RFID를 위한 이차잉여 기반의 개선된 상호인증 기법

(Improved Mutual Authentication Scheme based on Quadratic Residue for RFID)

박 한 나 † 김 세 일 ††
(Hannah Park) (Seil Kim)

천 지 영 †† 이 동 훈 †††
(Ji Young Chun) (Dong Hoon Lee)

요 약 최근 Chen 등은 태그 인증 시 서버의 전수조사를 막기 위해 제곱근을 구하는 어려움에 기반한 이차잉여를 이용한 상호인증기법을 제안하였다. 하지만 리더가 인증 시작 시 악의적으로 같은 랜덤 값을 보내는 경우 태그의 위치가 노출되는 문제가 발생한다. 또한 제한된 연산능력을 가진 저가태그에 해쉬함수와 제곱연산을 동시에 수행해야 하는 어려움이 존재한다. 따라서 본 논문에서는 Chen 등의 기법을 살펴보고, 이 기법이 갖는 문제점을 지적한다. 또한 태그에서 인증 시마다 랜덤 값을 새롭게 생성하여 위치추적에 안전하며, Chen 등의 기법과 달리 제곱연산만을 사용함으로써 보다 효율적인 이차잉여기반의 상호인증 기법을 제안한다. 제안하는 기법은 중앙 서버의 전수조사 없이 태그 인증이 가능하며 인증 시마다 비밀값의 갱신 없이도 전방향안전성을 만족하여 비밀값 동기화 과정이 필요 없다.

키워드 : RFID, 상호인증, 이차잉여, 저가태그

· 이 연구에 참여한 연구자(의 일부)는 '2단계 BK21사업'의 지원비를 받았음
· 이 논문은 제35회 추계학술대회에서 '개선된 이차잉여 기반의 RFID 상호인증 기법'의 제목으로 발표된 논문을 확장한 것임

† 학생회원 : 고려대학교 정보보호학과
hannah637@korea.ac.kr
†† 비 회 원 : 고려대학교 정보보호학과
sell82@korea.ac.kr
jychun@korea.ac.kr
††† 정 회 원 : 고려대학교 정보보호학과 교수
donghlee@korea.ac.kr

논문접수 : 2008년 12월 19일
심사완료 : 2009년 4월 3일

정보과학회논문지: 컴퓨팅의 실제 및 레터 제15권 제6호(2009.6)

Abstract Recently, Chen et al.'s proposed mutual authentication scheme based on the quadratic resiidue, finding the squaring root problem, for avoiding exhaustive search on the server. But, if a malicious reader sends same random value, the tag is traced by an adversary. Moreover, there is realization problem because of its limited ability to compute squaring and hash function. In this paper, we analyze Chen et al.'s scheme and its weakness. Furthermore we present an improved mutual authentication scheme based on the quadratic residue which solves the tracing problem by generating random value on the tag and uses only squaring. We also make the scheme satisfy to forward secrecy without updating and synchronizing and avoid exhaustive search.

