TRS 단말기용 스마트카드에서의 블록 암호 알고리즘의 동작 성능 비교 및 분석

안재환, 박용석, 안정철
한국전자통신연구원 부설연구소
e-mail:jaehwan@ensec.re.kr, parkys@ensec.re.kr, jcahn@ensec.re.kr

The comparison and the analysis of commercial algorithm performance in the smart cards of the TRS terminal

Jaehwan Ahn, Yong-seok Park, Jeong-chul Ahn
The Attached Institute of ETRI

요 약

본 논문에서는 디지털 TRS 시스템(TETRA)의 종단간 암호화에 사용되는 스마트카드의 성능 요구조건을 만족하는 상용 암호 알고리즘의 구현 가능성에 대하여 2가지 스마트카드에서 다룬다. 삼성전자의 16비트와 32비트 프로세서를 탑재한 스마트카드에서 각 알고리즘의 동작시간을 측정하였다. 성능 비교에 사용된 알고리즘들은 AES, ARIA, 3DES, SEED이다. 32비트 스마트카드에서는 알고리즘의 동작시간이 1.5ms에서 2.3ms사이에 존재하는 반면, 16비트 스마트카드에서는 2.8ms에서 8.2ms사이의 큰 차이로 존재한다. 단말기와 스마트카드의 통신 속도, 프로세서 계산 능력 등을 고려하여 상용스마트카드의 채택 가능한 칩과 알고리즘의 선정에 본 실험 결과는 참고자료가 될 수 있다.

1. 서론

디지털 TRS라고 불리는 TETRA(TErrestrial Trunked RAdio)는 유럽 ETSI(European Telecommunications Standardization Institute)에 의해 정의되는 공용 주파수 라디오 시스템 표준이다. 세계적으로 공공 안전, 응급 재난에 대처하기 위한 통신망으로 사용되고 있으며 그룹 통신용으로 주로 사용된다.

공공 안전을 다루는 기관에 의해 사용되는 시스템이기 때문에 별도의 보안대책이 요구된다. TETRA에서는 단말기들 사이, 단말기와 인프라 시스템 사이의 음성 및 데이터 보안을 위하여 2가지 수준의 보안 기능을 제공한다. 첫 번째 무선 구간 암호화는 단말기와 기지국의 무선구간에 대한 보안만 제공하고, 두 번째 종단간 암호화는 최종 단말기 사용자들 사이의 전 구간에 대한 암호화를 제공한다. 이 두 가지 암호화는 서로 다른 통신 계층에서 제공되며 서로 독립적으로 적용된다. 일반적으로 무선구간 암호화 기능은 사용 알고리즘과 운용 방식이 표준화되어 있기 때문에 단말기 자체에 내장되어 구현되며, 종단간 암호화 기능은 사용자별로 별도의 알고리즘을 사용하며 그 운용 방법도 상이할 수 있기 때문에 별도의 모듈을 통해 그 기능이 제공된다. 스마트카드를 사용하여 종단간 암호화를 구현하는 방법이 그 중의 하나이다.

스마트카드를 사용하는 방법은 스마트카드 인터페이스를 갖는 단말기에 범용적으로 사용할 수 있다는 점에서 비용 및 개발 기간 측면에서 유리하다고 볼 수 있다.

스마트카드가 암호모듈로서 정상적인 동작을 하기 위해서는 단말기의 요청에 대해 정해진 시간 안에 동작을 마치고 응답을 보낼 수 있어야 한다. 스마트카드의 응답 시간은 스마트카드 자체의 하드웨어적인 성능과 함께 알고리즘이 속도에 의해서 좌우된다.

이 논문에서는 공개되어 있는 여러 암호 알고리즘들을 스마트카드 내에서 구동해 봄으로써 TETRA 종단간 암호화용 스마트카드의 암호 알고리즘으로 사용될 수 있는지의 여부를 확인해 보고, 각 알고리즘의 속도 우위를 비교해 보도록 한다. 두 종의 스마트카드에서 실험을 진행함으로써 서로 상이한 환경의 스마트카드에서의 알고리즘 동작속도 또한 비교해 보도록 한다.

