情報保護學會論文誌
第 20卷 第 6號, 2010. 12

주성분 분석을 이용한 전력 분석 공격의 성능 향상*

김 희 석,[1†] 김 현 민,[1] 박 일 환,[2] 김 창 균,[2] 류 희 수,[3] 박 영 호[4‡]
[1]고려대학교 정보경영공학전문대학원, [2]한국전자통신연구원 부설연구소,
[3]경인교육대학교, [4]세종사이버대학교

The Performance Advancement of Power Analysis Attack Using Principal Component Analysis*

HeeSeok Kim,[1†] Hyunmin Kim,[1] IlHwan Park,[2] ChangKyun Kim,[2] Heuisu Ryu,[3] Young-Ho Park[4‡]
[1]Graduate School of Information Management and Security, Korea University,
[2]The Attached Institute of ETRI, [3]Gyeongin National University of Education, [4]Sejong Cyber University

요 약

최근, 전력 분석 공격의 성능 향상을 위해 다양한 신호 처리 기술에 대한 연구가 진행되고 있다. 그 중 신호 압축 기술은 전력 분석 공격 시 소요되는 연산시간을 상당히 단축할 수 있음에도 불구하고 신호 정렬, 잡음 제거 기술에 비해 연구가 미비한 실정이다. 기존의 신호 압축 기술은 신호의 특성을 제대로 고려하지 않아 오히려 전력 분석의 성능을 저하시킬 수 있다. 본 논문에서는 전력 신호의 특성을 고려하여 원신호의 의미있는 성분이 최대한 손실되지 않는 주성분 분석 기반의 신호 압축 기술을 제안한다. 또한 기존 방법과 제안하는 압축 기술의 실험적인 분석을 통해 각 압축 기술의 전력 분석 공격 성능을 비교한다.

ABSTRACT

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, the research about the signal compression is not enough than a signal alignment and a noise reduction; even though that can reduce considerably the computation time for the power analysis. But, the existing compression method can sometimes reduce the performance of the power analysis because those are the unsophisticated method not considering the characteristic of the signal. In this paper, we propose the new PCA (principal component analysis)-based signal compression method, which can block the loss of the meaningful factor of the original signal as much as possible, considering the characteristic of the signal. Also, we prove the performance of our method by carrying out the experiment.

Keywords: Side Channel Attack, Signal Compression, Principal component Analysis

I. 서 론

수학적으로 안전한 것으로 알려진 알고리즘조차도 구현 단계에서 고려되지 못한 부가적인 정보의 누출이 있다는 것이 알려졌고, 이로부터 비밀 정보를 알아낼 수 있는 부채널 공격(Side Channel Attack)이 소개되었다[1]. 알려진 부채널 공격에는 오류 주입 공격(fault insertion attack)[2,3], 시간 공격(timing attack)[1], 전력 분석 공격(power analysis attack)[4,5,6], 그리고 전

접수일(2010년 7월 13일), 수정일(2010년 10월 12일), 게재 확정일(2010년 11월 1일)
* 이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No. 2010-0011511)
† 주저자, heeseokkim@cist.korea.ac.kr
‡ 교신저자, youngho@sjcu.ac.kr

자기 누출 공격(electromagnetic emission attack)[7]등이 있으며 전력 분석 공격 중 차분 전력 분석 공격(Differential Power Analysis, DPA)과 상관 계수 전력 분석 (Correlation Power Analysis, CPA)은 가장 대표적인 분석법으로 알려져 있다. DPA와 CPA는 다수의 전력 파형에 대한 신호 처리, 통계적 특성을 이용해 키를 찾아내는 공격 방법으로 신호 처리 방법에 따라 큰 성능차이를 가질 수 있다. 신호 처리 기법은 크게 신호 정렬[8,9], 잡음 제거[10,11], 신호 압축[8,12]의 세 단계로 나눈다. 이 중 신호 정렬 기법과 잡음 제거 기법에 대한 연구가 활발히 진행되는 반면, 신호 압축 기술에 대한 연구는 아직까지 미비한 실정이다.

