실용적인 고차 부채널공격 대응에 대한 1차 상관전력분석 오류 키 특성 연구

안현진, 한동국
국민대학교 수학과
e-mail: {ahz012, christa}@kookmin.ac.kr

A Study on Characteristic of Ghost-Key Revealed from the 1st Order Correlation Power Analysis on the Practical High Order Side-Channel Attack Countermeasure.

Hyun-Jin Ahn, Dong-Guk Han
Dept. of Mathematics, Kookmin University

요 약

과거에는 보안디바이스의 안전성을 탑재된 암호알고리즘의 안전성에 의존하였다. 하지만 부채널 분석을 통해 암호알고리즘의 안전성과는 별개로 부채널 정보에 의한 보안디바이스의 물리적 취약성이 존재함이 밝혀졌다. 이러한 보안디바이스의 물리적 취약성을 보완하기 위해서는 최소 2차 상관전력분석에 대한 대응법이 간구되어야 한다. 최근 2차 상관전력분석에 대한 실용적인 대응법으로 1차 마스킹과 셔플링을 혼합한 방법을 많이 활용하고 있다. 하지만 1차 마스킹과 셔플링이 혼합된 부채널 대응법을 1차 상관전력분석으로 분석하였을 경우, 특이한 피크가 발생한다. 본 논문에서는 마스킹과 셔플링이 혼합된 부채널 대응법을 1차 상관전력분석으로 분석하였을 때, 특이한 피트가 발생함을 실험적으로 확인하였고, 그 피크 발생 원인을 소개한다. 뿐만 아니라, 피크 발생 정보를 추가적인 부채널 분석 정보로 활용할 수 있는 방법을 소개한다.

1. 서론

스마트디바이스의 발달과 함께 금융, 통신을 비롯한 다양한 분야에서 IC카드, USIM과 같은 보안디바이스가 활용되고 있다. 민감한 정보를 다루는 보안디바이스는 탑재된 암호알고리즘을 통해 정보를 안전하게 보호한다. 따라서 과거에는 보안디바이스의 안전성이 탑재된 암호알고리즘의 안전성에의해 보장되었다. 하지만 최근 암호알고리즘의 안전성과는 무관하게 보안디바이스에서 발생하는 물리적 정보에 의해 취약성이 존재함이 드러났다. 이러한 취약성을 보완하기 위해서는 최소 2차 상관전력분석에 대한 대응법이 마련되어야 한다. 2차 이상의 상관전력분석[1]에 대한 대응법으로 발표된 다양한 마스킹 기법([2], [3], [4])은 높은 연산비용으로 인해 비실용성문제를 안고 있다. 최근에는 이러한 문제를 해결하고자, 실용적인 대응방안으로 1차 마스킹과 셔플링 기법을 혼합한[5] 방법이 일반적으로 사용되고 있다. 이 대응법은 1차 상관전력분석(Correlation Power Analysis, CPA)[6]에 안전한 알고리즘 구현이 가능하도록 한다.

실용적인 대응법을 1차 CPA로 분석하였을 경우 특정 위치에서 특이한 피크가 발생한다. 이 피크는 옳은 키에 대한 정보를 제공하지는 않지만 부채널 분석에 대한 새로운 정보로 활용될 수 있다.

본 논문에서는 1차 마스킹과 셔플링이 함께 적용된 알고리즘을 1차 CPA로 분석하였을 경우 특정 위치에서 나타나는 피크의 발생을 실험적으로 보인다. 또한 평문과 Sbox 출력의 상관관계 규명을 통한 [1]오류 키(Ghost-Key)의 특성 파악으로 피크의 발생 원인을 규명한다. 뿐만 아니라, 피크 발생 정보를 추가적인 부채널 분석 정보로 활용할 수 있는 방안에 대해 소개한다.

2. 사전연구

2.1. 부채널 분석

부채널 분석(Side-Channel Analysis, SCA)은 1996년 Paul Kocher[7]가 최초로 제안하였으며, 암호알고리즘을 탑재한 보안디바이스의 암호알고리즘 구동으로 발생하는 부가적인 정보에 의존하여 키를 분석하는 기법이다. 분석에 사용되는 부채널 정보로는 전력, 전자파, 소리, 빛, 레이저 등이 있다. 이 중 소비전력을 부채널 정보로 활용하는 전력분석이 가장 많이 사용되고 있으며 본 논문에서는 전력분석 공격만을 다룬다.

