Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.6, Dec. 2016 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2016.26.6.1461

부채널 분석 성능향상을 위한 특이값분해 신호처리 기법에 관한 연구*

박 건 민,[1†] 김 태 원,[2] 김 희 석,[1‡] 홍 석 희[1]
[1]고려대학교, [2]SNTWORKS

Study on Singular Value Decomposition Signal Processing Techniques for Improving Side Channel Analysis*

Geonmin Bak,[1†] Taewon Kim,[2] HeeSeok Kim,[1‡] Seokhie Hong[1]
[1]Korea University, [2]SNTWORKS

요 약

부채널 분석에서 신호처리 기법은 차원 압축이나 잡음 제거를 통해 분석의 효율성과 성능을 높일 수 있는 전처리 기법이다. 특이값 분해를 이용한 신호처리 방법은 신호의 분산 정보나 경향성 등을 이용하여 주 신호 정보를 높이고 잡음 신호를 낮출 수 있어, 분석 성능 향상에 큰 도움이 된다. 대표적인 기법은 주성분분석과 선형판별분석 그리고 Singular Spectrum Analysis(SSA)가 있다. 주성분분석과 선형판별분석은 주 신호의 정보를 집약하여 차원 압축을 할 수 있으며, SSA는 본 신호를 주 신호와 잡음 신호로 분해하여 잡음 제거가 가능하다. 세 가지 기법 각각을 사용하거나 조합하여 사용할 경우 성능적인 측면을 비교할 필요가 있으며, 그에 대한 방법론이 필요하다. 본 논문에서는 세 기법을 개별적으로 사용할 경우와 조합하여 사용할 경우의 성능을 비교 분석하였으며, 신호 대 잡음비를 이용한 비교분석 방법론을 제시하였다. 제시한 방법론과 다양한 비교분석 실험을 통해 각 기법의 성능과 효율성을 확인하였다. 이로 인해 부채널 분석 분야의 많은 연구자들에게 유용한 정보를 제공할 것이다.

ABSTRACT

In side channel analysis, signal processing techniques can be used as preprocessing to enhance the efficiency and performance of analysis by reducing the noise or compressing the dimension. As signal processing techiniques using singular value decomposition can increase the information of main signal and reduce the noise by using the variance and tendency of signal, it is a great help to improve the performance of analysis. Typical techniques of that are PCA(Principal Component Analysis), LDA(Linear Discriminant Analysis) and SSA(Singular Spectrum Analysis). PCA and LDA can compress the dimension with increasing the information of main signal, and SSA reduces the noise by decomposing the signal into main siganl and noise. When applying each one or combination of these techniques, it is necessary to compare the performance. Therefore, it needs to suggest methodology of that. In this paper, we compare the performance of the three technique and propose using Sinal-to-Noise Ratio(SNR) as the methodology. Through the proposed methodology and various experiments, we confirm the performance and efficiency of each technique. This will provide useful information to many researchers in the field of side channel analysis.

Keywords: Side channel analysis, Principal Component Analysis, Linear Discriminant Analysis, Singular Spectrum Analysis, Preprocessing, Singular Value Decomposition

Received(10. 18. 2016), Modified(11. 17. 2016), Accepted(11. 23. 2016)

* 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학 ICT연구센터육성 지원사업의 연구결과로 수행되었음. (IITP-2016-R0992-16-1017)

† 주저자, bgm586@naver.com
‡ 교신저자, 80khs@korea.ac.kr(Corresponding author)

I. 서 론

부채널 분석(side channel analysis)은 기기에서 암호알고리즘이 동작할 때 설계자가 의도하지 않은 정보의 발생을 이용하여 비밀정보를 알아내는 방법이다. 수학적으로 공격이 어려운 알고리즘이라도 부채널 정보를 통해 어렵지 않게 공격이 가능하거나 취약점을 발견할 수 있다. 이러한 부채널 분석의 대표적인 방법에는 연산에 소요되는 시간정보를 이용하는 시간 분석(timing attack)[1], 연산 시 발생하는 전력소모량을 이용하는 전력 분석(power analysis)[2][8], 기기에서 발생하는 전자기파를 이용하는 전자기파 분석(electronic magnetic analysis)[3]이 있다. 다양한 방식으로 부채널 분석에 대한 관심과 연구가 증가하게 되면서 부채널 분석에 대한 안전성이 암호연산 기기에 대한 안전성 검증에 추가 기준이 되었으며, 암호알고리즘의 설계에도 중요한 고려대상이 되었다.

부채널 분석은 이용하는 정보의 질에 따라 분석 여부와 효율이 달라질 수 있다. 이에 따라 정보의 질을 향상시킬 수 있는 준비과정인 전처리(preprocessing) 과정이 부채널 분석의 중요 요소가 된다. 전처리란 수집한 데이터의 본질적인 정보를 쉽게 추출할 수 있도록 이용하고자 하는 부분 패턴을 선택하거나 이 부분 패턴을 고정하여 불필요한 정보를 제거하기 위한 예비적인 조작단계이다. 부채널 분석에서는 파형에 대해 다양한 신호처리 기법을 전처리로 적용하여 파형의 정보량을 증가시키는 것이 가능하다. 전력 분석에서 사용하는 신호처리 기법들에는 잡음제거(noise reduction)[16], 파형압축(compression of power traces)[4], 파형정렬(alignment of power traces)[15]등이 있다.