DPA와 CPA 공격에서 신호 압축 기술을 적용했을 때 가장 큰 장점은 분석 수행 시간의 단축과 메모리의 감소이다. 하지만 신호 압축으로 인해 원신호에서 전력 분석과 연관된 중요한 성분이 손실된다면 이는 분석 성능을 오히려 떨어뜨리는 원인이 된다. 따라서 고차원의 데이터를 저차원의 데이터로 바꾸는 신호 압축 기술을 수행할 때, 원신호의 의미 있는 성분이 최대한 손실되지 않도록 주의해야 한다. 기존의 신호 압축 기술에는 Raw integration[8], Maximum extraction[8], Sum of squares[8], Peak Selection[12] 방법 등이 존재한다. 위 압축 기법들은 상당히 직관적인 방법으로 신호의 특성을 전혀 고려하지 않았기 때문에 DPA 성능을 저하시키기도 한다.

본 논문에서는 기존의 압축 기술들의 문제점을 보완한 주성분 분석 (Principal Component Analysis, PCA)[13]을 이용한 새로운 신호 압축 기술을 제안한다. 제안하는 압축 기술은 기존 기술과 달리 전력 신호의 특성을 고려한 방법으로써, 한 클록 내에서 각 신호의 비중을 달리하여 신호를 압축하는 기법이다. 이를 위해 본 논문에서는 주성분 분석을 활용해 신호 압축에 사용할 수 있는 최적의 웨이트 벡터 (weight vector)를 찾았다. 또한 기존 압축 기술과 제안하는 압축 기술의 실험적인 비교 분석을 통해 제안하는 압축 기술이 기존 압축 기술보다 향상되었음을 확인하였다.

본 논문의 구성은 다음과 같다. 2절은 전력 분석을 위한 기존 신호 압축 기술을 소개하고, 3절에서는 제안하는 압축 기술에 대해 설명한다. 4절에서는 제안한 압축 기술과 기존 기술의 성능을 비교 분석하며, 5절에서 본 논문의 결론을 맺는다.

II. 기존의 신호 압축 기술

신호 압축 기술에 대한 기존의 연구들은 전력 신호의 특성을 반영하지 않는 다소 직관적인 접근 방법이다. 전력 분석을 위한 기존의 신호 압축 기술들은 다음과 같다

• Raw Integration

Raw Integration 기법은 각 클록 내의 모든 신호를 더해 한 포인트로 압축하는 기법으로 가장 기본적인 압축 기술이다. 이 기법은 전력 분석 관점에서 한 클록 내의 신호 전부는 모두 동등한 의미를 가지는 것으로 여긴다.

• Maximum Extraction

Maximum Extraction 기법은 각 클록 내의 신호에 대해 최대 값을 갖는 한 포인트의 신호를 추출하는 압축 기술이다. 이 기법은 한 클록내의 신호에서 가장 많은 전력을 소비하는 위치의 전력을 전력 분석 관점에서 가장 의미있는 신호로 판단하는 방법이다.

• Sum of Squares Method

Sum of Squares Method 기법은 각 클록 내의 모든 신호의 제곱 값을 더해 한 포인트로 압축하는 기술이다. 이 기법은 위의 두 압축 기술의 특징을 적절히 섞은 것이다. 즉, 한 클록내의 신호에서 가장 많은 전력을 소비하는 위치의 전력을 가장 의미있는 신호로 판단함과 동시에, 소비량이 작은 신호에 대해서도 의미를 부여하는 방법이다. 결국 각 신호 크기만큼 weight를 주어서 한 클록 신호를 더하는 방법이다.

전력 분석을 위한 최적의 신호 압축 기술은 한 클록 내의 신호 $x=[x(1), x(2), ..., x(m)]$의 각 포인트들에 대해 최적의 weight vector $w=[w(1), w(2), ..., w(m)]$ ($\| w \| = \sqrt{\sum_{t=1}^{m} w(t)^2} = 1$)를 찾는 것이다. Weight vector에 의해 원신호 벡터 x는 다음과 같이 한 포인트의 신호 X로 압축된다.

$$X = w^T x = \sum_{t=1}^{m} w(t)x(t) \quad (1)$$

앞에서 설명한 모든 신호 압축 기술 또한 이러한 weight vector에 의해 신호를 압축한 것이며 원 신호 $x=[x(1), x(2), ..., x(m)]$에 대해 각 신호 압축 기술에 대한 weight vector는 다음 표와 같다.

