Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.5, Oct. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.5.1013

주성분 분석 기반의 CPA 성능 향상 연구*

백 상 수,[1†] 장 승 규,[2] 박 애 선,[3] 한 동 국,[3‡] 류 재 철[4]
[1]솔라시아, [2]코나아이, [3]국민대학교, [4]충남대학교

A Study on CPA Performance Enhancement using the PCA*

Sang-su Baek,[1†] Seung-kyu Jang,[2] Aesun Park,[3] Dong-Guk Han,[3‡] Jae-Cheol Ryou[4]
[1]Sola-cia, [2]Konai, [3]Kookmin University, [4]ChungNam University

요 약

상관관계 전력 분석(Correlation Power Analysis, CPA)은 암호장비에서 알고리즘이 수행될 때 누설되는 전력 소비 신호와 알고리즘의 중간 계산 값의 상관도를 이용하여 비밀키를 추출하는 부채널 공격 방법이다. CPA는 누설된 전력 소비의 시간적인 동기 또는 잡음에 의해 공격 성능이 영향을 받는다. 최근 전력 분석의 성능 향상을 위해 다양한 신호 처리 기술이 연구되어지고 있으며, 그 중 주성분 분석 기반의 신호 압축 기술이 제안되었다. 주성분 분석 기반의 신호 압축은 주성분 선택 방법에 따라 분석 성능에 영향을 주기 때문에 주성분 선택은 중요한 문제이다. 본 논문에서는 CPA의 성능 향상을 위해 전력 소비와의 상관도가 높은 주성분을 선택하는 주성분 선택 기법을 제안한다. 또한 각 주성분이 갖는 특징이 다르다는 점을 이용한 주성분 기반 CPA 분석 기법을 제안하고, 기존 방법과 제안하는 방법의 실험적인 분석을 통해 공격 성능이 향상됨을 보인다.

ABSTRACT

Correlation Power Analysis (CPA) is a type of Side-Channel Analysis (SCA) that extracts the secret key using the correlation coefficient both side-channel information leakage by cryptography device and intermediate value of algorithms. Attack performance of the CPA is affected by noise and temporal synchronization of power consumption leaked. In the recent years, various researches about the signal processing have been presented to improve the performance of power analysis. Among these signal processing techniques, compression techniques of the signal based on Principal Component Analysis (PCA) has been presented. Selection of the principal components is an important issue in signal compression based on PCA. Because selection of the principal component will affect the performance of the analysis. In this paper, we present a method of selecting the principal component by using the correlation of the principal components and the power consumption is high and a CPA technique based on the principal component that utilizes the feature that the principal component has different. Also, we prove the performance of our method by carrying out the experiment.

Keywords: Side-Channel Attack, Correlation Power Analysis, Principal Component Analysis

I. 서 론

최근 스마트폰 및 태블릿 PC 등과 같은 작고 경량화 된 스마트 기기들이 많이 개발되고 있으며, 이를 이용한 정보 통신, 결제 수단, 사용자 인증 등의 서비스가 여러 분야에서 사용되고 있다. 이러한 서비스에는 개인 비밀 정보가 이용되고 있으며, 이는 안

접수일(2014년 9월 2일), 수정일(2014년 10월 8일,), 게재확정일(2014년 10월 8일)
* 본 연구는 2013년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(NRF-2013R1A1A2A10062137)
† 주저자, baek@sola-cia.com
‡ 교신저자, christa@kookmin.ac.kr(Corresponding author)

전하다고 알려져 있는 암호 알고리즘을 이용해 암호화 된다. 그러나 스마트 기기의 내장된 하드웨어에서 암호 알고리즘이 실행될 때, 전자파, 소비 전력, 알고리즘의 수행 시간 등의 부가 정보들이 발생하게 되는데, 이론적으로 안전하다고 알려진 알고리즘이라도 이러한 부가적인 정보들의 노출을 이용하여 비밀 정보를 알아 낼 수 있는 부채널 분석(Side Channel Analysis)이 소개되었다[1].

부채널 분석 방법 중 전력 분석(Power Analysis)은 장치(Device)의 암호 알고리즘이 실행되는 동안의 소비 전력을 분석하여 비밀 정보를 얻어 내는 것으로 효율적인 분석 방법으로 알려져 있다. 전력 분석 공격은 장치가 '0' 또는 '1'을 처리하는데 소비되는 전력이 서로 다르다는 점을 이용한다. 전력 분석은 단지 몇 번의 알고리즘이 실행되는 동안 발생하는 전력 신호를 관찰하여 비밀키 값을 유도해 내는 공격인 단순전력분석(Simple Power Analysis, SPA)과 수차례 알고리즘이 반복 실행되는 동안 수집된 전력 신호들을 두 집단으로 나누어 그 차분을 이용하여 분석하는 차분전력분석(Differential Power Analysis, DPA)[2]이 존재한다. DPA는 부채널 분석 중 가장 강력한 분석 방법 중 하나로 전력 소비 신호와 알고리즘의 중간 계산 값의 상관도를 이용하여 비밀키를 추출하는 상관전력분석(Correlation Power Analysis, CPA)[3]으로 발전, 연구 되어 왔다.

CPA는 다수의 전력 신호를 사용하여 통계적인 특성을 이용해 비밀키를 찾아내는 방법으로 다수의 전력 신호를 사용하는 만큼 분석하는 시간이 오래 걸리며, 필요한 메모리 또한 증가하게 된다. 이러한 문제를 해결하기 위해 신호 전처리 기법을 사용하며, 신호 전처리에는 신호 압축[10], 신호 정렬[7], 잡음 제거[8] 등이 존재한다. 많은 신호 전처리 방법들 중 신호 압축 기법은 분석 시간을 절약할 수 있으며, 메모리의 사용에 있어서도 큰 이점을 갖는다. 하지만 기존의 다양한 압축 기법들은 신호의 특성을 고려하지 않고 압축하기 때문에 CPA의 분석 성능 저하의 결과를 가져오기도 한다. 이러한 문제점을 보완하여 분석 성능의 향상을 가져올 수 있는 주성분 분석(Principal Component Analysis, PCA) 기반의 신호 압축 기술이 제안 되었다[9].

