전력을 헤밍웨이트로 변환하여 2차 전력 분석 성능을 향상시키는 방법

최완승, 한동국
국민대학교 수학과
e-mail:{karness, christa}@kookmin.ac.kr

A Method to Improve the Second-Order Power Analysis by Converting Power to Hamming Weight

Wan-Seung Choi, Dong-Guk Han
Dept. of Mathematics, Kookmin University

요 약

부채널 분석은 암호 기기가 노출하는 물리적 정보를 이용하여 키를 찾아내는 분석 기법이다. 이러한 부채널 분석의 대응 방안으로 마스킹, 셔플링과 같은 기술이 연구되어지고 있다. 그러나 이러한 대응 기법들 역시 2차 전력 분석에 취약점을 가지고 있다. 이 때, 일반적인 2차 전력 분석 기법의 이론적 분석 성능은 잡음의 영향을 받는 실제 분석 환경에서 현저하게 줄어드는 것을 알 수 있다. 본 논문에서는 2차 전력 분석의 분석 성능을 향상시키기 위해 기존의 탐지된 전력 정보를 직접 활용하지 않고, 전력 소모량을 헤밍웨이트로 대응시켜 이론적 계산 값과의 근사치를 높이는 방법을 제안한다. 실험 결과 일반적인 2차 전력 분석 기법에 비해 약 8%의 성능 향상을 보였다. 또한 전력 소모량과 중간 값 사이의 상관도를 높이기 위해 변환된 헤밍웨이트를 편중시켜 분석한 결과, 일반적인 2차 전력 분석 기법에 비해 10~20%의 분석 성능 향상을 가져왔다.

1. 서론

부채널 분석(Side Channel Attack, SCA)은 1996년 Paul Kocher[1]가 최초로 제안한 분석 기법으로, 암호 기기가 암호 알고리즘을 수행 시 노출하는 물리적 정보를 이용하여 키를 찾는 분석 기법이다. 그 중, 차분 전력 분석(Differential Power Analysis, DPA)은 가장 잘 알려진 기법이다. 상관 전력 분석(Correlation Power Analysis, CPA)은 차분 전력 분석 기법의 발달한 형태로, 수집한 전력 소모량과 추측한 키를 이용한 중간 값과의 상관계수를 계산하여 올바른 키를 얻는 분석 기법이다[2].

이러한 분석 기법에 취약한 암호 기기의 안전성을 높이기 위해 마스킹, 셔플링과 같은 대응 기법이 연구되었다. 마스킹 기법은 랜덤한 마스크 값을 생성하여, 중간 값의 키에 대한 정보를 감추는 기법이다[5]. 마스킹 기법은 사용하는 마스크 값의 개수에 따라 그 차수가 정해지는데, n개의 마스크 값을 사용하는 마스킹 기법을 n차 마스킹 기법이라 한다. n차 마스킹 기법을 적용한 암호 알고리즘은 n차 이하의 전력 분석에 안전하지만, $(n+1)$차 전력 분석에 대해 취약점을 가지고 있다. 높은 차수의 마스킹 기법을 적용할수록 분석에 필요한 전력 파형의 수가 증가되므로 분석의 복잡도를 증가시킬 수 있지만, 높은 차수의 마스킹 기법을 적용한 암호 알고리즘의 속도는 현저히 떨어진다. 따라서 암호 알고리즘의 효율성을 고려했을 때 1차 마스킹 기법을 사용하는 것이 일반적이다.

1차 대응 기법을 적용한 암호 알고리즘은 2차 전력 분석에 취약점을 가지고 있다. 2차 전력 분석 기법의 이론적 분석 성능은 전력 소모량에 포함된 잡음의 영향을 받는 실제 분석 환경에서 현저하게 줄어드는 것을 알 수 있다.