본 논문에서는 신호처리 적용과정에 특이값 분해(singular value decomposition)를 이용하는 기법에 대해 다룬다. 특이값 분해는 신호처리와 통계학 분야 등에서 자주 사용되며 행렬을 특이벡터들로 구성된 행렬과 특이값을 원소로 갖는 행렬의 곱으로 나타내는 방법이다. 특이값 분해를 이용하는 신호처리 기법들 중 부채널 분석 분야에서 사용하는 대표적인 기법은 주성분분석(Principal Component Analysis, PCA), 선형판별분석(Linear Discriminant Analysis, LDA)과 Singular Spectrum Analysis(SSA)가 있다. 주성분분석과 선형판별분석은 파형압축으로 사용가능하며 SSA는 잡음제거로 사용가능하다.

주성분분석은 파형압축을 통해 잡음을 제거하고 파형의 정보량을 높여 전력 분석 성능을 높일 수 있다[5]. 선형판별분석은 템플릿공격의 프로파일링 단계에 적용하여 차원을 줄여 성능과 효율을 높이는 것이 가능하며[6][10], 가장 이상적인 차원축소 방법으로도 제시되었다[9]. 또한, 신호 대 잡음비(Signal to Noise Ratio, SNR)를 증가시켜 전력 분석 성능을 향상시킨 경우가 있다[12]. SSA는 프로파일링 과정이 필요 없는 잡음제거 기법으로 제시되었다[7]. 그러나 세 기법을 비교분석한 기존연구가 없으며, 조합이 가능한지 확인할 필요가 있다.

본 논문은 이러한 특이값 분해를 이용하는 신호처리 기법들을 단일로 사용하거나 조합하여 사용할 경우에 대한 비교 분석을 하였다. 각 기법들의 성능 비교를 위한 방법론으로 신호 대 잡음비를 확인하는 것을 제안하였으며, 대칭키 암호알고리즘 AES(Advanced Encryption Standard)를 구현한 실제 보드(board)의 전력소비량 파형을 이용한 실험을 진행하였다. 전처리 기법을 처리한 파형들에 대하여 신호 대 잡음비를 계산하여 비교하였고, 방법론의 검증을 위하여 상관전력분석(Correlation Power Analysis, CPA)[8]을 통해 성능비교를 하였다.

본 논문의 구성은 다음과 같다. 2장에서는 앞서 제시한 특이값 분해를 이용하는 신호처리 기법들에 대해 살펴본다. 3장에서는 제안하는 비교분석 방법론을 적용하기 위한 각 신호처리 기법들의 적용 방법과 특징을 설명하며, 4장에서는 전처리 기법들을 비교한 실험결과를 제시한다. 마지막으로 5장에서는 결론을 기술한다.

II. 관련연구

2.1 주성분분석

주성분분석은 다차원으로 구성된 데이터들에 대하여 높은 차원에서의 정보를 유지하면서 낮은 차원으로 차원을 축소시키는 데이터 압축 방법이다. 전체 데이터들의 분산을 최대로 만드는 축으로 데이터를 사영시켜 데이터의 차원을 줄일 수 있다.

주성분분석을 적용하기 위해서는 먼저 각 다변량 데이터를 정규화(normalization)해야 한다. 다변량 데이터 $A=[a_1,a_2,...,a_m]$와 데이터의 평균 값

$w=\frac{1}{m}\sum_{i=1}^{m}a_i$에 대하여 정규화한 A는 $[a_1-w, a_2-w, ..., a_m-w]$가 된다. 다음으로 m차원의 데이터 k개에 대하여 $k\times m$행렬 X를 구성한다. 즉, 행렬 X의 각 행이 m차원의 데이터 하나가 된다. 이후, 행렬 $B=cov(X)$를 계산한 후 행렬 B에 대한 특이값 분해를 한다. 행렬 B는 $m\times m$ 정방행렬이므로, $B=U\times D\times U^{-1}$을 만족하고 U의 각 열은 B의 고유벡터(eigen vector), D는 대각성분이 고유값(eigen value)인 대각행렬이 된다. 차원축소를 하기 위해서는 m개의 고유벡터 중 축소시킬 차원 수만큼의 고유벡터를 선택하여 구성한 행렬을 다변량 데이터에 곱해준다. U의 각 열을 $u_i(1\le i\le m)$라 할 때, p개의 고유벡터로 구성된 $U^*=[u_1 u_2 \cdots u_p]$을 다변량 데이터 A에 곱한 $A^*=A\times U^*$가 차원이 m에서 p로 축소된 새로운 데이터가 된다. 고유값은 해당하는 고유벡터를 이용하여 사영한 데이터의 분산이므로, 고유값이 클수록 데이터의 특성을 잘 표현할 수 있는 고유벡터이다. 주성분분석을 이용하여 전력파형의 압축을하기 위해서는 다수의 파형이 필요하게 된다. 다수의 전력파형을 이용하여 주성분분석을 통해 각 파형에 곱해줄 가중치 벡터를 찾게 되며, 파형의 값이 시점에 따라 다른 가중치를 얻게 된다.

