TETRA 단말기용 스마트카드에서의 알고리즘 성능 비교

안재환 · 박용석· 정창호· 안정철

국가보안기술연구소

Comparison of Algorithm Performance in the Smart Card used as the TETRA terminal encryption module

Jae Hwan Ahn · Yong Seok Park· Chang-Ho Jung· Joung Chul Ahn

National Security Research Institute

E-mail : jaehwan@etri.re.kr

요 약

본 논문에서는 TETRA 시스템의 종단간 암호화에 사용되는 스마트카드의 성능요구조건을 만족하는 여러 암호 알고리즘의 구현 가능성에 대해 살펴본다. 삼성전자의 32 비트 스마트카드 IC에 독자 운영 프로그램을 동작시켜 알고리즘의 동작시간을 측정한다. 성능 비교에 사용된 알고리즘들은 국내외 표준으로 제정된 AES, ARIA, 3DES, SEED, IDEA이다. 스마트카드 프로토콜 분석기를 사용하여 스마트카드 입출력 시간을 측정하며 알고리즘 반복 수행을 통해 알고리즘만의 동작시간을 유추한다. 본 실험결과는 TETRA 시스템의 종단간 암호화용 스마트카드에 적용 가능한 암호 알고리즘 선정의 기초 자료로 활용될 수 있고, 우위의 성능을 가지는 알고리즘을 적용하여 스마트카드 운영 프로그램의 구현을 위한 충분한 여유시간을 확보하여 부가 기능을 구현하는데 적절히 활용될 수 있다.

ABSTRACT

It is studied the implementation possibility of some encryption algorithms which meet the performance requirements in the smart card used in the TETRA system End-to-End Encryption. It is measured the operation time of the algorithm in the smart card which has 32 bit smart card controller made by Samsung Electronics. The algorithms used in the performance comparison are AES, ARIA, 3DES, SEED, IDEA which are the domestic or international standards. The input and output time of the smart card are measured using the smart card protocol analyzer. The pure algorithm operation time is calculated by the repeated algorithm operations. This measurement results can be used as the criteria for the selection of algorithm which will be used in the TETRA End-to-End encryption system. The algorithm which has better performance can be used for the implementation of additional functions in the smart card, because of the enough time margin.

키워드

TETRA, 종단간 암호화, 스마트카드, Algorithm

Ⅰ. 서 론

TETRA는 ETSI (European Telecommunications Standardisation Institute)에 의해 정의되는 공용 주파수 라디오 시스템이다. 세계 각국의 공공안전, 응급 재난시의 통신망으로 사용되고 있으며 주용도는 그룹통신을 위한 것이다.

공공안전기관, 경찰과 같은 사용자들에 의해 사용되는 시스템이기 때문에 보안요구사항이 요구된다. TETRA에서는 시스템 보안을 위하여 2가지 수준의 기능을 제공한다.

첫 번째는 무선구간 암호화이다. 이는 사용자 단말과 기지국의 무선구간 사이에서의 사용자 데이터뿐만 아니라 시그널링 정보 및 사용자 ID 정보가 암호화된다. 무선구간을 벗어나 기지국 이후 단계에서 복호화되는데 이는 기지국 이후의 시스

템 내부에서 시그널링 정보 및 사용자 ID 정보가 사용되어야 하기 때문이다.

두 번째는 종단간 암호화이다. 이는 최종 사용자와 또 다른 사용자 사이의 시그널링 정보나 ID 정보는 암호화될 수 없으므로 대상에서 제외되고 사용자의 음성 및 데이터만이 암호화되어 전달된다.

