Journal of the Korea Academia-Industrial cooperation Society
Vol. 14, No. 3 pp. 1393-1401, 2013

http://dx.doi.org/10.5762/KAIS.2013.14.3.1393

13.56Mhz RFID 환경에서 안전한 보안 스킴 구축을 위한 암호 스킴 및 보안 프로토콜 연구

강정호[1], 김형주[1], 이재식[1], 박재표[2], 전문석[1*]
[1]숭실대학교 컴퓨터학과, [2]숭실대학교 정보과학대학원

A Study on Cryptography Scheme and Secure Protocol for Safety Secure Scheme Construction in 13.56Mhz RFID

Jung-Ho Kang[1], Hyung-Joo Kim[1], Jae-Sik Lee[1], Jae-Pyo Park[2] and Moon-Seog Jun[1*]
[1]**Department of Computer Science, Soongsil University**
[2]**Graduate School of Information Science, Soongsil University**

요 약 RFID란 개체에 Micro Chip이 내장된 태그를 부착하여 리더를 통해 개체를 인식한 후 서버와의 통신을 통해 개체를 인증하는 기술을 총칭한다. 다양한 RFID 태그 중, ISO/IEC 14443 표준 기반의 NXP사의 Mifare 태그는 13.56Mhz 대역의 RFID 카드로, 전 세계 시장의 72.5%를 점유하고 있다. Mifare 태그 중, 저가 태그인 Mifare Classic 태그는 제한적인 하드웨어 연산을 기반으로 보안이 제공됨에 따라, 다양한 공격에 의해 프로토콜 노출 및 키 복구 취약점이 발생하였다. 이에 본 논문에서는 13.56Mhz RFID 환경에서 안전한 보안 스킴 구축을 위한 암호 스킴 및 보안 프로토콜을 설계하였다. 제안하는 보안 스킴은 KS 생성 시 다양한 고정값과 비고정값을 사용하고, S-Box 연산을 수행하며, LFSR 연산과 S-Box 연산에 사용되는 값을 교차시켜, 기존 보안 스킴의 취약점과 스푸핑, 재생 공격과 같은 일반적인 RFID 보안 요구사항을 만족한다. 또한, 제한된 하드웨어 연산 능력과 기존 보안 스킴의 연장선상에서 설계되어, 현재 사용되는 Mifare Classic에 바로 적용 가능하다.

Abstract What is RFID Microchip tag attached to an object, the reader recognizes technology collectively, through communication with the server to authenticate the object. A variety of RFID tags, 13.56Mhz bandwidth RFID card, ISO/IEC 14443 standards based on NXP's Mifare tag occupies 72.5% of the world market. Of the Mifare tags, low cost tag Mifare Classic tag provided in accordance with the limited hardware-based security operations, protocol leaked by a variety of attacks and key recovery vulnerability exists. Therefore, in this paper, Cryptography Scheme and Secure Protocol for Safety Secure Scheme Construction in 13.56Mhz RFID have been designed. The proposed security scheme that KS generated by various fixed values and non-fixed value, S-Box operated, values crossed between LFSR and S-Box is fully satisfied spoofing, replay attacks, such as vulnerability of existing security and general RFID secure requirement. Also, It is designed by considering the limited hardware computational capabilities and existing security schemes, so it could be suit to Mifare Classic now.

Key Words : Cryptography Scheme, Mifare Classic, RFID, Secure Protocol, Secure Scheme

1. 서론

Radio Frequency Identification(이하 RFID)란 개체에 칩이 내장된 전자태그와 통신을 위한 안테나를 부착하여 리더에서 Radio Frequency(이하 RF)통신을 통해 개체를 인식한 후, 서버와 통신을 통해 개체를 인증하는 기술이

*Corresponding Author : Moon-Seog Jun(Soongsil Univ.)
Tel: +82-2-826-6526 email: mjun@ssu.ac.kr
Received February 13, 2013 Revised February 27, 2013 Accepted March 7, 2013

다. 초기 RFID 시스템은 기존의 바코드를 대체하는 형태로만 사용되었지만, 현재에는 교통, 출입통제 및 전자 결제, 물류, 유통 관리 등 생활 속 다양한 분야에서 LF(Low Frequency), HF(High Frequency), UHF(Ultra-High Frequency), 마이크로파(Micro-Frequency) 대역 별로 나뉘어 사용 중에 있다.

총 네 가지 RF 대역 중 13.56MHz 대역을 사용하는 HF 대역은, 다시 ISO/IEC 14443[1-4], ISO/IEC 15693, ISO/IEC 18092 표준을 기반으로 세 가지 분야로 나뉘게 된다. ISO/IEC 14443 표준은 비접촉식 근거리(Contactless Proximity) 무선통신 기술로 10cm 이내에서 태그 인식이 가능하며, 교통, 금융거래, 출입통제용 스마트카드(Smart Card)에 적용되는 대표적인 표준이다. ISO/IEC 15693 표준은 비접촉식 주변형(Contactless Vicinity) 기술로 1m 내외에서 태그 인식이 가능해, 항공화물인식 등의 스마트 레이블에 주로 활용되고 있다. ISO/IEC 18092 표준은 자기장 커플링 방식의 통신 기술로 NFC(Near Field Communication) 표준의 전신이다.

