이동통신망 환경에 적합한 블럭 암호 알고리즘의 비교 분석

정성혁, 김정태

목원대학교

Analyses and Comparision of Block Encryption Algorithm in Wireless Network

Sung-Hyuk, Jung, Jung-Tae Kim,

Mokwon University

E-mail : jtkim3050@mokwon.ac.kr

요 약

본 논문에서는 기존의 관용알고리즘을 비교 분석하고, 유무선 복합 통신망에서의 고속화를 위해 요구되는 암호알고리즘을 비교 분석한다. 기존에 사용되고 있는 블록 알고리즘의 경우, 고비도에 의해서 소프트웨어적 혹은 하드웨어적으로 설계하였을 경우, 현재의 이동통신망에 사용을 하였을 경우, 속도의 차이에 의해 사용이 불가능 하다. 따라서, 본 논문에서는 이동통신 환경망에 적합한 블록알고리즘을 제안하고 분석하고자 한다.

1. 서론

현재의 정보화 사회에서는 많은 정보들이 인터넷등의 매개체를 통해 공유를 하고 이러한 정보등을 이용하여 개인 또는 기업의 중요한 업무를 수행하고 있다. 따라서 공개용을 사용하는 정보 이외에 개인 또는 기업의 비밀 정보등도 이러한 매개체를 통해 상대방에게 전달되고 있는 현실이다. 따라서 오늘날에는 이러한 정보를 보호하기 위해 비공개 정보에 대한 암호화를 하고 이를 다시 복호화 하는 방식을 통해 주고 받는 이외의 장소에서 이러한 정보에 대한 노출을 보호하고 있다. 이를 암호 알고리즘이라 한다. 오늘날에는 이러한 알고리즘의 방식도 여러 종류로 나뉘어져 사용을 하고 있고, 정보화 사회의 발달에 따라 이러한 알고리즘도 계속 발전하고 있는 추세이다. 또한 정보화 추세에 발맞추어 암호화 과정의 속도 또한 중요한 요소로 자리잡고 있다. 암호화 알고리즘을 사용하는 목적은 기본적으로 통신하는 당사자 이외의 다른 사람에게 메시지를 알려주지 않기 위한 것이지만 그 밖에 다음과 같은 목적으로 암호를 사용한다.

· 기밀성(Confidentiality) : 암호를 사용하는 1차적인 목적이다. 허가된 사람 이외에는 그 내용을 알아볼 수 없도록 한다.

· 무결성(Integrity) : 외부의 요인으로 인해 데이터가 변조(변경, 삽입, 삭제 등)되었는지를 알 수 있도록 한다.

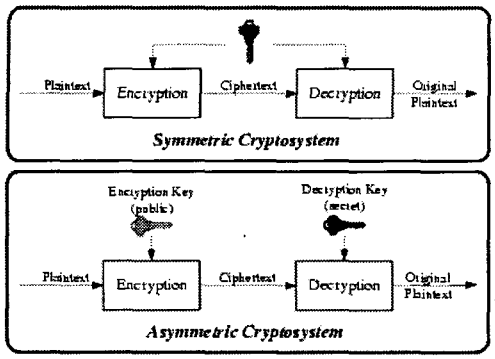
· 인증(Authentication) : 통신하고 있는 상대방이 실제로 맞는지를 확인하고, 서로에게 전송한 데이터가 위조되지 않았음을 확인할 수 있도록 한다.

· 부인방지(Non-repudation) : 이전의 통신내용을 보낸적이 없다고 속일 수 없도록 한다. 즉, 데이터를 받은 사람은 나중에라도 보낸 사람이 실제로 데이터를 보냈다는것을 증명할 수 있도록 한다.[1]

본 논문에서는 이러한 알고리즘이 어떠한 종류가 있는지 분석해 보고 이러한 알고리즘이 현재의 고속 통신에 이용하기 위한 최적의 알고리즘의 방법을 제시해 보도록 하겠다.

