신호의 표준편차를 이용한 부채널 공격 성능 향상

이유석*, 김용희*, 김형남*
*부산대학교 전자전기공학과

Performance Improvement of Side Channel Attacks using standard deviation of signals

You-Seok Lee*, Yong-Hee Kim*, Hyoung-Nam Kim*
*Dept. Electronics and Electrical Engineering, Pusan National University
* hnkim@pusan.ac.kr

Abstract: 강력한 부채널 공격기법 중의 하나인 차분전력분석(DPA) 기법은 암호화가 수행되는 동안 측정된 전력 소모량의 통계적 특성의 차를 이용하여 비밀키를 찾아낸다. DPA 를 이용한 공격을 효율적으로 수행하기 위해서는 측정된 신호의 동기가 정확히 일치해야 한다. 신호들 사이의 동기가 맞지 않으면 차분 공격 시 이용되는 평균에 의해 각 신호의 피크(Peak) 성분이 서로 상쇄되어 공격의 성능이 크게 저하된다. 이러한 동기문제를 해결하기 위해 에너지 신호기반 공격기법(Energy-based DPA)이 제안되었다. 그러나 이 방법은 신호의 불분명한 경계특성으로 인해 효과적인 부채널 공격을 수행하는데 어려움이 있다. 따라서 본 논문에서는 측정된 부채널 신호의 표준편차를 이용하여 에너지 신호 기반 공격기법에 존재하는 피크신호 분할의 모호성을 제거하여 부채널 공격 성능을 향상시키는 방법을 제안한다. 모의실험을 통하여 제안된 기법이 기존 부채널 공격의 효율성을 크게 증가시킴을 보인다.

Keywords: DPA, energy-based DPA, side channel attacks, standard deviation.

Ⅰ. 서론

보안기술을 필요로 하는 스마트 카드, 전자서명, 전자상거래 등의 각종 서비스가 보편화 되면서 개인 신상정보 및 기타 중요 정보의 보안에 관한 다양한 연구가 지속적으로 진행되고 있다. 정보 보안을 위한 암호화 알고리즘은 주로 반도체 칩에 구현되게 되는데 그 특성상 암호화 동작 시에 전력소모나 전자기장과 같은 여러 정보들을 누설하게 된다. 이러한 정보들을 부채널 정보라고 하며 이를 이용하여 암호화 장치의 정상적인 동작을 방해하거나 비밀키등의 중요정보를 추출하는 행위를 부채널 공격 (Side Channel Attack)이라 한다 [1].

현재까지 연구된 부채널 공격으로는 시차분석(TA: Timing Attack)[2], 전력분석(PA: Power Analysis)[3], 전자파 분석(EMA: ElectroMagnetic emission Analysis)[4]등의 분석으로 크게 나누어진다. 전력분석 기법은 다시 SPA(Simple Power Analysis)[3], DPA(Differential Power Analysis)[5], CPA (Correlation Power Analysis)[6]로 분류되는데 그 중에서 차분전력분석 공격기법인 DPA는 암호화 과정이 수행되는 동안 측정된 전력 소모량의 통계적 특성의 차를 이용하여 비밀키를 추정하는데 이러한 기법은 보안을 위협하는 강력한 요소로 작용하고 있다. 그러나 차분전력분석기법을 이용하여 부채널 공격을 수행하기 위해서는 측정된 신호의 동기가 정확히 일치해야 한다는 조건이 따른다. 만약 신호들 사이의 동기가 맞지 않으면 차분 공격 시 이용되는 평균에 의해서 각 신호들의 피크(Peak) 성분이 서로 상쇄되어 공격의 성능이 크게 저하된다. 이러한 동기문제를 해결하기 위해 에너지 신호 기반 공격기법(Energy-based DPA)[7]이 제안되었다. 이 기법은 신호에 존재하는 피크를 각각의 영역으로 분할한 후 분할된 피크의 에너지를 계산하여 얻어진 에너지 신호를 부채널 공격에 이용한다. 그러나 측정된 부채널 신호에 존재하는 피크의 불분명한 경계특성으로 인해 영역 분할의 모호성이 존재하여 효과적인 부채널 공격을 수행하는데 어려움이 따른다. 따라서 본 논문에서는 측정된 부채널 신호의 표준편차를 이용하여 에너지 신호 기반 공격기법에서 발생하는 피크신호 분할의 모호성을 제거함으로써 부채널 공격 성능을 향상시키는 기법을 제안한다.