보안수준으로 종단간 암호화 기능을 단말기 쪽에서 구현하고자 할 경우 단말기 내부 또는 외부에 암호화 기능을 담당하는 부분이 있어야 한다. 이 기능을 소프트웨어적인 방법과 하드웨어적인 방법으로 구현할 수 있는데 소프트웨어적인 방법은 암호화의 측면에서 바람직한 방법이 아니기 때문에 하드웨어적인 방법으로 별도의 암호모듈을 장착하거나 단말 보드에 통합하는 방법을 사용해야 한다. 또는 단말기 외부 인터페이스를 통해 연결하는 다른 장치를 생각할 수 있다. 단말기 내부에 암호모듈을 장착하거나 단말 보드에 통합하는 방법은 치명적인 약점을 가지고 있다. 단말기와 독립적으로 제작할 수 있는 장치가 아니기 때문에 단말기의 모델이 변경될 경우 별도의 암호모듈을 제작해야 하는 점이다. 종단간 암호화는 특수 직무를 수행하는 기관의 요구에 의해서 사용될 수 있는데, 수요가 많지 않을 경우 종단간 암호화 단말에 대한 비용이 커질 수밖에 없고 별도로 제작해야 한다는 것은 추가개발기간을 필요로 하게 된다.

이에 대한 대안으로 단말기 외부 인터페이스를 통해 다른 암호장치를 연결하여 사용하는 방법이 있다. 즉 단말기의 스마트카드 인터페이스를 통해 장착되는 스마트카드를 암호장치로써 사용하는 것이다. 이 방법을 사용함으로써 단말기 내부에 스마트카드 인터페이스를 구비하면 단말기 모델에 독립적으로 스마트카드를 통해 암호기능을 수행할 수 있게 된다[1].

스마트카드는 단말기의 명령에 대해 응답하는 기기이고 사용자의 음성데이터는 실시간으로 처리되어 전송되어야 한다. 즉 단말기의 암호화 요구에 정해진 시간 내에 응답을 줄 수 있어야 암호화 기능을 수행할 수 있게 된다. 이는 스마트카드 내부의 프로그램 구동 시간이 정해진 시간을 넘지 않아야 된다는 것을 의미한다. 스마트카드의 응답 시간은 스마트카드 자체의 하드웨어적인 성능과 함께 암호알고리즘의 속도에 의해서 좌우된다. 따라서 본 논문에서는 공개되어 있는 여러 암호알고리즘에 대해 스마트카드에서의 반응속도를 점검해 봄으로써 TETRA시스템의 종단간 암호화를 위한 스마트카드에서의 탑재가능성을 점검해 보고 각 알고리즘의 속도우위를 비교해 보도록 한다.

II. 종단간 암호화를 위한 스마트 카드의 요구조건

TETRA 시스템에서 30 ms의 시간 길이를 가지고 137 비트의 크기를 가지는 음성 코덱 ACELP의 출력 두 개가 모여 하나의 TDMA 프레임을 구성한다[3-5]. 하나의 TDMA 프레임을 구성하는 2개의 ACELP 출력의 비트 길이는 총 274 비트가 된다. 종단간 암호화는 이렇게 출력되는 ACELP의 274 비트와 스마트카드로부터 출력되는 KSS(Key Stream Segment)를 XOR시켜 암호문을 얻는다[5].

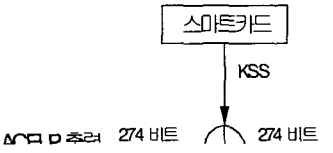

그림 4. 음성 데이터의 종단간 암호화

스마트카드는 한 번의 응답으로 60 ms 안에 274 비트의 KSS과 함께 부가 데이터 비트를 포함해 대략 400 비트열을 출력한다.

스마트카드 내부에서 128 비트의 블록 알고리즘을 사용한다고 할 때 4번 구동시켜 얻을 수 있는 데이터 길이이다. 실시간으로 만들어지는 ACELP의 출력을 올바로 암호화하기 위해서는 스마트카드에 KSS 출력을 요청하는 REQ 신호가 들어가서 스마트카드에서 400 비트열이 도달하기까지 60 ms 이내이어야 한다.