세 가지 표준 중 ISO/IEC 14443 표준을 기반으로 제작된 NXP사의 Mifare 태그는 국내·외 교통카드 및 출입통제 카드 용도로 사용되고 있으며, 2007년 NXP에 따르면 전 세계시장의 72.5%를 점유하고 있는 가장 대표적인 RFID 카드이다[5]. Mifare 태그 기반 RFID 태그 중 Mifare Classic 태그는 교통카드 및 간단한 출입통제 용도로 사용될 수 있는, 하드웨어적 연산이 제한적인 저가용 태그로 국·내외 교통카드로 사용되고 있다.

하지만, Mifare Classic 태그는 제한적인 하드웨어 연산을 기반으로 보안이 제공됨에 따라, 2008년 하드웨어 역공학, 부채널 공격, 난수 일치 공격 등 다양한 방법을 이용한 공격을 통해, 해당 카드의 암호화 스킴(Scheme) 및 통신 프로토콜이 여러 논문을 통해 노출되었다[6-8]. 2008년 'Defcon'에서는 Mifare Classic 기반의 교통카드를 해킹해 Chip에 저장된 금액정보를 공격자가 임의로 수정하는 해킹이 시현되었으며[9], 2010년 뉴스를 통해 국내 교통카드가 해킹되는 사례가 보도되었다[10].

이렇듯 Mifare Classic 기반 교통카드는 보안성이 깨진 상태이지만, 여전히 국·내외에서 교통카드로 사용되고 있으며, 과거 진행된 다양한 RFID 관련 보안 연구 결과는 Mifare Classic에서 제공하는 제한된 하드웨어 연산을 만족하지 못해 적용이 어렵거나, 암호 스킴 및 통신 프로토콜 보안 방법이 기 스킴 및 프로토콜과 상이하게 다르거나, 보안강도가 기 사용되던 암호 스킴 및 통신 프로토콜에 비해 떨어지는 문제점이 존재한다[11,12].

따라서 본 논문에서는 Mifare Classic 태그에서 기 사용되던 암호 스킴 및 통신 프로토콜을 기반으로, 제공하는 제한된 하드웨어 연산 능력과 메모리 접근방법을 고려해, 보안성이 향상된 암호 스킴 및 보안 통신 프로토콜을 제안한다.

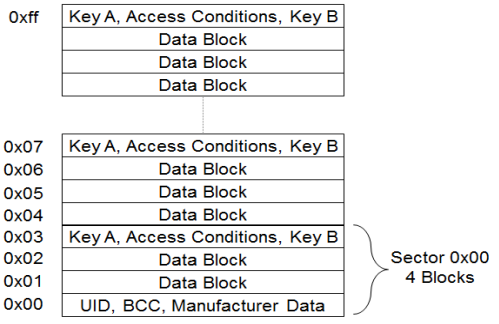
2. 관련연구

2.1 Mifare Classic

2.1.1 논리적 구조 및 제공 연산

Mifare Classic 태그의 논리적 메모리 구조는 16 Bytes 용량으로 이루어진 Block단위로 구분되며, 네 개의 Block이 모여 하나의 Sector를 형성한다. 태그는 제공하는 총 메모리 용량에 따라 1K, 4K로 구분될 수 있으며, Mifare Classic 1K 태그의 경우 64 Blocks 16 Sectors로 구성되어 있다.

각 Sector마다 각각 48 bits 크기의 Key A와 Key B가 저장되며, 특정 Sector 접근 시 저장된 특정 Key를 Seed 값으로 32 bits Session Key를 생성해 접근하게 된다. Sector 내 Block에 저장된 정보 접근 시 하위 Block부터 접근해야하며(Eg. Block 0x00 접근 후 Block 0x01 접근 가능), Sector간 접근 시에도 하위 Sector를 접근한 후 상위 Sector에 접근 가능하다[6-8].



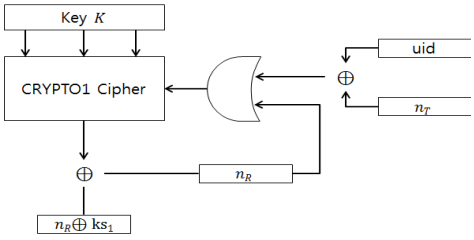
[Fig. 1] Mifare Classic Tag Logical Memory Structure

Mifare Classic 태그는 Value Block이라 불리는 금액, 출입권한 등과 같은 주요 정보가 저장되는 Block이 존재하며, Read, Write, Select, Delete 등과 같은 Operation 명령어를 지원하고, 보안을 위해 논리연산, 난수생성기, LFSR(Linear Feedback Shift Register)연산을 지원한다[13].

2.1.2 보안 스킴

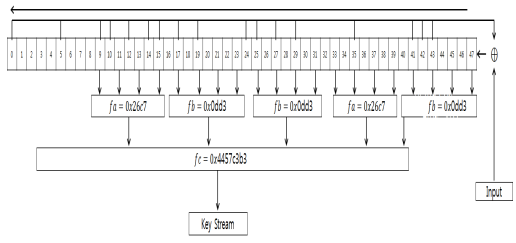
Mifare Classic 태그는 인증 시 0x04 Block부터 접근을 시도하며, Value Block에 접근하기 까지 각 Sector에 저

장된 48 bits의 Key를 Seed값으로 하여, 'CRYPTO1 Cipher'암호 스킴을 통해 Session Key로 사용되는 32 bits의 Key Stream을 생성해 통신을 수행한다. Mifare Classic 태그 보안 스킴은 Fig. 2와 같은 구조를 가지고 있으며, 정해진 Seed 값을 기반으로 Key Stream을 생성하는 역할을 한다. 'CRYPTO1 Cipher' 암호 스킴에는 첫 인증 시 사용되는 Block이 속한 Sector의 48 bits Key가 Seed 값으로 Input 되어 있다.



