Shift연산과 경량 연산자를 사용한 저비용 RFID 인증프로토콜

안효범* · 이수연**

요 약

유비쿼터스 환경에서 개인 프라이버시 보호를 위해 RFID 시스템 보안에 대한 연구가 활발히 이루어지고 있다. RFID 시스템 보안 중 XOR 기반의 기법은 다른 기법보다 단순하고 최저가로 구현될 수 있다. 그러나 사용자 프라이버시 보호를 위하여 동일한 비밀정보가 사용자 인증에 사용되기 때문에 비밀정보가 노출될 확률이 커진다. 따라서 본 논문에서는 기존의 XOR 기반 인증프로토콜을 개선한 경량화 된 연산자와 순환 시프트 연산을 사용한 인증프로토콜을 제안한다.

RFID Authentication Protocol Using Shift Operation and Light-weight Operations

Hyo Beom Ahn* · Su Youn Lee**

ABSTRACT

In ubiquitous environment the authentication protocol design for RFID security is studied to protect user privacy in RFID system. The XOR-based approach of RFID security is implemented inexpensively and simply. However because of using same security informations, ones of tag is disclosed easily. In this paper, we enhance the previous XOR-based authentication protocol using a circular shift operation.

Key words : RFID, Light-weight Operations, Authentication

* 공주대학교 정보통신학부
** 백석문화대학 컴퓨터정보학부

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 무선환경에서 제공하는 보안 프로토콜은 RFID 태그가 낮은 가격으로 공급되어져야하기 때문에 적합하지 않다. 이에 자원의 소모가 적으면서도 안전한 암호 알고리즘의 개발과 함께 최소의 자원을 사용하면서도 안전한 프로토콜의 개발이 필수적이다[1].

지금까지 제안된 해쉬 기반과 재암호화 기반의 대부분 인증프로토콜은 XOR 기반의 인증프로토콜보다 더 많은 안정성을 제공하지만 RFID 태그에 하드웨어적인 제약사항을 만족 시키지 못했다. 따라서 본 논문에서는 XOR 기반의 인증프로토콜에서 태그와 리더 간에 쌍방향 인증을 위해 최소의 자원을 활용하면서 사용자의 프라이버시 공격을 방지할 수 있는 shift연산자 기반의 저비용 RFID 인증프로토콜을 제안하고자 한다.

본 논문의 구성은 다음과 같다. 먼저 제 2장에서는 지금까지 연구된 RFID 인증프로토콜의 여러 기법들을 설명하고, 제 3장에서는 제안 된 인증프로토콜에 대해 구체적으로 설명하고 제 4장에서는 제안된 인증프로토콜과 기존의 인증프로토콜을 비교 · 분석한다. 마지막으로 제 5장에서는 결론을 맺는다.

2. 기존의 RFID 인증프로토콜

RFID 시스템에서는 리더를 소유한 공격자는 물리적인 접촉없이 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 인증프로토콜이 제안되었다. 본 절에서는 지금까지 제안된 사용자 프라이버시를 해결하기 위한 인증프로토콜을 살펴보고자 한다. 인증 프로토콜 접근 방식에 따라 3가지로 분류 할 수 있다.

2.1 해쉬 기반

해쉬 기반 기법은 해쉬 함수의 일방향성(One way property)을 이용하여 태그의 정보를 보호하는 기법이다. 그러나 RFID 시스템에서는 공격자가 리더와 태그의 통신을 도청하기 쉽기 때문에 채널에서 얻은 정보를 이용하여 재사용 공격과 스푸핑 공격을 수행할 수 있다.

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

이를 보완하기 위해 랜덤 접근 기법(RHLK)이 제안되었다. 태그는 메타 ID뿐만 아니라 난수 R과 자신의 임의의 여러 개의 ID 중에서 ID_k를 사용하여 생성한 $h(ID_k \| R)$을 리더에게 전송한다. 개선된 기법에서 태그는 임의의 난수를 사용하기 때문에 위치추적이 불가능하다.