2.2 선형판별분석

선형판별분석은 주성분분석과 유사한 방식을 통해 차원축소를 하지만 개념상의 차이점이 존재한다. 주성분분석은 데이터 전체의 분산이 최대가 되는 방향의 벡터를 찾는 반면, 선형판별분석은 데이터의 클래스 간의 분산을 최대로 할 수 있는 벡터를 찾는다. 선형판별분석은 클래스 내부의 분산은 최소화하면서 클래스 간의 분산은 최대화할 수 있는 방향의 벡터를 이용한다. 쉽게 말하면 주성분분석은 데이터의 최적표현의 관점으로 차원축소를 하고, 선형판별분석은 데이터의 최적분류의 관점으로 차원축소를 한다. Fig.1.을 통해 주성분분석과 선형판별분석의 차이를 확인할 수 있다. Fig.1.에서는 별모양(*)과 동그라미모양(○) 두 클래스의 2차원 데이터를 확인할 수 있다. 오른쪽 방향의 얇은 대각선 축이 주성분분석으로 찾을 수 있는 이상적인 방향의 벡터가 되며, 왼쪽 방향의 두꺼운 대각선 축이 선형판별분석으로 찾을 수 있는 이상적인 방향의 벡터가 된다. 그림에서 알 수 있듯이 주성분분석은 데이터의 클래스 구분과 관계없이 데이터 전체의 분산이 최대가 될 수 있는 벡터를 구하며, 선형판별분석은 데이터의 클래스 분류를 최대로 할 수 있는 벡터를 구한다. 따라서 선 형판별분석을 적용하기 위해서는 데이터의 클래스 정보를 얻는 것이 필요하다.

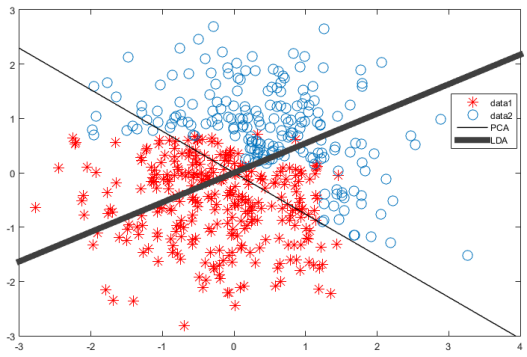

Fig. 1. The difference between PCA and LDA in 2-dimensions

다음은 선형판별분석을 이용한 데이터의 차원축소 방법이다. n개의 클래스를 갖는 다수의 m차원 데이터에 대해서, 각 클래스의 데이터 수를 $k_i(1\le i\le n)$라 하자. 각 클래스의 전체 데이터를 X_i라고 표현하면, X_i는 $k_i\times m$ 행렬이 된다. 선형판별분석을 위해서는 클래스 내 분산 행렬(within-class scatter matrix)과 클래스 간 분산 행렬(between-class scatter matrix)이 필요하다. 클래스 내 분산 행렬 S_w는 각 클래스의 공분산 행렬의 합으로 구한다. 즉, $S_w=cov(X_1)+cov(X_2)+...+cov(X_n)$와 같이 구하며 $m\times m$의 크기를 갖는다. 클래스 간 분산 행렬 S_b는 전체 클래스의 평균과 각 클래스의 평균 사이의 거리들을 더하여 구한다. 클래스 i의 평균을 $1\times m$행렬 $\overline{X_i}(1\le i\le n)$라 하면 전체 클래스의 평균은 $\overline{X}=\frac{1}{n}\sum_{i=1}^{n}\overline{X_i}$가 된다. 이를 통하여 클래스 간 분산 행렬은 $S_b=\sum_{i=1}^{n}k_i\left(\overline{X_i}-\overline{X}\right)^T\left(\overline{X_i}-\overline{X}\right)$와 같이 구할 수 있다. S_w는 최소화하고 S_b는 최대화할 수 있는 방향의 벡터는 $S_w^{-1}S_b$ 의 특이값 분해를 이용하여 구할 수 있다. $S_w^{-1}S_b$ 의 고유값과 이에 따른

고유벡터를 계산하여, 주성분분석 방법처럼 고유벡터 p개로 구성한 행렬을 데이터에 곱하여 차원을 m에서 p로 축소한다.

