논문 2005-42CI-1-5

유비쿼터스 컴퓨팅 환경에 적합한 RFID 인증 프로토콜에 관한 연구

(A Study on RFID Authentication Protocol suitable for Ubiquitous Computing)

양 형 규*, 안 영 화*

(Hyungkyu Yang and YoungHwa An)

요 약

최근 유비쿼터스 컴퓨팅에 대한 연구가 활발히 진행되고 있으며, 유비쿼터스 컴퓨팅의 실현을 위한 핵심기술로서 RFID 시스템에 대한 연구가 활발히 진행되고 있다. 유비쿼터스 환경에서 RFID 시스템이 사용자의 편리함을 가져다주는 장점이 있는 반면, 이로 인해 사용자의 프라이버시가 침해당할 수 있다는 문제점 또한 가지고 있다. 본 논문에서는 기존의 RFID 인증 메커니즘들이 가지고 있는 프라이버시 침해 문제를 분석하고 보다 안전하고 효율적으로 사용자의 프라이버시를 보호할 수 있는 RFID 인증 프로토콜을 제안한다. 제안하는 프로토콜은 공격자의 재전송 공격, 스푸핑 공격, 그리고 트레킹에 대해 안전하다.

Abstract

Recently, ubiquitous computing is being actively researched and one of the main technology in ubiquitous computing environments is recognized as RFID system. The RFID system has much benefits but simultaneously has some problems such as user's privacy violation. Therefore, in this paper, we analyze the privacy problems of previous methods and propose more secure and effective authentication method to protect user's privacy. The proposed protocol is secure against replay attack, spoofing attack and tracking by an attacker.

Keywords: RFID 인증 시스템, 일방향 해쉬 함수, 난수

I. 서 론

유비쿼터스 컴퓨팅에 대한 연구와 관심이 증대됨에 따라, 실생활에서 유비쿼터스 컴퓨팅 환경을 적용시키기 위한 핵심 기술로 RFID (Radio Frequency IDentification) 시스템이 주목받고 있다. RFID 시스템은 무선 주파수를 이용한 자동인식기술로서 물리적 접촉 없이 태그가 부착된 개체의 정보를 읽거나 기록할 수 있는 시스템이다. 최근 들어 물류 및 유통 비용의 절감을 위해 RFID 시스템이 큰 주목을 받고 있으며, 활발한 투자와 연구가 진행되고 있다. RFID 시스템이 주목을 받고 있는 또 다른 중요한 이유는 현재 사용되고 있는 바코드 시스템이 가지고 있는 일회성에 대한 문제를 해결할 수 있을 것으로 기대되기 때문이다. 물류 및 유통 시스템에 RFID 시스템을 적용할 경우, 물류 및 유통 관리의 자동화 뿐만 아니라 태그 내의 정보를 이용한 지속적인 서비스가 가능하기 때문에 많은 기업들이 RFID 시스템에 큰 관심을 보이고 있다. 그러나, 위에서 설명한 바와 같이 RFID를 이용한 기술이 많은 장점을 가지고 있지만, 사용자도 모르게 개인의 정보 노출, 위치 추적 등과 관련된 프라이버시 침해를 유발할 수 있다는 문제점 또한 가지고 있다.[1,2,3,4]

지금까지 이러한 프라이버시 침해 문제를 해결하기 위해 많은 연구가 진행되어 왔으며, 대표적인 방법으로 킬 명령어를 이용한 방법[5,6], 해쉬-락(Hash- Lock) 방법, 확장된 해쉬-락 방법, 블로커태그(Blocker tag)를 이용한 방법[7], 그리고 해쉬-체인(Hash-Chain)을 이용

정회원, 강남대학교 컴퓨터미디어공학부
(Department of Computer&Media Engineering, Kangnam University)
접수일자: 2004년11월30일, 수정완료일: 2005년1월11일

한 방법[8] 등이 제안되었다. 그러나 기존이 방법들은 태그의 재사용이 불가능하거나 재전송 공격, 스푸핑 공격 등에 취약하고 태그의 추적이 가능하므로 여전히 사용자 프라이버시 침해 문제를 완전하게 해결하지 못하고 있다.

