AES를 이용한 RFID 상호인증 프로토콜

김 석* · 한승조**

RFID Mutual Autentication Protocol Using AES

Seok Kim* · Seung-jo Han**

이 논문은 2012년도 조선대학교 연구비를 지원받았음

요 약

유비쿼터스 시대를 맞이한 현재 RFID(Radio Frequency Identification)의 사용은 급속한 증가추세에 있으며, 생활 전반에 걸쳐 사용되고 있다. 무선주파수를 이용하여 자동으로 데이터를 인식할 수 있는 RFID 시스템은 개인정보보호나 보안에 대해 취약하다. 또한 암호학적 안정성을 적용하기에 수동형 태그의 경우 하드웨어적으로 제한적인 문제를 가지고 있다. 본 논문에서는 임의비표(Nounce)라는 난수를 AES 암호화 알고리즘의 키로 사용하고 리더와 태그는 상호인증을 한다. 임의비표의 사용으로 보안적 취약점을 강화하고, 상호인증을 마친 후에만 서버에 접근하기 때문에 서비스 거부공격에 안전하다.

ABSTRACT

Recently use of RFID(Radio Frequency Identification) tends to be rapidly increased and will be also extended throughout the whole life. Using radio-frequency data can be recognized automatically in the RFID system is vulnerable to personal information protection or security. And passive tags have a hardware problem is the limit for applying cryptographic. This paper presents an authentication protocol using AES and Nounce. After completing mutual authentication server to access and strengthen security vulnerability to the use of the Nounce, because safety in denial of service attacks.

키워드

RFID, AES, 상호인증, 프로토콜

Key word

RFID, AES, Mutual authentication, Protocol

* 정회원 : 조선대학교 정보통신공학과 (shoo2715@nate.com)
** 종신회원 : 조선대학교 정보통신공학과 (교신저자)

접수일자 : 2012. 07. 27
심사완료일자 : 2012. 08. 12

Open Access http://dx.doi.org/10.6109/jkiice.2012.16.9.1963

Ⅰ. 서 론

RFID란 태그, 레이블, 카드 등과 같은 저장매체의 데이터를 무선 주파수를 이용하여 리더로 자동 인식하게 하는 기술을 말한다. 이것은 기존 바코드나 자기인식 장치의 단점을 보완하고 사용의 편리성을 향상시킨 차세대 핵심 기술이며 국방, 의료, 유통, 교통, 보안, 제조, 건설, 서비스, 행정 등 다양한 분야에 응용된다.

RFID 시스템은 태그, 리더, 백 엔드 서버로 구성되어 있다. 태그는 사람과 사물, 동물 등에 부착하여 식별 및 인식 정보를 송수신하는 장치이며 크게 능동형 태그(Active Tag)와 수동형 태그(Passive Tag)로 분류된다. 리더는 태그의 정보를 읽어내기 위해 태그와 송수신하는 장치이며 무선 주파수를 사용한다. 백 엔드 서버는 다수의 리더로부터 전송된 태그 정보에 대한 처리를 해주는 서버 시스템이다.

RFID 시스템은 그 편리함에도 불구하고 개인 정보보호나 보안에 대한 여러 가지 취약점을 가지고 있다.[1.2] 바코드 시스템과 비교하여 시야가림에 대한 문제가 없지만 그 문제로 인하여 태그는 항상 읽혀질 준비를 하고 있는 것 또한 사실이다. RFID 시스템의 핵심은 무선통신으로 이루어진 리더와 태그 사이의 데이터 교환이며, 외부의 공격을 받을 수 있는 여지가 있는 부분이다. 안전한 데이터 교환을 위하여 무선 네트워크에서 사용되는 보안 프로토콜을 적용시키는 것을 고려해볼 수 있겠으나, 이는 수동형 태그의 제한적 환경에 적용하기 힘든 것이 현실이다. 또한 백 앤드 서버에 대한 서비스 거부 공격(Denial of Service Attack)이 있을 수 있다.

본 논문에서는 수동형 태그의 하드웨어적으로 제한적인 환경에 적용 가능한 블록암호화를 사용하여 취약했던 공격에 대응하고 태그와 리더의 상호인증을 거친 후 백 엔드 서버에 접근함으로써 서비스 거부공격에 강한 프로토콜을 제안한다.