2. 관용 암호화 알고리즘

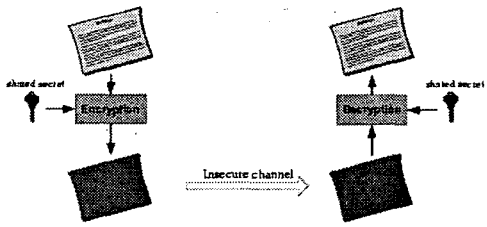
암호화 알고리즘은 현재 방식에 따라 공개키 암호화 알고리즘과 비밀키 암호화 알고리즘으로 구분지어 지고 있다. 이는 암호화하는 과정과 복호화 하는 과정에서 동일키를 사용하는지, 아니면 서로 다른 키를 사용하여 이러한 작업을 수행하는지에 따라 이러한 것을 구분 지을 수 있다.



[그림 1] 암호 알고리즘[1]

2.1 비밀 키 암호화 알고리즘

비밀 키 암호 알고리즘은 암호화에 사용된 키를 일반에게 공개하지 않고 개인이 서로 비밀로 하여 키를 아는 자만이 암호화된 정보를 볼 수 있도록 하는 알고리즘이다. 그래서 이 알고리즘은 쌍방이 사전에 암호화 키를 서로 공유해야만 한다. 이러한 알고리즘의 성질로 대칭키 암호 알고리즘으로도 불리고 있다. 알고리즘의 특징은 보면 앞서 말한 것과 같이 암·복호화 키를 동일하게 사용하고 있다. 또한 이러한 키에 대한 정보를 서로 공유를 하고 있으므로 암·복호화에 따른 처리 속도를 빨리 가져갈 수 있지만, 키의 생성과 관리 또한 사용자간의 키의 교환 과정에서 발생하는 키 예상 공격에 대한 대처가 취약한 단점이 있다. 대표적인 비밀키 암호화 알고리즘의 예로는 DES 알고리즘이 전세계적으로 널리 사용되고 있었으나. 짧은 키 길이 등으로 인한 안정성의 문제로 AES 블록 암호 알고리즘이 사용될 전망이다. 두 알고리즘 모두 블록 암호 알고리즘으로 문서를 일정한 단위로 분할해, 이렇게 분할된 문서 단위별로 암호문을 얻는 방식이다.



[그림 2] 비밀키 암호화 과정[1]

2.2 공개키 암호화 알고리즘

공개키 암호와 알고리즘은 암호화할 때에 사용되는 키를 공개한 알고리즘 방식이다. 따라서 정보의 암호화한 과정은 공개키를 통해 누구든지 이러한 방식을 알 수 있다. 하지만 이렇게 암호화된 것은 비공개되어 있는 개인키(비밀키) 등을 이용하여 복호화 과정을 수행하여야 한다. 따라서 공개키를 통해 한번 암호화된 문서는 개인이 가지고 있는 비밀키를 가지고서만 본래의 형태로 얻을 수 있다. 이러한 방식의 등장은 비밀키 알고리즘에서 사전에 비밀 키를 서로 공유하고 있어야 한다는 전제 조건이 붙게 된다. 따라서 이러한 비밀 키에 대한 안전한 전달이 요구된다. 따라서 이러한 문제점을 보완하기 위해 공개키 알고리즘이 등장하게 된 것이다.

공개키 암호를 구성하기 위해서는 다음과 같은 성질을 만족해야 한다.

· 암호문을 복호화하면 원래의 평문을 얻어야한다.

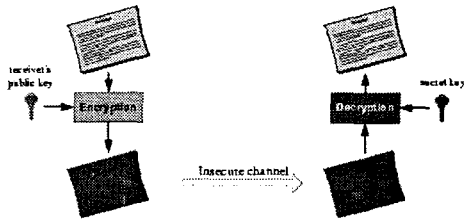
· 암호화 하는 함수는 누구나 계산할 수 있다.

· 비밀키를 모르면 함수의 복호화가 작업이 어렵다.

· 비밀키를 알면 함수의 복호화가 쉽게 계산하여 처리한다.

· 공개키로부터 비밀키를 구하는것은 현실적으로 불가능하다.

