情報保護學會論文誌
第20卷 第4號, 2010. 8

차분 전력 분석 공격의 성능 향상을 위한 전처리 기법*

이 유 석,[1†] 이 유 리,[2] 이 영 준,[2] 김 형 남,[2‡]
[1]한국전자통신연구원, [2]부산대학교

A Pre-processing Technique for Performance Enhancement of the Differential Power Analysis Attack*

You-Seok Lee,[1†] Yu-Ri Lee[2], Young-Jun Lee[2], Hyoung-Nam Kim[2‡]
[1]Electronics and Telecommunications Research Institute, [2]Pusan National University

요 약

차분 전력 분석(Differential Power Analysis, DPA) 기법은 암호화 과정 중 발생하는 누설정보를 이용하는 효과적인 부채널 공격(side-channel attack, SCA) 중의 하나로 알려져 있다. 그러나 공격에 사용되는 누설 전력 신호에는 암호화와 관련이 없는 동작에 의해 야기된 전력 신호가 함께 포함되어 있으며, 이로 인해 공격의 효율성이 크게 저하된다. 따라서 본 논문에서는 차분 전력 분석 기법의 공격 성능을 향상시키기 위해, 측정된 전력 신호로부터 암호화 과정에 관련된 부분만을 추출하는 전처리 방법을 제안한다. 모의실험 결과를 통해 제안된 전처리 방법을 적용한 차분 전력 분석 공격은 기존의 차분 전력 분석 공격에 비해 매우 적은 수의 누설 전력 신호만으로도 암호화 알고리즘에 사용된 비밀 키를 찾을 수 있음을 보인다.

ABSTRACT

Differential Power Analysis (DPA) is well known as one of efficient physical side-channel attack methods using leakage power consumption traces. However, since the power traces usually include the components irrelevant to the encryption, the efficiency of the DPA attack may be degraded. To enhance the performance of DPA, we introduce a pre-processing technique which extracts the encryption-related parts from the measured power consumption signals. Experimental results show that the DPA attack with the use of the proposed pre-processing method detects correct cipher keys with much smaller number of signals compared to that of the conventional DPA attack.

Keywords: Side channel attack, Differential power analysis, pre-processing technique

I. 서 론

부채널 공격 (Side Channel Attacks, SCAs)이란 암호화 알고리즘의 이론적 취약점이 아닌, 암호화 과정이 일어나는 동안 누설되는 물리적인 정보 (시간정보, 전력소비량, 전자기파 등) 를 이용하여 암호화 알고리즘에 사용된 비밀 키를 알아내는 공격 기법이다 [1,2]. 부채널 공격은 사용되는 누설 정보의 종류에 따라 시차 공격, 전력 분석 공격, 전자기 분석 공격 기법으로 구분된다. 지금까지 알려진 전력 분석 공격에는 단순 전력 분석 (Simple Power Analysis, SPA), 차분 전력 분석 (Differential Power Analysis, DPA) [3,4] 과 상관 전력 분석 (Correlation Power Analysis, CPA) [5] 등이 있으며 전자기 분석 공격 기법에는 단순 전자기 분석 (Simple Electro-

* 접수일(2010년 4월 30일), 수정일(1차: 2010년 7월 12일, 2차: 2010년 8월 10일), 게재확정일(2010년 8월 11일)
* 이 논문은 2008년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2008-0061842)
† 주저자, yslee75@etri.re.kr
‡ 교신저자, hnkim@pusan.ac.kr

Magnetic Analysis, SEMA) [6] 및 차분 전자기 분석 (Differential ElectroMagnetic Analysis, DEMA)[7] 등이 있다.