PCA를 이용한 신호 압축 기법의 가장 큰 특징 중 하나는 많은 성분들 중 의미 있는 성분만을 추출하여 신호를 압축한다는 점이다. 따라서 CPA의 분석 성능의 향상을 기대 할 수 있다. 그러나 PCA 기반 신호 압축은 주성분 선택 방법에 따라 분석 성능에 영향을 주기 때문에 주성분 선택은 매우 중요한 문제이다. 본 논문에서는 CPA의 성능 향상을 위해 전력 소비와의 상관도가 높은 주성분을 선택하는 주성분 선택 기법과 각 주성분이 갖는 특징이 다르다는 점을 이용한 주성분 기반 CPA 분석 기법을 제안한다.

논문의 구성은 다음과 같다. 2장에서는 CPA 개념에 대하여 소개하고, 3장에서는 기존의 주성분 선택 기법 및 주성분 분석 기반 신호 압축에 대하여 설명한다. 4장에서는 본 논문에서 제안하는 주성분 선택 기법인 상관성 선택(correlation selection, CS) 방법과 주성분 기반의 CPA 분석기법으로 Argument-Max CPA를 소개한다. 5장에서 상관성 선택 및 Argument-Max CPA에 대한 CPA 분석 성능의 실험결과를 기존의 방법과 비교 후, 6장에서 본 논문의 결론을 짓는다.

II. 상관전력분석(Correlation Power Analysis)

CPA는 암호 알고리즘이 실행될 때 소비되는 전력이 암호 장비의 중간 연산 값에 의존해 소비된다는 가정을 이용하여 비밀키를 추정하는 방법으로, 전력 분석 기법 중 가장 강력한 분석 기법으로 알려져 있다.

CPA 공격의 단계는 다음과 같다. 암호 알고리즘이 탑재된 기기로부터 암호 알고리즘을 실행시켜 누출되는 소비 전력 신호 n개를 수집한다. 각 전력 신호에 대응되는 n개의 임의의 평문에 대해 알고리즘의 중간 결과 값을 계산한다. 중간 결과 값을 계산하기 위해서는 전력 소비 모델을 정해야 하며, 전력 소비 모델은 각 기기에 따라 다르게 정의된다. 전력 소비 모델로는 해밍 디스턴스 모델(Hamming Distance Model)과 해밍 웨이트 모델(Hamming Weight Model)이 대표적이다. 암호 기기에 따라 전력 소비모델이 정해지면, 전력 소비모델에 의한 계산된 중간 결과 값과 수집된 전력 신호 사이의 상관관계를 구한다. 상관관계는 피어슨(Pearson)의 상관계수를 이용하여 계산한다. 다음의 식 (1)은 피어슨 상관계수를 이용하여 수집된 전력 신호와 전력 소비모델에 의한 계산된 중간 결과 값의 상관관계를 구하는 식이다. 식 (1)에서 X는 n개의 임의의 평문을

사용하여 전력 소비 모델에 의한 중간 결과 값들의 집합이며, Y는 장치로부터 누출되는 n개의 소비 전력 신호들의 집합을 의미한다.

$$corr(X,Y)=\frac{E(XY)-E(X)E(Y)}{\sqrt{var(X)var(Y)}}$$
$$=\frac{\sum_{i=1}^{n}(x_i-E(X))(y_i-E(Y))}{\sqrt{\sum_{i=1}^{n}(x_i-E(X))^2\sum_{i=1}^{n}(y_i-E(Y))^2}} \quad (1)$$

중간 결과 값과 전력 신호와의 상관도가 높을 경우, 상관계수의 크기도 높게 나타난다. 이는 곧 추측한 키와 실제 암호 알고리즘에 쓰인 키가 일치 한다는 것을 의미하며, 해당 연산이 이루어지는 부분을 정확히 추측했다고 할 수 있다. 피어슨 상관계수 $corr(X,Y)$는 두 분포 X,Y의 선형성을 의미하며, 다음의 특성을 지닌다.

여기서 두 집합 X와 Y가 $Y=aX+b$ 와 같이 선형적 관계가 있으며, 양의 상관관계를 가지면 상관계수는 1, 음의 상관관계를 가지면 -1에 가까운 값을 갖게 된다. 유사 관계가 있지 않게 되면 0에 가까운 상관계수 값을 갖는다. 이러한 특성을 이용하여 추측한 비밀키에 따른 상관계수를 바탕으로 실제 사용한 키를 구별한다.

III. 기존의 연구

PCA를 하는 목적은 데이터 집합의 차원을 낮추어 신호를 압축하는 것에 있다. 이때 기존의 압축 방법들은 각 포인트의 가중치를 1로 동일하게 부여한다. 그러나 PCA에서는 가중 벡터를 이용해 전력 신호를 압축하는 것은 동일하지만, 가중치를 주는 관점에서는 다르다. 신호의 의미 있는 포인트에는 좀 더 가중치를 부과하며, 그렇지 아니한 부분은 가중치를 덜 주어 압축하게 된다.

본 절에서는 기존에 연구되어진 PCA 기반 신호 압축 방법과 주성분 선택 기법에 대하여 설명한다.

3.1 주성분 분석 기반 신호 압축[9]

PCA는 이산 카루넨-뢰브 변환 또는 호텔링 변환으로 불린다. PCA는 고차원의 데이터를 저차원의 데이터로 차원을 감소시키는 방법으로, 다량의 데이터에서 선형적인 특징 또는 의미 있는 성분만을 추출하여 데이터를 압축하는 유용한 방법이다.