본 연구는 BK21 사업단의 연구비 지원에 의해 연구되었음.

Ⅱ. 부채널 공격기법

1. 차분전력분석 공격기법

그림 1은 Paul Kocher 등에 의해서 제안된 차분전력분석(DPA) 기법의 블록도를 나타낸 것이다. 이 기법은 디지털 신호의 출력 비트(bit)가 0 또는 1로 표현될 때 소모되는 전력에 차이가 있다는 점을 기반으로 한다. DPA 기법을 이용하여 비밀키 K_s 를 얻기 위해서는 M 번의 암호화 과정 시 발생하는 전력신호를 측정하고 동시에 각각의 암호화에 사용된 평문(Plaintext) 또는 암호문(Ciphertext)을 저장한다. 이때 각각의 전력소

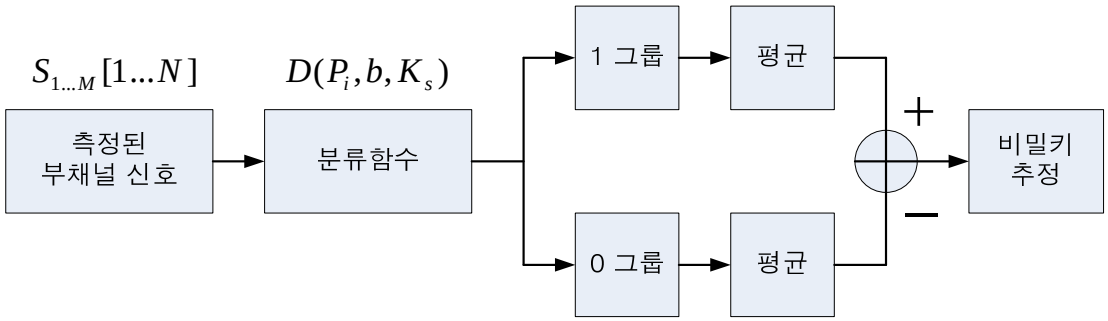

그림 1. 차분전력분석기법(DPA)의 블록도.

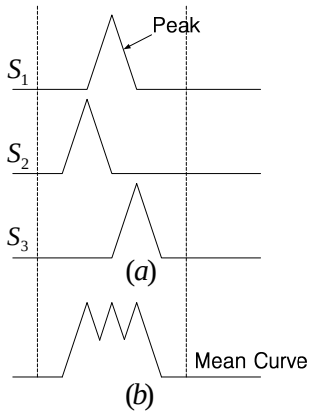

그림 2. (a)시간영역에서 측정된 동기가 틀어진 신호. (b) 동기가 틀어진 신호의 평균 곡선

모 신호는 N 개의 샘플로 구성되게 된다. 측정된 신호는 분류함수 $D(P_i,b,K_s)$ 에 의해서 0 또는 1의 그룹으로 나누어지는데 분류함수 결과값이 0 이면 0 그룹으로 1이면 1 그룹으로 각각 나누어진다. 분류함수에 의해 나누어진 각 그룹의 평균의 차이를 의미하는 차분신호 $\Delta_D(b)$ 는 평문 P_i 에 대한 소비 전력 신호를 $W(P_i)$ 라고 할 때 다음과 같이 구할 수 있다[5].

$$\Delta_D(b) = \frac{\sum_{i=1}^{M} D(P_i,b,K_s)W(P_i)}{\sum_{i=1}^{M} D(P_i,b,K_s)} - \frac{\sum_{i=1}^{M}(1-D(P_i,b,K_s))W(P_i)}{\sum_{i=1}^{M}(1-D(P_i,b,K_s))} \quad (1)$$

암호화 동작 중에 계산되는 비트들이 확률적으로 균일하게 분포하고 M 이 충분히 클 때 차분 신호 $\Delta_D(b)$ 는 추측된 비밀키가 틀리면 특정 피크가 나타나지 않게 되며, 옳으면 비트가 동작하는 특정 순간에서 큰 피크를 가지게 된다. 이렇게 나타난 피크들 중 가장 큰 값을 가질 경우의 K_s 값을 비밀키로 결정하게 된다.

2. 에너지 신호기반 공격기법.