본 논문에서는, 먼저 기존의 방법들에 대하여 간단하게 설명하고 이들이 가지고 있는 문제점들에 대하여 분석한다. 그리고 해쉬 함수와 난수를 이용하여 태그가 리더에게 전송하는 정보를 변형함으로써 공격자에 의한 사용자 프라이버시 침해를 방지할 수 있는 RFID 인증 프로토콜을 제안한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 RFID 시스템의 기본적인 구성과 개요에 대하여 설명하고, Ⅲ장에서는 기존의 인증 방법들과 이들이 가지고 있는 문제점에 대하여 분석한다. 다음으로 Ⅳ장에서는, 제안하는 프로토콜에 대하여 설명하고 안전성과 효율성을 분석한다. 마지막으로 Ⅴ장에서 결론을 맺는다.

Ⅱ. RFID 시스템

RFID 시스템은 일반적으로 태그, 리더, 그리고 백 앤드 데이터베이스로 구성되며, 그림 1에 도식화 하였다.

1. 태그(Tag)

태그는 리더의 요청에 대하여 태그에 저장된 식별 정보를 전송하는 것으로서, 무선 통신을 위한 결합장치(Coupling element)와 연산을 수행하고 정보를 저장하는 마이크로 칩 등으로 구성되어 있으며, 크게 능동형 태그(Active tag)와 수동형 태그(Passive tag)로 구분된다

- 능동형 태그(Active tag) : 능동형 태그는 태그 자체에 배터리를 내장하고 있으며, 이 배터리로부터 전력을 공급 받아 리더의 요청에 응답하게 된다. 자체 배터리를 내장하고 있으므로 원거리 정보 전송이 가능한 반면, 배터리 내장으로 인해 태그의 가격이 수동형 태그에 비해 상대적으로 높다는 단점이 있다.

- 수동형 태그(Passive tag) : 리더로부터 수신한 전자기파에 의해 유도된 전류를 전원으로 사용하며, 주로 근거리 정보 전송에 이용된다. 배터리를 내장하고 있지 않으므로 태그의 가격이 능동형 태그에 비해 상대적으로 낮으며, 태그의 수명이 반영구적이라는 장점을 가지고 있다.

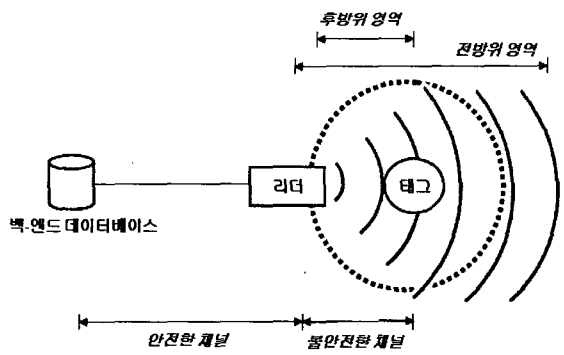

그림 1. 기본적인 RFID 시스템
Fig. 1. Basic RFID System.

2. 리더(Reader)

리더는 태그에게 식별정보를 요청하고, 태그가 전송한 식별 정보를 수신하여 태그를 인식하는 역할을 하는 장치이다. 리더는 수동형 태그에게 RF 신호(RF Signal)를 전송하여 전력을 공급하고, 태그로부터 수신한 정보를 백-엔드 데이터베이스에 전송한다.

3. 백-엔드 데이터베이스(Back-end Database)

백-엔드 데이터베이스는 리더가 수집한 정보를 저장 또는 관리하며, 연산 능력이 낮은 태그 또는 리더를 대신하여 복잡한 연산을 대신 수행하기도 한다. 태그를 식별할 수 있는 정보를 저장하고 있으며, 태그로부터 수집한 정보의 정당성을 판별하는 역할을 수행한다.

그림 1에서 전방위 영역(Forward range)은 리더가 RF 신호를 태그로 전송할 수 있는 범위를 나타내며, 후방위 영역(Backward range)은 태그가 리더의 요청에 대하여 자신의 정보를 전송할 수 있는 범위를 의미한다. (예, 915 MHz의 주파수를 사용하는 RFID 시스템의 경우, 태그의 전송 반경은 약 3미터 정도이며 리더가 전송할 수 있는 영역은 반경 약 100미터 정도라 할 수 있다[2,7].) 또한, RFID 시스템은 기본적으로 리더와 태그 사이의 통신은 불안전한 채널에서 이루어진다고 가정하고 있으며, 백-엔드 데이터베이스와 리더 간의 통신은 안전한 채널을 통해 이루어진다고 가정한다.

