스마트카드의 MESD 공격에 대한 실험적 분석[0]

안만기*, 이훈재**, 하재철***, 김동렬****, 문상재*

*경북대학교 전자전기공학부, **동서대학교 인터넷공학부,

***나사렛대학교 정보과학부, ****한국정보보호진흥원.

Experimental Analysis of MESD Attack on Smartcard.

MahnKi Ahn*, HoonJae Lee**, JaeCheol Ha***, DongRyeol Kim****, SangJae Moon*

*School of Electronic & Electrical Eng., KyungPook National Univ.

**School of Internet Engineering, Dongseo Univ.

***Division of Information Science, Korea Nazarene Univ.

****Korea Information Security Agency

요 약

스마트카드는 내부의 암호 알고리듬이 수행될 때, 비밀키와 관련된 여러 가지 물리적인 정보가 누출될 가능성이 있다. 이러한 물리적 정보 중에서 소비되는 전력을 측정하고 분석하는 차분 전력분석 공격은 매우 강력한 방법이다. 본 논문에서는 시차공격과 단순 전력분석 공격에 대응하는 몽고메리 멱승 알고리듬과 스칼라 상수배 알고리듬이 구현된 스마트카드에서 차분 전력 분석 공격의 방법 중에서 동일한 메시지를 이용하는 MESD 공격을 실험하고 실험과정에서 소모전력의 측정 개수와 표본화율 그리고 잡음의 관계를 분석한다.

I. 서론

스마트카드는 마이크로 프로세서와 메모리를 내장하고 데이터 연산 처리 기능과 저장 기능을 가진다. 그러나 암호 알고리듬을 구현할 때 고려되지 못한 부가 정보의 누출에 의하여 부-채널공격(side-channel attack)의 대상이 될 수 있다. 이러한 공격에는 수행시간 정보를 이용한 시차 공격, 오류 주입을 통한 오류 공격, 소모전력 정보를 이용한 전력분석 공격 그리고 전자기파를 이용하는 전자기 누출 공격 등이 있다[1-4]. 특히, 전력분석 공격은 스마트카드에 물리적 변환을 가하지 않고 직접 소모전력 신호의 특성을 파악하여 비밀키에 대한 정보를 알아내는 SPA와 통계적 방법으로 잡음성분을 제거한 후 소모전력평균에 대한 차분으로부터 비밀키를 알아내는 DPA로 분류된다.

Kocher [3]는 DES에 차분전력 공격을 처음으로 적용했고, Messerges [5]는 이진 멱승 알고리듬에 대하여 single exponent multiple data (SEMD) 공격, multiple exponent single data (MESD) 공격, 그리고 zero exponent multiple data (ZEMD) 공격 등을 적용하였다. MESD 공격은 두 개의 스마트카드(공격대상 카드와 키 값을 변경할 수 있는 비교용 카드)를 이용하여 공격하는 기술로서, 동일한 메시지를 적용하여 비밀키를 모르는 공격대상카드의 평균전력 파형과 비밀키 변경이 가능한 비교용 카드의 평균전력 파형을 차분함으로써 키 비트를 순차적으로 알아내는 방법이다.

본 논문에서는 몽고메리 멱승(Montgomery exponentiation) 알고리듬과 덧셈-뺄셈(addition-subtraction) 알고리듬을 사용하는 스마트카드에서 MESD 공격을 실험하여 표본화율과 수집해야 할 소모전력의 개수 그리고 잡음의 관계를 분석하고자 한다.

II. 소모전력 모델과 잡음 특성

1. 소모전력 모델

[0] 본 연구는 한국정보보호진흥원 과제 2002-S-073의 지원으로 수행하였습니다.

CMOS 소자의 경우 일반적으로 상태를 유지하고 있을 때보다 상태천이 시에 전력소모가 많이 발생하는 특징을 갖는다. 소모전력에서 유출되는 정보는 유동 전류(dynamic current)와 방전 전류(discharge current)에 의한 상태천이 수와 비트 '1'의 개수에 따른 해밍웨이트로 구분된다 [6].

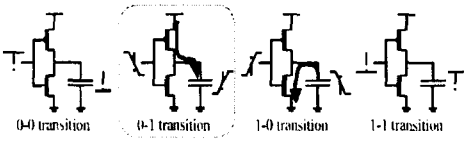

그림 1 : CMOS 인버터의 상태천이.