암호장비로부터 암호알고리즘을 실행하여 누출된 전력 신호 n개를 수집한다. 수집된 n개의 전력 신호는 각 m개의 포인트로 이루어져 있으며, 그 포인트에는 암호 장비로부터 발생하는 잡음(Noise)이 섞여 있다. 따라서 신호의 의미 있는 성분만을 추출하여 신호를 압축하는 PCA는 앞 절에서 설명한 CPA의 성능을 향상시킬 수 있다.

PCA를 이용한 신호 압축 기술 방법은 다음과 같다. c개의 포인트로 구성된 전력 신호 $X_s^{'}=\left\{\dot{x_{1,s}},\dot{x_{2,s}},\cdots,\dot{x_{n,s}}\right\}$로부터 공분산 행렬(covariance matrix) S_s를 연산한다.

본 논문에서 사용하는 기호는 아래와 같이 정의한다.

- $x_i=[x_{i,1},x_{i,2},\cdots,x_{i,m}]^T=[\dot{x_{i,1}},\dot{x_{i,2}},\cdots,\dot{x_{i,k}}]^T$
  : m개의 포인트로 구성된 i번째 전력 신호 $(1\le i\le n)$
- $x_{i,t}$
  : i번째 전력 신호의 t번째 포인트$(1\le t\le m)$
- $\dot{x_{i,s}}=[x_{i,(s-1)c+1},\cdots,x_{i,sc}]^T$
  : i번째 전력 신호를 c개의 포인트를 가진 k개 블록으로 분할 할 때,s번째 블록$(1\le s\le k)$
- $X=\{x_1,x_2,...,x_n\}$ 4
  : 전력 신호 n개로 구성된 $m\times n$행렬
- $X_s^{'}=\left\{\dot{x_{1,s}},\dot{x_{2,s}},\cdots,\dot{x_{n,s}}\right\}$
  : s번째 블록으로 구성된 $c\times n$행렬
- w
  : 가중 벡터

공분산 행렬은 다음의 식 (2)로 구할 수 있다.

$$S_s=\frac{1}{n}\sum_{i=1}^{n}\left(\dot{x_{i,s}}-\overline{\dot{x_s}}\right)\left(\dot{x_{i,s}}-\overline{\dot{x_s}}\right)^T \quad (2)$$

$\overline{\dot{x_s}}$는 각 $\dot{x_{i,s}}$들의 평균 벡터를 나타내며, 공분산 행렬로부터 특이값 분해(Singular Value Decomposition, SVD)를 통해 고유벡터와 고유값을 구한다. 이때, 가장 큰 고유값에 대응하는 고유벡

터는 전력 신호를 가장 잘 표현하는 제 1 주성분이 된다. 공분산 행렬은 $c \times c$의 행렬로 S_s의 계수(rank)는 c가 되므로 고유벡터는 c개 존재한다. c개의 고유값은 값이 큰 순서대로 정렬이 되며, 큰 고유값부터 차례로 원 신호와 시각적으로 유사한 고유벡터를 선택하여 압축을 위한 가중 벡터로 이용한다. 만약 고유값이 큰 순서대로 h개의 고유벡터가 선택되었다면, h개의 고유벡터를 더하여 하나의 가중 벡터 w를 구한다. 가중 벡터 w를 신호 $X_s^{'} = \{x_{1,s}^{\cdot}, x_{2,s}^{\cdot}, \cdots, x_{n,s}^{\cdot}\}$에 적용하여 압축된 신호 $\{w^T x_{1,s}^{\cdot}, w^T x_{2,s}^{\cdot}, \cdots, w^T x_{n,s}^{\cdot}\}$를 얻는다. $w^T x_{i,s}^{\cdot}$는 벡터의 내적으로 하나의 값을 갖는다. 따라서 1포인트의 값이 된다. 총 전력 신호의 개수는 n개로 동일하나 각 전력 신호의 포인트 수는 c개에서 1개로 줄어들어 $\frac{1}{c}$의 압축 효과를 얻는다. 위 과정을 k번 반복하여 k개의 포인트를 갖는 n개의 압축된 신호를 얻는다. 압축된 신호에 대하여 CPA 공격을 하여 암호 알고리즘의 키를 찾는다.

3.2 주성분 선택 기법

주성분 선택 기법으로 잘 알려진 방법으로는 스크리 그래프(Scree graph)를 이용하여 선택하는 방법과 분산의 누적량(Cumulative Percentage of Variance, CPV)을 이용하는 방법이 있다[4]. 이 두 가지의 주성분 선택 기법은 주성분의 크기 즉, 고유값의 크기에 의존한다. 스크리 그래프와 분산의 누적량을 이용한 방법 모두 내림차순으로 정렬된 고유값을 이용한다. 한 클럭의 신호로부터 계산된 공분산 행렬의 특이값 분해를 통해 내림차순 정렬된 고유값을 얻을 수 있다.

가장 널리 사용된 기법인 스크리 그래프 방법은 Fig.1.에서 설명하고 있다.

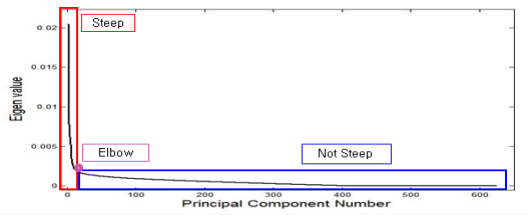


Fig. 1. Eigenvalues for the principal components 625 of the DES algorithm

특이값 분해를 통해 내림차순 정렬된 고유값들을 나타내면, 위 Fig.1.과 같이 굽은 지점(Elbow)이 발생하게 된다. 이 굽은 지점을 중심으로 경사가 가파른 부분을 'Steep'이라 하며, 완만한 지점을 'Not Steep'이라 한다. 이때 주성분의 선택은 '굽은 지점'을 기점으로 선택한다. 예를 들어 '굽은 지점'이 10이라 하면, 제 1주성분부터 차례로 10개를 선택한다.

