http://dx.doi.org/10.3745/KIPSTC.2011.18C.4.213

일반화된 신호 압신법에 기반한 향상된 차분전력분석 방법

최 지 선[†] · 류 정 춘[††] · 한 동 국[†††] · 박 태 훈[††††]

요 약

차분전력공격(Differential Power Analysis, DPA)의 효율성은 수집신호 정렬도를 비롯한 다양한 잡음에 많은 영향을 받는다. 최근에 Ryoo등은 잡음 신호를 극복하여 DPA의 분석성능 향상을 가져오는 효과적인 신호처리기법을 소개했다. 본 논문에서는 기존에 제안된 신호처리기법이 적용되지 않은 경우를 보이고, 이에 대한 해결방안으로 차분파형모델(Differential Trace Model, DTM)을 제안한다. 또한 제안된 DTM이 DPA 분석에 적합한가에 대해 이론적으로 증명하고 실험을 통해 검증한다.

키워드 : 부채널 분석, 차분전력공격, 전처리 기법, 차분파형모델

Enhanced Differential Power Analysis based on the Generalized Signal Companding Methods

Jisun Choi[†] · Jeong-Choon Ryoo[††] · Dong-Guk Han[†††] · Taehoon Park[††††]

ABSTRACT

Differential Power Analysis is fully affected by various noises including temporal misalignment. Recently, Ryoo et al have introduced an efficient preprocessor method leading to improvements in DPA by removing the noise signals. This paper experimentally proves that the existing preprocessor method is not applied to all processor. To overcome this defect, we propose a Differential Trace Model(DTM). Also, we theoretically prove and experimentally confirm that the proposed DTM suites DPA.

Keywords : Side-Channel Attack, Differential Power Analysis, Preprocessor Method, Differential Trace Model

1. 서 론

부채널 분석(Side Channel Analysis, SCA)은 기존의 암호 분석방법이 아닌, 암호시스템의 물리적인 구현으로부터 발생하는 암호연산의 시간이나 소비전력 및 전자파 등의 부채널 정보를 이용하여 알고리즘의 비밀 정보를 찾아내는 방법으로서, Chip기반의 보안 디바이스를 해독하는데 효과적인 기법으로 알려져 있다[1]. 그 중 차분전력분석(Differential Power Analysis, DPA), 상관전력분석(Correlation Power Analysis, CPA)은 소비되는 전력을 분석하는 방법으로서 강력한 분석기법이다[2]. 한 편, 부채널 분석에서 분석에 대한 효율성은 시간 불일치를 포함한 다양한 잡음에 영향을 받는다. 특히 DPA의 경우 이러한 잡음에 더 민감하며 신호의 시간 불일치와 잡음으로 인한 공격 효율성저하 극복 연구가 활발히 진행되고 있다[3,4]. 최근에는 Expanding에 기반한 A-law 압신 방법이 DPA의 분석성능 향상을 가져오는 효과적인 전처리 기법임이 소개되었다[4].

본 논문에서는 [4]에서 제안한 Expanding기반 A-law압신기법을 ARM Processor에 적용하여 A-law 압신법 적용시 Processor에 적합한 함수의 선택이 필수적임을 실험으로 증명하고 이러한 단점을 해결하기 위한 차분파형모델(Differential Trace Model, DTM)방법을 제안한다. 논문의 구성은 다음과 같다. 2장에서는 차분전력 분석과 분석 성능 향상을 위한 비선형 가중치 함수를 다룰 것이며, 3장에서는 제안된 기법의 개념과 특성, 이론적인 공격 효율성을 설명하고, 4장에서는 기존모델과 제안한 모델간의 성능을 비교·연구한다. 마지막으로 5장에서 논문을 마무리 짓는다.

