논문 02-27-6A-4 한국통신학회논문지 '02-6 Vol.27 No.6A

스마트카드의 전력분석공격 실험 방법에 관한 연구

정회원 이 훈 재*, 장 익 훈**, 최 희 봉***, 박 일 환***

A Study on the Experimental Methods of the Power Analysis Attack in a Smartcard

HoonJae Lee*, Ick-Hoon Jang**, Hee-Bong Choi***, Il-Hwan Park*** *Regular Members*

요 약

최근에 시간측정, 전력소모측정, 전자기파 방사측정 및 하드웨어적 강제에러주입 등의 부가정보를 사용한 공격 기법들이 연구되어지고 있다. 또한 부채널 정보를 줄이거나 측면공격으로부터 방어하는 기술들이 연구되고 있다. 본 논문에서는 차분전력분석 기법으로 DES 암호 알고리즘 공격에 대하여 실험·분석하였다. 그리고 DES 형태의 DPA 공격에 강한 소프트웨어 구현시의 방어대책을 제안하였다.

ABSTRACT

Attacks have been proposed that use side information as timing measurements, power consumption, electromagnetic emissions and faulty hardware. Elimination side-channel information or prevention it from being used to attack a secure system is an active ares of research. In this paper, differential power analysis techniques to attack the DES are experimented and analyzed. And we propose the prevention of DPA attack by software implementation technique.

Ⅰ. 서 론

스마트카드는 안전한 개인 정보저장 수단으로 잘 알려져 있지만 해킹될 경우 카드에 저장된 개인신용정보나 암호해독 키까지도 추출이 가능하여 IC 칩 기반의 전자화폐에 대한 위·변조와 개인정보의 악용이 가능해질 수 있다. 부채널(side-channel)에 의한 스마트 카드 공격 기술을 일반적으로 부채널 공격(side-channel attack)[1-2]이라고 부르며, 이러한 공격방법으로는 시간공격(TA, timing attack), 결함주입 공격(FA, fault-insertion attack), 전자기 누출 공격(electromagnetic emission attack), 그리고 전력분석공격(PA, power analysis attack)으로 나눌 수 있다. 전력분석공격은 단순 전력분석[3-4](SPA, simple power analysis), 차분 전력분석[3-9](DPA, differential power analysis), 추론 전력분석[10](IPA, inferential power analysis), 그리고 고차 차분 전력분석[11](HO-DPA, high-order differential power analysis) 공격으로 나누어진다. 전력 분석 공격은 카드 내부에 내장된 암호 알고리즘과 암호용 비밀키가 작동되는 순간에 IC 칩의 순간적인 전압 (전력)변화를 관측하여 각종 정보의 이진 코드를 읽어낸 후 통계적인 방법으로 중요 정보 분석은 물론 위·변조까지 가능한 암호해독 기술이다. DPA 기술은 전압변화를 관측할 수 있는 몇 가지 장치만 구비하면 비밀 키의 추정이 가능하기 때문에 전용의 해독기계 또는 슈퍼 컴퓨터를 동원한 전수공격 (brute-force attack) 보다 훨씬 효과적인 것으로 분석되고 있다. 이러한 DPA 기술이 개발되면서 전자상거래(EC) 분야의 지불수단 안전성 문제와 함께 국내외 스마트 카드 제조사와 IC 칩 기반 카드업계의 제품생산 계획 자체도 위협 받고있는 실정이다.

최근에는 부채널 공격에 대하여 자체 누설을 근본적으로 봉쇄하거나 또는 공격을 방어하는 기술이

* 동서대학교 인터넷공학부(hjlee@dongseo.ac.kr), ** 경운대학교 컴퓨터전자정보공학부, *** 국가보안기술연구소
논문번호 : 020223-0509, 접수일자 : 2002년 5월 9일

새로운 연구분야로 대두되고 있다. 특히 암호 코프로세서(co-processor)가 장착된 스마트카드 시스템에서 부채널 공격의 연구가 활발하다.

본 논문에서는 Kocher 형태의 스마트카드 DPA 공격[3-4]에 대한 실험분석 모델을 설정한 후 이를 검증하고자 축소형 모델로 실험한다. 실험 분석을 위하여 선정된 장치에는 DES 암호 알고리즘을 어셈블러로 구현한 후 8-비트 마이크로 프로세서형 스마트카드에 탑재하여 암호 알고리즘 실행 시에 발생되는 차분전력신호를 분석한다. 실험 결과 진짜 키를 포함하는 유사 키 군을 추정하고 있음을 확인하고, 실험 모델을 좀 더 확장할 경우에는 정확한 키를 해독할 가능성이 있음을 확인한다. 그리고 DPA 공격을 방어할 수 있는 소프트웨어적인 구현 방안을 제안한다.

Ⅱ. 전력분석공격

스마트카드는 내부에 전체 시스템의 안전성과 카드의 위조를 방어코자 사용자 비밀 키와 공인 인증서 등이 저장될 수 있고, 외부 전원으로부터 공급받는 전력에 의하여 구동된다. 이 때 스마트카드가 작동되면 비밀 데이터에 대한 연산이 이루어지므로 비밀 정보에 대한 누출 가능성이 매우 높다. 이러한 유형의 스마트카드 부채널 누출정보에 대한 부채널 공격 중에서 SPA와 DPA 공격에 대하여 알아본다.