〔표 1〕 기존 신호 압축 기술의 weight vector

신호 압축 기법	weight vector $w=[w(1), w(2), ..., w(m)]$
Raw integration	$w=[\frac{1}{\sqrt{m}}, \frac{1}{\sqrt{m}}, ..., \frac{1}{\sqrt{m}}]$
Maximum Extraction	$\begin{cases} w(t)=1 & ; t=arg\max_i x(i) \\ w(t)=0 & ; otherwise \end{cases}$
Sum of Squares	$w(t)=\frac{x(t)}{\| x \|}$

III. 제안하는 신호 압축 기술

앞 절에서 언급한 신호 압축 기술이 비록 DPA와 CPA의 성능을 높일 수 있겠지만 각 기술에서 사용한 weight vector는 비교적 단순한 방법에 의해 생성되어 최적의 weight vector라고 주장하기에는 다소 무리가 있다. 본 절에서는 최적의 m차원 weight vector $w=[w(1), w(2), ..., w(m)]^T$를 찾기 위해 주성분 분석의 개념을 활용한다. 즉, 공격에 이용되는 n개의 한 클록 신호 $x_i=[x_i(1), x_i(2), ..., x_i(m)]^T (1 \le i \le n)$에 대해 다음의 식을 만족하는 weight vector $g=[g(1), g(2), ..., g(m)]^T$를 찾는다.

$$g=\arg max_w \ Var\{w^Tx_1, w^Tx_2, ..., w^Tx_n\} \qquad (2)$$

식 (2)에서 $w^Tx_i=\sum_{j=1}^{m} w(j)x(j)$를 의미한다. 이러한 weight vector g를 찾는 작업은 원신호에서 전력 분석에 의미가 있는 신호를 데이터 값에 의존해 변동이 큰 신호 값으로 판단하는데 근거하여 수행된다.

압축 신호들로 이루어진 분포 $Z=\{w^Tx_1, w^Tx_2, ..., w^Tx_n\}$에 대해 $Var(Z)$의 값은 다음과 같이 변형된다.

$$Var(Z)=\frac{1}{n}\sum_{i=1}^{n}(w^Tx_i-w^T\bar{x})^2$$
$$=\frac{1}{n}\sum_{i=1}^{n}w^T(x_i-\bar{x})(x_i-\bar{x})^Tw=w^TSw$$
$$(S=\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(x_i-\bar{x})^T,$$
$$\bar{x}=[\frac{1}{n}\sum_{i=1}^{n}x_i(1), \frac{1}{n}\sum_{i=1}^{n}x_i(2), ..., \frac{1}{n}\sum_{i=1}^{n}x_i(m)]^T).$$

위의 식에서 S는 $m \times m$의 covariance 행렬이며 $\bar{x}$는 평균 벡터이다.

$Var(Z)$가 최대값을 갖도록 하는 열 벡터 w를 찾는 작업은 다음과 같이 수행된다.

$$Var(Z)=w^TSw-\lambda(w^Tw-1)$$
$$\frac{\partial Var(Z)}{\partial w}=2Sw-2\lambda w=0$$
$$\Rightarrow Sw=\lambda w$$
$$\Rightarrow Var(Z)=w^TSw=\lambda$$

위의 식에서 $Var(Z)$를 w로 편미분하여 0이 되도록 하는 벡터 w가 $Var(Z)$가 최대가 되도록 하는 후보 벡터가 될 수 있다. 이러한 작업은 데이터 벡터들의 covariance matrix S의 고유 벡터와 고유 값을 찾는 문제로 귀결된다. 위의 식에서 보는 바와 같이 해당 고유 벡터들에 대하여 선형 변환을 수행했을 때의 분산 값은 대응되는 고유 값이 된다. 따라서 가장 큰 고유 값 λ를 갖는 고유 벡터가 식 (2)을 만족하는 g가 된다. $Sw=\lambda w$를 만족하는 고유 벡터 w는 S의 rank 만큼 존재하게 되며 각 고유 벡터들은 서로 직교하는 성질을 갖는다. 따라서 찾고자 하는 선형 변환 벡터는 고유 값 λ 중 큰 값 순서대로 고유 벡터를 선택해 사용할 수 있다. $\lambda_1 \ge \lambda_2 \ge .... \ge \lambda_k$의 순서대로 고유 값들이 정렬되고 각 고유 값 λ_i에 해당하는 고유 벡터를 w_i라고 한다면, 고유 값이 큰 p개의 고유 벡터들 (w_1, w_2, ..., w_p)을 주성분 벡터로 투영해서 사용할 벡터들로 선택하면 된다.

