논문 14-39B-12-03 The Journal of Korean Institute of Communications and Information Sciences '14-12 Vol.39B No.12
http://dx.doi.org/10.7840/kics.2014.39B.12.831

저비용 RFID 인증을 위한 PUF 기반 암호화 프로세서와 상호 인증 프로토콜 설계

최 원 석◆, 김 성 수*, 김 용 환**, 윤 태 진*, 안 광 선***, 한 기 준°

Design of PUF-Based Encryption Processor and Mutual Authentication Protocol for Low-Cost RFID Authentication

Wonseok Che◆, Sungsoo Kim*, Yonghwan Kim**, Taejin Yun*, Kwangseon Ahn***, Kijun Han°

요 약

RFID 시스템은 무선 통신을 이용하여 운용되기 때문에 외부의 불법적인 공격에 노출되어 있으며 이에 대한 시스템 침해의 위험성이 높다. 이러한 공격들에 대한 보안 기법들 중 PUF 기반의 인증 기법이 존재한다. 그러나 기존의 PUF 기반 기법들은 해쉬나 AES 알고리즘을 함께 이용하기 때문에, 비용 및 성능적인 측면에서 저비용 RFID 태그에 적합하지 않다. 본 논문에서는, 저비용 RFID 인증을 위하여 PUF 기반 암호화 프로세서와 이를 이용한 상호 인증 프로토콜을 제안한다. PUF의 challenge-response 쌍들을 인증키로 활용하고, 이를 PUF의 특성을 이용하여 암호화함으로써 해쉬 및 AES 등의 알고리즘 사용을 배제하였다. 매 세션마다 변경되는 암호화 방법과 일회성 난수를 이용한 XOR 연산 기법을 활용함으로써 공격자의 challenge-response 쌍에 대한 분석을 차단하여 시스템 공격을 무력화 시킨다. 또한, PUF 특성으로 인하여 물리적 공격에 강하고 태그에 저장된 인증 데이터가 존재하지 않기 때문에 물리적 공격에 의한 태그 복제 위험을 방지한다. 제안된 PUF 기반의 암호화 프로세서는 저비용으로 구현되며 저면적 및 저전력의 특징을 갖는다.

Key Words : RFID, Security, PUF, Authentication, Protocol

ABSTRACT

The attacker can access the RFID systems illegally because authentication operation on the RFID systems are performed in wireless communication. Authentication methods based on the PUF were presented to defend attacks. Because of Hash and AES, the cost is expensive for the low-cost RFID tag. In this paper, the PUF-based encryption processor and the mutual authentication protocol are proposed for low-cost RFID authentication. The challenge-response pairs (PUF's input and output) are utilized as the authentication key and encrypted by the PUF's characteristics. The encryption method is changed each session and XOR operation with random number is utilized. Therefore, it is difficult for the attacker to analyze challenge-response pairs and attack the systems. In addition, the proposed method with PUF is strong against physical attacks. And the method protects the tag cloning attack by physical attacks because there is no authentication data in the tag. Proposed processor is implemented at low cost with small footprint and low power.

◆ First Author : School of Computer Science and Engineering, Kyungpook National University, theenemys@knu.ac.kr, 학생회원
° Corresponding Author : School of Computer Science and Engineering, Kyungpook National University, kjhan@knu.ac.kr, 정회원
* Department of Mobile Engineering, Kyungwoon University, {ninny, tjyun}@ikw.ac.kr
** Department of Computer Engineering, Kyungwoon University, hypnus@ikw.ac.kr
*** School of Computer Science and Engineering, Kyungpook National University, gsahn@knu.ac.kr, 정회원
논문번호 : KICS2014-04-114, Received April 7, 2014; Revised July 2, 2014; Accepted December 8, 2014

Ⅰ. 서 론

RFID(Radio Frequency Identification) 기술은 바코드 인식 기술의 한계를 극복하는 기술이며 물류, 재고 관리, 제조 및 서비스 산업 등의 여러 분야에서 적용 범위가 확대되고 있다. RFID 시스템은 리더와 태그 간의 무선 통신을 기반으로 하는 비접촉 인식 시스템이다. 그렇기 때문에 분산된 태그들은 물리적 및 비물리적 공격에 노출되어 있고 태그에 저장된 정보는 공격자로부터 안전하지 않다. RFID 시스템의 보안 문제를 해결하기 위한 기법들 중 PUF(Physically Unclonable Function), AES(Advanced Encryption Standard), 해쉬 함수에 대하여 설명하겠다.

PUF는 하드웨어 복제 방지 기술이며 물리적 공격에 강하다. 실리콘 PUF는 각 집적회로의 게이트 및 회선 지연 시간이 다름을 활용한 기술이다. 해쉬 함수는 주어진 원문에서 고정된 길이의 의사난수를 생성하는 연산기법이다. 단방향 함수이기 때문에 해쉬값에서 원문을 재현할 수 없다. 그리고 같은 해쉬값을 가진 다른 데이터를 작성하는 것도 어렵기 때문에 통신의 암호화, 사용자 인증, 디지털 서명 등에 응용된다. AES는 대칭키 암호로써 복호화를 위하여 연산과정을 거꾸로 수행한다. 그렇기 때문에 고난도의 수학적 구조를 가진다. 블록 길이는 128비트이며 키의 길이는 128/192/256비트 중에서 선택 가능하다.

기존의 PUF 기반 인증 방법들은 해쉬와 AES를 이용하여 공격자로부터 PUF의 출력을 보호한다[1-3]. 2003년, 보안 목적용의 250-1000 게이트는 약 미화 5센트이고 보안 프로토콜과 관련 연산은 초당 100회 통신을 만족해야 한다[4]. 그러나 해쉬와 AES를 구현하는 비용은 저비용 RFID 태그에서 활용하는데 있어 비싸고 대칭키를 태그 안에 저장해야만 하는 문제가 발생된다.