본 논문에서는 잡음의 영향을 최소화하기 위해 전력 소모량을 헤밍웨이트로 대응시키는 전력 변환 방법을 제안한다. 전력 변환 방법을 적용한 결과 일반적인 기법에 비해 8%의 성능 향상을 보였다. 또한 변환된 헤밍웨이트와 중간 값 사이의 상관도를 높이기 위해 헤밍웨이트 값을 0, 8 값으로 편중시켜 분석하였다. 분석 결과 일반적인 기법에 비해 10~20%의 성능 향상을 보였다.

2. 2차 전력 분석

2차 전력 분석은 두 지점의 전력 소모량을 이용해 키를 찾는 분석 기법이다. 1차 마스킹 기법이 적용된 암호 알고리즘은 모든 중간 값에 랜덤한 마스크 값이 적용되었기 때문에 1차 전력 분석으로 키를 찾아내는 것이 불가능하다. 따라서 동일한 마스크 값이 적용된 두 지점의 전력 소모량에 대해 마스크 값을 상쇄하는 작업이 필요하다. 동일한 마스크 값이 적용된 두 지점의 중간 값을 $X\oplus m$, $Y\oplus m$라 할 때, 두 값을 하면 마스크 값이 상쇄된 $(X\oplus m)\oplus(Y\oplus m)=X\oplus Y$ 을 얻을 수 있다. 따라서 두 지점에 대한 전력 소모량 $C(X\oplus m)$, $C(Y\oplus m)$에 대해 적절한 전처리 과정을 적용하여 마스크 값을 상쇄하면 전력

분석 기법을 통해 키를 찾아낼 수 있다.

<표 1> 전처리 함수의 결과와 실제 중간 값 사이의 상관도

$HW((X\oplus m)\oplus(Y\oplus m))$	상관계수
$HW(X\oplus m)\cdot HW(Y\oplus m)$	-0.09
$\lvert HW(X\oplus m)-HW(Y\oplus m)\rvert$	0.24
$(HW(X\oplus m)+HW(Y\oplus m))^2$	-0.04
$HW(X\oplus m)+HW(Y\oplus m)$	0.00
$HW(X\oplus m)-HW(Y\oplus m)$	0.00
X, Y: 8-bits 입력 값, m: 랜덤한 마스크 값	

<표 1>은 $HW(X\oplus m)$, $HW(Y\oplus m)$에 대해 전처리 한 결과와 $HW((X\oplus m)\oplus(Y\oplus m))$와의 상관계수를 나타낸다. $|HW(X\oplus m)-HW(Y\oplus m)|$의 상관계수가 0.24로 가장 상관도가 높은 것을 알 수 있다. 전력 소모량과 헤밍웨이트의 관계[1]에 의해 $HW(X\oplus m)$, $HW(Y\oplus m)$의 전력 소모량 $C(X\oplus m)$, $C(Y\oplus m)$에 대해 다음의 수식이 성립한다.

$$HW((X\oplus m)\oplus(Y\oplus m)) \approx |C(X\oplus m)-C(Y\oplus m)| \quad ①$$

수식 ①을 통해 1차 마스킹 기법이 적용된 암호 알고리즘의 중간 값에 대한 전력 소모량과 추측한 키를 이용한 중간 값과의 상관계수를 구할 수 있다.

3. 전력을 헤밍웨이트로 변환한 2차 전력 분석

본 논문에서는 마스킹 기법이 적용된 암호알고리즘 AES(Advanced Encryption Standard)의 1라운드 S-box 출력 부분을 분석 지점으로 선택하였다. 수집된 전력 소모량을 헤밍웨이트로 변환하는 전력 변환 방법을 적용하여 분석 성능을 비교한다. 또한 변환된 헤밍웨이트 값을 편중시키는 방법에 따라 분석 성능을 비교한다.

