논문 2010-47SP-1-19

마스킹 형태 변환 알고리즘에 대한 새로운 전력 분석 공격

(New Power Analysis Attack on The Masking Type Conversion Algorithm)

조 영 인*, 김 희 석*, 한 동 국**, 홍 석 희***, 강 주 성****

(Young In Cho, HeeSeok Kim, Dong-Guk Han, Seokhie Hong, and JuSung Kang)

요 약

전력 분석 공격의 다양한 대응법들 중 대칭키 암호의 경우, 암/복호화, 키 스케줄링의 연산 도중 중간 값이 전력 측정에 의해 드러나지 않도록 하는 마스킹 기법이 잘 알려져 있다. 대칭키 암호는 Boolean 연산과 Arithmetic연산이 섞여 있으므로 마스킹 형태 변환이 불가피하다. Messerges에 의해서 일반적인 전력 분석 공격에 안전한 마스킹 형태 변환 알고리즘이 제안되었고 이에 대한 취약성이 보고되었다. 본 논문에서는 Messerges가 제안한 마스킹 형태 변환 알고리즘에 대한 기존 전력 분석 공격이 불가능함을 보이고 새로운 전력 분석 공격 방법을 제안한다. 마스킹 형태 변환 알고리즘에 대하여 강화된 DPA와 CPA 공격 방법을 제시한 뒤 시뮬레이션 결과로써 제안하는 공격 방법으로 실제 분석이 가능함을 확인한다.

Abstract

In the recent years, power analysis attacks were widely investigated, and so various countermeasures have been proposed. In the case of block ciphers, masking methods that blind the intermediate results in the algorithm computations(encryption, decryption, and key-schedule) are well-known. The type conversion of masking is unavoidable since Boolean operation and Arithmetic operation are performed together in block cipher. Messerges proposed a masking type conversion algorithm resistant general power analysis attack and then it's vulnerability was reported. We present that some of exiting attacks have some practical problems and propose a new power analysis attack on Messerges's algorithm. After we propose the strengthen DPA and CPA attack on the masking type conversion algorithm, we show that our proposed attack is a practical threat as the simulation results.

Keywords: Side Channel Attack Countermeasure, Masking, Power Analysis Attack, DPA, CPA

I. 서 론

최근 들어 컴퓨터를 이용한 인터넷 사용의 급증과 정보통신 환경의 변화 등으로 스마트카드와 PDA같은 모바일 산업은 빠르게 성장하고 있다. 스마트카드는 소형 컴퓨터의 능력을 가진 신용카드 크기의 보안장치이므로 휴대하기 간편하다는 점이 가장 큰 이점으로 부각되고 있다. 사이버세계에서 스마트카드는 가치이전의 수단뿐만 아니라 전화카드, 이동통신 보안수단, 신분증, 교통카드, 금융 IC 카드 등 그 활용분야가 아주 다양하기 때문에 정보통신망 환경에서 스마트카드가 중요한 보안장치로 수요나 활용 면에서 급격한 증가율을 보이고 있다. 그리고 스마트카드 수요의 증가와 더불어 이에 대한 공격 방법으로 부채널 공격(Side Channel Attack)이 소개되었다[1]. 부채널 공격이란 수학적으로 안전한 것으로 알려진 알고리즘이 구현 단계에서 부가적인 정보를

* 학생회원, *** 정회원, 고려대학교 정보경영공학전문대학원
(Graduate School of Information Management and Security, Korea University)
** 정회원, **** 정회원, 국민대학교 수학과
(Department of Mathematics, Kookmin University)
※ 이 연구에 참여한 연구자(의 일부)는 '2단계 BK21 사업'의 지원비를 받았음.
※ 이 논문은 2008년 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임. (KRF-2008-313-D01028)
접수일자: 2009년6월23일, 수정완료일: 2010년1월5일

누출함으로써 이로부터 비밀 키의 값을 알아낼 수 있는 방법이다. 이러한 부채널 공격이 소개되면서 많은 암호 시스템 설계자들은 효율적인 대응법들을 연구하기 시작했고, 부채널 공격 중 하나인 차분 전력 분석(Differential Power Analysis, DPA)[2~4]과 상관 전력 분석(Correlation Power Analysis, CPA)에 대한 대응법으로는 마스킹 대응법(masking method)이 활발히 연구되고 있다[3, 6~8]. 마스킹 기법은 알고리즘의 변형을 통해 일차 차분 전력 분석을 방어하는 방법으로 노이즈 삽입, 임의의 지연, 랜덤 클록과 같은 하드웨어적인 대응법에 비해 그 비용이 저렴하다. 따라서 단가가 저렴한 스마트카드와 같은 장비에서는 일반적으로 가장 선호하여 사용되어진다. 대칭키 암호의 경우 Boolean 연산과 Arithmetic 연산이 섞여서 사용되므로 마스킹 기법이 적용될 경우 Boolean 마스킹과 Arithmetic 마스킹 사이의 변환이 가능하여야 하며 Messerges에 의하여 마스킹 형태 변환 알고리즘이 제안되었다[5]. [5]에서 제안된 마스킹 형태 변환 알고리즘은 일반적인 DPA를 막기 위해 랜덤 상수를 사용하고 있으나 [9]에서 이 알고리즘의 취약성을 제시하였다. 그러나 일반적인 전력 소비 모델에서는 [9]에서 제시한 취약성을 발견할 수 없으므로 [5]에서 제안된 마스킹 형태 변환 알고리즘은 일반적인 전력 분석 공격에 안전하다.