본 논문에서는 PUF 기반의 암호화 프로세서와 이를 활용한 저비용 RFID 인증 프로토콜을 제안한다. PUF의 입력과 출력은 Challenge-response 쌍으로 정의되고, 이를 PUF의 특성과 일회성 난수를 이용한 XOR 연산 기법으로 암호화하여 인증키로 이용한다. 제안 기법은 물리적 공격에 강한 PUF를 활용하였고 태그 내에 인증키와 같은 저장된 인증 데이터를 필요로 하지 않는다. 그렇기 때문에 태그에는 그 어떠한 인증 데이터도 존재하지 않는다. 따라서 RFID 시스템 상에서 공격자는 challenge-response 쌍들을 예측 및 분석하여 공격하기 어려우며, 물리적 공격에 의한 태그 복제 공격 또한 불가능하다. 제안된 암호화 프로세서는 저비용으로 구현되었고 저면적과 저전력의 특징을 가진다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구로써, RFID 시스템과 이에 대한 보안 위협 요소를 소개하고 기존의 PUF 기법과 경량 RFID 상호인증 프로토콜인 M^2AP를 설명한다. 3장과 4장에서는 본 논문에서 제안하는 PUF 기반의 암호화 프로세서와 인증 프로토콜에 대하여 설명한다. 5장에서는 제안 기법의 안전성과 효율성을 분석하고 6장에서 결론을 맺는다.

Ⅱ. 관련 연구

RFID 기술은 기존의 바코드 인식 기술을 대체하여 제조업, 서비스 산업, 유통 및 재고관리 산업 분야, 자재 유통 등 다양한 분야에서 보편화 되고 있다. 바코드는 비용이 매우 싼 반면, 저장 능력이 낮고 다시 프로그래밍을 할 수 없기 때문에 부적합한 경우가 늘어나고 있다. RFID는 현재 그 응용범위를 급속히 넓혀가고 있으며, 수많은 부분에 걸쳐 우리의 생활을 바꾸어 놓을 것으로 기대된다. 이 장에서는 RFID 시스템과 구성요소에 대하여 소개하고 RFID 시스템에서 발생할 수 있는 보안 위협에 대하여 설명한다. 또한 실리콘 PUF의 기본적인 설명과 더불어 PUF를 이용한 기존의 인증 방법들과 공격 유형을 고찰하고 경량 RFID 상호인증 프로토콜인 M^2AP 프로토콜에 대하여 설명한다.

2.1 RFID 시스템

RFID 시스템은 일반적으로 세 개의 요소로 구성되어 있다. 사물에 부착하는 태그, 이를 식별하는 리더와 태그의 정보를 저장하고 있는 서버로 구성된다. 일반적으로 리더는 제어 기능과 태그와 연결 기능을 하는 무선 주파수 모듈을 가지고 있으며 추가적 인터페이스(RS232, RS485 등)가 있어서 수신된 데이터를 다른 시스템으로 송신한다. 무선 주파수 모듈은 안테나를 통하여 태그로 신호를 전달하고 태그로부터 필요한 정보를 수신하게 된다. 태그는 유일한 식별자 정보를 가지고 있으며 자신의 식별 정보를 리더에게 전송한다[5].

리더에게 전송된 식별자 정보는 서버로 전송된다. 전송된 정보는 데이터 필터링, 즉 방대한 데이터들 중에서 의미 있는 데이터를 재구성하여 데이터양을 줄여준다. 서버는 주로 소프트웨어 애플리케이션으로 구성되며 구성요소는 응용 시스템의 요구 사항에 따라

형태와 기능이 달라진다. 주요 기능은 리더의 상태 모니터링, 리더의 데이터 흐름 관리로 데이터의 활용에 관련되어 있다. 모니터링의 경우, RFID 시스템 내에서 리더의 상태를 모니터링하고 보고하는 기능으로 다양한 장소에 여러 대의 리더를 설치하고 직접 눈으로 상태를 확인하는 것이 불가능한 환경에서 매우 중요한 기능이다.

2.2 RFID 시스템

2.2.1 물리적 공격

태그의 메모리 내 정보를 추출하는 공격 기법이다. 태그는 물리적 공격에 취약하며 외부의 물리적 공격에 강인한 메모리를 사용 시 비용이 증가한다. 물리적 공격으로 대칭키가 노출 된다면 모든 태그의 정보를 무력화시키는 위험성이 있고 전체 시스템에 영향을 미친다.

2.2.2 모델링 공격

지연 기반 PUF에 대한 선형 지연 모델이 발표되었다[6]. 이 공격 방법은 경로의 지연 시간 차이와 물리적 파라미터들을 이용한다. Challenge-response 쌍의 크기가 작고 공격자가 만든 challenge-response 쌍의 수가 많을수록 공격 성공 횟수가 높아졌다. 이 공격 실험은 매트랩 툴을 이용하여 수행되었다[7].

2.2.3 스푸핑 공격

공격자는 도청을 통하여 태그에서 전송하는 고유 정보를 얻는다. 그 이후 리더의 요청에 대해 공격자는 정상 태그를 대신하여 자신이 이전에 도청을 통하여 얻었던 정보로 응답한다. 따라서 공격자는 정당한 태그인척 위장하여 리더를 속일 수 있다.

2.2.4 위치 추적 공격

사용자가 태그가 부착된 상품을 소지하고 있을 경우 태그의 고유 식별 정보를 통하여 사용자와 연관성을 줄 수 있고 리더의 요청에 대하여 태그가 항상 동일한 값으로 응답 한다면 공격자는 사용자가 소지한 특정 상품의 도청을 통하여 이동경로를 추적하여 프라이버시를 침해 할 수 있다. 위치 추적 문제를 해결하기 위해서는 태그는 리더의 요청에 대하여 항상 다른 값을 전송하여야 한다.

2.2.5 중간자 공격

정당한 인증 개체인 것처럼 위장 후, 통신하고있는 리더와 태그 간에 끼어든다. 그리고 리더와 태그가 교환하는 통신 데이터를 자신의 데이터로 변경하여 조작함으로써 도청 및 통신 내용을 변경시키는 공격이다.

2.3 Physically Unclonable Function

PUF는 물리적 구조로 구성되어 있으며 PUF의 출력을 예측하기 어렵다. 또한, 구현은 쉽지만 복제가 불가능해야 한다. 이러한 측면에서 PUF는 단방향 함수의 성질을 갖는 아날로그 시스템이다[8]. 본 절에서는 실리콘 PUF에 대하여 설명하고 기존의 PUF 관련 연구를 기술한다.

2.3.1 실리콘 PUF

실리콘 PUF는 각 집적회로 고유의 물리적 특성들을 이용한다. 공정 과정에 의하여 각 집적회로는 각기 다른 게이트와 회선의 지연 시간을 가지게 된다. 따라서 같은 로직 설계임에 불구하고 각 PUF의 게이트와 회선의 지연 시간은 달라진다. 이러한 물리적 특성들 때문에 PUF를 복제하는 것은 어렵다.

