Hamming 값 분석을 통한 상관 전력분석 공격 성능 향상

이유석*, 송경원*, 김호원**, 김형남*
*부산대학교 전자전기공학과, **부산대학교 정보컴퓨터공학부

Enhancement of the Correlation Power Analysis Attack based on the Hamming Value Analysis

You-Seok Lee*, Kyung-Won Song*, Ho-Won Kim**, Hyoung-Nam Kim*
*School of Electrical Engineering, Pusan National University
*Dept. of Computer Science & Engineering, Pusan National University
* hnkim@pusan.ac.kr

Abstract: 부채널 공격은 암호화 과정 동안 발생하는 물리적 누설 정보를 분석하여 암호화에 사용된 비밀키를 알아내는 방법이다. 여러 부채널 공격 중에서 전력소모량의 상관 특성을 이용한 CPA (Correlation Power Analysis) 기법은 공격의 우수성 때문에 많은 연구가 수행되었다. 본 논문에서는 CPA 공격기법의 성능을 향상시키기 위해 통계적 특성치를 다변화하는 방안에 대해서 제안한다. 모의실험을 통하여 제안된 기법이 기존 부채널 공격의 효율성을 향상시킴을 보인다.

Keywords: Correlation Power Analysis, CPA, side channel attacks, Hamming weight.

Ⅰ. 서론

정보의 보호에 대한 관심이 크게 증가하면서 정보 보안을 위한 알고리즘 및 공격에 관한 다양한 연구가 지속적으로 진행되고 있다. 암호화 알고리즘이 구현된 하드웨어는 암호화 동작 시에 전력소모나 전자기장과 같은 물리적 정보들을 누설하게 되며 이를 이용하여 암호화 장치의 정상적인 동작을 방해하거나 비밀키등의 중요정보를 추출하는 행위인 부채널 공격 (Side Channel Attack)은 최근 보안의 큰 위협이 되고 있다.

여러 부채널 공격기법 중에서 전력소모 분석을 통한 공격을 수행하는 CPA (Correlation Power Analysis) [1]는 측정된 전력 소모량과 암호 알고리즘에 의한 특정 위치의 수행 결과값의 Hamming Weight 또는 Hamming Distance의 상관관계를 구하여 비밀키를 추정하는 방법으로, 최근 CPA에 기반한 다양한 연구가 수행되고 있다. 그러나 CPA의 경우 상관도에 이용되는 Hamming 값의 분포가 균일하지 않기 때문에 발생 빈도가 낮은 값에 대한 영향을 적용하기 위해서는 공격에 이용되는 부채널 신호의 수가 어느 정도 유지되어야 하는 단점이 있다. 따라서, 본 논문에는 Hamming 값 계산의 기준이 되는 bit들을 분할하여 상관 계수를 다변화 함으로써 CPA 공격기법의 성능을 향상시킬 수 있는 방법을 제안한다.

This work was supported by the Korea Science and Engineering Foundation (KOSEF) grant funded by the Korea government (MEST) (No. R01-2008-000-20987-0-(2008)).

Ⅱ. Correlation Power Analysis

상관 전력분석 기법인 CPA는 비밀키를 추정하기 위하여 측정된 신호와 암호화 연산 시 얻어지는 특정 위치의 결과값 사이의 상관계수를 이용한다. 이러한 결과값은 주로 Hamming Weight나 Hamming Distance가 사용되는데 Hamming Weight는 결과 bit 에서 ‘1’의 수에 의해 결정되며 Hamming Distance는 이전 값과 현재 bit 값 중에서 다른 값을 나타내는 bit의 수를 뜻한다. Hamming 값과 측정된 부채널 신호를 각각 H 와 W 라고 하면 상관계수 $\rho_{H,W}$ 는 다음과 같이 구해진다.

$$\rho_{H,W} = \frac{COV(H,W)}{\sigma_H \sigma_W} = \frac{E[HW] - E[H]E[W]}{\sigma_H \sigma_W}, \quad (1)$$

여기서 σ_H 와 σ_W 는 각각 Hamming 값과 부채널 신호의 표준편차를 나타낸다[1], [2]. 실제 공격에서 상관계수를 이용하여 키를 찾기 위해서는 모든 가능한 키 조합에 의한 상관계수를 구해야 하며 이때의 상관 계수 r 은 다음과 같이 나타낼 수 있다.

$$r_{i,j} = \frac{\sum_{d=1}^{N}(H_{d,i} - \overline{H_i})(W_{d,i} - \overline{W_i})}{\sqrt{\sum_{d=1}^{N}(H_{d,i} - \overline{H_i})^2 \sum_{d=1}^{N}(W_{d,i} - \overline{W_i})^2}}, \quad (2)$$

여기서 N은 공격에 이용된 부채널 신호의 수이며 j 와 i 는 각각 샘플 인덱스와 테스트된 키를 나타낸다.

