SEED 기반의 부분 암호화 기법을 이용한 RFID 백워드 채널 보호 기법

김성진* · 박석천**

RFID backward channel protection scheme by Partial Encryption scheme based on SEED

Sung Jin Kim* · Seok Cheon Park**

요 약

본 논문에서는 기존 RFID 보안 기법에서 나타나는 도청으로 인한 정보 유출 문제를 분석하고 이를 해결하기 위하여 RFID에 SEED 보안 알고리즘을 응용한 부분 라운드 및 부분 암호화 기법을 적용하고자 한다. 기존에 제시된 많은 태그보안 기법들이 있으나, 보안과 구현의 문제에서 아직 현실적인 접근이 미비한 실정이다. 따라서, 본 논문을 통해 보다 현실적인 구현의 관점에서 하나의 아이디어를 제공하고, SEED 기반의 비밀키 기반 암호화 알고리즘 기법을 적용하여 태그에서 리드간의 전송 취약구간인 백워드 채널상의 정보보안을 해결책을 제시하였다.

ABSTRACT

In this paper, we analyse eavesdrop problem of existing RFID security scheme and proposed improved SEED algorithm for RFID security. we suggest partial round process and security in SEED algorithm.

Existing scheme has vulnerability of security and implementation, so far from realization. Therefore In our paper, we proposed new scheme using modified SEED algorithm for backward channel protection.

키워드

RFID, 유비쿼터스보안, SEED, 보안알고리즘

Ⅰ. 서 론

유비쿼터스 기술중에서 RFID(Radio Frequency Identification) 기술은 유비쿼터스 컴퓨팅 환경에서 가장 기반이 되는 핵심적인 요소라 할 수 있다. 그러나 RFID의 특성상 사물과 사용자의 취득·이동·폐기 등의 정보가 기록되는 과정에서 이에 대한 추적과 접근이 용이한 사업자의 오·남용 및 개인 정보 침해가능성이 제기되고 있다. 특히, RFID 태그 시스템에서 보호되지 않은 태그는 도청, 트래픽 분석, 스푸핑(spoofing) 및 서비스 거부 공격(DOS:Denial of Service) 등의 공격에 취약하며, 이 외에도 세션 가로채기(hijacking), 재생공격(Replay) 공격, 중간자 공격(man In the Middle Attack), 물리적인 공격 등에도 취약하다[1].

이런 이유로 현재 활발히 RFID 보안 기술 연구가 이뤄지고 있는데 기밀성(confidentiality), 인증(authentication),

* 경원대학교 대학원 전자계산학과
** 경원대학교 소프트웨어학부 정교수

접수일자 : 2007. 8. 20

보안성(security) 등 다양한 보안 요소들이 결합된 형태로 이뤄지고 있다. 그러나, 아직까지 보안 기술은 초기 단계이며, 보안성이 온전히 구현되지 못하고 있다. 특히, RFID 태그 자료가 전송되는 과정인 백워드(Backward) 채널 정보 보호 기법에서 불법 리더에 의해 쉽게 도청을 당할 수 있는 상황에 대한 보안 연구는 미비한 실정이다. 따라서, 본 논문에서 현재까지의 RFID 정보보호 구현상에 현실 가능성을 재고한 부분 암호화 기반의 RFID 백워드 정보보호 기법을 제안한다.

Ⅱ. 관련연구

2.1. 태그-리더 사이의 채널 보호 기법

불법 도청자가 태그와 리더의 사이의 정보를 획득한다고 할 때, 단지 획득된 정보로는 사물의 형태나 가격 등 구체적인 정보를 알 수 없어 크게 위협이 되지는 않는다.

태그에서 리더로 전달되는 정보는 일종의 일련번호(serial number)에 불과하고 해당 일련번호를 리더가 읽었더라도 그 일련번호에 대응하는 구체적인 정보는 서버를 통해 전달받아야 하기 때문이다. 하지만 구체적인 정보는 획득하지 못하더라도 특정 일련번호를 가진 태그가 움직이는 것을 지속적으로 추적하는 것이 가능하므로 특정 개인의 위치 파악 등에 활용될 우려가 있어 또 다른 사생활 침해 문제를 초래할 수 있다.