Key words : RFID, mutual authentication, quadratic residue, low-cost tag

1. 서 론

RFID(Radio-Frequency IDentification) 시스템은 물품의 정보를 인식하기 위해 기존에 널리 사용되는 접촉식인 바코드와 달리 비접촉식으로 물품의 정보를 자동으로 인식하기 때문에 유통/물류 등 다양한 분야에서 주목받고 있다. 그러나 RFID 기술의 효율성에도 불구하고, 프라이버시 침해 문제와 시스템의 안전성에 대한 문제가 제기되면서 안전한 RFID 시스템을 위해 다양한 암호기법과 인증기법의 연구가 활발히 진행되고 있다. 초기에 Weis 등[1]은 해쉬함수와 의사난수 생성기를 이용하여 "해쉬락(Hash Lock)", "난수 해쉬락(Randomized Hash Lock)"기법을 제안하였으나 태그의 ID가 노출되어 태그의 프라이버시를 보장하지 못했다. 따라서 Ohkubo 등[2]은 해쉬체인(Hash Chain)을 이용하여 전방향안전성(Forward secrecy)을 만족하는 기법을 제안하였으나 재생공격(Replay attack)에 취약하였다. 또한 공격자 중간공격(Man-in-the-middle attack)에 안전한 상호인증의 필요성이 대두되면서, Yang 등[3,4]은 저가형 태그에서 상호인증 가능한 해쉬 기반의 기법을 제안하였다. Yang 등의 기법은 태그의 익명성과 위치정보와 태그사이의 비연결성을 제공하였으나 재생공격 등에 여전히 취약하였다. 따라서 2004년 Molnar 등[5]은 의사난수 함수(PRF: pseudo random function)를 사용한 기법을 제안하였으나 전방향안전성을 만족하지 못했다. 또한 모바일 RFID 환경이 나오면서 Tan 등[6]은 이에 대한 상호인증기법들을 제안하였으나 태그의 익명성을 보장하지 못했다. 더욱이 대부분의 기법들이 익명성 보장을 위해 태그ID의 함수값을 전송하여, 서버는 최대 저장된 태그의 수만큼 함수값을 구하여 전송받은 값과 일치하는 값을 찾는 전수조사(Exhaustive Search) 과정이 불가피하였다. 따라서 최근 Chen 등[7]은 제곱근을

구하는 어려움에 기반을 둔 이차잉여를 이용하는 상호 인증기법을 제안하였다. Chen 등의 기법은 기존의 대부분의 기법들에서 불가피했던 전수조사를 없앴다. 하지만 인증 시 리더가 악의적으로 같은 값을 보내게 되는 경우 태그의 위치추적의 문제가 발생한다. 또한 제한된 연산능력을 가진 저가형 태그에서 해쉬함수와 제곱연산을 동시에 연산하여 효율성에 문제가 발생한다.

따라서 본 논문에서는 Chen 등의 기법의 안전성과 효율성을 분석하고, 태그 또한 인증 시마다 랜덤 값을 생성하게 함으로써 위치추적의 문제를 해결한 기법을 제안한다. 제안된 기법은 제곱연산만을 사용하여 효율적이며 서버의 전수조사 없이도 태그 인증이 가능하다. 또한 비밀값의 갱신 없이도 전방향안전성을 만족하며 리더와 태그사이의 전송되는 정보량을 감소시켜 통신측면에서의 효율성 또한 증가시켰다.

본 논문의 구성 2장에서는 제안하는 기법에 대한 배경지식을 제시하고, 3장에서는 Chen 등 기법을 살펴본 후 이 기법의 효율성과 안전성을 분석한다. 4장에서는 Chen 등 기법을 효율성과 안전성 측면에서 개선한 새로운 기법을 제안하고 5장에서는 제안된 기법을 분석한다. 마지막으로 6장에 결론을 맺는다.

2. 배경 지식

이 장에서는 앞으로 제안할 기법에 대한 기본 지식을 제시한다.

2.1 RFID 시스템의 안전성을 위해 고려할 사항

RFID 시스템의 보안 및 프라이버시 보호를 강화하기 위해 반드시 다음과 같은 사항을 고려해야 한다. 여기서 리더와 서버 사이의 통신은 안전한 채널을 통해서 이루어진다고 가정하여 다루지 않는다.

2.1.1 프라이버시강화를 위한 요구사항

- 태그의 익명성(Tag anonymity): 태그의 ID는 태그와 리더사이의 통신에서 노출되어서는 안 된다.
- 위치정보와 태그사이의 비연결성(Individual location privacy): 태그와 리더사이에 발생하는 통신내용이 각 세션마다 태그의 ID와 독립적이어야 한다. 만약 공격자가 특정한 태그와의 통신내용을 식별하게 되면, 태그의 위치가 추적되어 프라이버시 문제가 발생한다.
- 전방향 안전성(Forward secrecy): 어느 시점에 공격자가 태그 내의 정보를 알게 되더라도, 이전의 태그를 지닌 소유주의 경로나 위치에 대한 정보를 얻을 수 없어야 한다.