2. 소모전력 파형과 잡음

스마트카드에서 측정되는 소모전력은 크게 4가지의 잡음성분과 연관성이 있다. 즉, 스마트카드에 결합된 외부 장치(PC, card reader)로 인한 외부잡음(external noise), 스마트카드 conductor 내부에 존재하는 전하의 랜덤한 운동으로 인한 내부잡음(intrinsic noise), 소모전력 파형을 표본화할 때 사용되는 A/D converter에 의한 양자잡음(quantization noise), 그리고 연산되는 데이터의 변화에 의한 알고리듬 잡음(algorithmic noise)으로부터 비롯된다. 내부잡음과 양자잡음은 크기가

표 1 : 표기와 의미.

표기	의 미
K	수집한 소모전력 파형의 개수
$S_i[j]$	소모전력 파형, $1 \le i \le K$
j^*	공격 비트 이후의 모든 비트 위치
ε	피크의 크기
σ^2	소모전력의 분산
α	$j \neq j^*$일 때, 알고리듬 잡음의 정도

다른 잡음에 비해 아주 작아서 무시할 수 있다.

스마트카드의 소모전력 파형에 포함된 잡음은 외부잡음과 알고리듬 잡음으로 볼 수 있으며, 잡음을 고려한 전체 소모전력 파형을 계산할 수 있다. 이때 공격 대상의 스마트카드는 8비트 마이크로프로세서를 사용하며 공격자는 MESD 공격을 실시한다. 외부잡음을 랜덤한 잡음으로 간주 할 때 차분 전력 파형에서 평균과 분산을 영역별로 구분하면 다음과 같다 [7].

가) 동일 영역 : 외부 및 기타 잡음과 비슷한 알고리듬 잡음

$$E[S_i[j] | (j \neq j^*)] = 0$$

$$Var[S_i[j] | (j \neq j^*)] = \frac{4\sigma^2 + \alpha \cdot \varepsilon^2/8}{K}$$

나) 피크 영역 : 외부 및 기타 잡음과 다른 알고리듬 잡음

$$E[S_i[j] | (j = j^*)] = \varepsilon$$

$$Var[S_i[j] | (j = j^*)] = \frac{4\sigma^2}{K}$$

신호 대 잡음비(signal-to-noise ratio:SNR)는 MESD 공격에서 다음과 같은 값을 가진다.

$$SNR = \frac{\sqrt{K} \cdot \varepsilon}{\sqrt{8\sigma^2 + \alpha \cdot \varepsilon^2/8}}$$

이는 수집하는 소모전력의 개수 K가 많을수록 SNR이 향상됨을 알 수 있으며, ε이 일정하다고 가정할 때 σ^2와 α에 의해 정해진다.

Ⅲ.공개키 암호 알고리듬의 차분 전력분석 공격 실험

차분 전력분석 공격을 실시할 때 공격자는 암호 알고리듬의 종류와 동작 시점들을 알고 있으며, 또한 비밀키의 비트 수 L을 알고 있다고 가정한다. 실험 과정은 논문 [8]을 참고한다.

1. RSA에서 SPA에 대응하는 몽고메리 멱승 알고리듬의 실험

RSA [9]는 모듈라 멱승(modular exponentiation) 연산 시 제곱과 곱셈을 실시한다. 1024비트 이상의 큰 정수를 빠르게 연산하기 위해 이진 연산 방법보다는 몽고메리 멱승 알고리듬을 사용한다. LR 방법을 사용하는 몽고메리 멱승 알고리듬의 최상위 비트는 항상 '1'이라고 가정한다. 기존의 몽고메리 멱승 알고리듬은 비밀키의 비트가 '1'일 때 조건문이 수행되어 시차공격과 단순 전력분석 공격에는 대응할 수 없다 [10]. 따라서 Coron이 제안한 바와 같이 비밀키의 비트 값에

```
INPUT : m, d = (d_{L-1},...,d_0)_2, n, R=2^L
OUTPUT : B[0] = m^d mod n
B[0] ← R mod n
A ← m·R mod n
for i from L-1 downto 0 do
    B[0] ← REDC(B[0], B[0])
    B[1] ← REDC(A, B[0])
    B[0] ← B[d_i]
endfor
B[0] ← REDC(B[0], 1)
return B[0]
```

그림 2 : SPA에 대응하는 몽고메리 멱승 알고리듬.