DPA와 CPA를 수행하기 위해서는 신호 압축을 수행하더라도 데이터 값의 헤밍 웨이트 또는 헤밍 디스턴스에 의존한 전력 소비 패턴이 유지되어야 한다. 만약 다수의 클록에서 소비된 전력을 한 번에 주성분 벡터를 이용해 변환한다면 이러한 선형성을 잃어버릴 수 있게 된다. 따라서 신호 압축은 한 클록 연산 상에서 이루어져야만 한다. 다음은 한 클록 내에서 원신호를 주성분 벡터로 변형 시키는 새로운 압축 기법이다. n개의 전력 파형에 대한 신호 압축 과정은 다음과 같다. (m:클록 사이즈, p:선택한 주성분 수)

- 신호 정렬 후, n개의 전력 파형 각각에 대해 한 클록에 해당하는 신호를 추출한다.
- 이 추출된 신호들을 $X=\{x_1, x_2, ..., x_n\}$으로 구성하고 covariance matrix $S=\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(x_i-\bar{x})^T$를 연산한다.
- Matrix S에 대해 고유 벡터들과 고유 값들을 구한다.

- 큰 고유 값들에 해당하는 p개의 고유 벡터들을 선택한다.(시각적으로 원신호와 연관 없어 보이는 잡음 성분으로 판단되는 고유 벡터들은 버린다.)
- 위에서 선택한 p개의 고유 벡터들을 더해 weight vector w를 구한다.
- 이 weight vector w를 이용, 신호 $X=\{x_1, x_2, ..., x_n\}$의 n개의 한 클록 신호들을 각각 한 포인트로 이루어진 n개의 신호 $\{w^T x_1, w^T x_2, ..., w^T x_n\}$로 압축한다.
- 각 클록에 대해 위의 과정을 반복 수행한다.

물론 위 과정에서 구한 weight vector는 클록 사이즈만 유지된다면 추가적으로 수집되는 전력 파형에 대해서도 동일하게 적용할 수 있다. 하지만 소프트웨어로 구현된 암호 연산기는 다수의 클록동안 이루어지므로 매 클록마다 위의 과정을 반복 수행하는 것은 많은 계산량을 요구한다. 따라서 이러한 경우 신호 압축 효과가 떨어지더라도 특정 클록에 대해서만 weight vector를 구한 후 모든 클록에 적용하는 것도 가능하다.

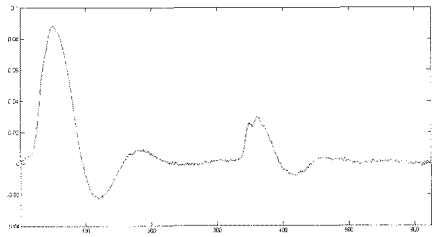
〔표 2〕 CPA를 위해 각 기법에 필요한 전력 파형 개수

	최초 수집 신호	Raw Integration	Maximum Extraction	Sum of Squares	Ours
파형개수	610	3200	610	620	380

IV. 성능 비교

본 절에서는 제안하는 신호 압축 기술과 기존의 신호 압축 기술의 성능을 비교하기 위해 각 신호 압축 기술에 대한 CPA를 수행하였다. 비교에 사용된 전력 신호 특징을 요약하면 다음과 같다.