3.1 전력 변환 방법

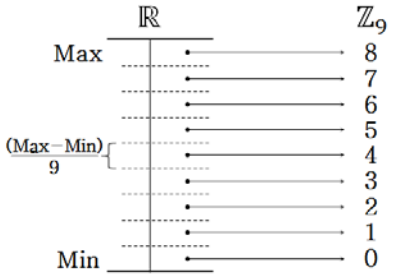
전력 분석 방법은 전력 소모량의 정의구간 R을 헤밍웨이트의 정의구간 Z_9로 대응시키는 방법이다.

일반적인 2차 전력 분석은 위의 수식 ①을 가정한다. 이 때, 수식 ①의 전력 소모량 $C(X\oplus m)$, $C(Y\oplus m)$이 잡음을 포함하기 때문에 실제 환경에서 이론적 분석 성능을 얻을 수 없다. 따라서 수식 ②와 같이 변환하는 방법을 이용하여 잡음의 영향을 최소화한다.

$$HW((X\oplus m)\oplus(Y\oplus m)) \approx |HW(X\oplus m)-HW(Y\oplus m)| \quad ②$$

3.1.1 균등 변환

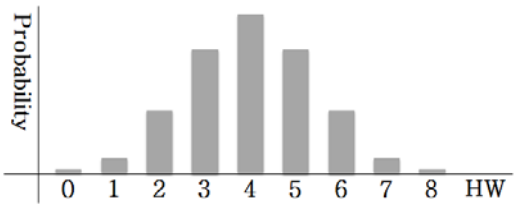
균등 변환은 측정된 전력 소모량이 중간 값의 헤밍웨이트에 비례한다고 가정한다. 분석 지점의 최대·최소 전력 소모량을 구해 그 사이를 동일한 비율로 9개의 구간으로 분할한다. 분할된 9개의 구간을 (그림 1)과 같이 헤밍웨이트와 대응시킨다.



(그림 1) 전력 소모량에서 헤밍웨이트로의 변환

3.1.2 이항분포에 의한 변환

이항분포에 의한 변환은 계산된 중간 값이 균일하게 분포되어있다고 할 때 중간 값의 헤밍웨이트가 이항분포를 따르는 것을 가정한다. 따라서 중간 값의 헤밍웨이트의 분포는 다음과 같은 형태로 나타난다.



(그림 2) 중간 값에 대한 헤밍웨이트의 분포

전력 소모량을 헤밍웨이트로 변환하였을 때, (그림 2)의 분포를 따르도록 변환 기준을 설정한다. 설정한 변환 기준에 맞게 전력 소모량을 각각의 헤밍웨이트와 대응시킨다.

3.2 전력 편중을 이용한 분석

3.1에서 전력 소모량을 헤밍웨이트로 변환하는 방법에 대해 소개하였다. 이 때, $HW(X\oplus m)$, $HW(Y\oplus m)$의 값이 4에 가까워질수록 양변 간의 상관도가 낮아짐을 알 수 있다. 예를 들어, $X\oplus m=(11110000)_2$, $Y\oplus m=(00001111)_2$ 일 때, 양변의 값은 각각 8, 0으로 서로 상이하므로 분석 시 상관도를 낮추는 원인이 된다.

본 실험에서는 S-box 출력 $S[p_i\oplus k_i]\oplus m$, $S[p_j\oplus k_j]\oplus m$에 대해 $HW(S[p_i\oplus k_i]\oplus m)$, $HW(S[p_j\oplus k_j]\oplus m)$의 값을 0과 8에 가까운 값에 편중시키며, 수식 ①, ②를 이용하여 분석을 수행한다. 편중시키는 방법은 사용하는 헤밍웨이트 값에 따라 다음과 같이 세 가지로 구분한다.