2. 차분전력 분석

2.1 분석 기법

대부분의 부채널 분석은 하나의 전력파형으로는 분석이 불가능하며 다수의 소비 전력을 수집해 통계치 활용으로 키를 찾아낸다. DPA분석은 통계치로 두 집단의 평균의 차를

† 준 회 원 : 국민대학교 수학과 석사과정
†† 정 회 원 : 국방대학교 근무
††† 정 회 원 : 국민대학교 수학과 조교수
†††† 정 회 원 : 국민대학교 수학과 교수
논문접수 : 2011년 3월 7일
심사완료 : 2011년 4월 12일

이용하며 비밀키 K_e를 추출하기 위해 평문P_j과 특정 비트 b_i에 해당하는 중간 값을 분류함수$D(P_j, b_i, K_e)$로 나타낼 때, 수식 (1)의 계산 값으로 분석 결과를 판단한다.

$$\triangle_D(b_i) = \frac{\sum_{j=1}^{N} D(P_j, b_i, K_e) S_{st(j)}}{\sum_{j=1}^{N} D(P_j, b_i, K_e)} - \frac{\sum_{j=1}^{N} (1 - D(P_j, b_i, K_e)) S_{st(j)}}{\sum_{j=1}^{N} (1 - D(P_j, b_i, K_e))} \quad (1)$$

($S_{st(j)}$: st의 시점에서 j번째 평문이 소모한 전력량,
N : 수집한 평문 수)

즉, 계산 값 $\triangle_D(b_i)$는 특정비트 b_i에 대해 분류함수 D로 분류한 두 전력량 집단의 평균의 차가 되며, 예측한 비밀키 K_e가 옳은 경우 구분된 두 집단 간의 평균 소비전력의 차이는 $\triangle_D(b_i) \neq 0$이 된다. 이 값을 DPA피크라 부른다. 한편 초기에 예측한 비밀키 K_e가 옳지 못한 경우에는 분류함수에 의한 분류가 무작위로 진행되어 평균의 차가 $\triangle_D(b_i) \approx 0$이 되므로 DPA피크를 확인 할 수 없다.

하지만, 실제 DPA 분석 환경은 비트 분포 조건을 완벽하게 만족하지 않고 한 비트 변화에 의한 전력차이가 극도로 작기 때문에 각 파형이 시간상 정확히 동기 되지 않았을 때 공격 성능이 상당히 저하된다. 이러한 DPA 단점을 극복하기 위한 방법으로 Messerges[5]와 Bevan[6]은 다중 비트를 이용한 DPA방식을 제안했고, 트레이스 간의 동기 불일치에 의한 성능 저하를 극복할 수 있는 구간 에너지 기반의 공격법[7]과 진폭에 따라 서로 다른 가중치로 처리하여 잡음의 영향을 최소화하는 신호처리법[4]이 제안되었다.

본 논문의 DPA분석은 PIC칩과 ARM칩에서 구현한 DES 알고리즘을 대상으로 비트 합 분석법을 사용한다[6].

2.2 비선형 가중치 함수

Ryoo등이 제안한 비선형 가중치 함수는 부채널 신호인 전력 및 전자장이 암호 연산 시에 많은 에너지를 소비하여, 진폭관점에서 수집 신호의 진폭이 큰 피크 값에 에너지가 집중되어 있다는 점에 착안한 신호 처리기법이다. 이는 Expanding기반의 A-law 압신법[1]을 부채널 신호에 대한 비선형 가중치 함수로 선택하여 전처리 후, DPA분석을 수행하여 최대 33%(시간영역)의 분석성능 향상을 가져왔다. 이 때 실험은 암호연산의 소비 전력 에너지가 피크 값에 집중되어 있는 PIC칩 프로세서가 사용되었다[4].