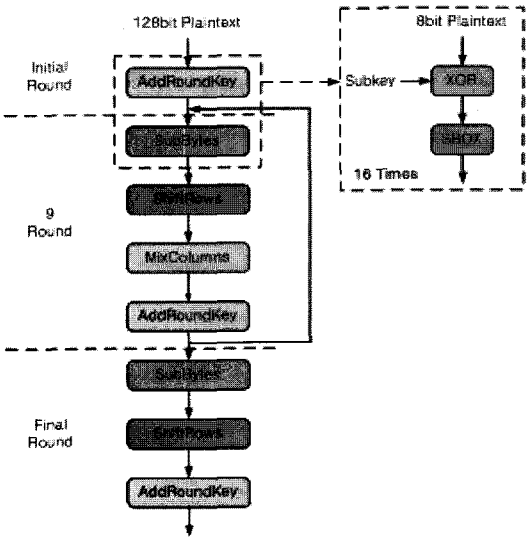
전력 분석 공격은 전력 소비 모델과 측정된 전력 신호의 통계적 특성을 비교, 분석하여 암호화에 사용된 키를 찾아내는 강력한 부채널 공격 방법이다. 그러나 측정된 전력 신호에는 암호화 과정에 의한 전력 소모 이외에도 잡음 및 해당 보안 장치를 구성하는 다양한 부품들의 동작에 의한 전력 소모가 함께 반영되어 있다. 이러한 문제는 평균 과정을 통해 측정된 전력 신호의 잡음을 줄임으로써 어느 정도까지는 해결이 가능하지만, 실제 키를 정확하게 추정하기 위해서는 여전히 많은 수의 전력 신호를 필요로 한다. 이는 측정 신호의 고차 통계 특성을 이용한 잡음 감소 기법[8] 및 웨이블릿 (Wavelet) 기반의 잡음 제거 기법[9] 등에 의해 해결될 수 있다. 그러나 측정된 전력 신호에 반영되어 있는 암호화 과정과 무관한 전력 소모의 영향을 극복할 수 있는 방법에 대한 연구는 이루어지지 않아, 여전히 많은 수의 전력 신호가 실제 키를 추정하기 위해 요구된다.

본 논문에서는 이러한 연구의 일환으로, 측정된 전력 신호 파형에서 암호화 동작과 직접적으로 관련된 부분의 파형만을 추출하여 이를 차분 전력 분석 공격에 적용하는 전처리 방법을 제안한다. 제안된 전처리 방법을 적용한 차분 전력 분석 공격은 기존의 차분 전력 분석 공격에 비해 매우 적은 수의 전력 신호로도 '0'과 '1' 그룹들의 평균을 보다 정확하게 추정한다. 따라서 암호화 과정에 사용된 키를 보다 적은 수의 전력 신호로 정확하게 추정함으로써, 기존 차분 전력 분석 공격의 효율을 향상시킨다.

본 논문은 다음과 같이 구성된다. 2장에서는 본 논문에서 공격 대상으로 사용하고 있는 AES (Advanced data Encryption Standard) 알고리즘과 차분 전력 분석 공격을 통하여 비밀 키를 추정하는 과정에 대해 간략히 설명한다. 3장에서는 AES 알고리즘 동작 시 측정된 전력 신호 파형을 예로 들어 본 논문에서 제안하는 전처리 과정에 대해 상세히 설명하고, 4장에서 모의실험을 통해 제안된 전처리 기법을 적용한 차분 전력 분석 공격의 성능을 분석한다. 마지막으로, 5장에서 본 논문의 결론을 맺는다.

II. 사전 연구 (Previous works)

본 장에서는 암호화 알고리즘 중의 하나인 AES와



[그림 1] AES-128 알고리즘 동작 과정

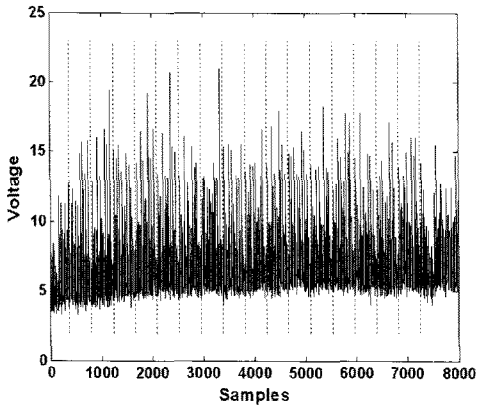
차분 전력 분석을 통하여 AES 알고리즘에 사용된 비밀 키를 추정하는 과정에 대해 간략하게 살펴본다.