· 사용자의 공개키와 사용자의 신분을 연결할 수 있는 공개키 기반 구조가 필요하다.[1]



[그림 3] 공개키 암호화 과정[1]

공개키 암호의 암·복호화 함수의 대부분은 수학적으로 어려운 문제를 가지고 있다. 따라서 이러한 수학적 소인수 분해의 결과를 알면 월래의 수는 곱셈에 의해 간단히 구해지는 사실에 바탕을 두는 RSA 알고리즘이 공개키 알고리즘의 대표적인 것으로 세계 표준이라 불린다.

3. ARIA 암호화 알고리즘

이상의 관용의 대표적인 알고리즘을 알아보았다. 여기에서의 알고리즘은 대부분 비용적인 부분의 문제로 암호 알고리즘이 소프트웨어로 구현되고 있지만, 모발일 기기나 네트워크 장비와 같이 PC에 배해 낮은 성능의 CPU를 사용하거나, 고속으로 정보를 처리해야 할 경우에는 이러한 소프트웨어적인 처리의 한계가 생기게 된다.[2] 따라서 고속의 데이터 처리를 위해서는 이러한 소프트웨어적인 개념을 벗어난 다른 개념의 암호화 방식이 나와야 한다. 현재 이러한 관용적인 방식의 대안으로 ARIA알고리즘 방식을 사용하고 있다. 이러한 알고리즘 방식은 대한미국 표준 암호 알고리즘 방식으로 민간 암호화 알고리즘 시드와 함께 행정 서비스용으로 보급되고 사용하고 있으며, 스마트 카드 등의 초경량 환경및 고성능 서버 환경 등에서 시드에 비하여 상대적인 장점을 가지고 있다.

3.1 알고리즘 구조

- 기본구조 : ISPN (Involutional SPN) 구조
- 입/출력 크기 : 128 bit
- 키 크기 : 128, 192, 256 bit
- 라운드 키 크기 : 128 bit
- 라운드 수 : 키 크기에 따라 12,14,16 라운드

이 사양을 블록 단위(8 bit)로 정리하면 표 1과 같다. 이 때, 입/출력 블록 크기를 N_b, 입력 키 블록 크기를 N_k, 그리고 라운드 수를 N_r로 나타내면 다음 표와 같이 된다.

Item	N_b	N_k	N_r
ARIA-128	16	16	12
ARIA-192	16	24	14
ARIA-256	16	32	16

[표 1] ARIA 사양

라운드 함수는 다음과 같은 세 부분으로 구성되어 있다.

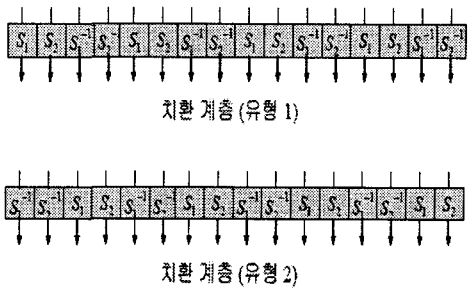
1. 라운트 키 더셈(AddRoundKey): 128bit 라운드 키를 라운드 입력 128bit별 XOR한다.
2. 치환 계층(SubstLayer): 두 유형의 치환 계층이 있으며 각각은 2종의 8bit 입/출력 S-box와 그들의 역변환으로 구성된다.
3. 확산 계층(DiffLayer): 간단한 16 × 16 involution 이진 행렬을 사용한 바이트 간의 확산 함수로 구성되어 있다.

3.2 알고리즘 구성 계층

3.2.1 치환 계층

지환 계층은 8bit 입/출력 S-box들로 구성된다. 이는 다음의 성질은 만족하도록 구성된다.

- 최대 차분/선형 확률 : 2^{-6}
- 대수적 차수 : 7
- 고정점, 반고정점이 없을 것



[그림 4] 치환 계층의 유형

3.2.2 확산 계층

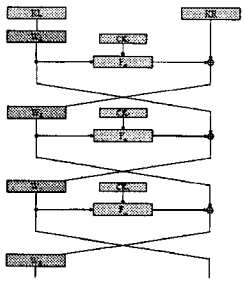
확산 계층은 ARIA와 다른 블록 암호를 구별짓는 주요 부분으로 16 × 16 involution 이진 행렬을 사용한다.