본 논문에서는 일반적인 전력 소비 모델에서 [9]에서 제시한 공격 방법으로는 [5]의 마스킹 형태 변환 알고리즘이 분석 불가능함을 보이고 이에 대한 새로운 전력 분석 공격 방법을 제안한다. 새로운 DPA 공격 방법은 전력 파형에 제곱을 취하는 신호 전처리 방법을 이용하는 것으로써 옳은 키를 추측하였을 경우 차분이 0이 아닌 파형을 얻을 수 있고 CPA 공격 방법 또한 전력 파형에 제곱을 취하고 중간 값의 해밍웨이트를 특정 값에 대입시킴으로써 공격에 성공한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 마스킹 기법과 마스킹 형태 변환 방법에 대한 간단한 소개와 함께 기존에 제안된 공격 방법에 대해 설명하였다. Ⅲ장에서는 마스킹 형태 변환 알고리즘이 실제 일반적인 전력 소비 모델에서 기존에 제안된 공격 방법으로 분석이 불가능함을 수식과 함께 시뮬레이션 결과를 통하여 확인하였다. Ⅳ장에서는 새로운 공격 방법을 제안하고 시뮬레이션 결과를 통하여 일반적인 전력 소비 모델에서 기존의 공격 방법과 달리 분석이 가능함을 보였다. 마지막으로 Ⅴ장에서 논문의 결론을 맺었다.

Ⅱ. 관련 연구

1. 마스킹 기법

전력 분석 공격이 수행되면서 여러 가지 대응 방법들이 소개되었다. 그 중 암호 알고리즘의 연산이 수행되는 도중 중간 값의 정보를 숨기는 마스킹 기법이 일반적으로 잘 알려져 있다.

마스킹 기법은 구체적으로 평문 m에 대하여 암호문 c를 얻기 위해 마스킹 난수 r을 이용하여 $m \oplus r$(⊕: xor)의 암호문 $c'(=c \oplus r')$을 구한 후, 최종적으로 c를 얻기 위해 $c' \oplus r'$의 연산을 수행한다. (경우에 따라 마스킹 기법은 다르게 구성한다.) 따라서 암호화 중 중간 값을 알 수 없기 때문에 일반적인 전력 분석 공격은 성공할 수 없다. 이러한 마스킹 기법을 사용한 경우, $m \oplus r$의 암호문 $c'(=c \oplus r')$에서 r'을 알아야 실제 원하는 암호문 c를 얻을 수 있다. 하지만 블록암호 알고리즘은 비선형 연산을 수행하므로 수정되지 않은 블록 암호 시스템에서 r'값은 m에 따라 다르며 이 값을 중간 값의 누출 없이 아는 것도 상당한 연산을 필요로 한다.

각 암호 연산들의 입력 값 및 중간 계산 값들에 대해서 랜덤화를 수행하기 위해 두 가지 형태의 마스킹 방법을 사용한다. 첫 번째는 마스킹 연산으로 XOR 연산을 사용하는 Boolean 마스킹이고 두 번째는 프로세서의 레지스터 크기가 K비트라 할 때 $\bmod 2^K$에서 덧셈과 뺄셈 연산을 사용하는 Arithmetic 마스킹이다. 두 가지의 기본적인 마스킹 방법에 따라 주어진 값 x를 랜덤 마스크 r_x로 마스킹 하여 x'을 생성하는 방법은 다음과 같다.

Boolean 마스킹 $x' = x \oplus r_x$

Arithmetic 마스킹 $x' = (x - r_x) \bmod 2^K$

2. 마스킹 형태 변환 방법

SEED, IDEA등과 같은 암호 알고리즘의 마스킹 기법을 고려할 때, 비선형 연산인 덧셈 연산과 S-box 연산에 대한 마스킹 방법이 조화를 이룰 수 있는 전체 구조에 대한 설계가 동시에 이루어져야 하며 이로 인해 Boolean 마스킹과 Arithmetic 마스킹 사이의 변환 알고리즘에 대한 고려가 불가피하다. 예를 들어, 대칭키 암호 연산의 중간 값인 (x, y)가 덧셈 연산의 입력 값으로 Boolean 마스킹 되어$(x \oplus r_x, y \oplus r_y)$ 입력된다면, 우선 설계자는 이 값을 Arithmetic 마스킹 값으로 변환

$(x-r_x, y-r_y)$ 한 후, 덧셈 연산을 수행하고 그 결과 값 $((x+y)-(r_x+r_y))$을 다시 Boolean 마스킹으로 변환 $((x+y)\oplus(r_x+r_y))$ 하는 작업을 수행해야만 한다. 하지만, 이 변환 과정에서 중간 값인 (x,y)는 평문이 m이고 키가 k일 때, $m\oplus k$ 또는 S-box$(m\oplus k)$와 같은 값이므로 마스킹 되지 않은 평문 형태로 노출된다면 이는 차분 전력 분석에 취약하게 된다. 즉, 변환 과정 중 모든 값은 편중되지 않은 난수에 의해 가려져야만 한다. 이 변환 과정을 차분 전력 분석으로부터 안전하게 구성하기 위해 Messerges는 [5]에서 마스킹 형태 변환 알고리즘을 제안하였다. Messerges가 제안한 마스킹 형태 변환 알고리즘은 알고리즘 1, 2와 같다.

알고리즘 1을 수행해서 얻게 되는 결과는 입력 값 $x'\oplus r_x = A+r_x$를 만족하는 A이다. 즉, 알고리즘 1에서의 결과 값인 A는 마스킹이 되지 않았을 때의 중간 값 x를 유지하면서 Boolean 마스크된 $x'(x\oplus r_x)$ 값을 Arithmetic 마스크된 $A(x-r_x)$ 값으로 출력한다. 알고리즘 1은 중간 값 x가 노출되지 않도록 랜덤 상수 C를 사용하고 있다. 즉, 알고리즘 1의 step3에서 마스킹 되지 않은 중간 값 x가 1/2의 확률로 노출되고 $\overline{x}$ 또한 1/2의 확률로 노출되므로 일반적인 DPA와 CPA에 안전하게 구성되어진다. Arithmetic 마스크된 값을 Boolean 마스크된 값으로 변형하는 알고리즘 2도 알고리즘 1과 유사하게 구성되며 같은 안전성을 가진다.

```
BooleanToArithmetic {
Input : x'(=x⊕r_x), r_x
  Output : A(=x-r_x)
   step 1 : randomly select : C=0 or C= -1

2 : B=C⊕r_x ;  /* B=r_x or B=r_x~ */
3 : A=B⊕x' ;  /* A=x or A=x~ */
4 : A=A-B ;  /* A=x-r_x or A=x~-r_x~ */
5 : A=A+C ;  /* A=x-r_x or A=x~-r_x~-1 */
6 : A=A⊕C ;  /* A=x-r_x */
7 : Return A ;
}
```