관계없이 항상 "REDC()"연산을 실시하는 방법[11]을 적용하여 그림 2와 같이 실계한다. 이러한 대응 방안도 비트 d_i의 값에 따라 REDC(B[0],B[0])에 입력되는 데이터 값이 같지 않으면 연산 과정에서 상이한 결과가 나타난다. 추측키의 두 번째 비트가 다르면 세 번째 비트에서 연산되는 데이터가 달라지게 된다. 최하위 비트는 다음 비트의 소모전력을 얻을 수 없으므로 전탐색 방법을 사용한다.

비밀키 $d_i=1010111_{(2)}$일 때 입력 메시지 m=5, 소모전력의 측정 개수 K=100으로 설정하여 실험하면 그림 3과 같은 부분적인 실험 결과를 얻는다. 공격자가 두 번째 비트를 '1'로 추측할 때 세 번째 비트 위치부터 피크가 형성됨을 보여주고 있다.

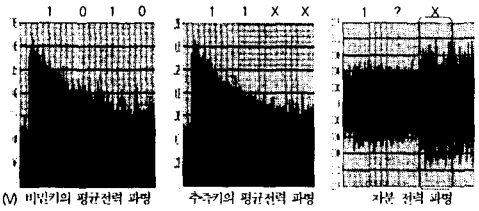

그림 3 : SPA에 대응하는 몽고메리 알고리듬의 차분 전력 파형.

2. ECC에서 SPA에 대응하는 덧셈-뺄셈 알고리듬의 실험

INPUT : P, $d_i=(d_{L-1},...,d_0)_2$
OUTPUT : $Q[0] = dP$

$Q[0] \leftarrow P$
for i from L-2 downto 0 do
  $Q[0] \leftarrow 2Q[0]$
  $Q[1] \leftarrow Q[0]+P$
  $Q[-1] \leftarrow Q[0]-P$
  $Q[0] \leftarrow Q[d_i]$
endfor
return $Q[0]$

그림 4 : SPA에 대응하는 덧셈-뺄셈 알고리듬.

타원곡선 암호시스템(ECC)은 1985년 Miller [12]와 Koblitz [13]에 의해 독립적으로 제안된 방식으로 유한체 상에서 정의된 타원곡선 식을 만족하는 점들의 집합에서 적당한 연산을 적용하여 그룹을

정의하고 이 그룹에서 암호시스템을 구성한다. 본 논문에서는 유한체 $GF(p)$에서 Weierstrass 방정식 $y^2=x^3+ax+b$를 만족시키는 Affine 좌표계로 표현된 타원곡선 상에 한 점 P와 다른 한 점 Q가 주어질 때 연산하는 과정을 공격한다.

non-adjacent form(NAF)를 사용하는 덧셈-뺄셈 알고리듬은 두 번째 비트가 반드시 '0'이다. 하지만 세 번째 비트에서는 '0'과 '1' 그리고 '-1'의 경우를 모두 고려해야 한다. 반면 비밀키 비트가 '1'이나 '-1'임을 알면 반드시 다음 비트는 '0'임을 알 수 있다. 그림 4는 SPA에 대응하는 덧셈-뺄셈 알고리듬으로 부가적인 연산을 실시한다.

그림 5는 K=300으로 설정할 때 두 번의 추측을 실시한 결과 파형이다. 비밀키 $d_i=1001001101_{(2)}$에서 "001"을 대상으로 두 번째 비트를 추측한 일부 파형이다. 추측이 틀린 경우 세 번째 비트 위치에서부터 피크를 볼 수 있다.

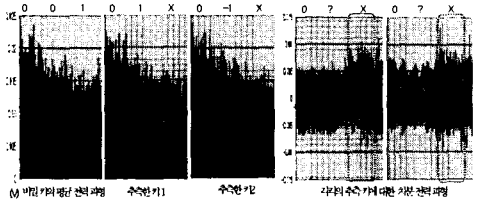

그림 5 : SPA에 대응하는 덧셈-뺄셈 알고리듬의 차분 전력 파형.

IV. 실험 파라메터 분석

차분 전력분석 공격 시, 데이터 수집과정에서 최소의 소모전력의 측정 개수를 가지고 데이터 분석과정에서 비밀키를 알아내는 것이 소요시간을 줄일 수 있다. 따라서 SPA에 대응하는 몽고메리 먹승 알고리듬과 덧셈-뺄셈 알고리듬에서 소모전력의 측정 개수와 클럭당 표본화율 그리고 잡음의 상호 연관성을 분석한다. 스마트카드의 시스템 클럭은 3.58MHZ로 한 클럭당 0.28us이다.