- 하드웨어 구조 : 〔14〕 (CHES 2009, DPA Contest 파형)
- 암호 알고리즘 : DES
- 한 클록의 길이 : 625 포인트
- 한 파형에 속한 클록 수 : 31 클록
- 분석 라운드 : 1 라운드
- 최초 수집 신호에서 한 클록에 해당하는 전력 파형 :



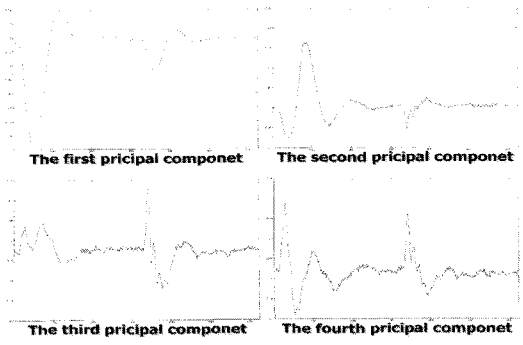
〔그림 1〕 원신호의 한 클록 파형

한 클록에서 전력 파형들로 구성된 covariance matrix의 고유 벡터와 고유 값을 구한 후, 큰 고유 값을 갖는 네 개의 고유 벡터를 도식화하면 다음과 같다.

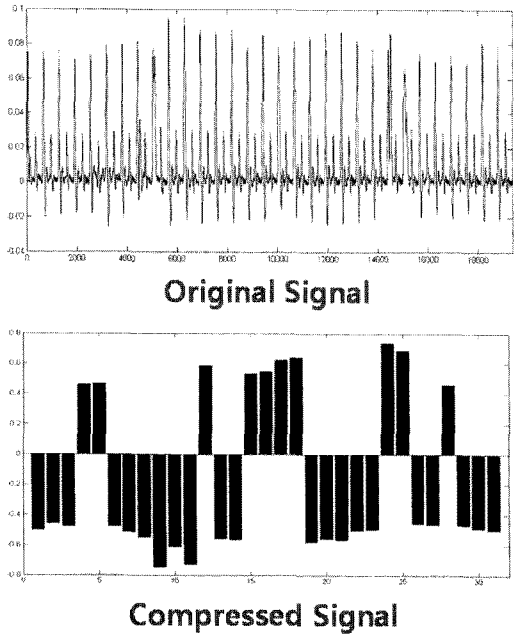
〔그림 2〕와 같이 첫 번째 고유 벡터와 두 번째 고유 벡터는 압축 전의 최초 수집 신호와 거의 같은 굴곡을 갖는 반면, 세 번째와 네 번째의 고유 벡터는 최초 수집 신호와 상당히 다른 굴곡이어서 의미 없는 노이즈 성분으로 판단하였다. 따라서 본 실험에서는 첫 번째, 두 번째의 고유 벡터만을 더하도록 weight vector $g(p=2)$로 사용하였으며 이 weight vector와 식 (1)을 이용해 각 클록의 전력 신호를 한 포인트로 압축하였다. 〔그림 3〕은 최초 수집 신호와 압축 신호에 대한 그림이다.

위의 그림에서 보는 바와 같이 양의 방향으로만 소비되던 신호가 신호 압축 후 양과 음의 방향으로 분포됨을 확인할 수 있었다. 이는 각 클록 신호에 대해 주성분 분석을 수행했을 때, 고유 벡터의 성분은 동일하나 방향이 반대가 될 수 있기 때문에 나타나는 현상이다. 하지만, 이러한 현상은 전력 분석을 수행했을 때, 상관 계수의 절대값을 비교하면 되므로 문제가 되지 않는다.