알고리즘 1. Boolean 마스킹에서 Arithmetic 마스킹으로의 형태 변환 알고리즘

```
ArithmeticToBoolean {
Input : A(=x-r_x), r_x
Output : A(=x⊕r_x)
step 1 : randomly select : C=0 or C= -1
2 : B=C⊕r_x ;  /* B=r_x or B=r_x~ */
3 : A=A⊕C ;  /* A=x-r_x or A=x~-r_x~-1 */
4 : A=A+C ;  /* A=x-r_x or A=x~-r_x~ */
5 : A=A+B ;  /* A=x or A=x~ */
6 : A=A⊕B ;  /* A=x⊕r_x */
7 : Return A ;
}
```

알고리즘 2. Arithmetic 마스킹에서 Boolean 마스킹으로의 형태 변환 알고리즘

3. 마스킹 형태 변환 방법의 취약성

[5]에서 제안된 마스킹 형태 변환 알고리즘은 수행 시 마다 랜덤하게 선택되어진 C 값에 의해 중간 값이 x 또는 $\overline{x}$로 연산된다. 따라서 x의 특정 비트가 랜덤하게 바뀌므로 일반적인 DPA에는 안전하다.

[9]에서는 이 알고리즘의 취약성에 대해 기술하고 있으며 공격자가 예측한 중간 값 x의 두 비트에 대해 다음 순서로 DPA를 수행한다면 키가 노출될 수 있다고 주장하고 있다.

- 추측한 x값의 특정 두 비트에 따라 전력 파형을 네 개의 집합으로 나눈다. $(X_{00}, X_{01}, X_{10}, X_{11})$
- 각 집합의 평균 파형을 구한다. $(\mu_{00}, \mu_{01}, \mu_{10}, \mu_{11})$
- 평균 파형을 이용해 $D=(\frac{\mu_{00}+\mu_{11}}{2})-(\frac{\mu_{01}+\mu_{10}}{2})$의 차분 파형을 얻는다.
- 차분 파형 D들 중, 가장 큰 차분을 갖는 값에 해당하는 키를 선택한다.

III. 기존 분석 방법 활용의 어려움

본 장에서는 Messerges가 제안한 일반적인 전력 소비 모델에서 기존에 제안된 [9]의 공격 방법은 적용 불가능함을 보이고 시뮬레이션 결과를 통하여 이를 확인한다. Messerges가 제안한 전력 소비 모델(C)은 다음과 같다.

$$C = offset + \varepsilon HW(Data) + N$$

(이때, $offset, \varepsilon$: 상수, N : 노이즈, $HW(Data)$: $Data$의 해밍웨이트)

또한 [9]에서 제안된 분석 방법 뿐 아니라 일반적인 CPA 공격 방법으로도 [5]의 마스킹 형태 변환 알고리즘이 쉽게 분석 불가능함을 상관계수를 통하여 증명하고 역시 시뮬레이션 결과로 이를 확인한다. 공격은 8 비트 환경으로 DPA는 기존 방법과 마찬가지로 2 비트에 대하여, CPA는 8 비트에 대하여 시뮬레이션 하였다. 시뮬레이션 환경으로 상수 $\varepsilon = 3.72\,mA$, $offset = 10\,mA$ 이고 $N(0, (1.9636\,mA)^2)$의 가우시안 분포를 따르는 노이즈를 주입하였다.

1. [9]의 DPA 공격 방법

일반적인 전력 소비 모델의 경우 노이즈를 제거한 소비 전력이 데이터의 해밍웨이트와 정확히 1차 선형 관계를 가지므로 [9]에서 제안한 공격 방법은 분석에 성공할 수 없다. 즉, [9]에서 제안한 차분 파형을 얻어내는 방정식으로부터 다음의 수식이 성립한다. (N_{00}, N_{01}, N_{10}, N_{11})는 추측한 x값의 특정 두 비트에 따른 평균 전력 소비 모델의 노이즈를 의미한다.

$$\begin{aligned} D &= \left(\frac{\mu_{00}+\mu_{11}}{2}\right) - \left(\frac{\mu_{01}+\mu_{10}}{2}\right) \\ &= \left(\frac{(offset+N_{00})+(offset+2\varepsilon+N_{11})}{2}\right) \\ &\quad - \left(\frac{(offset+\varepsilon+N_{01})+(offset+\varepsilon+N_{10})}{2}\right) \\ &\approx 0 \end{aligned}$$

따라서 키 값을 정확히 추측해 분류가 옳게 되더라도 공격자는 이러한 차분 특성에 의해 분석에 실패하게 된다. 그림 1의 시뮬레이션 결과를 통하여 이를 확인할 수 있다. 틀린 키 255개에 대한 전력 파형의 차분 값 중에서 가장 큰 차분 값을 D_{wrong}, 옳은 키에 대한 전력 파형의 차분 값을 $D_{correct}$라 할 때, 그림 1은 전력 파형 개수 별 해당 위치에서의 $D_{correct}/D_{wrong}$을 나타낸다. $D_{correct}/D_{wrong}$ 값이 1보다 크다면 옳은 키의 차분 값이 틀린 키의 어떤 차분 값보다도 크므로 분석이 가능하다. 그림 1에서는 100000개의 trace를 이용할 때, $D_{correct}/D_{wrong}$값이 1 보다 작은 값으로 수렴하게 되어 분석이 불가능함을 알 수 있다.

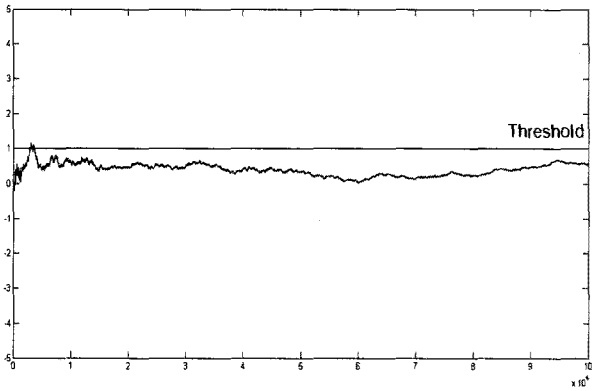


그림 1. [9]에서 제안된 DPA 공격 방법의 시뮬레이션 결과

Fig. 1. The Simulation result of DPA attack [9].