2.1.2 시스템 보안 공격 유형

- 재생공격(Replay attack): 태그와 리더사이에 발생한 세션정보를 재전송함으로 유효한 인증을 발생시키는 공격을 말한다.
- 서비스거부공격(DOS attack): 공격자가 태그와 서버 사이에 전송되는 메시지를 막거나, 위조된 메시지를 태그에 전송하여, 태그와 서버사이의 정상적인 인증이 일어나지 못하도록 막는 공격이다.
- 공격자 중간 공격(Man-in-the-middle attack): 공격자가 태그와 리더 사이의 세션정보를 태그와 리더는 공격당하고 있는 사실을 모르게 가로채거나 관찰할 수 있는 공격이다.

2.2 이차잉여

서로 다른 두 큰 소수 $p, q(\in Z_n)$에 대하여 $n=pq$라 하자. 만약 $y=x^2 \bmod n$이 해를 갖는다면, 즉 y의 제곱근이 존재하면, y를 $\bmod n$에 대한 이차잉여라고 한다. 이 때 $y=x^2 \bmod n$을 만족하는 x를 찾는 것은 p, q에 대한 정보 없이는 n을 인수분해하는 어려움과 동일하다.

3. Chen 등의 기법

2008년 Chen 등[7]은 제곱근을 구하는 어려움에 기반을 둔 이차잉여를 이용한 상호인증 기법을 제안하였다. Chen 등의 기법은 태그를 식별하기 위한 전수조사를 하지 않는 장점을 가지고 있다. 하지만 리더가 악의적으로 같은 값을 보내게 되는 경우 태그의 위치가 추적가능하고, 제한된 능력을 가진 저가태그에서 해쉬함수와 제곱연산을 함께 연산하는 어려움이 발생한다.

3.1 Chen 등의 기법

Chen 등의 기법은 초기설정 단계와 인증 단계인 두 단계로 이루어져있다.

[초기설정 단계]

서버는 두 개의 큰 소수 p, q를 생성하고, $n=pq$를 계산한다. $h()$는 일방향 해쉬함수이고 $PRNG()$는 의사난수 생성기라고 할 때, $n, PRNG(), h()$는 공개된다. 서버는 태그의 메모리에 $TID, h(TID), r$을 입력한다. 이 때 TID는 태그의 ID를 나타내고 $r(\in Z_n)$은 난수를 나타낸다. 서버는 각각의 태그에 해당하는 $TID, h(TID), r, r_{old}$ 값을 데이터베이스에 저장해준다(처음 $r=r_{old}$이고, $h(TID)$ 값은 나중에 서버에서 태그를 찾기 위한 값으로 사용된다.).

[인증단계]

인증과정은 그림 1과 같다.

step 1. 리더는 임의로 $s(\in Z_n)$값을 선택하고 $hello$메시지와 s를 같이 브로드캐스트한다.

step 2. 태그는 리더로부터 받은 s값과 $TID, h(TID), r$를 이용하여 $X, R, h(x), h(r)$를 계산하여 보낸다.

