Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.6, Dec. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.6.1055

선형판별분석을 이용한 전력분석 기법의 성능 향상*

강 지 수,[1,2†] 김 희 석,[3‡] 홍 석 희[2]
[1]삼성전자, [2]고려대학교, [3]한국과학기술정보연구원

The Enhanced Power Analysis Using Linear Discriminant Analysis*

Ji-su Kang,[1,2†] HeeSeok Kim,[3‡] Seokhie Hong[2]
[1]Samsung Electronics Co., Ltd., [2]Korea University, [3]Korea Institute of Science and Technology Information

요 약

전력소모량을 이용한 부채널 분석의 성능 향상을 위해 다양한 분석기법이 제안되고 있다. 이들 중, 사전처리 단계에서 적용 가능한 파형압축은 전력분석을 위한 소요시간을 단축하고 수집신호의 잡음성분을 줄이기 위해 널리 사용되는 방법이다. 본 논문에서는 영상처리 등에 많이 사용되고 있는 선형판별분석(Linear Discriminant Analysis)을 이용한 전력분석기법을 제안한다. 또한, 실험을 통해 기존의 파형압축방법 중 가장 성능이 좋은 것으로 알려진 주성분분석(Principal Component Analysis)을 이용한 방법과의 성능 비교를 통해 제안기법의 우수성을 증명한다.

ABSTRACT

Recently, various methods have been proposed for improving the performance of the side channel analysis using the power consumption. Of those method, waveform compression method applies to reduce the noise component in pre-processing step. In this paper, we propose the new LDA(Linear Discriminant Analysis)-based signal compression method finding unique feature vector. Through experimentations, we are comparing the proposed method with the PCA(Principal Component Analysis)-based method which has known for the best performance among existing signal compression methods.

Keywords: Side-Channel Analysis, Power Analysis, Linear Discriminant Analysis

I. 서 론

부채널 분석(Side Channel Analysis)이란 장치 내에 구현된 암호연산기능에 대해 설계자가 의도하지 않은 채널의 정보를 이용해 암호를 분석하는 기법을 통칭한다. 이러한 부채널 분석에는 기기의 동작시간을 이용한 시간 분석(Timing Analysis)[1], 기기의 전력소모량을 이용하는 전력 분석(Power Analysis)[2,3], 기기에서 방출되는 전자기파를 이용한 전자기파 분석(Electric Magnetic Analysis)[4], 의도적인 오류 주입에 의해 야기된 장비의 오동작을 이용한 오류 주입 분석(Fault Injection Analysis)[5] 등이 있다. 보안 장비에 대한 최근 보안성 평가 기준은 이러한 부채널 분석에 대한 안전성을 중요한 요소로 평가하고 있다.

가장 많이 사용되는 부채널 분석 기법인 전력 분석에는 단순전력분석(Simple Power Analysis), 차분전력분석(Differential Power Analysis)[2], 상관전력분석(Correlation Power Analysis)[3], 고차 차분전력분석(Higher-Order Differential

접수일(2014년 8월 25일), 수정일(2014년 10월 13일), 게재확정일(2014년 10월 15일)
* 본 연구는 미래창조과학부 및 정보통신산업진흥원의 대학 IT연구센터육성 지원사업의 연구결과로 수행되었음 (NIPA-2014-H0301-14-1004)
† 주저자, js82.kang@samsung.com
‡ 교신저자, hs@kisti.re.kr(Corresponding author)

Power Analysis)등의 공격이 제안되어 왔으며 이러한 분석의 성능을 높이기 위해 다양한 신호 처리 기법이 활용되고 있다. 신호 처리 기법 중 하나인 파형압축[6]은 최초 전력분석 시간 단축을 위해 제안되었으나 주성분분석(Principal Component Analysis, PCA)을 이용한 가중치벡터를 사용한 압축 기법이 소개된 이후로 신호압축이 신호의 잡음 제거 및 전력 분석의 성능 향상도 가능케 함이 알려졌다.

본 논문에서는 선형판별분석(Linear Discriminant Analysis, LDA)을 이용한 전력분석을 제안한다. 선형판별분석은 주성분분석과 함께 얼굴 인식과 같은 패턴인식 분야에서 인식률을 높이기 위해 사용되는 데이터 마이닝 기법[7]으로, 두 분석 방법은 신호의 특성을 반영하는 특징벡터를 찾는데 사용된다는 점은 같지만 신호를 해석하는 접근방향에서 차이를 갖는다. 선형판별분석의 가장 큰 특징은 클래스로 분류된 다차원공간의 데이터에 대해 최적의 분류를 위한 특징벡터를 찾는다는 것이다.