2.1 AES 알고리즘 [10]

기존의 표준 암호 알고리즘이었던 DES (Data Encryption Standard) 를 대체할 목적으로 개발된 AES는 128, 192 및 256 비트 단위의 평문과 비밀 키를 수용할 수 있는 유연성을 가지며, 기존의 공격기법 (linear 및 differential 공격 등) 에 대해 안전한 것이 특징이다. [그림 1]은 AES-128 알고리즘의 동작과정을 블록도로 나타낸 것이다. 각 라운드마다 비밀 키를 이용하여 암호화 되며, 행의 편이, 열의 혼합과정을 통하여 최종 암호문이 만들어진다. 이때, 각 라운드의 'AddRoundKey' 연산은 8비트 블록 단위로 평문과 XOR 연산을 수행 후 S-Box를 통한 16번 치환 과정으로 이루어진다.

2.2. 차분 전력 분석 (Differential Power Analysis: DPA) 공격 [3,4]

P. Kocher 등에 의해 제안된 차분 전력 분석 공격은 암호화 동작 시 저장되는 특정 비트의 값이 "1"일 때의 소비 전력과 "0"일 때의 소비 전력이 다르다는 가정을 이용하여 비밀 키를 찾아내는 방법이다. 차분 전력 분석 공격을 수행하기 위해 공격자는 M개의 평문에 대한 암호화를 수행하며 이때 발생하는 전력 소



〔그림 2〕 AES 암호화 과정에서 두 번째 round 동작 시 측정된 전력 신호

모를 각각 N개의 이산 샘플로 측정하여 저장한다. 그리고 공격자는 평문 $P_i(i=1,\ldots,M)$와 추정 키 값(key hypothesis) K_k를 입력으로 하는 선택 함수(selection function) $D(P_i, K_k)$의 결과 값을 기록한다. 선택 함수는 식 (1)과 같이 정의된다.

$$D(P_i, K_k) = P_b[SBOX(P_i \oplus K_k)] \quad (1)$$

여기서, $P_b[\bullet]$는 치환 함수 (substitution-box, S-Box) 의 8 비트 출력 중 b번째 비트의 값을 나타내고 K_k는 비밀 키로 추정될 수 있는 모든 키 값을 나타낸다. 그리고 $SBOX(x)$는 AES 알고리즘에 사용된 치환 테이블에 근거한 8비트 단위의 치환 함수이다.

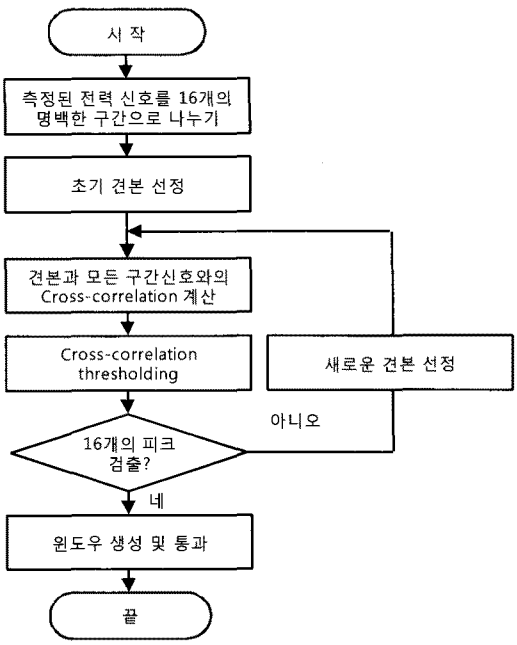
선택 함수는 평문과 추정 키의 조합에 따라 "0" 또는 "1"의 값을 출력으로 가지는데, 공격자는 이에 대응되는 측정된 전력 소비 파형을 0 그룹 혹은 1 그룹으로 분류한다. 이후, 분류된 각 그룹에 속한 파형들의 평균의 차(Difference), $\Delta_D[1,\ldots,N]$를 모든 추정 키에 대해 계산한다. M개의 평문 $P_i(i=1,\ldots,M)$가 암호화 되는 동안 측정된 M개의 N 샘플 전력 신호를 $W_i[1,\ldots,N](i=1,\ldots,M)$ 라 하고 추정 가능한 키가 256개라고 가정하면, 256개의 모든 키에 대한 각 평균의 차, $\Delta_D[1,\ldots,N]$는 다음 식 (2)와 같이 구할 수 있다.