포워드 채널만 보호하는 방법은 해킹으로부터 보호하고자 하는 태그의 반응 거리 밖에 불순한 목적을 가진 리더가 있을 때에는 이러한 리더로부터 태그 정보를 보호할 수 있지만, 태그의 반응 거리 안에 불순한 목적을 가진 리더가 있을 경우에는 해킹이나 도청을 막을 수 없다. 이와 같은 문제를 해결하기 위해 태그와 리더 간의 통신 내용 자체를 보호하기 위한 정보 보호 기법이 필요하다. 그림1은 백워드 채널의 취약성을 나타난다.

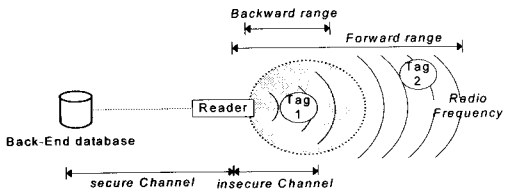

그림 1. 백워드 채널의 취약성
Fig 1. Vulnerability of Backward Channel

포워드 보안과 관련한 대표적인 알고리즘으로는 트리워킹(tree walking) 알고리즘이 있다[2]. 리더는 자신의 전파 범위에 있는 태그가 복수개인 경우 전파 충돌로 태그를 인식하지 못하게 되며, 그럴 경우 ID의 첫 비트가 0인 태그에 대해서만ID를 먼저 대답할 것을 다시 요청한다. 이런 충돌 발생시 태그의 ID에 대한 정보를 리더가 구체적으로 명시하기 때문에 도청자 입장에서는 리더의 전파를 탐지하는 것만으로도 주위에 어떤 ID를 가지는 태그가 존재하는지를 수집할 수 있다.

원거리에서 도청을 시도할 경우, 리더가 태그에게 보내는 질의는 도청 가능하지만 질의에 대한 태그의 응답은 신호가 약하기 때문에 도청할 수 없다. 블라인드 트리워킹(Blinded Tree Walking) 알고리즘은 이러한 사실을 활용하여 포워드 보안을 개선한 방법이다[3]. 이 방법을 사용하면 태그에 대한 ID 정보를 리더가 유출시키지 않으므로 포워드 채널에 대한 도청 방지 기능을 쉽게 제공할 수 있다.

트리워킹 방법의 또 다른 보완책으로는 난수적 트리워킹 알고리즘(randomized tree walking)이 있다[4, 5]. 이 방법에서는 태그가 자신의 실제 ID가 아닌 난수값을 이용하여 생성한 가상 ID를 질의에 대한 응답으로 보내고, 리더는 이를 이용하여 태그를 선별해 나간다. 트리워킹을 통해 각 태그에 대한 선별이 끝나면 리더는 태그 별로 실제 ID를 질의하여 응답을 받는다. 이렇게 되면 포워드 채널에 대한 도청자는 가상 ID에 대한 정보만 수집할 뿐, 실제 ID에 대한 정보는 얻을 수 없다.

한편, 근거리에 있는 도청자인 경우 태그가 최종적으로 보내는 실제 ID를 얻을 수 있기 때문에 백워드 채널에 대한 보안은 여전히 이루어지지 않는다. "전파식별(RFID) 보급 활성화를 위한 역기능 및 정보보호 대책연구"[6]에서는 백워드 채널 보안을 위해 태그가 실제 ID를 전송할 때 리더가 동시에 임의의 난수값을 전파시켜 도청자가 교란된 정보를 얻게 한다. 이러한 신호를 도청하였을 경우, 충돌이 발생한 비트를 정확히 재생해 낼 수 없으므로 백워드 보안이 유지된다. 그러나 이 방법은 정보를 암호화해서 보내는 방법이 아니기 때문에 태그와 리더간의 동기화가 정확히 이루어지지 않을 경우 도청자가 태그의 ID를 직접 획득할 수도 있다는 문제점이 있다. 지금까지 살펴 본 정보보호 기법들을 요약하면 표 1과 같다.