선형판별분석은 템플릿 공격의 템플릿 생성을 위한 프로파일링 단계에서 데이터의 차원을 줄이는데 적용된 경우가 있으나[8,9], 이러한 방법은 공격자가 비밀키를 모르는 상태의 일반적인 부채널공격에 적용할 수는 없다,

제안 기법은 전력 분석에 이용되는 내부상태값에 대해 클래스를 분류하고 선형판별분석을 이용해 파형을 압축함으로써 신호 대 잡음비(Signal-to-Noise Ratio, SNR)[10]를 증가시켜 전력분석공격의 성능 향상을 기대한다.

전력분석에서 선형판별분석을 이용하기 위해 비밀키에 종속적인 내부상태값에 대한 클래스를 분류하는 것은 직관적으로 어렵다고 판단되지만, 본 논문에서는 AES(Advanced Encryption Standard)와 같이 전단사함수를 비선형연산으로 사용하는 대부분의 대칭키 암호의 경우 이러한 내부상태값을 클래스로 분류하는 것이 가능함을 보인다. 또한 제안 기법은 내부상태값이 연산되는 시점을 정확히 모른다 하더라도 분석이 가능한 공격기법으로 차분전력분석, 상관전력분석과 같은 조건하에서 수행될 수 있는 분석기법이다. 본 논문에서는 제안 기법의 우수성을 증명하기 위해 32비트 ARM프로세서에 구현된 암호알고리듬의 전력파형을 측정하여 주성분분석을 활용한 기존 파형압축과의 성능을 비교하였다. 실험 결과, 제안 기법이 공격에 이용되는 파형개수가 더 적을 뿐 아니라 신호 대 잡음비 또한 증가하는 것으로 확인되었다.

본 논문의 구성은 다음과 같다. 2절에서는 전력분석 향상기법의 하나인 신호압축과 이를 위해 본 논문에서 적용한 선형판별분석에 대해 소개한다. 3절에서는 선형판별분석을 이용한 전력분석을 제안하며 4절에서는 실험을 통해 제안 기법의 우수성을 증명한다. 5절에서 결론을 짓는다.

II. 관련연구

2.1 신호압축을 이용한 전력분석공격

전력분석은 부채널 분석 방법 중 가장 대표적인 방법으로 암호모듈이 포함된 장치의 동작에 따른 전력소모량을 측정, 이를 이용해 장치 내부의 비밀정보를 알아내는 방법이다. 전력분석은 반도체 회로에서 소모하는 전력이 연산의 종류와 내부상태값에 의존한다는 원리를 이용하며, 공격방법에 따라 적게는 한 개에서 많게는 수십만 개의 파형정보를 수집해 통계적인 방법으로 비밀키를 찾아내게 된다.

전력분석의 성능 향상을 위해 다양한 신호처리기법들이 제안되어져 왔다. 주로 사용되는 기법들로는 정렬되지 않은 신호를 정렬시키기 위한 신호정렬, H/W 필터나 증폭기 또는 S/W 필터를 이용하여 잡음을 줄이는 신호 필터링 및 증폭, 수집한 파형들 전체를 사용하지 않고 공격에 유리한 파형을 선별해 사용하는 파형선별, 파형을 압축해 분석의 효율성을 높이고 잡음을 제거하는 파형압축 등이 제안되어 있으며, 이와 같은 기법들은 단독으로 사용되지 않고 복합적으로 사용된다.

파형압축은 일정 구간에 걸쳐 나타난 파형신호를 압축된 신호로 표현하는 방법이다. 이 방법은 단순히 전력분석의 소요시간을 줄이기 위한 목적이 아닌, 잡음 성분을 줄이고 분석에 필요한 의미 있는 데이터를 추출해 분석 성능을 향상케 한다. 신호압축기법의 개요를 Fig.1.에 도식화했다.

기존에 널리 사용되던 압축방법들로는 구간의 모든 값을 더해 사용하는 raw integration, 구간에 포함된 가장 큰 값을 추출해 사용하는 maximum extraction, 구간 내 값들의 제곱의 합을 사용하는 sum of squares method 등과 같은 방법이 있으며 이러한 방법들은 구간 내 모든 신호가 같은 가중치를 갖는다는 특징이 있다.

반면, 가장 최근에 제안된 주성분 분석을 이용한

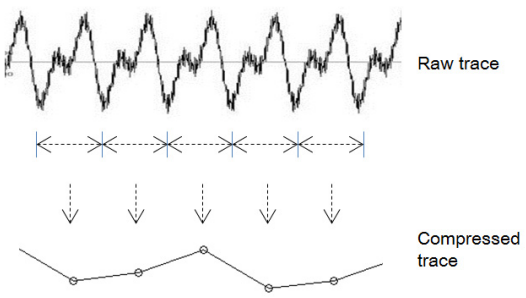

Fig. 1. Trace compression

파형압축은 잡음성분을 줄이고 신호의 특징을 가장 잘 나타낼 수 있는 가중치벡터를 구해 벡터상으로 데이터를 투영시켜 신호를 압축하는 방법으로 구간 내 신호들이 각각 다른 가중치를 갖게 된다[11]. 이 방법은 현재까지 제안된 파형압축 기법 중 가장 성능이 좋은 것으로 알려져 있다.