2.3 Singular Spectrum Analysis

Singular Spectrum Analysis(SSA)는 CHES 2015에서 부채널 분석에 처음으로 도입한 신호처리 기법이다[7]. 경제학, 통계학, 기상학 등 다양한 분야에서 사용하는 방법으로, 데이터의 주기성과 경향성, 변동성을 분석하여 데이터를 분해할 수 있는 기법이다. 부채널 분석에서는 SSA를 이용하여 전력파형를 여러 개의 파형으로 분해하여 주 신호와 잡음 신호로 구분지어 잡음을 제거하는 전처리 기법으로 사용한다. SSA는 주성분분석, 선형판별분석과는 다르게 단일 파형에 적용이 가능한 방법이다. 즉, 파형의 클래스 정보나 다수의 파형 정보가 필요 없다.

SSA는 크게 분해(decomposition)와 재결합(reconstruction) 두 단계로 진행하며, 각 단계도 두 단계로 이루어져 세부적으로는 총 네 단계로 진행한다. 분해 단계는 embedding과 특이값 분해(Singular Value Decomposition, SVD)로 구성되며, 재결합 단계는 diagonal averaging과 grouping으로 구성된다.

① embedding단계는 하나의 파형을 궤적행렬(trajectory matrix)형태로 변환하는 과정으로, 파형의 정보를 파악하기 위한 윈도우(window, 단위구간)의 크기 설정이 필요하다. 길이 m의 파형 $a=[a_1,a_2,...,a_m]$에 대하여 궤적행렬 A는 식(1)과 같이 구성한다.

$$A=\begin{pmatrix} a_1 & a_2 & \cdots & a_D \\ a_2 & a_3 & \cdots & a_{D+1} \\ \vdots & \vdots & \ddots & \vdots \\ a_W & a_{W+1} & \cdots & a_m \end{pmatrix} \quad (1)$$

여기서 W는 윈도우의 크기이며, $D=m-W+1$을 만족한다.

② 특이값 분해 단계에서는 A에 대한 특이값 분해를 진행한다. $A\times A^T$에 대한 고유값을 $\lambda_i(1\le i\le W)$라 하고, 그에 따른 고유벡터를 $u_i(1\le i\le W)$라 하자. $\lambda_1\ge\lambda_2\ge ...\ge\lambda_W$ 를 만족하도록 고유값과 고유벡터를 재배열한다. 그 후 식(2)를 만족하는 A_i를 구성하며, $A_i=\sqrt{\lambda_i}\,u_iv_i^T$와 $v_i=\dfrac{A^Tu_i}{\sqrt{\lambda_i}}$ 를 만족한다. 이로써, λ_i에 따라 A를 분해한다.

$$A=A_1+A_2+...+A_W \quad (2)$$

③ 다음으로 분해한 A_i를 파형의 형태로 다시변환하기 위해 diagonal averaging단계를 진행한다. 식(1)처럼 역 대각 성분이 동일한 형태의 행렬은 길이 m의 파형으로 변환이 가능하다. 식(2)의 A_i들을 이와 같은 형태로 변환하는 단계가 diagonal averaging이다. 역 대각 성분이 동일한 형태로 만들기 위해 각 역 대각의 성분의 평균을 각 역 대각의 성분들로 치환한다. 역 대각 성분이 치환된 행렬은 embedding단계의 반대 방법으로 파형의 형태로 변환한다.

④ 마지막 grouping단계에서는 파형 형태로 변환한 A_i들을 주 신호와 잡음신호로 구분한다. 고유값 λ_i의 크기를 기준으로 주 신호와 잡음 신호 분류하여 두 분류 각각의 합을 계산한다. 이러한 과정의 SSA를 전력파형에 적용하여 파형의 잡음을 제거한다.

III. 제안하는 비교분석 방법론

앞선 장들에서 보았듯이 주성분분석과 선형판별분석, SSA는 특이값 분해를 이용하고 신호의 정보량을 향상시킬 수 있다는 공통점을 가지고 있다. 이에 따라 세 가지 기법의 성능비교가 필요하며, 조합하여 사용할 경우 상호간의 조화를 이루는지 혹은 충돌이 생기는지 살펴볼 필요가 있다. 본 장에서는 이 기법들을 단일 혹은 조합하여 사용할 때 적용방법과 성능비교를 위한 방법론을 설명한다.

3.1 전처리과정

주성분분석과 선형판별분석, SSA는 모두 특이값 분해를 이용하지만, 차이점이 분명히 존재한다. 주성분분석과 선형판별분석은 파형의 정보량을 증가시키지만, 본래의 목적은 파형압축이다. 반면, SSA는 잡음제거가 목적이다. 적용의 목적이 다른 만큼 변환된 파형의 형태도 상이하다. 주성분분석과 선형판별분석은 파형압축을 위한 벡터를 찾아 파형에 곱해지는 선

