情報保護學會論文誌
第18卷 第2號, 2008. 4

# 신호 압신법을 이용한 차분전력분석 공격성능 향상*

류 정 춘[1†], 한 동 국[2], 김 성 경[1], 김 희 석[1], 김 태 현[1], 이 상 진[1‡]

[1]고려대학교 정보경영공학전문대학원, [2]한국전자통신연구원

# Performance Enhancement of Differential Power Analysis Attack with Signal Companding Methods*

JeongChoon Ryoo[1†], Dong-Guk Han[2], Sung-kyoung Kim[1], HeeSeok Kim[1], Tae Hyun Kim[1], Sangjin Lee[1‡]

[1]Graduate School of Information Management and Security, Korea University,

[2]Electronics and Telecommunications Research Institute

## 요 약

지금까지 제안된 많은 부채널 공격법(Side Channel Attack, SCA) 중 수집신호의 통계적 특성을 기반으로 하는 차분전력분석(Differential Power Analysis, DPA) 방법은 키를 해독하는 데 아주 효과적인 방법으로 알려져 있다. 그러나, 이 방법은 수집신호의 시간적인 동기 및 잡음에 따라 공격 성능에 상당한 영향을 받는다. 따라서 본 논문에서는 DPA에서 잡음에 의한 영향을 효과적으로 극복하는 새로운 방법을 제안하다. 제안된 방법의 성능은 DES 연산중인 마이크로 컨트롤러 칩의 전력소비 신호를 이용해서 기존 방식의 DPA와 시간 및 주파수 영역에서 비교한다. 실험을 통해 제안된 전처리 시스템의 성능 평가는 키 해독에 필요한 필요 평문의 수를 기준으로 계산할 경우, 기존의 방식과 비교하여 시간 영역에서 33%, 주파수 영역에서 50%의 성능이 개선되는 등 아주 우수한 결과를 보여주고 있다.

## ABSTRACT

Among previous Side Channel Analysis (SCA) methods, Differential Power Analysis (DPA) based on the statistical characteristics of collected signals has been known as an efficient attack for uncovering secret key of cryptosystems. However, the attack performance of this method is affected very much by the temporal misalignment and noise of collected side channel signals. In this paper, we propose a new method to surmount the noise problem in DPA. The performance of the proposed method is then evaluated while analyzing the power consumption signals of Micro-controller chips during a DES operation. Its performance is then compared to that of the original DPA in the time and frequency domains. When we compare the experimental results with respect to the needed number of traces to uncover the secret key, our proposed method shows the performance enhancement 33% in the time domain and 50% in the frequency domain.

**Keywords** : Side-Channel Attack(SCA), Differential Power Analysis(DPA), Correlation Power Analysis(CPA), Companding Method, Signaling Processing Gain

---

접수일: 2007년 11월 2일; 채택일: 2007년 12월 28일

* "본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원 사업의 연구결과로 수행되었음" (IITA-2008- (C1090-0801-0025))

† 주저자 jcwillow@naver.com

‡ 교신저자 sangjin@korea.ac.kr

# Ⅰ. 서 론

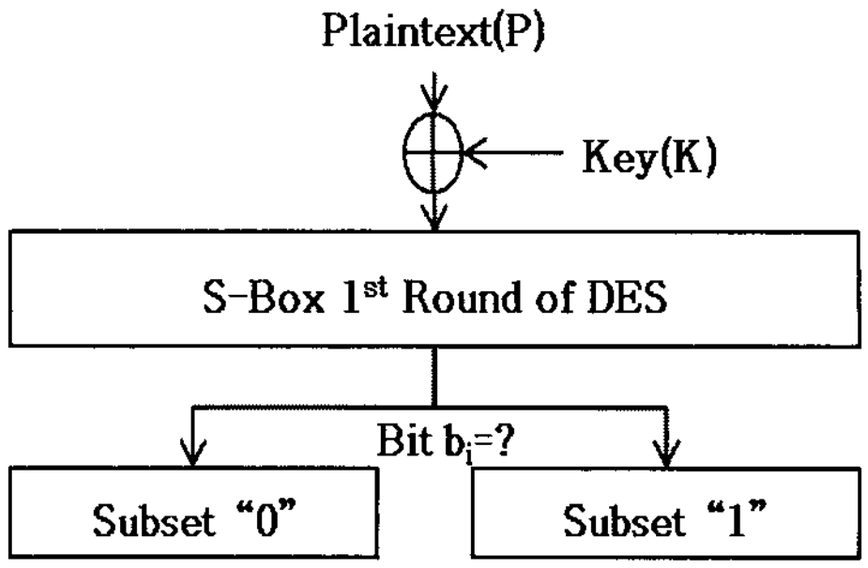
부채널 분석은 암호시스템의 물리적인 구현으로부터 나오는 암호연산의 시간, 소비전력 및 전자장과 같은 정보를 이용하는 공격법이다. 지금까지 소비전력을 이용하는 유명한 공격법으로는 단순전력분석(Simple Power Analysis, SPA), 차분전력분석(DPA)[1,2] 및 상관전력분석(Correlation Power Analysis, CPA)[3] 등이 잘 알려져 있다. 또한 전자장을 이용한 방법으로도 유사하게 단순전자기분석(Simple ElectroMagnetic Analysis, SEMA), 차분전자기분석(Differential ElectroMagnetic Analysis, DEMA)이 있다[4,5].