표 1. 도청 방지 기법 비교
Table 1. Comparison of Eavesdrop Detection scheme

요구조건 도청방지기법	포워드 보호	백워드 보호	암호화
트리워킹	x	x	x
블라인드 트리워킹	o	x	o
난수적 트리워킹	o	x	o
백워드 채널 보호	o	o	x

2.2. 태그-리더 사이의 암호화 기법

현재 RFID 시스템에서는 암호학적인 방법을 이용한 인증 기법을 주로 연구하고 있으며, 현재까지 해쉬-락 기법, 확장된 해쉬-락 기법, 외부 재 암호화 기법, 해쉬-체인 기법, 해쉬 기반 ID 변형기법, 개선된 해쉬 기반 ID 변형 기법 등이 제안되었다. 그러나, 지금까지 제안된 RFID 인증 기법들은 재전송 공격에 취약하거나, 위치정보를 노출시키는 등 많은 문제점을 가지고 있다.

또한, 국제표준화기구(ISO)를 비롯하여, ITU·ANSI·IEEE 등 여러 국제기구에 암호표준으로 제안된바 있는 RSA 알고리즘은 공개키와 개인키로 인터넷에서 사용하는 정보(특히 전자우편)를 암호화하고 복호화할 수 있는데, 동작원리는 매우 복잡한 수학으로 개인키의 암호를 해독하려면 슈퍼컴퓨터로도 1만년 이상이 소요되므로 공개키 암호방식의 대명사로서 거의 모든 분야에 응용되고 있다. 그러나 계산량이 많은 것이 단점으로 꼽힌다. 비트 수에 따라 다르나 펜티엄급 컴퓨터에서 공개키와 개인키를 만들려면 짧게는 20여 초, 길게는 몇 분까지 기다려야 한다. 복호화에도 많은 계산량이 요구되고 있어 휴대용 단말기에서는 사용하기 어렵다. 그래서 이런 문제를 해결하기 위해 본 논문에서는 RFID 백워드 채널 보호의 대안으로 SEED 알고리즘을 적용한다.

Ⅲ. 기존 SEED 알고리즘

3.1. 기존 SEED 방식 전체 구조

SEED는 대칭키 암호알고리즘으로, 블록 단위로 메시지를 처리하는 블록 암호알고리즘이다[7]. SEED 알고리즘의 전체 구조는 Feistel 구조로 이루어져 있으며, 128비트의 평문 블록단위당 128비트 키로부터 생성된 16개의 64비트 라운드 키를 입력으로 사용하여 총 16라운드를 거쳐 128비트 암호문 블록을 출력한다. 또한, 각 단계별 연산에 사용되는 기호는 표 2와 같다.

표 2. 연산 기호
Table 2. Operation Symbol

기호	의미
&	비트단위 AND 연산
⊞	a⊞b, $(a+b) \bmod 2^{32}$ 모듈라 연산
⊕	비트단위 exclusive OR 연산
<< n	n 비트 좌측 rotation 연산
>> n	n 비트 우측 rotation 연산
‖	연결 연산
Ki,o, Ki,1	오른쪽, 왼쪽 라운드 키

그림 2는 SEED 알고리즘의 전체구조를 도식화한 것이다.

전체 처리과정은 입력된 128비트 입력 평문블록을 2개의 64비트 블록(L0(64),R0(64))으로 나누어, 16개의 64비트 라운드 키를 이용하여 16라운드를 수행한 후, 최종 128비트 암호문 블록(L16(64),R16(64))을 출력하는 과정을 수행한다.

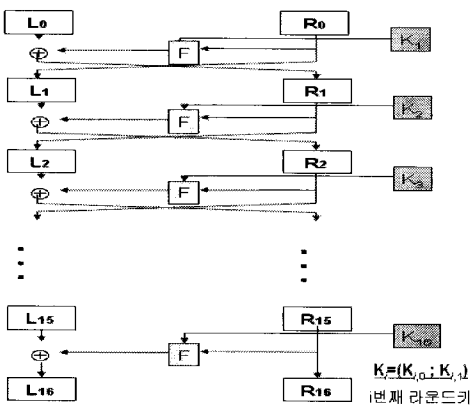

그림 2. SEED 전체 구조도
Fig 2. Structure of SEED

3.1.1 F 함수

Feistel 구조를 갖는 블록 암호알고리즘은 F 함수의 특성에 따라 구분될 수 있다. SEED의 F 함수는 수정된 64비트 Feistel 형태로 구성된다. F 함수는 각 32비트 블록 2개(C, D)를 입력으로 받아, 32비트 블록 2개(C', D')를 출력한다. 즉, 암호화 과정에서 64비트 블록(C, D)와 64비트 라운드 키 Ki=(Ki,0;Ki,1)를 F 함수의 입력으로 처리하여 64비트 블록(C', D')을 출력한다. 이때, 사용되는 연산은 XOR연산과 G-함수, ADD/Modular 연산이며 연산식은 다음 식(1)과 같다.