1) 암호알고리즘에 사용되지 않은 키가 부채널 분석에 특이점을 나타내는 경우 오류 키(Ghost-Key)라 한다.

2.2. 전력 분석 공격

전력 분석 공격은 하드웨어에서 '0', '1'을 처리하는데 따르는 전력 소모가 다르다는 점을 이용하며, 일반적으로 헤밍웨이트 모델(Hamming Weight Model), 헤밍디스턴스 모델(Hamming Distance Model)[8]을 소비전력 모델로 사용한다. 분석에 사용되는 암호알고리즘의 소비전력파형 수에 따라 전력분석 방법은 크게 두 가지로 구분된다.

첫 째, 적은 수의 소비전력 파형을 관찰하여 키 값을 유도하는 단순전력분석(Simple Power Analysis, SPA)

둘 째, 동일한 키를 사용하는 다수의 소비전력 파형 사이의 상관관계를 통계적으로 분석하여 키 값을 유도하는 차분전력분석(Differential Power Analysis, DPA)

특히, DPA에서 통계적 분석에 상관계수를 사용하는 분석을 상관전력분석(Correlation Power Analysis, CPA)이라 하며, 다른 통계적 분석을 적용하는 분석방법에 비해 CPA의 분석 성능이 월등히 좋은 것으로 나타난다. 따라서 본 논문에서는 CPA를 DPA로 사용한다. 분석에 사용되는 위치의 수에 따라 CPA의 차수가 정해진다. n개의 위치를 공격에 사용하는 경우 n차 CPA[1]라 하며, 부채널 분석 대응법에 따라 공격에 사용되는 CPA의 차수가 정해진다. 특히, 2차 이상의 차수를 갖는 CPA를 고차상관전력분석(High-Order Correlation Power Analysis, HOCPA)이라 한다.

2.3. 부채널 분석 대응법

부채널 분석 공격에 대한 대응방법으로 마스킹 기법([2], [3], [4])과 셔플링 기법[5]이 제안되었다. 마스킹 기법은 중간 값 정보를 임의의 값으로 감추는 것이며, 간단하게 램덤한 값과 감추고자 하는 정보를 exclusive or 연산함으로써 구현이 가능하다. 마스킹 기법을 통해 CPA에 요구되는 중간 값과 실제 연산값을 다르게 함으로써 CPA가 불가능 하도록 한다. 이 때, 분석에 고려되는 마스크의 개수에 따라 마스킹의 차수가 정해진다.

셔플링 기법은 중간 값이 연산되는 위치가 매번 바뀌도록 함으로써 CPA에 필요한 파형 수를 증가시키는 대응법이다. 예를 들어 128비트 키를 사용하는 AES(Advanced Encryption Standard)[9]에 셔플링 기법을 적용하는 경우, 16개의 Sbox 연산이 순차적으로 발생하는 Subbytes 함수에 적용하는 것이 일반적이다. 순차적으로 수행되는 Sbox의 연산 순서를 랜덤하게 함으로써 Subbytes 함수에 셔플링 기법을 적용할 수 있다.

마스킹 기법은 중간 값 추측을 차단하여 CPA가 불가능 하게 하는 반면, 셔플링 기법은 중간 값 추측은 가능하지만 분석에 필요한 파형 수, 분석 시간을 증가시킴으로써 현재의 컴퓨팅 환경에서 분석이 불가능하게 하는 대응법이다.

3. 마스킹과 셔플링을 혼합한 대응법에 대한 1차 CPA분석

기존에 발표된 2차 상관전력분석에 대한 대응법([2], [3], [4])은 대응법구성에 따르는 높은 연산 오버헤드와 현재의 공격능력(연산 능력, 메모리 등)으로 인해, 1차 마스킹 기법과 셔플링 기법의 혼합 적용이 2차 상관전력분석에 대한 실용적인 대응기법으로 통용된다. 이러한 대응기법은 2차 마스킹 기법에 준하는 부채널 분석에 대한 안전성을 제공함과 동시에 2차 상관전력분석 대응법이 적용된 암호알고리즘의 실용화가 가능하도록 한다. 실용적인 대응법이 적용된 암호알고리즘에 1차 CPA를 수행할 경우 키와 관련된 어떠한 정보도 얻을 수 없지만 특정 부분에서 특이한 피트가 발생한다.