1.) 사용하는 헤밍웨이트 값 : (0, 1, 7, 8)
2.) 사용하는 헤밍웨이트 값 : (0, 1, 2, 6, 7, 8)
3.) 사용하는 헤밍웨이트 값 : (0, 1, 2, 3, 5, 6 ,7, 8)

4. 실험 결과

MSP430 Chip Board에서 1차 마스킹 기법이 적용된 AES[8]에 대해 1라운드 S-box 부분을 500MS/s의

1) $C(x)=\epsilon HW(x)+\alpha$ (전력 소모량과 헤밍웨이트의 관계)
ϵ: 단위 헤밍웨이트의 전력 소모량, x: 입력 값, α: 잡음
$C(x)$: 입력 x에 대한 전력 소모량
$HW(x)$: 입력 x의 헤밍웨이트 값

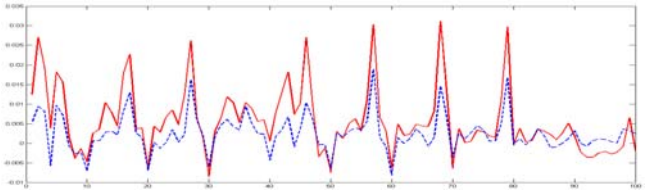
Sampling rate로 총 100,000개를 수집하였다. 첫 번째, 두 번째 S-box 출력 부분을 이용하여 분석을 수행하였으며, 먼저 일반적인 기법과 균등 변환, 이항분포에 의한 변환을 적용한 분석 결과를 비교한다. 그리고 이항분포에 의한 변환을 적용한 분석에 대해 헤밍웨이트를 편중시키는 기법 1, 2, 3을 각각 적용하여 분석 결과를 비교한다.

<표 2> 일반적인 기법과 전력 변환을 적용한 분석 결과

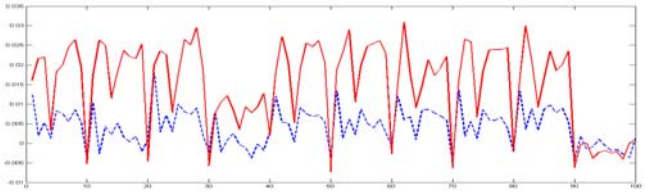
	옳은 키	오류 키	Ratio[2]
수식 ①	0.03113	0.01899	1.63928
수식 ② & (3.1.1)	0.03088	0.01802	1.71365
수식 ② & (3.1.2)	0.03357	0.01904	1.76313

<표 2>는 일반적인 기법과 전력 변환을 각각 적용한 분석결과로써 옳은 키와 오류 키의 상관계수를 나타낸다. 일반적인 기법과 균등 변환을 적용한 경우 옳은 키를 찾아내지 못하였지만, 이항분포에 의한 변환을 적용하였을 때, 옳은 키를 찾은 것을 확인하였다.

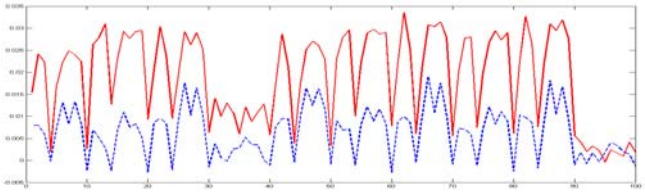
(그림 3, 4, 5)는 각 기법에 대한 분석 결과를 나타낸다. 그림의 가로축은 첫 번째, 두 번째 S-box 출력 부분을 포함한 10포인트의 추정구간에 대한 모든 조합[3]을 의미하며, 세로축은 각 조합에 대한 분석 결과인 상관계수를 의미한다. 옳은 키와 오류 키의 상관계수는 각각 빨간 직선과 파란 점선으로 표시하였다.



(그림 3) 일반적인 분석 결과



(그림 4) 균등 변환을 적용한 분석 결과



(그림 5) 이항분포에 의한 변환을 적용한 분석 결과

일반적인 기법과 균등 변환을 적용한 경우 옳은 키와 오류 키의 상관계수의 형태가 선명하게 구분되지 않지만, 이항분포에 의한 변환 기법을 적용하였을 때는 선명하게 구분됨을 확인할 수 있다.