본 논문에서는 그림 1과 같은 arbiter 기반의 PUF를 이용한다. 이것은 스위칭 박스들과 arbiter로 구성되어 있다. Arbiter 기반의 PUF는 저비용 RFID 태그와 같은 제한된 자원을 가진 플랫폼에 적합하다[2].

각 스위칭 박스는 2개의 MUX로 구현되었고 arbiter는 latch로 구현되었다. Arbiter 기반의 PUF는 같은 레이아웃 길이를 가지는 두 개의 경로(상단 경로와 하단 경로)를 가지고 있다. 두 경로는 서로 다른 지연 시간을 가지고 있기 때문에 각 경로의 신호가 arbiter에 도달하는 시간은 다르다. Arbiter는 어떤 경로의 신호가 더 빨리 도달하는지에 따라 1비트의 출력 값을 결정한다.

상승 신호가 상단 및 하단 경로로 동시에 입력되고 각 C[i]는 스윗칭 박스들의 MUX에 입력된다. C[i]가 0이면 상단 신호와 하단 신호는 현재 경로를 유지하고 1이면 상단 신호는 하단 경로로 이동하고 하단 신호는 상단 경로로 이동한다. 이와 같은 방식으로 상단 신호와 하단 신호는 서로 경쟁하며 arbiter에 도달하게 된다. Latch의 D 입력인 상단 신호가 더 빨리 도달 한

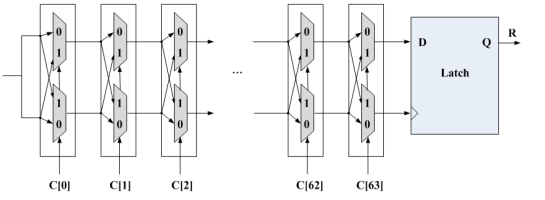


그림 1. Arbiter 기반 PUF
Fig. 1. Arbiter-based PUF

다면 출력 값은 1이 되고 하단 신호가 더 빠르다면 출력 값은 0이 된다.

2.3.2 랜덤 해쉬를 이용한 PUF 구조

그림 2는 랜덤 해쉬 기반의 PUF 구조를 나타낸다. PUF는 아날로그 시스템 기반이기 때문에 노이즈를 가지고 있다. Challenge에 대한 Response가 조금씩 변경된다는 의미이다. Challenge-response 쌍들을 암호 키로 사용하기 위해서는 challenge에 대한 response를 고정시켜야 한다[1].

이 문제에 대한 해결책으로 BCH code, RS code와 같은 오류 정정 부호(Error Correction Code)가 이용될 수 있다. Challenge-response 쌍이 생성될 때 redundancy 정보를 추출할 수 있고 이것은 response를 정정하는데 이용된다. 이를 통해 PUF는 동일한 challenge-response 쌍들을 생성할 수 있다[1,2].

물리적 파라미터들은 PUF를 정의한다. 만약 공격자가 물리적 파라미터의 정보를 알아낸다면 PUF 복제는 가능해진다. 이 파라미터들을 모델화하기 위하여 공격자는 challenge-response 쌍들의 분석을 시도할 수 있다. 그렇기 때문에 저자는 이러한 공격을 막기 위하여 랜덤 해쉬를 이용한다. 랜덤 해쉬는 단방향 함수이다. 그러므로 공격자는 랜덤 해쉬에 의하여 연산된 response를 분석하는 것이 어려워진다[1].

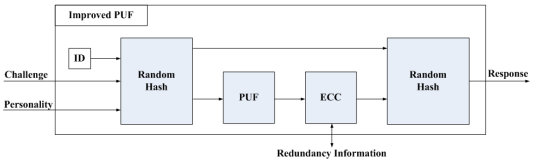


그림 2. 개선된 PUF
Fig. 2. Improved PUF

2.3.3 저비용 인증 방법

각 PUF의 출력 값은 다르다. 따라서 challenge-response 쌍들은 인증에 사용될 수 있다. PUF의 1비트 출력은 적합하지 않고 지수 형식의 challenge-response 쌍들이 인증에 활용된다.

Challenge-response 쌍들은 데이터베이스에 저장된다. 인증이 수행될 때 challenge에 대한 response를 수신한 뒤 데이터베이스에 저장된 해당 response와 동일한지 비교한다. 중간자 공격을 막기 위하여 이미 인증에 사용된 challenge-response 쌍들은 재사용되지 않는다[2].

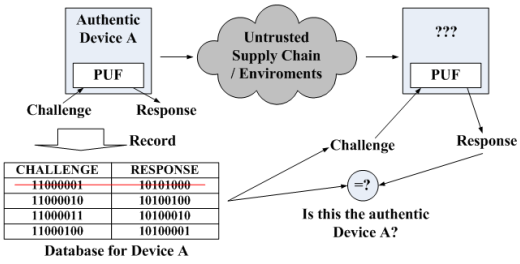


그림 3. PUF 기반의 인증 방법
Fig. 3. PUF-based authentication method

2.4 경량 RFID 인증 프로토콜

Peris-Lopez 외 3명은 경량 RFID 상호인증 프로토콜인 M^2AP[12]를 발표하였고 해당 프로토콜은 그림 4와 같다. 각 태그는 96-bit IDS(Index-pseudonym)와 4개의 파트로 이루어진 96-bit key인 K(K = K1 ‖ K2 ‖ K3 ‖ K4)를 저장하고 있다. 상호인증 프로토콜을 수행하기 전, 리더는 태그로부터 IDS를 수신한다. 그림 4와 같이, 상호인증 단계에서 태그는 리더로부터 $IDS_{tag(i)}^{(n)} \oplus K1_{tag(i)}^{(n)} \oplus n1 \| (IDS_{tag(i)}^{(n)} \wedge K2_{tag(i)}^{(n)}) \vee n1$ 메시지를 수신하여 리더 인증 여부를 결정한다. 태그는 리더를 인증한 후에 그림 4와 같이 메시지를 전송하면 리더는 태그의 인증 여부를 결정하고 상호 인증이 완료되면 IDS와 K의 갱신 작업을 수행한다.