단말기가 REQ 신호를 보내면서 스마트카드의 출력비트열이 단말에 도착하기까지의 시간 계산을 위해서 다음 항목들을 살펴보아야 한다

- 스마트카드로의 REQ신호가 완전히 전달되는 시간
- 스마트카드 내부 운영 프로그램에서 입출력 루틴을 처리하고 알고리즘을 제외한 모든 기능을 수행하는 시간
- 스마트카드 내부 알고리즘이 동작하는 시간
- 스마트카드에서 만들어진 400 비트의 데이터가 단말로 완전히 전달되는 시간

크게 분류해 보면 입출력 핀을 통한 전송시간과 스마트카드 내부 동작시간으로 분류할 수 있다. 전송시간은 단말과 스마트카드의 전송속도(baud rate)의 약속을 통해 이루어지며 사용되는 스마트카드 IC의 성능에 의해 좌우된다고 할 수 있다.

스마트카드는 ISO 7816의 전송 프로토콜에 의해 작동하는데 REQ 신호는 명령 APDU에 의해 스마트카드로 전달되고 응답 데이터는 응답 APDU에 의해 단말기로 전달된다. 표준 전송 프로토콜로 T=0 프로토콜과 T=1 프로토콜이 있는데 본 실험에서는 T=1 프로토콜을 사용해 구현하였다. T=1 프로토콜에서 REQ신호를 구성하는 데이터 길이는 헤더를 합하여 8 바이트가 되고, 응답 데이터는 54 바이트가 된다[6]. 입출력 모두

합해 비트로 계산하여 496 비트가 된다. 본 실험에서 지원되는 전송속도 223.2 kbps에서 496 비트의 전송을 계산하면 소요되는 시간은 2.2 ms가 된다. 참고로 9600 bps에서는 51.6 ms가 계산된다.

스마트카드 내부 동작시간은 스마트카드 운영 프로그램의 동작에 소요되는 시간과 순수 알고리즘의 동작에 소요되는 시간으로 나눌 수 있다. 스마트카드 내부 동작에 소요되는 시간은 프로토콜 분석기를 통해 측정할 수 있다. 프로토콜 분석기는 하드웨어적으로 입출력 핀을 통해 전달되는 데이터의 흐름을 살펴보는 장비이기 때문에 알고리즘만의 동작시간을 파악할 수는 없다. 순수 알고리즘만의 동작시간을 얻기 위한 방법은 3장의 성능측정에서 다룬다.

실험을 통해 다음과 같이 전체 소요되는 시간을 구할 수 있다.

전체 시간 = SMC 운영 프로그램 동작 시간 + 알고리즘 동작 시간 + 전송 시간 + 여유시간

부가기능 포함가능성을 고려하여 운영 프로그램 동작 시간과 여유시간을 길게 30 ms로 잡고 전송시간 2.2 ms를 반영하면 알고리즘의 동작은 27.8 ms 내에 이루어져야 한다. 즉 128 비트 블록 알고리즘을 4번 구동하는데 소요되는 시간이 27.8 ms 이내이어야 한다. 즉 알고리즘은 512비트 /27.8 ms = 18.4 kbps 이상으로 동작하여야 한다. 이의 가정은 전송속도가 223.2 kbps로 동작해야 한다는 것이다.

III. 각 알고리즘의 성능 측정 및 비교 분석

실험에 사용된 스마트카드는 삼성전자의 32 비트 스마트카드 IC를 사용하였으며 독자 개발된 운영 프로그램을 통하여 전체 동작을 수행한다. 알고리즘 부분이 모듈화되어 있어 각 실험시마다 알고리즘만을 교체하여 동작시간을 측정한다. 스마트카드는 내부 동작 클럭에 의해 속도가 좌우되는데 본 카드에서는 14 MHz로 클럭을 설정하였다.

성능측정에 사용된 알고리즘들은 국내외 표준으로 제정된 ARIA, AES, SEED, 3DES, IDEA로 최적화된 상태의 코드를 사용하였다. 출력비트의 크기가 같도록 운영 모드를 설정하였으며 사용된 키 크기는 모두 128 비트이다. 실험값의 안정성을 위해 5회 이상 반복하여 측정한 값의 평균을 취하였다.