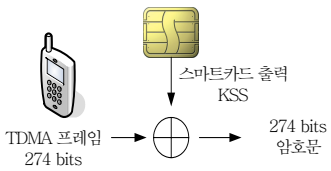
알고리즘들의 속도 측정 결과는 TETRA 시스템뿐만 아니라 스마트카드 내에서 알고리즘을 구동하는 다른 시스템에서도 참고 자료로 활용할 수 있다.

2. 스마트카드 동작 환경

외부와의 인터페이스가 다르고, 내부 프로세서의 종류도 다른 두 종의 스마트카드에서 실험을 진행한다. 첫 번째는 기존 ISO 7816-3의 시리얼 인터페이스를 가지는 스마트카드로 삼성전자의 S3FJ9SK 칩을 사용한다. 두 번째는 ISO 7816-12의 USB 인터페이스를 가지는 스마트카드로 삼성전자의 S3FC9UB 칩을 사용한다.

TETRA 표준에서 정의하는 종단간 암호화용 스마트카드의 인터페이스는 시리얼 인터페이스이다. USB 인터페이스 장치는 아직은 표준화되어 있지 않은 단계로 여기에서는 성능 비교자료로서 사용된다. 두 가지 스마트카드의 하드웨어적인 주요 차이점은 사용 프로세서와 외부인터페이스종류가 다르다는 점이다. 시리얼 인터페이스 스마트카드에서는 223.2 kbps의 속도로 데이터 전송을 하며 데이터 전송속도가 고려해야 할 시간요소가 된다. 이에 반해 USB 인터페이스에서는 최대 12 Mbps 속도의 데이터 전송이 가능하기 때문에 데이터 전송시간이 전체 소요시간에서 차지하는 비중이 작으며 스마트카드 자체 동작과 알고리즘 동작에 소요되는 시간이 전체시간에서 중요한 비중을 차지한다. 시리얼 인터페이스 장치에서는 데이터 전송속도도 고려해야 할 시간요소가 된다.

스마트카드를 사용하는 TETRA의 종단간 암호화 방법은 60ms 간격으로 나타나는 274 비트의 음성 TDMA 프레임에 스마트카드에서 생성하는 키스트림 274비트를 XOR 시켜 출력하는 것이다. XOR 동작은 스마트카드 외부에서 일어나며 스마트카드에서는 (그림 1)과 같이 주어진 시간 안에 키스트림(KSS)만을 생성하면 된다.



(그림 1) 음성 데이터의 종단간 암호화

스마트카드로부터 키스트림을 얻기 위해 소요되는 총 시간은 다음의 항목들을 더함으로써 계산할 수 있다.

□ 단말기에서 스마트카드로 요청 신호을 전달하는 시간
□ 스마트카드 내부 운영 프로그램에서 입출력 루틴을 처리하고, 알고리즘을 제외한 다른 기능을 수행하는 시간
□ 스마트카드 내부 알고리즘 동작 시간
□ 스마트카드에서 만들어진 비트열이 단말기로 전달되는 시간

이 실험에서 입출력에 사용되는 데이터의 비트수는 헤더 정도를 포함하여 500비트 정도이다. 시리얼 인터페이스의 전송속도 232.2 kbps에서 시간을 계산하면 2.15 ms가 된다. USB 인터페이스의 전송속도로 계산하면 42 us정도가 된다.

실험에 사용된 스마트카드는 기본 제어 프로그램으로 상용 스마트카드 OS가 아닌 네이티브 타입의 프로그램을 사용하였다. 즉 스마트카드를 OS 없이 직접 제어하는 방식을 사용하였다. 범용적인 적용을 위해서 제어프로그램 처리 시간으로 30ms 정도를 할애한다면 시리얼 인터페이스에서는 알고리즘 구동에 28.85ms, USB 인터페이스에서는 29ms 정도를 사용할 수 있다. 20ms의 시간을 알고리즘 동작에 할애하면 충분할 것이다.