1. 표본화율에 따른 소모전력의 측정 개수

표 2는 몽고메리 알고리듬과 덧셈-뺄셈 알고리듬에서 표본화율을 변경할 때, 공격이 성공한 경우에 최소의 소모전력의 측정 개수를 보여준다. 이때 공격의 성공 여부는 차분 파형에서 공격 대상의 비트 위치를 포함한 이전의 동일 영역과 이후의 피크영역이 문턱전압 V_{th}=3mV 이상의 전압차를 가지며 두 영역이 확실히 구분 가능한 경우를 말한다.

표본화율이 최초 0.035일 때 비밀키의 비트당 샘플의 개수를 두 배 정도 증가시키면서 측정하였다. 표본화율이 작아도 소모전력의 측정 개수가 많으면 공격이 가능하며, 표본화율이 증가하면 소모전력의 측정 개수가 적어도 동일한 결과를 얻을 수 있다. 그러나 초기의 소모전력의 측정 개수가 200에서 50으로 감소할 때는 표본화율이 두 배씩 증가되었으나, 계속 증가시켜도 소모전력의 측정 개수가 비례적으로 감소하지 않는 것을 볼 수 있다. 이는 알고리듬 잡음보다는 외부잡음의

영향이 크기 때문이다. 공격이 성공하기 위해서는 표본화율의 증가보다 최소한 50개와 100개 이상의 소모전력의 측정 개수가 요구됨을 보여주고 있다. 따라서 실험의 소요시간과 소모전력 데이터의 처리시간을 고려하여 표본화율이 0.14일 때 각각의 소모전력의 측정 개수가 가장 적합하다.

표 2 : MESD 공격이 성공 시 표본화율에 대한 최소의 소모전력 측정 개수.

표본화율		소모전력 측정 개수	
(Sample /clk)	(Sample /sec)	몽고메리 멱승	스칼라 곱셈
0.035	1.25×10^4	200	300
0.07	2.5×10^5	100	200
0.14	5.0×10^5	50	100
0.28	1.0×10^6	50	100
0.7	2.5×10^6	50	100

그림 6은 몽고메리 멱승 알고리듬에서 소모전력의 개수와 클럭 당 샘플링 수를 변경할 때 공격이 성공한 경우의 차분 전력 파형이다. 외부잡음의 영향으로 소모전력의 개수가 적을수록 차분 시에 연산과정이 같은 동일 영역에서도 차분 전압 크기가 증가하는 것을 볼 수 있다. 따라서 표본화율의 증가로 소모전력의 측정 개수를 줄이는 것은 한계가 있다.

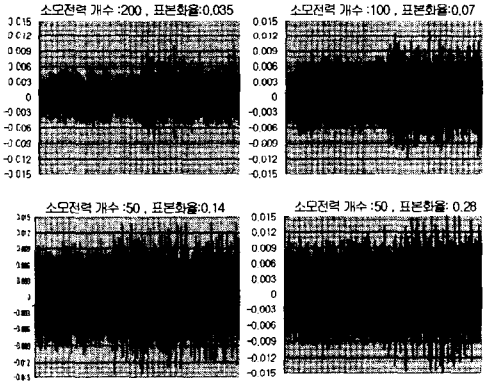

그림 6 : MESD 공격이 성공 시 표본화율과 소모전력 개수.

2. 잡음에 따른 소모전력의 측정개수

그림 7은 표본화율이 0.14로 고정되었을 때 몽고메리 알고리듬의 소모전력의 개수에 따른 차분 파형이다. 소모전력 개수가 많을수록 더욱 선명한 차분 파형을 볼 수 있다. 즉, 소모전력의 개수가 25일 때 외부잡음과 알고리듬 잡음의 영향이 증가하여 연산 과정이 같은 동일 영역과 피크 영역을 구분할 수 없다. 그러나 소모전력의 개수가 50으로 공격이 성공한 경우, 외부잡음과 알고리듬 잡음도 감소하지만 서로 다른 알고리듬 잡음에

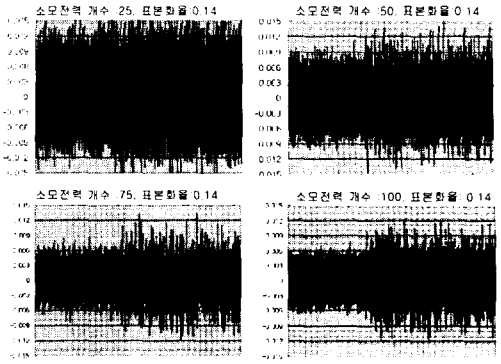

그림 7 : 표본화율의 고정 시 소모전력 개수와 잡음의 영향.