$$\Delta_D[1,\ldots,N] = \frac{\sum_{i=1}^{M} D(P_i, K_k)\, W_i[1,\ldots,N]}{\sum_{i=1}^{M} D(P_i, K_k)} - \frac{\sum_{i=1}^{M} (1 - D(P_i, K_k))\, W_i[1,\ldots,N]}{\sum_{i=1}^{M} (1 - D(P_i, K_k))} \quad (2)$$

수식 (2)에서 추정 키와 비밀 키가 일치하는 경우에는 분류함수에 의해 측정된 전력 신호가 0 그룹과 1 그룹으로 정확하게 분류되므로 해당 키에 대한 평균의 차, $\Delta_D[1,\ldots,N]$의 특정 부분에서 다른 추정 키에 대한 평균 차에 비해 큰 값을 가지는 피크(Peak)가 나타난다. 이러한 과정을 통하여 차분 전력 분석 공격은 가장 큰 피크 값을 나타내는 추정 키 K_k를 실제 키로 추정함으로써 암호화에 사용된 키를 찾아낼 수 있다.

III. 제안하는 전처리 기법 (Proposed preprocessing method)

2장에서 살펴본 바와 같이, AES는 128비트의 평문에 대해서 8비트 XOR 연산 및 치환 과정을 반복적으로 16번 수행한다. 측정된 전력 신호에는 이러한 반복과정이 그대로 반영되어 비슷한 형태의 전력 소비 파형이 16번 순차적으로 나타나게 된다. 〔그림 2〕는 AES 알고리즘 동작 시 두 번째 라운드의 치환 과정 동안 측정된 전력 소비 신호 파형을 나타내며, 위에서 언급한 바와 같이, 8비트의 16개 블록의 치환 과정에 의한 전력 소비가 명확하게 구분되는 것을 알 수 있다. 즉, AES 알고리즘에 대한 부채널 공격 시에는 하나의 S-Box 단위로 비밀 키를 추정하게 되며 이때 해당 구간의 전력 신호 파형만을 이용하여 전력 분석을



〔그림 3〕 제안하는 전력 신호 전처리 기법

수행함으로써 공격의 효율을 높일 수 있음을 직관적으로 알 수 있다.

그러나 각 S-box 에 해당하는 신호만을 이용하여 차분 전력 분석 공격을 수행하더라도 여전히 많은 수의 전력신호가 필요하게 되는데, 이는 공격에 이용되는 전력 신호에 AES 알고리즘이 구현된 휴대용 개인 정보 단말기 또는 네트워크 장비를 구성하는 다양한 장치들에 의한 전력 소모도 함께 포함되어 있기 때문이다. 이로 인해, 실제 키를 찾기 위해서는 암호화 과정과 무관한 전력 소모 효과를 줄여야 하므로 많은 수의 측정 전력 신호가 필요하게 되며, 결과적으로 전력 분석 공격의 효율이 떨어지게 된다. 따라서 16개의 구간으로 나누어진 전력 신호에서 S-Box의 동작과 직접적으로 관련이 있는 전력 소비 부분만을 추출하여 이를 전력 분석 공격에 사용한다면, 공격의 효율을 크게 높일 수 있을 것이다.

이를 위해 본 논문에서는 측정된 전력 신호에서 암호화에 의한 신호만을 추출하는 전처리 기법을 개발함으로써 차분 전력 분석 기법의 공격 효율성을 향상시키는 방법을 제안하였으며 그 과정은 [그림 3]에 제시되어 있다. 제안된 전처리 기법에 대한 자세한 설명은 다음과 같다.