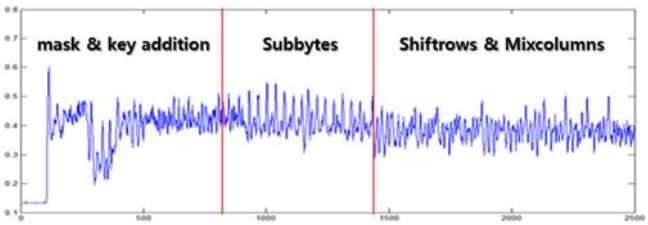
본 장에서는 피크의 발생을 실험적으로 보이고 발생 피크에 대한 원인 분석과 부채널공격 정보로 활용방안에 대해 소개한다.

3.1 마스킹과 셔플링을 혼합한 대응법에 대한 1차 CPA 분석 결과

우리는 마스킹, 셔플링이 적용된 암호알고리즘의 1차 CPA에 대한 정보 누수를 실험적으로 확인하였다.

0x000102030405060708090a0b0c0d0e0f를 128비트 비밀키로 사용하고 ARM 프로세서에서 암호화를 수행하는 마스킹, 셔플링이 적용된 AES[4] 1라운드의 전력파형 50만개를 250MS/s로 수집하였으며, Raw Integration[2] 압축기법을 1/10로 적용하였다. 또한 1차 CPA 수행 시 헤밍웨이트를 소비전력 모델로 하는 1라운드의 Sbox 출력[3]을 중간값으로 사용한다.

(그림 1)은 마스킹, 셔플링이 적용된 AES 1라운드 파형으로 가로축은 수집된 전력파형의 포인트, 세로축은 전력 소모량을 나타낸다. SPA를 통해 크게 3단계의 연산(mask & key addition, Subbytes, Shiftrows & Mixcolumns)이 수행된다는 사실을 확인할 수 있다.



(그림 1) 1차 마스킹, 셔플링이 적용된 AES 1라운드

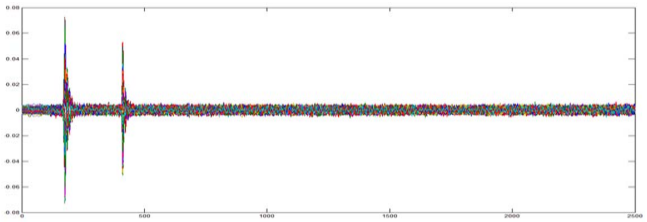
1차 CPA를 16 바이트 키에 각각 수행한 결과 모두 유

2) Raw Integration : 파형을 일정 구간으로 분할하고 각 구간내의 모든 포인트를 합하여 하나의 점으로 압축하는 기법

3) 헤밍웨이트 모델을 소비전력 모델로 하는 1라운드 $Sbox$출력 중간값: $HW(Sbox(PT_{r,i} \oplus GKey_{r,i}))$, $PT_{r,i}$: r라운드 i번째 바이트 평문, $GKey_{r,i}$: r라운드 i번째 바이트 추측키 후보

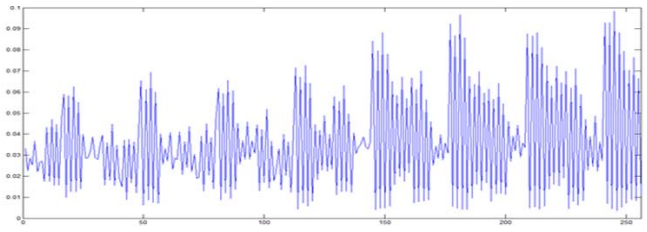
사한 분석 결과를 보였으며, 그 중 첫 번째 바이트 키에 대한 분석 결과를 설명한다.