2. 일반적인 CPA의 공격 방법

알고리즘 1의 step3과 알고리즘 2의 step5에서 보면 수행 시 마다 랜덤하게 선택되어진 C 값에 의해 중간 값이 x또는 $\bar{x}$로 노출된다. 8 비트 환경을 가정하므 x로 x의 해밍웨이트를 $HW(x)$라 하면 $\bar{x}$의 해밍웨이트는 $8-HW(x)$와 같게 된다. 공격에 $2n$개의 평문을 이용한다고 하면 C 값이 랜덤하게 선택되므로 n번의 수행에서는 중간 값 x가 노출되고 나머지 n번의 수행에서는 $\bar{x}$가 노출된다. 일반적인 전력 소비 모델에서의 CPA 공격을 수행하기 위해 다음과 같이 상관계수를 구하도록 한다.

- $2n$개의 평문을 이용할 때, 중간 값 x의 전력 파형의 집합을 X라 하면

$$X = \left\{ \begin{matrix} offset+\varepsilon t_i+N_i \mid t_i = HW(x_i)\ (1 \le i \le n), \\ t_i = 8-HW(x_i)\ (n+1 \le i \le 2n) \end{matrix} \right\}$$

  이고, w_i를 중간 값 x_i의 해밍웨이트라고 하면 w_i을 원소로 갖는 집합 W는 다음과 같다.

$$W = \{w_i \mid w_i = HW(x_i)\ (1 \le i \le 2n)\}$$

- X와 W의 상관계수($\rho_{X,W}$)를 구한다.

Theorem 1. X와 W의 상관계수($\rho_{X,W}$)는 0으로 수렴한다.

proof. APPENDIX를 참고한다.

Theorem 1에서 확인할 수 있듯이 옳은 키를 추측했다 하더라도 일반적인 CPA의 상관계수는 0으로 수렴

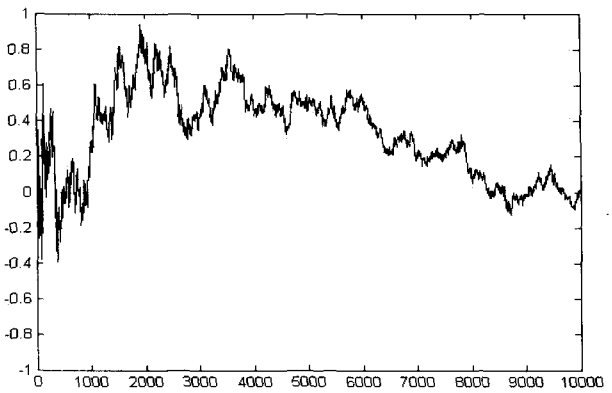


그림 2. 일반적인 CPA 공격 방법의 시뮬레이션 결과
Fig. 2. The Simulation result of the general CPA attack.

하므로 분석에 성공할 수 없다. 이는 그림 2의 시뮬레이션 결과를 통하여 확인할 수 있다. 틀린 키 255개에 대한 전력 파형의 상관계수 중 가장 큰 상관계수를 C_{wrong}, 옳은 키에 대한 전력 파형의 상관계수를 $C_{correct}$라 할 때, 그림 2는 전력 파형 개수 별 해당 위치에서의 $C_{correct}/C_{wrong}$을 나타낸다. $C_{correct}/C_{wrong}$ 값이 1보다 크다면 옳은 키의 상관계수가 틀린 키의 어떤 상관계수보다도 크므로 분석이 가능하다. 그림 2에서는 10000개의 trace를 이용할 때, $C_{correct}/C_{wrong}$값이 1 보다 작은 값으로 수렴하게 되어 분석이 불가능함을 알 수 있다.

Ⅳ. 제안하는 공격 방법

본 절에서는 Messerges가 제안한 일반적인 전력 소비 모델에서 공격이 가능한 새로운 전력 분석 공격 방법을 제안한다. 본 논문에서는 신호 전처리 과정으로 전력 파형을 수집한 후 각 파형들을 제곱한 파형을 구한다. 제안하는 DPA 공격 방법은 기존의 분석 방법과 달리 신호 전처리 기법을 사용하여 옳은 추측 값에 대하여 차분을 발견할 수 있으며, CPA 공격 방법에서도 신호 전처리 기법과 새롭게 부여하는 값을 이용함으로써 옳은 키에 대하여 0이 아닌 상관계수를 찾을 수 있다.

제안하는 전력 분석 공격의 가정은 기존 공격 방법과 동일하며 제안하는 분석 방법의 시뮬레이션 결과는 다음 소절에서 확인한다.

1. 제안하는 DPA 공격 방법

제안하는 DPA 공격 방법은 전력 파형의 제곱을 취하여 노이즈를 제거한 소비 전력이 데이터의 해밍웨이트와 1차 선형 관계를 갖지 않도록 한다. 위와 같은 신호 전처리 기법을 사용하면 노이즈 제거 효과 외에도 수식적으로 공격이 성공할 수 있는 근거를 제공할 수 있다. $v(2 \le v \le 8)$비트 DPA 공격을 수행하는 과정은 다음과 같다.

- 추측한 x값의 특정 v비트의 해밍웨이트에 따라 전력 파형의 제곱을 취하여 v개의 집합으로 나눈다. 이때 x값의 특정 v비트의 해밍웨이트가 α이면 x의 전력 파형의 제곱은 집합 X_α'에 속하게 된다. $(X_0', X_1', X_2', \cdots, X_v')$
- 각 집합의 평균 파형을 구한다.$(\mu'_0, \mu'_1, \mu'_2, \cdots, \mu'_v)$
- 평균 파형을 이용해 차분 파형 D 를 얻는다.

$$D = \frac{\left(\sum_{i=0}^{\left\lfloor \frac{v}{2}-1 \right\rfloor} \frac{\mu'_i + \mu_{v-i}'}{2} \right)}{\left\lfloor \frac{v}{2} \right\rfloor} - \left(\frac{\mu'_{\left\lfloor \frac{v}{2} \right\rfloor} + \mu'_{v-\left\lfloor \frac{v}{2} \right\rfloor}}{2} \right).$$

- 차분 파형 D들 중, 가장 큰 차분을 갖는 값에 해당하는 키를 선택한다.