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. 이 기법에서는 리더의 질의에 대해 태그는 매번 다른 응답을 하므로 공격자는 태그의 이동경로를 파악할 수 없게 된다. 또한, 그 세션에서 해쉬 함수의 값이 노출되더라도 해쉬 함수의 일방향 성질에 의해서 이전의 세션에 대한 정보를 얻을 수 없다. 이러한 성질로 인해 사용자의 프라이버시를 보호할 뿐만 아니라 사용자의 위치 정보를 보호할 수 있다. 그러나 이 기법에서는 데이터베이스의 해쉬 연산량이 태그의 수에 비례한다는 취약점을 갖는다.

2.2 재 암호화 기반

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.

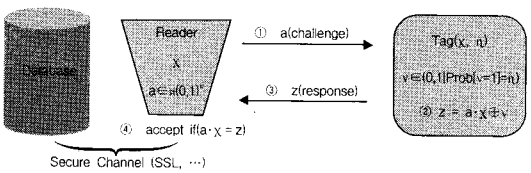
Satio 등에 의해서 제안 기법[6]인 Universal 재 암호 기법은 재 암호화 과정이 일어날 때 공개키 없이 임의의 랜덤값을 사용하여 재 암호화가 이루어지는 기법이다. 그러나 태그의 정보에 재 암호화 과정이 여러 번 일어나더라고 단 한 번의 복호화 과정으로 원래의 메시지를 복원할 수 있다.

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 XOR 기반

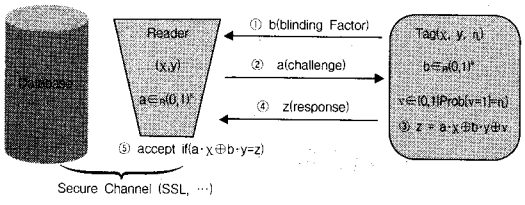
해쉬 기반과 재 암호화 기반의 기법들은 최소한의 연산만을 수행하는 태그가 사용되는 환경에 적용하기에는 적합하지 않다. XOR 기반의 기법은 해쉬 기반의 기법보다 더 단순한 비트 연산을 사용하여 RFID의 프라이버시를 보호하는 기법으로 최저가의 RFID태그에 적용 가능한 기법이다. 따라서, 본 논문에서 제안한 저비용 RFID 인증프로토콜은 XOR 기반으로 개발된 프로토콜이다.

Juels는 사용자의 프라이버시를 보호하며 최소한의 암호학적 함수를 사용하는 기법을 제안하였다[8]. 제안된 기법은 간단한 비트 연산인 XOR연산을 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(그림 1).



(그림 1) HB 프로토콜

이 기법은 수동적인 공격자에 대해서 안전할 수 있으나 공격자가 a값을 자신에게 유리하게 선택하여 리더에게 전송한다면 응답 값 z에서 x에 대한 값을 알아낼 수 있다.



(그림 2) HB$^+$ 프로토콜

따라서 Juels는 능동적인 공격에 안전한 HB^+ 기법을 제안하였다[10]. (그림 2) 이 기법은 리더와 태그 간에 추가적으로 y라는 비밀값을 서로 저장하고 이전 기법과 달리 b라는 임의의 값을 태그가 전송하는 기법이다.

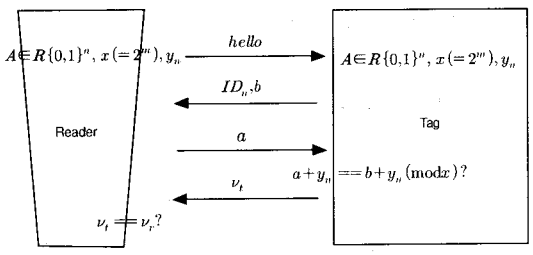
하지만 제안된 기법은 1비트의 값으로 태그를 인증하는 것이기 때문에 그를 관리하는 환경에서는 오류 발생의 확률이 많다. 그러므로 다수의 태그 정보를 다루는 환경에서 사용하기에는 부적합하며 이 기법은 안전성 측면에서 취약성을 갖는다[10].