(i : 라운드 수)

C' = G[G[G{(C⊕Ki,0)⊕(D⊕Ki,1)}⊞(C⊕Ki,0)]⊞G{(C⊕Ki,0)⊕(D⊕Ki,1)}]⊞G[G{(C⊕Ki,0)⊕(D⊕Ki,1)}⊞(C⊕Ki,0)]

D' = G[G[G{(C⊕Ki,0)⊕(D⊕Ki,1)}⊞(C⊕Ki,0)]⊕G{(C⊕Ki,0)⊕(D⊕Ki,1)}] ----------식(1)

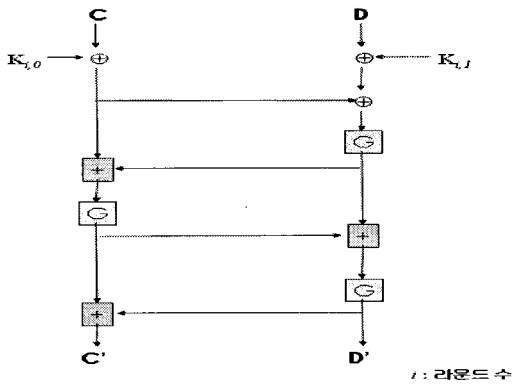

그림 3 F-함수 구조도
Fig 3. Structure of F-Function

3.1.2 G 함수

G 함수는 보안기능 향상을 위해 효과적으로 설계된 부분으로 F 함수와 라운드 키 생성단계에서 사용된다. 32 비트의 입력이 4개의 8-비트 블럭으로 분리되며 각 분리된 블록은 S-box를 통해 비트단위 AND 연산을 수행한다. 이때, m0, m3값이 이용된다.

결과적으로 32-비트의 G함수 입력은 128-비트로 확장된다. 확장된 블록은 서로 XOR 과정을 통해 다시 32-비트 크기의 출력으로 재구성된다. G 함수의 구조는 그림 4와 같다.

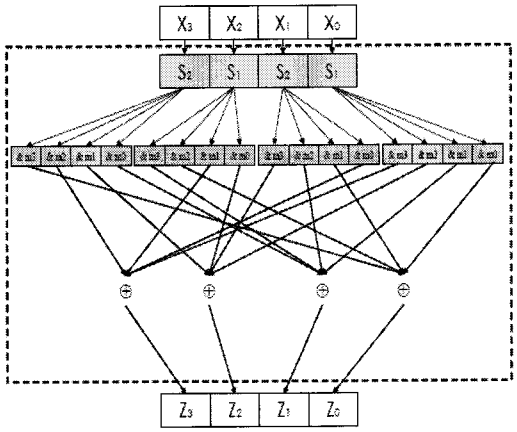

그림 4. G-함수 구조도
Fig 4. Structure of G-Function

이때, 입력되는 4개의 8-비트 입력(X0, X1, X2, X3)을 받아 G함수를 통해 생성되는 결과(Z0, Z1, Z2, Z3)의 산출식은 다음 식(2)와 같다

Z0=(S1(X0)&m0)⊕(S2(X1)&m1)⊕(S1(X2)&m2)⊕(S2(X3)&m3)

Z1=(S1(X0)&m1)⊕(S2(X1)&m2)⊕(S1(X2)&m3)⊕(S2(X3)&m0)

Z3=(S1(X0)&m2)⊕(S2(X1)&m3)⊕(S1(X2)&m0)⊕(S2(X3)&m1)

Z4=(S1(X0)&m3)⊕(S2(X1)&m0)⊕(S1(X2)&m1)⊕(S2(X3)&m2)

----------식(2)

3.1.3 라운드 키 생성과정

라운드 키 생성과정은 128비트 암호키를 64비트 블럭씩 좌우로 나누어 각 블록을 좌측-로테이트 쉬프트 연산을 반복한 후, ADD/ 모듈라 연산과 G-함수 연산을 수행한 후, 라운드 키(ki,j)가 생성된다. 각 라운드에 사용되는 라운드키는 다음과 같은 방식으로 생성한다.