Ⅲ. 기존의 RFID 인증 프로토콜

본 장에서는 기존에 제안된 RFID 인증 방법들과 이들이 가지는 문제점들에 대하여 간략하게 설명한다. 일

반적으로 RFID 시스템에서의 공격은 불안전한 채널을 통해 이루어지게 되며, 여기서 사용하고 있는 태그들은 모두 수동형 태그를 고려하여 설계된 것이다.[9]

1. KILL 명령어 기법

Kill 명령어 방법은 태그가 자신의 데이터 필드에 저장된 패스워드를 외부에서 받은 경우, 태그를 영구적으로 정지시킴으로써 더 이상 리더의 질의에 응답하지 않게 만드는 방법이다. 이 방법은 명령이 수행된 이후, 제대로 완료되었는지 확인하기 어려우며 한번 정지된 태그의 재사용이 불가능하다는 단점을 가지고 있다. 이 방법은 암호학적 기법을 사용하지 않은 물리적 기법이라 할 수 있다.

2. 블로커 태그

이 방법은 블로커 태그라고 불리는 태그를 물체에 부착하여 사용자의 프라이버시를 보호하는 보안 방법이다. 블로커 태그는 프라이버시가 요구되는 태그의 정보를 요구하는 불법적인 리더의 요청에 대해 이진 트리(Binary Tree) 구조에 연계된 모든 태그의 정보를 전송하는 방법이다. 이와 같은 방법을 통해 특정 태그에 대해 프라이버시를 보호하게 된다.

이 방법은 태그의 응답에 대한 충돌 회피 기법으로 제안된 트리 구조를 사용함으로써 프라이버시가 요구되는 태그와 그렇지 않은 태그를 구분하고 특정 영역을 할당함으로써 효율성을 가질 수 있다는 장점을 가지고 있다. 이 방법 또한 Kill 명령어 방법과 마찬가지로 물리적 보안 기법의 하나이다.

3. 해쉬-락 프로토콜

해쉬-락 프로토콜은 태그의 ID를 은닉하기 위해 metaID를 이용하는 잠김(locked)과정과 ID를 마지막 단계에서 노출하는 풀림(unlocked)과정으로 분류할 수 있다. 이 프로토콜에서는 각각의 태그가 소유한 ID를 숨기기 위해 metaID를 이용하지만, metaID가 매 세션마다 고정되어 사용되므로 공격자에 의한 트래킹이 가능하다는 단점이 있다. 또한 공격자가 정당한 리더로 위장하여 태그에게 응답을 요청하고, 이를 통해 스푸핑 공격이 가능하다는 단점을 가지고 있다.

그림 2는 해쉬-락 프로토콜의 구성을 나타낸 것이다.

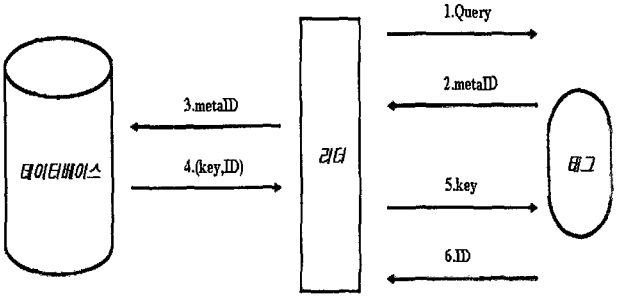

그림 2. 해쉬-락 프로토콜
Fig. 2. Hash-Lock Protocol.

4. 확장된 해쉬-락 프로토콜

이 프로토콜은 해쉬-락 프로토콜의 확장된 형태로, 태그는 해쉬함수와 난수생성기를 포함하고 있다. 이 프로토콜에서 태그는 매 세션마다 난수생성기와 해쉬함수를 이용하여 새로운 인증 정보를 생성하여 리더에게 응답하게 된다. 그러나 프로토콜의 종료 과정에서 리더가 실제 ID를 태그에서 전송하게 되어 공격자에 의한 프라이버시 침해를 유발할 수 있다. 또한, 해쉬-락 프로토콜과 동일한 문제점을 가지고 있다.

그림 3은 확장된 해쉬-락 프로토콜을 나타낸 것이다.