1. SPA

SPA[3-4]는 스마트카드에서 연산되는 암호 프로세서의 전력소비를 관찰하여 카드 내부에 저장되어 있는 비밀 키를 직접 공격하는 방법이다. 프로세서의 명령에 따라 각기 다른 전력을 갖는다는 사실을 스마트카드 외부에서 관측할 수 있으며, 이로부터 키 또는 순간 작동 중인 명령에 대한 정보(hamming weight, 이진 수 분포 등)를 추론하는 공격방법이다. SPA 공격에 대한 방어 기술로는 조건 점프 명령(conditional branching operation)을 배제시키는 방법과 하드웨어적인 구현(hard-wired hardware implementation) 기술을 적용하는 방법 등[3-5]이 알려져 있다. 여기에서 하드웨어적인 방법으로는 클럭 자체에 대한 랜덤화 기법이 있다.

2. DPA

DPA[3-9]는 SPA 보다 방어하기 어려운 공격방법이며, SPA가 소비 전력을 관찰하는 것에 반하여 DPA는 비밀키와 정확히 상관관계 (correlation)를 가지는 정보를 추출하기 위해 통계적인 분석(statistical analysis)과 에러정정 (error correction) 기술을 사용한다. 즉, 스마트 카드가 암호연산 실행 시에 소비되는 전력을 표본화하여 그 데이터를 수집한 다음 표본화된 데이터로부터 잡음신호를 감소시키고 차분 (differential) 신호의 명확성을 높이기 위해서 디지털 신호 해석 및 통계기법을 적용하여 분석하는 공격이다.

DPA 공격방법은 전력소비 데이터를 수집한 후 이를 분석하기 위하여 통계적인 분석방법을 사용하여야 한다. 먼저 정확한 비밀키가 들어갔을 때 그 비밀키와의 반응을 알 수 있는 분류함수(partitioning function) 또는 선택함수(selection function) D(key, data)를 정하여야 하는데, 이 함수는 특정 비트나 바이트의 해밍 중을 조사하여 데이터 수집단계에서 수집한 데이터를 분류하는 함수이다. 이러한 분류함수로 데이터를 적절히 분류한 후 가능한 비밀키의 집합에서 키를 추측하여 통계적인 방법으로 비밀키를 찾아낼 수 있으며, 다음은 Kocher 형태의 DPA[3-4] 공격 단계를 나타내었다.

1) 전체 구하려는 스마트 카드의 n 비트 비밀키 K를 $(k_{n-1}, k_{n-2},\cdots, k_1, k_0)$라 정의하고, 최상위 혹은 최하위 비트의 순서로 순차적으로 키의 일부가 입력되어 연산된다고 가정한다.

2) 먼저 키의 일부인 k_i 또는 $\{k_i,\cdots,k_j\}$를 미리 가능한 키 영역에서 추측한다.

3) 추측한 키와 전력신호 데이터를 구할 때 쓴 평문을 입력으로 연산을 수행한 후 분류함수를 이용하여 전력신호 데이터를 분류한다.

$S_0=\{S_i[j] \mid D(\text{key, data}) = 0 \text{ or low hamming weight}\}$

$S_1=\{S_i[j] \mid D(\text{key, data}) = 1 \text{ or high hamming weight}\}$

4) 양분한 데이터를 각각 평균하여 차분 신호를 구한다.

$$\Delta_D[j]=\frac{1}{|S_0|}\sum_{S_i[j]\in S_0}S_i[j]-\frac{1}{|S_1|}\sum_{S_i[j]\in S_1}S_i[j] \quad (1)$$

5) 평문과 전력소비신호의 샘플 수 t 값이 크고, 추측한 키가 옳지 않다면 $\Delta_D[j]$ 신호가 거의 0에 수렴한다. 키가 반응하는 지점에서 non-zero이고 추

측한 키가 맞다면

$$\lim_{t\to\infty}\Delta_D[j]\approx \text{nonzero} \quad \text{if guess is correct} \qquad (2)$$
$$\lim_{t\to\infty}\Delta_D[j]\approx 0 \quad \text{if guess is incorrect}$$

6) 추측이 옳지 않다면 다시 2)로 돌아간다.

7) 추측이 옳다면 그 키가 스마트 카드의 실제 내부 키의 일부가 된다.

상기 과정을 계속 반복하여 내부에 내장된 전체 키 값 (비밀키)을 그림 1과 같은 방법으로 찾을 수 있다. 각각 하나의 Δ_D에 대하여 가능한 키를 모두 입력한 다음 그 중에 하나인 실제 키를 찾는 방법이다.

DPA 공격에서 중요한 기술은 분류함수인 D(key, data)를 어떻게 설정하는가 하는 점이며, 구현된 암호 알고리즘에 따라 설정 방법이 큰 차이가 있을 수 있다.