① 128비트 입력키를 32비트씩 4개의 조각으로 나눈 다음(A, B, C, D),
② K1, 0 = G(A+C-KC0) ; K1, 1 = G(B-D+KC0) (단, KC0 : 1 라운드상수)로 제1라운드 키를 생성하고,
③ A||B = (A||B) >> 8
④ K2, 0 = G(A+C-KC1) ; K2, 1 = G(B-D+KC1) (단, KC1 : 2 라운드 상수)로 제2라운드 키를 생성하고,
⑤ C||D = (C||D) << 8

⑥ K3, 0 = G(A+C-KC2) ; K3, 1 = G(B-D+KC2) (단, KC2 : 3 라운드상수)로 제3라운드키를 생성하고,
⑦ 각 라운드에 대해 반복하여 해당 라운드의 키를 생성한다.

Ⅳ. 제안 알고리즘을 이용한 백워드 채널 보호 기법

RFID 태그의 한정된 컴퓨팅 환경 즉, 암호화에 할당된 게이트 수(패시브 태그일 경우, 약 3,000게이트), 회로 크기, 전원공급 문제 등에서 메시지를 암호화하는 데에는 많은 제약이 따른다. 따라서, 기존의 공개키1 알고리즘인 SEED 알고리즘을 RFID 시스템에 적용하는 것이 무리가 따른다. 본 논문에서는 태그의 한정된 성능으로도 간단하게 암호화 작업을 할 수 있는 SEED의 수정 알고리즘을 제안한다.

4.1 SEED 기반의 백워드 채널 보호 기법 정의

태그와 리더 간에 전송되는 메시지를 암호화할 경우 인증에 관련된 문제점을 해결할 수 있다. 그러나, 기존의 보안 프로토콜들은 리더로부터 송신되는 포워드 채널만 보호하는 방법에 사용되어 졌다.

포워드 채널만 보호하는 방법은 해킹으로부터 보호하고자 하는 태그의 반응 거리 밖에 불법 도청 리더가 있을 때에는 이러한 리더로부터 태그 정보를 보호할 수 있지만, 태그의 반응 거리 안에 불법 도청 리더가 있을 경우에는 해킹이나 도청 등의 행위를 막을 수 없다. 즉 리더가 태그에서 질의를 전송하는 백워드(Backward) 채널에 대해서는 아무런 보호도 이뤄지지 않는다. 따라서, 본 논문에서는 RFID 태그와 허가 받은 리더 사이에서 정보를 주고받을 때, 백워드 채널의 해킹을 막기 위해 실제 ID를 전송할 때 태그에서 고유 ID를 암호화하여 리더로 전송한다.

리더는 암호화된 ID로부터 복호화 단계를 거쳐 원래의 ID를 획득함으로서 보안이 유지되게 된다. 이 과정에서 암호화 및 복호화는 SEED알고리즘을 이용하여 RFID 태그 ID의 암호화 및 메시지 전송에 적용한다.

4.2. 제안 알고리즘 전체 구조

본 논문에서 제안하는 SEED의 수정 알고리즘의 적용 시, 사전 조건은 다음과 같다.

첫째, 처리 메시지의 크기는 EPC 코드 체제를 기준으로 하여 96비트단위로 처리한다. 본 논문에서는 그림 5의 SGTIN-96 코드체제를 기초하여 설명한다.

MSB LSB

구 분	Header	Filter Value	Partition	Company Prifix	Item Reference	Serial Number
비트크기	8	3	3	20-24	24-4	38

그림 5. SGTIN-96 코드
Fig. 5. SGTIN-96 Code

둘째, 실제 태그내 회로구성을 위해 기존 SEED 알고리즘에서 사용되는 암호 함수는 경량화된 함수로 재구성됨을 전제로 한다.

셋째, 태그 및 리더간 전송에서 리더에서 태그로의 포워드 전송은 암호화에 의해 안전구간으로 설정하며, 태그에서 리더간의 백워드 전송시 암호화 문제를 고려대상으로 한다.

이러한 조건에서 수정된 SEED 알고리즘의 적용 내용은 다음과 같다.

