# 해시 체인 기법을 개선한 RFID 상호 인증 프로토콜

이강영, 송주석
연세대학교 컴퓨터과학과
e-mail : {gylee, jssong}@emerald.yonsei.ac.kr

# RFID Mutual Authentication Protocol of Improved Hash-chain Mechanism

Gang Young Lee, JooSeok Song
Dept. of Computer Science, Yonsei University

**요 약**

RFID 시스템은 장차 현재의 바코드 시스템을 대체할 수단으로 발전하고 있으며 점차 그 응용범위가 확대됨에 따라 개인정보 노출 등 보안요소에 대한 요구가 증대되고 있다. 지금까지 해시 기반의 인증기법과 재 암호화 기반의 인증기법이 소개되었으며 본 논문은 현재까지 소개된 인증기법에 존재하는 문제점을 지적하고 해시 기반의 인증기법에 기반하여 위치 추적, 재전송, 스푸핑 공격에 안전한 상호 인증 프로토콜을 제안한다.

## 1. 서론

RFID 는 IC 칩이 내장된 태그와의 무선통신을 통한 개체 식별 시스템으로서, 센서 네트워크와 더불어 유비쿼터스 컴퓨팅 환경 구현을 위한 기술로 각광받고 있다. RFID 시스템은 장차 현재의 바코드를 대체할 수단으로 발전하고 있으며 그 응용 범위가 점차 확대되는 추세이다.

그러나 별도의 물리적 접촉 없이 정보를 주고받기 때문에, 허가되지 않은 사람이 개인의 신상이나 위치 정보를 무단으로 채취할 있는 문제점이 존재한다[2].

이러한 문제점에 대응하기 위한 RFID 시스템의 보안에 관한 연구가 다양하게 이루어져왔고, 해시 기반 인증 방법과 재 암호화 기반 인증 방법이 소개되었다. 본 논문은 해시 기반 인증 방법에 기반한 재전송 공격에 안전한 인증 프로토콜을 제시한다.

본 논문의 구성은 다음과 같다. 2 장에서 RFID 시스템과 연관된 보안 요소를 알아보고, 3 장에서는 지금까지 소개된 RFID 보안 기법에 대해 분석하며, 4 장에서는 앞서 소개된 보안 방식을 보완한 프로토콜을 제안한다. 그리고 5 장에서는 제안된 프로토콜의 보안성을 검증하고 6 장에서 결론을 맺는다.

## 2. RFID 시스템과 보안

RFID 시스템은 크게 세 부분으로 구성되어 있다. 식별정보가 저장된 태그(Tag)와 이를 인식하고 다시 기록할 수 있는 리더(Reader), 그리고 백-엔드 데이터베이스(Back-End Database)로 나뉘어진다. 여기서 리더와 백-엔드 데이터베이스가 유선을 통하여 제한적인 접근환경에서 통신을 하는데 반해, 태그와 리더의 통신은 개방된 공간에서 무선으로 이루어지기 때문에 도청에 노출될 수밖에 없고, 특히 RFID 태그는 제한된 계산능력으로 인해 복잡한 암호화/복호화 연산을 수행하기에는 어려움이 따른다.

따라서 본 논문은 리더와 태그 사이의 통신에 관한 보안성에 초점을 두고, 리더와 백-엔드 데이터베이스 간에는 다양한 기술을 통한 안전한 통신채널이 구성되어 있다고 가정하며, 이러한 가정에 기반한 RFID 시스템 설계시의 고려해야 할 보안 위협은 다음과 같다[1,5].

**트래픽 분석(위치 추적):** 공격자는 도청을 통해 얻은 트래픽을 분석하여 여러 가지 정보를 알아낼 수 있다. 내용이 암호화 되어있더라도 태그와 리더의 통신간에 동일한 비트패턴이 발생할 경우, 특정 비트패턴의 이동을 감지함으로써 태그의 위치 추적이 가능하게 된다. 이를 방지하기 위해선 매 연결시마다 다른 비트패턴을 생성하는 알고리즘이 필요하다.

**재전송 공격**: 태그와 리더 간의 통신에서 질의나 응답에 해당하는 메시지를 도청하여 저장했다가 태그나 리더에게 재전송하여 인가되지 않은 리더에게 태그 정보를 전달하거나 공격자의 태그가 정상 태그인 것처럼 작동하게 하는 공격이다.

**서비스 거부 공격**: RFID 시스템이 정상적인 작동을 못하도록 하는 위협이다. 공격자가 리더/태그 역할을 하는 장비를 이용하여 리더와 태그에 수많은 질의를 하여 리더와 태그가 정상적인 질의나 응답을 제대로 처리하지 못하도록 한다.