Theorem 2. 제안하는 DPA 공격 방법의 2 비트 차분 값, 즉 $v=2$일 때

$$D = \frac{\left(\sum_{i=0}^{\left\lfloor \frac{v}{2}-1 \right\rfloor} \frac{\mu'_i + \mu_{v-i}'}{2} \right)}{\left\lfloor \frac{v}{2} \right\rfloor} - \left(\frac{\mu'_{\left\lfloor \frac{v}{2} \right\rfloor} + \mu'_{v-\left\lfloor \frac{v}{2} \right\rfloor}}{2} \right)$$ 는

대략 ε^2이다.

proof. APPENDIX를 참고한다.

즉, 옳은 추측 값에 의해 차분이 발생하는 파형을 발견할 수 있으므로 제안하는 DPA 공격 방법에 의해 [5]의 마스킹 형태 변환 알고리즘의 취약성이 발견된다.

2. 제안하는 CPA 공격 방법

제안하는 CPA 공격 방법은 제안하는 DPA 공격 방법과 마찬가지로 전력 파형의 제곱을 취하여 소비 전력이 연산되는 중간 데이터의 해밍웨이트와 1차 선형 관계를 갖지 않도록 한다. 제안하는 $v(2 \le v \le 8)$ 비트 CPA 공격을 수행하는 과정은 다음과 같다.

- $2n$개의 평문을 이용할 때, 추측한 x값의 전력 파형 제곱의 집합을 X'이라 하고 $\overline{HW}(x)$를 x의 특정 v 비트의 해밍웨이트라 하자.

$$X' = \left\{ \begin{matrix} (offset + \varepsilon t_i + N_i)^2 \mid t_i = \overline{HW}(x_i)\ (1 \le i \le n), \\ t_i = v - \overline{HW}(x_i)\ (n+1 \le i \le 2n) \end{matrix} \right\}$$

일반적인 CPA 공격 방법에서 X와 x_i의 해밍웨이트 집합과의 상관계수를 구했다면 제안하는 CPA 공격 방법에서는 X'과 x_i와 $\overline{x_i}$의 해밍웨이트 제곱의 평균 집합 W'과의 상관계수를 구하도록 한다. $W' = \{w_i' \mid 1 \le i \le 2n\}$의 원소 w_i'은 다음과 같다.

$$w_i' = \frac{\overline{HW}(x_i)^2 + \{v - \overline{HW}(x_i)\}^2}{2}$$

- X'과 W'의 상관계수($\rho_{X',W'}$)를 구한다.
- 가장 큰 상관계수를 갖는 값에 해당하는 키를 선택한다.

표 1은 제안하는 전력 분석 방법으로 8 비트 공격을 수행할 경우 추측한 중간 값 x_i의 해밍웨이트에 따른 w_i'를 나타낸 표이다.

표 1. x_i의 해밍웨이트에 따른 w_i' 값
Table 1. The value of w_i' according to $\overline{HW}(x_i)$.

x_i의 Hamming Weight($\overline{HW}(x_i)$)	부여하는 값(w_i')
0 또는 8	32
1 또는 7	25
2 또는 6	20
3 또는 5	17
4	16

Theorem 3. 제안하는 CPA 공격 방법의 2 비트 상관계수, 즉 $v=2$일 때 X'와 W'의 상관계수($\rho_{X',W'}$)는 대략 $\frac{\varepsilon}{2\sqrt{2(offset+\varepsilon)^2+0.25}}$ 이다.

proof. APPENDIX를 참고한다.

Theorem 3. 에서 확인 할 수 있듯이 옳은 키를 추측했다면 해당 소비 전력 파형의 제곱의 집합(X')과 부여한 값(W')에 대해서 0이 아닌 상관계수를 구할 수 있게 된다.

Corollary 1. X'와 W'의 상관계수($\rho_{X',W'}$)는 $offset = -\varepsilon$일 때, 최대값을 갖는다.

Corollary 1은 Theorem 3을 통하여 쉽게 도출될 수 있다. 상관계수의 특성에 따라 $offset$값을 적절히 조절한다면 보다 큰 상관계수를 발견할 수 있게 된다. 즉, Corollary 1에 의해서 $offset = -\varepsilon$가 되도록, 수집한 전력 파형에서 $offset+\varepsilon$의 상수 값을 뺀 후 파형을 제곱하는 추가적인 신호 전처리 과정을 수행한다면 가장 큰 상관계수를 얻게 된다.

Theorem 2, 3을 통하여 제안하는 2비트 DPA, CPA 공격 방법으로 알고리즘 1, 2가 분석 가능함을 이론적으로 보였다. 또한 공격 비트 수를 늘인다면 보다 좋은 분석 결과를 얻을 것이라 예상할 수 있다.

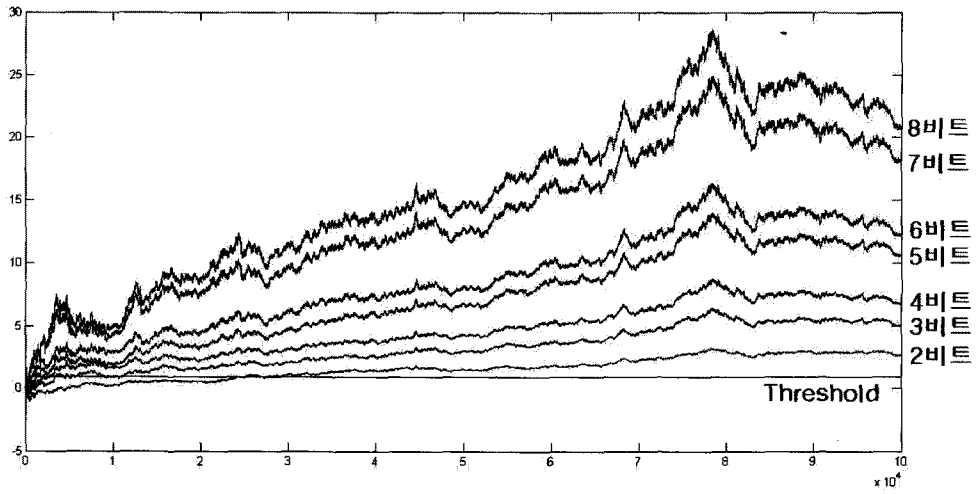


그림 3. 제안하는 v비트 DPA 시뮬레이션 결과
Fig. 3. The Simulation result of the proposed v bit DPA.