Ⅱ. 본 론

RFID 시스템에서 태그와 리더간 데이터 교환은 무선통신을 사용한다. 리더가 태그의 고유한 식별정보를 요청하고 태그가 응답한 식별정보를 백 엔드 서버로 전송하여 태그의 정보를 읽어 들인다. 하지만 RFID의 시스템의 통신과정에서 도청공격(Eavesdropping Attack), 위치 추적 공격(Location Tracking), 재전송 공격(Replay Attack), 도청을 통한 스푸핑 공격(Spoofing Attack), 서비스 거부공격 등과 같은 보안적 취약점을 가지고 있으며, 이를 해결하기 위해 많은 연구가 진행되어 왔다.

2.1. 기존 RFID 시스템 보호 기법

기존의 RFID 시스템의 보호 기법으로는 물리적 보호 기법과 암호학적 인증 기법으로 나눌 수 있다.

물리적 보호 기법으로는 대표적으로 'Kill', Tag, Faraday Cage[3], Active Jamming[4]과 같은 방법이 있으며, 'Kill' Tag 기법은 'Kill' 명령어를 통해 태그의 기능을 정지시켜버리는 방법으로 재사용 할 필요가 없는 경우에 사용하는 방법이다. Faraday Cage 기법은 태그 자체에 그물(Mesh)이나 박막(Foil)을 입혀 무선 주파수가 침투하지 못하도록 하는 방법이다. 그러나 무선 주파수가 침투 할 수 있어야 할 때에도 주파수 교신을 하지 못하게 하기 때문에 사용에 따른 불편함이 우려된다. 항상 읽혀져야 할 태그에 대해서 악의적인 목적으로 무선신호가 침투하지 못하도록 한다면 태그 자체가 없는 것으로 인식 될 수 있는 점 또한 문제가 된다. Active Jamming 기법은 리더에서 태그의 정보를 읽어내기 위해 보내는 신호를 방해할 목적으로 방해신호발생장치를 사용하며, 태그의 정보를 보호할 수 있지만 불법적으로 이용할 소지가 크고 오히려 방해신호에 의해 다른 RFID 시스템을 손상시킬 수 있기 때문에 특별한 경우에 사용하는 방법이다.

암호학적 인증기법으로는 공개키 암호, 대칭키 암호, 해시함수를 사용하여 각 노드간 통신 과정에서 노출되는 정보를 암호화함으로써 악의적인 공격자로부터 시스템을 보호하는 방식이다.

2.1.1. 해시-락(Hash-Lock) 인증 프로토콜

MIT에서 저가형 태그에서 리소스제한 문제를 해결하면서 인가를 받은 리더에만 태그 정보를 전송하기 위한 방법으로 해시-락 인증 프로토콜을 제안하였다. 그러나 공격자가 metaID를 도청하여 정당한 리더에게 전송 시 리더는 공격자에게 정당한 키를 전달하는 문제점이 있다. 해시-락은 도청공격, 스푸핑 공격, 재전송 공격, 위치추적 및 서비스 거부 공격에 매우 취약하다.[5]

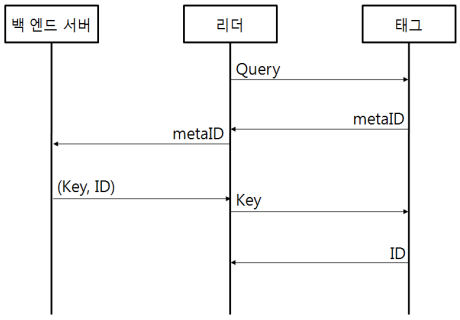

그림 1. 해시-락 인증 프로토콜
Fig. 1 Hash-Lock Protocol

2.1.2. 확장된 해시-락(Extended Hash-Lock) 인증 프로토콜

확장된 해시-락 기법은 태그가 난수 생성기를 갖는다는 것을 가정하여 제안한 방식으로 기존 해시-락에서 리더의 Query 수신에 같은 metaID를 전송하여 발생하는 위치 추적공격에 문제를 해결하였지만 스푸핑, 재전송 공격에 여전히 취약하다.[6]