[Fig. 2] Mifare Classic Security Scheme

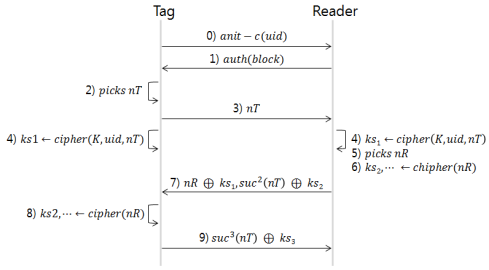
첫 번째 Key Stream을 생성하기 위해 'UID ⊕ NT'값이 'CRYPTO1 Cipher'암호 스킴에 Input되며, 정해진 암호화 연산을 통해 32 bits의 Key Stream이 생성된다. 두 번째 Key Stream은 'UID ⊕ NT' 값이 아닌 nR값이 Input 값으로 사용되며, 세 번째 Key Stream 부터는 Input 값이 존재하지 않는다[6-8].



[Fig. 3] CRYPTO1 Cipher Scheme

Fig. 3은 'CRYPTO1 Cipher' 암호 스킴 구조이다. 48 bits LFSR을 기반으로 하고 있으며, polynomial $f(x) = x^{44} + x^{43} + x^{42} + x^{36} + x^{30} + x^{28} + x^{26} + x^{25} + x^{20} + x^{18} + x^{16} + x^{15} + x^{13} + x^{11} + x^{10} + x^{6} + 1$ 이다. 첫 번째 Key Stream 생성을 예로 'CRYPTO1 Cipher' 동작 과정을 설명하면 다음과 같다.

LFSR에는 48 bits의 Seed Key값이 저장되어 있다. 'UID ⊕ NT'가 Input 값으로 x^{48}의 위치로 입력되며, 1 bits가 입력될 때, LFSR 내부 값은 1 bits shift 연산을 행한다. Shift 연산을 행한 후 정해진 20 자리에서 Filter Function으로 값이 입력되며 두 단계의 Filter Function을 통해 첫 번째 Key Stream ks1의 첫 번째 bit가 생성된다. 32 bits의 Key Stream을 생성하기 위해 위의 과정을 32번 반복하게 된다[6-8].



[Fig. 4] Mifare Classic Tag Authentication Protocol

Mifare Classic 태그 보안 스킴을 이용한 통신 프로토콜은 Fig. 4와 같으며, suc()는 polynomial $f(x) = x^{16}+x^{14}+x^{13}+x^{11}+1$ 기반의 Pseudo-Random Generator Successor함수이다. Fig. 4는 Mifare Classic 통신 프로토콜로 자세한 사항은 다음과 같다.

0) 태그는 식별값 UID를 리더에게 전송한다.
1) 리더는 인증하고자 하는 Block값을 전송한다.
2) 태그는 32 bits 난수를 생성한다.
3) 생성된 32 bits 난수는 리더에게 전송된다.
4) 태그는 48 bits Key K를 Seed 값으로 가지는 CRYPTO1 Cipher 암호 스킴에, UID와 nT를 Input 하여 첫 번째 Key Stream인 32 bits ks1를 생성한다. 리더는 태그가 전송한 UID와 매칭되는 K값을 검색한 후 K, UID, nT를 이용해 첫 번째 Key Stream인 ks1를 생성한다.
5) 리더는 ks2를 생성하기 위해 32 bits 난수 nR을 생성한다.
6) 리더는 CRYPTO1 Cipher 암호 스킴에, nR을 Input 하여 두 번째 Key Stream인 ks2를 생성한다.
7) 리더는 nR ⊕ ks1, suc^2(nT) ⊕ ks2를 태그에게 전송한다.
8) 태그는 '단계 4'에서 생성한 ks1과 'nR ⊕ ks1'을 XOR 연산하여, 리더를 검증하고 nR을 얻는다. 또한, nR을 이용해 ks2를 생성하고 suc^2(nT)를 연산해, 리더가 전송한 suc^2(nT) ⊕ ks2 값을 검증한다.
9) 태그는 ks3과 suc^3(nT)를 생성해 XOR 연산하여 리더에게 전송하며, 리더 역시 ks3과 suc^3(nT)를 생성해 태그의 전송 값을 검증한다[6-8].

2.1.3 보안 취약점

Mifare Classic 태그 해킹을 위해 사용된 공격 기법은 다양하다. Chip 자체를 광학 사진기를 찍어 논리 게이트 웨이를 알아내는 공격과 시간 및 전력 소비량 등을 기반으로 연산을 유추하는 부채널 공격이 사용되었으며, 태그에서 생성되는 난수를 일치시키기 위한 공격과 알려진 평문 공격 등 다양한 공격이 수행되었다. 공격 수행 결과 들어난 Mifare Classic 태그의 프로토콜은 쉽게 Key 값을 알아낼 수 있는 수준의 보안강도를 지녔으며, Key의 비밀성 또는 연산의 어려움에 보안을 의존하지 않고, 보안 스킴의 비밀성에 보안을 의존한 것으로 밝혀졌다. 또한, 이미 보안성이 깨진 'The Hitag2 Cipher'와 유사한 암호 스킴을 이용해 'CRYPTO1 Cipher' 암호 스킴의 보안성이 더욱 쉽게 깨지게 되었다. 물리적 공격을 배제한 Mifare Classic 태그의 주된 취약점은 다음과 같다[6-8].