또한, Lopez에 의해서 LMAP와 M^2AP이 제안되었는데, 이 방법은 비트연산인 XOR와 AND 그리고 덧셈 mod 2^m을 사용한다[11, 12]. 제안된 방법은 상호인증을 제공하고 위치추적공격을 막을 수 있지만, 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 동기화에 대한 공격(de-synchronization attack)과 완전노출공격(full Disclosure attack)에 취약점이 있다는 것을 분석하였고, 이에 대한 대안으로 재동기화(re-synchronization)를 제시하였으나 하나의 태그에 대한 많은 상태 정보를 저장해야하는 문제를 갖게 된다. 그러한 이유로 유비쿼터스 환경에서는 이러한 상태저장 프로토콜(stateful protocol)이 적당치 않음을 보여준다.

즉, 유비쿼터스 환경 같은 많은 태그들이 필요한 환경에서는 XOR과 같은 간단한 연산을 사용하면서 상태정보의 저장이 필요 없이 상호인증과 태그에 대한 공격을 막을 수 있는 프로토콜이 요구된다. 이에 간단한 상태 정보를 저장하고, 경량화된 연산을 사용하는 프로토콜이 필요하다.

3. 제안된 인증프로토콜

사용자의 프라이버시를 보호할 수 있는 인증 프로토콜은 식별정보가 직접 전송되지 않고 매 세션마다 전송되는 인증 정보를 변경하여 위치 추적이나 트래픽 분석 공격에 대한 안전성을 해공해야 한다. 제안 기법은 비밀정보를 이용하여 매 세션마다 다른 키(k)를 제공하도록 하여 한 세션에서 사용된 정보가 유출되더라도 다음 세션에 아무런 영향을 주지 않고 인증단계를 수행할 수 있다. (그림 3)은 제안 프로토콜의 상호 인증 단계이다.



(그림 3) 제안된 인증프로토콜의 상호인증 단계

3.1 태그와 리더의 상호인증

제안된 인증프로토콜은 n비트의 비밀정보(A), $x(=2^m)$를 공유하고, 이전에 사용된 매 세션마다 변경되는 y_n을 저장한 상태에서 인증프로토콜을 수행한다. 이 방법에서 사용된 연산자는 XOR($\oplus$)와 AND($\wedge$) 그리고 mod 2^m(+)을 사용한다.

단계 1 : 리더는 태그에게 hello 메시지를 보낸다.

단계 2 : 태그는 리더에게 자신의 ID_n과 랜덤 값 b를 선택하여 전송한다.

단계 3 : 리더는 태그로부터 받은 b를 이용하여 식 (1)이 만족되도록 a를 생성하여 태그에게 보낸다.

$$a+y_n = b+y_n \quad (1)$$

단계 4 : (리더의 인증)
a를 받은 태그는 식 (1)에 의해서 $a = b \pmod{x}$의 관계가 성립하는지를 검사하여 리더(reader)인지를 확인한다.

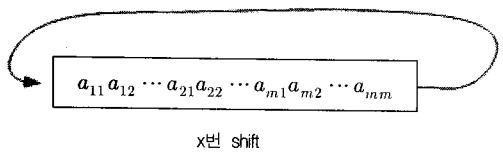
단계 5 : (태그의 인증)

태그는 자신을 인증받기 위하여, 식 (2)와 같이 리더가 보내온 a를 사용하여 y_{n+1}과 K를 계산한다. K는 식 (3)과 같이 비밀 정보 A와 y_{n+1}에서 하위 비트 r비트를 취하여 순환자리이동(cyclic shift)을 통해 얻어진다.

$$y_{n+1} = a + y_n \tag{2}$$

$$K = shift(A, [y_{n+1}]_r) \tag{3}$$

여기서 shift 연산은 A를 $[y_{n+1}]_r$번 순환자리 이동을 시킨다.



