# 해쉬락과 실시간을 이용한 RFID보안 인증 프로토콜

배우식*, 이원호, 한군희*
*백석대학교 정보통신학부
아주자동차대학
e-mail : bws@motor.ac.kr*, wheel@motor.ac.kr,
hankh@bu.ac.kr*

# RFID Security Authentication Protocol Using Hash Lock and Real Time

Woo-Sik Bae*, Won-Ho Lee, Kun-Hee Han*
*Division of Information & Communication Baekseok University
Ajou Motor College

요 약

RFID 시스템에서 태그와 리더사이의 통신은 무선을 통해 이루어짐에 따라 보안상 많은 취약점이 존재한다. 본 논문에서는 여러 보안 문제 중 프라이버시 보호를 위한 기존 기법의 취약점을 보완하여 태그가 리더로부터 수신한 난수로부터 매 세션마다 실시간으로 새로운 해쉬 함수를 생성하는 인증 프로토콜을 제안한다. 제안된 해쉬 기반 인증 프로토콜은 스푸핑 공격, 재전송 공격, 트래픽 분석 및 위치 추적 등의 공격에 대해 안전하며 연산을 최소화하여 다양한 적용성을 제공한다.

## 1. 서론

RFID(Radio Frequency Identification)는 앞으로 사용의 편리성향상으로 개인 및 산업 전반에 활용이 예상 되며 국내·외적으로 많은 연구가 진행 되고 있다. 그러나 마이크로칩에 내장된 정보를 무선주파수를 이용하여 읽어내기 때문에 RFID기술은 도청, 트래픽 분석, 서비스거부 공격, 메시지유실, 트래킹 공격, 스푸핑 공격 등 많은 취약점 들을 지니고 있어서 보안이나 프라이버시 보호문제에 심각한 문제를 야기할 수 있다. 따라서 RFID시스템이 활성화되기 위해서는 보안 문제에 대한 해결이 되어야 한다.

본 논문에서는 RFID의 프라이버시 문제를 해결하기 위한 기존 제안된 해쉬락(Hash-Lock)기법[1], 해쉬 체인(Hash Chain)기법[2], 해쉬기반 ID변형기법[3] 등이 해결하지 못한 문제점 분석을 통해 보다 안전하고 효율적으로 사용자의 프라이버시를 보호할 수 있는 인증 프로토콜을 제안 한다. 제안하는 프로토콜은 해쉬 함수 와 난수 및 실시간을 이용하여 공격자의 공격에 안전하고 실시간을 이용함으로써 추후 예상되는 불필요 태그의 산재된 공해로 시스템에 누적되는 부하문제를 줄여줄 수 있는 방식을 제안하며, 분산된 데이터베이스에서도 적용이 가능한 다양한 보안성 및 적용성을 제공하는 메커니즘을 제안하고자 한다.

## 2. 관련연구

### 2.1 해-쉬락 기법

태그의 식별 값인 MetaID가 고정되어 있으며 출력되는 데이터가 같아 전송 되었는지 확인할 수 있다. 그리고 리더기와 태그사이의 통신채널은 도청이 가능하여 공격자는 Key를 획득할 수 있다. [그림 1]은 해-쉬락 기법의 구조도 이다.