앞서 설명한 것과 같이 차분전력분석기법은 분류함수에 의해 나누어진 각 신호들의 평균의 차를 이용하여 얻은 특정 순간에 나타나는 피크의 크기에 근간하여 비밀키를 추정하기 때문에 신호들의 동기가 매우 중요하다. 만약 측정된 신호들의 동기가 맞지 않으면 차분공격 시 이용되는 평균에 의해서 각 신호들의 피크성분이 서로 상쇄되어 그 크기가 달라지기 때문에 공격의 효율이 크게 떨어지게 된다. 이러한 차분공격 기법에서의 신호들 간의 비동기 문제를 해결하기 위하여 에너지 신호기반 공격기법(Energy-based DPA)[7]이 제안되었다.

시간영역에서 측정된 부채널 신호들 간의 동기는 평균 곡선(mean curve)을 이용하면 틀어진 정도를 쉽게 알 수 있다. 그림 2의 (a)와 같이 세 개의 부채널 신호가 측정되었다고 가정하자. 이 신호들의 평균으로 얻은 신호를 살펴보면 그림 2의 (b)와 같이 각 신호들에 존재하는 피크의 분포 범위를 쉽게 알 수 있는데 만약 이러한 피크의 분포 범위가 하나의 동일한 영역 안에 포함될 정도로 작으면 그 분할 영역 내에 존재하는 피크의 에너지는 피크의 위치에 상관없이 동일하다. 이러한 사실에 근간하여 에너지 신호기반 부채널 공격기법은 시간영역에서 측정된 부채널 신호를 적당한 크기의 영역으로 나누어 각각의 영역에서 신호의 에너지를 계산한 후 기존의 신호를 분할 영역의 개수만큼의 데이터를 가지는 에너지 신호로 변환하여 부채널 공격에 이용한다. 이러한 방법은 피크가 분할 영역 범위 내에 존재하여 적당한 영역으로 분할이 되기만 하면 되므로 신호들 사이의 동기문제를 효과적으로 해결할 수 있다.

Ⅲ. 제안하는 부채널 공격 기법

측정된 부채널 신호를 DPA 에 적용하기 위해서는 신호들 사이의 동기가 맞아야 한다. 그러나 일반적으로 암호화 동작을 정확하게 알 수 있는 트리거(trigger) 신호가 없을 뿐만 아니라 트리거 신호가 있다 하더라도 실제 암호화 동작 타이밍의 지터(jitter)에 의해 측정된 신호들간의 동기를 맞추기가 매우 어려우며 이러한 비동기 문제는 부채널 공격의 성능을 크게 저하시키는 요인이 된다[7][8]. 이러한 비동기 문제는 앞 절에서 설명한 에너지 신호기반 공격기법을 이용하여 어느 정도 해결할 수 있으나 실제 환경에서는 측정된 피크를 적당하게 분할하기 어렵다.

그림 3 은 센서노드 장치에서 암호화 과정이 수행되는 동안 측정한 100 개의 부채널 신호를 나타낸

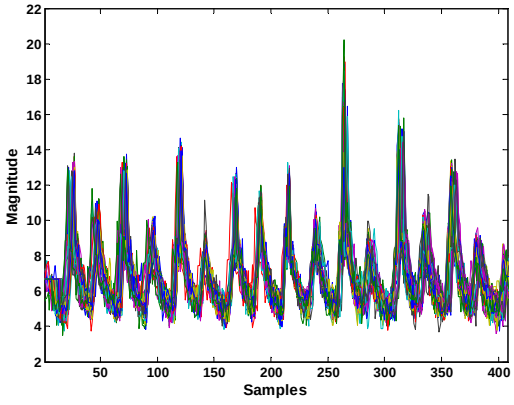

그림 3. 측정된 100 개의 부채널 신호.

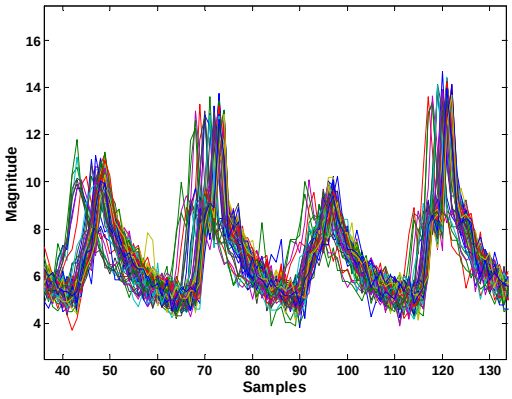

그림 4. 30~140 샘플구간에 해당하는 100 개의 부채널 신호.