첫째, 암호화의 핵심인자는 리더로부터 전송받은 라운드 횟수(r)와 태그에서 생성하는 암호화 함수의 적용 횟수(e)로 한다.

또한, 공격자가 이를 알 수 없다는 사실에 근거한다. 즉 리더로부터 받은 라운드 키(Ki0,1)와 태그 내에서 생성된 암호화 함수 적용횟수(e)는 공격자에게 노출되지 않고 이 값들이 없으면, 공격자가 원본 메시지 복원이 불가능하다는 것을 전제로 한다.

둘째, 기존 SEED알고리즘에서는 정해진 라운드 횟수(16회)와 고정된 암호화 사이즈를 두고 있으나, 제안 알고리즘에서는 라운드 횟수와 암호화에 사용되는 비트수를 가변적으로 구성하여 태그내의 연산량을 경량화하였다. 즉 리더로부터 받는 라운드 횟수를 가변크기($r \leq 16$)로 설정함으로써 라운드 횟수 자체를 암호화 인자로 활용함과 동시에 태그 연산량을 줄이는 효과를 기대할 수 있다. 또한, 제안 알고리즘의 기반을 96비트로 설정하였으나, 전체 비트를 암호화하지 않고 그중 일정비트만을 부분적으로 암호화하여 태그 연산량을 줄이는 동시에 암호화 인자로 암호 비트수와 그 자리값을 활용하였다. 이상의 내용을 정리하면 다음 표 3과 같다.

표 3. RFID보안을 위한 제안 SEED 알고리즘 수정 내용
Table 3. Modified Factor of Proposed SEED Algorithm

알고리즘	기존 SEED	제안 SEED
암호화 횟수	16 라운드 고정	r 라운드 가변
암호함수 적용횟수	고정	가변
암호 대상 비트	고정 메시지 사이즈	가변 사이즈

그림 6는 수정된 SEED 알고리즘에 바탕을 둔 RFID 정보보호 시스템을 나타낸다. 제안 시스템에서 전체 처리과정은 96비트 입력 평문블록(ID)을 2개의 48비트 블록(L(48),R(48))으로 나누어, r-개의 48비트 라운드 키를 이용하여 r-라운드를 수행한 후, 최종 96비트 암호문 블록(Lr(48), Rr(48))을 출력한다.

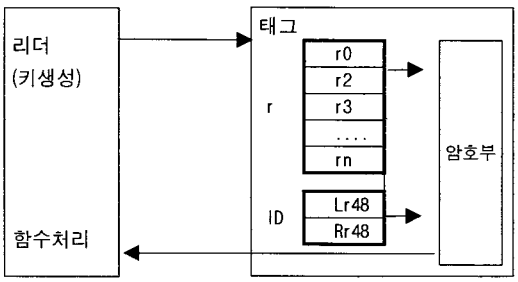

그림 6. 제안 RFID 태그 정보보호 기법
Fig 6. Proposed RFID Tag's Encryption Scheme

RFID 시스템에서 제안 알고리즘을 통한 정보보호 처리 절차는 다음과 같다. 리더부분과 태그부분으로 나눠 다음과 같이 설명한다.

4.3 리더기 처리 절차

리더는 태그와 통신하기 전에 난수 r, En, s와 ki,0, ki,1 값을 생성한다. 이때, r은 SEED 암호화를 위한 라운드횟수이며, s는 암호함수 적용횟수, Ls, Rs는 각각 암호화 시작비트로 G함수 처리시의 시작비트로 태그의 96비트 코드중 LSB 비트(38비트), RSB 비트(38비트)로부터 일정비트자리를 의미한다. 만약, Es가 5이면 LSB로부터 좌측으로 5번째 비트부터 LSB비트까지 5비트을 암호화하게 된다. 공격자는 몇 비트부터 암호화 되었는지 알 수 없기 때문에 암호화의 효율을 얻을 있다. 라운드 키(Ki0,1)는 그림 2에서의 좌우측 라운드 적용값이 된다. 이 값들은 리더에 보관되어 메시지의 복호화에 사용한다.

4.4. 태그의 처리 절차

태그는 리더로부터 전송받은 인자를 이용하여 메시지를 암호화 하여 태그로 전송한다. 태그에서 암호화 처리 단계는 다음과 같다.