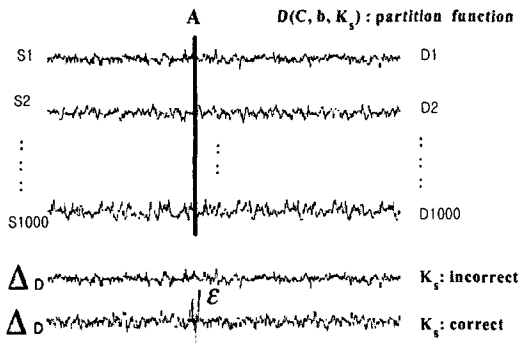


그림 1. Kocher 형태의 DPA 분석 파형

Ⅲ. DPA 실험 및 분석

1. 실험 준비 사항

전력분석 파형 측정을 위한 실험 준비 사항 및 실험 환경(그림 2 참조)은 다음과 같다.

1) 디지털 오실로스코프 1대(1 GHz 이상 샘플링 기능 보유; PC 상으로 디지털 데이터의 저장이 가능하여야 한다.)

2) 스마트카드 리더기 및 카드 각 1대(카드 리더 확장기판 포함)

3) 가변 저항 10~150 ohm 1개(일반적인 관측을 위하여 50 ohm 정도의 저항이 필요로 하며, 측정 파형의 시각적 인지도를 조정하기 위하여 가변저항을 사용하였다. 일반적으로 저항 값이 작을 때 전력 측정 파형이 시각적으로 더욱 잘 구분될 수 있다.)

4) 퍼스널 컴퓨터 1대(데이터 저장 및 분석용, Windows95 이상)

5) 스마트카드용 에뮬레이터 1대(선택사항)

6) 스마트카드용 어셈블러(선택사항)

7) 스마트카드 구동용 PC 프로그램(선택사항)

8) 스마트카드용 마이크로프로세서 데이터 북(선택사항)

9) 스마트카드 탑재용 어셈블리 프로그램 구현

10) 전력분석용 PC 시뮬레이션 프로그램(분류데이터 생성용 프로그램; DPA 분석용 프로그램) 구현 등

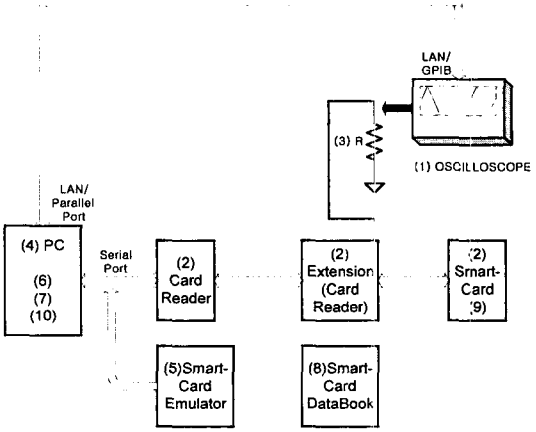


그림 2. 전력분석 실험환경 구성도

2. DPA 분석 모델 설정

DPA 분석을 위한 전력측정 구성은 그림 3과 같다. SPA 공격은 DES 암호에 대한 공격에 부적합하며, IPA 공격은 소스코드가 공개되지 않은 경우에 적용하는 공격법으로 일반적으로 DPA 공격보다 약한 방법이기 때문에 본 실험에서는 DPA 공격을 실험 모델로 선정하게 되었다.

DPA 분석을 위하여 다음과 같은 전제조건이 필요하다.

1) 본 실험에서 공격 대상이 되는 암호 알고리즘은 DES로 설정한다.

2) 카드 리더기와 8-비트 CPU의 스마트카드가 구비되어야 한다.

3) 스마트카드 CPU용 어셈블러로 선정된 암호 알고리즘이 구현되어야 한다.

4) DPA 분석 시 입력 데이터는 다음과 같다.

$(N=1000, M=100000)$

· 평문데이터: $P[0], P[1], P[2], \cdots, P[N-1]$

· 암호문데이터: $C[0], C[1], C[2], \cdots, C[N-1]$

· 전력 데이터:

$S[0][0], S[0][1], S[0][2], \cdots, S[N-1][M-1]$

· 분류함수데이터:

$D_0[64][8], D_1[64][8], D_2[64][8], \cdots D_N[64][8]$

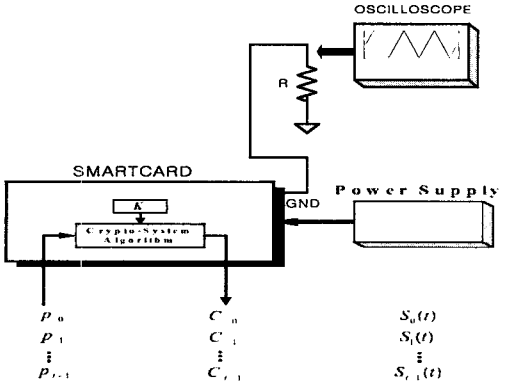


그림 3. 전력파형 측정 구성도

DPA 분석 모델은 다음과 같이 설정하였으며, 실제 실험에 있어서는 1/10 축소 모델(N=100, M=10,000)을 실험 분석한다.

1) 암호문에 사용될 키 K가 설정되어 있다고 가정하고, $K=K[0], K[1], \cdots K[k-1]$라고 표현한다. 본 실험에서는 k=56-비트로 키 데이터는 $K=K[0], K[1], \cdots K[55]$와 같이 설정한다.