(그림 4) 순환자리 이동

구해진 K는 태그를 인증하기 위한 인증자를 생성하기위해 사용된다. 인증자 v는 식 (4)와 같다.

$$v_t = (b + y_n) \wedge (a + y_n) \oplus K \tag{4}$$

생성된 v_t는 태그의 인증을 위하여 리더에게 전송한다.

단계 6 : 리더는 식 (2)와 비슷하게 태그로부터 전송된 b를 이용하여 식 (5)와 같이 y_{n+1}를 계산하고, 식 (3)과 같이 K를 계산하고 알고 있는 정보를 이용하여 같은 방법으로 식 (4)를 통해 리더는 v_r를 계산할 수 있다.

$$y_{n+1} = b + y_n \tag{5}$$

리더는 자신이 계산한 v_r와 v_t와 같다면 태그를 인증하게 된다.

3.2 추적성 피하기 위한 ID의 갱신

RFID 보안 프로토콜에서 상호인증과 같이 고려해야할 사항은 바로 태그의 ID를 통한 제 3자에 대한 추적성 공격을 피하는 것이다. 추적성을 피하기 위해서는 태그를 인식하기 위해 사용되는 식별자를 변경해야 하는데, 태그는 다음에 사용될 식별자 ID_{n+1}를 생성하기 위해, 상호인증과정에서 얻은 값 K, a, 그리고 y_n과 현재 사용하는 ID_n을 이용한다. 식 (6)은 태그가 식별자를 갱신하는 식을 보여준다.

$$\text{Tag} : ID_{n+1} = K \wedge (a + y_n) \oplus ID_n \tag{6}$$

또한, 리더도 같은 방법으로 얻어진 정보를 이용하여 식 (7)처럼 태그의 식별자를 갱신한다.

$$\text{Reader} : ID_{n+1} = K \wedge (b + y_n) \oplus ID_n (\mathrm{mod} x) \tag{7}$$

식 (6)과 식 (7)에서 사용된 $b + y_n = a + y_n = y_{n+1}$으로 이미 식 (2)와 식 (5)에서 계산되어 다시 계산할 필요는 없다.

3.3 ID의 복구

갱신과정 중 태그와 리더간의 통신의 실패로 갱신정보의 비동기화가 발생할 수 있다. 비동기화는 리더와 태그가 서로 다른 비밀정보를 갖게 되어 이후 통신에서 이를 올바른 비밀정도를 갖도록 서로 동기화 하는 과정이 요구된다. [12]에서는 동기화 작업을 실시하기 위해 데이터베이스에 이전의 모든 비밀정보를 저장하는 대안을 제시하였는데, 이는 리더와 태그에게 많은 오버헤드의 발생을 요구한다. 제안된 상호 인증프로토콜에서는 이를 좀 더 효율적으로 처리하기 위하여 저장 공간에 대한 부하를 줄일 수 있는 동기화 과정을 가질 수 있다.

비동기화는 두 가지 경우가 발생할 수 있다. 즉, 태그에서 갱신을 하지 않았을 경우와 리더가 정보를 갱신하지 않았을 경우로 나누어 볼 수 있다. 그러나 리더에서는 인증 작업이 끝나야 ID를 갱신하

게 됨으로 복구과정이 요구되지 않는다.

태그의 경우에는 전사적 공격(brute-force attack)에 의해서 비동기화가 발생할 수 있다. 이때, 다음번 정당한 리더와의 통신 때 자신의 이전 ID를 복구함으로써 태그와의 동기화 작업을 할 수 있다.

ID복구의 전제 조건 중에 태그는 이전 과정에서 사용한 K를 저장하여 식 (8)을 수행해야 한다.

$$ID_n = K \wedge y_n \oplus ID_{n-1} \quad (8)$$

태그는 자신의 비밀정보의 갱신으로 인하여 리더와 비동기가 일어나면, 자신의 이전 정보를 현재 저장된 ID_n을 통해 ID_{n-1}을 다음과 같이 유도해 낼 수 있다.

$$ID_{n-1} = ID_n \oplus (K \wedge y_n) \quad (9)$$

이렇게 유도된 이전의 ID_{n-1}을 이용하여 리더와 상호인증을 통해 새로운 ID를 재발급 받으면 된다.