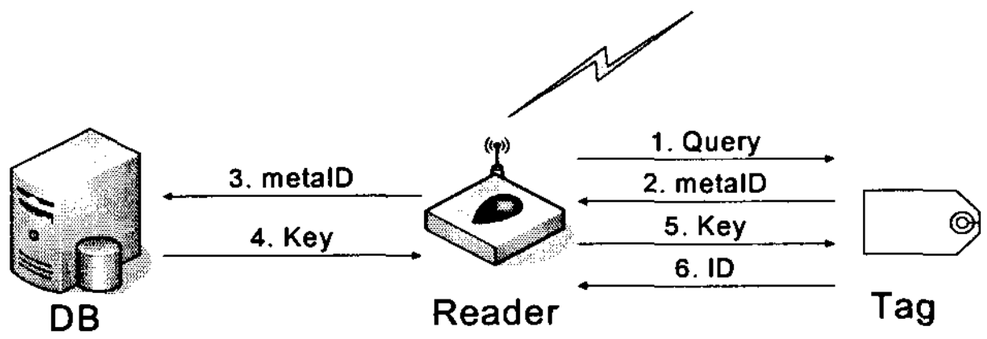


그림 1. 해쉬-락 기법

### 2.2 해쉬 체인 기법

서로 다른 두개의 해쉬 함수를 사용하는 해쉬 체인 기법[2]은 잘못된 응답이 수신 되었을 경우 데이터베이스는 고유한 모든 ID에 대해 ∞번의 해쉬를 수행할 가능성이 있으며 [그림 2]는 해쉬 체인 기법의 동작 과정 이다.

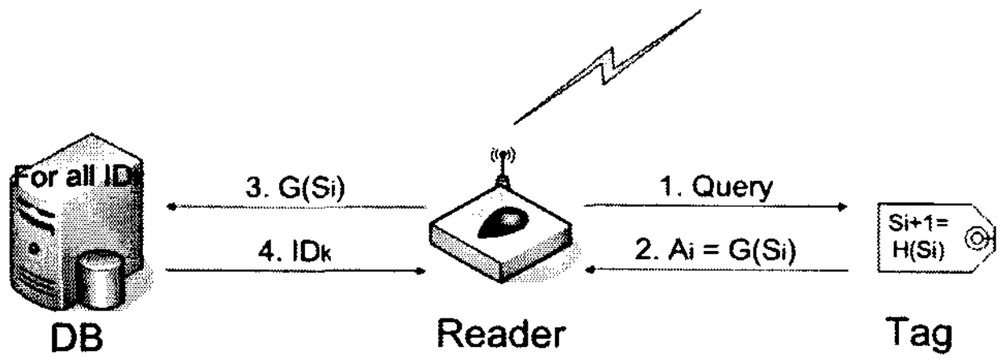


그림 2. 해쉬 체인 기법

### 2.3 해쉬 기반 ID변형 기법

[그림 3] 는 공격자가 정당한 리더로 가장해 태그로부터 H(ID), H(i⊕ID),Δi를 획득하고, 정당한 태그가 다음 인증세션을 수행하기 전에 이 정보들을 리더의 질의에 대한 응답으로 이용하면 공격자는 정당한 태그로 인정받을 수 있다.

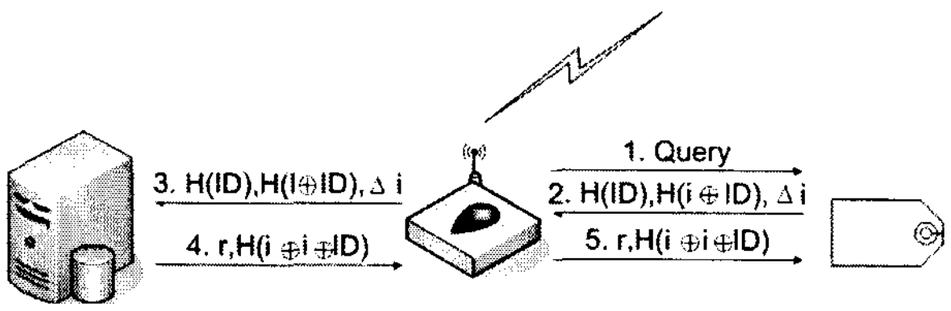


그림 3. 해쉬 기반 ID 변형 기법

## 3. 제안 프로토콜

### 3.1 구조

리더가 처음 태그에게 질의를 할 때 난수와 실시간을 함께 전송하고, 태그는 리더로부터 수신한 난수와 실시간을 자신이 가지고 있는 ID및 시간으로 해쉬한 값을 이용하여 응답하게 된다.

제안 프로토콜에서 사용되는 파라미터는 다음과 같으며, [그림 4]는 제안하는 프로토콜의 기본 구조를 나타낸 것이다.