부채널 공격을 수행할 때 부채널 신호와 함께 나오는 잡음 및 시간 불일치는 부채널 공격의 효율성을 저하시키는 주된 요소였다. 지금까지 신호의 시간 불일치에 의한 공격 효율성의 저하를 극복하기 위한 많은 연구가 진행되었고, 특히 Gobotys[6]의 주파수 영역으로의 변환에 의한 공격법은 많은 계산량을 필요로 하나 시간 불일치에 의한 공격 효율성의 저하를 어느 정도는 극복할 수 있었다. 그러나 부채널 신호와 함께 출현하는 잡음의 특성에 대한 연구는 많이 되었으나, 이를 진폭에 따라 서로 다른 가중치로 처리하여 잡음의 영향을 최소화하기 위한 실무적인 방법은 거의 연구되지 못했다.

본 논문에서는 부채널 분석의 대표적인 방법인 DPA 공격을 기준으로 신호의 수집 시 필연적으로 동반되는 잡음의 전 처리를 통하여 DPA 공격 성능을 향상시키는 새로운 방법을 제안한다. 본 논문의 구성은 다음과 같다. 우선 2장에서는 지금까지 제안된 중요한 DPA 공격법을 소개하고, 3장에서는 제안된 공격법의 개념과 이론적인 공격 효율성을 설명하고, 4장에서는 기존의 DPA 공격법과 제안된 공격법의 성능을 비교하였다. 마지막으로 5장에서는 향후의 연구 분야 및 결론으로 마무리하였다.

# Ⅱ. DPA 공격법

이 장에서는 간단히 DPA의 개념을 시간 및 주파수 영역에서 살펴본다. DPA 공격은 암호화 연산 시 알고리즘의 전력소비가 데이터에 의존한다는 점을 이용하며, 임의의 입력 데이터에 대한 많은 수의 전력소비 패턴을 획득하여 입력 데이터에 대한 분류함수의 전력소비 특징을 분석한다. .




〔그림 1〕 DPA 공격을 위한 분류함수

이러한 분석 시, DPA는 입력 데이터가 "1"에 해당하는 비트를 처리하는 전력소비 패턴이 "0"에 해당하는 비트를 처리하는 전력소비 패턴과 다르다는 사실에 기반하고 있다. 예를 들어 임의의 키 K를 해독하기 위해서 DPA는 입력데이터 P와 분석하고자 하는 비트 $b_i$[2]를 예측하는 분류함수 D(P, $b_i$, K)를 사용한다. 위의 [그림 1]은 DPA 공격을 위한 분류함수의 개념도이다.

## 2.1. 시간 영역 분석

시간 영역의 공격법에서 DPA는 첫 번째로 서로 다른 선택 평문 P를 입력으로 일련의 소비전력 파형을 수집하고, 두 번째로 소비전력 파형에 상응하는 평문과 추정한 비밀 키 K 값을 기준으로 수집신호 파형을 구분하여, 분류함수 D(P, $b_i$, K)가 "1"인 트레이스의 평균과 D(P, $b_i$, K)가 "0"인 트레이스의 평균의 차이를 취한 값 $\Delta D(b_i)$를 계산한다. 만약 추정한 비밀 키 K 값이 옳으면 구분된 두 집단 간의 평균 소비전력의 차이는 비트 "$b_i$"를 계산하는 순간 시간인 $\tau$에서 $\Delta D(b_i) \neq 0$이 되며 DPA 피크로 불리는 값이 일반적으로 나타난다. 그러나 올바르지 못한 키에 대해서는 두 집단 간의 평균 소비전력의 차이는 $\Delta D(b_i) \approx 0$이 되며 피크 값이 나타나지 않을 것이다.

이러한 공격 방식의 경우 한 비트의 변화에 의한 전력치의 변화는 극도로 작으며 각 트레이스가 정확히 동기화되지 않을 경우 $\tau$의 조그만 불일치에 의한 DPA 공격의 성능은 아주 줄어든다. 지금까지 이러한 DPA의 단점을 극복하기 위한 방법으로 Messerges[7]와 Bevan[8]은 단일 비트를 이용한 DPA가 아닌 다중 비트를 이용한 DPA 방식을 제안하였고, 최근에는 DPA 시 트레이스 간의 동기 불일치에 의한 성능 저하를 극복할 수 있는 구간 에너지 기반의 공격법[9]이 제안되

기도 하였다.