형변환이며 이로 인해 변환된 파형은 본래의 파형과는 다른 형태의 모습을 갖게 된다. 이와 달리 SSA는 파형을 여러 개의 파형으로 분해하여 분류를 한 후 재합성하는 형태이기 때문에, 본래의 파형과 유사한 형태를 갖는다. 따라서 세 기법을 조합할 경우 주성분분석과 선형판별분석을 같이 사용하는 방법은 벡터를 곱해 변형된 파형에 대해 또 다른 벡터를 찾는 것이 무의미하기 때문에 옳지 않다. 또한, 주성분분석이나 선형판별분석을 적용한 후 SSA를 적용하는 방법은 파형의 왜곡을 가져오기 때문에 이 역시 옳은 방법이 아니다. 그러므로 세 기법을 조합하는 것은 SSA를 적용한 후 주성분분석이나 선형판별분석의 적용이 올바른 방법이다. 이러한 각 기법의 성질을 토대로 조합을 통한 조화를 이룰 수 있는지 알아보기 위해 다섯 가지의 전처리를 수행하였으며, 해당 과정은 Fig.2.를 통해 확인할 수 있다. 이는 SSA, 주성분분석, 선형판별분석을 단일로 적용한 세 가지와 SSA를 적용한 후 주성분분석을 통한 압축, SSA를 적용한 후 선형판별분석을 통한 압축으로 총 다섯 가지의 전처리를 진행한 것이다.

주성분분석과 선형판별분석 같은 파형압축 방법은 보통 기기의 동작 클록에 해당하는 크기의 배수를 단위 길이로 하여 압축을 진행한다. 이는 일반적인 CPU가 명령어 하나를 처리할 때 복수의 클록이 필요하기 때문이다. 본 논문에서는 각 보드의 클록에 해당하는 시점들을 단위 길이로 하여 주성분분석과 선형판별분석을 진행하였다. 또한 파형에서 클록이 시작되는 위치를 정확히 알지 못하므로 단위길이를 한 시점씩 이동해가며 압축을 진행하였다. 이는 파형의 길이를 줄이는 방법이 아니지만 세 기법의 성능 비교를 더 정확하게하기 위해 진행하였다. 주성분분석과 선형판별분석에는 주요 변수로 특이값 분해 이후 선택하는 고유값에 의한 고유벡터가 있다. 선택하는 고유벡터에 따라 분석의 성능이 달라지기 때문에 이에 대한 연구가 여전히 진행 중[13]이며 정확한 기준이 없다. 그러나 고유값의 크기가 클수록 파형의 정보량을 높이는 고유벡터라는 통념이 있으며, 식(3)의 전체 고유값에 대한 선택하는 고유값의 비율을 이용하여 이 값이 일정 수치를 넘게 하는 고유값들을 이용하는 방법이 자주 이용된다. 식(3)의 λ_i는 고유값을 나타내고 총 m개이며, p는 선택하는 고유값의 개수를 나타낸다. PCA와 LDA의 경우 선택하는 고유값이 변수가 되며, 일반적으로 고유값이 큰 경우 의미를 갖는다. 단일의 고유값을 선택할 수도 있지만, 논문에서는 가장 성능이 좋은 PCA, LDA를 이용하는 경우를 가정하기위해 식(3)의 값이 0.95이상이 되는 값들을 선택하였다. 이는 최적의 고유값 하나를 선택해야 하는 고충을 없애고 효과적인 성능비교를 가능하게 한다.

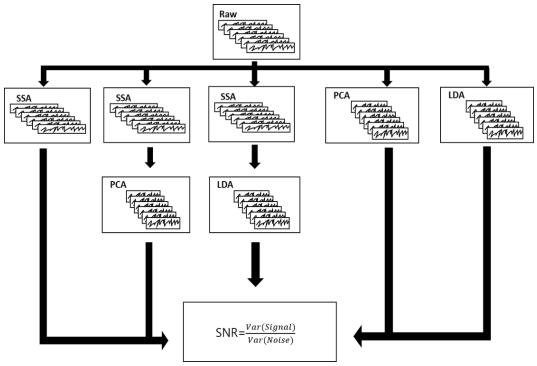

Fig. 2. Experimental procedure (Raw: without preprocessing)

$$\phi(p)=\frac{\sum_{i=1}^{p}\lambda_i}{\sum_{i=1}^{m}\lambda_i}, where\ 1\le p\le m \tag{3}$$

SSA의 경우 2.3절에서 알 수 있듯이 윈도우의 크기와 주 신호로 선택할 고유값이 중요한 변수가 된다. 본 논문에서는 윈도우의 크기를 클록에 해당하는 시점크기의 배수로 변화시키며 사용하였다. 선택하는 고유값은 가장 큰 것부터 하나 혹은 다수를 선택하거나 식(3)의 값이 0.95이상이 되게 하는 것들을 선택하였다. 이를 통해 변수에 따른 성능이 좋았던 SSA 방법에 대해서 주성분분석과 선형판별분석을 적용하였다.