$x=h(TID)\oplus r\oplus s$
$X=x^2 \bmod n$
$R=r^2 \bmod n$

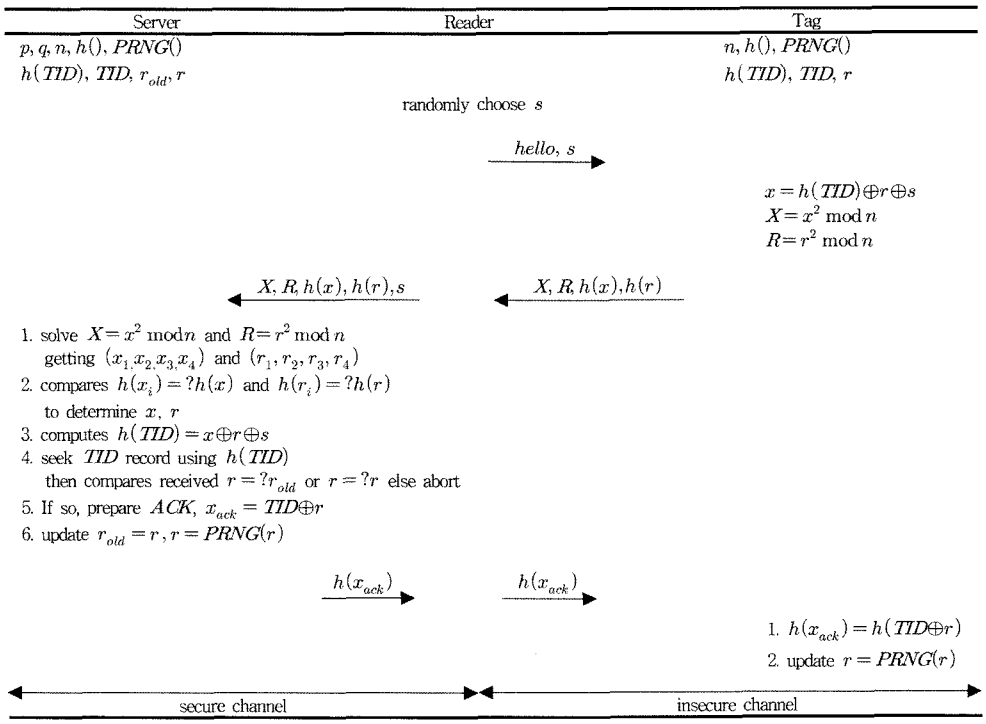

그림 1 Chen 등의 기법

step 3. 리더는 태그로부터 받은 $X, R, h(x), h(r)$과 처음 태그에게 보냈던 s값을 서버에게 보낸다.

step 4. 서버는 리더가 보낸 $X, R, h(x), h(r), s$을 통해 X, R의 제곱근 $(x_1, x_2, x_3, x_4), (r_1, r_2, r_3, r_4)$을 계산한다. 각 $x_i, r_i (1 \le i \le 4)$의 해쉬값 계산하여 $h(x), h(r)$과 비교, 정당한 x, r을 구한 뒤 $h(TID) = x \oplus r \oplus s \oplus$를 계산한다. 이후 $h(TID)$값을 이용하여 TID를 찾고 r값의 유효성을 점검한다. 유효할 경우 $h(x_{ack} = TID \oplus r)$를 계산하여 전송한다. 그 후 $PRNG(r)$을 계산하여 r값을 갱신한다.

step 5. 리더는 받은 메시지를 태그에게 전달하고 태그는 $h(x_{ack}) = h(TID \oplus r)$을 확인하고 서버를 인증한다. 인증이 성공한 경우, 태그도 $PRNG(r)$을 계산하여 r값을 갱신한다.

3.2 Chen 등의 기법 취약성

Chen 등의 기법은 태그의 프라이버시를 위해 태그 ID의 해쉬함수값을 사용하므로 태그의 익명성을 만족하며, 전수조사 없이 태그의 식별이 가능하다. 또한 인증절차가 끝날 뒤 r값을 갱신하여 전방향안전성을 만족하고, 이차잉여의 어려움에 의해, 재생공격, 서비스거부공격, 공격자중간공격에 안전하다. 하지만 악의적인 리더가 같은 랜덤값 s을 보내는 경우, 위치추적의 문제와 제한된 능력을 가진 저가태그에서 해쉬함수와 제곱연산을 동시에 연산해야 하는 어려움이 있다.

- 위치추적의 문제: r값이 갱신되기 전까지 악의적인 리더가 계속 같은 s를 보내게 되는 경우 태그가 계산하여 보내는 값 $X, R, h(x), h(r)$이 매 요청마다 같아짐으로 TID값을 알 수는 없지만 특정 태그와 전송되는 값 사이에 연결성이 생기게 된다.
- 계산적 비효율성 문제: 저가태그의 경우, 한정적인 연산만이 수행가능하다. Chen 등의 기법은 안전한 인증을 위해 세 번의 $h()$와 두 번의 모듈러 제곱계산을 수행해야 한다. 하지만 저가태그의 제한적인 연산능력 때문에 두 연산을 함께 연산하기에는 무리가 따른다.