그림 4. M^2AP 프로토콜
Fig. 4. M^2AP protocol

Ⅲ. PUF 기반 암호화 프로세서

2장에서 언급된 기존 방법들은 해쉬와 AES를 이용하여 PUF의 출력을 암호화한다. 그러나 이 방법들은 해쉬와 암호화 기능에 대한 로직 구현과 연산에 대한 비용 증가를 초래할 수 밖에 없으며 저비용 RFID 태그에 부적합하다. 또한 태그 안에 저장된 대칭키는 비휘발성 데이터로 존재함으로써 공격에 노출되어 있다.

본 논문은 PUF 기반의 암호화 프로세서 [19]와 이를 활용한 저비용 RFID 인증 프로토콜을 제안한다. Challenge-response 쌍들은 제안 프로세서 안에 휘발성 데이터로써 존재하고 이를 인증키로 활용한다. 서버는 암호화된 challenge를 태그에 부착된 제안 프로

세서로 전송한다. 프로세서는 response를 생성하고 이를 암호화하여 서버로 전송한다. 각 response는 유일하기 때문에 서버는 challenge-response 쌍들을 이용하여 각 태그를 구별하고 인증한다.

여러 유형의 공격들을 막기 위하여 서버는 challenge를 암호화하고 제안된 암호화 프로세서는 response를 암호화한다. Challenge-response 쌍들은 PUF의 특성들로 암호화되고 이 암호화 방법은 매회 변경된다. 따라서 암호화된 challenge-response 쌍들은 항상 다르다.

3.1 프로세서 구조

PUF 기반의 암호화 프로세서는 암호화된 challenge를 복호화하고 arbiter 기반 PUF와 N비트 병렬 입력/병렬 출력 시프트 레지스터를 이용하여 response를 생성한다. 본 논문에서는 D 플립플랍을 이용하여 arbiter를 구현하였다. 최종적으로 response를 암호화하여 출력한다.

Arbiter 기반의 PUF는 N비트 challenge로부터 1비트 response를 생성한다. N비트 response를 출력하기 위하여 입력된 challenge는 N번 변경되어야 한다. N비트 병렬 입력/ 병렬 출력 시프트 레지스터를 이용하여 challenge를 변경시킨다. 그림 5는 제안된 N비트 PUF의 구조를 보여준다. C(Challenge)가 N비트 병렬 입력/병렬 출력 시프트 레지스터에 입력되고 레지스터는 $C_0^{'}$을 출력한다. 이 때, $C_0^{'}$와 C는 동일하다. Arbiter 기반 PUF는 $C_0^{'}$로부터 $R_0^{'}$을 생성한다. $R_0^{'}$은 레지스터의 LSB 플립플랍에 시프트되고 레지스터는 $C_1^{'}$을 출력한다. 위 방식을 N번 반복하면 $R_{N-1}^{'}$이 레지스터에 시프트 될 때 N비트 response가 생성된다. $R_i^{'}$는 유일하고 이것을 challenge에 시프트함으로써

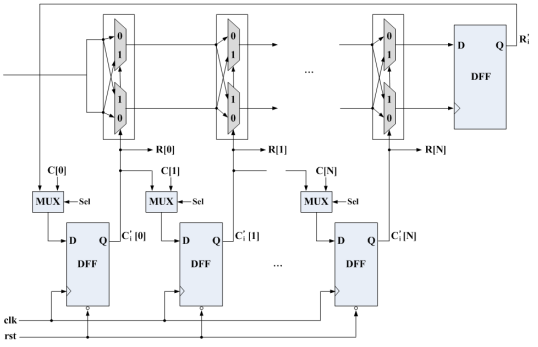


그림 5. 제안된 N비트 PUF
Fig. 5. Proposed N-bit PUF

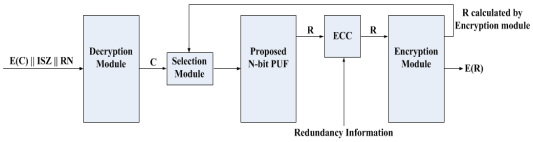


그림 6. 제안된 PUF 기반 암호화 프로세서
Fig. 6. Proposed PUF-based encryption processor

N비트 response를 생성한다. 따라서 N비트 response는 유일하다.

PUF 기반의 암호화 프로세서는 제안된 N비트 PUF를 이용한다. 그리고 ECC, 암호화 및 복호화 모듈을 가지고 있다. E(C)는 암호화된 challenge를 의미하고 ISZ는 instruction 크기를 의미한다. RN은 난수를 의미하고 R은 response를 의미한다. ISZ와 RN을 연접한 암호화된 challenge는 복호화 모듈에 전송된다. 복호화 모듈은 ISZ와 RN을 이용하여 E(C)를 복호화하고 challenge를 N비트 PUF에 입력한다. N비트 PUF는 response를 생성한 뒤 ECC 모듈에 입력한다. 노이즈가 발생되기 때문에 ECC 모듈을 통하여 response의 오류를 정정한다. 암호화 모듈은 정정된 response를 암호화하여 출력한다. 다음 장에서 암호화 및 복호화 모듈에 대하여 상세히 설명하겠다.

3.2 암호화 모듈

암호화된 challenge가 PUF 기반 암호화 프로세서로 전송될 때 instruction 크기 값과 난수가 함께 전송된다. Response의 특정 비트들은 instruction field로 결정된다. Instruction field는 response 내의 분산된 비트들로 구성된다. 그림 7은 instruction field 구조의 한 예를 보여준다.

기호 는 배타적 OR 연산자를 의미하고 기호 ‖ 는 연접 연산자를 의미한다.

Instruction 크기가 2일 때,

$$Instruction\ code' = R[1] \oplus R[0] \tag{1}$$

Instruction 크기가 4일 때,

$$Instruction\ code' = R[6] \oplus R[5] \| R[1] \oplus R[0] \tag{2}$$

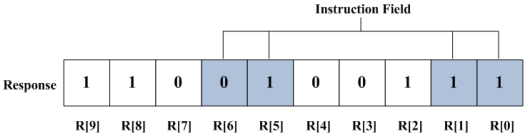


그림 7. Instruction field의 예
Fig. 7. An example of instruction field

Instruction code'는 instruction 크기 값에 의하여 변경된다. Instruction code'가 생성된 후 이것은 난수와 함께 배타적 OR 연산이 수행된다.

$$Instruction\ code = Instruction\ code' \oplus Random\ number \quad (3)$$

그림 7의 예를 설명하면, instruction 크기가 4일 때 instruction code'의 이진 값은 10이다. 그리고 난수의 이진 값은 11이라고 가정한다. $10 \oplus 11$의 연산 결과는 01이다. 따라서 instruction code의 이진 값은 01이다.