ARIA의 확산 계층은 다음과 같은 설계 방향을 가지고 설계되었다.

- AES에 강력한 분석 방법들에 대하여 내성을 가져야 한다. 이를 위해서 AES의 확산 함수 처리 단위(32 bit)보다 큰 단위의 확산 함수를 사용한다.
- 8 bit, 32 bit 소프트웨어 및 하드웨어 구현에 적합해야 한다.
- 동종의 확산 함수 중에서 안전성과 효율성을 고려할 때 제일 우수해야 한다.

3.2.3 키 확장

1) 초기화 과정



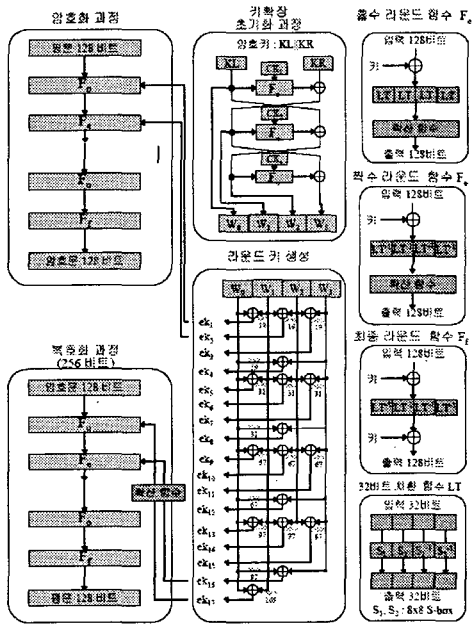
[그림 5] 초기화 과정

초기화 과정에서는 암/복호화 한 라운드를 F 함수로 하는 256 bit 입/출력 3라운드 Feistel 암호를 이용하여, 암호키(MK)로부터 네 개의 128 bit 값 W_0, W_1, W_2, W_3를 생성한다.

$$W_0 = KL$$
$$W_1 = F_0(W_0, CK_1) \oplus KR$$
$$W_2 = F_e(W_1, CK_2) \oplus W_0$$
$$W_3 = F_0(W_2, CK_3) \oplus W_1$$

2) 라운드 키 생성 과정

라운드 키 생성 과정에서는 네 개의 128 bit W_0, W_1, W_2, W_3를 조합하여 암호화 라운드 키 ek_i와 복호화 라운드 키 dk_i를 생성한다.



[그림 6] ARIA 알고리즘

4. 결론

현재의 정보의 전달 구조는 인터넷등과 무선 단말기등의 매체를 통해 무수히 많은 양의 정보가 동시에 전달되고 또한 고속의 통신이 이루어 지고 있는 시대이다. 또한 이러한 정보에는 제 3자에게 공개가 되어 지지 않아야 할 비공개 정보도 포함 되어있다. 따라서 현재에는 앞서 설명한 것과 같은 관용의 보안 알고리즘을 가지고 이러한 보안 정보에 대한 대책을 마련하고 사용하는 실정이다. 하지만 정보화 시대에 고속의 통신을 이루어 지고 있는 시점에 이러한 관용의 보안 알고리즘 때문에 데이터의 전송에 지장을 받아서는 안되어야 한다. 따라서 현 시점에서는 보안과 더불어 속도적인 면에서도 생각을 해 보아야 할 때다. 따라서 본문에서 설명된 ARIA 알고리즘을 이용하여 소프트웨어적인 개념을 넘어선 하드웨어적으로도 보완을 이루어 이러한 점의 개선을 이루어야 할 때다.

참고 문헌

[1] 퓨전 시스템 암호 체계 센터 , '암호 알고리즘 및 프로토콜의 이해'

[2] 암호화 알고리즘 ARIA의 FPGA 기반의 하드웨어 구현

[3] www.nsri.re.kr/ARIA, 국가보안기술연구소

[4] SEED 블록 암호 알고리즘의 파이프라인 하드웨어 설계

[5] www.rootca.or.kr/kcac.html , 한국정보보호진흥원