하지만 Ryoo등이 제안한 신호처리기법의 이론을 살펴 볼 때에, 암호연산의 소비 전력 에너지의 분포가 서로 다른 특성을 지니는 ARM칩 프로세서의 경우 동일 비선형 가중치 함수의 적용에 의한 분석이득을 볼 수 없다. 즉, ARM칩 프로세서는 암호 연산관련 소비 전력 에너지가 파형의 진폭이 적은 부분에 집중되어 있기 때문에 Expanding기반이 아닌 Compressor 기반의 A-law 압신법을 선택하여 신호처리를 해야 한다.

1) ITU-T 음성코딩표준, 음성 코딩 영역에서 사용되는 A-law 압신 알고리즘[8]

〈표 1〉 DPA분석 성능 비교 (파형 개수기준)

	일반파형	Expanding 기반	Compressor 기반	처리이득
PIC칩[2]	600	400	X	33%
ARM칩	7,000	X	5,000	29%

<표 1>은 PIC칩과 ARM칩에서 각각 분석에 필요한 일반파형의 수를 기준으로 신호처리의 분석 성능을 나타낸다. 이는 비선형 가중치 함수를 통한 DPA성능향상은 암호 프로세서 칩에 적절한 압신(Companding) 신호처리 기법의 선택이 필수적임을 뜻한다.

3. 차분 파형 모델

Ryoo등이 제안했던 DPA분석 성능향상에 효과적인 비선형 가중치 함수 적용은 분석자가 사전에 목표 암호체계의 진폭 분포 특성을 알고 있어야 하기 때문에 임의의 실험 환경에서 보편적으로 적용될 수 없다는 약점을 지닌다. 본 장에서는 이를 보완하기 위한 방법으로 새로운 모델을 제안한다. 제안하는 파형 모델은 DPA공격을 수행할 때에 암호체계 특성에 관계없이 오직 Compressor기반 함수를 비선형 가중치 함수로 사용한다.

3.1 이론

부채널 정보의 특성에 따라 전력소모 파형 모델을 다음과 같이 구분한다.

-단순 파형 모델(Simple Trace Model, STM): 부채널 정보로 암호연산 도중에 수집된 원 신호파형을 사용

-차분 파형 모델(Differential Trace Model, DTM): 단순 파형 집단으로부터 임의로 선택한 파형을 참조파형이라 할 때, 단순 파형에서 참조파형을 뺀 생성한 파형을 사용

단순파형은 다음과 같이 세 가지 성분으로 구성할 수 있다:

$$S_{st(j)} = S_{d(j)} + S_{t(j)} + S_{n(j)} \quad (2)$$

여기서, $S_{st(j)}$는 수집한 단순 파형이며, 나머지 각 성분의 특성은 다음과 같다.

- $S_{d(j)}$는 암호 알고리즘과 그 구현에 의존한 신호의 일부로서 알고리즘과 구현 플랫폼 특성에 의존적이다. 따라서 암호 연산 데이터와 무관한 수치이며 DPA를 포함한 부채널 공격의 경우 이 성분은 자명하게 결정된다.

- $S_{t(j)}$는 중간 값의 해밍웨이트에 의존하여 변하는 신호의 부분이다. 암호연산 도중 매우 짧은 순간(τ)동안 지속되는 것으로써 부채널 분석에서 $S_{t(j)} = \varepsilon \bullet H(w)$로 나타낸다. 이 때 $H(w)$는 중간 값 w의 해밍웨이트이고 ε은 해밍웨이트 혹은 해밍디스턴스 단위에 해당하는 물리적인 양을 뜻한다.

- $S_{n(j)}$는 균일한 형태 또는 가우시안 분포 등의 특성을 지닌 파형의 시간 미정렬과 양자화 잡음 등이 그 원인이다.

2) [4]의 결과

이러한 모든 잡음들은 각각 독립적인 원인에 의해 발생한다고 가정한다.