것이며 그림 4 는 측정된 부채널 신호의 특정부분을 확대하여 나타낸 것이다. 그림에서 보듯이 실제 하드웨어에서 측정된 부채널 신호는 암호화 동작 타이밍의 지터가 크게 존재하여 피크를 적당한 영역으로 분할하기 쉽지 않으며 샘플링 정보를 이용하여 적당한 길이의 샘플을 기준으로 나눈다고 하여도 피크가 어떤 영역으로 분할되느냐에 따라서 에너지로 변환된 신호가 달라지게 된다. 즉 피크 신호의 시작과 끝을 분명하게 구분하기 어렵다. 이러한 피크 신호 분할의 모호성은 에너지 신호기반 부채널 공격기법의 성능을 열화 시키는 주된 요인으로 작용한다. 따라서, 본 논문에서는 측정된 부채널 신호의 표준편차를 문턱값으로 이용하여 신호에 존재하는 피크를 적당한 영역으로 쉽게 분할할 수 있도록 하여 에너지 신호기반 부채널 공격 기법의 성능을 향상시키는 방법을 제안한다.

우선 측정된 부채널 신호로부터 다음 식과 같이 각 샘플들 간의 표준편차를 구한다.

$$\mathrm{Std}[j]=\left(\frac{\sum_{k=1}^{M}\left|S_k[j]-\mu[j]\right|^2}{M}\right)^{1/2},\ j=1,\ldots,N\ . \quad (1)$$

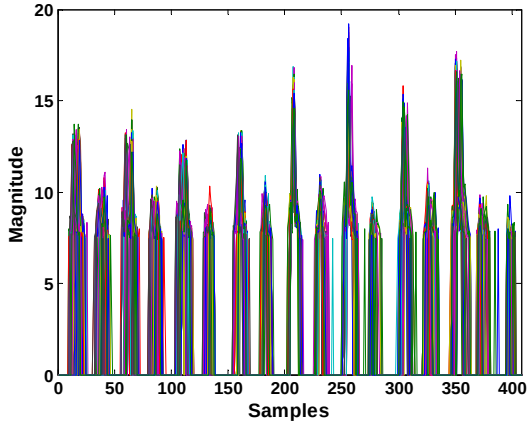

그림 5. 제안된 기법을 적용한 부채널 신호.

여기서 $S_k[j]$ 는 측정된 k 번째 부채널 신호이며 $\mu[j]$는 M 개 신호들의 j 번째 샘플들 간의 평균이다. 그런 다음 N 개의 샘플을 가지는 표준편차들의 평균을 구하여 문턱값 T 를 설정한다. 얻어진 문턱값보다 낮은 에너지를 가지는 신호를 잡음으로 간주하고 0 으로 치환하여 새로운 부채널 신호 S_n 을 얻으며 그 식은 다음과 같다.

$$S_n[j]=\begin{cases}S_k[j] & S_k[j]\ge T\\ 0 & S_k[j]<T\end{cases}\quad j=1,\ldots,N\ . \quad (2)$$

식 (2)에서 보듯이 문턱값보다 낮은 에너지를 가지는 신호성분은 모두 제거되어 각 피크의 구분이 원활해지므로 에너지 신호기반 공격기법에 존재하는 피크 영역 분할의 모호성이 제거되어 효율적인 공격을 수행할 수 있게 된다.

Ⅳ. 모의 실험

제안된 부채널 공격 향상기법의 성능평가를 위하여 모의실험을 수행하였다. 성능평가를 위한 모듈로는 무선 센서 네트워크 장치인 Telos 모듈을 사용하였으며 에너지 신호기반 부채널 공격기법과 제안된 부채널 공격기법의 성능을 키를 찾기 위한 최소의 파형 수에 근거하여 평가하였다. 부채널 신호는 200 MHz 샘플링으로 4,000 개를 측정하여 실험하였다. 실험에 사용된 모듈이 8 MHz 클럭으로 동작하기 때문에 하나의 피크는 25 샘플에 걸쳐 나타나게 되나 실험장치들의 부 정확성으로 인해 24 개의 샘플에 걸쳐 나타남을 확인하였다.