## 2.2. 주파수 영역 분석

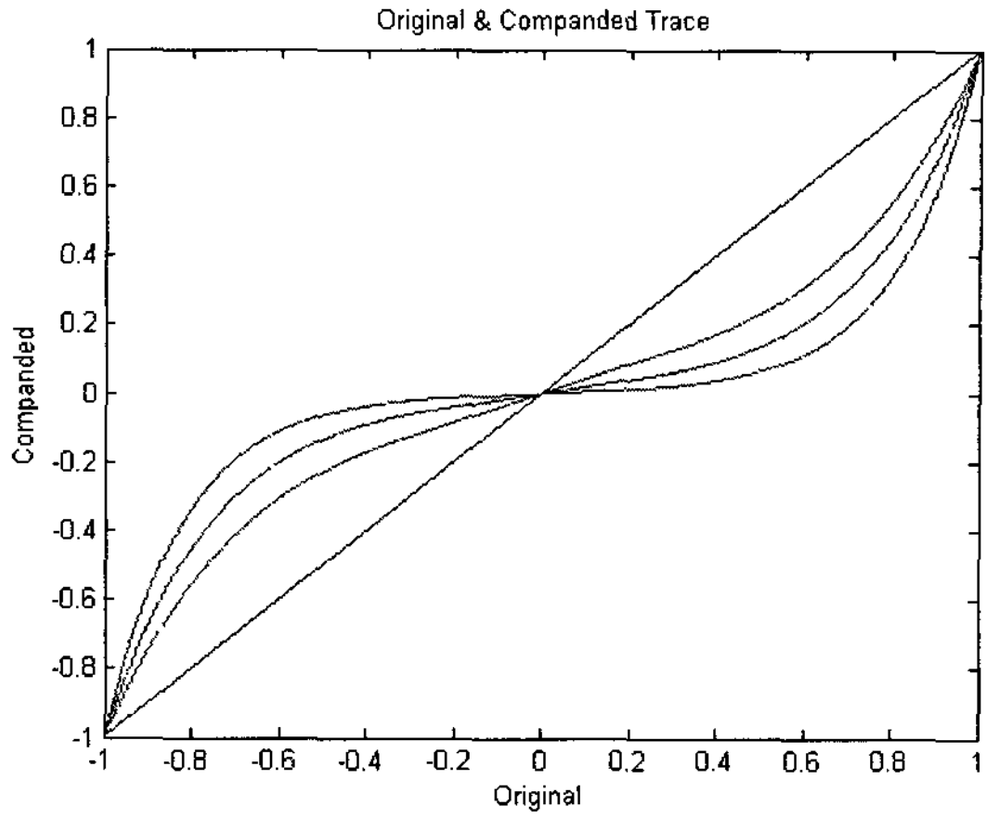
주파수 영역에서의 공격법은 많이 제시되지 못하였지만 Gebotys는 시간 영역의 동기 불일치에 의한 영향은 주파수 영역에서 신호의 크기에 영향을 미치지 않는다는 천이 특성(Shift Property)을 이용한 공격법을 제시하였다. 비록 이 방법은 주파수 변환 과정에서 계산량이 많이 필요하였지만 Gebotys가 제안한 주파수 영역의 분석법은 시간영역에서 분석하지 못했던 암호 알고리즘에 대한 DPA 공격법을 성공적으로 수행하였다.

주파수 영역에서의 DPA 공격법도 시간영역과 같이 첫 번째로 공격자는 서로 다른 선택 평문 P를 입력으로 일련의 소비전력 파형을 수집하여 각 수집파형의 전력밀도(Power Spectral Density)를 계산한다. 두 번째로 공격자는 소비전력 파형에 상응하는 평문과 추정한 비밀 키 K 값을 기준으로 수집파형의 전력밀도를 구분하여, 분류함수 D(P, $b_i$, K)가 "1"인 트레이스와 D(P, $b_i$, K)가 "0"인 트레이스의 평균 전력밀도의 차이를 계산한다. 만약 추정한 비밀 키의 값이 옳으면 구분된 두 집단 간의 평균 전력밀도의 차이는 아주 클 것이고, 그렇지 않으면 두 집단 간의 평균 전력밀도의 차이는 거의 없을 것이다. 이 방식은 주파수 별 차분 전력밀도 신호의 크기가 의미 있는 신호인가를 판단하기 위한 경계신호의 선택이 아주 중요하다. 일반적으로 경계신호로는 주파수 별 표준편차의 정수 배를 선정하는 데, 이 경계값의 적절한 선택으로 차분 전력 분석의 에러 확률과 잡음의 영향을 최소화 하여 주파수 영역 분석의 성능을 조금 더 향상 시킬 수 있다.

# Ⅲ. 제안 기법

## 3.1. 개념

암호화 키 검출은 부채널 신호에 기반하고 있기 때문에 부채널 신호의 신호 대 잡음 비는 키 검출의 효율성에 결정적인 영향을 미친다. 그러나 수집 신호의 신호 대 잡음 비는 임의적으로 바꿀 수 없는 값이다. 따라서 수집신호의 신호 대 잡음 비를 유지한 상황에서 부채널 신호의 암호연산 관련 필요부분을 증폭하고 암호연산과 직접 관련되지 않은 부분은 감소시키는 기법의 적용은