1) 측정된 전력 신호의 파형을 육안으로 관찰하여, 16개의 각 S-box 치환 동작에 의한 구간 파형들로 구분한다.
2) 16개 구간의 신호 파형 중 1개 구간의 파형을 초기 견본 파형 T 로 선택한다.
3) 선정된 견본 파형과 전 구간 신호 파형과의 상호 상관관계(cross-correlation)를 한 샘플씩 이동하면서 식 (3)을 통해 계산한다.

$$Corr_j = \frac{E(T[1,...,L]\,W[j,...,j+L-1])}{\sqrt{VAR(T[1,...,L])\,VAR(W[j,...,j+L-1])}} - \frac{E(T[1,...,L])E(W[j,...,j+L-1])}{\sqrt{VAR(T[1,...,L])\,VAR(W[j,...,j+L-1])}} \quad (3)$$

여기서 L은 견본 파형의 길이를 의미하고, j 는 샘플 인덱스로 $[1,...,L]$까지의 값을 가진다. $\sqrt{VAR(T[1,...,L])}$ 와 $\sqrt{VAR(W[j,...,j+L-1])}$ 는 각각 견본 파형 $T[1,...,L]$ 와 전력 신호 파형 $W[j,...,j+L-1]$의 표준편차를 의미한다.

4) 계산된 상호 상관관계(cross-correlation)를 식(4)와 같이 제한하여 피크의 개수 P가 16이 되는지 판단한다.

$$P = \sum_{j=1}^{N-L} (Corr_j \geq \theta_T) \quad (4)$$

여기서 θ_T는 문턱 값으로 1에 가까운 값으로 설정되나, 측정된 전력 신호의 신호 대 잡음비 (SNR) 에 따라 가변될 수 있다.

5) 만약 16개의 피크를 검출할 수 없는 경우, 현재의 견본 파형이 S-Box 치환 동작과 직접적으로 관계없는 H/W 동작에 의한 전력 소비를 여전히 반영하고 있음을 의미한다. 그러므로 S-Box 치환 동작과 관계있는 파형 구간만을 추출하기 위해 새로운 견본 파형을 생성하고 3단계로 돌아가 알고리즘을 계속 수행한다. 새로운 견본 파형은 초기 견본 파형을 한 피크의 샘플 개수인 L_R 만큼 줄여가며 선정한다. 측정된 전력 신호 파형에서 전력 소모는 피크로 나타나게 되고 이 피크들은 데이터 버스가 동작하는 주파수 마다 발생하므로, 이를 샘플링한 주파수로 나누어 주면 각 피크들 간의 간격 샘플 개수인 L_R을 식 (5)와 같이 구할 수 있다.

$$L_R = \frac{f_s}{f_{bus}} \quad (5)$$

즉, 제안하는 전처리 기법은 구분된 구간 파형에 포함된 피크들이 암호화 과정에 직접적으로 관계된 피크인지 판단하여 그렇지 않을 경우, 각 피크들을 제외해 나가면서 S-box 치환동작과 정확하게 관계된 구간을 찾는다.

6) 만약 16개의 피크를 검출할 수 있는 경우, 견본 파형의 길이를 가지는 윈도우를 식 (6)과 같이 생성한다.

$$H[n] = \begin{cases} 1, & SP_i \leq n < SP_i + L_T \\ 0, & otherwise \end{cases} \quad (where\ i = 1,...,16) \quad (6)$$

여기서 L_T는 최종적으로 선택된 견본 파형의 길이를 의미하고, SP_i는 i 번째 피크를 가지는 샘플의 인덱스를 의미한다. 전 구간의 전력 신호에 생성된 윈도우를 통과시킴으로써 각 S-Box의 동작과 직접적인 관련이 있는 전력 신호 파형을 얻을 수 있다.