2.2 선형판별분석

선형판별분석은 클래스로 분류되어있는 다차원공간의 데이터에 대해 클래스간의 분산이 최대가 되는 특징벡터를 찾는 방법이다.

선형판별분석은 주성분분석과 비교될 수 있는데, 두 방법의 공통점은 다차원 데이터의 특성을 반영하는 특징벡터를 찾는다는 것이고, 차이점은 선형판별분석이 데이터의 클래스 정보를 사용해 클래스 간의 분산이 최대가 되는 최적분류성질의 특징벡터를 찾는 반면, 주성분분석은 전체데이터의 분산이 최대가 되는 최적표현성질의 특징벡터를 찾는다는 것이다.

기하학적 이해를 돕기 위해 2차원 데이터를 통한 예를 Fig.2.와 Fig.3.에 나타내었다.

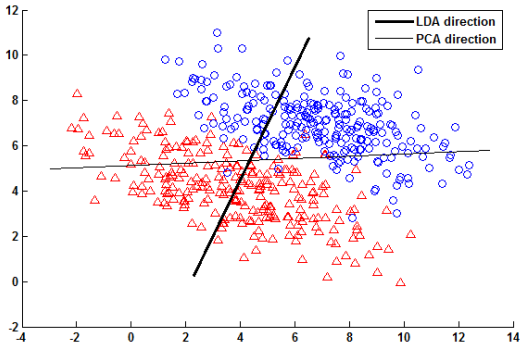

Fig. 2. LDA vs. PCA Direction

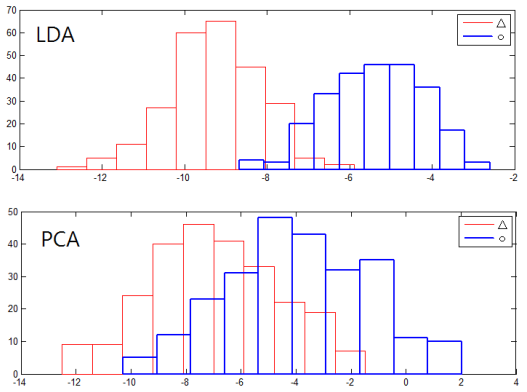

Fig. 3. Data Distribution after LDA&PCA

Fig.2.에 표시된 500개의 2차원 데이터는 2개의 클래스로 분류되어 있고, 각각 파랑색(○)과 빨강색(△)으로 표시되어 있다. 해당 데이터에 대해 선형판별분석과 주성분분석을 이용해 찾은 각각의 첫 번째 특징벡터의 방향을 데이터와 함께 표시했다. Fig.3.은 선형판별분석과 주성분분석을 이용해 구한 각각의 첫 번째 특징벡터를 이용해 1차원으로 압축한 데이터의 분포를 히스토그램으로 나타낸 것이다.

주성분분석을 통해 계산된 특징벡터는 데이터의 클래스 분류와는 무관하게 전체 데이터들의 분산이 가장 큰 방향을 갖는다. 따라서 해당 벡터위로 데이터를 투영시켜 데이터를 압축하면 분산이 큰 성분들에 의한 특성은 유지되고, 나머지 성분들에 의한 특성은 감소하게 된다. 해당 성질을 전력파형의 신호압축에 적용하면 신호에 대한 성분은 유지시키면서 잡음에 의한 성분을 줄이는 효과를 볼 수 있다.

선형판별분석은 접근하는 방향에 차이가 있다. 선형판별분석을 통해 계산한 특징벡터는 클래스 내부의 분산은 최소로 하면서 클래스간의 거리가 가장 커지는 방향을 갖는다. 해당 벡터위로 데이터를 투영시켜 압축하게 되면 클래스간의 데이터를 명확하게 구분할 수 있게 된다.

전력분석의 성능과 연관 지을 수 있는 전력파형의 성질은 내부상태값이 같은 경우의 신호들은 분산이 최소여야 하고, 내부상태값이 다른 경우의 신호들은 최대의 분산을 가져 구분이 용이하게 되는 것이다. 이는 선형판별분석을 이용한 파형압축에서 클래스로 구분된 데이터들이 데이터 압축을 통해 갖게 되는 성질과 정확히 대응된다.

따라서 본 논문에서 제안하는 선형판별분석을 이

용한 파형압축을 적용할 경우, 전력분석의 성능 향상을 기대할 수 있음을 직관적으로 알 수 있다.

III. 선형판별분석을 이용한 파형압축 방법

본 절에서는 수집된 파형정보를 선형판별분석을 이용해 압축하는 전처리 방법을 설명한다.

