X$이다. 이것을 식(3)에 대입하면

$$\hat{e}(P, (r+h)t W_X) = \hat{e}(P, (r+h) w_X) \quad (4)$$

여기서 $B = (r+h) w_X$이므로 식(4)에 대입하면 $\hat{e}(P, (r+h) w_X) = \hat{e}(P, B)$을 얻을 수 있다. 즉, $\hat{e}(P_X, A + h W_X) = \hat{e}(P, B)$가 성립함을 증명한다. ■

3.2 은닉서명을 이용한 리더 인증기법

제안기법에서 인증과정은 서명에 사용되는 파라메타와 객체들의 초기화 값을 설정하는 초기화단계와 서명을 요청, 생성 및 검증하는 인증 단계로 구성된다. 초기화 과정은 위에서 기술한 것과 같으므로 여기서는 인증 과정만 구체적으로 기술한다.

제안기법에서는 서명 생성에서 리더 장치 사용자의 익명성을 보장하기 위하여 서명메시지를 해쉬함수를 이용하여 은닉된 서명메시지로 변화시켜 서명을 수행한다. 제안기법은 백-엔드가 은닉서명메시지를 리더에 보내어 리더의 서명을 생성하고 그 서명 검증을 통하여 리더를 인증한다. 즉, 인증 단계는 그림 1에서와 같이 5개 단계로 수행된다.

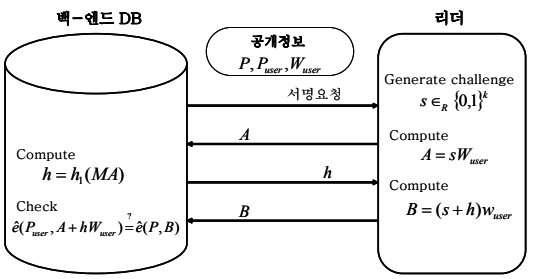

그림 1. 은닉서명 이용한 리더 인증 기법

단계 1: 백-엔드 DB는 리더를 인증하기 위하여 리더에게 서명 요청을 한다.

DB → Reader: 서명요청

단계 2: 리더는 랜덤 난수를 $s \in Z/l$ 선택하고 난수와 자신의 공개키 W_{user}를 이용하여 $A = s W_{user}$,를 계산하여 백-엔드 DB에게 전송한다.

Reader:

Generate challenge $s \in_R \{0,1\}^l$

Compute

$A = s W_{user}$

Reader → DB: A

단계 3: 백-엔드 DB는 리더 관련 정보로 메시지(M)를 구성하고 전송받은 A 값과 함께 해쉬 값(h)을 계산한다. 그리고 은닉된 메시지를 포함한 해쉬 값을 리더에 전송한다.

DB:

Compute

$h = H_1(M.A)$

DB → Reader: h

단계 4: 리더는 전송받은 해쉬값 h와 난수 s, 자신의 개인키 w_{user}를 사용하여 서명값 B를 생성하여 백-엔드 DB에 전송한다.

Reader:

Compute

$B = (r+h) w_{user}$

Reader → DB: B

단계 5: 백-엔드 DB는 리더 관련 은닉 정보가 포함된 서명값 B에 대하여 A값, h값 및 리더의 공개키를 이용하여 서명의 정당성을 검증한다.

$$\hat{e}(P_X, A + h W_X) \stackrel{?}{=} \hat{e}(P, B)$$

위의 식에 의하여 서명 검증으로 어떤 리더인지 모르지만 누구든지 리더의 정당성에 대하여 인증할 수 있다.

Ⅳ. 안전성 및 성능 평가

4.1 안전성 분석

1) 암호학적 안전성이 강인하다. 제안 리더 인증

기법은 암호학적으로 이산대수 문제의 어려움 및 일방향 해쉬 함수의 안전성을 기반으로 하였으며 Weil-Pairing을 적용한 은닉 서명을 이용하여 현존의 암호학적 공격에 안전하다.