4. 제안된 인증프로토콜의 분석

본 장에서는 제안된 인증프로토콜을 기존 XOR 기반의 HB[9]와 HB$^+$[10] 그리고 단순한 비트위주 연산을 사용하는 M^{2}AP 인증프로토콜과 안정성과 효율성 측면에서 비교 · 분석하였다.

4.1 안정성

안정성에서는 태그와 리더사이의 인증프로토콜에서 수행될 수 있는 공격방법을 분석하였다. 발생할 수 있는 공격은 <표 1>에서 보는 것과 같이 트래픽 분석, 재전송 공격, 스푸핑 공격, 위치추적 공격, 비동기 공격을 대상으로 하여 분석하였다.

트래픽 분석은 소극적인 형태의 공격으로 공격자는 도청한 내용 혹은 태그에게 질의를 하여 얻은 응답을 분석하므로 공격에 활용하는 것이다. 그러나 제안된 프로토콜에서는 누가 질의를 했던 간에 태그는 매번 다른 ID를 사용하여 접속하기 때문에 공격자는 어떠한 정보도 얻을 수 없다.

〈표 1〉 안정성 비교 · 분석

구분	HB	HB$^+$	M^{2}AP	제안 프로토콜
트래픽 분석	×	×	○	○
재전송 공격	×	○	○	○
스푸핑 공격	×	○	○	○
위치추적 공격	×	×	○	○
비동기 공격	×	×	×	○
완전노출 공격	×	×	×	○

재전송 공격은 인증프로토콜 과정 중에 인터셉트된 교환정보를 재전송하여 태그와 리더로 가장할 있는 공격기회를 부여하는데, 제안 프로토콜에서는 태그와 리더를 인증하기 때문에 재전송공격은 무의미하게 된다.

위치추적은 태그의 ID가 바뀌지 않기 때문에 공격자로부터 태그의 위치가 노출되는 공격이다. 제안된 프로토콜에서는 매 세션마다 ID가 변경되기 때문에 공격자로부터 위치추적공격을 회피할 수 있다.

스푸핑 공격은 공격자가 리더를 속이기 위해 태그인척 또는 태그를 속이기 위해 리더인 척하는 공격이다. 제안된 프로토콜의 단계 3, 단계 4를 통해 쌍방 인증을 수행하고 공격자는 태그인 척하기 위해 y_{n+1}과 K를 계산해야 하는데 이는 비밀정보 A로부터 유도되므로 공격자는 이를 만들어 낼 수 없다.

M^{2}AP는 [13]에서의 분석에서처럼 비동기공격에 취약점을 가지고 있고, 이의 대안으로서 이전에 사용된 IDS를 데이터베이스에 저장하는 것이다. 그러나 제안된 인증프로토콜은 이전에 사용된 ID를 복구할 수 있기 때문에 이전에 사용된 IDS를 모두 저장하기 하지 않더라도 인증프로토콜 단계에서 인증이 되어야만 다음에 사용될 ID와 비밀정보 y_n을 저장하기 때문에 이를 필할 수 있고, 공격에 노출되더라도 이전 단계의 ID를 복구할 수 있기 때문에 비동기 공격을 능동적으로 방어 할 수 있다.

완전노출 공격은 공격자가 리더와 태그사이에

서 공격을 수행하는 형태로 리더에 대한 초기 인증작업이 없기 때문에 태그로부터 받은 IDS를 이용하여 리더에게 그 정보를 보내고 키를 얻어낼 수 있다. 그러나 제안 프로토콜은 초기 ID와 nonce를 발송하여 리더로부터 식 (1)과 같은 조건의 nonce를 리더가 보내주지 않는다면 이를 무시하기 때문에 더 이상 공격을 진행할 수가 없게 된다.

4.2 효율성

효율성의 평가는 각 인증방법에서 요구되는 연산자의 사용횟수를 통해 측정하였다. 비교에 사용된 연산자들을 보면 <표 2>와 같다.