파형의 두 번째 종류인 차분파형은 정의에 의해 수식 (3)으로 표현된다.

$$\begin{aligned} S_{dt(j)} &= S_{st(j)} - S_{st(k)} \qquad (3) \\ &= [S_{d(j)} + S_{t(j)} + S_{n(j)}] - [S_{d(k)} + S_{t(k)} + S_{n(k)}] \\ &= [S_{d(j)} - S_{d(k)}] + [S_{t(j)} - S_{t(k)}] + [S_{n(j)} - S_{n(k)}] \end{aligned}$$

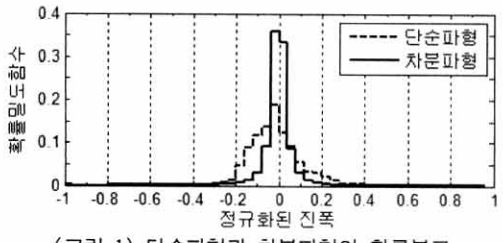
여기서 $S_{st(k)}$는 참조파형으로서 단순파형 중 k번째 파형을 선택한 것이다. 앞서 살펴본 단순 파형의 성분과 마찬가지로 수식 (3)에 표현한 성분의 특성을 살펴볼 수 있다. 차분파형을 구성하는 세 성분의 특성은 다음과 같다.

- S_d는 실제로 통계적인 성질을 지니는 값이 아니며 암호 알고리즘과 구현 특성에 의존하여 결정된다. 따라서 $S_{d(j)} - S_{d(k)}$값은 clock transition edge에서 참조파형과 파형 간의 시간 불일치 정보를 배제하면 매우 작은 값으로 수렴한다.
- S_t는 중간 값의 해밍웨이트에 의존하기 때문에 그 차분($S_{t(j)} - S_{t(k)}$)은 임의로 선택된 참조파형과의 해밍디스턴스 모델 분석이 된다. 즉 이 성분은 기존의 해밍디스턴스 모델을 적용한 상황과 동일하기 때문에 차분파형모델이 단순파형모델과 동일 한 암호 연산 정보를 가진다고 판단할 수 있다.
- S_n은 차분파형의 경우 평균, 분산과 같은 통계적 성질을 변화시킨다. 이 성분이 차분에 의해 바뀐 내용은 다음 소절에서 다룬다.

실제로 새로 정의한 차분파형이 DPA분석에 적합한지 식 (3)의 $S_{dt(j)}$를 식(1)의 $S_{st(j)}$에 대입하여 판단할 수 있다. 대입 시, 임의로 선택한 참조파형 $S_{st(k)}$에 해당하는 수치는 서로 상쇄되어 DPA 결과 $\triangle_D(b_i)$에 어떠한 영향도 미치지 않는다. 이는 우리가 제안한 차분파형모델이 DPA공격에서 STM이 사용되었던 방법과 동일하게 적용가능하고 부채널 신호에 임의적인 조작을 가하지 않은 모델 이라는 것을 이론적으로 증명한 것이다.

3.2 차분 파형의 특성

(그림 1)은 S-box연산에 의한 전력소모파형을 정규화 시킨 단순파형과 차분파형 각 8,000개에 대해 진폭에 따른 확률분포를 나타낸 것이다. 두 종류의 파형은 그 평균과 분산이 서로 다름이 쉽게 확인된다. 특히 차분파형의 확률분포는 0을 기준으로 좌우 대칭의 성질을 보이지만 단순파형의 경우 그 분포가 0을 기준으로 좌측으로 치우쳐 있다.

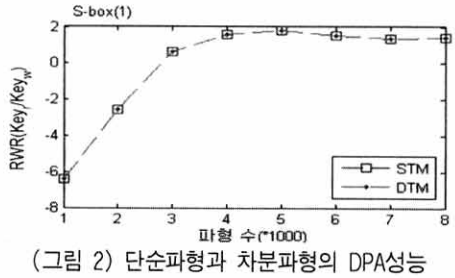


(그림 1) 단순파형과 차분파형의 확률분포

이는 차분파형의 경우 암호 알고리즘과 수행플랫폼에 무관한 암호 데이터 관련 정보의 분포가 0주위에 있음을 뜻하며 결국 A-law 비선형 가중치 함수 적용 대상으로 차분파형이 더 적합함을 알 수 있다.