3. 시뮬레이션 결과

제안하는 전력 분석 공격 알고리즘의 시뮬레이션 결과를 확인해 보도록 하자. 시뮬레이션 환경은 기존 공격 방법의 것과 동일하다.

(1) 제안하는 DPA 공격 방법의 시뮬레이션 결과

그림 3에서 제안하는 DPA 공격 방법의 시뮬레이션 결과를 확인해보도록 하자. 4.1 절에서 서술한 바와 같이 추측한 중간 값의 특정 비트의 해밍웨이트에 따라 분류한 후 수집한 전력 파형에 제곱을 취하여 차분을 구하고 $D_{correct}/D_{wrong}$을 계산한 결과이다. 그림 3에서 100000개의 trace를 이용할 때, 8 비트 시뮬레이션 환경에서 비트 별 $D_{correct}/D_{wrong}$의 값은 1 보다 훨씬 큰 값에서 수렴하며 v 비트 공격을 수행할 경우 v가 클수록 그 값이 커짐을 확인할 수 있다.

(2) 제안하는 CPA 공격 방법의 시뮬레이션 결과

그림 4는 제안하는 CPA 공격 방법의 시뮬레이션 결과이다. 4.2 절에서 서술한 바와 같이 전력 파형에 제곱을 취한 파형의 집합과 새롭게 부여하는 값을 원소로 갖는 집합간의 상관계수를 구한 후 $C_{correct}/C_{wrong}$을 계산한 결과이다. 그림 3에서 10000개의 trace를 이용할 때, 8 비트 시뮬레이션 환경에서 비트 별 $C_{correct}/C_{wrong}$의 값은 역시 1 보다 훨씬 큰 값에서 수렴하며 v 비트 공격을 수행할 경우 v가 클수록 상관계수가 커짐을 확인할 수 있다.

V. 결 론

본 논문에서는 Messerges가 제안된 마스킹 형태 변환 알고리즘에 대하여 기존에 제안된 전력 분석 방법이 일반적인 소비모델에서 공격 불가능함을 보이고 이를 시뮬레이션 결과를 통하여 확인하였다. 그리고 새로운 공격 방법으로 강화된 DPA와 CPA 공격 방법을 제안하였으며, 제시한 공격들이 실제로도 적용될 수 있는 구체적인 분석 방법을 이론적으로 증명하였다. 뿐만 아니라 제안하는 공격 방법이 일반적인 전력 소비 모델에서 공격 가능함을 시뮬레이션 결과를 통하여 확인하였다. 제안하는 공격 방법은 마스킹 형태 변환 알고리즘에 대한 공격 방향을 제시한다.

참 고 문 헌

[1] P. Kocher, J. Jaffe, and B. Jun, "*Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Others Systems.*" CRYPTO'6, LNCS 1109, pp.104-113, Springer-Verlag, 1996.

[2] P. Kocher, J. Jaffe, and B. Jun, "*Differential power analysis,*" CRYPTO'9, pp.388-397, Springer -Verlag, 1999.

[3] P. Kocher, J. Jaffe, and B. Jun, "*Introduction to differential power analysis and related attacks,*"i http://www.cryptography.com/dpa/technical, 1998.

[4] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "*Power analysis attacks on modular exponentiation in Smart cards,*" Proc. of

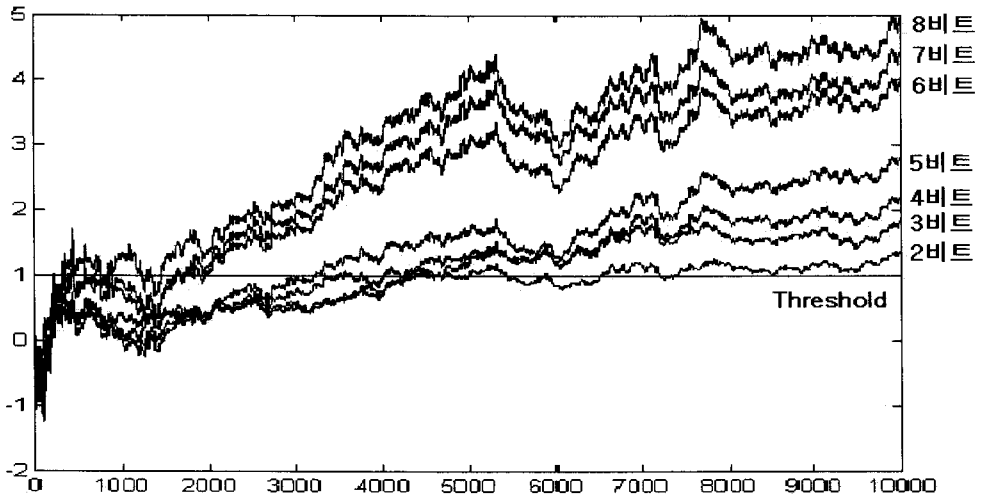


그림 4. 제안하는 v비트 CPA 시뮬레이션 결과
Fig. 4. The Simulation result of the proposed v bit CPA.

Workshop on Cryptographic Hardware and Embedded Systems, pp.144-157, Springer-Verlag, 1999.

[5] T. Messerges, "*Securing the AES Finalists Against Power Analysis Attacks*," Proc. Seventh Int'l Workshop Fast Software Encryption (FSE 2000), pp. 150-164, 2001.