〈표 2〉 인증프로토콜에서 사용된 연산

	XOR(⊕)	OR(∨)	AND(∧)	mod 2^m(+)
HB	○	×	×	×
HB^+	○	×	×	×
M^2AP	○	○	○	○
제안프로토콜	○	×	○	○

〈표 3〉 인증을 위한 연산자 계산량 비교

	HB	HB^+	M^2AP	제안 프로토콜
통신 오버헤드	1+r	2+r	2	3
XOR	r	2r	1	1
OR	-	-	2	-
AND	-	-	2	-
MOD	-	-	1	3

주) r : 라운드의 횟수를 의미한다.

HB는 인증을 하는데 사용되는 연산자는 한번의 XOR을 사용하고, HB^+는 2번의 XOR을 사용한다. 그러나 이 두 프로토콜의 특징은 여러 번의 라운드를 통해 지정한 오류허용한도를 측정하기 때문에 라운드만큼의 연산이 요구된다. 그러나 M^2AP와 제안된 프로토콜은 단 한번의 라운드를 사용한다. 이러한 이유 때문에 효율성의 측면에서 인증프로토콜에서 요구되는 통신오버헤드와 프로토콜에서 사용되는 연산자의 수를 나누어 측정하였다. <표 3>은 연산자의 계산량에 대한 비교를 보인다.

위의 계산량 분석에서는 HB와 HB^+에서는 태그를 인식하기 위한 과정이 생략되어 있기 때문에 다른 프로토콜에서도 이 부분의 통신 오버헤드는 제외시켰다. M^2AP과 제안 프로토콜의 총 연산자의 사용수는 8번과 6번으로 제안된 프로토콜의 연산의 수가 적음을 알 수 있다. 여기서 + 연산자는 2의 m승으로 모듈라 연산을 하는데 이 연산은 m비트가 나머지로 계산됨으로 다른 연산자와 수행시간의 차가 크지 않다.

5. 결 론

본 논문에서는 연산량이 적은 XOR 기반 RFID 인증프로토콜을 여러 공격으로부터 보호할 수 있는 새로운 방법을 제안하였고, 제안된 인증프로토콜에 대하여 HB와 HB^+, 그리고 M^2AP와 비교하였다. 제안된 프로토콜은 고정된 비밀정보와 매 세션마다 변경되는 비밀정보를 사용한다. 변경되는 비밀정보는 단순 논리 연산자와 순환이동연산(circular shift operator)를 사용하기 때문에 태그에 많은 부하를 주지 않도록 회로 구성이 가능하다. 또한, 비동기공격에 대하여 적은 노력으로 ID를 복구하여 태그와 리더의 정보를 동기화 할 수 있다는 장점을 가지고 있다. 향후에는 인증을 위해 교환되는 난수들에 대하여 더 많은 복잡도를 부여하여 제 3자로부터 공격을 보호하기 위한 연구와 RFID 환경에 적합한 경량화 된 인증프로토콜에 대한 연구가 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 '04, 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 SCN2004, Vol. 3352 LNCS, pp. 149-164, Sep. 2004.

[8] A. Jule, "Authentication Pervasive Devices with Human Protocols", To appear Crypto 2005, Aug 2005.

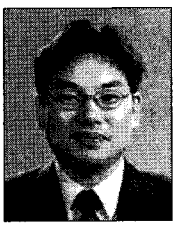
[9] A. Jule and R. Pappu, "Squealing euros: Privacy protection in RFID-enable banknote", In proceedings of Financial Cryptography-FC '03, Vol. 2742 LNCS, pp. 103-121, Sep. 2003.

[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, LM AP : 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/RFIDSec06/.

[12] P. Peris-Lopez, J. C. Hernandes-Castro, J. M. Estevez-Tapiador, and A. Ribagorda. M2 AP : 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.



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 교수

이 수 연

1990년 단국대학교 전산학과 학사
1993년 단국대학교 전산통계학과 석사
2003년 성균관대학교 전기전자 및 컴퓨터공학부 박사
1997년~현재 백석문화대학 컴퓨터정보학부 교수