4. 제안된 기법

본 절에서는 제곱연산만을 사용하는 저가태그에서 효율적으로 수행 가능한 개선된 이차잉여기반의 상호인증 기법을 제안한다. 제안되는 기법은 전방향안전성을 위해 중앙서버에서 r값을 갱신하지 않으며, 태그를 식별하기 위해 전수조사 또한 실시하지 않는다. 또한 Chen 등[7]의 기법에 드러난 위치추적의 문제를 태그 또한 매 인증 시마다 새로운 랜덤한 값을 생성하는 방법으로 해결하였다.

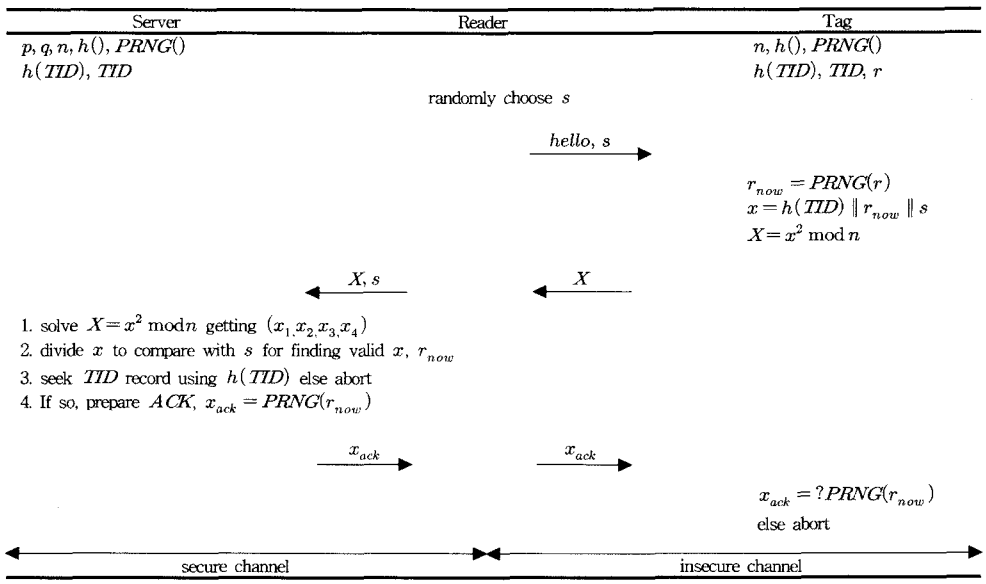

그림 2 제안된 기법

4.1 제안된 기법

제안하는 기법은 초기 설정 단계, 인증단계인 두 단계로 구성되어 있다.

[초기설정단계]

서버는 두 개의 큰 소수 $p, q(\in Z_n)$를 생성하고, $n=pq$를 계산한다. $n, PRNG(), h()$는 공개하고, 서버는 태그의 메모리에 $TID, h(TID), r$을 입력한다. 반면 서버도 $TID, h(TID)$값을 데이터베이스에 저장해준다(여기서 $h(TID)$값은 나중에 서버에서 태그를 찾기 위한 값으로 사용된다.).

[인증단계]

인증단계는 그림 2와 같다.

step 1. 리더는 임의로 $s(\in Z_n)$값을 선택하고 *hello*메시지와 s를 같이 브로드캐스트한다.

step 2. 태그는 리더로부터 받은 s값과 태그에 저장되어있던 $TID, h(TID), r$를 이용하여 다음과 같이 $X, h(x)$를 계산하여 리더에게 보낸다.