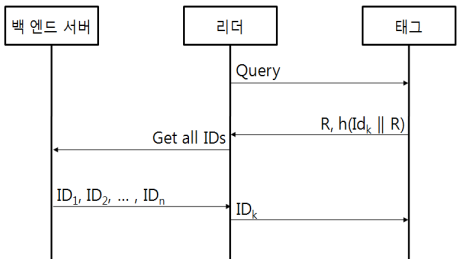

그림 2. 확장된 해시-락 인증 프로토콜
Fig. 2 Extended Hash-lock Protocol

2.1.3. 해시-체인(Hash-Chain) 인증 프로토콜

해시-체인 인증 프로토콜은 두 개의 해시함수로 구성되어있다. 리더의 Query에 대해 매번 다른 응답을 전송하기 때문에 위치추적에 안전하다. 두 개의 해시함수를 사용하기 때문에 도청공격, 재전송 공격에도 안전하다. 하지만 공격자가 불법적인 리더기로 정당한 태그에게 Query를 보내게 되면 리더 태그간의 동기화로 이루어진 인증과정에 문제가 발생하게 된다. 또한 두 개의 해시함수를 사용하기 때문에 저가형 수동형 태그에 적합하지 않은 단점이 있다.[7]

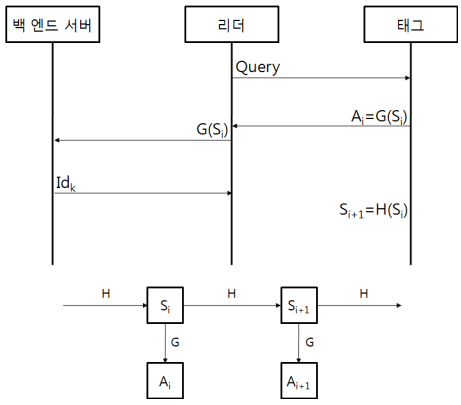

그림 3. 해시-체인 인증 프로토콜
Fig. 3 Hash-Chain Protocol

2.2. AES 블록암호화

AES(Advanced Encryption Standard, 고급암호표준)은 1990년대 들어 DES(Data Encryption Standard)암호의 가능성이 높아지고, 1998년을 기점으로 DES는 표준 기한이 만료됨에 따라 미국 표준기술연구소에서 새로운 블록암호를 공모하였고, Rijndeal은 다른 기술보다 보안성, 성능, 효율성, 구현 용이성, 유연성 등의 항목에서 가장 우수한 기술로 평가받았고, 또한 이 기술은 서로 다른 다양한 컴퓨터 환경에서도 우수한 성능을 보여주고 메모리를 적게 차지해 스마트카드 등 메모리 용량이 적은 장치에서 손쉽게 사용될 수 있다는 특징이 있다.[8]

또한 최근에 4,000게이트 미만으로 AES 연산기를 구현함에 따라 AES가 수동형 태그에 적합함을 보여주고 있다.[9]

Ⅲ. 제안 프로토콜

기존의 RFID 시스템의 암호학적 인증 기법은 일반적으로 해시 함수를 이용한 방법으로써 태그의 정보가 쉽게 노출되기 때문에 스푸핑 공격, 재전송 공격, 위치추적 공격 등에 취약하고 태그의 복제가 가능하다.[10]

제안하는 프로토콜은 AES블록암호화 알고리즘을 사용하여 리더 태그간 무선주파수를 통해 전송되어지는 데이터에 안정성을 높이고, 임의비표(난수)를 사용하여 리더와 태그를 상호 인증하였다. 제안하는 프로토콜의 인증과정은 그림 4와 같다.

표 1. 시스템 파라미터
Table. 1 System parameters

용어	내용
TagID	태그의 고유 식별 값
N	임의비표(난수)
E	AES 암호문
k	AES 암호문 키 값
⊕	XOR 연산

본 논문에서 제안하는 프로토콜의 인증과정을 설명하기에 앞서 다음사항을 가정한다.

- 서버와 리더 사이에는 안전한 통신채널을 사용한다.
- 리더와 태그는 AES 연산이 가능하고, 임의비표를 생성할 수 있는 난수 발생기를 가지고 있다.
- 리더와 태그는 사전에 AES블록암호화 알고리즘의 키 값을 안전한 방법으로 공유하고 있다.

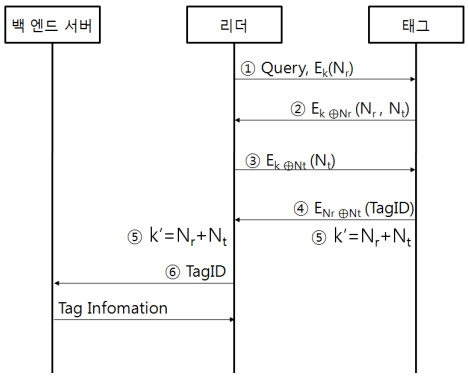

그림 4. 제안하는 인증 프로토콜
Fig. 4 New Authentication Protocol

① R→T : Query, Ek(N_r)

리더는 질의와 함께 리더에서 생성한 임의비표 (N_r)를 AES 블록암호화 하여 Query와 함께 전송한다.