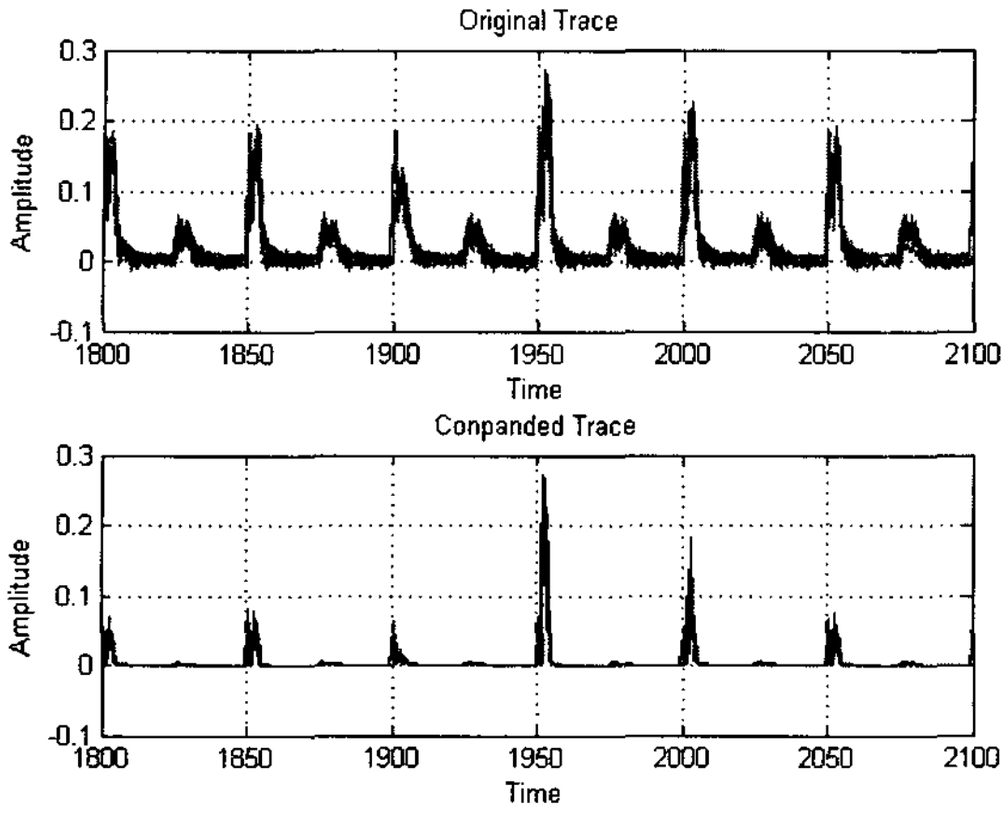

〔그림 2〕 A-law 그래프

DPA 공격 시 아주 중요하다.

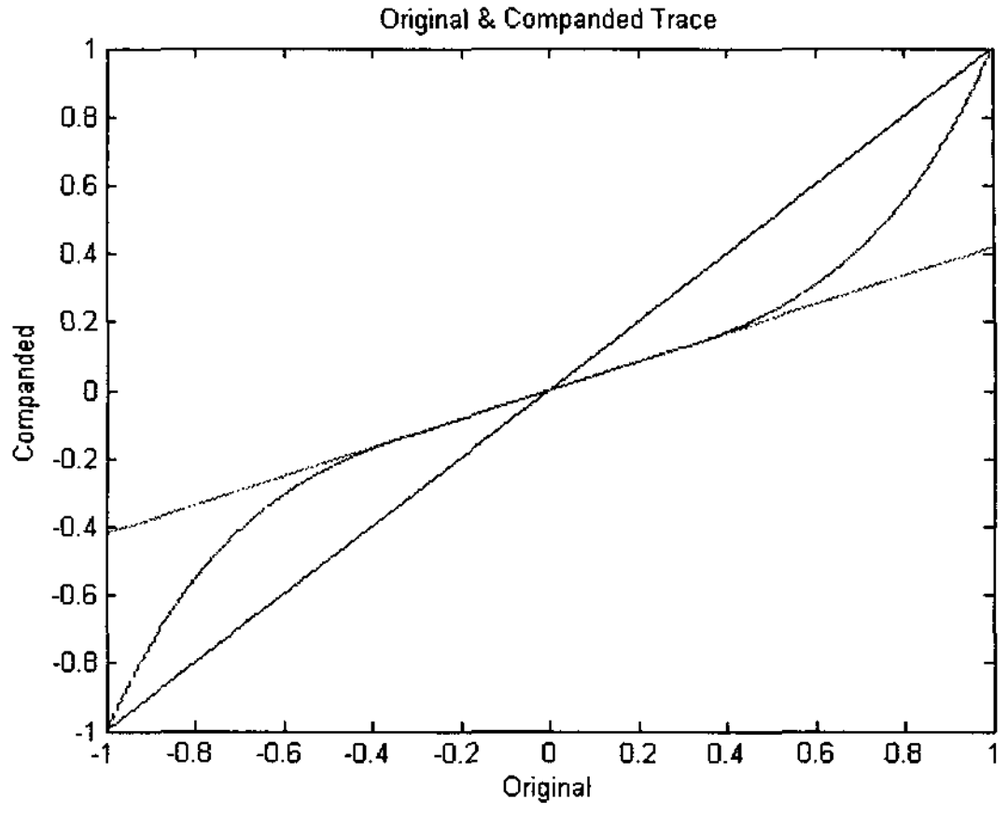
본 논문에서는 부채널 신호의 전력(Power) 및 전자장(Electromagnetic Energy)의 특성이 실제 암호 연산 시에 많은 에너지를 소비하므로 진폭의 관점에서 보면 수집 신호의 피크(Peak) 값에 에너지가 집중되어 있다는 점에 착안하였다. 따라서 신호의 크기를 기준으로 진폭이 큰 부분은 증폭하고 작은 부분은 압축하는 기법으로 신호의 진폭에 따라 가중치(Weighting)를 다르게 줄 수 있는 압신법(Companding)[13]을 전처리 기법으로 적용하였다. 본 논문에서는 구체적인 압신법으로 음성신호의 전 처리를 위해 유럽지역에서 표준으로 사용되는 A-law 방식을 적용 모델로 선정하였다. 위의 [그림 2]는 A-law 방식의 압신법 그래프이다.

위의 그래프는 음성신호의 비 균등(Non-uniform) 양자화 시에 많이 사용되는 A-law 압신법을 역으로 적용한 경우를 나타낸 것으로 대각선으로 된 그래프는 원래의 신호를 그대로 사용하는 것으로 압신 계수 값 A=1.0이고 나머지 그래프들은 신호의 크기에 따라 다른 가중치를 적용하는 그래프로 A-law의 경우 A의 값은 [1.0 … 87.6] 사이의 값이다. 즉, 압신 계수 A를 이용하여 진폭이 작은 신호는 압축하고 진폭이 큰 신호는 증폭하여 상대적으로 부채널 분석에 필요한 신호의 에너지를 많이 활용하는 비율을 결정하고 있음을 볼 수 있다. 다음은 압신법의 개념과 A-law 방법을 적용하였을 때의 실제 DES 연산 시에 출현하는 부채널 신호인 전력 소비 신호에 미치는 영향을 그림으로 상세히 나타내어 설명하고 있다.