2) 그림에서처럼 N개의 평문 데이터 $P_0, P_1, P_2, \cdots, P_{N-1}$와 이에 대응하는 암호문 데이터 $C_0, C_1, C_2, \cdots, C_{N-1}$를 확보한다. 이렇게 설정된 데이터를 각각 평문 배열 $P[0], P[1], P[2], \cdots, P[N-1]$ 및 암호문 배열 $C[0], C[1], C[2], \cdots, C[N-1]$라 둔다. 본 실험에서는 100쌍의 평문데이터와 암호문 데이터를 확보한다.

· 평문 데이터 : $P[0], P[1], P[2], \cdots, P[N-1]$

· 암호문 데이터: $C[0], C[1], C[2], \cdots, C[N-1]$

3) t=0,1,2,...,N-1에 대하여 전력 파형 데이터 $S_0, S_1, S_2, \cdots, S_{N-1}$을 측정한다. 여기에서 샘플 데이터는 N=100개의 시점에 대하여 한번에 각각 M=10,000 측정점(point)이상을 수집한다. 이렇게 수집된 전력 데이터 배열을 $S[0][0], S[0][1], S[0][2], \cdots, S[N-1][M-1]$ 라 둔다.(실제로 이 데이터는 100개의 데이터 파일로 구성되어 있을 수 있다.)

· 전력 데이터 :

$S[0][0], S[0][1], S[0][2], \cdots, S[N-1][M-1]$

4) 키의 일부인 $K[i]$ 또는 $\{K[i], \cdots, K[j]\}$를 추정한다. 본 실험에서는 DES에서 적정한 분류 함수를 선택하여 제1 라운드에서 첫 번째 S-box1에 입력되는 6-비트 입력 키 $K_6[1]$를 추정한다. (6-비트의 추정에는 최대한 2^6의 경우의 수가 생긴다. 아래는 6-비트의 키 그룹이다.)

10	51	34	60	49	17	33	57	2	9	19	42
3	35	26	25	44	58	59	1	36	27	18	41
22	28	39	54	37	4	47	30	5	53	23	29
61	21	38	63	15	20	45	14	13	62	55	31

5) 암호문과 S-box 출력 값 및 키에 따라 다음과 같이 사전에 계산된 분류함수를 입력한다.

$$D[i] = D(C_1[i], C_6[i], K_6[1])$$
$$= C_1[i] \oplus SBOX1(C_6[i] \oplus K_6[1])$$

여기에서, $C_1[i]$ = S-box #1의 첫 번째 #1 비트와 XOR되는 암호문 $C[i]$의 1-비트, $C_6[i]$ = 보조키 $K[1]$과 XOR되는 암호문 $C[i]$의 6-비트, $K_6[1]$ = S-box #1으로 입력되는 제1 라운드 보조키 6-비트, SBOX1(x)= S-box #1의 주소 x로부터 얻어지는 결과 비트 #1을 되돌리는 함수이다.

6) N=100 종류의 전력 소모 데이터로부터 S-box #1이 작용하는 시점에서의 데이터 값을 예측한 후 상기 분류 함수에 따라 다음과 같이 전력 신호를 두 개의 그룹으로 나눈다.

$$S_0 = \{S[i][j] \mid D(\cdot,\cdot,\cdot) = 0\}$$

$$S_1 = \{S[i][j] \mid D(\cdot,\cdot,\cdot) = 1\}$$

7) 각 세트에 대하여 평균 전력 신호를 계산한다.

$$A_0[j] = \frac{1}{|S_0|}\sum_{i,j} S[i][j] \qquad if \qquad S[i][j] \in S_0$$

$$A_1[j] = \frac{1}{|S_1|}\sum_{i,j} S[i][j] \qquad if \qquad S[i][j] \in S_1$$

여기에서, $|S_0| + |S_1| = N$이 된다.

8) 두 개의 평균값을 서로 뺀 이산 시간 DPA 바이어스 신호 $T[j]$는 다음과 같이 얻어진다.

$$T[j] = A_0[j] - A_1[j]$$

9) 다음과 같이 기대값으로 진짜 키(correct key) 인지 여부를 결정한다.

$$T[j] = E[Sij \mid (D(\cdot,\cdot,\cdot) = 0)] - E[Sij \mid (D(\cdot,\cdot,\cdot) = 1)]$$
$$= E[Sij] - E[Sij] = A_0[j] - A_1[j] \approx 0 \quad \forall j$$

(in case of the incorrect key)

$$T[j] = E[S_{ij} \mid D(\cdot,\cdot,\cdot) = 0] - E[S_{ij} \mid D(\cdot,\cdot,\cdot) = 1] = \varepsilon$$

for $j=j^*$ (in case of the correct key)

10) 진짜 키가 아니면 6-비트 키 값을 다르게 설정하여 진짜 키를 찾을 때까지 최대 2^6=64번까지 6)~9)과정을 반복한다.

11) 나머지 S-box #2~#8에 대하여 새로운 키 그룹에서 6-비트의 키 값을 추정하여 6)~10)과정을 실행한다.(본 단계가 끝나면 6x8 = 48비트의 보조 키를 모두 찾을 수 있게 된다.)