5. 해쉬-체인 프로토콜

해쉬-체인 프로토콜은 서로 다른 두개의 해쉬함수를 사용하고 초기 비밀 정보를 갖는다. 이 프로토콜은 두 개의 서로 다른 해쉬함수를 이용하여 리더에 대한 응답 메시지들 간의 관계를 공격자에게 노출시키지 않도록

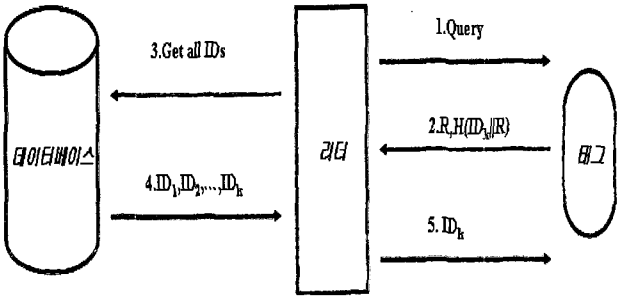

그림 3. 확장된 해쉬-락 프로토콜
Fig. 3. Randomized Hash-Lock Protocol.

표 1. 기존 프로토콜들의 안전성 비교
Table 1. Security of existing protocols.

인증방식	재전송 공격	스푸핑 공격	트래킹
해쉬-락	X	X	X
확장된 해쉬-락	X	X	X
해쉬-체인	X	X	O

X : 안전하지 못함, O : 안전

제안된 프로토콜이다. 이 프로토콜은 매 세션마다 랜덤한 응답을 생성하므로 사용자의 프라이버시 보호가 가능하다. 또한 백-엔드 데이터베이스는 프로토콜을 수행하기 위해서 모든 비밀정보에 대응하는 태그의 ID를 검색해야 하므로 많은 계산량을 요구한다.

표 1은 기존 프로토콜들의 안전성을 비교한 것이다.

Ⅳ. 제안 프로토콜

본 장에서는 기존 프로토콜들에서 문제점으로 지적되었던 재전송 공격과 스푸핑 공격에 대하여 안전한 RFID 인증 프로토콜을 제안한다.

1. 구성

본 논문에서 제안하는 RFID 시스템의 기본 구성은 일반적인 RFID 시스템의 구성과 동일하게 구성되어 있다. 백-엔드 데이터베이스는 태그의 ID와 관련 데이터를 저장하고 있으며, 리더는 난수 생성기를 이용하여 난수를 생성한다. 그리고 태그는 ID와 리더로부터 전송받은 난수를 이용하여 리더의 요청에 대한 응답을 생성한다.

제안 프로토콜에서 사용되는 파라미터는 다음과 같으며, 그림 4는 제안하는 프로토콜을 나타낸 것이다. 또한 본 논문에서 제안하는 프로토콜에 사용하는 태그는 기존의 인증 메커니즘들과 마찬가지로 수동형 태그를 고려한다.

[파라미터]

- query : 태그의 응답을 요청하는 리더의 요청
- ID : 태그에게 할당된 고유 정보
- h( ) : 일방향 해쉬 함수
- R : 리더가 매 세션마다 생성하여 태그에게 전송하는 난수
- S : 태그가 매 세션마다 생성하여 리더에게 전송하는 난수
- | : 연접(Concatenate function)

그림 4는 제안하는 프로토콜의 구성과 동작 과정을 나타낸 것이다. 제안하는 프로토콜의 동작은 그림에 나타난 것과 같은 순서로 동작하게 되며, 그 과정은 다음 절에서 자세히 설명하도록 한다.

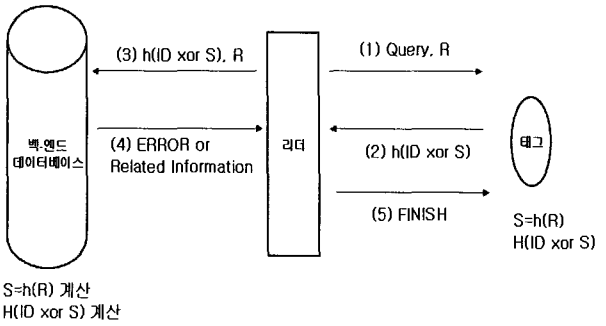

그림 4. 제안하는 RFID 인증 프로토콜
Fig. 4. Proposed RFID Authentication System.

2. 인증 과정

제안한 프로토콜의 인증 과정은 다음과 같다.

(1) 리더 → 태그 : 리더는 태그에게 query와 난수 R을 전송한다.

query, R

(2) 태그 → 리더: 리더로부터 수신한 R을 이용하여 랜덤 수 S를 생성하고, 이를 이용하여 응답(response)을 생성하여 리더에게 전송한다.

$$S=h(R),$$
$$response = h(ID \oplus S)$$

(3) 리더 → 백-엔드 데이터베이스 : 리더는 수신한 response와 R을 데이터베이스에게 전송한다.

response, R

(4) 데이터베이스 → 리더 : 백-엔드 데이터베이스는 리더로부터 전송받은 R을 이용하여 S(S=h(R))를 계산한다.