(1) 난수 일치 문제

저가용 RFID 태그의 경우 Chip의 하드웨어적 연산 제한으로 인해 의사난수함수는 특정 난수를 생성한 후 일정 시간이 지난 후 동일한 난수를 생성하게 되며, Mifare Classic의 경우 전력 및 응답시간을 이 전 인증 시와 동일하게 설정할 경우 0.618s 마다 동일한 난수를 생성할 수 있다.

(2) suc() 함수 취약점

Pseudo-Random Generator Successor함수 suc()는 polynomial $f(x) = x^{16}+x^{14}+x^{13}+x^{11}+1$를 기반으로 하고 있어 32 bits의 난수를 Seed 값으로 연산할 경우 Half 영역만 Mixing되는 문제점이 존재한다.

또한, 첫 난수 생성 후 해당 난수만을 suc() 함수 연산 후 인증의 용도로 사용해 인증에 필요한 정보 값이 쉽게 노출되는 문제점을 야기하였다.

(3) 알려진 평문 공격

통신 프로토콜에서 리더가 '7)'의 단계를 수행한 후 일정시간동안 태그로부터 응답이 없을 경우, 리더는 중지명령어(halt : 5000)와 ks3을 XOR연산하여 태그에게 전송한다. 이 때, halt 명령어는 이미 알려진 평문으로 XOR 연산을 통해 쉽게 ks3을 알아낼 수 있다.

(4) nR 노출

Key Stream 생성 시 리더에서 생성하는 값은 32 bits 난수밖에 존재하지 않아, ProxMark3와 같은 태그와 리더 역할을 수행할 수 있는 공격 장비를 이용해 UID 및 nT의 값 등을 '0000.....0'으로 전송할 경우 nR 값을 알아낼 수 있다.

(5) LFSR Rollback

앞서 알려진 (1) ~ (4)의 취약점을 기반으로 ks3, ks2, ks1 등을 알아낸 후 도청을 통해 UID와 nT를 알아낸 후 LFSR Rollback 연산을 통해 Seed Key 값을 알아낼 수 있다.

2.2 기존 RFID 보안 연구

RFID가 활성화됨에 따라 다양한 RFID 보안 프로토콜 및 보안 스킴 연구가 활발하게 진행되어 왔다. 하지만, Hash Based RFID Protocol의 경우 Mifare Classic 태그에서 해당 연산을 지원하지 않아 사용될 수 없으며, EPC Class-1 Generation-2와 같은 저가용 태그에 맞춰진 프로토콜의 경우, 연산은 지원하나 RFID에서 요구되는 재생공격, 스푸핑 공격 등에 취약해, Mifare Classic 태그에 적용될 수 없다. 또한, 기존 보안 스킴 연구가 Mifare Classic 태그에서 사용되던 보안 스킴과 상이하게 달라, 적용가능성이 떨어지는 문제점이 존재한다[14-16].

3. 제안하는 보안 스킴

본 논문에서 제안하는 보안 스킴은 암호화 스킴과 보안 프로토콜로 구성된다. NXP에서 제공하는 Mifare Classic 태그의 Specification을 기반으로 설계해, 하드웨어 연산 제한을 받지 않으며, 기존에 사용되던 Mifare Classic 태그의 보안 스킴을 기반으로 설계해, 적용가능성이 타 보안 스킴 연구에 비해 높다. 또한, RFID에서 요구되는 보안 요구사항을 충족하였으며, 기존 Mifare Classic 태그의 보안 스킴 취약점을 해결하였다. 제안하는 보안 스킴에서 사용되는 용어 및 표기는 Table 1과 같다.

[Table 1] The Terms and Symbols Used in Proposed Scheme

UID	Unique Identification (32 bits)
N_T	Tag Random number (32 bits)
N_{R_n}	Reader Random number (32, 48 bits)
K_n	LFSR Seed Key (48 bits)
KS_n	Key Stream n (32 bits)
R_{ksn_1}	First 32 bits Redundance bits from S-Box (Used for Authentication Value)
R_{ksn_2}	Second 32 bits Redundance bits from S-Box (Used for Cryptography Input Value)

R_{ksn_3}	Third 48 bits Redundance bits from S-Box (Used for next KS's S-Box Input Value)
R_{ksn_4}	Forth 16 bits Redundance bits from S-Box (Used for next Sector's S-Box Input Value)
LFSR	48 bits Linear Feedback Shift Register
S-Box	Substitution-Box (Input : 48 bits / Output : 24 bits)

3.1 Proposed Mifare Classic Security Scheme

제안하는 Mifare Classic 태그의 보안 스킴은 인증하고자 하는 Sector의 48 bits Key K_A를 Seed값으로 하여, 'Proposed Cryptography' 암호 스킴을 통해 Session Key로 사용되는 32 bits의 Key Stream을 생성해 통신 프로토콜에서 사용한다.

Proposed Mifare Classic Security Scheme은 Fig. 5와 같은 구조를 가지고 있다. 한 Sector당 Key 값이 저장된 Block을 제외한, 세 개의 Data Block에 접근하기 위해 세 개의 Key Stream을 생성한다. 이 때, 각 Key Stream 생성을 위해 Proposed Cryptography에서는, LFSR 연산에 Input될 값과 S-Box 연산에 사용될 값으로, 고정된 값과 비고정된 값의 연산 결과 값을 사용하며, LFSR과 S-Box의 Input 값이 교차돼 연산되도록 설계하였다.