Response의 암호화 방법은 bitwise NOT, circular shift, feedback 연산들로 구성된다. Bitwise NOT 연산 방법은 instruction code에 의하여 변경된다. Instruction 크기가 N이고 난수가 N/2비트라면 instruction code 종류의 수는 $2^{N/2}$이다. 따라서 Bitwise NOT 연산 방법의 수는 $2^{N/2}$이다.

Response 내의 특정 비트들은 bitwise NOT과 circular shift 연산들의 대상이 된다. Instruction field는 이 연산들의 대상에 포함되지 않는다. Bitwise NOT과 circular shift 연산들이 수행된 후 response는 feedback 연산에 의하여 N비트 PUF에 입력된다.

그림 8은 response에 대한 bitwise NOT과 circular shift 연산들의 예를 보여주고 있다. R[3]과 R[8]은 bitwise NOT 연산에 의하여 반전된다. R[2]~R[4]와 R[7]~R[9]는 left circular shift 연산이 수행된다. R[0], R[1], R[5] 그리고 R[6]은 instruction field이기 때문에 연산 대상에서 제외된다.

Response는 bitwise NOT과 circular shift 연산들에 의하여 연산된 후에 feedback 연산에 의하여 N비트 PUF로 입력된다. 셀렉션 모듈은 challenge 대신에 response를 N비트 PUF에 입력한다. Feedback 연산을

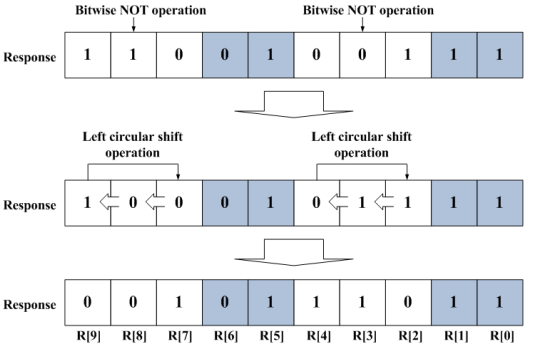


그림 8. Bitwise NOT과 circular shift 연산들의 예
Fig. 8. An example of bitwise NOT and circular shift operations

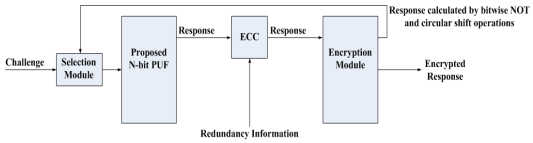


그림 9. Feedback 연산
Fig. 9. Feedback operation

마지막으로 response는 암호화된다.

3.3 복호화 모듈

Challenge의 특정 비트들은 instruction field로 셋팅된다. 서버에서는 (1), (2)와 (3)의 연산 과정을 통하여 instruction code가 생성된다. Challenge에 대한 암호화 방법은 bitwise NOT과 circular shift 연산들로 구성되며 instruction code에 의하여 변경된다. Challenge와 response의 암호화 방법의 수는 동일하다. 서버는 challenge를 암호화 한 뒤 instruction 크기 값과 난수를 연접하여 PUF 기반 암호화 프로세서로 전송한다.

암호화 프로세서는 수신한 instruction 크기 값과 난수를 이용하여 암호화된 challenge를 복호화한다. Bitwise NOT과 circular shift 연산들을 역연산함으로써 challenge를 복호화한다.

그림 10은 challenge의 복호화에 대한 bitwise NOT과 circular shift 연산들의 예를 보여주고 있다. C[2]~C[4]와 C[7]~C[9]는 right circular shift 연산이 수행된다. 그리고 C[3]과 C[8]은 bitwise NOT 연산에 의하여 반전된다. C[0], C[1], C[5] 그리고 C[6]은 instruction field이기 때문에 연산 대상에서 제외된다.

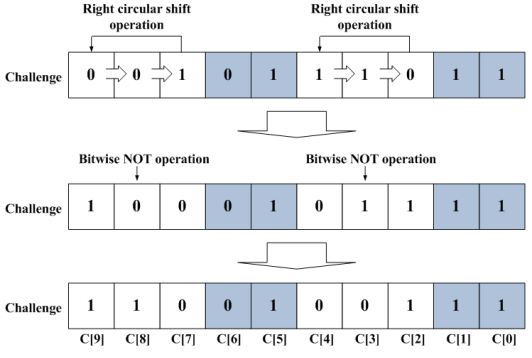


그림 10. Challenge의 복호화 과정에 대한 예
Fig. 10. An example of decryption process for challenge

3.4 구현 결과

본 논문에서 제안된 PUF 기반의 암호화 프로세서

는 Xilinx Spartan 2 FPGA를 대상으로 Verilog HDL을 사용하여 구현되었다. Xilinx ISE 툴을 이용하여 설계하였고 ModelSim 툴을 이용하여 시뮬레이션 하였다. ECC(Error Correcting Code) 모듈은 구현에서 제외되었다. 표 1은 암호화 방법의 수에 따른 게이트와 클럭 사이클의 수를 보여준다. 면적과 전력 측면에서 제안 방법의 비용이 낮은 것을 확인할 수 있다.

표 1. 프로세서 하드웨어 크기 및 처리 시간
Table 1. Gate size and clock cycles for the processor

	32-bit challenge		64-bit challenge	
Instruction field size	8	10	10	12
Gates	1,219	1,242	2,323	2,369
Clock cycles	135		263	

Ⅳ. 상호 인증 프로토콜

4.1 표기법

표 2는 인증 프로토콜에서 사용되는 표기법을 나타낸다.

표 2. 표기법
Table 2. Notation

C	Challenge
R	Response
E()	Encryption
D()	Decryption
ISZ	Instruction size
RS	Random number generated by server
RD	Random number generated by reader
RT	Random number generated by tag
⊕	XOR operator
‖	Concatenation operator

4.2 초기화 단계

각 PUF 기반 암호화 프로세서는 RFID 태그에 부착되며 그 기능은 제안 프로토콜에 사용될 수 있도록 확장된다. 서버에서는 instruction 크기 값과 난수에 따른 challenge-response 쌍들이 데이터베이스에 저장되어 있다. 그리고 리더는 난수에 대한 Challenge-response 쌍들을 가지고 있다. Challenge-response 쌍들을 이용하여 각 태그를 인증하기 때문에 하나의 challenge에 대하여 모든 response는 서로 다르다. 서버는 데이터베이스에 저장된 challenge-response 쌍들을 이용하여 인증 작업을 수행한다. 서버가 challenge를 태그로 전송할 때마다 challenge는 무작위로 선택된다. 난수 또한 전송될 때마다 새롭게 갱신된다.