압축 기술의 성능을 비교하기 위한 중요한 요소는 신호 압축에 필요한 시간을 줄이고 최초 수집 신호의



〔그림 2〕 한 클록 신호의 고유 벡터들

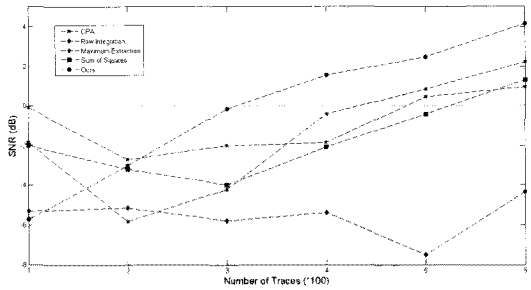


〔그림 3〕 최초 수집 신호와 제안하는 압축 기법에 의해 압축된 신호

의미있는 성분이 최대한 손실되지 않도록 하는 것이다. 하지만 기존 방법들과 제안하는 압축 기술은 weight vector가 사전에 계산된다면 신호를 압축하는데 필요한 시간은 거의 같다. 따라서 본 논문에서는 압축 시간을 따로 비교하지 않고 각 압축 기술에 대해 DES 1 라운드의 48 비트 모든 키를 찾기 위해 필요한 트레이스 개수를 실험을 통해 비교하였다. 다음 표는 주성분 분석을 이용한 신호 압축 기술이 기존의 다른 압축 기술인 Raw Integration, Maximum Extraction, Sum of Squares Method에 비해 성능이 우수함을 나타낸다.

〔표 2〕에서 제안하는 압축 기술을 이용해 CPA를 수행할 때, 키를 찾기 위해 필요한 전력.파형의 개수는 압축 전의 최초 수집신호에 대한 CPA에 필요한 전력 파형의 개수보다 상당히 적다. 이는 본 제안 기법인 주성분 분석 기반의 압축 기법이 분석 대상 파형의 암호 연산 부분을 비교적 잘 파악했기 때문에 나타나는 현상이다.

〔그림 4〕는 각각의 신호 압축 방식에 따른 전력 분석의 성능을 S/N 비로 비교한 그림이다. S/N 비의 측정 방법은 1 라운드의 첫 번째 6 비트 키에 대해 올바른 키일 경우의 상관 계수 값과 올바르지 못한 키일 경우의 상관 계수 값 중 최고치를 데시벨(dB) 단위로



〔그림 4〕 기존 압축 기술과 제안 압축 기술의 S/N 비 비교

비교한 결과이다. 따라서 0〔dB〕 이상의 값을 가지는 경우에는 올바른 키를 찾는다고 판단할 수 있다.

V. 결 론

본 논문에서는 전력 분석의 성능 향상을 위한 새로운 신호 압축 기술을 제안하였다. 제안하는 신호 압축 기술은 기존 압축 기술과 달리 전력 신호의 특성을 고려하여 주성분 분석을 통해 찾은 weight vector로 신호를 압축하였다. 본 논문의 신호 압축 기술을 하드웨어로 구현된 DES 연산 파형에 적용해 CPA를 수행했을 경우, 기존 압축 기술들이 약 610~3200개의 전력 파형을 필요로 하는 반면, 본 기술은 약 380 개의 파형으로 분석이 성공함을 확인할 수 있었다. 이는 제안하는 압축 기술이 기존 기술에 비해 상당한 성능 향상이 있음을 의미한다. 본 압축 기술의 성능은 본 논문에서의 성능 비교를 통해 하드웨어로 구현된 암호 모듈에 대해 검증되었다. 따라서, 소프트웨어로 구현된 암호 모듈이 소비한 전력 파형에 대해 본 압축 기술을 적용해 성능을 비교하는 것이 향후 과제이다.

참고문헌

〔1〕 P. Kocher, J. Jaffe, and B. Jun, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Others Systems," CRYPTO 1996, LNCS 1109, pp. 104-113, Springer-Verlag, 1996.

〔2〕 Bellcore Press Release, "New threat model breaks crypto codes," or D. Boneh, R. A. DeMillo, and R. J. Lipton, "On the importance of checking cryptographic protocols for faults," EUROCRYPT 1997,

LNCS 1233, pp. 37-51, Springer-Verlag, 1997.

[3] S. M. Yen, S. J. Kim, S. G. Lim, and S. J. Moon, "A countermeasure against one physical cryptanalysis May Benefit Another Attack," ICISC 2001, LNCS 2288, pp. 414-427, Springer-Verlag, 2001.

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

[5] P. Kocher, J. Jaffe, and B. Jun, "Introduction to differential power analysis and related attacks," Available online at http://www.cryptography.com/dpa/technical, 1998.

[6] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Power analysis attacks on modular exponentiation in Smart cards," CHES 1999, LNCS 1717, pp. 144-157, Springer-Verlag, 1999.

[7] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, "The EM Side-Channel(s)," CHES 2002, LNCS 2523, pp. 29-45, Springer-Verlag, 2003.