3.2 신호 대 잡음비를 이용한 성능비교

신호 대 잡음비(Signal to Noise Ratio, SNR)는 부채널 분석에서 전력파형의 정보량을 비교하기 위한 지표로써 자주 이용한다[11]. 본 논문에서는 특이값 분해를 이용하는 전처리에 대한 비교를 위한 지표로 SNR을 제안한다. SNR은 식(4)와 같이 나타낼 수 있다.

$$SNR = \frac{Var(Signal)}{Var(Noise)} \quad (4)$$

식(4)의 $Var(Signal)$은 주 신호의 분산을 나타내며 $Var(Noise)$는 잡음 신호의 분산을 나타낸다. 주 신호의 분산은 연산 중간 값에 따라 전력파형을 분류하여 분류한 각 클래스의 평균파형들의 분산으로 계산할 수 있으며, 잡음 신호의 분산은 각 파형과 해당하는 클래스의 평균파형의 차이를 잡음 신호로 하여 모든 잡음 신호들의 분산으로 계산할 수 있다. 이때 분류의 기준이 되는 중간 값은 S-box출력의 해밍웨이트(hamming weight)혹은 해밍디스턴스(hamming distance)를 이용한다.

S-box출력 1바이트에 대한 해밍웨이트를 분류 기준으로 하여 SNR을 계산하는 방법은 다음과 같다. 1바이트의 해밍웨이트는 0부터 8까지 9개의 값을 가지므로 9개의 클래스로 파형을 분류할 수 있다. $C_k\,(0 \le k \le 8)$를 해밍웨이트가 k인 파형 X_i들의 인덱스 i의 집합이라 하고, $E_k(0 \le k \le 8)$를 해밍웨이트가 k인 파형들의 평균파형이라 하자. $E = \{E_0, E_1, E_2, E_3, E_4, E_5, E_6, E_7, E_8\}$라 하면 $Var(Signal) = Var(E)$와 같다. 또한, $Y = \{\, Y_i |\, Y_i = X_i - E_k \text{ for } all\ i \in C_k \ \ where\ 0 \le k \le 8\}$라 하면 $Var(Noise) = Var(Y)$가 된다. 이를 통해 식(4)의 SNR값을 계산할 수 있다.

부채널 분석성능은 파형의 정보량에 비례하므로 전처리 기법의 성능비교 방법으로 SNR을 이용하는 것은 타당한 방법이다.

IV. 실험 결과

본 장에서는 실제 보드를 통해 수집한 전력파형을 대상으로 세 전처리 기법을 혼합 적용하여 성능비교를 하였다. 대응기법이 없는 AES-128비트 알고리즘이 구현된 세 종류의 보드를 대상으로 실험하였다. SAKURA-G와 SASEBO-G2보드의 경우 FPGA상에 구현되어있으며, MSP430보드의 경우 소프트웨어를 통해 구현되었다. 3장에서 제시한 방법론을 적용하여 성능비교를 하였으며, 방법론의 검증을 위하여 상관전력분석을 진행하였다. 실험의 과정은 앞선 Fig.2.와 같다.

4.1 SAKURA-G

SAKURA-G보드를 통해 수집한 전력파형의 경우 AES-128비트의 10개 라운드 연산이 일어나는 모든 부분이 나타나도록 파형을 수집하였으며, 수집한 파형의 형태는 Fig.3.과 같다. 오실로스코프는 Lecroy WaveRunner 204Xi-A를 이용하였으며, 5000개의 파형을 수집하였다. sampling rate는 10GS/s이며, 사용된 FPGA의 클록 주파수는 48MHz이다. 따라서 클록에 해당하는 시점 수는 약 208이 된다. SSA에 사용한 윈도우 크기는 클록의 길이로 하며, 고유값은 두 번째로 큰 값을 선택한 것이 성능이 좋았다. SNR을 측정하기 위한 분류의 기준인 중간 값은 하드웨어 파형이기 때문에 10라운드의 S-box 입력 값 첫 바이트와 암호문 첫 바이트 사이의 해밍디스턴스를 사용하였다. table 1.은 전처리 방법에 따른 SNR의 값, 상관전력분석의 최대 상관계수의 값을 나타낸 것이며, 전처리 중 raw는 수집한 파형의 원본을 뜻한다. 이를 통해 SNR과 상관계수의 값이 비례한 결과를 나타냄을 알 수 있다. 전처리의 경우 선형판별 분석을 단일로 사용할 경우 SNR이 가장 높음을 보인다.

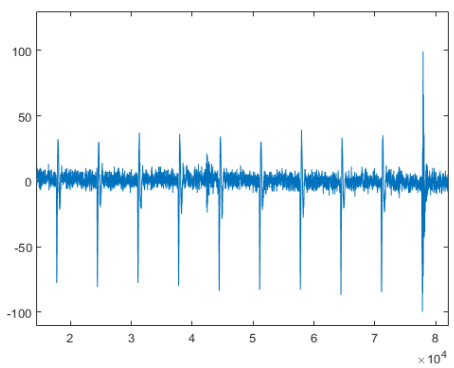

Fig. 3. AES-128 power trace(SAKURA-G)

Table 1. SNR & correlation of CPA (SAKURA-G)

preprocessing	SNR	correlation
Raw	0.0389	0.1006
PCA	0.0779	0.1156
LDA	0.1037	0.1345
SSA	0.0918	0.1309
SSA+PCA	0.0998	0.1309
SSA+LDA	0.0971	0.1327