3.3 차분파형모델 성능 증명

성능 증명을 위한 실험은 DES알고리즘의 첫 번째 라운드, 8개의 S-box를 선택하여 입력으로 ARM칩의 경우 랜덤한 8,000개 평문을, PIC칩은 1,000개의 평문에 해당하는 신호를 사용하였다.



(그림 2) 단순파형과 차분파형의 DPA성능

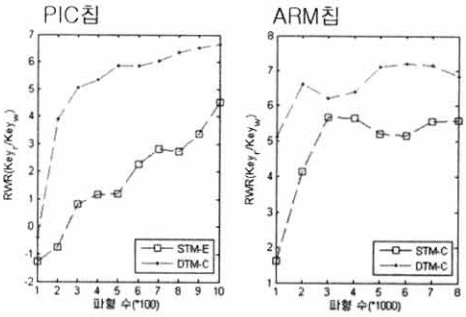
STM과 DTM에 대한 DPA분석결과는 두 칩 모두 각 S-box마다 동일한 DPA 피크를 지닌다. (그림 2)는 이러한 결과를 설명하기 위해 ARM칩의 첫 번째 S-box에 대한 키 추출 성공 여부를 RWR[3]로 보여준다. 다른 S-box에서도 결과는 이와 동일하다. 이로써 차분파형 모델이 DPA공격에 사용 될 수 있을 뿐만 아니라 STM과 분석환경이 이론적으로 동일함을 실험을 통해 확인하였다. 이 결과는 암호 수행 플랫폼과 무관하게 비선형 가중치 DPA공격을 적용할 수 있는 차분파형의 이점을 잘 드러낸다.

4. 분석 성능 비교

본 장에서는 기존 STM에서 신호처리 기법의 DPA성능과 제안한 DTM에서 신호처리 기법의 DPA성능을 비교할 것이다. 성능 분석에 앞서, 용어의 혼란을 막기 위해 다음의 약어를 정의한다.

- STM_E: Expanding함수가 적용된 단순파형모델
- STM_C: Compressor함수가 적용된 단순파형모델
- DTM_C: Compressor함수가 적용된 차분파형모델

실험 대상 및 분석 환경은 3.3절의 환경과 동일하다.



(그림 3) STM, DTM에 비선형가중치 적용 후 분석 성능

3) Right key와 Max-wrong key의 Amplitude 비율(RWR > 0 인 경우 키 추출 성공)

(그림 3)은 첫 번째 S-box의 부분키를 DPA분석하여 분석 성능비를 나타낸 것으로 좌측은 PIC칩, 우측은 ARM칩에 대한 분석이다. 두 칩 모두, STM분석에서는 각 칩 특성에 적합한 함수기반의 비선형 가중치함수를 선택하고 DTM분석에서는 Compressor함수를 비선형 가중치함수로 선택하였다. 결과는 칩 특성에 맞추어 알맞은 신호처리를 하였던 STM분석보다 제안한 DTM을 적용한 후에 모델에 적합한 신호처리 결과의 분석 성능비가 같은 파형 수를 기준으로 더 높은 값을 가지며 좋은 성능을 나타낸다. 나머지 S-box에 대한 결과도 이와 유사하다.

5. 결 론

본 논문에서는 DPA부채널 공격의 성능을 획기적으로 개선할 수 있는 전처리 방법의 우월성을 입증함과 동시에 분석을 위해 필연적으로 함수의 종류를 선택해야하는 한계점을 지적하고 이러한 문제가 해결될 수 있는 차분파형모델을 제안했다. 또한 제시한 방법이 실제 DPA공격에 적용 가능함을 이론적으로 증명하고 실험으로 검증하였다.