의한 뚜렷한 차분 파형을 볼 수 있다. 따라서 소모전력의 개수가 증가할수록 크기의 변화가 일정한 외부잡음은 감소하며 크기의 변화가 서로 다른 알고리듬 잡음은 더욱 정밀하게 분포되어 2장 2절에서 언급한 신호 대 잡음비(SNR)가 증가하는 것을 볼 수 있다. 그러므로 알고리듬 잡음은 소모전력 파형에서 전압의 변화를 말해준다.

3. 표본화율과 잡음

표본화율이 증가하면 알고리듬 잡음이 정확하게 샘플링되지만 원하지 않는 외부 잡음도 더욱 정확하게 샘플링된다. 따라서 공격자는 실험과정에서 정밀한 장비와 세심한 실험을 통하여 표본화율과 소모전력 측정 개수의 최적화된 관련성을 확보하면 소모전력 측정 개수에 비중을 두고 공격을 실시하는 것이 소요시간을 줄일 수 있다.

V. 결 론

본 논문에서는 부-채널 공격 중에서 가장 강력한 전력분석 공격을 MESD 공격 방법으로 실험하였다. 시차공격과 SPA 공격에 대응하는 방법을 적용한 스마트카드에서 MESD 공격을 적용하여 표본화율과 잡음 그리고 소모전력의 측정개수의 관계를 분석하였다. 이는 차분 전력분석 공격에서 잡음과 소모전력의 측정개수를 분석하여 공격의 소요 시간을 줄일 수 있다. 이러한 공격을 방어하기 위하여 SPA/DPA 공격과 기타 다른 부-채널 공격에도 대응할 수 있는 알고리듬을 개발하고 사용하는 것이 중요하다.

참고문헌

[1] P. Kocher, "Timing Attacks on Implemen- tations of Diffie-Hellman, RSA, DSS, and Other Systems," in *CRYPTO'96*, pp. 104-113, 1996.

[2] E. Biham and A. Shamir, "Differential Fault Analysis of Secret Key Cryptosystems" , in *CRYPTO'97*, pp. 513-525, 1997.

[3] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in *CRYPTO'99*, pp. 388-397, 1999.

[4] Josyula R. Rao and Pankaj Rohatgi, "EMpowering Side-Channel Attacks", Available at http://eprint.iacr.org/complete/

[5] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Power Analysis Attacks on Moular Exponentiation in Smart cards", in *CHES'99*, pp. 144-157, 1999.

[6] K. Tiri, M. Akmal and I. Verbauwhede, "A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart card", in The preliminary conference program, *ESSCIRC 2002*, available on Web site http://cle.unipv.it/esscirc2002/

[7] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "investigations of Power Analysis Attacks on Smartcards", in *USENIX*, 1999.

[8] 안만기, 곽동진, 이훈재, 하재철, 문상재, "먹승 알고리듬의 데이터 변화를 이용한 스마트 카드의 차분 전력분석 공격", *통신정보합동학술대회*, Vol 12, No. 1, pp. IV-A.1.1~4, April, 2002

[9] R. L. Rivest, A. Shamir, and L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Communica- tions of the *ACM*, 21, pp. 120-126, 1978.

[10] Gael Hachez and J.J. Quisquater " Montgomery Exponentiation with no Final Subtractions: Improved Results", in *CHES'00*, pp. 293-301, 2000.

[11] J. S. Coron, "Resistance Against Differential Power Analysis for Elliptic Curve Crypto- systems", in *CHES'99*, pp. 292-302, 1999.

[12] N. Koblitz, "Elliptic curve crypto-systems," Mathematics of Computation, vol. 48, pp. 203-209, 1987.

[13] V. Miller, "Uses of elliptic curves in crypto in cryptography," in *CRYPTO'85*, pp. 417-426, 1985.