4.2 SASEBO-G2

SASEBO-G2 파형은 DPA contest v2[14]에서 제공하는 파형 20000개를 실험에 이용하였다. AES-128비트의 10개 라운드 연산이 일어나는 모든 부분을 포함하고 있으며, 파형의 형태는 Fig.4.와 같다. sampling rate는 5GS/s이며, 사용된 FPGA의 클록 주파수는 24MHz이다. 이를 통해 클록에 해당하는 길이가 약 208임을 알 수 있다. 윈도우 크기는 클록 길이로 하며 두 번째로 큰 고유값을 선택한 SSA가 성능이 좋았다. SNR을 측정하기 위한 분류 기준은 SAKURA-G와 같은 방식을 사용하였다. table 1.과 같은 방식으로 table 2.에 성능비교를 정리하였다. SAKURA-G의 경우와 비슷한 성능비교 결과를 나타내었으며, 선형판별분석의 단일 적용이 가장 성능이 좋았다.

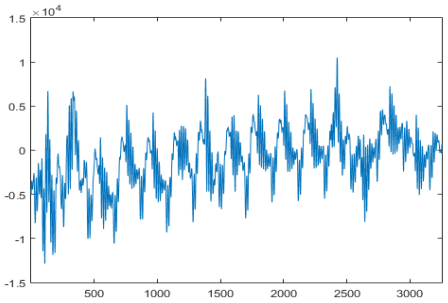

Fig. 4. AES-128 power trace(SASEBO-G2)

Table 2. SNR & correlation of CPA (SASEBO-G2)

preprocessing	SNR	correlation
Raw	0.0088	0.0619
PCA	0.0124	0.0746
LDA	0.0175	0.0829
SSA	0.0149	0.0741
SSA+PCA	0.0144	0.0722
SSA+LDA	0.0165	0.0776

4.3 Scarf MSP430

다음은 부채널 검증 보드 scarf-MSP430[17]에 대한 실험 결과이다. 대응기법이 없는 AES-128비트 알고리즘을 소프트웨어를 이용하여 구현하였으며, 전력파형은 첫 번째 라운드에 해당하는 부분을 수집하였다. 오실로스코프는 Lecroy WaveRunner 204Xi-A를 이용하였으며, 5000개의 파형을 이용하였다. sampling rate는 200MS/s이며, 사용된 프로세서의 동작 주파수는 8MHz이다. 클록에 해당하는 시점 수는 25이며, 파형의 형태는 Fig.5.와 같다. SSA는 윈도우 크기를 클록 길이로 사용하고 식 (3)이 0.95이상인 고유값을 이용한 경우가 성능이 좋았다. 해당 파형은 소프트웨어 파형이므로 첫 번째 라운드 S-box 출력 값 첫 바이트의 해밍웨이트를 분류 기준으로 하여 SNR을 측정하였다. 각 기법의 비교결과는 table 3.와 같다. 해당 결과 역시 SNR과 상관계수의 값이 상응하는 것을 보이며, 선형판별분석이 가장 좋은 성능을 보였다.

V. 분석 및 결론

본 논문에서는 특이값 분해를 이용하는 신호처리 방법을 전력분석을 위한 전처리 기법으로 적용하여 각 기법의 성능을 실험을 통해 비교하였다. 각 기법을 단일로 사용하거나 조합하여 사용할 때 적용하는 과정을 설명하였으며, 성능의 비교를 위한 방법론으로 SNR의 비교를 제시하였다.

실제 보드를 통해 수집한 전력파형을 이용하여 실

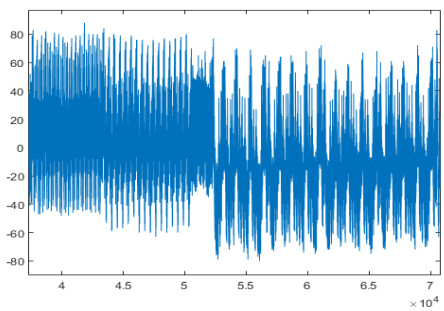

Fig. 5. AES-128 power trace(MSP430),1Round

Table 3. SNR & correlation of CPA (MSP430)

preprocessing	SNR	correlation
Raw	2.88	0.63
PCA	6.99	0.78
LDA	11.80	0.86
SSA	6.81	0.78
SSA+PCA	6.59	0.77
SSA+LDA	8.52	0.81

험을 진행하였으며, 각각의 실험결과를 제시하였다. SNR을 통한 성능을 비교한 결과, 주성분분석, 선형판별분석 그리고 SSA를 단일로 적용할 경우에는 선형판별분석의 성능이 가장 좋았다. SSA와 주성분분석, SSA와 선형판별분석을 조합할 경우 SSA만을 적용한 경우보다 성능이 상승하지만, 선형판별분석만을 적용한 경우와 비슷하거나 낮은 성능을 가졌다. 이러한 SNR의 비교 결과는 상관전력분석을 통한 검증 결과와 상응하였다.