4.3 제안 프로토콜

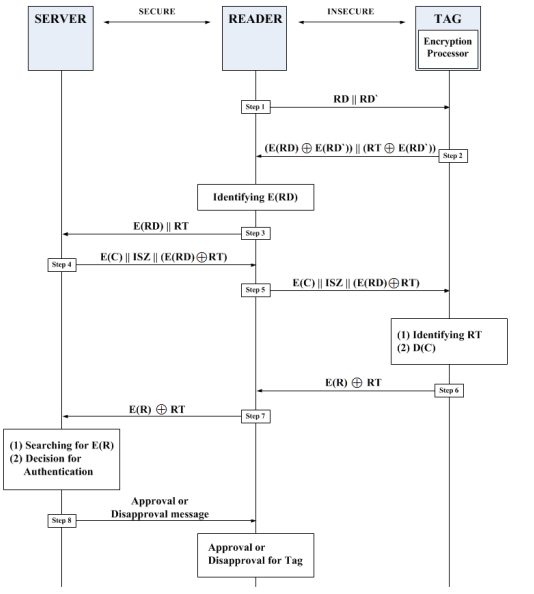


그림 11. 제안된 RFID 상호 인증 프로토콜
Fig. 11. Proposed mutual authentication protocol

4.3.1 Step 1

리더는 태그에게 난수 RD, RD‘를 연접하여 전송한다.

4.3.2 Step 2

태그는 리더로부터 수신받은 RD, RD‘를 암호화하여 E(RD)와 E(RD‘)를 생성한 후, 난수 RT를 생성한다. E(RD)와 RT에 대하여 각각 E(RD‘)를 이용하여 XOR 연산을 한 뒤, 연산된 E(RD)와 RT를 연접하여 리더로 전송한다.

4.3.3 Step 3

리더는 태그로부터 E(RD‘)로 XOR 연산된 E(RD)와 RT를 수신한다. 리더는 E(RD‘)를 이미 가지고 있으므로 이 값을 이용하여 E(RD)와 RT로 복호화한다. 태그는 리더가 전송한 RD에 대한 E(RD)를 전송하였으므로 리더는 정당한 태그로 인증한다. 이 후, 서버로 E(RD)와 RT를 연접하여 전송한다.

4.3.4 Step 4

서버는 E(C)와 이에 대한 instruction size, ISZ, 그

리고 RT와 XOR 연산된 E(RD)를 연접하여 리더로 전송한다.

4.3.5 Step 5

리더는 서버로부터 수신한 E(C), ISZ, 그리고 RT와 XOR 연산된 E(RD)를 태그로 전송한다.

4.3.6 Step 6

태그는 Step 2로부터 E(RD)를 가지고 있으므로 이를 이용하여 RT의 수신 여부를 확인할 수 있다. 태그는 정당한 RT를 수신하였다면 정당한 리더로 인증한다. 그리고 ISZ, E(RD)를 이용하여 E(C)를 복호화한 뒤, R을 암호화한다. 태그는 암호화된 R에 대하여 RT를 XOR 연산한 뒤, 이를 리더로 전송한다.

4.3.7 Step 7

리더는 태그로부터 수신한 RT와 XOR 연산된 E(R)을 서버로 전송한다.

4.1.8 Step 8

서버는 RT를 가지고 있으므로 이를 이용하여 RT와 XOR 연산된 E(R)로부터 E(R)을 복호화 한다. 서버는 기전송한 E(C)에 대한 E(R)이 일치하는지 확인하고 정당한 태그로 인증한다. 이후, 서버는 리더로 태그 승인 메시지를 전송한다.

V. 성능 비교 및 분석

5.1 보안성 비교분석

본 논문에서는 PUF의 특성들을 이용하여 challenge-response 쌍들을 암호화한다. 첫 번째 특성은 PUF의 물리적 특성이다. 제안된 N비트 PUF는 PUF의 물리적 특성으로 설계되었고 이것을 이용하여 response를 암호화하였다. 두 번째 특성은 challenge-response 쌍들이다. 동일한 challenge임에 불구하고 각 PUF는 유일한 response를 생성한다. 그렇기 때문에 challenge-response 쌍들을 서로 다르게 암호화된다. 또한 일회성 난수를 이용하여 challenge-response 쌍들을 암호화함으로써 불법적인 공격을 차단한다.

RFID 인증 작업이 수행될 때 공격자들이 무선 통신 상에서 도청할 수 있는 유효한 데이터는 오직 암호화된 Challenge-response 쌍들뿐이다. RFID 태그는 어떠한 정보도 저장하고 있지 않으며 서버 측 데이터베이스 내에 태그 정보가 저장되어 있다. 따라서 태그와 프로토콜에 대한 공격이 성공한다 하더라도 공격자는 어떠한 태그 정보도 취득할 수 없다.

본 절에서는, 제안 기법이 해결할 수 있는 물리적 공격, 모델링 공격, 중간자 공격, 스푸핑 공격, 재전송 공격, 위치 추적 공격, 상호 인증에 대한 보안성을 분석하여 기술한다. 그리고 제안 프로토콜과 2장에서 기술된 경량 RFID 상호인증 프로토콜인 M^2AP 프로토콜의 보안성을 비교 분석한다.

5.1.1 물리적 공격

Response는 bitwise NOT과 circular shift 연산들에 의하여 계산되어진 후 feedback 연산에의하여 N비트 PUF로 입력된다. 이 방법으로 response는 암호화된다. 암호화된 response는 휘발성 메모리에 저장되고 이 메모리는 접근할 수 없도록 설정된다[7]. 또한 태그는 비밀 키와 같은 인증 관련 데이터를 저장하지 않는다. 그렇기 때문에 공격자는 물리적 공격을 통하여 response나 암호화된 response를 추출하기 어렵고 인증 관련 데이터를 취득할 수 없다. 이를 통해 물리적 공격으로부터 인증 키 관리 문제를 해결하였다.