**스푸핑 공격**: 특정 태그로 위장하여 리더가 잘못된

이 논문은 2008 년도 정부(과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임(No. R01-2006-000-10614-0)

정보를 인식하게 하거나 정상적인 리더인 것처럼 가장하여 무단으로 태그 정보를 수집하는 공격이다.

## 3. 관련 연구

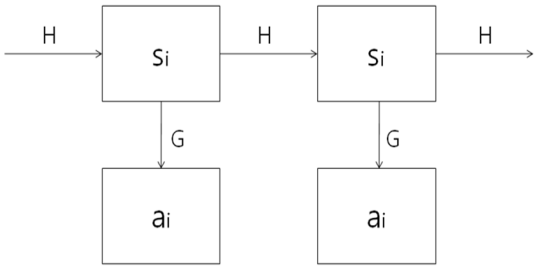
현재까지 리더와 태그 사이의 보안을 위한 다양한 인증 프로토콜이 소개되었으며[2,3,4], 크게 해시 기반의 프로토콜과 재 암호화 기반의 프로토콜로 나뉠 수 있다. 해시 기반의 프로토콜에는 해시 락 프로토콜과 해시 체인 기법이 존재하며, 재 암호화 기반 프로토콜은 ElGamal 공개키 기술을 응용하여 유로화 지폐 식별을 위해 제안되었다. 이들의 간략한 특징은 다음과 같다.

**해시 락 프로토콜(Hash lock protocol)**[3]: 태그가 잠김상태일 때는 리더의 요청에 대해 자신의 ID 를 전송하지 않고 자신의 key 에 대한 해시값인 metaID 를 리더에게 보내고, 리더는 metaID 에 해당하는 key 를 돌려준다. 자신의 key 와 같은 key 를 받으면 락을 해제하고 자신의 ID 를 전송한다. 그러나 매번 같은 metaID 비트패턴을 발생시키기 때문에 위치추적에 쉽게 노출될 수 있다.

**랜덤화된 해시 락 프로토콜(Randomized hash lock protocol)**[3]: 해시 락 프로토콜을 확장한 것으로 태그와 리더의 통신에 난수를 사용하여 동일한 비트패턴이 발생하는 것을 방지한다. 그러나 인증이 완료되는 시점에서 ID 를 노출하게 되며, 재전송 공격을 통해 인증이 가능하다.

**해시 체인 기법**[2]: 2 개의 해시함수를 사용하여 태그의 값을 매번 바꾸어 저장한다. 매 세션마다 다른 값을 전송하게 되므로 트래픽 분석을 통한 위치추적이 불가능하다.

그러나 i 번째 통신에서 i-1 번째 사용된 응답을 전송하면 인증이 가능하므로 스푸핑 공격에 취약한 단점이 있다.




(그림 1) 해시 체인 기법

**재 암호화 기법**: 유로화 지폐 식별을 위해 제안되었으며 ElGamal 공개키 기술을 응용하였다. 다른 기법에 비해 안전한 인증을 할 수 있으나 공개키 관리상 확장이 용이하지 않다.

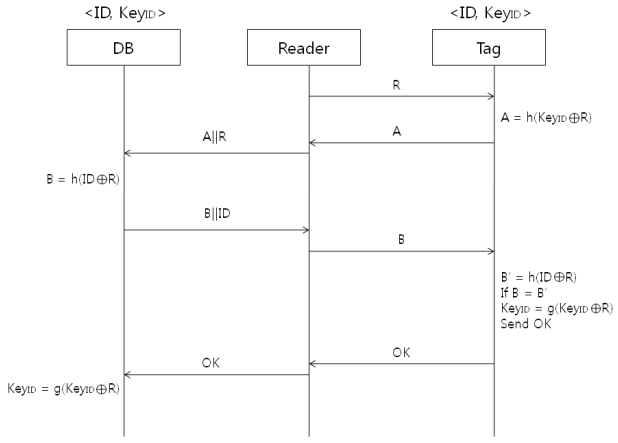
## 4. 해시 체인 기법을 이용한 상호 인증 프로토콜

본 장에서는 이전에 제시된 문제점을 바탕으로 해시 체인 기법을 이용한 상호 인증 프로토콜을 제안한다.

다음은 제안하는 프로토콜의 작동방식을 설명한다.

1. 초기화 단계
   태그의 ID 와 key 를 각각 생성하여 태그에 할당하고 백-엔드 데이터베이스에 저장한다.