실험에 사용한 알고리즘들은 3DES, AES, ARIA, SEED이다. AES, ARIA, SEED는 소프트웨어적인 방법으로 구현이 되었으며 3DES는 스마트카드 칩에 하드웨어적으로 구현되어 있는 기능을 활용하였다. 최근의 스마트카드 칩들이 3DES의 기능은 하드웨어적으로 구현해 놓고 있기 때문에 이 기능을 사용하였으며, 소프트웨어적으로 구현된 다른 알고리즘들과의 상대적인 속도비교는 힘들다. 하드웨어적으로 구현된 3DES를 이용하였을 경우에는 속도가 어떠한지에 대한 참고자료가 될 것이다.

알고리즘들의 속도 비교를 위해 키 스케쥴링에 의한 시간지연은 반영하지 않기로 하였다. 키 스케쥴링은 스마트카드를 인식하고 키의 변경이 이루어진 뒤 초기에 이루어지는 사항으로 시간 측면에서 매번 동작시킬 필요는 없다. 즉 비교대상이 되는 알고리즘 동작은 블록 알고리즘이 4번 수행되는 것이다. 128 비트의 블록 알고리즘을 사용하고 생성해야 하는 비트열이 274비트이기 때문에 3번 수행되고, 체크섬을 계산하기 위한 1번의 수행이 포함되어 4번 구동되어야 한다.

실험에 사용된 스마트카드는 S3FJ9SK와 S3FC9UB 칩이 적용된 스마트카드로 개발용 보드에서 실험이 수행되어 관련 데이터들의 수집이 이루어졌다.

3. 스마트카드에서의 알고리즘 성능 계산

스마트카드 내부에서의 알고리즘 동작속도를 구하기 위해서는 스마트카드 외부에서 시간을 측정하여야 한다. 스마트카드 외부에서 파악할 수 있는 시간은 스마트카드에 입력을 주고 출력이 나타날 때까지의 시간이다. 이 시간은 입력 데이터가 스마트카드의 입력 버퍼를 거쳐서 프로세서에서 프로그램에 의해서 처리되고 해당 알고리즘이 동작한 뒤에 출력 버퍼를 통해 스마트카드 외부 핀에 데이터가 나타나기까지의 총 시간이다.

알고리즘만의 동작시간은 알고리즘이 1회 동작한 경우와 2회 동작한 경우의 시간 차이를 구함으로써 얻을 수 있다. 이는 내부 프로그램에서 알고리즘을 수회 동작 가능하도록 하여 측정할 수 있다.

알고리즘이 1회 수행된 스마트카드 동작시간을 T1, 2회 수행된 동작시간을 T2, 알고리즘이 1회 동작하는데 소요되는 시간을 ALGT, 기타 스마트카드의 하드웨어적인 부분과 기본적인 제어프로그램이 동작하는데 소요되는 시간을 OST라고 하면 다음의 식을 만들 수 있다.

$$T1 = OST + ALGT \qquad \text{(수식 1)}$$

$$T2 = OST + ALGT*2 \qquad \text{(수식 2)}$$

$$\rightarrow \Delta T = T2 - T1 = ALGT \qquad \text{(수식 3)}$$

$\rightarrow OST = T1 - ALGT$ (수식 4)

스마트카드 제어 프로그램의 동작시간 (OST)는 알고리즘 동작 회수에 거의 영향을 받지 않는다. T2와 T1의 차이를 알고리즘 동작시간이라고 말할 수 있고, 각 알고리즘에 대해 위의 수식을 적용함으로써 알고리즘 동작 시간을 구할 수 있다.

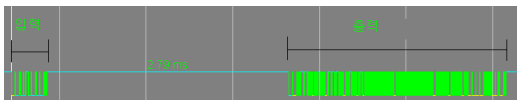
T1과 T2의 측정은 시리얼 인터페이스를 가지는 스마트카드의 경우 스마트카드 프로토콜 분석기(STAR3150)를 통해서, USB 인터페이스를 가지는 스마트카드의 경우에는 USB 프로토콜 분석기(LE 620HS)를 통해서 할 수 있다.

4. 각 알고리즘의 성능 비교

실험에 사용된 스마트카드는 두 가지 종류로 모두 독자 개발된 제어 프로그램을 통하여 전체 동작을 수행한다. 첫 번째 시리얼 인터페이스를 가지는 스마트카드는 삼성전자의 32비트 스마트카드 IC를 사용하며 두 번째 USB 인터페이스를 가지는 스마트카드는 16비트 스마트카드 IC를 사용한다. 첫 번째 카드에 사용된 프로세서는 ARM9이며 두 번째 카드에 사용된 프로세서는 CalmRISC16이다. 전체적인 알고리즘 속도는 두 번째 스마트카드에서 낮게 나온다.