3.2 Proposed Cryptography Scheme

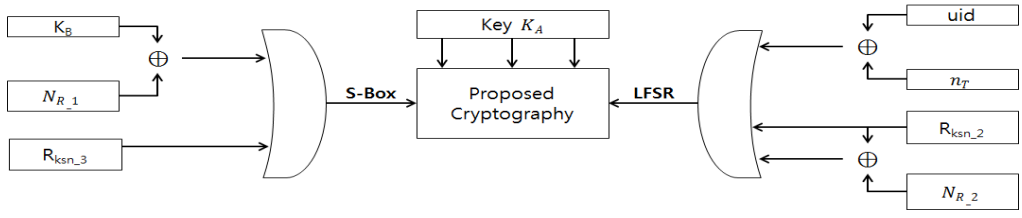
제안하는 Cryptography Scheme은 Fig. 6과 같다. Filter Function과 LFSR은 'CRYPTO1 Cipher' 암호 스킴 Polynomial만 동일할 뿐, Input 값의 큰 차이가 있으며, LFSR에서의 출력 값이 Filter Function 연산을 수행하기 전 S-Box 연산 값과 XOR 연산 후 Filter Function에 Input 된다.

3.2.1 S-Box 연산 과정

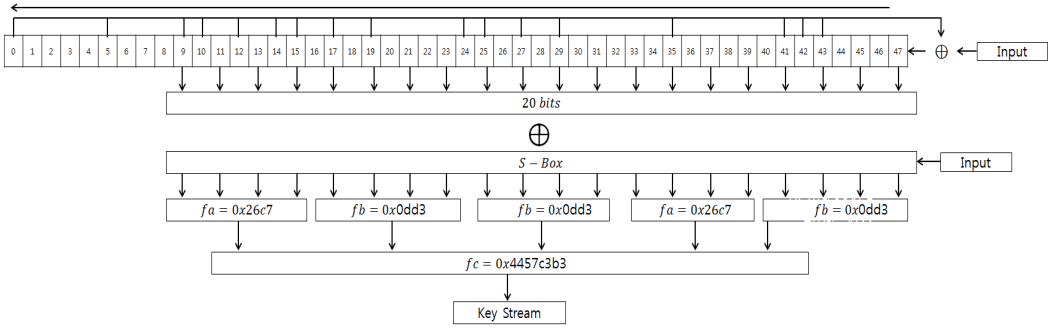
RFID 태그는 인증 시 빠른 인증을 위해 정보의 확인이 아닌 연산 결과를 확인한다. 즉, 암호문을 복호화하여 평문화하는 작업이 필요하지 않으며, 동일하게 암호문을 만들어 비교하는 작업이 필요하다. 따라서 S-Box의 역함수가 필요하지 않으므로, 고정된 길이의 Input과 Output이 필요하지 않아, 48 bits를 Input으로 받아 24 bits Output을 출력하는 S-Box를 사용한다.

LFSR이 1 bit Shift 해 Filter Function과 연산하기 위한 20 bits를 출력할 때, S-Box는 24 bits를 출력하여 LFSR에서 출력된 20 bits와 XOR 연산한다. 연산된 결과는 Filter Function으로 입력되며, Filter Function 연산을 수행해 Key Stream의 1 bit를 출력한다. 다시 LFSR이 1 bit Shift 하여 다음 Key Stream bit를 출력하고자 할 때, S-Box에 입력될 48 bits 역시 1 bit Shift 하여 연산에 들어가, 첫 S-Box 출력 값과 다른 값을 출력한다.

32 bits Key Stream을 출력하기 위해 S-Box는 총 32번의 연산을 수행하며, 이 때 발생된 잉여 bits는 4 bits씩 32번, 총 128 bits가 발생한다. 발생한 잉여 bits는 인증정보로 32 bits, LFSR Input 값으로 32 bits, 다른 Key



[Fig. 5] Proposed Mifare Classic Security Scheme



[Fig. 6] Proposed Cryptography Scheme

Stream 생성을 위한 S-Box Input 값으로 48 bits가 사용되며, 나머지 16 bits는 다음 Sector의 S-Box Input 값으로 사용하기 위해 보관한다.

3.2.2 Key Stream 생성 과정

한 Sector당 세 개의 Data Block을 접근하기 위해 세 개의 Key Stream을 생성하며, 각 Key Stream별 LFSR과 S-Box Input 값은 Table 2와 같다.

[Table 2] LFSR and S-Box Input Values for Key Stream

	LFSR Input Values	S-Box Input Values
KS_1	K_A, UID $\oplus$ N_T	$K_B \oplus N_{R\_1}$
KS_2	$R_{KS1\_2} \oplus N_{R\_2}$	R_{KS1_3}
KS_3	R_{KS2_2}	R_{KS2_3}

3.3 Proposed Secure Protocol

제안하는 보안 프로토콜은 Proposed Mifare Classic Secure Scheme과 Proposed Cryptography Scheme을 기반으로 설계하였으며, 프로토콜의 세부 동작 과정은 Fig. 7과 같다.

① ~ ⑥ 리더는 태그를 감지하고 RF 시그널을 보내며, 태그는 RF 시그널을 전력으로 Wake Up 상태로 전환된다. 태그는 자신의 UID를 리더에게 전송하며, 리더는 S-Box Input 값으로 사용될 48 bits의 난수를 생성해, 인증 요청 명령어와 함께 태그에게 전송한다. 태그는 KS_1을 생성하는데 사용될 난수를 생성해 리더에게 전송한다.

⑦ 리더는 태그의 UID에 매칭되는 K_N값을 검색한 후, KS_1을 생성한다. 또한, KS_2 생성을 위한 난수를 생성하고 KS_2를 생성한다.