2. 인증 단계
   1) 리더는 난수 R 을 생성하여 태그에게 질의를 보낸다.
   2) 태그는 단방향 해시 함수 h 를 이용하여 $A = h(Key_{ID} \oplus R)$을 계산하여 리더에게 전송한다.
   3) A 를 받은 리더는 자신이 생성한 난수 R 과 함께 백-엔드 서버로 보낸다.
   4) 백-엔드 서버는 자신이 가진 $Key_{ID}$ 들과 R 을 이용하여 $h(Key_{ID} \oplus R)$를 만족하는 $Key_{ID}$ 를 검색한다.
   5) $Key_{ID}$ 를 발견하면 태그 인증이 완료되고 그것과 짝을 이루는 ID 를 이용하여 $B = h(ID \oplus R)$를 계산한 다음 리더에게 전달한다.
   6) 리더는 백-엔드 서버로부터 전달받은 B 를 태그에게 전송하고 ID 는 자신이 취하게 된다.
   7) 태그는 처음에 받은 R 과 자신이 가진 ID 를 이용하여 $h(ID \oplus R)$를 계산한 다음 전달받은 B 값과 비교하여 일치하면 리더 인증이 완료되며 자신의 $Key_{ID}$ 를 단방향 해시함수 $g(Key_{ID} \oplus R)$로 갱신하고 OK 신호를 보낸다.
   8) 리더는 백-엔드 서버에 OK 신호를 전달하고, 이 신호를 전달받은 백-엔드 서버도 역시 이 세션에 사용된 $Key_{ID}$ 를 $g(Key_{ID} \oplus R)$로 갱신하고 세션을 종료한다.




(그림 2) 제안된 프로토콜

## 5. 보안성 검증

본 장에서는 기존의 프로토콜과 비교하여 제안된 프로토콜의 보안성을 검증하도록 한다.

먼저, 리더는 태그로부터 직접 ID 를 받을 수 없고, 오로지 key 를 통해 백-엔드 데이터베이스로부터만 ID 를 얻을 수 있기 때문에 본 논문이 가정하는 상황에서는 태그의 정보가 직접 노출되지 않으므로 안전하다고 할 수 있다.

또한 난수를 사용하여 통신하기 때문에 질의와 응답이 이루어질 때마다 다른 비트패턴이 생성되므로 도청을 통한 위치 추적이 불가능하다.

마지막으로, 정상적인 통신이 이루어질 때마다 태그의 key 가 계속 바뀌고 key 의 갱신에는 별도의 해시 함수가 사용되기 때문에 재전송 공격으로부터 안전하다.

가능한 공격의 유형에 따라 이미 소개된 프로토콜과의 비교 결과는 표 1 과 같다.

**<표 1> 공격 유형별 기존 프로토콜과의 비교**

| | 해시 락 프로토콜 | 랜덤화된 해시 락 프로토콜 | 해시 체인 프로토콜 | 제안된 프로토콜 |
|---|---|---|---|---|
| 위치 추적 | O | X | X | X |
| ID 외부 노출 | O | O | X | X |
| 재전송/스푸핑 공격 | O | O | O | X |

(O: 가능, X: 불가능)

## 6. 결론

본 논문은 기존의 RFID 인증 기법을 분석하고 해시 체인 기법을 개선하여 재전송 공격에 안전한 상호 인증 프로토콜을 제안하였다.

제안된 프로토콜에서 태그의 ID 는 리더와 백-엔드 데이터베이스 사이의 안전한 채널에서만 전달되므로 태그는 자신의 ID 를 무선 통신상에 직접 노출하지 않아도 되며, 위치 추적 및 재전송, 스푸핑 공격에 안전하다.

## 참고문헌

[1] Boyeon, S. and J. M. Chris (2008). RFID authentication protocol for low-cost tags. Proceedings of the first ACM conference on Wireless network security. Alexandria, VA, USA, ACM.

[2] M. Ohkubo, K. Suzuki, S. Kinoshita, “Cryptographic approach to “privacy-friendly” Tags”, RFID Privacy Workshop, 2003

[3] S.A.Weis, S.Sarma, R.Rivest, and D.Engels, “Security and privacy aspects of low-cost radio frequency identification systemds”, LNCS

[4] 김배현, 유인태, “반사공격에 안전한 RFID 인증 프로토콜”, 한국통신학회, 2007

[5] 김승빈, 이택, 이명락, 인호, “해시 체인 보안 취약성을 개선한 RFID 인증 프로토콜”, 한국정보처리학회, 2008