5.1.2 모델링 공격

공격자는 challenge-response 쌍들을 도청하여 PUF의 물리적 파라미터들에 대한 분석을 시도 할 수 있다[2,9]. 그렇지만 challenge가 아닌 response를 이용하여 암호화하였기 때문에 모델링 공격을 차단한다.

5.1.3 중간자 공격

본 제안 기법에서는 매 세션마다 갱신되는 challenge-response 쌍들과 일회성 난수를 이용하여 암호화하고 상호 인증을 수행한다. 태그는 RD, RD'를 암호화 한 뒤 일회성 난수를 이용하여 XOR 연산 후, 이를 리더에게 전송하기 때문에 공격자는 리더의 E(RD)와 태그의 난수를 분석하여 추출할 수 없다. 또한, 매 세션마다 해당 값이 변경되기 때문에 데이터 재사용을 통한 공격도 불가능하다.

5.1.4 스푸핑 공격

공격자는 challenge-response 쌍들을 복제하여 스푸핑 공격을 시도할 수 있다. 제안 기법에서는, 매 세션마다 갱신되는 challenge-response 쌍들과 일회성 난수를 이용하여 암호화하고 전송한다. 따라서 공격자는 불법적으로 취득한 challenge-response 쌍들의 분석과 데이터의 재사용이 불가능하다.

5.1.5 재전송 공격

제안된 암호화 프로세서를 통한 암호화 방법과 일회성 난수를 이용한 XOR 연산을 이용하여 데이터를

암호화한다. 따라서 리더와 태그 간 insecure 채널 통신에서의 데이터는 항상 갱신되며 재사용되지 않기 때문에 재전송 공격이 불가능하다.

5.1.6 위치 추적

서버와 태그는 암호화된 challenge-response 쌍을 상호 간 전송할 때 난수를 이용한다. 암호화된 challenge-response 쌍과 난수는 전송 될때 마다 갱신되기 때문에 위치 추적 문제를 해결한다.

5.1.7 상호 인증

서버와 태그는 상호 간의 난수를 이용하여 상호 인증을 수행한다. 리더는 태그로 난수 RD를 전송하고 해당 난수에 대한 E(RD)를 수신함으로써 태그를 인증한다. E(RD)는 태그의 response와 난수와 연산되어 전송되므로 공격자에게 노출되지 않는다. 태그는 생성한 난수를 리더로 전송한 뒤, 해당 리더가 태그 난수를 다시 전송했다면 리더를 인증한다. 태그 난수는 암호화된 리더 난수 E(RD), E(RD')와 XOR 연산하여 전송되기 때문에 안전하다.

제안 프로토콜과 경량 RFID 상호인증 프로토콜 M^2AP의 보안성을 비교 분석한 결과는 표 3과 같다. M^2AP 프로토콜은 리더의 난수와 IDS 및 K의 갱신 방법을 이용하기 때문에 재전송 공격, 위치 추적 공격, 도청 공격에 안전하다. 그러나 태그는 리더로 IDS를 전송하므로 공격자에게 노출될 수 있으며 리더의 난수만으로 상호 인증을 수행하므로 이 또한 안전한 상호 인증 방법이 아니다. 공격자의 IDS 및 인증 관련 데이터의 도청 및 분석이 용이해지기 때문에 상호 인증과 중간자 공격에 대한 취약성을 가지고 있다. 또한, 태그는 IDS 및 K를 저장하고 있으므로 물리적 공격에 안전하지 않다.

표 3. 제안 프로토콜과 M^2AP 프로토콜의 보안성 비교 분석
Table 3. Security analysis of proposed protocol and M^2AP protocols

	Proposed	M^2AP
Physical attack	Safe	Unsafe
Man-in-the-middle attack	Safe	Partially safe
Reply attack	Safe	Safe
Eavesdropping	Safe	Safe
Location tracking	Safe	Safe
Mutual Authentication	Safe	Partially safe

5.2 성능 비교

Arbiter 기반의 PUF는 N비트 challenge로부터 1비트 response를 생성한다. N비트 response를 생성하기 위해서는 레지스터가 필요하고 또한 challenge를 변경시켜 주어야 한다[2]. 본 논문에서는 N비트 병렬 입력/병렬 출력 시프트 레지스터를 사용하였다. 생성된 1비트 response를 레지스터에 시프트하는 방식으로 N비트 challenge를 변경함은 물론 N비트 response를 생성하였다. 이 방식은 비용 측면에서 효율적이다. 1비트 response는 유일하기 때문에 N비트 response 또한 유일하다.

표 4는 해쉬, AES와 제안 프로세서의 하드웨어 성능을 비교하여 나태내고 있다. MD5, SHA-1, SHA-256은 Feldhofer 등[13]이 제안하였고 AES는 Mangard 등[9]이 제안하였다. 인증 프로토콜에서 사용되는 Hash, AES 기법들의 게이트와 클럭 사이클을 비교하였을 때, 제안 프로세서의 게이트와 클럭 사이클은 가장 크기가 작은 SHA-256의 게이트 수와 MD5의 클럭 사이클 수보다 작음을 확인할 수 있다.

표 4.하드웨어 성능 비교
Table 4. Hardware performance comparison

Function	Gates	Clock cycles
MD5[13]	8,400	612
SHA-1[13]	8,120	1,274
SHA-256[13]	10,868	1,128
AES[9]	10,799	-
제안 프로세서	2,369	263

Ⅵ. 결 론

RFID 태그는 한정된 자원을 가진 플랫폼이기 때문에 저비용 인증 방법이 요구된다. 인증 기법에 사용되는 해쉬 함수나 AES를 구현할 경우, 하드웨어 비용이 커지기 때문에 저비용을 요구하는 RFID 태그에 구현하기 어렵다. 본 논문에서는 저비용 RFID 인증을 위한 PUF 기반의 암호화 프로세서와 RFID 상호 인증 프로토콜을 제안하였다. PUF의 특성과 논리 연산을 이용하여 암호화 기능을 구현하였기에 저비용으로 RFID 태그 구현이 가능하다.

본 제안 기법은 PUF의 특성을 활용하고 태그 내 저장된 인증 데이터를 필요로 하지 않기 때문에 물리적 공격에 안전하다. 또한, 상호 인증을 통하여 중간자 공격 등 여러 유형의 공격을 차단한다. 본 논문에

서는 PUF의 특성을 이용한 제안 기법이 기 언급한 불법적인 공격에 대한 보안성을 가지고 있으며 저비용 RFID 인증 시스템에 적합함을 증명하였다.