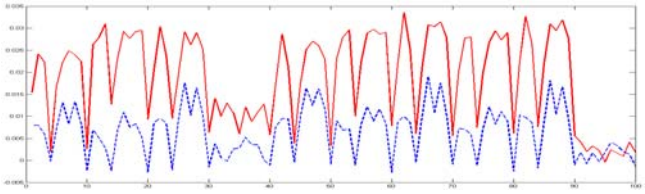
다음은 이항분포에 의한 변환 기법을 적용하고, 변환된 헤밍웨이트 값을 편중시켜 분석한 결과이다.

<표 3> 편중 방법에 따른 분석 결과

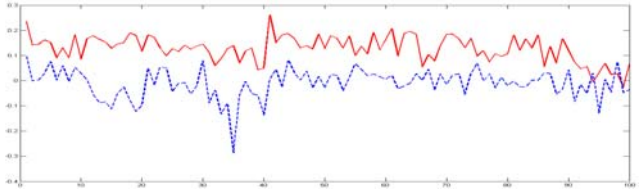
	옳은 키	오류 키	Ratio
(0-8)	0.03357	0.01904	1.76313
(0-1, 7-8)	0.26170	0.28690	0.91217
(0-2, 6-8)	0.11334	0.06290	1.80191
(0-3, 5-8)	0.04966	0.02549	1.94822

<표 3>은 일반적인 기법과 헤밍웨이트를 편중시켜 분석한 결과로써 옳은 키와 오류 키의 상관계수를 나타낸다. 편중 기법 2, 3을 적용하였을 때 Ratio가 일반적인 기법과 비교해 높은 것을 확인할 수 있다.

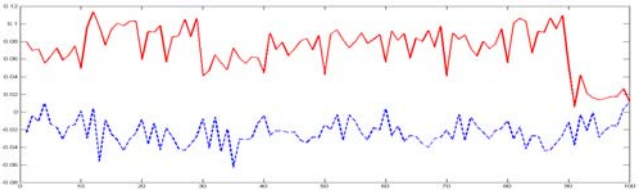
(그림 6, 7, 8, 9)는 각 기법에 대한 분석 결과를 나타낸다. 그림의 가로축은 첫 번째, 두 번째 S-box 출력 부분을 포함한 10포인트의 추정구간에 대한 모든 조합을 의미하며, 세로축은 각 조합에 대한 분석 결과인 상관계수를 의미한다. 옳은 키와 오류 키의 상관계수는 각각 빨간 직선과 파란 점선으로 표시하였다.



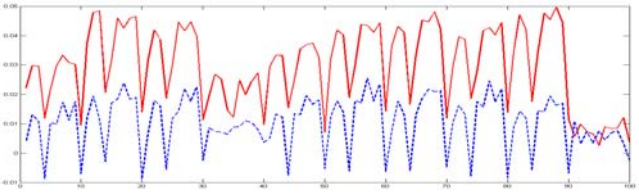
(그림 6) (0-8)의 헤밍웨이트를 사용한 분석 결과



(그림 7) (0-1, 7-8)의 헤밍웨이트를 사용한 분석 결과



(그림 8) (0-2, 6-8)의 헤밍웨이트를 사용한 분석 결과



(그림 9) (0-3, 5-8)의 헤밍웨이트를 사용한 분석 결과

2) (옳은 키의 최대 상관계수) / (오류 키의 최대 상관계수)
3) S-box 출력 위치에 대한 정확한 정보를 알 수 없기 때문에, 추정구간에 대한 모든 조합을 이용하여 분석을 수행한다.

편중 기법을 적용하지 않은 일반적인 기법과 편중 기법 1, 3을 적용한 경우 옳은 키와 오류 키의 상관계수의 형태가 선명하게 구분되지 않지만, 편중 기법 2를 적용하였을 때는 선명하게 구분됨을 확인할 수 있다.