기존의 차분 전력 분석 공격에서는 0 그룹과 1 그룹으로 분류된 파형들을 모든 샘플에 대해 평균하므

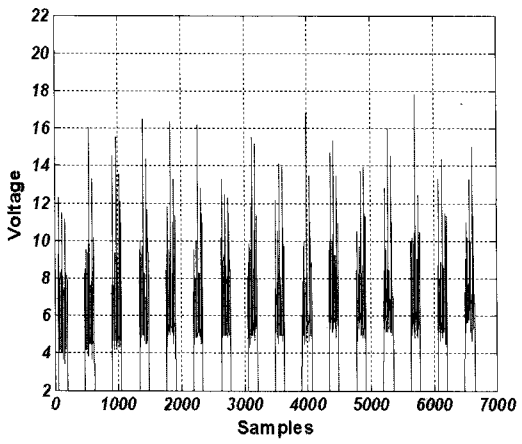
〔표 1〕 모의실험 파라미터

파라미터	값
샘플링 주파수	200 MHz
데이터 버스 주파수	8 MHz
문턱값(thr)	0.9
측정된 전력 신호 파형길이	6880 샘플
견본 파형 수정길이(L_R)	25 샘플
최종 견본 길이(L_T)	150 샘플
사용한 전력 신호 개수(M)	4000 개

로, 암호화 과정과 관련 없는 불필요한 전력까지 평균 과정에 사용되어 적은 수의 전력 신호로는 신호에 포함되어 있는 암호화와 관련이 없는 파형에 의한 효과를 효과적으로 줄일 수 없다. 그러나 제안된 전처리 기법을 적용한 차분 전력 분석 공격에서는 각 S-Box의 동작에 관계된 구간의 전력 신호만을 추출하여 사용하므로 적은 수의 전력 신호의 평균으로도 신호에 잔류하는 잡음 등의 성분을 제거해 줄 수 있어, 암호화에 사용된 비밀 키를 보다 효과적으로 추정할 수 있다.

IV. 모의실험

제안된 전처리 기법을 적용한 차분 전력 분석 공격의 성능을 평가하기 위해, 무선 센서 네트워크 장비 "mote IV"로 AES 암호화 과정을 구동시켜 누설되는 전력 소비 신호를 측정하였다. 〔표 1〕은 신호 측정 및 모의실험에 사용된 각종 파라미터를 나타낸다. 본 논문에서 제안된 전처리 기법을 적용하여 얻은 최종 견본의 길이는 150샘플로서, 이는 총 6,880 샘플의 전체 전력 소모 파형을 육안으로 구분한 430 샘플로 이루어진 16개 구간 파형에서 각각 150 샘플만이 해당 S-box 치환동작과 직접적으로 관련되어 있다는 것을 의미한다. 제안된 전처리 기법이 적용된 전력 신호 파형은 〔그림 4〕와 같다.



〔그림 4〕 제안된 전처리 기법을 적용한 전력 신호 파형

〔표 2〕는 기존의 전력 분석 공격과 제안된 전처리 기법을 적용한 전력 분석 공격의 비밀 키를 찾기 위해 필요한 측정된 전력 신호의 개수를 나타낸다. 각 공격 방법에 대해 필요한 전력 신호의 개수를 알아보기 위해 50개씩 전력 신호의 개수를 증가시켜 가며 모의실험을 반복 수행하였다. 공격이 성공한다는 것은 128비트의 비밀 키를 모두 정확하게 추정하는 것을 의미한다. 몇몇 비트들을 정확하게 추정하고 나머지 비트들에 대해서는 전수 공격 등의 방법을 통해 쉽게 추정할 수 있으나, 비밀 키를 알 수 없는 실제상황에서는 추정된 비밀 키 중 어느 것이 정확한 비밀 키인지를 판단할 수 없다. 따라서 모든 128비트의 비밀 키를 정확하게 추정할 수 있어야 한다. 기존의 차분 전력 분석 공격은 4,000개의 측정된 전력 신호를 모두 사용하더라도 각 S-Box의 비밀 키를 정확하게 찾을 수 없었던 반면, 제안된 전처리 기법을 적용한 차분 전력 분석 공격 방법은 모든 S-Box에 대해서 매우 적은 수의 전력 신호를 사용하여 비밀 키를 찾을 수 있었다.