반면, 분산의 누적량을 이용한 방법은 고유값이 갖는 분산의 누적량을 계산하여 주성분을 선택하게 된다. 각 고유값들은 각기 다른 분산을 갖게 되며, 고유값이 큰 성분일수록 분산의 크기도 큰 값을 갖는다. 스크리 그래프와 마찬가지로 내림차순 정렬된 고유값을 이용하는 반면 고유값이 큰 순서대로 각 고유값이 갖고 있는 분산을 합하여 정해진 비율 이상이 될 때, 해당하는 주성분과 고유벡터를 선택한다. 일반적으로 분산의 누적량이 70%~90% 되도록 주성분을 선택한다. 전체 고유값의 개수를 c개라 하고 분산의 누적량이 70~90%가 되도록 하는 고유값의 개수를 h, i번째의 고유값이 갖는 분산의 크기를 l_i라 하자. h개의 고유값이 갖는 분산을 더한 분산 누적 비율을 t_h라 하면, t_h는 다음과 같다.

$$t_h = 100 \frac{\sum_{i=1}^{h} l_i}{\sum_{i=1}^{c} l_i} \tag{3}$$

t_h의 값이 70~90%가 될 때의 h를 구한 후, 제 1주성분부터 h개의 주성분을 선택하여 가중 벡터로 사용한다.

IV. 제안하는 주성분 선택 기법과 주성분 기반의 CPA 분석기법

4.1 주성분 선택 기법

본 절에서는 CPA의 분석 성능을 높이기 위한 주성분 선택 기법에 대하여 소개한다. CPA는 전력 신호와 중간 계산 값과의 상관관계에 따라 상관계수가 가장 높은 통계적 방법을 이용하기 때문에 CPA의 분석 성능을 높이기 위해서는 전력 신호와 유사성이 높은 주성분을 선택하는 것이 바람직하다. 하지만 기

존의 주성분 선택 기법들은 고유값의 크기와 분산에 의존하게 되어 신호처리의 관점에서 효율이 미비할 수가 있다. 따라서 본 논문에서는 i번째 주성분 w_i와 평균 전력 신호와의 상관관계를 이용한 상관성 선택 방법을 제안한다.

주성분을 선택하기에 앞서 기존 방법과 같이 수집한 전력 신호로부터 한 클럭에 해당하는 포인트를 이용하여 공분산 행렬을 구한다.

한 클럭이 c개의 포인트로 이루어진 n개의 전력 신호로부터 공분산 행렬을 만들고, 특이값 분해를 통해 계수 만큼의 고유값을 얻게 된다. 즉, $c \times c$의 행렬의 계수는 c이므로 c개의 고유값 $w_i (i=1,...,c)$를 얻을 수 있다. 다음으로 전력 신호의 평균 신호 $\overline{X_s} = \frac{1}{n}\sum_{i=1}^{n} \dot{x}_{i,s}$를 구하여 주성분 w_i의 상관계수 $corr(\overline{X_s}, w_i)$을 계산한다. 구해진 총 c개의 상관계수는 상관계수가 큰 순서대로 정렬한다. 이때, 가장 큰 상관계수의 값은 한 클럭의 전력 신호와 가장 유사한 주성분이라는 것을 의미한다. 상관계수가 큰 순서대로 내림차순 정렬하면 Fig.1.과 유사한 그림을 얻을 수 있으며, 스크리 그래프의 선택방법의 굽은 지점을 선택하여 주성분의 개수를 선택한다.

본 절에서 설명하는 상관성 선택은 전력 신호와 전력 신호로부터 계산된 고유값과의 상관관계를 계산하여 그 상관도가 가장 높은 주성분을 선택하는 방법이다. 전력 신호와 중간값의 상관도를 이용해 올바른 비밀키를 추정하는 CPA의 관점에서 전력 신호와 상관계수가 가장 높은 주성분을 선택하는 것이 CPA의 분석 성능 향상을 가져온다.

4.2 주성분 기반 CPA 분석기법

기존의 주성분 기반 CPA 분석기법은 선택 기법에 의해 선택된 주성분을 모두 더하여 하나의 가중 벡터를 만들어 압축된 신호를 만든다[9]. 이 기법은 각 주성분을 더하여 의미 있는 신호의 정보가 누적되어 분석하고자 하는 대상의 정보를 많이 얻을 수 있어 상승효과를 얻을 수 있다. 하지만 반대로 첫 번째 주성분부터 h번째의 주성분까지 모두 더할 경우, 특정 분석 지점에 대한 불필요한 정보인 잡음이 섞이는 경우가 발생한다. 특정 분석 지점에 적절한 주성분이 존재할 수 있고, 다른 주성분들이 잡음처럼 작용할 수 있다. 신호 압축을 할 때, 의미 있는 정보만을 추출하여 신호를 다시 표현 하는 것이 주성분 분석의 목적이라면, 잡음이 섞인 주성분으로 신호를 표현하는 것은 공격 성능을 떨어트리는 결과를 초래할 수 있다. 따라서 본 절에서 제안하는 기법은 앞 절의 주성분 선택 기법으로부터 선택된 h개의 주성분 각각에 대하여 원 신호를 압축해 CPA 공격을 수행하는 PCA 기반 Argument-Max CPA를 소개한다.