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

[9] 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, Springer-Verlag, 2006.

[10] J. Ryoo, D. Han, S. Kim and S. Lee, "Performance Enhancement of Differential Power Analysis Attacks with Signal Companding Methods," IEEE Signal Processing Letters, Vol. 15, Issue 2008, pp. 625-628, IEEE, October 2008.

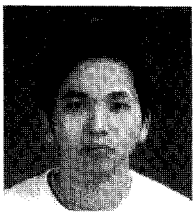
[11] T. Le, J. Clediere, C. Serviere, and J. L. Lacoume, "Noise Reduction in Side Channel Attack Using Fourth-Order Cumulant," IEEE Transactions on Information Forensics and Security, Vol. 2, Issue 4, pp. 710-720, IEEE, July 2007.

[12] Y. Kang, D. Choi, B. Chung, H. Cho, and D. Han, "Efficient Key Detection Method in the Correlation Electromagnetic Analysis Using Peak Selection Algorithm," Journal of Communications and Networks, Vol. 11, No. 6, pp. 556-563, KICS, November 2009.

[13] I. T. Jolliffe. Principal Component Analysis. Springer-Verlag, New York, 1986.

[14] S. Guilleya, P. Hoogvorsta, and R. Pacaleta, "A fast pipelined multi-mode DES architecture operating in IP representation," Integration, the VLSI Journal Vol. 40, Issue 4, pp. 479-489, July 2007.

〈著者紹介〉



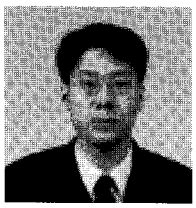
김 희 석 (HeeSeok Kim) 학생회원
2006년 2월: 연세대학교 수학과 졸업(학사)
2008년 2월: 고려대학교 정보경영공학전문대학원 공학석사
2008년 3월~현재: 고려대학교 정보경영공학전문대학원 박사과정
〈관심분야〉 부채널 공격, 암호시스템 안전성 분석 및 고속구현, 암호칩 설계 기술

김 현 민 (Hyunmin Kim) 학생회원
2006년 2월: 동국대학교 전자공학과 졸업(학사)
2008년 12월: 삼성전자 반도체 총괄, 메모리 사업부 연구원
2009년 3월~현재: 고려대학교 정보보호대학원 석사과정
2010년 9월~현재: Katholieke Universiteit of Leuven, COSIC, International Scholar.
〈관심분야〉 부채널 공격 및 대응기법 연구, 암호칩 설계 기술, 초경량 암호 설계 기술

박 일 환 (IlHwan Park) 정회원
1988년 2월: 고려대학교 수학과 졸업
1990년 2월: 고려대학교 수학과 석사
1996년 2월: 고려대학교 수학과 박사
1996년 5월: 한국전자통신연구원
2000년 1월~현재: 한국전자통신연구원 부설연구소
〈관심분야〉 정보보호이론

김 창 균 (ChangKyun Kim) 정회원
2001년2월: 경북대학교 전자전기공학부 졸업
2003년2월: 경북대학교 전자공학과 석사
2003년3월~현재: 경북대학교 전자공학과 박사과정
2004년11월~현재: 한국전자통신연구원 부설연구소
〈관심분야〉 부채널분석, 스마트카드보안, 암호알고리즘구현

류 희 수 (Heuisu Ryu) 정회원
1989년 2월: 고려대학교 수학과 이학사
1992년 2월: 고려대학교 수학과 이학석사
1999년 5월: 미국 Johns Hopkins 수학과 Ph.D
2002년 9월~현재: 경인교육대학교 수학교육과 부교수
〈관심분야〉 암호이론 및 알고리즘, 정보보호교육, 정수론, 수학교육



박 영 호 (Young-Ho Park) 정회원
1990년 2월: 고려대학교 수학과 이학사
1993년 2월: 고려대학교 수학과 이학석사
1997년 2월: 고려대학교 수학과 이학박사
2002년 3월~현재: 세종 사이버 대학교 부교수
〈관심분야〉 정수론, 공개키 암호, 암호 프로토콜, 부채널 공격