2) 리더의 위장이 불가능하다. 보통 RFID시스템에서 리더의 인증을 태그가 맡아서 하게 되는데 이것은 제한된 자원의 영향을 받는 태그의 측면에서 강인한 인증이 불가능하다. 따라서 기존 기법들에서는 리더의 위장공격에 노출된다고 할 수 있다. 제안 리더 인증 기법은 초특이 타원곡선 Weil-Pairing을 적용한 은닉 서명을 기반으로 인증하였다. 따라서 이산대수 문제의 어려움에 의하여 리더가 선택한 난수 s를 알아낼 가능성이 없으면 리더의 위장이 불가능하다.

3) 리더의 익명성을 제공한다. 제안 리더 인증 기법에서는 랜덤 난수 s,t와 리더의 ID정보를 일방향 해쉬 함수 h1을 이용하여 은닉 시켰으므로 리더에 대한 정당성은 검증할 수 있지만 리더가 어떤 것인지는 알 수 없다. 그러므로 은닉 서명 기반의 식별 정보의 익명성을 제공하여 리더의 위치 추적을 불가능하게 한다.

4.2 효율성 분석

이 논문의 리더인증에 사용한 은닉 서명은 초특이 타원 곡선 Well-pairing을 적용한 ID기반 공개키 암호 방식으로 GDHP의 어려움을 기반으로 하고 있으며 타원 곡선 상에서 덧셈 연산으로 이루어지므로 유한체상의 어느 연산보다 연산속도가 빠르고 짧은 길이의 키에 비해 강인한 안전성을 갖는다.

표 2은 제안 리더 인증 기법에 사용된 은닉 서명과 기타 익명 기술들의 효율성을 비교한 결과이다.

표 2. Well-pairing 기반의 은닉서명 기법의 효율성 평가

기법		연산
Mix Network 기반 기법	RSA /ElGamal	지수/곱셈연산
전자서명 기반 기법	RSA /ElGamal	지수/곱셈연산
제안 기법	ECC	덧셈연산

표 2에서 보면 기존 익명 기술은 주로 RSA와 ElGamal 공개키 암호기법을 기반으로 이루어져 있으며 이는 지수연산과 곱셈연산을 기반으로 계산된다. 또한 이런 공개키 암호기법은 안전성을 보장하기 위하여 현재 2048비트의 키의 사용을 권장하고 있다. 그러나 제안 기법에서는 160비트 키를 사용하고 암호화 연산이 덧셈으로 설계되어 기존 1024비트 키 지수연산(RSA)과 곱셈연산(ElGamal)을 기반으로 하는 인증 기법들보다 계산양 측면에서 효율적이다.

V. 결 론

RFID 기술은 다양한 인간의 생활 전반에 활용되어 무한한 부가가치의 창출이 가능하여, 향후 전 세계적인 산업구조, 시장구조의 변화뿐만 아니라 인간의 삶의 형태까지 변화시키게 될 유비쿼터스 컴퓨팅의 기반 기술로서 인식되고 있다. 그러나 기존 RFID 시스템은 비용문제, 무선 환경의 보안 취약성 및 프라이버시 침해와 같은 새로운 보안문제점이 발생하고 있다.

이 논문에서는 제안한 리더 인증 기법은 리더 사용자 프라이버시 보호 측면에서 이산대수 어려움을 기반으로 Weil-Pairing 유한군을 적용한 타원곡선 암호알고리즘을 응용하여 리더를 인증하였고, 리더 식별정보를 그대로 사용하지 않고 일방향 해쉬 함수를 기반으로 은닉하여 사용하였으므로 사용자 익명성이 보장되었다. 또한 제안 기법은 ECC암호기법을 이용하여 설계되어 기존의 RSA나 ElGamal 공개키 암호를 이용한 인증 기법보다 계산속도가 빠르다는 장점을 갖고 있어 자원의 제약을 받는 이동성 리더기에 적용이 가능하게끔 설계되었다. 그러나 초특이 타원곡선 Weil-Pairing을 적용한 공개키 암호기법은 개발이 어렵고 타원곡선 암호의 고유의 보안취약성이 존재할 수 있으므로 잠재된 위협이 있다는 문제점이 있다.