$r_{now} = PRNG(r)$
$x = h(TID) \| r_{now} \| s$
$X = x^2 \bmod n$

여기서 사용되는 r_{now}는 태그가 매 세션마다 새롭게 생성하는 값으로 위치추적을 막는 역할을 한다.

step 3. 리더는 태그로부터 받은 X과 처음 태그에게 보냈던 s값과 함께 서버에게 보낸다.

step 4. 서버는 리더가 보낸 X, s을 통해 X의 제곱근 (x_1, x_2, x_3, x_4)을 계산한다. 각 $x_i (1 \le i \le 4)$를 분해하여 s값이 나오는 유효한 x을 찾고, r_{now}을 구한다. 서버는 $h(TID)$값을 이용하여 TID를 찾고 인증을 한다.

step 5.[1] 인증 후에 서버는 $x_{ack} = PRNG(r_{now})$ 계산하여 리더에게 전송한다.

step 6. 리더는 받은 메시지를 태그에게 전달한다. 태그는 $x_{ack} = ?PRNG(r_{now})$을 확인하고 서버를 인증한다.

5. 제안된 기법의 안전성 및 효율성 분석

제안된 기법은 태그 또한 세션마다 $PRNG(r)$를 통해 랜덤한 값을 생성하여 위치추적의 문제를 해결하였다. 또한 서버에서 r값을 갱신하는 부분을 생략하여 동기화 과정을 줄이면서 여전히 전방향안전성을 만족한다(표 1). 무엇보다도 해쉬함수와 제곱연산을 모두 사용하던 Chen 등[7]의 기법과 달리 제안된 기법은 제곱연산만을 사용하여 보다 효율적이다.

5.1 제안된 기법의 안전성 분석

- 태그의 익명성: 태그의 TID값을 보내는 것이 아니라 일방향 해쉬함수 $h()$를 이용해 $h(TID)$값을 보내어 태그의 익명성이 보장된다. 만약 X, s를 통해 $h(TID)$를 구하려고 할 때, 비밀값 p, q를 모르므로 X의 제곱근을 구할 수 없어 이 또한 태그의 익명성을 보장한다.
- 위치정보와 태그사이의 비연결성: 태그 또한 랜덤 값을 $PRNG()$를 통해 생성하므로, 리더가 악의적으로 같은

1) 상호인증이 불필요한 경우에는 즉, 단방향 인증이 요구되는 환경에서는 step 5부터는 생략하여 사용 가능하다.

s값을 보낸다고해도 태그의 랜덤값으로 인해 매번 다른 값이 계산되어 어떤 연결성도 존재하지 않는다.

- 전방향안전성: 각 인증세션마다 새롭게 s, r_{now}이 생성됨으로, 어떤 시점에서 공격자가 태그내의 정보를 알게 되어도, 노출된 정보로 이전의 태그 소유자의 경로를 추적하거나 이전의 위치정보를 얻을 수 없다.
- 재생공격: 매 세션마다 생성되는 s, r_{now}에 의해서 전송되는 정보가 다르게 되어 공격자가 재전송하여도 전송된 X를 나누어 구한 r_{now}이 유효하지 않아 공격에 실패하게 된다.
- 서비스거부공격: 매 인증을 위해 s, r_{now}가 독립적으로 생성되므로 다음 인증에 영향을 미치지 않는다. 따라서 서비스거부 공격 이후에도 태그와 서버사이에 정상적인 인증이 일어나게 된다.
- 공격자중간공격: 공격자가 세션정보를 가로채거나 관찰할 수 있으나 서버가 가진 비밀값 p,q값을 모르고는 인증에 필요한 유효한 값을 계산할 수 없다.