〔표 2〕 각 S-Box의 비밀 키를 추정하기 위한 최소 전력 신호 개수

S-Box	차분 전력 분석 공격	
	기존 차분 전력 분석 공격	제안한 기법을 적용한 차분 전력 분석 공격
1	Fail	400
2	Fail	150
3	Fail	100
4	1750	500
5	Fail	550
6	Fail	300
7	Fail	100
8	Fail	450
9	Fail	200
10	Fail	250
11	Fail	350
12	Fail	300
13	Fail	250
14	Fail	450
15	Fail	100
16	Fail	250

V. 결 론

본 논문에서는 기존의 차분 전력 분석 공격의 효율성을 향상시키기 위해, 측정된 전력 신호로부터 암호화 동작과 관련된 신호 파형만을 추출하는 전처리 방법을 제안하였다. 본 논문에서 제안한 전처리 기법을 적용한 차분 전력 분석 공격은 암호화 과정에 사용된 비밀 키를 추정하기 위해 필요한 전력 신호의 수를 크게 감소시켜 공격의 효율을 향상시켰다. 제안한 전처리 기법은 상관 전력 분석 (CPA) 공격 및 전자기 분석 공격에도 적용이 가능할 것으로 보이며, 이에 대한 연구는 향후에 공격 성능 분석 및 대응 방안 연구를 중심으로 진행할 예정이다.

참고문헌

[1] S. Mangard, E. Oswald, and T.Popp, Power Analysis Attacks: Revealing the Secrets of Smart Cards, Springer Science+ Business Media, LLC., 2007.

[2] P. Kocher, J. Jaffe, and B. Jun, "Introduction to Differential Power Analysis and Related attacks," White Paper, Cryptography Research, http://www.cryptography.com/dpa/technical, 1998.

[3] P. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems," Advances in Cryptology-Crypto. 1996, LNCS 1109, pp. 104-113, 1996.

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

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

[6] J.J. Quisquater and D. Samyde, Electromagnetic Analysis (EMA): Measures and Countermeasures for Smart Cards, in Proceedings of e-Smart 2001.

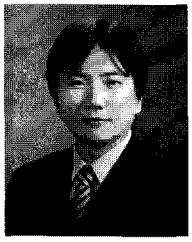
[7] K. Gandolfi, C. Mourtel, and F. Oliver, Electromagnetic Attacks: Concrete Results, in Proceedings of CHES 2001.

[8] 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.

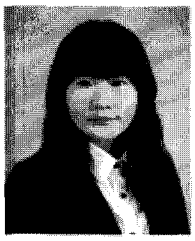
[9] 류정춘, 한동국, 김성경, 김희석, 김태현, 이상진, "웨이블릿 기반의 차분전력분석 기법 제안," 정보보호학회논문지, 19(3), pp.27-34, 2009년 6월.

[10] Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, 2001.

〈著者紹介〉



이 유 석 (You-Seok Lee) 정회원
2003년 2월: 부산대학교 전자공학과 졸업
2006년 2월: 부산대학교 전자전기공학과 석사
2009년 8월: 부산대학교 전자전기공학과 박사
2009년 9월~현재: 한국전자통신연구원 선임연구원
〈관심분야〉 디지털 방송신호처리, 적응신호처리, 부채널 공격



이 유 리 (Yu-Ri Lee) 학생회원
2010년 2월: 부산대학교 전자전기공학부 졸업
2010년 3월~현재: 부산대학교 전자전기공학과 석사과정
〈관심분야〉 부채널 공격, 디지털 방송신호처리

이 영 준 (Young-Jun Lee) 학생회원
2006년 2월: 부산대학교 전자전기공학부 졸업
2008년 2월: 부산대학교 전자전기공하과 석사
2008년 3월~현재: 부산대학교 전자전기공학과 박사과정
〈관심분야〉 디지털 방송신호처리, 적응신호처리, 부채널 공격

김 형 남 (Hyoung-Nam Kim) 정회원
1993년 2월: 포항공과대학교 전자전기공학과 졸업
1995년 2월: 포항공과대학교 전자전기공학과 석사
2000년 2월: 포항공과대학교 전자전기공학과 박사
2000년 3월~2003년 2월: 한국전자통신연구원 선임연구원
2003년 3월~2007년 2월: 부산대학교 전자전기통신공학부 조교수
2007년 3월~현재: 부산대학교 전자전기통신공학부 부교수
〈관심분야〉 적응신호처리, 레이더 신호처리, 디지털 방송신호처리, BCI