12) 56-비트 키 중에서 찾아지지 않은 나머지 8-비트는 기지 평문 공격을 이용하여 평문-암호문 쌍을 이용한 공격으로 찾는다.

3. DPA 실험 및 방어대책

본 실험을 위하여 스마트카드용 어셈블리 프로그램과 DPA 분류 데이터 생성·분석 프로그램이 필요하다.

그림 5는 스마트카드에 어셈블리 언어로 구현된 DES 암호 알고리즘 작동에 따른 암호화 시작점과 끝점간의 시간을 관측한 파형이며, 상단의 가운데 왼쪽으로 "0" 펄스와 가운데 오른쪽 "0" 펄스간이 암호화에 걸리는 시간이다. 이 시간은 대략 5ms 정도이다.

그림 6은 관측할 S1-box의 암호화 시간 위치를 나타내는 파형이며, 그림에서 상단 2번째 파형 "0"와 "0" 사이의 간격이 이를 나타낸다. 이 시간은 대략 25 μs 정도 이다. 하단 파형은 카드리더기에 연결된 미소 저항 측정점에서 관측된 암호해독을 위한 전력정보 파형이다.

실험분석을 위하여 N=100개의 전력 샘플데이터를 수집하여 전력 분석 공격 실험을 실시하였다. 스마트카드 리더기에서 동작하는 S1-box 동작 시점에서 데이터 샘플링을 실시하였고, 그림 7은 첫 번째, 두 번째, 세 번째, 그리고 100번째 전력 샘플데이터에 대하여 S1-box 시작 위치에서 1,000개의 샘플 포인트를 도시한 관측 파형이다.

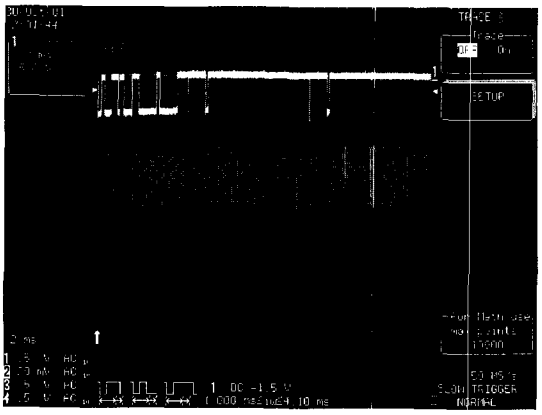


그림 5. DPA 분석을 위한 DES 암호 시간영역 파형

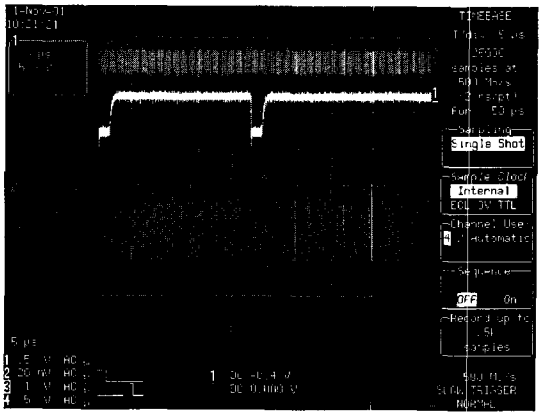
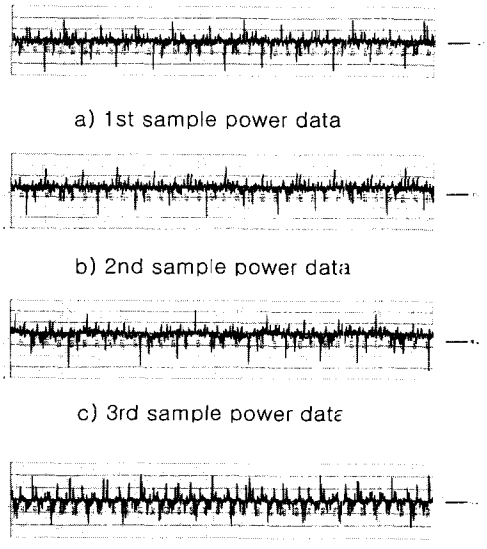


그림 6. DES S8-box에서의 시작과 끝을 나타내는 파형



a) 1st sample power data

b) 2nd sample power data

c) 3rd sample power data

d) 100th sample power data

그림 7. 수집된 전력 샘플데이터(DES의 S1-box 시작 위치에서의 1,000 샘플포인트)

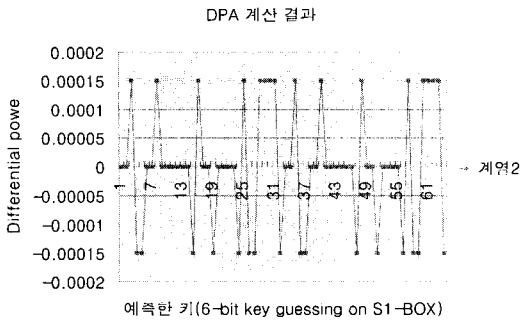


그림 8. S1-box에 대한 결과(correct key = $011100_2 = 28_{10}$ 가정)