[6] E. Oswald and K. Schramm. "*An Efficient Masking Scheme for AES Software Implementations*," TM WISA 2005, LNCS 3786, pp. 292 - 305, Springer, 2006.

[7] E. Oswald, S. Mangard, N. Pramstaller, and V. Rijmen., "*A Side-Channel Analysis Resistant Description of the AES S-box*," FSE 2005, LNCS 3557, pp. 413 - 423, Springer, 2005.

[8] J. Bl¨omer, J. Guajardo, and V. Krummel. "*Provably Secure Masking of AES*," SAC 2004, LNCS 3357, pp. 69-83, Springer, 2005.

[9] J.S. Coron, L. Goubin, "*On Boolean and Arithmetic Masking against Differential Power Analysis*," Proc. of CHES'00, pp. 231-237, 2000.

APPENDIX

Notation

- $H=\begin{Bmatrix} t_i \mid t_i = HW(x_i)\ (1 \le i \le n), \\ t_i = 8 - HW(x_i)\ (n+1 \le i \le 2n) \end{Bmatrix}$.
- $\overline{H}=\begin{Bmatrix} t_i \mid t_i = \overline{HW}(x_i)\ (1 \le i \le n), \\ t_i = 2 - \overline{HW}(x_i)\ (n+1 \le i \le 2n) \end{Bmatrix}$,
  $\overline{HW}(x_i)$는 x_i의 특정 두 비트의 해밍웨이트.
- $E(X)$: X의 기댓값.
- $\sigma_X = \sqrt{E(X^2) - \{E(X)\}^2}$: X의 표준편차.
- $\rho_{X,W} = \dfrac{E(XW) - E(X)E(W)}{\sigma_X \sigma_W}$: X, W의 상관계수.

본 논문에서는 차분 값과 상관계수를 구하는 Theorem 증명에 있어 노이즈의 영향을 무시한다는 가정하에 증명을 진행하도록 한다.

표 2. Theorem 1, 3에 사용되는 기댓값
Table 2. Expacted values of Theorem 1, 3.

Notation	기대값
Theorem 1	
$E(H)$	4
$E(W)$	4
$E(HW)$	16
Theorem 3	
$E(\overline{H})$	1
$E(\overline{H^2})$	1.5
$E(\overline{H^3})$	2.5
$E(\overline{H^4})$	4.5
$E(W')$	1.5
$E(W'^2)$	2.5
$E(\overline{H}W')$	1.5
$E(\overline{H^2}W')$	2.5

(이때, W는 8 비트, W'는 2 비트 CPA에 사용되는 집합이다.)

Theorem 1. X와 W의 상관계수($\rho_{X,W}$)는 0으로 수렴한다.

proof. 일반적인 8 비트 CPA 공격을 위해 상관계수 $\rho_{X,W}$를 구하도록 한다.

$$\rho_{X,W} = \frac{E(XW) - E(X)E(W)}{\sigma_X \sigma_W}$$

$$= \frac{\dfrac{\sum_{1}^{n}(offset + \varepsilon HW(x_i))w_i + \sum_{n+1}^{2n}(offset + \varepsilon(8 - HW(x_j)))w_j}{2n}}{\sigma_X \sigma_W}$$

$$- \frac{\left\{\dfrac{\sum_{1}^{n}(offset + \varepsilon HW(x_i)) + \sum_{n+1}^{2n}(offset + \varepsilon HW(8 - x_j))}{2n}\right\}E(W)}{\sigma_X \sigma_W}$$

$$= \frac{offset\,E(W) + \varepsilon E(HW) - \{offset + \varepsilon E(H)\}E(W)}{\sigma_X \sigma_W}$$

$$= \frac{0}{\sigma_X \sigma_W}$$

$$= 0$$

Theorem 2. 제안하는 DPA 공격 방법의 2 비트 차분 값, 즉 $v = 2$일 때

$$D = \frac{\left(\sum_{i=0}^{\lfloor \frac{v}{2} - 1 \rfloor} \frac{\mu'_i + \mu_{v-i}'}{2}\right)}{\left\lfloor \frac{v}{2} \right\rfloor} - \left(\frac{\mu'_{\lfloor \frac{v}{2} \rfloor} + \mu'_{v - \lfloor \frac{v}{2} \rfloor}}{2}\right)$$ 는

대략 ε^2이다.

proof. D가 본 논문에서 제안하는 DPA 공격 방법의 차분이라 할 때, 기존에 제안되었던 공격 방법과 마찬가지로 2 비트 DPA를 수행할 경우의 차분 D는 아래와 같이 구할 수 있다. 여기서 c_i는 X_i의 원소의 개수이다 $(i=0,1,2)$.

$$D=\left(\frac{\mu'_0+\mu_2'}{2}\right)-\mu'_1$$

$$=\frac{\frac{\sum_{k=1}^{c_0}(offset)^2}{c_0}+\frac{\sum_{r=1}^{c_2}(offset+2\varepsilon)^2}{c_2}}{2}-\frac{\sum_{s=1}^{c_1}(offset+\varepsilon)^2}{c_1}$$

$$=\frac{\sum_{k=1}^{c_0}(offset^2)}{2c_0}+\frac{\sum_{r=1}^{c_2}(offset^2+4\varepsilon^2+4\varepsilon\, offset)}{2c_2}$$

$$-\frac{\sum_{s=1}^{c_1}(offset^2+\varepsilon^2+2\varepsilon offset)}{c_1}$$

$$=\varepsilon^2$$

Theorem 3. 제안하는 CPA 공격 방법의 2 비트 상관계수, 즉 $v=2$일 때 X'와 W'의 상관계수($\rho_{X',W'}$)는 대략 $\frac{\varepsilon}{2\sqrt{2(offset+\varepsilon)^2+0.25}}$이다.

proof. 제안하는 공격 방법으로 2 비트 CPA 공격을 위해 상관계수 $\rho_{X',W'}$를 구하도록 한다. 2 비트가 아닌 $v(3\le v\le 8)$ 비트 CPA 공격시에는 $\overline{H}$, W'집합과 이에 따른 기대값들을 갱신하여 상관계수를 구할 수 있다.