3.1 수집파형의 클래스 분류

파형압축에 선형판별분석을 적용하기 위해서는 몇 개의 클래스로 파형을 분류할 것인지 결정해야 하고, 파형들을 분류하기 위한 방법이 필요하다.

선형판별분석의 목적은 2.2에서 언급했듯이 파형압축을 통해 상관전력분석의 성능을 높이기 위함이다. 따라서 이상적인 클래스 분류는 상관전력분석에 사용되는 전력모델의 내부상태값 입력에 따른 출력값에 따라 파형들을 분류하는 것이다.

그러나 대부분의 전력분석 공격시나리오에서 공격자는 고정되어있는 비밀키에 대해 평문을 랜덤하게 바꿔가며 전력파형을 수집하게 되므로 정확한 내부상태값을 알 수 없고, 클래스 분류를 위해 전력모델을 적용하는 것은 불가능 하다.

본 논문에서는 공격의 목표가 되는 내부상태값이 가질 수 있는 모든 경우에 대해 클래스를 나누고 선형판별분석을 적용했다. 이 때, 공격자는 파형과 함께 수집된 평문들과 공격의 목표가 되는 내부 상태값의 관계를 이용할 수 있다.

8비트의 입출력을 갖는 AES S-box로 예를 들어보자. AES 1라운드 에서 평문은 키와 XOR연산 후 S-box에 입력된다. 공격자는 분석의 목표가 되는 내부상태값인 S-box출력의 정확한 값은 알 수 없지만, 비밀키가 고정되어있고 S-box가 전단사함수라는 특징을 이용하면 해당되는 평문값을 이용해 S-box의 8비트 출력 값에 대한 256개의 클래스로 파형을 분류할 수 있다. 이와 같은 원리를 이용하면 치환을 위해 전단사함수가 사용되는 대부분의 암호알고리즘 공격에 선형판별분석을 적용할 수 있다. Fig.4.에 평문정보를 이용해 수집된 파형을 c개의 클래스로 분류하는 예를 도식화 했다.

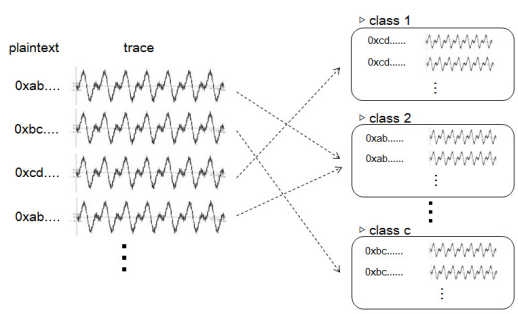

Fig. 4. Trace classification for LDA

3.2 압축대상 구간선정

전력파형에 대한 클래스 분류가 완료되면, 수집된 파형에 대해 압축을 진행할 시점과 구간을 선정해야 한다. 구간과 시점을 정하는 방법은 정형화 되어있는 알고리듬이 존재하는 것은 아니며, 공격자는 알고리즘의 구현방법에 대한 정보나 관련지식을 활용하여 최적의 구간과 시점을 정하게 된다.

압축구간의 단위는 보통 한 클록에 해당하는 크기를 기준으로 배수에 해당하는 길이를 사용하는데, 범용 CPU의 경우 한 명령어 처리에 복수의 클록이 소모되는 것을 고려한다. 한 클록의 길이는 측정 장치의 세팅값이나 파형의 모습을 관찰해 알 수 있다.

공격을 수행하기 위한 목표시점인 POI(Point Of Interest)는 한 개의 파형 또는 몇 개의 파형의 평균파형을 관찰해 정하게 되며, POI선정이 불가능하다면 파형압축은 파형전체를 대상으로 진행한다.

3.3 특징벡터 연산과정

압축대상구간에 포함된 데이터를 압축하기 위한 특징벡터는 다음과 같이 계산한다.

① n개의 수집파형에 대해 압축대상구간의 길이를 m이라고 하자. 해당 구간의 데이터 X는 식(1)과 같이 $n \times m$의 크기를 갖는 행렬로 표현할 수 있다. 이때 각 원소 $x_{i,j}$의 index i,j는 파형번호와 포인트 번호이다.

$$X = \begin{bmatrix} x_{1,1} & \cdots & x_{1,m} \\ \vdots & \ddots & \vdots \\ x_{n,1} & \cdots & x_{n,m} \end{bmatrix} \quad (1)$$

② 파형정보 X를 c개의 클래스로 분류한다. 이때 클래스의 개수 c와 분류방법은 3.1에서 설명한

원리에 따라 정해진다.

$$X_c = \begin{bmatrix} x_{1,1} & \cdots & x_{1,m} \\ \vdots & \ddots & \vdots \\ x_{n_c,1} & \cdots & x_{n_c,m} \end{bmatrix} \quad (2)$$

③ 클래스로 분류된 파형그룹 $X_1, X_2, \ldots X_c$의 평균 파형 $\overline{X_1}, \overline{X_2}, \ldots, \overline{X_c}$과 X전체의 평균파형 $\overline{X}$를 계산한다. 이때, 계산된 평균 파형들은 각각 $1 \times m$의 행렬이 된다.