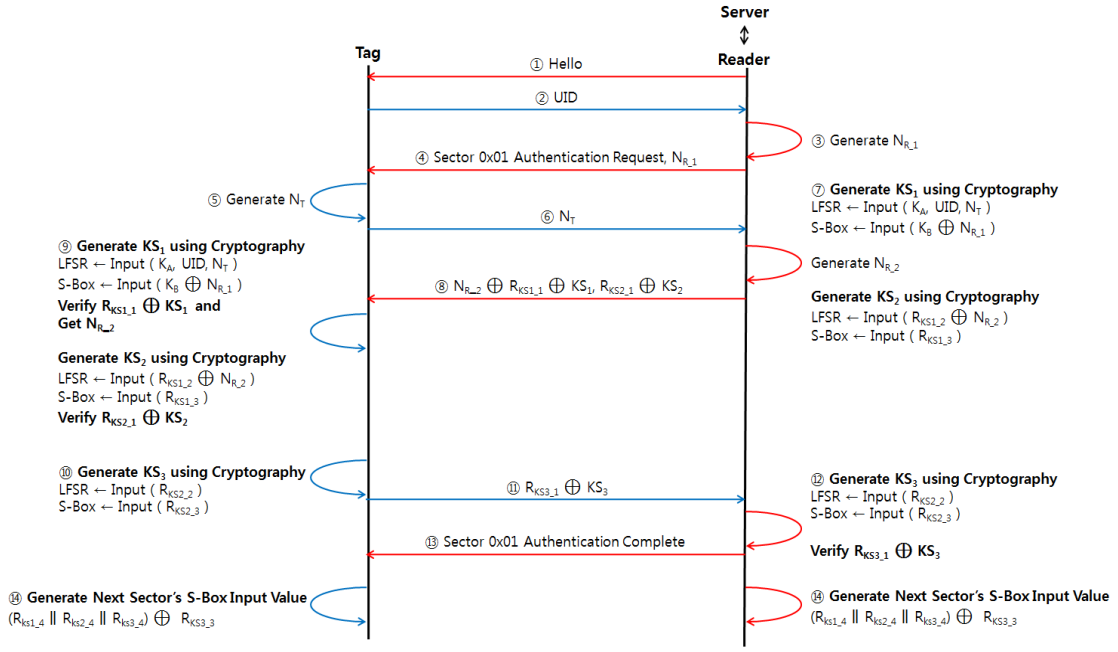
⑧ 리더는 자신이 생성한 난수 N_{R_2}와 KS_1 생성 과정 중 도출된 R_{KS1_1}값을 KS_1로 XOR 연산하여 전송하며, KS_2와 KS_2 생성과정 중 도출된 R_{KS2_1}값을 KS_2로 XOR 연산하여 전송한다.

⑨ 태그는 KS_1을 생성하여 $N_{R\_2} \oplus R_{KS1\_1} \oplus KS_1$ 비교를 통해 리더를 검증하고, N_{R_2}를 얻는다. 또한, N_{R_2}를 이용해 KS_2를 생성하여 $R_{KS2\_1} \oplus KS_2$ 비교 검증한다.

⑩ ~ ⑪ 태그는 마지막 Block 인증을 위한 KS_3을 생성해 R_{KS3_1}와 XOR연산하여 리더에게 전송한다.

⑫ ~ ⑬ 리더는 KS_3을 생성해 R_{KS3_1}와 XOR연산하여 태그로부터 전송된 값을 비교 및 검증하며, 모든 검증이 성공할 시 인증에 성공한다.

⑭ 마지막으로 태그와 리더는 $KS_{1,\ 2,\ 3}$ 생성 시 S-Box에서 발생돼 보관하고 있던 잉여 bits R_{ks1_4}, R_{ks2_4}, R_{ks3_4}을 연접한 후 R_{KS3_3}와 XOR 연산하여, 다음



[Fig. 7] Proposed Secure Protocol

Sector 인증 시 S-Box의 초기 Input 값으로 사용하도록 한다.

4. 성능평가 및 비교분석

본 장에서는 제안하는 Mifare Classic 보안 스킴이 기존 Mifare Classic 태그의 보안 취약점과 RFID에서 발생할 수 있는 일반적인 공격에 대한 안전성 보유 여부를 검증한다. 또한, 현재 진행되고 있는 다른 RFID 보안 스킴과의 비교분석을 통해 제안하는 Mifare Classic 보안 스킴의 보안강도를 분석한다.

4.1 성능평가

(1) 난수 일치 문제 및 suc() 함수 취약점

기존 Mifare Classic 보안 스킴은 태그의 난수를 일치시키는 공격이 수행될 경우, KS_1이 동일한 값이 계속 출력되며, KS_2와 KS_3과 XOR 연산되는 suc(N_T) 역시 동일한 값이 출력되는 문제점을 가지고 있다.

하지만, 제안하는 Mifare Classic 보안 스킴에서는 KS 생성 시, 난수 일치 공격을 막기 위해 리더에서 생성되는 난수와 S-Box를 사용한다. 또한, 정보 유추가 비교적 쉬운 suc(N_T) 함수를 사용하지 않고, S-Box 연산 결과 값을 사용해 난수 일치 공격을 통한 KS 노출 취약점을 해결하였다.