임의의 평문데이터 100종과 이로부터 수집된 전력 파형 100종, 그리고 발생된 분류함수 100종에 대한 축소 모델 실험 결과는 그림 8과 같다. 그림에서 세로 축의 차분 전력이 +/- 정점이 되는 지점에서의 가로축 값이 정확한 키(correct key)이다. 그림에서 보는 바와 같이 본 실험 데이터에서는 단일 정점이 아니라 여러 개의 정점이 나타나기 때문에 정확한 키를 추정하기 위해서는 좀 더 많은 데이터와 정밀한 실험 방법이 필요함을 알 수 있다. 그리고 본 실험에서 분석된 키는 정확한 키가 아니라 이를 포함하고 있는 유사 키 그룹을 추정하고 있음을 알 수 있다. 즉, 축소 모델링에 따라 키 추측의 신빙성은 다소 떨어지지만, 원래 키를 포함하는 유사키 군을 정확히 추정하고 있음을 알 수 있다(키를 바꾸어서 실시한 다른 실험 결과에서도 마찬가지임). 하지만 실험에 의한 암호 해독시 대략적인 키 추정이 S-box마다 1/4로 단축되기 때문에 8개의 S-box에 대하여 전체 $1/2^{16}$의 키 공간이 줄어들게 된다. 결국 본 실험에서 키 검색의 수는 2^{56}에서 2^{40}으로 줄어드는 효과를 나타내고 있다. 또한 좀 더 정밀한 실험이 실시된다면 (이 경우 키 검색수는 2^{17}, 표1 참조) DES에 대한 전력분석공격(암호 해독)이 실험적으로 가능함을 보여주고 있다.

본 실험 결과로부터 완전한 DPA 공격이 이루어지기 위해서는 다음과 같은 조건들이 갖추어져야 할 것으로 판단된다.

1) 스마트카드에 대한 사전 정보가 충분하게 제공되어야 한다. 암호 분석을 위하여 마이크로프로세서 구조(또는 하드웨어 구조), 메모리 구조, 활용 메모리(RAM, PROM, EEPROM) 등에 대한 사전 정보가 충분하게 제공되어야 한다.

2) 스마트카드에 대한 응용 프로그램, 암호화 프로그램(S/W 또는 H/W)을 탑재하거나 또는 적절히 수정·변경할 수 있는 환경이 갖추어질 필요가 있다. 스마트카드를 PC상에서 구동시키거나 또는 암호화 알고리즘의 마이크로코드를 분석하여 예측 대상인 부분 키가 작동하는 위치를 정확하게 추정하지 않으면 실험분석은 실패할 가능성이 높다.

3) 경우에 따라서는 스마트카드용 마이크로프로세서에 대한 에뮬레이터를 필요로 할 수도 있다. 마이크로코드에 대한 분석이나 특정 명령어의 정확한 동작 타이밍 정보 등을 분석하기 위하여 필요로 한다.

4) 아주 정밀한 수준의 계측 장비를 보유하여야 한다. 수~수십 GHz의 샘플링이 가능하고, 디지털 데이터 저장능력이 높은(예를 들면, 수십 ms~수 sec 분량의 데이터 저장이 되는 수백 Mbyte~수십 Gbyte 급) 계측장비가 필요하며, 컴퓨터 시뮬레이션을 위한 수집 데이터 저장을 위하여 PC와 연동될 필요가 있다.

5) 수집된 여러 개(예, 1,000개)의 데이터 시작 위치를 정확히 일치시킬 필요성이 있으며, 이에 따른 계측기의 정확한 트리거 기능이 요구된다. 그렇지 않을 경우 키 작용 시점에 대한 정보가 분산될 수 있기 때문에 데이터의 신빙성이 떨어질 수 있다.

다른 한편으로, 일부의 전력원은 DPA 관측에 있어서 전자파 방사라든가 열 잡음 등의 노이즈를 유발시킨다. 장치의 클럭이나 샘플 클럭에 부합함으로서 발생되는 양자화 에러는 또 다른 노이즈를 유발시킨다. 그리고 상관성이 없는 궤적들의 일시적인 불일치(uncorrelated temporal misalignment of traces)는 측정장비에게 상당한 노이즈를 유발시킨다[3-4]. 데이터 수집이나 DPA 분석 과정에서 요구되는 샘플의 수를 줄이거나 또는 방해요소를 우회하는 몇 가지 개선사항이 적용될 수도 있다. 예를 들면, 측정값의 크기 대신에 변경점(variation)의 중요성을 찾음으로서 측정장치의 편차를 줄일 수 있다. 이같은 접근법의 변형 예로 자동 템플릿(automated template) DPA를 들 수 있다[3-4]. 좀 더 복잡한 선택함수가 적용될 수도 있다. 그 중에는 고차 HO-DPA 함수가 있는데, 이 함수는 어떤 궤적 안에서 다수의 샘플을 조합하는 함수이다. 선택함수는 다른 궤적에 대하여 다른 값의 가중치(weight)를 할당할 수 있으며, 또는 두 개의 카테고리 이상으로 궤적을 분할할 수 있다. 이러한 선택 함수는 많은 방어책을 속일 수 있거나 또는 평문이나 암호문에 대한 부분 정보 또는 무정보일 때에도 공격이 가능할 수 있게 해줄 수도 있다. 산술 평균보다는 다른