데이터베이스는 저장하고 있는 모든 ID와 S값을 이용하여 리더로부터 수신한 값과 비교하여 일치하는 값을 검색한다.

계산된 $h(ID \oplus S)$?= 수신한 $h(ID \oplus S)$

만약 일치하는 값이 검색되지 않으면, 에러(error)메시지를 리더에게 전송하고, 일치하는 값이 검색되면 태그를 인증하고 관련 정보를 리더에게 전송한다.

ERROR or Realated Information

(5) 리더 : 리더는 데이터베이스로부터 수신한 값이 ERROR일 경우, 태그와의 통신을 중단하고, 정상적인 인증이 되었을 경우에는 데이터베이스로부터 전송받은 관련정보(related information)을 이용하여 상품에 대한 요금부과와 같은 과정을 수행한다. 그리고 태그에게 인증 과정의 종료를 알리는 종료 메시지를 전송한다.

FINISH(Successful)

3. 안전성

RFID 인증 프로토콜에서 고려해야 하는 가장 중요한 안전성의 개념은 사용자가 소지하고 있는 RFID 태그에 저장된 정보를 추적하여 사용자의 위치 추적과 같은 트래킹에 대한 것이다. 또한 최근에는 이러한 트래킹에 대한 문제 뿐만 아니라 능동적 공격자를 가정하여 재전송 공격과 스푸핑 공격 등에 대해서도 많은 논의가 이루어지고 있다. 이는 RFID 인증 프로토콜에 암호학적인 기법을 도입하려는 시도에서 기인하였으며 재전송 공격과 스푸핑 공격 또한 중요하게 고려하여야 할 사항이다.

앞에서 간략하게 설명한 기존의 인증 프로토콜들에서는 재전송 공격, 스푸핑 공격에 취약하였으며, 또한 공격자에 의한 트래킹이 가능하였다. 본 장에서는 제안하는 인증 프로토콜이 트래킹과 재전송 공격, 그리고 스푸핑 공격에 대한 안전성에 대하여 설명한다.

제안하는 프로토콜은 태그가 리더로부터 수신한 난수를 이용하여 또 다른 난수를 생성하고, 이를 이용하여 매 세션마다 다른 응답을 생성하여 전송하기 때문에, 재전송 공격과 스푸핑 공격에 대하여 안전하며, 공격자에 의한 트래킹도 방지할 수 있다.

만약 공격자가 리더와 태그 사이에서 전송되는 정보를 도청하여, 다음 세션에서 정당한 리더나 태그로 위장을 시도하는 재전송 공격의 경우, 태그와 리더가 매 세션마다 랜덤수를 이용하여 응답을 생성하므로, 이전 세션의 랜덤 수를 알고 있는 공격자라 하더라도 새로운 세션에서의 랜덤 수를 알지 못하면 리더에게 정당한 태그인 것처럼 위장하여 속이는 것이 불가능하다. 그러므로 제안하는 프로토콜은 재전송 공격에 안전하다.

또한 공격자가 이전 세션에서 전송되는 정보를 도청하여, 리더로부터 생성된 이전 세션의 랜덤 수를 알고 있다 하더라도, 이를 이용하여 다음 세션에서 리더와 태그에게 정당한 리더와 정당한 태그인 것처럼 속이는 것이 불가능하다. 그러므로 제안하는 프로토콜은 스푸핑 공격에 안전하다.

표 2. 제안 프로토콜의 안전성
Table 2. Securities of the proposed protocol.

공격의 유형	안전성 여부
재전송 공격	안전 (재전송 공격 불가)
스푸핑 공격	안전 (스푸핑 공격 불가)
트래킹	안전 (트래킹 불가)

이러한 특징으로 인해, 태그에서는 매 세션마다 서로 다른 응답, 즉 랜덤한 응답을 생성하여 리더에게 전송하므로, 공격자가 태그를 추적하기 위해 태그에서 전송되는 모든 정보를 수집한다 하더라도, 그 정보들에 대한 연관성을 찾는 것이 불가능하다. 일반적으로 RFID 시스템에서의 위치 트래킹을 동일한 태그로부터 나오는 응답들을 모두 수집하여, 그 응답이 가지고 있는 연관성을 파악하여 응답들에 대한 링크를 통해 이루어지는 경우가 대부분이다. 그러나 제안하는 프로토콜의 경우, 동일할 태그로부터 나오는 모든 응답들이 매 세션마다 다르게 응답을 하게 되므로 공격자가 모든 응답을 도청한다 하더라고 응답만 가지고 동일한 태그로부터 전송된 응답이라는 것을 알 수 없다. 그러므로 제안하는 프로토콜은 위치 트래킹에 안전하다.