References

[1] B. Gassend, D. Clarke, M. V. Dijk, and S. Devadas, "Silicon physical random functions," in *Proc. 9th ACM Conf. Comput. Commun. Security*, pp. 148-160, USA, Nov. 2002.

[2] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. 44th Annu. ACM IEEE Design Automation Conf.,* pp. 9-14, USA, Jun. 2007.

[3] G. E. Suh, C. W. O'Donnell, and S. Devadas, "Aegis: A single-chip secure processor," *IEEE Design & Test of Computers*, vol. 24, no. 6, pp. 570-580, Nov.-Dec. 2007.

[4] S. E. Sarma, S. A. Weis, and D. W. Engels, "Radio-frequency identification: Security risks and challenges," *RSA Laboratories Cryptobytes*, vol. 6, no. 1, 2003.

[5] K. Finkenzeller, *RFID Handbook: Fundamentals and Application in Contactless Smart Cards and Identification*, 2nd Ed, NY: Wiley, 2003.

[6] B. Gassend, D. Clarke, M. V. Dijk, and S. Devadas, "Delay-based circuit authentications and applications," in *Proc. 2003 ACM Symp. Appl. Comput.*, pp. 294-301, 2003.

[7] E. Öztürk, G. Hammouri, and B. Sunar, "Towards robust low cost authentication for pervasive devices," *6th Annu. IEEE Int. Conf. Pervasive Comput. Commun.*, pp. 170-178, Mar. 2008.

[8] D. Naccache and P. Frėmanteau, "Unforgeable identification device, identification device reader and method of identification," *U.S. Patent*, no. 5,434,917, Jul. 1995.

[9] S. Mangard, M. Aigner, and S. Dominikus, "A highly regular and scalable AES hardware architecture," *IEEE Trans. Computers*, vol. 52, no. 4, Apr. 2003.

[10] M. Majzoobi, F. Koushanfar, and M. Potkonjak, "Lightweight secure PUFs," *IEEE/ACM Int. Conf. Computer-Aided Design*, pp. 670-673, Nov. 2008.

[11] D. Lim, J. W. Lee, B. Gassend, G. E. Suh, M. V. Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," *IEEE Trans. Very Large Scale Integration (VLSI) Syst.*, vol. 13, pp. 1200-1205, Oct. 2005.

[12] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda, "A minimalist mutual-authentication protocol for low-cost RFID tags," *Ubiquitous Intelligence and Computing*, vol. 4159, pp. 912-923, 2006.

[13] M. Feldhofer and C. Rechberger, "A case against currently used hash functions in RFID protocols," *OTM Workshops 2006*, vol. 4277, pp. 372-381, 2006.

[14] Y. K. Lee, K. Sakiyama, L. Batina, and I. Verbauwhede, "Elliptic-curve-based Security Processor for RFID," *IEEE Trans. Computers*, vol. 57, no. 11, Nov. 2008.

[15] M. Stamp, *Information Security Textbook (Principles And Practice)*, 1st Ed., NY: John Willey & Sons Inc., 2005.

[16] S. Oh, K. Chung, T. Yun, and K. Ahn, "An RFID mutual authentication protocol using one-time random number," *J. KICS*, vol. 36, no. 7, pp. 858-867, 2011.

[17] J. Shin, S. Oh, C. Jeong, K. Chung, and K. Ahn, "Improved an RFID mutual authentication protocol based on hash function," *J. KICS*, vol. 37C, no. 3, 2012.

[18] J. Lee, S. Oh, T. Yun, K. Chung, and K. Ahn, "An ultra-lightweight RFID authentication protocol using index," *J. KICS*, vol. 37C, no. 1, 2012.

[19] W. Choi, S. Kim, Y. Kim, Y. Park, and K. Ahn, "PUF-based encryption processor for the RFID systems," *2010 IEEE 10th Int. Conf. Comput. Inf. Technol(CIT).*, pp. 2323-2328, Bradford, Jun.-Jul. 2010.

최 원 석 (Wonseok Che)

2007년 2월 : 안동대학교 컴퓨터공학과 학사
2011년 2월 : 경북대학교 전자전기컴퓨터학부 석사
2013년 3월~현재 : 경북대학교 컴퓨터학부 박사과정
<관심분야> RFID, 임베디드 시스템, Security

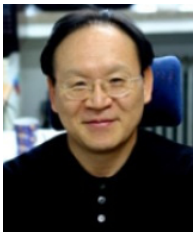
윤 태 진 (Taejin Yun)

1994년 2월 : 경북대학교 컴퓨터공학과 학사
1996년 2월 : 경북대학교 컴퓨터공학과 석사
2012년 2월 : 경북대학교 컴퓨터공학과 박사
현재 : 경운대학교 모바일공학과 부교수
<관심분야> 임베디드 시스템, 정보보안

김 성 수 (Sungsoo Kim)

2002년 2월 : 금오공과대학교 컴퓨터공학과 학사
2005년 2월 : 경북대학교 컴퓨터공학과 석사
2012년 2월 : 경북대학교 컴퓨터공학과 박사
2013년~현재 : 경운대학교 모바일공학과 조교수
<관심분야> 임베디드 시스템, RFID, 센서 네트워크

안 광 선 (Kwangseon Ahn)



1972년 2월 : 연세대학교 전기공학과 학사
1975년 2월 : 연세대학교 전자공학과 석사
1980년 2월 : 연세대학교 전자공학과 박사
1977년 3월~2014년 8월 : 경북대학교 컴퓨터학부 교수
<관심분야> 임베디드 시스템 설계, RFID

김 용 환 (Yonghwan Kim)

2004년 2월 : 경운대학교 컴퓨터공학과 학사
2006년 2월 : 경북대학교 컴퓨터공학과 석사
2013년 2월 : 경북대학교 컴퓨터공학과 박사
2012년~현재 : 경운대학교 컴퓨터공학과 연구교수
<관심분야> RFID, 임베디드 시스템

한 기 준 (Kijun Han)

1979년 2월 : 서울대학교 전기공학과 학사
1981년 2월 : KAIST 전기 및 전자공학과 석사
1985년 2월 : University of Arizona, Dept. of ECE (M.S.)
1987년 2월 : University of Arizona, Dept. of ECE (Ph.D.)
1988년~현재 : 경북대학교 컴퓨터학부 교수
<관심분야> 무선 네트워크