Fig.2.는 PCA 기반 Argument-Max CPA를 나타내는 알고리즘으로 다음과 같이 공격한다. 한 클럭의 포인트 c개로 이루어진 n개의 전력 신호 $\hat{X} = \{\dot{x_1}, \dot{x_2}, \cdots, \dot{x_n}\}$ 와 h개의 주성분 $\{w_i | 1 \le i \le h\}$ 각각에 대해 내적을 계산하여 $\widetilde{X_i}$를 구한다.

$$\begin{aligned}
\widetilde{X_1} &= w_1^T \hat{X} = \{w_1^T \dot{x_1}, w_1^T \dot{x_2}, \cdots, w_1^T \dot{x_n}\}, \\
\widetilde{X_2} &= w_2^T \hat{X} = \{w_2^T \dot{x_1}, w_2^T \dot{x_2}, \cdots, w_2^T \dot{x_n}\}, \\
&\vdots \\
\widetilde{X_h} &= w_n^T \hat{X} = \{w_n^T \dot{x_1}, w_n^T \dot{x_2}, \cdots, w_n^T \dot{x_n}\}
\end{aligned}$$

$\frac{1}{c}$로 압축된 전력 신호 $\widetilde{X_i} (1 \le i \le h)$에 대하여 CPA 공격을 한 번씩 수행하여 총 h번의 CPA 공격을 수행 후, 가장 좋은 성능을 보이는 결과를 선택한다.

AES 알고리즘의 경우 비밀키 16byte를 1byte씩 16개로 나누어 분석을 하는데, 각각의 고유벡터를 가중 벡터로 사용하여 압축된 전력 신호는 CPA 공격의 결과에 각기 다른 결과를 보인다. 이는 분석하는 byte에 따라 각 주성분이 신호를 표현하는 정도가 다르기 때문이다. 앞 절의 주성분 선택 기법에

Algorithm 1. Argument-Max CPA based on PCA	
INPUT	$\{w_i \mid 1 \le i \le h\}, \hat{X} = \{\dot{x_1}, \dot{x_2}, \cdots, \dot{x_n}\}$
OUTPUT	$Argu\_max = \{CPA(\widetilde{X_1}), CPA(\widetilde{X_2}), \cdots, CPA(\widetilde{X_h})\}$
Step 1. For $i = 1$ to h do $\widetilde{X_i} = w_1^T \hat{X}$	
Step 2. For $i = 1$ to h do $CPA(\widetilde{X_i})$	
Step3. Return $Argu\_max = \{CPA(\widetilde{X_1}), CPA(\widetilde{X_2}), \cdots, CPA(\widetilde{X_h})\}$	

Fig. 2. Argument-Max CPA based on PCA

의해 선택된 제 1 주성분은 전체 신호를 가장 잘 표현하는 주성분이지만 CPA 분석 지점에 대해서는 특정 주성분이 CPA에 필요한 의미 있는 정보를 더 포함 할 수 있다.

Argument-Max CPA는 선택한 주성분의 개수 h만큼 CPA 공격을 수행한다. 따라서 시간 및 계산의 복잡도는 h배만큼 커지는 것을 알 수 있다. 하지만, 전력 신호를 구성하는 포인트의 수가 $\frac{1}{c}$로 줄었기 때문에 CPA 공격의 수행 시간 및 계산량 또한 $\frac{1}{c}$로 줄어든다. 즉, CPA 공격을 수행함에 있어 계산 복잡도는 주성분의 개수에 반비례, 한 클럭의 포인트 수 c에 비례하여 시간 및 계산 복잡도가 감소한다.

V. 실험 결과

5.1 실험 환경

본 절에서는 하드웨어 DES와 하드웨어 AES의 전력 신호에 대하여 각각 두 가지의 실험을 하였다. 첫 번째는 3절에서 설명한 주성분의 선택 기법 두 가지와 본 논문에서 제안하는 상관성 선택 기법의 성능 비교를 위한 실험으로 선택된 고유벡터를 모두 더하여 하나의 가중 벡터로 사용하는 기존의 PCA 기반 신호 압축을 적용하여 분석 성능을 비교한다. 두 번째는 본 논문에서 제안하는 PCA 기반 Argument-Max CPA의 분석 성능과 기존의 PCA 기반 신호 압축 기법의 분석 성능을 첫 번째 실험에서 가장 좋은 성능을 보인 주성분 선택 기법을 적용하여 비교한다.

실험은 하드웨어 DES과 AES에 대하여 진행하였다. 실험에 사용된 전력 신호는 DPA contest[5]로부터 얻은 전력 신호로 그 세부 사항은 Table 1.과 같다.

Table 1. Experimental environment

	DES	AES
Trace Count	5,000	11,000
Trace Point	20,003	3,253
Clock Size	625	210
Target Round	1 Round	10 Round

DPA contest 웹 사이트에서는 하드웨어 DES와 AES의 전력 신호뿐만 아니라 FPGA로 구현된 Verilog 파일을 제공한다. 하드웨어 DES와 AES는 라운드 단위로 구현되었는데, 이는 곧 한 클럭이 동작할 때, 알고리즘의 라운드 내 모든 서브함수가 수행되어짐을 의미한다. 따라서 하드웨어 DES의 경우 16개 클럭의 동작으로 16라운드가 수행되며, AES의 경우 10개의 클럭으로 10라운드가 수행되어 1회의 암호화가 이루어진다. 분석 성능의 비교를 위하여 비밀키를 찾기 위한 최소 분석 신호의 수를 기준으로 하였다. DES 암호 알고리즘의 경우 1라운드 48비트 키, AES 암호 알고리즘의 경우 10라운드 128비트 키를 찾는다.