스마트카드 운영 프로그램과 알고리즘을 스마트카드 IC에 탑재하여 동작 가능한 상태로 만들고 PC의 스마트카드 리더와 스마트카드 사이에 프로토콜 분석기를 연결한 후 스마트카드 제어 프로그램을 이용해 PC에서 암호화 REQ 신호를 보내면 일정 시간 뒤에 KSS를 담고 있는 응답 신호가 PC에 도착한다. 통신과정의 일련의 신호값들은 중간에 위치하는 프로토콜 분석기에 의해 읽히고 분석된다. 그림 2에 분석기에 의해 읽혀진 신호의 일부분을 보인다. PC의 명령이 전달되는 시간과 스마트카드 내부에서 처리되는 시간, 그리고 스마트카드에 의해 만들어진 데이터가 PC로 전달되는 시간을 보여준다.

그림 5. 프로토콜 분석기가 가로챈 신호

스마트카드의 입력과 출력에 사용되는 데이터의 길이는 비교에 사용되는 알고리즘마다 일정하기 때문에 알고리즘들의 비교를 위해서는 스마트카드 내부동작에 의해 소요되는 시간만을 비교대상으로 한다. 그림 2에서는 3.84 ms가 스마트카드 내부동작에 소요된 시간을 의미한다.

표 1은 비교 대상의 알고리즘들로 실험을 했을 때 측정된 스마트카드 내부동작 시간을 나타낸 것이다.

표 1. 각 알고리즘별 스마트카드 내부동작 시간

알고리즘	시간(ms)
ARIA	1.58
AES	1.55
SEED	1.78
IDEA	1.65
3DES	2.96

표 1의 값은 스마트카드 내부 동작시간을 나타낸 것이기 때문에 이를 스마트카드 운영프로그램에 의한 시간과 순수 알고리즘의 동작에 의한 시간으로 분리해야 한다.

운영 프로그램 내에서 순수 알고리즘을 구동하는 부분을 2회 구동하도록 하여 측정한 결과와 1회 구동하여 측정한 결과를 비교하여 알고리즘의 구동 시간과 그 외 운영 프로그램의 구동 시간을 구별할 수 있다.

알고리즘을 1회 구동했을 때의 스마트카드 내부 동작 시간을 T1, 2회 구동했을 때의 시간을 T2, 운영 프로그램 동작 시간을 OST, 알고리즘 1회 동작 시간을 ALGT라고 하면 다음과 같은 식을 만들 수 있다.

T1 = OS + ALGT

T2 = OS + ALGT *2

T2와 T1의 차이가 ALGT, 즉 알고리즘 구동 시간이 된다. 이는 알고리즘 횟수에 관계없이 운영 프로그램 동작 시간이 일정하기 때문에 가능하다.

위 식을 토대로 위의 알고리즘들을 2회 구동하여 측정한 결과와 1회 구동하여 측정한 결과를 표로 나타내면 표 2와 같다.

표 2. 알고리즘 구동 횟수에 따른 시간측정

알고리즘	시간(ms)		
	1회	2회	차이(알고리즘 구동시간)
ARIA	1.58	2.14	0.56
AES	1.55	2.08	0.53
SEED	1.78	2.54	0.76
IDEA	1.65	2.28	0.63
3DES	2.96	4.91	1.95

결과적으로 각 알고리즘들의 동작은 3DES를 제외하고는 1 ms 안쪽에서 이루어짐을 확인할 수 있다. 3DES만이 1 ms를 넘는데 AES에 비해 3.68 배 정도 느리다고 할 수 있다.

표 2와 위의 알고리즘 동작 시간 계산식으로부터 운영 프로그램의 동작시간이 공통적으로 1.02 ms 정도 나옴을 알 수 있다.