다음 [그림 3]은 본 논문에서 제안한 전처리 기법의




〔그림 3〕 전처리 전·후의 신호 변화




〔그림 4〕 신호처리 이득 그래프

적용 전과 후에 신호에 미치는 영향을 나타낸 것으로 위 그래프 압신법을 적용하기 전의 원 신호를 나타내고 아래 그래프는 압신법을 적용한 후의 신호를 나타내고 있다.

위의 그림에서와 같이 암호 연산과 관련이 적은 부분인 진폭이 작은 신호는 거의 "0"으로 압축되었고 상대적으로 암호연산이 직접 일어나는 부분의 신호는 크기는 줄었지만 정보를 담고 있는 것을 볼 수 있다.

### 3.2. 이득 계산

이 장에서는 앞에서 적용한 압신법이 DPA 공격의 효율성에 미치는 영향을 평가하기 위하여 압신법을 이론적인 측면에서 검토하고자 한다. 다음 수식은 본 논문에서 적용한 A-law 방식의 압신 함수의 수식이다.

$$y(t)=\begin{cases}\dfrac{K}{A}x(t) & ; \quad |x(t)|\le\dfrac{1}{K}\\ \mathrm{sgn}(x(t))Exp(K(|x(t)|-1)) & ; \quad \dfrac{1}{K}<|x(t)|\le 1\end{cases}$$

$$Here \quad K=1+\log_e(A)\ \text{and}\ \mathrm{sgn}(x(t))=\begin{cases}1: & x(t)\ge 0\\ -1: & x(t)<0\end{cases}$$

위의 수식을 보면 압신법은 신호의 처리 구간을 크게 두 구간으로 나누고 있음을 볼 수 있다. 즉, 선형 연산을 하여 신호를 압축하는 부분과 지수 연산을 수행하여 신호를 증폭하는 부분이다. [그림 4]는 압신법을 적용하였을 때의 신호에 미치는 영향을 도식적으로 나타내고 있다. 선형 연산을 수행하는 수식의 기울기를 연장하여 지수 연산을 수행하는 영역간의 상대적인 신호처리[14] 이득을 나타낸 그림이다.

위의 그림에서 A=87.6으로 가정하고 압축하는 영역과 증폭하는 영역의 신호처리의 이득(Gain)을 가로축의 값 x(t)=1에서 구하면 다음과 같다.

$$Gain = 20\log\left(\frac{\mathrm{sgn}(x(t))Exp(K(|x(t)|-1))}{\frac{K}{A}x(t)}\right)$$

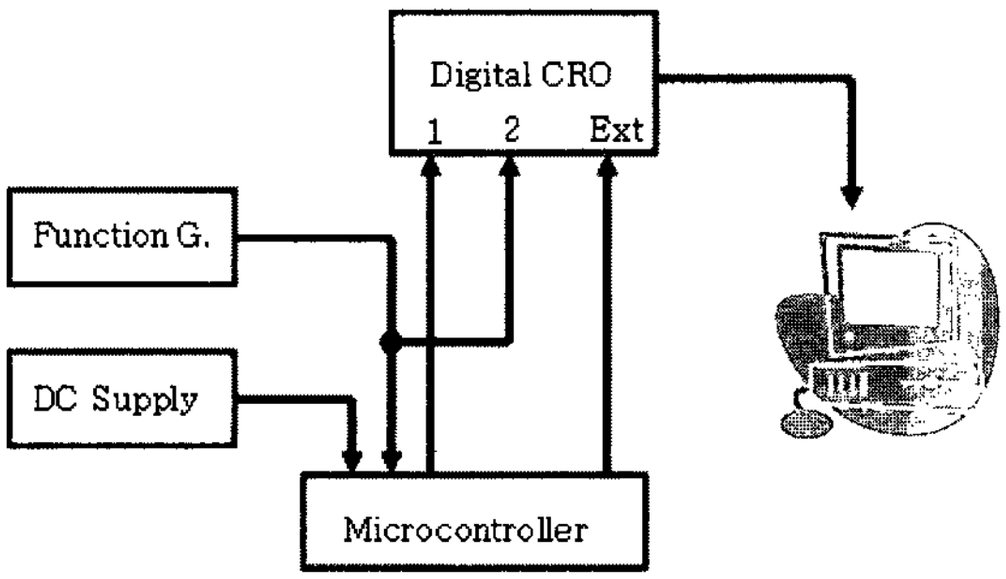
$$= 20\log\left(\frac{A}{K}\right) = 20\log(16) \approx 24\,dB$$

본 결과는 A=87.6를 사용할 경우 압축 영역과 증폭 영역을 비교할 경우 상대적 이득을 최대 약 24dB 정도 얻을 수 있음을 보여 주고 있다. 따라서 압신법을 적용하여 상대적으로 신호를 압축 및 증폭함으로 암호 연산에 중요한 정보를 포함하고 있는 신호의 DPA 공격 활용도를 높여 본 공격법의 효율성을 개선할 수 있음을 이론적으로 알 수 있다.