(그림 2)는 1바이트 추측키(Guessing-Key, GKey) 후보를 가능한 모든 값(0x00~0xff)으로 가정하였을 경우 얻을 수 있는 256개의 1차 CPA 분석 결과를 모두 ploting한 그림이고, 가로축은 수집된 전력파형의 포인트와 동일하고 세로축은 상관계수를 나타낸다. 결과를 통해 앞부분에서 특이한 피크가 발생하는 것을 확인할 수 있으며, (그림 1)의 SPA 결과와 비교하여 mask & key addition 부분에서 피트가 발생하는 것을 확인할 수 있다.



(그림 2) 첫 번째 키 CPA(0x00~0xff)

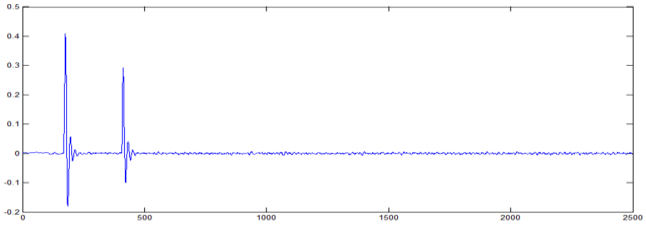
(그림 3)은 1바이트 추측키 후보를 가능한 모든 값(0x00~0xff)으로 가정하였을 경우 얻을 수 있는 256개의 1차 CPA 분석 결과 중 각 추측키 후보의 최댓값만 ploting한 것으로 가로축은 256개의 추측키 후보를 나타내고 세로축은 각 추측키 후보가 갖는 최대 상관계수를 나타낸다. (그림 3)을 통해 옳은 키(0x00)의 상관계수가 현저히 낮은 것을 확인할 수 있으며, 키 후보별 최대 상관계수의 값이 일정한 주기성을 띔을 알 수 있다.



(그림 3) (그림 2)의 추측키 후보별 최대 상관계수

3.2 오류 키 발생원인 분석

평문과 수집파형의 포인트별 상관계수 분석을 통해 (그림 2)에서 확인한 피크의 발생위치는 평문 데이터가 로드되는 부분과 동일하다는 사실을 알 수 있다. (그림 4)는 첫 번째 바이트 평문과 전력파형의 동일한 포인트에 해당하는 전력소모량의 상관계수를 모든 포인트에 대해 계산한 결과이며, 가로축은 수집된 전력파형의 포인트와 동일하고 세로축은 상관계수를 나타낸다. (그림 2)의 피크 발생위치와 (그림 4)의 피크 발생위치가 동일함을 확인할 수 있다.



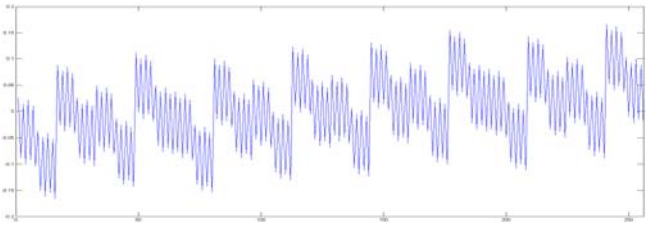
(그림 4) 첫 번째 바이트 평문과 수집파형의 상관계수

평문 데이터가 로드되는 부분에서 Sbox 출력을 중간값으로 하는 1차 CPA의 피크가 발생하였으므로, Sbox 출력과 평문의 상관관계를 확인하기 위해 <표 1>의 실험을 수행하였다.

<표 1> 평문과 Sbox 출력의 상관관계 분석 실험

단계 1. for $GKey_{1,1}=0$ *to* 256
단계 2. for $PT_{1,1}=0$ *to* 256
단계 2.1. $HW(Sbox(PT_{1,1}\oplus GKey_{1,1}))$ *end* for
단계 3. $Corr(HW(PT_{1,1}), HW(Sbox(PT_{1,1}\oplus GKey_{1,1})))$ *end* for
$Corr(X, Y)$: 집합 X와 Y의 상관계수

(그림 5)는 <표 1>의 실험 결과로 가로축은 256개의 추측키 후보를, 세로축은 상관계수를 나타낸다. 결과를 통해 평문과 Sbox 출력의 상관관계는 추측키 후보에 대해 일정한 패턴을 나타내는 것을 알 수 있다. 그 패턴은 $[Gkey_1, Gkey_2]$[4]를 하나의 주기로 8개의 주기가 발생하며, 각 주기에서 $Gkey_1$, $Gkey_2$가 가장 높은 상관계수를 가진다는 사실을 확인할 수 있다.