부채널 분석의 성능은 일반적으로 SNR과 비례한다고 알려져 있다. SNR은 연산 중간 값에 따라 파형을 분류하고 분류한 클래스에 따라 주 신호의 분산을 잡음 신호의 분산으로 나눈 값이다. 즉, 중간 값에 따른 클래스간의 거리가 커질수록 SNR이 커지며 이는 분석 성능의 상승을 가져온다. LDA는 최적의 분류관점의 신호처리 기법이므로 SNR의 상승에 가장 적합한 기법이라고 볼 수 있다.

기법을 조합한 방법이 선형판별분석보다 성능이 상승하지 않은 이유로는, SSA가 잡음제거의 방법이기 때문에 적용을 하여도 클래스 내 분산의 크기가 작아질 뿐 선형판별분석을 통해 찾는 벡터의 성질이 변하지 않기 때문으로 보인다. 또한 SSA에서 주신호로 선택하는 파형에 대한 명확한 기준이 아직 없기 때문에, SSA만 적용할 경우 성능이 상승하였어도 선형판별분석이나 주성분분석에 필요한 성분이 제거되었을 가능성도 있다.

References

[1] P. C. Kocher, J. Jae, and B. Jun, "Timing Attacks on Implementations of Diffie-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] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, "The EM Side-Channel(s)," CHES 2002, LNCS 2524, pp. 29-45, 2003.

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

[5] 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.

[6] 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.

[7] S. M. Del Pozo, F. X. Standaert, "Blind Source Separation from Single Measurements using Singular Spectrum Analysis," CHES 2015, LNCS 9293, pp.42-59, 2015.

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

[9] N. Bruneau, S. Guilley, A. Heuser, D. Marion, O. Rioul, "Less is More-Dimensionality Reduction from a Theoretical Perspective," CHES 2015, LNCS 9293, pp. 22 - 41, 2015.

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

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

[12] Kang, Ji-Su, HeeSeok Kim, and Seokhie Hong. "The Enhanced Power Analysis Using Linear Discriminant Analysis." Journal of the Korea Institute of Information Security and Cryptology 24.6 (2014): 1055-1063, 2014.

[13] E. Cagli, C. Dumas, E. Prouff, "Enhancing Dimensionality Reduction Methods for Side-Channel Attacks," CARDIS 2015, LNCS 9514, pp. 15-33,

2016.

〔14〕 TELECOM ParisTech SEN research group: DPA Contest (2nd edition) (2009-2010) http://www.DPAcontest.org/v2/

〔15〕 T.H.Le, J. Clédière, C. Servière, and J.L.Lacoume, (2007, April). "Efficient solution for misalignment of signal in side channel analysis". ICASSP 2007, In 2007 IEEE International Conference on Acoustics, Speech and Signal Processing-ICASSP'07 (Vol. 2, pp. II-257), 2007

〔16〕 T.H. Le, J. Clediere, C. Serviere, and J.L. Lacoume, "Noise Re-duction in Side channel Attack Using Fourth-Order Cumulant," IEEE Transactions on Information Forensics and Security, vol. 2, no. 4, pp. 710-720, Dec. 2007.

〔17〕 YongJe Choi, DooHo Cho, and JaeCheol Ryou, "Implementing Side Channel Analysis Evaluation Boards of KLA-SCARF system," Journal of The Korea Institude of Information Security & Cryptology, 24(1), pp. 229-240, Feb. 2014.

〈저자소개〉

박 건 민 (Geonmin Bak) 학생회원
2015년 2월: 고려대학교 수학과 학사
2015년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 부채널 공격

김 태 원 (Taewon Kim) 학생회원
2010년 2월: 광운대학교 수학과 학사
2012년 8월: 고려대학교 정보보호대학원 석사
2012년 8월~2016년 2월: 고려대학교 정보보호대학원 박사수료
2016년 3월~현재: (주)SNTWORKS 책임연구원
〈관심분야〉 부채널 공격, 스마트 카드 보안, 암호시스템 안전성 분석 및 고속구현

김 희 석 (HeeSeok Kim) 정회원
2006년: 연세대학교 수학과 학사
2008년: 고려대학교 정보보호대학원 석사
2011년: 고려대학교 정보보호대학원 박사
2011년 9월~2012년 12월: Bristol University 박사후 연구원
2013년~2016년 8월: 한국과학기술정보연구원(KISTI) 선임연구원
2015년~2016년 8월: 과학기술연합대학원대학교(UST) 조교수
2016년 9월~현재: 고려대학교 과학기술대학 수학과 조교수
〈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: ㈜시큐리티 테크놀로지 선임연구원
2003년 3월~2004년 2월: 고려대학교 정보보호기술연구센터 선임연구원
2004년 4월~2005년 2월: K.U. Leuven ESAT/SCD-COSIC 박사후 연구원
2005년 3월~2013년 8월: 고려대학교 정보보호대학원 부교수
2013년 9월~현재: 고려대학교 정보보호대학원 정교수
〈관심분야〉 대칭키 및 공개키 암호 알고리즘, 부채널 공격 및 대응기법, 디지털 포렌식