## Ⅳ. 실험 결과

### 4.1. 실험 환경

본 실험에서는 DES[11] 연산 동안 Micro-Controller로부터 소비되는 전력신호를 측정한다. 실험 대상이 되는 암호 시스템은 PIC16F84A[12]을 사용하여 구현하였다. 실험에서 사용한 칩은 기본적으로 8비트 연산을




〔그림 5〕 전체 실험 환경

수행하며, 암호 알고리즘인 DES는 어셈블리 언어로 구현되어 있다. 이 때, DES의 키는 PIC칩에 저장되어 있고 임의의 입력 값에 대한 암호화 연산 중에 일어나는 부채널 신호인 소비전력파형을 획득한다. 구체적인 사용 장비로는 DC Power Supply를 이용하여 +5V의 전력을 외부에서 공급하고, Function Generator를 이용하여 1MHz의 Sine Wave를 공급하게 된다. 그리고 소비전력파형을 측정하기 위하여 Tektronix사의 TDS3032B의 디지털 오실로스코프(CRO)를 사용한다. 그리고 실험을 수행한 환경은 일반적인 사무실 환경이다. 다음 [그림 5]는 전체 실험 환경에 대한 도식화이다.

본 실험에서는 DES의 첫 번째 라운드를 공격 대상으로 선정하였다. 실험 수행 방법은 먼저 1,000 개의 임의의 선택 평문을 입력으로 하여 공격 파형을 첫 번째 라운드를 기준으로 수집하였고 본 논문에서 제안한 압신법을 전처리 기법으로 적용하여 DES의 8개 S-Box 각각에 대하여 기존의 방법과 본 논문에서 제안하는 방법의 성능을 측정하여 DPA 공격의 효율성을 비교하였다.

## 4.2. 성능 비교

본 논문에서는 DPA 공격 방법으로 S-box의 각 비트에 대한 DPA 공격의 결과 값을 합하여 이 값을 기준으로 공격을 수행하였다. 실험에서와 같이 비트 합(Sum)에 의한 결과 값을 각 S-box별 키 해독 방식으로 선택함으로 DPA 공격법의 성능 비교에 필요한 평문의 수를 획기적으로 줄일 수 있었다. 지금까지 언급한 비트 합에 의한 공격법은 다음의 수식과 같다.

$$\sum_{i} \Delta_D(b_i)$$

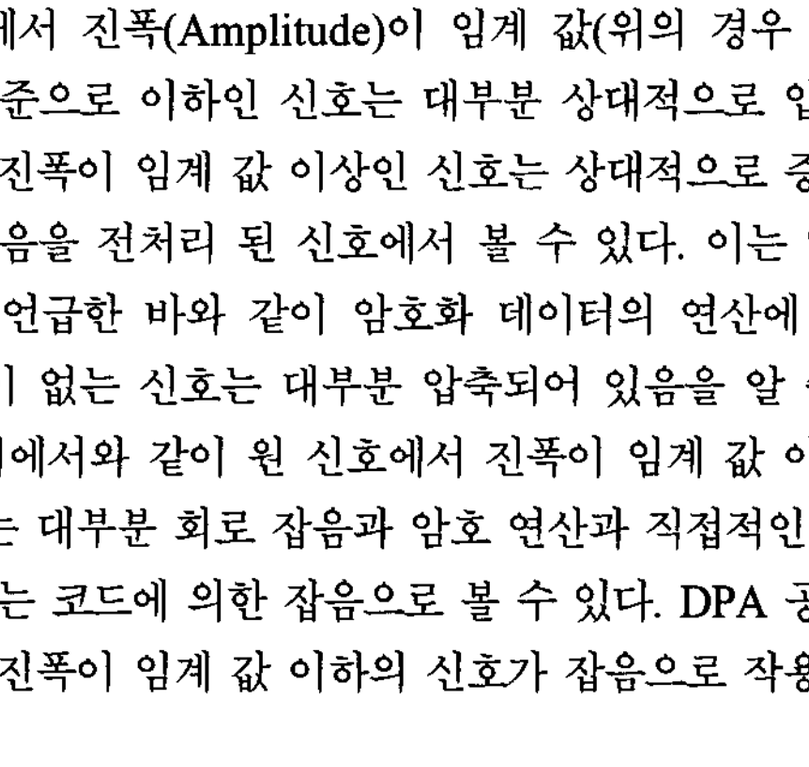
예를 들어 DES의 경우에는 각 S-box의 공격 시 i=1,2,3,4로 4 비트 합 방식을 사용하여 공격법을 구성할 수 있다. 비트 합 방식은 각 비트의 연산결과가 서로 거의 독립인 DES 공격법으로 아주 효율적인 방식이다. 이렇게 비트 합에 의한 성능 비교 분석법을 통해 본 논문에서는 1,000개의 신호를 이용하여 제안한 전처리 방법에 의한 DPA의 성능을 기존의 방법과 비교하였다.

다음은 본 논문에서 제안하여 적용한 기법이 DPA 공격에 어떠한 긍정적인 효과를 미치는 지 평가하기위해 시간 영역과 주파수 영역에서의 기존 방식과 본 논문에서 제안하고 있는 압신법을 적용한 경우의 성능 비교 결과이다.