CPA 공격기법은 하나의 특정 bit를 대상으로 공격

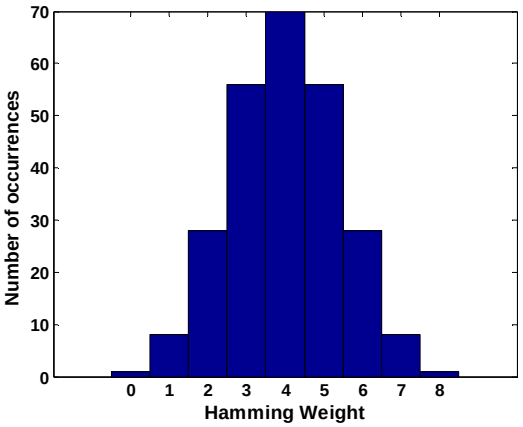

그림 1. Hamming Weight 의 히스토그램.

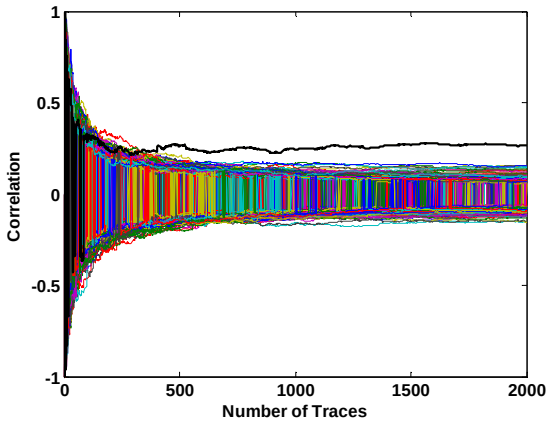

그림 2. 첫 번째 서브키를 찾기 위한 상관 계수 결과값.

하는 DPA와는 달리 Hamming Weight 또는 Hamming Distance를 이용하기 때문에 모든 bit의 영향을 고려한 공격을 수행하므로 DPA보다 나은 성능을 가지고 있다. 그러나 bit의 분포 특성상 Hamming 값들이 균일하게 분포하지 않기 때문에 공격에 이용되는 신호들의 수를 일정수준 이상 유지해야 비밀키를 정확하게 추정할 수 있다. 따라서 본 논문에서는 이러한 CPA 공격의 단점을 극복하기 위한 방안을 제시한다.

Ⅲ. 제안하는 부채널 공격 기법

CPA 의 단점을 설명하기 위하여 한가지 예를 제시한다. 공격에 이용할 수 있는 출력 bit 는 8 개로 가정하고 Hamming Weight 를 이용하여 CPA 공격을 수행한다고 가정하자. 이때 Hamming Weight 가 가지는 최대값은 8, 그리고 최소값은 0 이 된다. 가능한 모든 값을 히스토그램을 이용하여 나타내보면 그림 1 에 제시하였다. 각각의 Hamming Weight 값이 나타날 확률을 계산하면 다음과 같다.

$$\begin{aligned} &P[HW=0]=P[HW=8]=1/256 \\ &P[HW=1]=P[HW=7]=8/256=1/32 \\ &P[HW=2]=P[HW=6]=28/256=7/64 \\ &P[HW=3]=P[HW=5]=56/256=7/32 \\ &P[HW=4]=70/256=35/128 \end{aligned}, \quad (3)$$

식 (3)에서 보듯이 대부분의 Hamming Weight 값은 2 와 6 사이의 값을 가지게 된다. 만약 정확한 공격을 위해서 적어도 모든 경우의 Hamming Weight 값이 10 번 이상 적용되어야 한다고 가정하면 적어도 2560 번 이상의 공격이 수행되어야 함을 뜻한다. 이러한 점은 CPA 공격 기법의 성능을 저하시키는 요인이 되므로 이를 극복하기 위한 방안을 제시한다.