Fig.3.은 하드웨어 DES의 한 클럭에 해당하는 신호를 나타낸다. 하드웨어 DES는 총 20,003포인트로 이루어져 있으며 Fig.3.에서와 같이 한 클럭의 신호[625포인트]가 주기적으로 반복된다. 한 클럭의 신호로부터 공분산 행렬을 구한 뒤 특이값 분해를 이용하여 고유값과 고유벡터를 구한 후, 주성분 벡터를 고유값이 큰 순서대로 내림차순 정렬한다. Fig.4.는 하드웨어 DES 전력 신호의 고유값이 큰 4개의 고유벡터를 나타내는 그림이다. 시각적으로 원 신호와 유사함을 갖는 고유벡터가 있는 반면, 원 신호와 유사함을 볼 수 없는 고유벡터도 존재하였다. DES는 총 8개의 S-box가 존재하고 분석 지점을 S-box 출력부분을 대상으로 하였다. 따라서 모든 키를 찾기 위해 8개의 S-box로 나누어 분석을 하였다.

Fig.5.는 하드웨어 AES의 한 클럭에 해당하는 신호로서 암호 알고리즘 AES의 10라운드의 부분에 해당된다. 분석 라운드를 10라운드로 선택한 이유는 하드웨어 특성상 한 클럭의 신호에 1개 라운드의 연산이 이루어지기 때문이다. 즉, 한 클럭 신호에 한 라운드의 정보가 담겨 있어, 라운드 안의 함수를 공격할 수 없다. 만약 1라운드를 분석 라운드로 하였다면 AES 암호 알고리즘의 특성상 확산 계층이 존

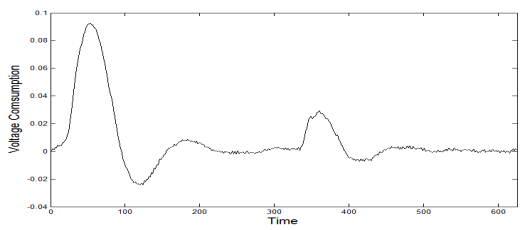


Fig. 3. A clock signal of hardware DES

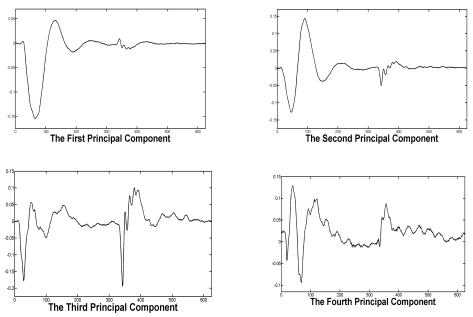


Fig. 4. The principal component of the hardware DES

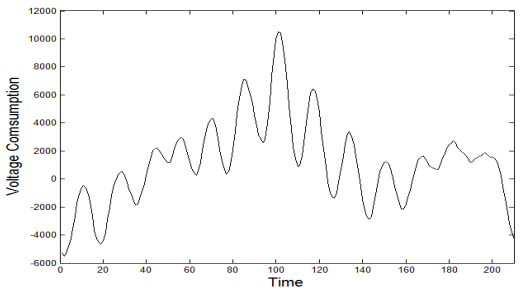


Fig. 5. A clock signal of hardware AES

재하여 비밀키를 워드(word, 32bit)단위로 추측을 해야 한다. 따라서 확산 계층 부분이 없는 10라운드를 분석 라운드로 하였다. AES의 경우 분석 지점을 16개의 S-box 출력 부분으로 하였으며, 128bit의 키를 찾기 위해 8bit 씩 16번 분석을 시도한다.

Fig.6.은 차례로 첫 번째 주성분부터 네 번째 주성분까지 그래프로 표현한 것이다. 원 신호와 시각적으로 유사한 고유벡터가 존재하는 반면, 유사성이 없는 고유벡터들도 존재한다. 다음의 실험에서 이러한 고유벡터를 주성분을 이용하여 CPA의 성능에 어떠한 영향을 미치는지 알아본다.

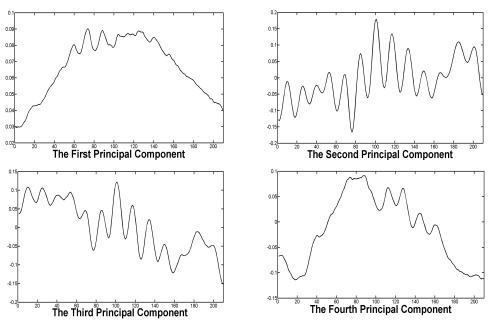


Fig. 6. The principal component of the hardware AES

5.2 실험 결과

5.2.1 주성분 선택 기법

기존의 주성분 선택 기법인 스크리 그래프 및 분산의 누적량을 이용한 주성분 선택 방법과 비교하기 위해 기존의 주성분을 더하는 방법[9]으로 전력 신호를 압축하였으며, 압축된 신호를 CPA 공격하였다. 대조군으로써 원신호에 대한 CPA 결과도 함께 표로 작성하였다.

Table 2.는 하드웨어 DES의 모든 키를 찾기 위해 필요한 최소 평문의 수를 나타낸다. PCA를 적용하지 않은 전력 신호에 대하여 48 비트 비밀키를 모두 찾기 위해 최소 평문이 평균 300여개를 필요로 한다. 여기서 평균 평문의 수란 각 S-box의 출력 부분을 분석하기 위한 최소 평문의 수를 모두 더한 후, S-box의 수로 나눈 것을 의미한다. 원신호의 모든 키를 찾기 위해 필요한 최대 평문의 수는 600여개가 필요하다.

기존의 주성분 선택 기법인 스크리 그래프 방법은 평균 300여개로 PCA를 적용하지 않은 원신호의 평균 평문의 수와 비슷하지만, 모든 키를 찾기 위한 최대 평문의 수는 800여개로 더 많은 수의 평문을 필요로 한다. 반면, 분산의 누적량을 이용하여 주성분을 선택 했을 때는 평균 200여개의 평문을 필요로 한다. 앞선 스크리 그래프 보다 100여개가 적은 수로 분석이 가능하였고, 최대 평문수도 500여개로 300여개가 적은 평문이 필요로 한다. 제안하는 기법은 분산 누적량 방법과 비슷한 성능을 보였다. 평균 200여개의 평문이 필요하였고, 키 전부를 찾기 위한 최대 평문수도 500여개로 유사한 성능을 보였다.