(그림 5) 평문과 Sbox 출력의 상관관계 분석 실험결과

3.3 오류 키 정보의 활용

실험을 통해 1차 마스킹과 셔플링이 혼합된 대응법에 1차 CPA로 발생한 특이점은 평문과 Sbox 출력의 상관관계에 의해 발생함을 확인하였다. 이러한 특이점은 암호화를 수행하기 위해 로드되는 평문과 연관된 부분에서 발생하지만 옳은 키에 대한 어떠한 정보도 노출하지 않는다.

4) $GKey_1 \equiv 16 \bmod 32$, $GKey_2 = (Gkey_1 + 31) \bmod 256$를 만족하는 추측키 후보 $Gkey_1$, $Gkey_2$

그러나 평문 데이터 로드의 위치 정보는 SPA 관점에서 분석 구간 설정의 근거로 작용하여 분석시간 단축의 효과를 보일 수 있다. 또한 평문 데이터 로드 특성을 노출시킴으로써 알고리즘의 대응법 적용여부, Template[10] 구성위치 등 부채널 분석에 대한 새로운 공격 정보를 제공할 수 있다. 특히, 적은 수의 마스킹을 사용하고 평문 데이터와 마스킹의 특정 연산을 수행하는 1차 마스킹, 셔플링 기법은 평문데이터 로드 부분의 정보가 공격자로 하여금 안전성을 위협하는 결정적인 정보로 활용될 수 있다.

4. 결론

본 논문에서는 실용적인 고차차분전력분석 대응법(1차 마스킹, 셔플링)이 적용된 알고리즘에 대한 1차 CPA 수행 후 평문 데이터가 로드되는 부분에서 특이점이 발생함을 실험을 통해 확인하였다. 평문과 Sbox 출력의 상관관계 분석 실험을 통해 평문과 Sbox 출력의 상관관계가 존재함을 확인하였고 이러한 상관관계의 주기성에 대해 해석하였다. 또한 1차 CPA로 발생한 특이점은 키에 대한 정보를 직접 노출하지는 않지만 공격자로 하여금 평문데이터의 로드 부분을 알 수 있도록 하여 공격 구간의 축소, 대응법의 적용여부, Template 구성위치 제공 등의 새로운 부채널공격 정보로 활용 가능함을 보였다. 따라서 이 정보가 공격자로 하여금 유용하게 사용되지 않도록 안전한 구현(Secure Implementation)이 요구된다.

Acknowledgements

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

참고문헌

[1] J.S. Coron, E. Prouff, and M. Rivain, “Side Channel Cryptanalysis of a Higher Order Masking Scheme”, CHES 2007, LNCS 4727, pp. 28-44. 2007.

[2] M. Rivain, and E. Prouff, “Provably Secure Higher-Order Masking of AES”, CHES 2010, LNCS 6225, pp.413-427, 2010.

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

[4] L. Goubin, and A. Martinelli, “Protecting AES with Shamir’s Secret Sharing Scheme”, CHES 2011, LNCS 6917, pp. 79-94. 2011.

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

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

[7] P. Kocher, J. Jaffe, and B. Jun, “Differential Power Analysis”, CRYPTO 1999, LNCS 1666, pp. 388-397, 1999.

[8] S. Mangard, E. Oswald, and T. Popp, “Power Analysis attacks Revealing the secrets of smart cards”, Chapter 3. POWER CONSUMPTION, pp. 27-43, Springer, 2007.

[9] National Institute Standards and Technology: Advanced Encryption Standard (AES). Publication 197 (2001).

[10] S. Chari, J.R. Rao, and P. Rohatgi, “Template Attacks”, CHES 2002, LCNS 2523, pp. 13-28, 2003.