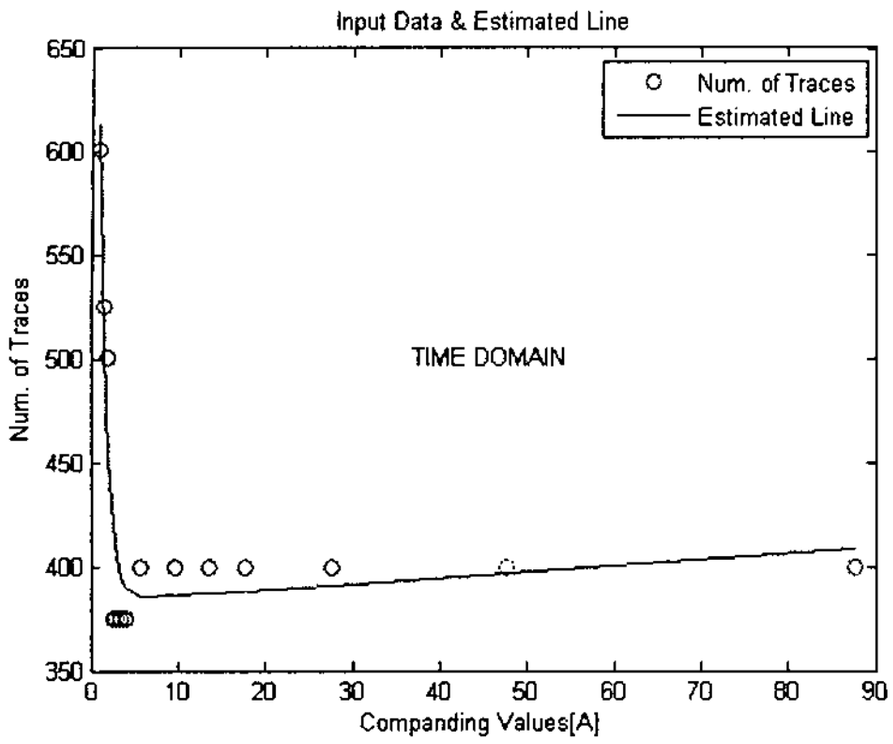
### 4.2.1 시간 영역

다음 [그림 6]은 본 논문에서 제안한 기법이 획득한 신호 전체 구간에 미친 영향을 시간 영역에서 보여주고 있다.

위의 [그림 6]에서 보면 압신법을 적용하였을 때 원 신호에서 진폭(Amplitude)이 임계 값(위의 경우 0.15)를 기준으로 이하인 신호는 대부분 상대적으로 압축되었고 진폭이 임계 값 이상인 신호는 상대적으로 증폭되어 있음을 전처리 된 신호에서 볼 수 있다. 이는 앞 장에서 언급한 바와 같이 암호화 데이터의 연산에 직접 연관이 없는 신호는 대부분 압축되어 있음을 알 수 있다. 위에서와 같이 원 신호에서 진폭이 임계 값 이하인 신호는 대부분 회로 잡음과 암호 연산과 직접적인 관계가 없는 코드에 의한 잡음으로 볼 수 있다. DPA 공격에서는 진폭이 임계 값 이하의 신호가 잡음으로 작용하여




〔그림 6〕 전처리 전·후의 시간영역 신호파형




〔그림 7〕 압신 계수 대 필요 트레이스 수

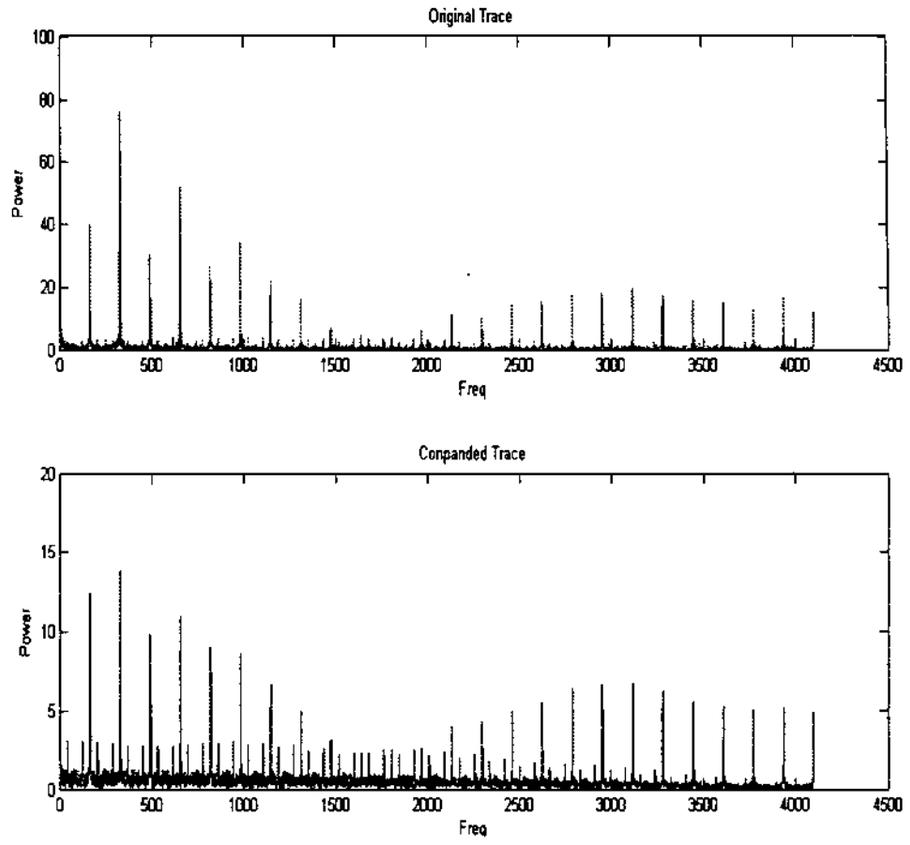
DPA의 성능에 악영향을 미치는 것을 전처리 과정을 통하여 제거할 수 있음을 보여주고 있다. 위의 [그림 7]은 압신 함수의 계수(A)값 변화에 따른 DPA 공격의 효율성을 S-Box의 비트 합으로 계산한 결과를 압신 계수 대비 필요한 트레이스의 수로 평가한 결과를 보여주고 있다.