실험에 사용된 암호알고리즘은 AES(Advanced Encryption Standard)이다[9]. AES 는 비밀키 결정을 위해 사용 가능한 비트가 모두 8 개이므로 키 결정의 정확도를 향상시키기 위하여 각각의 비트에 의해 구해진 출력 파형의 합을 구한 후, 이때 가장 큰 피크를 가지는 키를 최종 비밀키로 결정하였다.

그림 5 는 제안된 기법으로 구한 문턱값을 실제 측정된 신호에 적용한 파형을 나타낸 것이다. 그림에서

표 1. 키를 얻기 위한 최소 파형 수

	에너지 신호기반 공격기법	제안된 공격기법
1 키	750	400
2 키	400	150
9 키	1900	450

보듯이 문턱값을 이용한 전처리 과정에서 낮은 에너지를 가지는 신호가 모두 제거되어 피크 영역 분할의 모호성이 제거됨을 알 수 있다. 표 1 은 에너지 신호기반 부채널 공격 기법과 제안된 공격기법의 성능을 3 개의 키에 대하여 비교한 것이다. 표 안의 숫자는 키를 찾기 위해 필요한 최소 파형 수이다. 표 1 에서 보듯이 비록 에너지 신호기반 공격기법으로 첫 번째와 두 번째 키를 각각 750 개와 400 개의 파형으로 찾을 수 있었으나 제안된 기법을 이용하면 두 번째 키의 경우 62% 이상의 효율을 증가시켜 각각 400 개와 150 개의 부채널 신호만으로도 키를 찾는 것이 가능해진다. 아홉 번째 키의 경우에는 신호의 동기가 크게 틀어져 키를 찾기 위해서는 1900 개의 부채널 신호가 필요함에도 불구하고 제안된 기법을 이용하여 신호에 존재하는 피크 영역 분할의 모호성을 제거하게 되면 76% 이상 효율이 증가되어 500 개 이하의 부채널 신호 만으로도 키를 추출하는 것이 가능해 진다.

V. 결론

본 논문에서는 에너지 신호기반 부채널 공격기법의 성능을 향상시키기 위하여 측정된 부채널 신호의 표준편차를 문턱값으로 이용하는 방법을 제안하였다. 제안된 방법을 적용함으로써 측정된 신호에 존재하는 피크 영역 분할의 모호성을 효과적으로 제거하여 기존의 부채널 공격기법의 성능을 비밀키를 찾기 위해 필요한 최소 파형 수에 근간하여 최대 76% 이상 향상 시킬 수 있었다. 제안된 기법은 비록 키를 찾기 위한 방법이나 앞으로 스마트 카드나 다른 보안장비 등에 적용하여 부채널 공격에 대한 취약점을 분석하여 향후 물리적 공격에 대한 대비책을 마련하는데 크게 도움을 줄 수 있을 것이다.

참고문헌

[1] S. Mangard, E. Oswald, and T. Popp, Power Analysis Attacks: Revealing the Secrets of Smart Cards, 2007 Springer Science+ Business Media, LLC.

[2] Paul C. Kocher, “ Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems,” *Advances in Cryptology-Crypto*. 1996, LNCS 1109, pp 104-113.

[3] P. Kocher, J. Jaffe, and B. Jun, “ Introduction to differential power analysis and related attacks,” 1998, White Paper, Cryptography Research.

[4] K. Gandolfi, C. Mourtel, and F. Olivier, “ Electromagnetic Analysis: Concrete Results,” *in Proceedings of CHES 2001*, LNCS 2162, pp. 255-265, Springer-Verlag.

[5] P. Kocher, J. Jaffe, and B. Jun, “ Differential Power Analysis,” *in Proceedings of CRYPTO 1999*, LNCS 1666, pp. 388-397, Springer-Verlag, 1999.

[6] E. Brier, C. Clavier, and F. Olivier, “ Correlation power analysis with a leakage model,” *in Proceedings of CHES 2004*, LNCS 3156, pp. 16-29, 2004.

[7] T-H. Le, J. Clédière, C. Servière, J-L. Lacoume, “ Efficient Solution for Misalignment of Signal in Side Channel Analysis,” *in Proceedings of ICASSP 2007*. vol. 2, pp. II-257-II-260, April 2007.

[8] N. Homma, S, Nagahima, Y. Imai, T. Aoki, A. Satoh, “ High-Resolution Side-Channel Attack Using Phase-Based Waveform Matching,” *in Proceedings of CHES 2006*, LNCS 4249, pp. 187-200, 2006

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