④ 각 클래스의 공분산 행렬을 더한 값인 within scatter matrix(S_w)와 전체 평균과 각 그룹 평균과의 거리를 더한 값인 between scatter matrix (S_b)를 계산한다. 이 때, N_{X_i}는 각 클래스가 포함하는 파형의 개수 이다. 계산결과인 S_w와S_b는 각각 $m \times m$의 행렬이 된다.

$$S_w = cov(X_1) + cov(X_2) + \ldots + cov(X_c) \quad (3)$$

$$S_b = \sum_{i=1}^{c} N_{X_i} (\overline{X_i} - \overline{X})(\overline{X_i} - \overline{X})^T \quad (4)$$

⑤ S_b는 최대가 되고, S_w는 최소가 되는 방향을 찾기 위해 S_w의 역행렬 S_w^{-1}를 계산하고, 최종적으로 행렬 $S_w^{-1}S_b$에 대해 고유벡터(eigenvector)와 고윳값(eigenvalue)을 계산한다.

3.4 고유벡터의 선택과 파형압축

3.3의 과정 ⑤를 통해 공격자는 m개의 고유벡터를 얻게 된다. 이후, 대응되는 고윳값의 오름차순 크기에 따라 정렬하고, 상위 w개의 고유벡터를 파형압축에 사용하게 된다.

선택한 고유벡터 v를 이용하여 X를 1차원으로 압축한 결과 Y를 계산한다.

$$Y = X \bullet v = \begin{bmatrix} x_{1,1} & \cdots & x_{1,m} \\ \vdots & \ddots & \vdots \\ x_{n,1} & \cdots & x_{n,m} \end{bmatrix} \begin{bmatrix} v_1 \\ \vdots \\ v_m \end{bmatrix} = \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} \quad (5)$$

고유벡터의 순위는 선형판별분석의 성질인 클래스 간의 분산을 크게 만드는 성능과 동일시 할 수 있다. 그러나 실제 파형압축을 통한 공격을 진행해 보면 파형압축에 사용된 고유벡터의 순위와 신호 대 잡음비 값이 항상 비례하는 것은 아님을 확인할 수 있다. 따라서 공격성공률을 높이기 위해서 공격자는 상위 w개의 벡터를 선택하여 파형압축을 진행, 각각을 통해 압축된 데이터를 전력분석에 사용하게 된다.

사용되는 고유벡터의 개수 증가는 공격의 시간 복잡도를 증가시키게 되므로, 높은 신호 대 잡음비 값이 발생하는 고유벡터의 순위를 공격의 성능의 한 요소로 말할 수 있다.

IV. 성능 비교

제안하는 선형판별분석을 이용한 파형압축의 성능을 비교해보기 위해 개발보드에 구현된 암호알고리듬에 대해 전력분석을 진행했다.

4.1 실험환경

다음과 같은 환경에서 전력파형을 수집했으며, 수집된 파형 한 개의 모습은 Fig.5.와 같다. X축은 시간을 나타내며 Y축은 해당 시간에 소모된 전력을 나타낸다. AES가 동작하지 않는 상태에서 파형수집이 시작되어 17,000포인트 정도부터 AES의 동작으로 전력소모가 증가하는 것을 볼 수 있다.

- ◉ 프로세서: S3C2410 (32비트 ARM)
- ◉ 프로세서 동작 주파수: 12 MHz
- ◉ 오실로스코프 : Lecroy WaveRunner 204Xi-A
- ◉ H/W 필터 및 Amplifier : 사용안함
- ◉ Sampling Rate: 200 Msample/sec

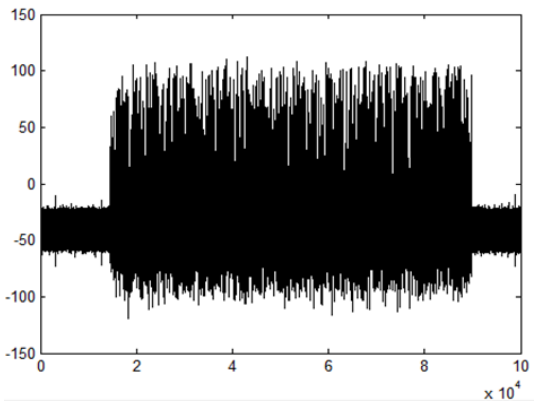

Fig. 5. AES-128 power trace (on S3C2410)
(X-axis: time, Y-axis: power consumption)

◉ 구현 알고리듬: AES-128 Encryption
◉ 한 클록의 길이: 20 포인트
◉ 파형수집 개수: 20,000 개

4.2 실험과정

먼저 압축하지 않은 파형에 대한 상관전력분석을 진행했다. AES 1라운드의 첫 번째 부분키 1바이트를 목표로, S-box출력의 해밍웨이트(hamming weight)를 전력모델로 사용했다. 해당 모델은 추후 압축된 파형을 이용한 공격에도 공통으로 사용했다.