V. 결 론

RFID 시스템은 유비쿼터스 컴퓨팅 환경을 구현하기 위해 핵심적인 기술로 주목받고 있으며, 여러 국·내외 연구소와 기업들에서 RFID 시스템에 대한 연구가 활발히 진행되고 있다. RFID 시스템은 사용자들에게 생활의 편리함 뿐만 아니라 물류비용 절감등과 같은 경제적인 측면에서도 크게 기여할 것으로 기대된다. 그러나 RFID 시스템이 가지고 있는 특성으로 인해 사용자에 대한 프라이버시 침해 문제를 야기할 수 있다. 이러한 문제를 해결하기 위해 사용자의 프라이버시를 보호하기 위한 여러 인증 메커니즘들이 제안되었으나, 여전히 사용자의 프라이버시를 효율적으로 보호하지 못하고 있으며, 인증 메커니즘 자체의 안전성에도 많은 문제점을 가지고 있다.

본 논문에서는 기존의 인증 메커니즘들에 대하여 설명하고, 이들이 가지고 있는 문제점들에 대하여 분석하였다. 이러한 분석 결과를 바탕으로, 태그가 리더로부터 수신한 난수를 이용하여 새로운 난수를 생성하고 매 세션마다 서로 다른 응답을 생성하여 전송함으로써 기존의 메커니즘들에서 문제점으로 지적되었던 재전송 공격과 스푸핑 공격, 그리고 공격자에 의한 트래킹에 안전한 인증 메커니즘을 제안하였다.

제안하는 프로토콜은 안전성과 효율성을 바탕으로 유비쿼터스 컴퓨팅에 관한 연구를 진행함에 있어 다양하게 활용될 수 있을 것으로 기대된다.

참 고 문 헌

[1] S. A. Weis, S. E. Sarma, R. L. Rivest, D. and W. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", Security in Pervasive Computing 2003, LNCS 2802, pp.201-212, Springer-Verlag, 2004.

[2] D. Henrici, P. Müller, "Tackling Security and Privacy Issues in Radio Frequency Identification Devices", Pervasive 2004, LNCS 3001, pp.219-224, Springer-Verlag, 2004.

[3] F. Klaus, "RFID Handbook", second edition, Jone Willey & Sons, 2003

[4] Cloak:Personal/corporate management of wireless devices and technology, 2003. http://www.mobilecloak.com.

[5] S.A.Weis, "Security an Privacy in Radio-Frequency Identification Devices" MS Thesis. MIT. May 2003.

[6] S. E. Sarma, S. A. Weis, D. W. Engels. "RFID systems, Security & Privacy Implications", White. Paper MIT-AUTOID-WH-014, MIT AUTO-ID CENTER, 2002.

[7] A. Juels, R. L. Rivest, M Szydlo, "The Blocker Tag : Selective Blocking of RFID Tags for consumer Privacy", In Proceedings of 10th ACM Conference on Computer and Communications Security, CCS 2003, pp.103-111, 2003.

[8] 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.

[9] S. E. Sarma, S. A. Weis, and D. W. Engels, "RFID Systems and Security and Privacy Implications", CHES 2002, LNCS 2523, pp.454-469, Springer-Verlag, 2003.

저 자 소 개

양 형 규(정회원)

1983년 성균관대학교 전자공학과 학사 졸업.

1985년 성균관 대학교 전자공학과 석사 졸업.

1995년 성균관 대학교 정보공학과 박사 졸업.

1984년~1990년 삼성전자 컴퓨터 부문 선임연구원

1995년 현재 강남대학교 컴퓨터미디어공학부 부교수

<주관심분야: 네트워크 보안, 암호 프로토콜>

안 영 화(정회원)

1975년~1990년 성균관대학교 전자공학과 (학사, 석사, 박사)

1983년 3월~1990년 2월 해군사관학교 전자공학과 교수

2002년 3월~2003년 2월 Florida State University, 방문교수

1990년 3월~현재 강남대학교 컴퓨터미디어 공학부 교수

<주관심분야: 정보보호, 네트워크 보안>