[파라미터]

- Query : 질의, 태그의 응답을 요청
- ID : 태그 고유의 비밀 인증 정보
- H( ) : 일 방향 해쉬 함수
- $R_t$ : 리더가 태그에게 전송하는 DB시간(μs)
- $R_r$ : 리더가 생성하여 태그에게 전송하는 난수
- $T_t$ : 태그에 저장되어 있는 시간(μs)
- $R_{tn}$ : 태그에 기록될 시간(μs)
- $D_n$ : 데이터베이스에서 태그에게 전송되는 명령
- || : 연접(Concatenate function)

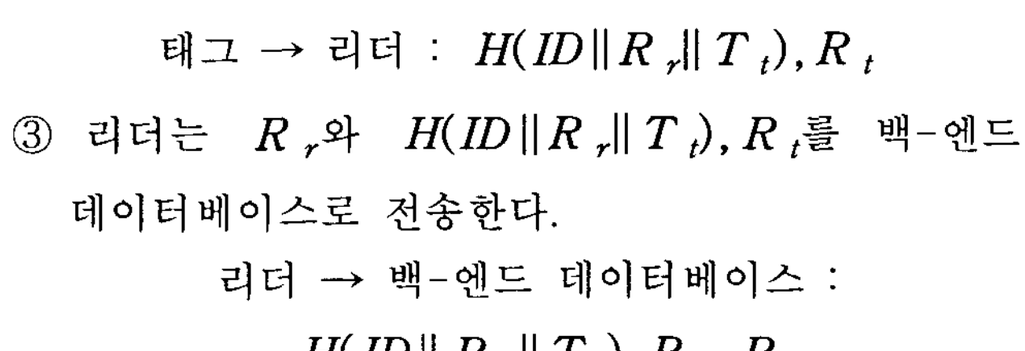


그림 4. 제안 프로토콜의 구조

### 3.2 인증과정

① 리더는 태그들에게 Query와 $R_t, R_r$를 함께 브로드캐스팅 한다.

리더 → 태그 : Query, $R_t, R_r$

② 태그는 ID와 자신이 가지고 있던 $T_t$를 $R_r$와 연접한 후 해쉬 하여, $R_t$와 함께 Query에 대한 응답으로 리더에게 전송한다.

태그 → 리더 : $H(ID \| R_r \| T_t), R_t$

③ 리더는 $R_r$와 $H(ID \| R_r \| T_t), R_t$를 백-엔드 데이터베이스로 전송한다.

리더 → 백-엔드 데이터베이스 :

$H(ID \| R_r \| T_t), R_r, R_t$

④ 백-엔드 데이터베이스에 저장된 ID를 $R_t, R_r$와 연접 하여 해쉬한 값과 리더로부터 수신한 $H(ID \| R_r \| T_t), R_r, R_t$를 비교하여 태그를 인증한다.

백-엔드 데이터베이스 → 리더 :

계산된 $H(ID \| R_r \| T_t), R_r, R_t$ =

수신한 $H(ID \| R_r \| T_t), R_r, R_t$

인증이 성공하면 $H(ID \| R_r \| T_t), R_{tn}, D_n$를 리더에게 전송한다.

⑤ 리더는 백-엔드 데이터베이스로부터 수신한 $H(ID \| R_r \| T_t), R_{tn}, D_n$를 태그에게 전송한다.

리더 → 태그 : $H(ID \| R_r \| T_t), R_{tn}, D_n$

태그는 자신의 ID와 인증 세션에서 생성한 $R_t$, $T_t$를 연접하여 해쉬한 값과 리더로부터 수신된 $H(ID \| R_r \| T_t), R_{tn}$를 확인하여 인증하고 $R_{tn}$을 기록하며 필요에 따라 $D_n$명령을 수행하고 인증세션을 성공적으로 종료 한다.

### 3.3 제안프로토콜의 안전성

#### 3.3.1 스푸핑 공격에 대한 안전성

공격자가 정당한 리더로 가장하여 Query, $R_r$, $R_t$를 전송하면, $H(ID \| R_r \| T_t), R_t$를 획득할 수 있으나 악의적인 태그에 넣어 응답으로 보내지게 되면 이미 시간이 지나간 상태의 정보 $H(ID \| R_r \| T_t), R_t$로는 인증을 할 수가 없어 스푸핑 공격이 불가능 하게 된다.