이후, 실험은 선형판별분석과 주성분분석으로 파형을 압축하고 압축한 파형에 대해 상관계수분석을 하는 방법으로 진행되었으며 정량적 비교를 위해 신호 대 잡음비를 함께 계산해 공격 결과와의 연관성을 분석했다. 각 압축기법의 압축단위구간에 따른 성질을 알아보기 위해 압축단위구간은 1클록에 해당하는 20포인트를 기준으로 16클록에 해당하는 320포인트까지 두 배씩 증가시키며 진행했으며, 공격시점은 파형을 압축하지 않고 수행한 상관전력분석의 결과를 이용해 옳은 키의 상관계수가 가장 높았던 시점을 중심으로 하는 한 개의 구간에 대해 진행했다.

신호 대 잡음비는 식(6)과 같이 신호와 잡음 각각에 대한 분산의 비율로 계산되며, 정확한 내부 상태값을 알기위해 올바른 키 정보를 포함하는 전력모델이 사용된다.

$$SNR = \frac{Var(Signal)}{Var(Noise)} \quad (6)$$

식을 구성하는 각 요소는 다음과 같이 계산된다.

◉ Var(Signal) : 수집한 전력파형을 S-box출력의 해밍웨이트(0~8)에 따라 9개 그룹으로 분류한 뒤, 그룹별 평균파형의 분산을 계산
◉ Var(Noise) : 각 전력파형과 S-box출력의 해밍웨이트에 해당하는 평균파형과의 차이를 Noise로 보고, Noise값들의 분산을 계산

4.3 실험결과

압축하지 않은 파형을 이용한 상관계수분석의 결과를 2차원 공간에 표시한 결과는 Fig.6과 같다. X축은 시간을 나타내며, Y축은 해당 시점에서 계산된 상관계수를 나타낸다. 옳은 키에 대한 상관계수는 파란색, 나머지 255개의 틀린 키에 대한 상관계수는 어두운 회색으로 나타냈다.

1라운드의 S-box 연산이 진행되는 부분에서 옳은 키에 대해 높은 상관계수가 발생하지만 틀린 키들의 상관계수들과 구별이 되지 않아 공격이 실패하는 결과를 확인했다. 옳은 키에 대한 상관계수가 복수의 peak로 나타나는 원인은 크게 두 가지로 유추할 수 있다. CPU내부에서 한 명령어가 여러 클록에 걸쳐 처리되기 때문이고, 파형정보에서 연산이 일어나는 시점이 일치하지 않았을 가능성 때문이다.

이후 진행된 압축방법에 따른 상관전력분석의 결과를 표와 그림을 통해 정리했다. Table 1.에 압축방법과 구간에 따라 상위 5개의 특징벡터를 사용해 압축한 파형의 신호 대 잡음비를 계산해 표기했으며, 상관전력분석을 통해 부분키가 찾아진 경우는 음영으로 나타냈다. Table 2.는 신호 대 잡음비와 공격에 필요한 최소 파형개수와의 관계를 알아보기 위해 네 가지 경우에 대해 공격 성공에 필요한 최소 파형개수를 측정한 결과를 나타낸 것이다.

Fig.7.은 파형압축에서 가장 신호 대 잡음비가 좋

Table 1. SNR & attack result using PCA/LDA

Method	Length	Rank of Eigenvector				
		1st	2nd	3rd	4th	5th
LDA	20	0.013	0.004	0.000	0.002	0.015
	40	0.002	0.014	0.008	0.004	0.009
	80	0.046	0.007	0.071	0.023	0.018
	160	0.006	0.094	0.020	0.003	0.051
	320	0.022	0.184	0.070	0.013	0.010
PCA	20	0.013	0.000	0.005	0.003	0.004
	40	0.002	0.005	0.004	0.001	0.004
	80	0.003	0.005	0.002	0.002	0.005
	160	0.002	0.004	0.005	0.002	0.005
	320	0.003	0.007	0.003	0.007	0.003

Table 2. Number of traces required to attack

Method	Length	Rank	SNR	# of Traces
LDA	320	2nd	0.184	500
	80	1st	0.046	1500
PCA	40	2nd	0.005	15000
	80	4th	0.002	18500