② T→R : $E_{k\oplus Nr}(N_r \oplus N_t)$

태그는 리더로부터 받은 메시지를 사전에 공유한 키 값으로 복호화 하여 리더의 임의비표(N_r)를 획득하게 되고, 태그 자신은 임의비표(N_t)를 생성한다. 태그는 사전에 공유한 키 값(k)과 획득한 리더의 임의비표(N_r), 획득한 리더의 임의비표(N_r)와 자신이 생성한 임의비표(N_t)를 각각 XOR연산하여 암호화 키 값, 암호문으로 하는 메시지를 리더로 전송한다.

③ R→T : $E_{k\oplus Nt}(N_t)$

리더는 태그로부터 전송받은 메시지를 복호화하여 자신이 최초 전송한 임의비표(N_r)와 태그가 생성한 임의비표(N_t)를 획득하게 된다.

최초 리더 자신이 전송했던 임의비표와 획득한 임의비표를 비교하여 같다고 한다면 태그는 정상적인 태그로서 인증 받게 된다.

리더는 태그에게 사전에 공유한 키 값(k)과 전송받은 태그의 임의비표(N_t)를 XOR 연산하고 그것을 새로운 키 값으로, 태그가 생성한 임의비표(N_t)를 암호문으로 하는 메시지를 전송한다.

④ T→R : $E_{Nr\oplus Nt}$(TagID)

태그는 리더로부터 전송받은 메시지를 복호화하여 자신이 전송한 임의비표(N_t)를 획득하게 된다. 태그 자신이 전송했던 임의비표와 획득한 임의비표를 비교하여 같다고 한다면 이 또한 정상적인 리더로서 인증 받게 된다.

태그는 리더의 임의비표와 자신의 임의비표를 XOR 연산하여 얻어진 값을 키 값으로 하여 자신의 고유 식별 값을 암호문으로 하는 메시지를 리더에게 전송한다.

①~④번까지의 과정을 통해 리더와 태그는 상호인증을 하게 되고 서로의 임의비표를 XOR연산하여 얻어진 값을 키 값으로 하여 가장 중요한 정보인 태그 고유의 식별 값을 암호문으로 한 메시지를 리더에게 전송한다.

⑤ k'= Nr ⊕ Nt

이 과정은 사전에 공유한 키 값을 다음 인증과정에서 보다 향상된 보안성을 제공하기 위하여 새로운 키 값으로 갱신하는 과정이다.

⑥ R→S : TagID

리더는 백 엔드 서버에게 태그의 정보를 요청한다.

Ⅳ. 시뮬레이션 및 비교 분석

4.1. 시뮬레이션 환경

시뮬레이션은 OPNET 12.0에서 구현하였으며, 기본적인 RFID 시스템과 같다. 중간에 공격자를 두어 도청공격과 서비스 거부 공격을 시도하도록 구성하였다.

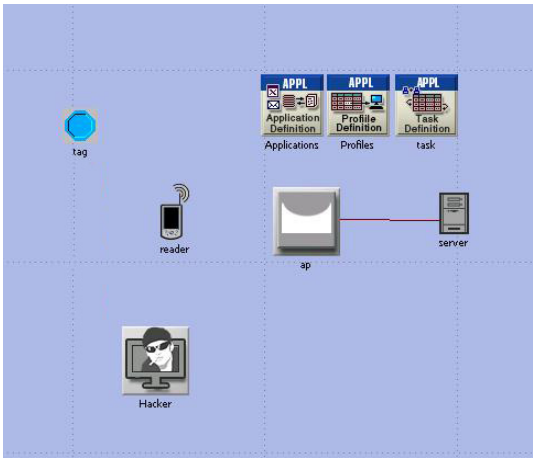

그림 5. 시뮬레이션 환경
Fig. 5 Simulation environment

표 2. 시뮬레이션 환경
Table. 2 Simulation environment

Statistics	Value
Scenario Size	10m X 10m
Tag Data Rates	1 Mbps
Readers Data Rates	11 Mbps
Tag Transmit Power	0.001 W
Readers Transmit Power	0.005 W
Tag Type	Passive
Simulation Time	1 hour

4.2. 시뮬레이션 결과 및 비교분석

시뮬레이션은 RFID 시스템 환경에서 해시-락, 확장된 해시-락, 해시-체인 프로토콜과 제안한 프로토콜을 비교하였다. 공격자는 도청공격을 통해 정당한 리더로서 가장하여 태그와 백 엔드 서버를 공격한다.