(2) 알려진 평문 공격

제안하는 프로토콜에서는 KS 생성 시 다양한 고정값과 비고정값을 사용하고, S-Box 연산을 수행하며, LFSR 연산과 S-Box 연산에 사용되는 값을 교차시켜, 임의로 태그 응답을 중단시켜 리더로부터 알려진 평문인 Halt 명령어와 KS의 XOR 연산 값을 얻은 후, 계속해서 KS를 복구하는 취약점을 해결하였다.

공격자에게 KS_3이 노출돼도, S-Box 값과 R_{KS1_1} 등의 인증 시 사용되는 정보를 알아낼 수 없어 Key Stream을 복구할 수 없다.

(3) N_R 노출 및 LFSR Rollback

제안하는 Mifare Classic 보안 스킴에서는, ProxMark3와 같은 공격 도구를 사용해 UID와 N_T를 '0' 값으로 통일한 후 NR 유추 및 유추를 통한 LFSR Rollback 공격을 수행하여도, KB와 리더에서 생성된 난수를 연산하여 S-Box를 수행하기 때문에, 항상 다른 KS 및 인증 정보 값이 출력돼, 공격에 안전하다.

(4) 재사용 공격

공격자가 프로토콜상의 ④, ⑧, ⑪을 스니핑하여 재사용 공격을 시도하였을 경우, 태그와 리더에서 생성되는 난수를 기반으로 해당 값이 인증 시마다 변하기 때문에 재사용 공격에 안전하다.

(5) 기타 공격

본 논문에서 제안하는 Mifare Classic Secure Scheme에서는 Key Stream 즉, Session Key를 사용해 각 인증 시 사용되는 키와 전송되는 값이 다르므로 스푸핑 공격과 프라이버시 침해에 안전하며, Forward Security가 가능하다. 마지막으로, 서버와 리더 그리고 태그에서 전송되는 데이터를 공격자가 수집하여도 수집된 데이터에 대한 의미를 알 수 없도록 설계하여 도청공격에 안전하다.

4.2 비교분석

Mifare Classic 시스템에서는 리더와 서버는 하드웨어 설계 시 공간, 구성, 연산 능력 등에 제한이 없는 반면, 태그는 하드웨어 연산 능력에 제한이 있어 Hash, DES, RSA 등과 같은 연산이 불가능하다. 따라서 비교분석 시 일반적인 RFID 보안 요구사항 만족 여부를 판별할 뿐 아니라, 실제 Mifare Classic에 적용 가능한 Scheme인지 여부를 판별해야 한다. 제안하는 Mifare Classic Secure Scheme의 보안강도 비교분석 결과는 Table 3과 같다.

[Table 3] Security comparative analysis

	Origin Mifare Classic [6][7][8]	HR [14]	H_ID [15]	Ch_P [16]	Proposed Scheme
Suitable to Mifare Classic	SU	NS	NS	SU	SU
Forward Security	NS	NS	NS	SU	SU
Mutual Authentication	SU	NS	NS	SU	SU
Privacy	SE	VU	VU	SE	SE
Replay Attack	VU	VU	VU	VU	SE
Spoofing Attack	VU	VU	VU	VU	SE
Eavesdropping	VU	SE	SE	SE	SE
Known Text Attack	VU	SE	SE	SE	SE
Nance Problem	VU	SE	SE	SE	SE
Key Issue	VU	SE	SE	VU	SE

SE: Secure, VU : Vulnerable
SU : Suitable, NS : Not Suitable

5. 결론

본 논문에서는 현재 국·내외에서 교통카드 및 출입통제 용도로 시장 점유율이 가장 높은 Mifare Classic 태그의 문제점을 해결하고자 안전한 보안 스킴 구축을 위한 암호 스킴 및 보안 프로토콜을 제안 하였다.

본 논문에서 제안하는 암호 스킴 및 보안 프로토콜 기반의 Mifare Classic Secure Scheme은 NXP의 Specification을 기반으로 태그의 하드웨어적 성능을 고려하여 태그의 연산 능력 안에서 암호 스킴 및 보안 프로토콜을 설계하였으며, 즉시 Mifare Classic 태그에 적용 가능하도록 기존 보안 스킴을 기반으로 설계하였다.

Mifare Classic Secure Scheme은 태그 뿐 아니라, 리더에서 생성된 난수를 Key Stream 생성 시 S-Box를 통해 연산하도록 하였으며, 잉여 bits가 남도록 설계 하여 인증 정보로 사용함으로써, RFID 태그가 가지고 있는 난수 일치 공격 문제 및 suc함수의 후속 값 유추가 쉬운 취약점을 해결하였다. 또한, 매번 다른 세션 키를 생성하도록 하여 재전송 공격과 스푸핑 공격, 도청 공격 등에 안전하며 상호 인증이 가능하다.

RFID 기술이 탑재된 스마트 단말이 증가함에 따라, 다양한 공격 도구를 이용해 해킹을 시도해야 했던 과거와 달리, Mifare Classic 기반의 교통 카드는 스마트 단말을 이용해 쉽게 해킹이 이루어 질수 있다. NXP의 Specification과 기존 보안 스킴을 고려해 설계된 제안하는 보안 스킴은 실적용 가능하며, RFID 환경에서 들어난 모든 보안 취약점에 안전하므로, 국내·외 교통 카드 및 출입통제카드로 가장 활발하게 사용되고 있는 현재, 가장 필요 시 되는 안전한 보안 스킴으로 평가할 수 있다.