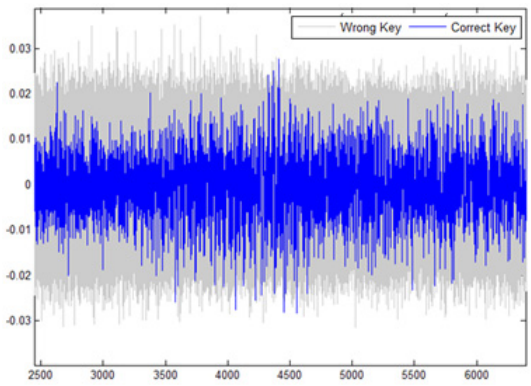

Fig. 6. CPA Result (using 20,000 trace)
(X-axis: time, Y-axis: correlation coefficient)

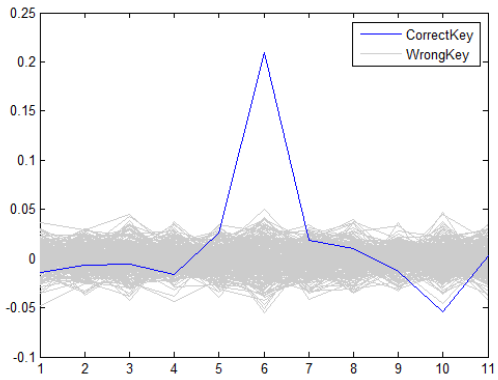

Fig. 7. CPA Result (compressed with LDA)
(X-axis: time, Y-axis: correlation coefficient)

았던 조건을 이용해 압축한 파형의 상관계수분석 결과를 나타낸 것이다. 비교를 위해 Fig.6.과 같은 구간에 대해 공격을 진행했으며, 파형압축에는 선형판별분석방법을 이용해 320포인트 단위로 특징벡터를 계산하고 두 번째 순위의 특징벡터를 이용했다.

실험결과는 다음 세 가지 관점으로 분석해 볼 수 있다.

◉ 신호 대 잡음비 : 선형판별분석을 이용해 압축한 신호가 대체적으로 더 높은 값을 갖는 것을 볼 수 있다. 신호 대 잡음비는 공격이 성공하는 최소 파형개수와 반비례하는 모습을 보여준다. 즉, 높은 신호 대 잡음비를 갖는다는 것은 파형개수가 제한되었을 때 공격성공률이 더 높다는 것을 말한다.

◉ 압축단위구간 : 선형판별분석의 경우 파형압축 단위 구간이 넓어질수록 높은 신호 대 잡음비를 갖는 것을 확인했다. 이를 통해 선형판별분석을 이용한 파형압축은 관심있는 신호가 정렬이 잘 되어있는 경우보다는, 범용 CPU의 특성이나 잡음에 의해 신호가 넓은 구간으로 분산되는 경우에 대한 공격에서 강점을 갖는다는 것을 알 수 있다. 이러한 성질은 좁은 구간에 대한 압축을 진행하는 것 보다 넓은 구간에 대해 압축을 하면서 구간내에 분포된 정보들을 집중시켜 해당 정보를 이용할 수 있는 방법이라는 면에서 의미를 갖는다.

◉ 특징벡터순위 : 압축된 파형을 이용한 상관계수공격이 성공한 특징벡터의 순위를 살펴보면, 선형판별분석을 이용해 계산한 특징벡터의 경우 주성분분석에 비해 상위의 벡터를 사용한 압축에서 공격성공이 더 많이 관찰되는 것을 볼 수 있다. 이는 공격의 효율성이 더 높다는 것을 의미한다.

V. 결 론

본 논문에서는 전력분석 향상을 위한 신호압축에 선형판별분석을 적용하여 기존의 주성분분석을 적용하는 방법과 비교하였다.

선형판별분석은 데이터의 클래스정보를 이용해 최적분류 목적의 특징벡터를 찾는다는 점에서 주성분분석과 다른 성격을 갖는다. 선형판별분석을 전력분석에 적용하기 위해 평문/암호문 정보를 이용해 전력파형의 클래스를 분류하고 신호를 압축하는 방법을 제안했다.

실험을 통해 선형판별분석과 주성분분석의 성능을 비교한 결과, S/W로 구현된 암호알고리듬의 전력파형과 같이 공격의 목표가 되는 신호의 시점이 분산되어 있는 경우에는 신호압축에 선형판별분석을 적용하는 것이 주성분분석을 적용하는 것보다 신호 대 잡음비, 공격성공률, 공격효율성면에서 우수한 성능을 갖는 것을 확인했다.