Hamming Weight 의 발생 빈도를 살펴보면 ‘ 4’ 값이 가장 높은 것을 알 수 있다. 따라서 8bit 를 각각 4bit 씩 분할하게 되면 분할된 영역에서 계산된 Hamming Weight 는 최대값과 최소값으로 각각 0 과 4 를 가지게 되며 이전의 경우와는 달리 그 발생빈도가 상당히 높음을 알 수 있다. 분할된 bit 의 Hamming Weight 값의 확률은 식 (4) 와 같다.

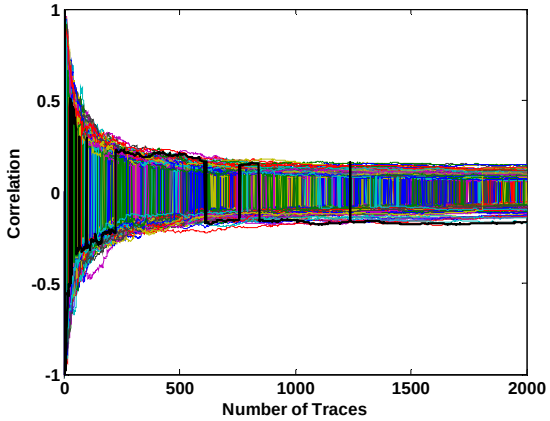

그림 3. 16 번째 서브키를 찾기 위한 상관 계수 결과값.

$$\begin{aligned} &P[HW=0]=P[HW=4]=1/16 \\ &P[HW=1]=P[HW=3]=4/16=1/4 \\ &P[HW=2]=6/16=3/4 \end{aligned}, \quad (4)$$

위와 같이 Hamming Weight 의 계산에 이용되는 bit 를 분할하여 각각의 값을 계산하여 적용하게 되면 적어도 10 번 이상의 Hamming Weight 값이 적용되어야 한다고 하더라도 160 번의 공격만 수행되면 되므로 보다 적은 수의 부채널 신호로 암호화에 사용된 키를 찾을 수 있다.

Ⅳ. 모의 실험

제안된 공격기법의 성능평가를 위하여 모의실험을 수행하였다. 무선 센서 네트워크 장치인 Telos 모듈을 성능평가를 위한 모듈로 사용하였으며 부채널 공격기법의 성능을 키를 찾기 위한 최소의 파형 수에 근거하여 평가하였다. 부채널 신호는 200 MHz 샘플링으로 2,000 개를 측정하여 실험하였다.

실험에서 사용된 암호알고리즘은 AES (Advanced Encryption Standard)이다[3]. AES 의 키는 128 bit 이며 16 개의 서브키 단위 (1byte)로 계산된다. 각각의 서브키를 추정하기 위한 공격시 계산되는 Hamming Weight 의 최소값과 최대값은 각각 0 과

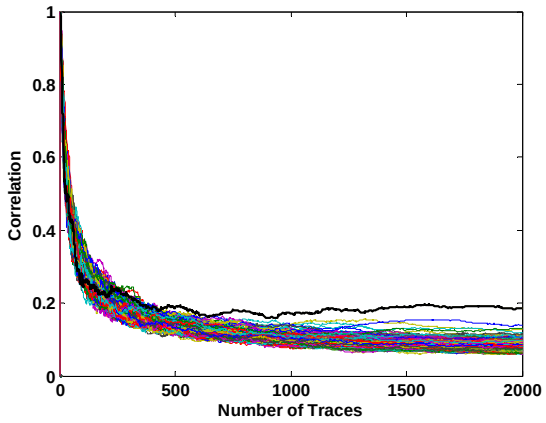

그림 4. 제안된 기법을 적용하여 계산된 첫 번째 키에 해당하는 상관계수 결과값.

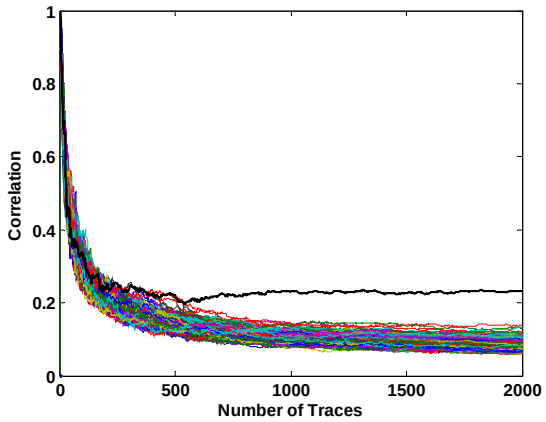

그림 5. 제안된 기법을 적용하여 계산된 첫 번째 키에 해당하는 상관계수 결과값.