5. 결론

본 논문에서는 전력 소모량에 포함된 잡음의 영향을 최소화하기 위해 전력 소모량을 헤밍웨이트로 변환하는 방법을 사용하였다. 전력 소모량을 헤밍웨이트로 변환하는 방법으로 균등 변환과 이항분포에 의한 변환을 사용하였다. 두 변환 기법 모두 일반적인 2차 상관 전력 분석 기법에 비해 좋은 분석 성능을 보였으며, 이항분포에 의한 변환을 적용하였을 때, 8%의 성능 향상을 보였다. 이항분포에 의한 변환 기법에 대해, 변환된 헤밍웨이트를 편중시켜 분석을 수행하였다. (0-1, 7-8)의 헤밍웨이트를 사용한 경우 분석이 되지 않았지만, (0-2, 6-8), (0-3, 5-8)의 헤밍웨이트를 사용한 경우 각각 2%, 10%의 성능이 추가적으로 향상되었다. 결과적으로 일반적인 2차 상관 전력 분석에 비해 10~20%의 성능 향상을 보였다. 옳은 키와 오류 키의 상관계수 형태를 살펴보았을 때, (0-3, 5-8)의 헤밍웨이트를 사용한 경우 보다 (0-2, 6-8)의 헤밍웨이트를 사용한 경우가 더욱 뚜렷하게 구분됨을 확인할 수 있다. 결과적으로 본 논문에서 제안한 방법이 일반적인 기법에 비해 더 좋은 것으로 판단할 수 있다.

Acknowledgements

이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임 (2012-0007285)

참고문헌

[1] P. Kocher, J. Jaffe, and B. Jun, “Differential power analysis,” Advances In Cryptology - CRYPTO′ 99, LNCS 1666, pp. 388-397, Springer-Verlag, Santa Barbara, USA, August 1999.

[2] E. Brier, C. Clavier, F. Olivier, “Correlation Power Analysis With a Leakage Model.”, CHES 2004, LNCS 3156, pp. 16-29, Springer, 2004.

[3] S. Chari, C. Jutla, J. Rao, and P. Rohatgi, ″Towards Sound Approaches to Counteract Power-Analysis Attacks.″ CRYPTO ′99, LNCS 1666, pp. 398-412, Springer, 1999.

[4] T. Messerges, “Using Second-Order Power Analysis to Attack DPA Resistant Software.”, CHES 2000, LNCS 1965, pp. 238-251, Springer, 2000.

[5] JS. Coron, L. Goubin, ″On Boolean and Arithmetic Masking against Differential Power Analysis.″, CHES 2000, LNCS 1965, pp. 231-237, Springer, 2000.

[6] JS. Coron, E. Prouff, M. Rivain, ″Side Channel Cryptanalysis of a Higher Order Masking Scheme.″, CHES 2007, LNCS 4727, pp. 28-44, Springer, 2007.

[7] H. Kim, S. Hong, J. Lim, “A Fast and Provably Secure Higher-Order Masking of AES S-Box”, CHES 2011, LNCS 6917, pp. 95-107. Springer 2011.

[8] C. Herbst, E. Oswald, S. Mangard, “An AES Smart Card Implementation Resistant to Power Analysis Attacks.”, LNCS 3989, pp. 239-252, Springer, 2006.

[9] S. Mangard, E. Oswald, T. Popp, “Power Analysis Attacks: Revealing the Secrets of Smart Cards.”, Chapter 10, Attack On Masking, pp. 245-272, Springer, 2007.

[10] J. Cho, D. Han, “Security Analysis of the Masking-Shuffling based Side Channel Attack Countermeasures.”, SERSC, 2012.

[11] E. Oswald, S. Mangard, “Template Attacks on Masking－Resistance is Futile”, CT-RSA 2007, LNCS 4377, pp. 243-256, Springer, 2007.

[12] Y. Kim, T. Sugawara, N. Homma, T. Aoki, A. Satoh, “Biasing Power Traces to Improve Correlation in Power Analysis Attacks.”, COSADE 2010.