표 1 제안된 기법과 기존의 기법들의 안전성 비교

기 법	P1	P2	P3	A1	A2	A3	M	B
Weis 등[6]	X	X	X	X	O	X	X	O
Ohkudo [5]	O	O	O	X	X	X	X	O
Yang 등[3,4]	X	X	X	O	O	O	X	X
Molnar 등[2]	O	O	X	O	O	O	O	O
Chen 등[7]	O	X	O	O	O	O	O	X
Proposed	O	O	O	O	O	O	O	X

(P1:태그의 익명성, P2:위치정보와 태그사이의 비연결성, P3:전방향안전성, A1:재생공격, A2:서비스거부공격, A3:공격자 중간 공격, M: 상호인증, B: 전수조사)

5.2 제안된 기법의 효율성 분석

제안된 기법을 태그, 서버, 통신량의 경우로 나누어 분석하였다[표 2].

- 태그의 경우: 제안된 기법에서는 단 한 번의 제곱연산만을 사용하므로 Chen 등의 기법에 비해 효율적이다.
- 서버의 경우: 태그에 비해 뛰어난 능력을 가지고 있으나, Chen 등의 기법은 9번의 해쉬함수 계산과 2번의 제곱근을 구하는 연산을 수행해야한다. 하지만 제안된 기법에서는 단 한 번의 제곱근 연산만을 수행함으로 계산적인 효율성이 증가한다. 또한 태그식별을 위해 전수조사없이 $h(TID)$를 이용해 태그를 찾을 수 있다.
- 통신량의 경우: Chen 등의 경우 $X, R, h(r), h(r)$를 전송하지만 제안된 기법에서는 오직 X만을 전송하므로 통신량이 절반이상 감소하게 된다.

6. 결 론

최근 Chen 등은 제곱근을 구하는 어려움에 기반을 둔 이차잉여를 이용하는 상호인증기법을 제안하였다. 그러나 Chen 등의 기법은 태그의 위치추적의 문제와 해쉬함수와 제곱연산을 함께 사용하여 저가태그에 많은 연산량을 요구하는 문제가 발생한다. 따라서 본 논문에서는 Chen 등의 기법에 대한 안전성과 효율성을 분석하고, 전수조사 없이 제곱연산만을 사용하여 저가태그를 위한 보다 효율적인 이차잉여기반의 상호인증 기법을 제안하였다. 또한 r값을 갱신하지 않고도 전방향안전성(Forward secrecy)을 만족하며, 위치추적의 문제를 해결하는 기법을 제안하였다.

표 2 제안된 기법과 기존의 기법들의 효율성 비교

기 법	태그의 연산량	서버의 연산량
Weis 등[6] randomized hash-locking	1 hash/PRF	n hash/PRF 전수조사
Ohkudo 등[5]	2 hash	$n(i+1)$ 전수조사
Yang 등 [3,4]	2 hash	$2n$ hash 전수조사
Molnar 등[2]	2 PRF	$n+1$PRF 전수조사
Chen 등[7]	3 hash, 2 squaring	9 hash, 2 squaring root solving
Proposed	1 squaring	1 squaring root solving

참 고 문 헌

[1] S.A. Weis, S.E. Sarma, R.L.Rivest, D.W.Engels, Security and privacy aspects of low-cost radio frequency identification systems, Security in Pervasive Computing 2003. LNCS No.2802, pp. 201-212, 2004.

[2] M. Ohkudo, K. Suzki, S. Kinoshita, Cryptographic approach to privacy-friendly tags, RFID Privacy Workshop, 2003.

[3] J. Yang, J. Park, H. Lee, K. Kim, Mutual authentication protocol for low-cost RFID, Handout of the Encrypt Workshop on RFID and Lightweight Crypto, 2005.

[4] J. Yang, K. Ren, K. Kim, Security and privacy on authentication protocol for low-cost radio, the 2005 Symposium on Cryptography and Information Security, 2005.

[5] CC Tan, B Sheng, Q Li, Serverless search and authentication protocols for RFID, IEEE PerCom, 2007.

[6] D. Molnar, D. Wagner, Privacy and security in library RFID: issues, practices, and architectures, Conference on Computer and Communications Security CCS'04, pp. 210-219, 2004.

[7] Y. Chen, J. Chou, H. Sun, A novel mutual authentication scheme based on quadratic residues for RFID systems, computer networks 52, pp. 2373-2380, 2008.