Table 3.은 하드웨어 AES의 128bit 키를 찾기

Table 2. CPA result of the principal component selection techniques on DES (Unit:*100)

S-box	1st	2nd	3rd	4th	5th	6th	7th	8th
normal	3	6	3	1	3	1	1	1
Scree graph	3	8	1	2	1	1	1	1
CPV	3	5	1	1	1	1	1	1
CS	3	5	1	1	1	1	1	1

Table 3. CPA result of the principal component selection techniques on AES (Unit:*100)

S-box	1st	2nd	3rd	4th	5th	6th	7th	8th
normal	63	21	60	99	94	56	37	104
Scree graph	50	17	28	56	108	47	21	87
CPV	50	18	28	86	108	48	12	87
CS	50	15	28	52	105	46	15	77
S-box	9th	10th	11th	12th	13th	14th	15th	16th
normal	40	40	46	57	65	108	69	43
Scree graph	38	13	35	67	55	110	57	41
CPV	40	13	35	67	55	102	55	41
CS	12	11	35	70	55	102	55	41

위해 CPA 공격에 필요한 평문의 수를 정리한 표이다. AES의 전력 신호에 대한 CPA 분석 결과 128bit의 비밀키를 찾기 위해 필요한 평균 평문이 6,300여개이며, 모든 키를 찾기 위해 필요한 최대 평문의 수는 10,800여개이다. 기존 스크리 그래프와 분산의 누적량 기법에서는 각각 평균 5,200개, 5,100개의 평균 평문의 수가 필요하였으며, 최대 11,000개, 10,800개의 평문 정보가 필요하였다. 반면 제안하는 기법인 상관성 선택은 평균 4,800여개의 평문 정보, 최대 10,500여개의 평문 정보로 분석이 가능하였다. 하드웨어 DES에서는 제안하는 기법이 분산 누적량 방법과 유사한 결과를 보인 반면, AES의 전력 신호에서는 평균 300여개의 전력 신호가 적게 필요로 하였다.

5.2.2 주성분기반 CPA 분석기법

앞선 주성분 선택 기법의 실험으로 상관성 선택이 기존의 주성분 선택 기법과 성능이 유사하거나 향상됨을 점을 보였다. 따라서 본 실험에서는 주성분 선택 기법으로 상관성 선택을 적용하여 실험을 진행한다.

Table 4.는 기존의 PCA 기반 신호 압축 기법과 Argument-Max CPA의 기법에 대하여 계산량 차이를 비교한 표이다. 선택된 주성분이 h개라 할 때, 기존 기법을 적용할 때 필요한 계산량은 $(h-1)$번의 벡터 덧셈 연산과, 1번의 행렬 곱의 연산을 필요로 한 반면, Argument-Max CPA의 경우 h번의 행렬 곱 연산을 필요로 한다. 또한 CPA의 분석 횟수에서도 기존 기법의 경우 1회만 시행하지만 Argument-Max CPA의 경우 h회 시행한다.

Table 4. Complexity of the existing techniques and Argument-Max method

	Exist	Argument-Max
Addition	$h-1$	·
Multiplication	1	h
Number of CPA	1	h

Argument-Max CPA는 기존의 기법에 비해 h배의 시간이 더 소요되지만, CPA 공격에 사용한 분석 평문의 수는 보다 적은 평문을 필요로 한다. Table 5.와 Table 6.은 각각 DES 및 AES 전력 신호를 CPA하여 필요한 평문 정보를 정리한 표이다.

DES의 모든 키를 찾기 위해 원신호에 필요한 평균 평문 정보는 약 300여개, 최대 600여개이다. 기존 기법이라 함은 상관성 선택으로부터 선택된 주성분을 모두 더한 벡터를 가중 벡터로 사용한 것을 의미한다. 기존 기법은 평균 200여개, 최대 500여개의 평문 정보를 필요로 한다. 반면 본 논문에서 제안하는 Argument-Max CPA는 평균 200여개의 평문 정보가 필요하다는 점에선 기존의 기법과 비슷하지만, 모든 키를 찾기 위한 최대 평문 정보는 400여개로 기존의 기법에 비해 100여개 적은 평문이 필요하였다.

또한 AES의 128 비트 모든 키를 찾기 위해 원신호는 평균 6,300여개의 평문 정보가 필요하며, 최대 10,800여개의 평문 정보가 있어야 한다. 기존의 주성분 기반인은 평균 4,800여개의 평문으로 원신호에 비해 약 1,500여개 적은 평문으로 분석이 가능하였다. 최대 필요한 평문 정보는 10,500개이다. 반면 제안하는 기법인 Argument-Max CPA는 기존 기법에 비해 월등한 성능을 보였다. 기존 기법의 약 54%의 평문 정보만으로 128bit의 모든 키를 찾을 수 있었으며, 최대 평문 정보 또한 기존 기법의 약 48%인 5,500여개만으로 전체 128bit를 모두 찾을 수 있었다.