References

[1] ISO/IEC 14443-1:2008, Identification cards - Contactless integrated circuit cards - Proximity cards - Part 1: Physical characteristics

[2] ISO/IEC 14443-2:2010, Identification cards - Contactless integrated circuit cards - Proximity cards - Part 2: Radio frequency power and signal interface

[3] ISO/IEC 14443-3:2011, Identification cards - Contactless integrated circuit cards - Proximity cards - Part 3: Initialization and anticollision

[4] ISO/IEC 14443-4:2008, Identification cards - Contactless integrated circuit cards - Proximity cards - Part 4: Transmission protocol

[5] NXP, "NXP takes lead on security for contactless smart cards", November, 2011.

[6] de Koning Gans, G., Hoepman, J.-H., Garcia, F.D. "A practical attack on the MIFARE Classic", Proceedings of the 8th Smart Card Research and Advanced Application Workshop (CARDIS 2008). LNCS, vol. 5189, pp.267 – 282. Springer, Heidelberg, 2008.
DOI: http://dx.doi.org/10.1007/978-3-540-85893-5_20

[7] Flavio D. Garcia, Gerhard de Koning Gans, Ruben Muijrers, Peter van Rossum, Roel Verdult, Ronny Wichers Schreur, and Bart Jacobs, "Dismantling Mifare Classic", ESORICS 2008, LNCS 5283, pp. 97 – .114, 2008.
DOI: http://dx.doi.org/10.1007/978-3-540-88313-5_7

[8] Flavio D. Garcia Peter van Rossum Roel Verdult Ronny Wichers Schreur, “Wirelessly Pickpocketing a Mifare Classic Card”, 30th IEEE Symposium on Security and Privacy, 2009.

[9] Russell Ryan, Zack Anderson, Alessandro Chiesa, "Anatomy of a Subway Hack", Defcon, 2008.

[10] MBC,http://imnews.imbc.com/replay/nwdesk/article/2587138_5780.html

[11] Il-Ho Park, "Design of Mutual Authentication Protocol using Key Exchange in RFID System", KAIS's Spring Conference, 2010.

[12] Woo Sik Bae, Jong Yun Lee, "Random Number-based Security Authentication Protocol for RFID System", KAIS's Spring Conference, 2010.

[13] NXP, "MF1ICS70 Functional specification", Rev. 4.3 . 14, December, 2009.

[14] S. Piramuthu, “On existence proofs for multiple RFID Tags”, IEEE Computer Society Press. In IEEE International Conference on Pervasive Services, Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing - SecPerU 2006, pp. 317-320, June 2006.
DOI: http://dx.doi.org/10.1109/PERSER.2006.1652252

[15] Yungjoo Hwang, Soomi Lee, Donghun Lee, Jongin Lim, “Authentication Protocols for Low-Cost RFID in Ubiquitous Environment”, CISC'S04, pp. 120-122, Jun. 2004.

[16] Hung-Yu Chien, Che-Hao Chen, “Mutual authentication protocol for RFID conforming to EPC class-1 generation-2 standards”, Computer Standards & Interfaces, vol. 29, Elsevier Science Publishers, pp. 254 – 259, Feb. 2007.
DOI: http://dx.doi.org/10.1016/j.csi.2006.04.004

강 정 호(Jung-Ho Kang) **[정회원]**

- 2000년 2월 : 서울과학기술대학교 컴퓨터공학과 공학사
- 2002년 2월 : 서울과학기술대학교 컴퓨터공학과 공학석사
- 2004년 2월 ~ 현재 : 숭실대학교 컴퓨터학과 박사수료
- 2010년 7월 ~ 현재 : 플럼소프트 대표

<관심분야>
M2M, 네트워크 보안, 암호 프로토콜, NFC

박 재 표(Jae-Pyo Park) **[정회원]**

- 2004년 8월 : 숭실대학교 컴퓨터학과 공학박사
- 2008년 9월 ~ 2009년 8월 : 숭실대학교 정보미디어 기술연구소 전임연구원
- 2010년 3월 ~ 현재 : 숭실대학교 정보과학대학원 교수

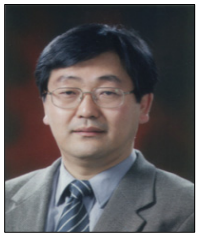
<관심분야>
컴퓨터통신, 보안, 암호학, 멀티미디어 통신

김 형 주(Hyung-Joo Kim) **[정회원]**

- 2008년 8월 : 단국대학교 컴퓨터과학과 공학사
- 2010년 8월 : 숭실대학교 컴퓨터학과 공학석사
- 2010년 9월 ~ 현재 : 숭실대학교 컴퓨터학과 박사수료

<관심분야>
Authentication, M2M, NFC, RFID, Security Scheme

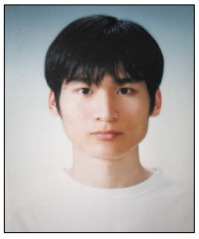
전 문 석(Moon-Seog Jun) **[정회원]**



- 1989년 2월 : University of Maryland Computer Science 공학박사
- 1989년 3월 ~ 1991년 2월 : New Mexico State University physical Science Lab 책임연구원
- 1991년 3월 ~ 현재 : 숭실대학교 정교수

<관심분야>
인터넷 보안, 네트워크 보안, 인증 시스템, 정보보호

이 재 식(Jae-Sik Lee) **[정회원]**



- 2005년 8월 : 가천대학교 컴퓨터공학과 공학사
- 2007년 8월 : 숭실대학교 컴퓨터학과 공학석사
- 2007년 9월 ~ 현재 : 숭실대학교 컴퓨터학과 박사수료

<관심분야>
인증 이론 및 시스템, 암호프로토콜, 개인정보보호