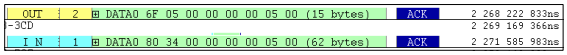
실험에 사용된 알고리즘은 3DES, AES, ARIA, SEED이며 사용된 키는 112비트인 3DES를 제외하고 모두 128비트이다. 오차를 고려하여 5회 이상 반복하여 측정한 값의 평균을 취하였다. 편차는 0.5%정도만을 보이며 전체 동작시간의 계산에 큰 영향을 주지는 않는다. 본 실험에서 3DES의 경우 두 가지 스마트카드에서 카드 내부의 하드웨어 엔진을 사용하였기 때문에 소프트웨어적인 방법에 비해 빠른 속도를 보인다.

시리얼 인터페이스를 가지는 스마트카드에서의 프로토콜 분석기 화면은 (그림 2)와 같다. 입력 비트열과 출력비트열이 표시되며 이 사이의 구간값이 스마트카드의 내부 처리시간이 된다. 여기서는 2.79ms가 이에 해당한다.



(그림 2) 프로토콜 분석기에 의해 읽혀진 신호

USB 인터페이스를 가지는 스마트카드에서의 프로토콜 분석기 화면은 (그림 3)과 같다. 화면상에서 마우스를 위치하여 각 패킷의 시간값을 알 수 있으며 이를 바탕으로 입력과 출력 사이의 시간간격을 구할 수 있다.



(그림 3) USB 프로토콜 분석기로 읽은 신호

(그림 3)에서 OUT이 터미널에서 스마트카드로 보내지는 데이터이며 IN이 스마트카드에서 터미널로 들어오는 데이터이다. OUT의 ACK에서의 시간값과 IN에서의 시작값 차이가 스마트카드 동작시간이다.

알고리즘의 성능비교를 위해서는 입력과 출력 사이의 시간구간에 대한 측정값만을 필요로 한다. 입출력에 소요되는 시간은 모든 알고리즘에서 동일한 값을 보이며, 특히 USB 인터페이스를 가지는 스마트카드에서는 전체 측정시간에서 2% 정도로 미미한 값으로 나타난다.

<표 1>은 시리얼 인터페이스 스마트카드에서의 각 알고리즘이 적용된 경우의 스마트카드 내부 동작시간을 나타내며, <표 2>는 USB 인터페이스 스마트카드에서의 동작시간을 나타낸다.

<표 1> 시리얼 인터페이스 카드에서 각 알고리즘에 대한 스마트카드 전체의 동작시간

적용알고리즘	시간(ms)
3DES	1.29
AES	2.78
ARIA	3.10
SEED	2.29

<표 2> USB 인터페이스 카드에서 각 알고리즘에 대한 스마트카드 전체의 동작시간

적용알고리즘	시간(ms)
3DES	0.74
AES	3.33
ARIA	8.63
SEED	4.55

수식 3을 이용하며 계산한 알고리즘만의 동작시간은 <표 3><표 4>과 같다.