분석성능은 대부분의 S-box에서 DTM에 비선형 가중치를 적용한 성능이 STM에 비선형 가중치를 적용한 결과에 비해 우월한 성능을 지닌다. 그 원인은 DTM의 분포가 0을 기준으로 대칭의 성질을 지니는 A-law기반 비선형 가중치 함수에 더 적합하기 때문임을 밝혔다.

향후 제안한 모델과 전처리 방식을 다양한 보안장비에 적용하여 DPA의 공격 성능 개선효과를 연구할 것이며, 부채널 신호처리에 적합한 비선형 가중치 함수 개발과 분석이 더 연구해야할 분야로 남아있다. 본 연구의 결과는 차세대 전자주민증과 같은 전자 ID 등에 활용될 스마트 칩에 대한 물리적 취약성 분석에 효율적으로 활용될 것으로 사료된다.

참 고 문 헌

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

[2] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," CRYPTO 1999, LNCS 1666, Springer-Verlag, pp.388-397, 1999.

[3] C. Gebotys, S.Ho, and A. Tiu, "EM Analysis of Rijndael and ECC on a Wireless Java-Based PDA", CHES 2005, LNCS 3659, Spreinger-Verlag, pp.250-264, 2005.

[4] J-C.Ryoo, D-G.Han, S-K.Kim, and S-J.Lee, "Performance Enhancement of Differential Power Analysis Attacks With Signal Companding Methods", IEEE Signal Processing Letters, Vol.15, pp.625-628, 2008.

[5] T.S.Messerges, E.A.Dabbish, and R.H.Sloan, "Examining smart-card security under the threat of power analysis attacks", Journal of IEEE Trans. on Computers, Vol.51, Issue 5, pp.541-552, 2002.

[6] R.Bevan and E.Knudsen, "Ways to Enhance DPA", ICISC 2002, LNCS 2587, Springer-Verlag, pp.327-342, 2003.

[7] T-H.Le, J.Clediere, C.Serviere, and J-L.Lacoume, "Efficient solution for misalignment of signal in side channel analysis", ICASSP, pp.257-260, 2007.

[8] N.S.Jayant, Peter Noll, Digital Coding of Waveforms: Principles and Applications to Speech and Video, Prentice Hall, 1984.

최 지 선

e-mail : zssun@kookmin.ac.kr
2009년 국민대학교 수학과(학사)
2009년~현 재 국민대학교 수학과 석사과정
관심분야 : 부채널 분석 및 대응법, 화이트 박스 암호, 무선 보안, 등

류 정 춘

e-mail : jcwillow@naver.com
1988년 경북대학교 전자공학과(학사)
1990년 경북대학교 정보통신 석사(공학석사)
2009년 고려대학교 정보보호대학원 박사(공학박사)
1999년~현 재 국방대학교 근무
관심분야 : 정보통신, 정보보안, 신호처리, 정보처리응용 등

한 동 국

e-mail : christa@kookmin.ac.kr
1999년 고려대학교 수학과(학사)
2002년 고려대학교 수학과 석사(이학석사)
2005년 고려대학교 정보보호대학원 박사(공학박사)
2004년~2005년 일본 Kyushu Univ., 방문연구원
2005년~2006년 일본 Future Univ.-Hakodate, Post.Doc.
2006년~2009년 한국전자통신연구원 정보보호연구본부 선임연구원
2009년~현 재 국민대학교 수학과 조교수
관심분야 : 공개키 암호시스템 안전성 분석 및 고속 구현, 부채널 분석, RFID/USN 정보보호 기술 등

박 태 훈

e-mail : thpark@kookmin.ac.kr
1980년 경북대학교 수학교육과(학사)
1982년 서울대학교 수학과 석사(이학석사)
1994년 University of North Carolina at Chapel Hill 박사(이학박사)
1995년~현 재 국민대학교 수학과 교수
관심분야 : Hyperbolic System, Computational Fluid Dynamics, Scientific Computation, 암호이론