그림 6에서 볼 수 있듯이 해시-락과 해시-체인 프로토콜은 공격자의 도청공격에 인증이 이루어지는 것을 볼 수 있고, 해시-체인 프로토콜과 제한한 프로토콜 그래프 중간에 끊어져 인증이 완료되지 않은 것을 볼 수 있다. 하지만 두 개의 해시함수를 사용하는 해시-체인 프로토콜의 경우 시스템에 많은 부하를 주기 때문에 인증 지연시간이 가장 높게 나타났다. 제안한 프로토콜은 임의비표를 사용하고, AES암호화 알고리즘을 사용하여 공격자가 도청 공격을 통해 메시지를 획득했다 하더라도 사전에 안전하게 공유한 키 값으로 암호화하였기 때문에 공격자는 알 수 없는 값이 된다. 또한 복호화 하였다 하더라도 리더와 태그에서 각각 생성한 임의비표이기 때문에 의미 없는 수가 된다. 또한 매 Query 마다 다른 수가 전송되기 때문에 위치추적 공격에도 안전하다.

자신이 생성한 임의비표와 전송받은 임의비표가 같은 값인지 판단하여 상호인증이 이루어지는 점 또한 도청공격을 통해 정당한 리더로써 가장한 불법적인 리더의 스푸핑 공격에 대해서도 안전하다. 재전송 공격은 도청공격으로 획득한 메시지를 이후 정당한 리더의 요청에 전송하여 스푸핑 공격 등으로 사용할 수 있지만 매 인증마다 키 값이 갱신되고 임의비표를 사용하기 때문에 상호인증이 될 수 없다.

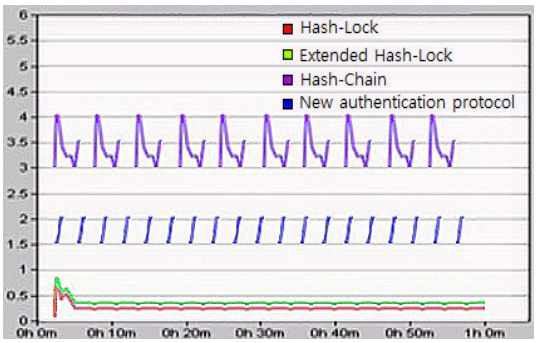

그림 6. 리더-태그간 인증 지연시간(Delay Time/sec)
Fig. 6 Authentication Delay time between Reader and Tag

그림 7은 백 엔드 서버에서 측정한 평균 데이터 처리율이며, 해시-락, 확장된 해시-락, 해시-체인 프로토콜이 제안한 프로토콜보다 약 60bits/sec 만큼 높게 나타났다. 이는 기존의 프로토콜들이 공격자의 도청공격으로 인한 재전송공격에 백 엔드 서버가 응답하고 있음을 알 수 있다.

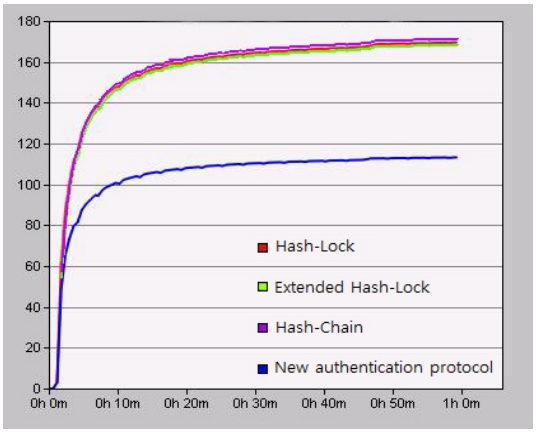

그림 7. 백 엔드 서버의 데이터 처리율(bits/sec)
Fig. 7 Data process ratio in backend server (bits/sec)

기존 프로토콜의 경우 리더와 태그의 상호인증이 이루어지지 않은 상태에서 백 엔드 서버에게 접근하기 때문에 불법적인 리더가 백 엔드 서버에게 서비스 거부 공격을 시도한다면 RFID 시스템 전체에 많은 영향을 끼친다.