표 1. DES-like 알고리즘에서 DPA 방어 대책 제안

항목	1) 기존 방안 (6-bit key guessing)	2) 두 개의 S-box씩 묶어서 수행 (12-bit key guessing)	3) 네 개의 S-box씩 묶어서 수행 (24-bit key guessing)	4) 여덟개의 S-box씩 묶어서 수행 (48-bit key guessing)
제안 내용	원래의 방법으로 S-box를 순차적으로 프로그래밍 할 경우이므로 별도의 대책이 요구됨.	인접하는 S-box를 두 개씩 묶어서 프로그래밍 할 경우임.	인접하는 S-box를 네 개씩 묶어서 프로그래밍 할 경우임.	S-box를 모두 묶어서 프로그래밍 또는 하드웨어 구현할 경우임.
S-box 입출력 비트수	Input: 6-bit Output:4-bit # of S-box groups: 8	Input: 12-bit Output: 8-bit # of S-box groups: 4	Input: 24-bit Output: 16-bit # of S-box groups: 2	Input: 48-bit Output: 32-bit # of S-box groups: 1
공격 순서	S1-box → S2-box → S3-box → S4-box → S5-box → S6-box → S7-box → S8-box	S1,S2-box ↓ S3,S4-box ↓ S5,S6-box ↓ S7,S8-box	(S1,S2,S3,S4) ↓ (S5,S6,S7,S8)	(S1,S2,S3,S4, S5,S6,S7,S8)
공격 단계 수	8	4	2	1
분석 복잡도	$[2^6 x8] \times 2^{(56-48)} = 2^{17}$	$[2^{12} x4] \times 2^{(56-48)} = 2^{22}$	$[2^{24} x2] \times 2^{(56-48)} = 2^{33}$	$[2^{48} x1] \times 2^{(56-48)} = 2^{56}$

함수를 사용한 데이터 분석은 보편적이지 않는 통계분포를 갖는 데이터 세트에 대해서도 유용하게 될 수도 있다[3-4].

한편, DES 형태의 알고리즘에 대한 DPA 방어대책으로 다음과 같은 S-box 동시처리 기법을 표1과 같이 제안한다. 이 방법은 S-box를 2개씩 묶어서(S1과 S2, S3와 S4, S5와 S6, 그리고 S7과 S8) 동시 클럭에 처리될 수 있도록 구현하는 원리이다. 이 경우에는 기존 DPA 계산 복잡도보다 2^5배의 복잡도를 개선할 수 있게된다. 또한 S-box를 4개씩 묶어서 동시 클럭으로 처리할 경우에는 또다시 2^{16}의 복잡도가 가산되며, 8개 씩 묶어서 동시 처리할 경우에는 2^{39}의 복잡도가 가산된다. 즉, DES에 대한 DPA 공격 계산 복잡도는 기존방법에서 2^{17}, 2개씩 묶어서 프로세싱할 경우에는 2^{22}, 4개씩 묶어서 프로세싱할 경우에는 2^{33}, 마지막으로 8개 단위로 한꺼번에 프로세싱이 될 경우에는 전수공격에서의 계산복잡도인 2^{56}에 이를 수 있다. 결과적으로 DES 형태의 DPA 방어 대책으로 제안된 S-box를 동시 처리하는 기법에서 8개를 동시 처리할 경우의 계산 복잡도는 전수공격의 복잡도에 이를 수 있기 때문에 좋은 방어대책이 될 수 있다.

상기의 소프트웨어적인 DES 구현에서는 CPU 성능상 한 클럭에서 여러개의 S-box를 동시에 작동시킬 수 없기 때문에 이와같은 근본적인 취약점을 가지며, 이를 하드웨어적으로 구현시에는 S-box 8개를 동시에 한 클럭으로 처리할 수 있기 때문에 이러한 공격으로부터 벗어날 수 있을 것으로 판단된다.

결론적으로 본 논문에서는 스마트카드에 소프트웨어적으로 탑재된 DES 형태의 알고리즘은 차분전력분석 공격에 취약하여 암호 해독이 가능함을 축소 모델 실험을 통하여 보여주었다. 이에 따라 전자상거래 보안을 위하여 DES 형태의 암호 알고리즘을 스마트카드에 탑재 시에는 소프트웨어적인 구현을 피하고 하드웨어적인 구현을 하는 것이 유리하며, 부채널에 의한 해킹 방어 대책이 반드시 추가될 필요가 있음을 알 수 있었다.