실험에 사용된 알고리즘들은 2장에서 제시한 스마트카드에서의 알고리즘 속도 요구조건인 27.8 ms 이내를 모두 만족한다고 할 수 있다. 그러나 위 구동시간은 스마트카드 IC의 성능에 많은 의존성을 가지기 때문에 실험에 사용된 스마트카드 IC의 성능에 미치지 못하는 환경에서는 구동시간이 많이 늘어날 수 있다. 스마트카드에 사용된 CPU와 지원되는 내부 클럭값이 성능좌우의 요인이 될 수 있다.

본 실험에서는 223.2kbps라고 하는 빠른 전송속도로 비트 전송을 하는데 낮은 전송속도만이 지원되는 스마트카드라고 하면 위 27.8 ms 이내라는 요구조건은 수 ms 이내로 낮아 질 수도 있다.

본 실험환경은 운영 프로그램이 기본적인 동작을 하도록 만든 환경이기 때문에 부가의 기능을 추가하여 스마트카드를 구현할 경우에는 전체 스마트카드 내부 동작에 소요되는 시간이 많이 늘어날 수 있음을 고려해야 한다.

스마트카드 환경에서 측정된 위 결과는 인텔 PC기반 환경에서 측정한 값과 비교해 볼 수 있는데 같은 알고리즘 코드를 바탕으로 PC에서 측정한 값은 표 3과 같다.

표 3. 각 알고리즘별 PC에서의 동작 시간(알고리즘 반복 50만회)

알고리즘	시간(s)
ARIA	1.325
AES	1.078
SEED	4.422
IDEA	15.672
3DES	29.063

빠르기의 순서상으로는 PC에서와 스마트카드에서의 결과가 비슷하지만 속도차이 측면에서는 대비되는 결과를 살펴볼 수 있다. 이는 사용된 CPU의 명령 실행 구조, 메모리 사용 환경 및 기타 실행환경의 차이에서 발생한다고 볼 수 있다.

IV. 결 론

TETRA의 종단간 암호화에 사용되는 스마트카드에서 구현될 수 있는 알고리즘들에 대해 살펴보았다. 총 5개의 알고리즘들을 구동하여 알고리즘만의 성능측정을 하였는데, 가장 빠른 속도를 지닌 것은 AES이고, 가장 느린 것은 3DES임을 확인할 수 있었다. 측정에 사용된 알고리즘 모두 1ms 내외의 동작시간을 보였다. PC환경에서 측정한 결과와 비교했을 때 빠르기 순서상에서는 비슷한 결과이지만 PC환경에서와 같은 현격한 차이를 보이지는 않았다.

가장 빠른 실행속도를 얻기 위해서 AES를 사용할 수 있겠지만 3DES를 제외한 다른 알고리즘도 30% 정도의 성능차이 범위 내에서 고려해 볼 만 하다. 동작 속도 측면에서는 실험에 사용된 알고리즘 모두 종단간 암호화용 스마트카드에 사용 가능하다고 볼 수 있다. 단 비도의 개선을 위해서 128 비트를 넘는 키 크기를 사용한다고 하면 성능차이 5%정도에서 ARIA와 AES를 선택하여 사용할 수 있겠다.

참고문헌

[1] Dittmar, R. "Smart Card Based End-to-End Security for TETRA Radio Networks", IEE Seminar on(Digest No. 2003/10059), pp 8/1 ~ 8/5, Feb, 2003

[2] John Dunlop, Demessie Girma, James Irvine, Digital Mobile Communications and the TETRA system, John Wiley & Sons, Ltd, 2003

[3] ETSI EN 300 392-1, Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 1: General Network Design, 2005

[4] ETSI EN 300 392-2, Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 2: Air Interface, 2005

[5] ETSI EN 300 392-7, Terrestrial Trunked Radio(TETRA); Security; Synchronization mechanism for end-to-end encryption, 2003

[6] ISO/IEC 7816-3 Identification cards-Integrated circuit cards with contacts - Part 3: Electronic signals and transmission protocols