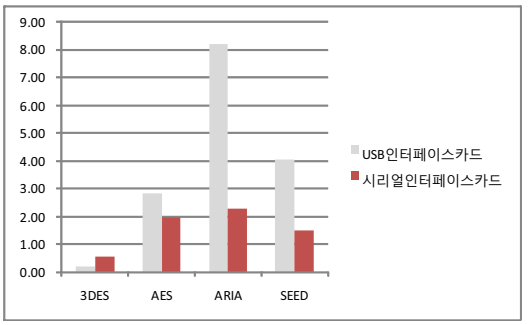
<표 3> 시리얼 인터페이스 카드에서 각 알고리즘의 동작시간

적용알고리즘	시간(ms)
3DES	0.58
AES	2.00
ARIA	2.32
SEED	1.51

<표 4> USB 인터페이스 카드에서 각 알고리즘의 동작시간

적용알고리즘	시간(ms)
3DES	0.22
AES	2.85
ARIA	8.20
SEED	4.07

두 가지 경우를 비교하면 (그림 3)과 같다. 16비트 CalmRISC를 사용하는 시리얼인터페이스 카드에서와 32비트 ARM9을 사용하는 USB인터페이스 카드에서의 알고리즘 속도결과가 약간 상이하다. 3DES는 하드웨어를 사용하기 때문에 가장 작은 동작시간을 갖는 것을 볼 수 있다. AES는 두 가지 스마트카드에서 양호한 동작을 보이며 ARIA의 시간이 두 가지 스마트카드에서 큰 변화값을 보이는 것을 볼 수 있다. 32비트 카드에서는 각 알고리즘의 속도가 1.6ms에서 2.3ms내외로 큰 편차를 보이지 않는 반면에 16비트 카드에서는 2.8ms에서 8.2ms로 큰 차이를 보인다. 알고리즘 고유의 특성으로 동작 프로세서의 처리능력에 따른 차이를 나타낸다고 볼 수 있다.



(그림 4) 각 스마트카드에서 각 알고리즘의 동작시간(ms)

시리얼 인터페이스에서의 제어 프로그램 동작시간은 매 알고리즘에서 1.02 ms 정도로 차이가 거의 없음을 알 수 있다. USB 인터페이스에서도 매 알고리즘마다 0.48ms로 역시 차이가 미미함을 알 수 있다.

두 가지 종류 스마트카드에서 알고리즘 동작시간은 2장에서 제시한 알고리즘 속도 요구조건을 모두 만족한다고 할 수 있다. 두 가지 스마트카드 칩의 경우에서처럼 칩의 종류에 따라 알고리즘의 동작시간은 많은 차이를 보인다고 볼 수 있다. 그러나 실험에 사용된 두 가지 종류 스마트카드는 시간조건을 만족하므로 TETRA 암호화용으로 사용가능하며 각 알고리즘도 역시 사용가능함을 알 수 있다.

5. 결론

두 가지 스마트카드에서 TETRA의 종단간 암호화에 사용가능한 알고리즘들에 대해 살펴보았다. 물론 USB 인터페이스를 가지는 스마트카드의 경우 인터페이스 부분에 대한 표준이 없기 때문에 바로 사용될 수는 없지만 향후 인터페이스에 대한 표준이 만들어진다면 적용될 수 있는 부분이다.

3DES, AES, ARIA, SEED의 총 4가지 상용 알고리즘들을 동작시켜 알고리즘만의 동작시간 계산을 하였다. 32비트 카드에서는 AES, ARIA, SEED 알고리즘 속도가 1.6ms에서 2.3ms내외로 큰 편차를 보이지 않는 반면, 16비트 카드에서는 2.8ms에서 8.2ms로 큰 차이를 보인다. 3DES의 경우 하드웨어를 사용하였으며 비도에서도 낮기 때문에 비교대상에서 제외하였다. 위 알고리즘들 모두 TETRA 암호화를 위한 시간요구조건을 모두 만족한다고 볼 수 있고, 두 가지 스마트카드에서 키 확장성이나 알고리즘 비도, 속도 측면을 고려하면 AES가 좋은 선택조건이라 할 수 있다.

동작속도 측면에서 실험에 사용된 스마트카드와 알고리즘 모두 종단간 암호화용 스마트카드로 사용가능하다고 볼 수 있다. 본 결과는 스마트카드 내부 프로세서, 메모리 및 실행 환경에 의해 좌우될 수 있는 값이며, 스마트카드에서 알고리즘을 구동하는 시스템에서 참고자료로 사용될 수 있다.

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, v1.3.1, Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 1: General Network Design, 2005

[4] ETSI EN 300 392-2, v3.2.0, Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 2: Air Interface, 2005

[5] ETSI EN 300 392-7, v3.0.2, Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security, 2007

[6] ETSI EN 300 109, v1.1.1, Terrestrial Trunked Radio (TETRA); Security; Synchronization mechanism for end-to-end encryption, 2007

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

[8] ISO/IEC 7816-12 Identification cards-Integrated circuit cards - Part 12: Cards with contacts - USB electrical interface and operating procedures

[9] Wolfgang Rankl, Wolfgang Effing, Smart Card Handbook, 3rd edition, 2003