단계 1에서는 리더로부터 받은 s, r을 적용하여 암호함수를 횟수만큼 적용한다.

단계 1: F함수 처리

```
C'= for(i=1; i++; i<= Ls)
   { for(ir=1; ir++; ir<= r)
    {
     {F - left 함수 with ki,0}
    }
    }
D'= for(j=1; j++; j<= Rs)
   { for(jr=1; jr++; jr<= r)
    {
     {F -right 함수 with ki,1}
    }
    }
```

이때, 수행되는 F-left 함수는 2개의 XOR 연산 3개의 모듈라 연산 및 3개의 G함수를 수행하고, F-right 함수는 2개의 XOR 연산 2개의 모듈라 연산 및 3개의 G함수를 수행한다.

단계 2에서는 LSB, MSB의 s 시작점부터 논리합 연산을 수행하여 암호화한다.

단계 2: G함수 연산

(X: 입력값, m:임의의 16진값-fc, f3, cf, 3f)

```
Z0=(S(Xs)&m0)
Z1=(S(Xs)&m1)
Z3=(S(Xs)&m2)
Z4=(S(Xs)&m3)
```

단계 3에서는 S-box 적용단계로 실제 태그 내에 구현하기 위해서는 많은 게이트수를 요구함으로 ‖연산을 수행하도록 간소화하였고, 향후 태그 메모리 개선에 따라 개선된 연산을 고려한다.

단계 3: S-box 연산

S:Z → Z,S(X) = Z0||Z1||Z2||Z3

기존의 SEED 알고리즘 표준은 128비트 암호키를 이용하여 메시지를 128비트 불록 단위로 암·복호화하는 알고리즘이다. 제안 보안 시스템은 EPC 표준 RFID 시스템의 96비트의 표준을 따른다.

V. SEED 기반의 백워드 채널 보호 기법 분석

제안 알고리즘의 성능 분석은 보안측면과 성능측면으로 구분하여 분석하였다.

5.1. 보안 분석

본 논문에 제안된 수정 SEED 암호 시스템의 보안성능은 백워드 채널(태그에서 리더로 전송시)에 정보보호에 측면에서 공격자가 획득할 수 있는 정보는 암호화된 96비트의 비트열이다.

본 논문에서는 태그내의 현실적인 암호화 모듈을 구현하기 위해 전체 코드를 암호화하지 않고 96비트 코드 중 일정부분(Es)을 일정횟수(En) 만큼 암호화하였다.

또한, 정형화된 라운드수 만큼 반복하여 함수를 적용하지 않고 랜덤하게 함수 적용회수(r)를 사용하여 함으로써 이상의 비밀키가 노출되지 않는다고 가정할 경우, 암호화된 위치 파악이 어렵다. 따라서 복원이 불가능하다. 단, 이때의 전제는 포워드(리더 → 태그) 구간의 전송은 안전한 것으로 가정한다.

5.2. 성능 분석

본 논문에서는 태그의 암호화 모듈의 경량화에 관점에서 암호화에 위해 소요되는 계산량과 시간측면에서 분석한다.

태그내에서 메시지 연산에 사용되는 암호 함수는 다음과 표 4와 같다.

Table 4. Operation Method of Tag Encryption
표 4. 제안 기법에서의 태그 암호 연산식

부 분	제안 기법의 연산량
암호연산(MSB)	2⊕+3⊞+6&+3‖
암호연산(LSB)	2⊕+3⊞+7&+3‖
전체 암호연산	4⊕+6⊞+13&+6‖

태그 코드중 MSB와 LSB의 부분으로 나눠 기존의 SEED 알고리즘에 F-함수에 준하여 연산하도록 하고 Ⓖ 연산 은 다시 &연산을 수행하기 때문에서 &연산으로 대치하여 전체 연산량을 추정하여 식(3)과 같다.

$$Tag_{Enc()} = 4\oplus + 6\boxplus + 13\& + 6\| \text{ ---------- 식(3)}$$

식(3)을 일반화하여 태그에서 연산되는 총 연산량을 구하면 식(4)와 같다.

$$\sum_{i=1}^{10 \le s \le 72} \cdot \sum_{j=1}^{3 \le r \le 16} Tag_{Enc()} \text{ ---------- 식(4)}$$