최근의 고성능 AP(Application Processor)는 많은 부가기능이 탑재되고 저전력으로 설계되어 기존에 사용되고 있는 8비트나 16비트 칩에 비해 신호 대 잡음비가 상대적으로 감소하는 양상을 보인다. 또한 S/W구현은 의도적으로 분기문 없이 수행되도록 구현하지 않았다면 값에 의존하는 분기문에 의해 동일한 암호연산일 경우에도 동작 클록수에 변동이 발생하게 되며, OS(Operating System)위에 암호

연산이 탑재되었을 경우는 OS단에서 암호연산과 독립적으로 발생하는 주기적인 인터럽트(interrupt)나 작업관리자의 개입으로 인해 일반적으로 공격목표 시점이 정확하게 일치하지 않는다. 따라서 공격목표 시점이 분산되어 있는 상황에서 이점을 갖는 선형판별분석을 이용한 파형압축은 최신 IT환경에 적용될 수 있는 부채널 분석 향상기법이라고 할 수 있다.

본 논문에서 성능비교를 위해 언급한 주성분분석은 신호압축 이외에도 파형선별[12], 옳은 키 선별을 위한 구별자[13]등 전력분석의 다양한 부분에 적용되고 있다. 선형판별분석을 해당 부분에 적용해 성능을 비교하는 것이 추후 연구과제이다.

References

[1] P. C. Kocher, J. Jae, and B. Jun., "Timing Attacks on Implementations of Die-Hellman, RSA, DSS, and Other Systems," CRYPTO 1996, LNCS 1109, pp. 104-113, Springer-Verlag, 1996.

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

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

[4] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi., "The EM Side-Channel(s)," CHES 2002, LNCS 2524, pp. 29-45, 2003.

[5] A. Moradi, MTM. Shalmani, M. Salmasizadeh, "A Generalized Method of Differential Fault Attack Against AES Cryptosystem," CHES 2006, LNCS 4249, pp. 91-100, 2006.

[6] S. Mangard, E. Oswald, and T. Popp, "Power Analysis Attacks: Revealing the secrets of smart cards," pp, 82-86, Springer, 2007.

[7] PN Belhumeur, JP Hespanha, DJ Kriegman, "Eigenfaces vs. Fisherfaces: Recognition using class specific linear projection," IEEE Transactions on pattern analysis and machine intelligence, VOL 19, No. 7, 1997.

[8] E. Oswald and P. Rohatgi, "Using Subsapce-Based Template Attacks to Compare and Combine Power and Electromagnetic Information Leakages," CHES 2008, LNCS 5154, pp. 411-425, 2008.

[9] O. Choudary, M. G. Kuhn, "Efficient Tmeplate Attacks," CARDIS 2013, LNCS 8419, pp. 253-270, 2014.

[10] S. Mangard, E. Oswald, and T. Popp, "Power Analysis Attacks: Revealing the secrets of smart cards," pp, 73-79, Springer, 2007.

[11] L. Batina, J. Hogenboom, Jasper G.J. van Woudenberg, "Getting More from PCA: First Results of Using Principal Component Analysis for Extensive Power Analysis," CT-RSA 2012, LNCS 7178, pp.383-397, 2012.

[12] Y. Kim, H. Ko, "Using Principal Component Analysis for Practical Biasing of Power Traces to Improve Power Analysis Attacks,"ICISC 2013, 2013.

[13] Y. Souissi, M. Nassar, S. Guilley, J. Danger, F. Flament, "First Principal Components Analysis: A New Side Channel Distinguisher," ICISC 2010, LNCS 6829, pp. 407-419, 2011.

〈저자소개〉

강 지 수 (Ji-su Kang) 정회원
2008년 2월: 한양대학교 전자전기공학전공 졸업
2008년 3월~현재: 삼성전자 DS부문 SYS.LSI 사업부 연구원
2013년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 암호 연산기 최적화 구현, 부채널 분석 및 대응법

김 희 석 (HeeSeok Kim) 정회원
2006년: 연세대학교 수학과 학사
2008년: 고려대학교 정보보호대학원 공학석사
2011년: 고려대학교 정보보호대학원 공학박사
2011년 9월~2012년 12월: Bristol University 박사후 연구원
2013년~현재: 한국과학기술정보연구원 (KISTI) 과학기술정보보호실 선임연구원
〈관심분야〉 부채널 공격, 암호시스템 안전성 분석 및 고속구현, 암호칩 설계 기술, 보안관제, 네트워크 보안

홍 석 희 (Seokhie Hong) 종신회원
1995년 : 고려대학교 수학과 학사
1997년 : 고려대학교 수학과 석사
2001년 : 고려대학교 수학과 박사
1999년 8월~2004년 2월 : (주)시큐리티 테크놀로지스 선임연구원
2003년 3월~2004년 2월 : 고려대학교 정보보호기술연구센터 선임연구원
2004년 4월~2005년 2월 : K.U. Leuven ESAT/SCD-COSIC 박사후연구원
2005년 3월~2013년 8월: 고려대학교 정보보호대학원 부교수
2013년 9월~현재 : 고려대학교 정보보호대학원 정교수
〈관심분야〉 대칭키 암호 알고리즘, 공개키 암호 알고리즘, 디지털 포렌식