표 1. 키를 얻기 위한 최소 파형 수

서브키	CPA 공격기법	제안된 공격기법
1 키	338	651
16 키	Fail	542

8 이며 SBOX 출력 값을 기준으로 공격을 수행하였다.

그림 2 는 기존의 CPA 공격기법에 근간하여 첫 번째 서브키를 찾기 위해 1~2000 개까지 부채널 신호가 증가할 때마다 계산된 상관계수를 나타낸다. 굵게 표시 된 선은 실제 암호화에 사용된 키가 추정되었을 때 계산된 상관 계수 값의 변화를 나타낸다. 그림에서 보듯이 계산에 이용된 부채널 신호가 증가할수록 다른 추정치에 의한 상관계수 값은 0 에 가깝게 수렴하지만 실제 사용된 키에 해당하는 추정치에 의한 상관계수 값은 부채널 신호의 수를 증가시키더라도 0.2 이상의 값을 유지하는 것을 알 수 있다. 이때 실제 키에 해당하는 추정치에 의한 상관계수 값은 부채널 신호 수가 338 이상일 때부터 가장 큰 값을 유지하므로 해당 서브키를 찾기 위한 부채널 수의 최소값은 338 이 된다. 16 번째 서브키를 찾기 위해 계산된 상관계수 값은 그림 3 에 나타내었다. 그림에서 보듯이 어떠한 추정치도 일정한 값을 유지하지 못함을 알 수 있으며 이는 기존의 CPA 를 이용한 공격기법으로 키를 찾지 못함을 뜻한다. 비록 첫 번째 서브키를 적은 수의 부채널 신호를 이용하여 추정하였다 하더라도 단 하나의 서브키 추정에 실패한다는 것은 전체 128bit 의 키를 알아낼 수 없다는 것을 뜻하기 때문에 CPA 공격기법 만으로는 AES 알고리즘에 사용된 키를 찾을 수 없다는 것을 알 수 있다.

그림 4 와 그림 5 는 제안된 방법을 이용하여 첫 번째와 16 번째의 서브키를 찾기 위해 CPA 공격을 수행한 결과를 각각 나타낸 것이다. 그림에서 보듯이 첫 번째 서브키는 651 개의 부채널 신호로, 그리고 16 번째 키는 542 개의 부채널 신호로 정확하게 추정 가능함을 알 수 있다. 키를 얻기 위한 최소 파형수를 표 1 에 정리하였다. 기존의 공격기법의 결과와 비교해보면 첫 번째 서브키의 경우 공격의 성능이 저하된 것을 알 수 있는데, 이는 Hamming Weight 를 분할 하여 적용할 경우 값의 범위가 0~8 에서 0~4 로 줄어들어 각각의 Weight 에 대한 효과가 어느 정도 감소되기 때문에 나타나는 현상이다. 그러나 16 번째의 경우를 보면 기본의 CPA 공격으로 찾을 수 없는 서브키를 542 개의 부채널 신호만을 이용하여 찾을 수 있으며 이는 전체 128bit 키를 찾을 수 있다는 것을 뜻한다. 결론적으로 제안된 기법은 기존의 공격기법 성능을 전체적으로 향상 시킬 수 있음을 알 수 있다.

V. 결론

본 논문에서는 상관관계 분석을 이용한 CPA 공격기법의성능을 향상시키기 위하여 공격에 이용되는 Hamming 값을 분할하여 적용하는 방법을 제안하였다. 제안된 방법을 적용함으로써 기존의 방법으로 찾지 못했던 서브키를 모두 찾아 냄으로써 보다 안정적인 공격을 수행할 수 있었다. 제안된 기법을 근간으로 스마트 카드나 다른 보안장비의 부채널 공격 취약점을 분석하여 향후 물리적 공격에 대한 대비책을 마련하는데 크게 도움을 줄 수 있을 것이다.

참고문헌

[1] E. Brier, C. Clavier, F. Olivier, " Correlation Power Analysis with a Leakage Model," in *Proceedings of CHES 2004*, LNCS 3156, pp. 16-29, Springer-Verlag, 2004.

[2] Alberto leon-Garcia, *Probability and Random Processes for electrical Engineering*, 2nd ed. Reading, MA: Addison-Wesley Publishing Company, Inc., 1994.

[3] National Institute of Standards and Technology (NIST). FIPS-197: Advanced Encryption Standard, November 2001.