Table 5. CPA result of applying PCA techniques on DES (Unit:*100)

S-box	1st	2nd	3rd	4th	5th	6th	7th	8th
normal	3	6	3	1	3	1	1	1
Exist	3	5	1	1	1	1	1	1
Argument -Max	3	2	4	2	1	1	1	1

Table 6. CPA result of applying PCA techniques on AES (Unit:*100)

S-box	1st	2nd	3rd	4th	5th	6th	7th	8th
normal	63	21	60	99	94	56	37	104
Exist	50	15	28	52	105	46	15	77
Argument-Max CPA	33	22	36	48	19	28	43	34
S-box	9th	10th	11th	12th	13th	14th	15th	16th
normal	40	40	46	57	65	108	69	43
Exist	12	11	35	70	55	102	55	41
Argument-Max CPA	12	14	45	21	41	51	55	6

VI. 결 론

본 논문에서는 PCA기반의 CPA의 성능을 향상시키기 위해 주성분 선택 기법으로 상관성 선택 기법을, 압축 기법으로 Argument-Max CPA를 제안하였다. 하드웨어 DES의 전력 신호에서는 분석 성능이 크게 향상됨을 보이지 않았다. 그 이유는 DES의 전력 신호의 CPA 성능이 약 1천개 미만의 신호로부터 분석이 되는 상한치에 이르렀다고 할 수 있다. 반면 AES에서는 상관성 선택과 압축 기법으로서의 Argument-Max CPA가 CPA의 분석 성능에 있어서 월등한 효과를 냈다.

분석 결과, 계산적으로 제안한 Argument-Max CPA는 기존의 기법보다 많은 계산량을 필요로 하였지만, CPA의 공격의 분석 성능 관점에서 Argument-Max CPA 기법이 훨씬 적은 수의 전력 신호, 평문을 필요로 하였다.

현재의 컴퓨팅 환경은 더욱 발전하고 있으며, 그에 따라 속도도 빨라지고 있다. 하지만 현실적으로 암호 알고리즘을 수행시켜 얻게 되는 소비 전력 정보를 많이 얻지 못하는 것이 사실이다. 따라서 더 적은 평문 정보를 이용하여 최대의 분석 성능을 보이는 것이 더 효과적이라고 할 수 있다.

References

[1] P.Kocher, J.Jaffe, and B.Jun, "Introduction to differential power analysis and related attacks," White Paper, Cryptography Research. Available : http://www.cryptography.com, 1998.

[2] P.Kocher, J.Jaffe, and B.Jun, "Differential power analysis," Advances In Cryptology CRYPTO′99, LNCS 1666, pp. 388-397, 1999.

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

[4] I.T. Jolliffe, Principal Component Analysis, Second Edition, John Wiley & Sons, pp. 111-118, 2002.

[5] DPA contest website, http://www.dpacontest.org/index.php, 2008.

[6] G.Pirest, J.J.Quisquater, "A differential fault attack technique against SPN structures, with application to the AES and KHAZAD," Cryptographic Hardware and Embedded Systems, LNCS 2779, pp. 77-88, 2003.

[7] N.Homma, S.Nagashima, Y.Imai, T.Aoki, and A.Satoh, "High-resolution side channel attack using phase-based waveform matching," CHES 2006, LNCS 4249, pp. 187-200, 2006.

[8] T.Le, J.Clediere, C.Serviere, and J.L.Lacoume, "Noise reduction in side channel attack using fourth-order cumulant," IEEE Transactions on Information Forensics and Security, Vol.2, Issue 4, pp. 710-720, July 2007.

[9] H.S. Kim, H. Kim, I. Park, C.K. Kim, H. Ryu, Y.H. Park, "The performance advancement of power analysis attack using principal component analysis," Journal of the Korea Institute of Information Security and Cryptology, 20(6), pp. 15-21, Nov., 2010.

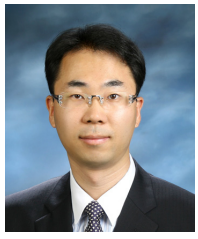
[10] S.Mangard, E.Oswald, and T.Popp, Power Analysis Attacks : Revealing the secrets of smart cards. Springer, pp. 82-86, 2007.

〈저 자 소 개〉

백 상 수(Sang-su Baek) 정회원
1999년 2월: 충남대학교 컴퓨터과학과 졸업
2001년 2월: 충남대학교 컴퓨터과학과 석사 졸업
2002년 3월~현재: 충남대학교 컴퓨터과학과 박사과정
2007년~현재: ㈜솔라시아 이사
〈관심분야〉 스마트카드, 암호, 모바일보안

장 승 규 (Seung kyu Jang) 정회원
2012년 2월: 국민대학교 수학과 졸업
2014년 2월: 국민대학교 수학과 석사
2014년 3월~현재: 코나아이 재직
〈관심분야〉 부채널 분석, 스마트 카드, 정보보호 등

박 애 선 (Aesun Park) 학생회원
2011년 2월: 국민대학교 수학과 졸업
2013년 2월: 국민대학교 수학과 석사
2014년 3월~현재: 국민대학교 금융정보보안학과 박사과정
〈관심분야〉 부채널 분석 및 대응법, 신호처리, 스마트 카드 평가 등



한 동 국 (Dong-Guk Han) 종신회원
1999년 2월 고려대학교 수학과 졸업(학사)
2002년 2월 고려대학교 수학과 석사 (이학석사)
2005년 2월 고려대학교 정보보호대학원 박사 (공학박사)
2004년 4월~2005년 4월: 일본 Kyushu Univ., 방문연구원
2005년 4월~2006년 4월: 일본 Future Univ.-Hakodate, Post.Doc.
2006년 6월~2009년 2월: 한국전자통신연구원 정보보호연구단 선임연구원
2009년 3월~현재 국민대학교 수학과 부교수
〈관심분야〉 공개키 암호시스템 안전성 분석 및 고속 구현, 부채널 분석 및 대응법 설계, IoT 정보보호 기술

류 재 철 (Jae-Cheol Ryou) 종신회원
1985년 2월: 한양대학교 산업공학과 졸업
1988년 2월: Iowa State University 전산학과 석사 졸업
1990년 2월: Northwestern University 전산학과 박사 졸업
1991년~현재: 충남대학교 전기정보통신공학부 교수
〈관심분야〉 인터넷 보안