V. 결 론

본 논문에서는 스마트카드 암호해독을 위하여 Kocher 형태의 DPA 공격 실험분석 모델을 설정한 후 이를 축소하여 실험을 실시하였다. 실험 분석을 위하여 선정된 장치에는 DES 암호 알고리즘을 어셈블러로 구현한 후 8-비트 마이크로프로세서형 스마트카드에 탑재하였고, 암호 알고리즘 실행 시에 발생되는 차분전력신호를 수집·분석하였다. 이를 위하여 100개의 전력 샘플데이터를 수집하여 전력분석 공격 실험을 실시하였으며, 그 결과 축소형 모델에서의 키 검색 횟수는 2^{56}에서 2^{40}으로 줄어들는 효과를 확인할 수 있었다. 또한 정밀한 모델로는 완전한 DPA 공격이 가능하다는 사실을 보여주었다. 즉, 스마트카드에 소프트웨어적으로 탑재된 DES 형태의 알고리즘은 차분전력분석 공격에 취약하여 암호 해독이 가능함을 축소 모델을 통한 실험으로 보여주었으며, 이에 따라 전자상거래 보안을 위해서는 스마트카드에 탑재 시 소프트웨어적인 구현을 피하고 하드웨어적인 구현을 하는 것이 유리하며, 스마트카드에는 반드시 부채널에 의한 해킹 방어 대책이 추가될 필요가 있음을 확인하였다.

마지막으로 DES 형태의 DPA 방어 대책으로 S-box를 동시 처리하는 기법을 제안하였으며, 8개를

동시 처리할 경우에 계산 복잡도는 전수공격의 복잡도에 이를 수 있기 때문에 좋은 방어대책이 될 수 있다.

참 고 문 헌

[1] John Kelsey, Bruce Schneier, David Wagner, and Chris Hall, "Side Channel Cryptanalysis of Product Cipher," Proceedings of ESORICS'98, pp.97-112, Springer-Verlag, Sep. 1998.

[2] John Kelsey, Bruce Schneier, David Wagner, and Chris Hall, "Side Channel Cryptanalysis of Product Cipher (final version)," in the site, 2000.

[3] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in Proceedings of Advances in Cryptology-CRYPTO'99, pp. 388-397, Springer-Verlag, 1999.

[4] P. Kocher, J. Jaffe, and B. Jun, "Introduction to Differential Power Analysis and Related Attacks," http://www.cryptography.com/dpa/technical, 1998.

[5] Thomas S. Messerges, Ezzy A. Dabbish and Robert H Sloan, "Investigations of Power Analysis Attacks on Smartcards," Proceedings of USENIX Workshop on Smartcard Technology, pp. 151-161, May 1999.

[6] S. Chari, C. Jutla, J. Rao, P. Rohatgi, "Towards Sound Approaches to Counteract Power-Analysis Attacks," in Proceedings of Advances in Cryptology-CRYPTO'99, pp. 398-412, Springer-Verlag, 1999.

[7] E. Biham, A. Shamir, "Power Analysis of the Key Scheduling of the AES Candidates," the 2nd AES conference, 1999.

[8] T.S. Messerges, E.A. Dabbish, and R.H. Sloan, "Power analysis attacks of modular exponentiation in smartcards," CHES'99.

[9] L. Goubin and J. Patarin, "DES and differential power analysis," CHES'99.

[10] P. Fahn and P. Pearson, "IPA: A new class of power attacks," CHES'99.

[11] T.S. Messerges, "Using Second-Order Power Analysis to Attack DPA Resistant Software," CHES'2000, pp.238-251.

이 훈 재(Hoon-Jae Lee) 정회원

1985년 2월 : 경북대학교 전자공학과 졸업(학사)
1987년 2월 : 경북대학교 전자공학과 졸업(석사)
1998년 2월 : 경북대학교 전자공학과 졸업(박사)

1987년 2월~1998년 1월 : 국방과학연구소 선임연구원
1998년 2월~2002년 2월 : 경운대학교 컴퓨터전자정보공학부 조교수
2002년 3월~현재 : 동서대학교 인터넷공학부 정보네트워크공학전공 조교수
<주관심 분야> 정보보호, 네트워크보안, 정보통신

장 익 훈(Ick-Hoon Jang) 정회원

1986년 2월 : 경북대학교 전자공학과 (공학사)
1988년 2월 : 경북대학교 대학원 전자공학과 (공학석사)
1998년 8월 : 경북대학교 대학원 전자공학과 (공학박사)
1988년 2월~1994년 2월 : 국방과학연구소 연구원
1998년 3월~현재 : 경운대학교 컴퓨터전자정보공학부 조교수
<주관심 분야> 영상처리, 영상압축, 컴퓨터비젼

최 희 봉(Hee-Bong Choi)

1984년 2월 : 부산대학교 전기공학과 졸업(학사)
1987년 2월 : 부산대학교 전기공학과 졸업(석사)
1997년 2월 : 성균관대학교 전전컴공학부 박사과정

1987년 2월~2000년 1월 : 국방과학연구소 선임연구원
2000년 1월~현재 : 한국전자통신연구원 부설 국가보안기술연구소 선임연구원
<주관심 분야> 정보보호, 네트워크보안, 보안시스템 설계

박 일 환(Il-Hwan Park)

1988년 2월 : 고려대학교
수학과 졸업(학사)
1990년 8월 : 고려대학교
수학과 졸업(석사)
1996년 2월 : 고려대학교
수학과 졸업(박사)

1996년 5월~1999년 12월 : 한국전자통신연구원 선임 연구원
2000년 1월~현재 : 국가보안기술연구소 선임연구원
<주관심 분야> 암호이론, 정보통신보안