#### 3.3.2 재전송 공격에 대한 안전성

정당한 리더의 Query, $R_t$, $R_r$는 매 세션마다 변하기 때문에 $H(ID \| R_r \| T_t), R_t$도 매 세션마다 바뀌게 된다. 그러므로 공격자는 도청으로 획득한 $H(ID \| R_r \| T_t), R_t$를 다음 세션에서는 응답으로 사용할 수 없으므로 재전송 공격에 안전하다.

#### 3.3.3 트래픽 분석과 위치 추적에 대한 안전성

공격자가 Query, $R_t$, $R_r$를 태그에게 전송하여도 다음 세션에서는 실시간이 바뀌고 태그는 매 세션마다 변하는 응답 $H(ID \| R_r \| T_t), R_t$를 전송하므로 공격자는 트래픽 분석이 불가능 하고 태그의 위치도 추적할 방법이 없게 된다.

#### 3.3.4 정보전송 방해에 대한 안전성

제안 프로토콜은 상호 인증을 제공하므로 정보전송 방해 공격을 탐지할 수 있으며 [표 1]은 기존 프로토콜과의 안전성 비교표 이다.

**표 1. 제안프로토콜의 안전성**

| | 해쉬-락 기법 | 해쉬-체인 기법 | 해쉬기반 ID변형기법 | 제안프로토콜 |
|---|---|---|---|---|
| 스푸핑 공격 | 취약 | 취약 | 취약 | 안전 |
| 재전송 공격 | 취약 | 취약 | 안전 | 안전 |
| 트래픽 분석 공격 | 취약 | 안전 | 안전 | 안전 |
| 위치정보 노출 | 취약 | 안전 | 안전 | 안전 |
| 전송방해 공격 | 안전 | 안전 | 안전 | 안전 |

### 3.4 제안 프로토콜의 효율성

태그는 해쉬 함수 연산 및 실시간 데이터 저장만 하므로 저가 태그 및 모든 태그에서 구현 가능할 것이다. 또한 [표 2]와 같이 인증세션동안 해쉬함수 2회, 난수 1회의 연산만을 수행 하므로 연산 부담도 크지 않으며 적용이 가능하다.

**표 2. 제안프로토콜의 효율성**

| | 해쉬-락 기법 | 해쉬-체인 기법 | 해쉬기반 ID변형기법 | 제안프로토콜 |
|---|---|---|---|---|
| 인증 | 양방향 | 단방향 | 양방향 | 양방향 |
| 태그 연산량 | 해쉬1회 | 해쉬2회 | 해쉬3회 | 해쉬1회 |
| 리더 연산량 | - | - | - | 난수1회 |
| DB연산량 | - | n(1+i)회 | 해쉬3회 난수1회 | 해쉬1회 |

## 4. 결론

제안한 프로토콜은 태그가 리더로부터 수신한 난수 및 실시간으로부터 새로운 해쉬 함수를 생성하여 매 세션마다 다른 응답을 전송할 수 있도록 함으로써 공격자의 재전송 공격, 스푸핑 공격, 위치추적 등에 안전한 프로토콜로써 안전성과 효율성이 뛰어나다고 할 수 있다. 그리고 앞으로 신기술이 적용된 태그에도 실시간 데이터를 지속적으로 입력함으로 도처에 산재되어 있는 수많은 태그중 필요한 태그만 사용하고 오래되고 불필요한 태그들은 동작을 종료해 줌으로써 서버부담을 줄이고 추후 생길 불필요 태그를 처리할 수 있는 방법이 될 것으로 기대된다.

## 참고문헌


[1] S. Weis et al., "Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems," Security and Pervasive Computing 2003, LNCS2802, pp. 201-202.

[2] M. Ohkubo, K. Suzuki and S. Kinoshita, "Hash-Chain Based Forward-Secure Privacy Protection Scheme for Low-Cost RFID," Proceedings of the SCIS 2004, pp. 719-724, 2004.

[3] Gildas Avoine and Philippe Oechslin "RFID Traceability : A Multilayer Problem", Financial Cryptography, March 2005.