참 고 문 헌

〔1〕 Yong-Zhen Li, Young-Bok Cho, Nam-Kyoung Um, and Sang-Ho Lee, “Security and Privacy on Authentication Protocol for Low-Cost RFID,” Proceeding of the 2006 International Conference on Computational Intelligence and Security(CIS06), Part 2, pp. 1101-1104, Nov. 2006.

〔2〕 A. Juels “RFID Security and Privacy: A Research Survey,” In IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, 2006, pp. 381-394

〔3〕 D. L. Chaum, “Untraceable Electronic Mail,

Return Addresses, and Digital Pseudonyms," Communications of the ACM, vol. 24, no. 2, 1981, pp.84-88.

〔4〕 A. Serjantov, P. Sewell1 "Passive-attack analysis for connection-based anonymity systems," In International Journal of Information Security, Vol. 4, Num. 3, 2005, pp.172-180

〔5〕 D. L. Chaum, V. Heyst, "Group Signature," Advances in Cryptology-Eurocrypt 1991, LNCS 547, pp.257-265.

〔6〕 D. Boneh, X. Boyen and H. Shacham, "Short group signatures," Advances in Cryptology-Crypto 2004, LNCS 3152, pp.41-55.

〔7〕 D. Boneh and X. Boyen, "Short signatures without random oracles," Advances in Cryptology-Eurocrypt 2004, LNCS 3027, pp.56-73.

〔8〕 R. L. Rivest. "Chaffing and Winnowing: Confidentiality without Encryption," CryptoBytes 4(1), RSA Laboratories, 1998, pp.12-17.

〔9〕 R. L. Rivest, A. Shamir, Y. Tauman "How to Leak a Secret," Asia-CRYPT 2001, LNCS 2248, pp.552-565.

〔10〕 S. Brands, "Untraceable Off-line Cash in Wallets with Observers," CRYPTO'93, LNCS 773, pp.302-318.

〔11〕 M. Bellare, C. Namprempre, D. Pointcheval, M. Semanko, "The One-More-RSA-Inversion Problems and the Security of Chaum's Blind Signature Scheme," Journal of Cryptology, June 2003, pp.185-215.

〔12〕 D. L. Chaum, "Security Without Identification: Transaction Systems to Make Big Brother Obsolete," Commun. ACM, 1985, pp.1030-1044.

〔13〕 J. Camenisch, A. Lysyanskaya, "Signature Schemes and Anonymous Credentials from Bilinear Map," CRYPTO 2004, LNCS 3152, pp.56-72.

〔14〕 A. Shamir, "How to Share a Secret," Commun. ACM, 22, 1979, pp.612-613.

김 석 매 (Shi-Mei Jin) 정회원

2004년 8월 충북대학교 전자계산학 이학석사

2004년 9월~현재 충북대학교 전자계산학과 박사수료

<관심분야> M-Commerce, 정보보호, 알고리즘

이 영 진 (Yong-Zhen Li) 정회원

1997년 6월중국 연변대학교 물리학과 이학석사

2007년 2월 충북대학교 전자계산학과 이학박사

2008년 3월~현재 중국연변대학교 컴퓨터과학 및 기술학과 교수

<관심분야> 정보보호, 네트워크 보안, 프라이버시

이 상 호 (Sang-Ho Lee) 정회원

1981년 2월 숭실대학교 전자 계산학과 공학석사

1989년 2월 숭실대학교 전자 계산학과 공학박사

1981년~현재 충북대학교 전기전자컴퓨터공학부 교수

<관심분야> Protocol Engineering, Network Security, Network Management

이 충 세 (Chung-Sei Rhee) 정회원

1989년 University of South Carolina, 전산학 박사

University of North Dakota 전산학과 조교수

1991년~현재 충부대학교 전지전자컴퓨터공학부 교수

<관심분야> 결함허용, 알고리즘 및 전문가 시스템, 정보보안