제안하는 프로토콜의 경우 상호인증이 이루어진 후에 백 엔드 서버에 접근하는 방식을 가지고 있어 불법적인 리더의 서비스 거부공격을 제외한 정상적인 접근에만 응답함으로써 서비스 공격에 안정성을 보장한다.

표 3. 기존 인증 프로토콜과 제안한 프로토콜 비교 분석
Table. 3 Comparative analysis existing authentication protocol and new authentication protocol

구분	도청 공격	위치 추적 공격	스푸핑 공격	재전송 공격	서비스 거부 공격
해시-락	×	×	×	×	×
확장된 해시-락	×	○	×	×	×
해시-체인	○	○	×	○	×
제안한 프로토콜	○	○	○	○	○

○ : 안전 , × : 취약

Ⅴ. 결 론

RFID 시스템은 유비쿼터스 시대의 기반기술로써 리더와 태그 사이의 데이터 전송은 무선 주파수를 통하여 이루어지므로 여러 가지 악의적인 공격에 취약하다. 기존의 인증 프로토콜의 경우 여러 가지 공격에 안전하지 못하고 수동형 태그에 하드웨어적으로 적용하기 힘든 점이 있다.

제안하는 프로토콜은 기존의 인증프로토콜보다 AES 블록 암호화를 사용하기 때문에 연산이 많은 단점이 있으나, AES가 하드웨어적으로 제한적인 수동형 태그에 적용 가능함을 최근 연구에서 입증한 바 기존 프로토콜에서 대칭키 암호화의 키노출로 발생하는 보안적인 문제들을 해결 하였으며 특히 상호인증을 거친 후 백 엔드 서버에 접근하여 인증되지 않은 불법적인 리더의 접근을 차단하므로써 서비스 거부 공격에 강한 프로토콜이다.

참고문헌

[1] D. Lin, H. G. Elmongui, E. Bertino, and B. C. Ooi, "Data management in RFID applications", International conference on database and expert system application, LNCS 4653, 2007.

[2] Miyako Ohkubo. Koutatou Suzuki and Shingo Kinoshita, "Cryptographic Approach to Privacy-Friendly Tags.", Submitted 2003.

[3] Klaus Finkenzeller, "RFID HANDBOOK-Fundamentals and Applications in Contactless Smart Cards and Identification", Second Edition, translated by Rachel Waddington, 2002.

[4] H.Y. Chien, "Secure Access Control Schemes for RFID System with Anonymity", In Proceedings of 1005 national Workshop on Future Mobile and Ubiquitous Information Technologies. 2006.

[5] D. Henrici and P. Müuller, "Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers," Proceeding of the Second IEEE Annual Conference on Pervasive Computing and Communication Security, pp. 149-153, Mar. 2004.

[6] CRYPTOREC reports, published 2002 in Japen.
[7] M. Ohcubo, K. Suzuki, and S kinoshita, "Hash-Chain Based Forward-Secure Privacy Protection Seheme for Low-Cost RFID", Proceeding of the SCIS 2004, pp.719-724, 2004.
[8] J. Daemen, V. Rijmen, " The Design of Rijndeal," AES-The advanced Encryption Standard, Springer-Verlog, Berlin, Heidelberg, New York, 2002.
[9] 구본석, 유권호, 양상훈, 장태주, 이상진, "RFID 태그를 위한 초소형 AES 연산기의 구현", 정보보호학회논문지, 제16권, 제5호, pp.67-77, 2006. 10.
[10] J. Yang, J. Park, and K. Kim "Security and Privacy on Authentication Protocol for Low-Cost Radio", In The 2005 Symposium on Cryptography and Information Security. 2005.

저자소개

김 석(Seok Kim)

1993년 전남대학교 무기재료공학과(학사)
2008년 조선대학교 정보통신공학과(공학석사)
2008년~현재 조선대학교정보통신공학과(박사수료)
※관심분야 : 통신보안시스템설계, 네트워크 보안

한승조(Seung-jo Han)

1980년 조선대학교 전자공학과(학사)
1982년 조선대학교 전자공학과(공학석사)
1994년 충북대학교 전자계산학과 (공학박사)
1986년 6월~1987년 3월 : 뉴올리언즈대학 객원교수
1995년 2월~1996년 1월 : 택사스대학 객원교수
2000년 12월~2002년 3월 : 버클리대학 객원교수
1998년 3월~현재 : 조선대학교 전자정보통신공학부 교수
※관심분야 : 통신보안시스템설계, S/W 불법복제방지 시스템, ASIC 설계