$$\rho_{X',W'}=\frac{E(X'W')-E(X')E(W')}{\sigma_{X'}\sigma_{W'}}$$

1) $E(X'W')-E(X')E(W')$

• $E(X'W')$

$$=\frac{\sum_{1}^{n}(offset+\varepsilon\overline{HW}(x_i))^2w_i'+\sum_{n+1}^{2n}(offset+\varepsilon(2-\overline{HW}(x_j)))^2w_j'}{2n}$$

$$=offset^2E(W')+\varepsilon^2E(\overline{H^2}W')+2\varepsilon^2E(W')-2\varepsilon^2E(\overline{H}W')$$
$$+2\varepsilon offset\,E(W')$$

$$=1.5offset^2+2.5\varepsilon^2+3\varepsilon offset$$

• $E(X')$

$$=\frac{\sum_{1}^{n}(offset+\varepsilon\overline{HW}(x_i))^2+\sum_{n+1}^{2n}(offset+\varepsilon(2-\overline{HW}(x_j)))^2}{2n}$$

$$=offset^2+\varepsilon^2E(\overline{H^2})+2\varepsilon^2-2\varepsilon^2E(\overline{H})+2\varepsilon offset$$

$$=offset^2+1.5\varepsilon^2+2\varepsilon offset$$

• $E(X')E(W')=1.5offset^2+2.25\varepsilon^2+3\varepsilon offset$

$\therefore\ E(X'W')-E(X')E(W')=0.25\varepsilon^2$

2) $\sigma_{X'}\sigma_{W'}$

• $\sigma_{X'}=\sqrt{E(X'^2)-E(X')^2}$

• $E(X'^2)$

$$=\left\{\frac{\sum_{1}^{n}(offset+\varepsilon\overline{HW}(x_i))^4+\sum_{n+1}^{2n}(offset+\varepsilon(2-\overline{HW}(x_j)))^4}{2n}\right\}$$

$$=offset^4+4.5\varepsilon^4+10\varepsilon^3offset+9\varepsilon^2offset^2+4\varepsilon offset^3$$

• $E(X')^2$

$$=\left\{\frac{\sum_{1}^{n}(offset+\varepsilon\overline{HW}(x_i))^2+\sum_{n+1}^{2n}(offset+\varepsilon(2-\overline{HW}(x_j)))^2}{2n}\right\}^2$$

$$=offset^4+2.25\varepsilon^4+6\varepsilon^3offset+7\varepsilon^2offset^2+4\varepsilon offset^3$$

• $\sigma_{X'}=\sqrt{2.25\varepsilon^4+4\varepsilon^3offset+2\varepsilon^2offset^2}$

$$=\sqrt{2\varepsilon^2(offset+\varepsilon)^2+0.25\varepsilon^2}$$

• $\sigma_{W'}=0.5$

$\therefore\ \sigma_{X'}\sigma_{W'}=0.5\sqrt{2\varepsilon^2(offset+\varepsilon)^2+0.25\varepsilon^2}$

3) $\frac{E(X'W')-E(X')E(W')}{\sigma_{X'}\sigma_{W'}}$

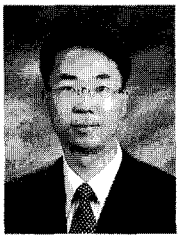
$$=\frac{0.25\varepsilon^2}{0.5\varepsilon\sqrt{2(offset+\varepsilon)^2+0.25}}$$

$$=\frac{\varepsilon}{2\sqrt{2(offset+\varepsilon)^2+0.25}}$$

$\therefore\ \rho_{X',W'}=\frac{\varepsilon}{2\sqrt{2(offset+\varepsilon)^2+0.25}}$

저 자 소 개

조 영 인(학생회원)
2006년 2월 한양대학교 수학과 학사
2009년 2월 고려대학교 정보경영공학전문대학원 공학석사
2009년 9월~현재 고려대학교 정보경영공학전문대학원 박사과정
<주관심분야 : 암호칩 설계 기술, 부채널 공격, 암호시스템 고속구현>



한 동 국(정회원)-교신저자
1999년 2월 고려대학교 수학과 학사
2002년 2월 고려대학교 수학과 이학석사
2005년 2월 고려대학교 정보보호대학원 공학박사
2004년 4월~2005년 4월 일본 Kyushu Univ., 방문연구원
2005년 4월~2006년 4월 일본 Future Univ.-Hakodate, Post.Doc.
2006년 6월~2009년 2월 한국전자통신연구원 정보보호연구단 선임연구원
2009년 3월~현재: 국민대학교 수학과 조교수
<주관심분야: 암호시스템 안전성 분석 및 고속구현, 부채널 분석, RFID/USN 정보보호 기술>

강 주 성(정회원)
1989년 2월 고려대학교 수학과 학사
1991년 2월 고려대학교 수학과 이학석사
1996년 2월 고려대학교 수학과 이학박사
1997년~2004년 ETRI 선임연구원
2004년~현재 : 국민대학교 수학과 부교수
<주관심분야 : 암호 알고리즘, 암호 프로토콜>

김 희 석(학생회원)
2006년 2월 연세대학교 수학과 학사
2008년 2월 고려대학교 정보경영공학전문대학원 공학석사
2008년~현재 고려대학교 정보경영공학전문대학원 박사과정
<주관심분야 : 부채널 공격, 암호시스템 안전성 분석 및 고속구현, 암호칩 설계 기술>

홍 석 희(정회원)
1995년 2월 고려대학교 수학과 학사
1997년 2월 고려대학교 수학과 이학석사
2001년 2월 고려대학교 수학과 이학박사
1999년 8월~2004년 2월 (주)시큐리티 테크놀로지스 선임연구원
2003년 3월~2004년 2월 고려대학교 시간강사
2004년 4월~2005년 2월 K.U. Leuven 박사후 연구원
2005년 3월~2008년 8월 고려대학교 정보경영공학전문대학원 조교수
2008년 9월~현재 고려대학교 정보경영공학전문대학원 부교수
<주관심분야: 대칭키 암호 알고리즘, 공개키 암호 알고리즘, 포렌식>