제안 방식에서는 최소 10의 암호비트(MSB, LSB 각각 5개씩)에서 최대 72비트까지만 암호화하는 부분암호방식을 취하고, 라운드 연산도 최소 3회에서 16까지로 부분라운드를 채택한다. 따라서, Te, Tr을 암호및 라운드 연산에 소요되는 시간이라 할 경우, 총 연산량은 최소 10Te×3Tr개에서 최대 72Te×16Tr개만큼의 태그 암호연산(Tagenc())를 수행한다. 따라서, 암호화 모듈이 동일하다고 했을 경우, 96비트 전체 비트를 암호화하는 방식에서 소요되는 비용인 96E×16R에서 비해 최대 9.6배의 계산효율과 5.3배의 라운드 반복 효율을 기대할 수 있다. 태그내 암호모듈을 구현한 실제비교대상이 없으나, 본 논문에서 제안하는 방식을 통해 제안적인 컴퓨팅 파워를 가진 태그에서 3,000게이트이하로 보안 모듈을 구현할 수 있는 방향을 제시하고자 한다.

VI. 결 론

최근 전 세계적으로 RFID 도입에 따른 사생활 침해를 방지하기 위한 법안 마련에 여러 나라들이 고심하고 있다. 가까운 장래에 RFID 산업이 활성화되면 정보보호 및 사생활 침해가 국가, 사회적인 핵심 이슈로 등장할 것이다. 이에 대비해 정보보호를 위한 법과 제도의 제정과 더불어 이를 뒷받침할 수 있는 정보보호 기반기술 개발을 서둘러야 할 추세이다.

따라서, 본 논문에서 RFID 보안 기법에서 요구되는 조건인 태그와 리더간의 백워드 채널 데이터 전송 암호화를 고려해서 SEED 기반의 백워드 채널 보호 기법을

제안했다. 향후 보안 기법 구현 시 태그의 제한적인 연산 능력과 한정된 메모리 공간의 최소 사용, 실시간 상호 작용을 위한 처리속도 개선 등의 문제들을 해결해야 한다.

참고문헌

[1] E. Fujisaki and T. Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In CRYPTO' 99, pages 537-554. Springer-Verleg, 1999. LNCS no. 1666

[2] Marcel Jacomet, Adrian Ehrsam, Urs Gehrig, "Contactless Identification Device With Anticollision Algorithm," IEEE Computer Society, CSCC'99, Conference on Circuits, Systems, Computers and Communications, 4th-8th July 1999, Athens, Greece, ISBN 960-8052-03-3, pp 269-273.

[3] Stephen Weis, Sanjay Sarma, Ronald Rivest, and Daniel Engels, "Security and privacy as- pects of low-cost radio frequency identification systems," International Conference on Security in Pervasive Computing, March 2003.

[4] Stephen August Weis, "Security and Privacy in Radio-Frequency Identification Devices," MASSACHUSETTS INSTITUTE OF TECHNOLOGY, 2003.

[5] Ari Juels, Ravikanth. Pappu, "Squealing euros: Privacy protection in RFID-enabled banknotes," In Proceedings of Financial Cryptography, 2003.

[6] "전파식별(RFID) 보급 활성화를 위한 역기능 및 정보보호 대책연구,"한국전산원, 2004.

[7] 한국정보보호진흥원, "128 비트 블록암호알고리즘 (SEED) 개발 및 분석보고서." version 1.1, 2003. 10. 23.

저자소개

김 성 진(Sung Jin Kim)

1996년 서경대학교 컴퓨터과학과 (공학사)
1998년 경원대학교 대학원 전자계산학과(공학석사)
2008년 : 경원대학교 대학원 전자계산학과(공학박사)
※관심분야 : Ubiquitous Computing, RFID, 정보보호

박 석 천(Seok Cheon Park)

1977년 고려대학교전자공학과 학사
1982년 고려대학교 대학원 컴퓨터 공학 석사
1989년 고려대학교 대학원 컴퓨터 공학 박사
1979년～1985년 금성통신연구소
1991년～1992년 University of California, Irvine Post Doc.
1988년～현재 경원대학교 소프트웨어학부 정교수
※관심분야 : 차세대 인터넷, 멀티미디어 통신, Mobile Network