[그림 7]에서 보면 A=1인 경우, 압신을 하지 않은 원 신호는 키를 해독하기 위하여 600개의 신호가 필요하고, 압신을 하는 경우에는 압신 계수가 A=2.5 이상에서 거의 400개의 신호가 압신 계수 값에 관계없이 필요함을 알 수 있다. 이는 압신 함수를 이용한 전 처리를 통하여 DPA 공격의 성능을 키 해독에 필요한 신호 관점에서 계산하면 약 33% 이상의 성능 개선 효과가 있음을 알 수 있다.

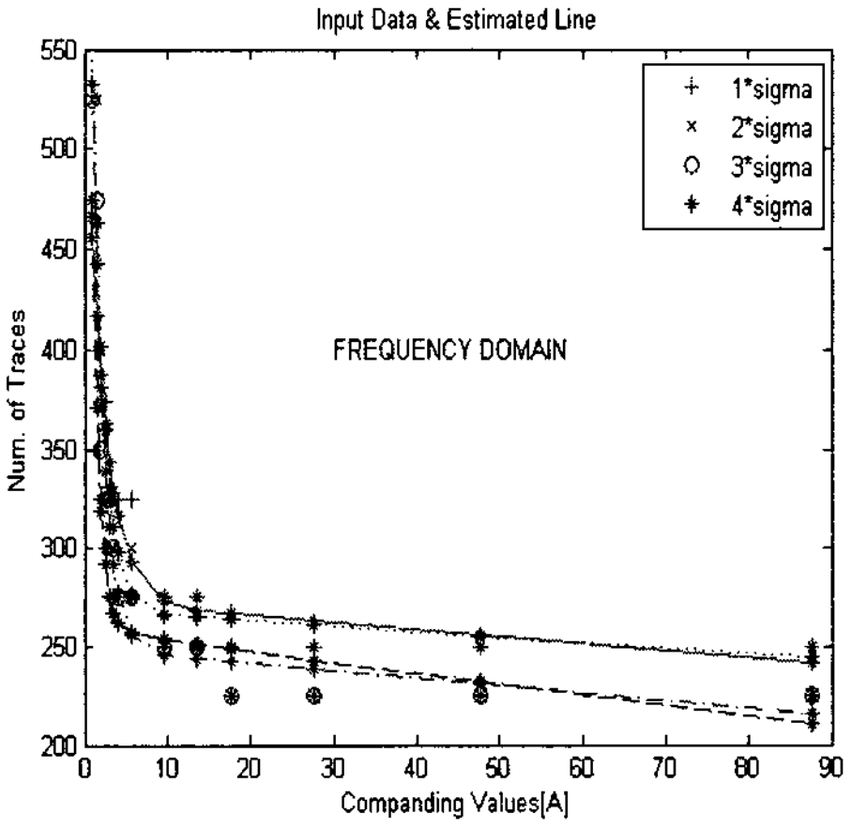
### 4.2.2 주파수 영역

다음 [그림 8]은 본 논문에서 제안한 기법이 신호에 미친 영향을 주파수 영역에서 보여주고 있다. 주파수 변환은 각 트레이스 5,000개의 표본을 Zero Padding 기법을 이용하여 8,192개의 표본으로 변환한 후 계산한 4,096개의 주파수 영역으로 표현하였다.

[그림 8]의 전처리 전후의 주파수 영역 에너지 분포 특성을 보면 원 신호의 주파수 별 전력은 크기가 [0..80] 사이에서 분포하며 상대적으로 작은 에너지를 가지고 있는 신호의 주파수 표현을 구체적으로 하지 못함을 알 수 있다. 그러나 전 처리를 한 경우의 신호는 주파수 별 전력이 [0..15] 사이에서 존재하며 각 주파수 별 절대 에너지는 원 신호 대비 상당히 압축되어 있음을 볼 수 있으나 각 주파수간의 상대적인 에너지의 변




〔그림 8〕 전처리 전·후의 주파수 영역 에너지 분포




〔그림 9〕 압신 계수 대 필요 트레이스 수

환은 더욱 세밀하게 표현하고 있음을 알 수 있다. 이는 전처리 된 신호의 경우 암호화 연산 시에 필요한 정보의 표현을 구체적으로 할 수 있음을 의미한다.

위의 [그림 9]는 전처리 함수의 계수 값 변화에 따른 DPA 연산의 효율성을 S-Box의 비트 합으로 계산한 결과를 주파수 영역에서 보여주고 있다. 주파수 영역에서의 DPA 계산은 기준 값을 분산의 1, 2, 3, 4 배로 각기 다르게 하여 압신 계수 대비 키 해독에 필요한 트레이스의 수를 각각의 경우에 대하여 계산하였다. [그림 9]에서 보면 A=1인 경우의 원 신호는 선택한 분산의 배수에 관계없이 약 500개의 신호가 필요하고 전처리 신호의 경우에는 A=17.5 이상에서 기준 값을 분산의 배수 얼마로 선정하는가에 거의 관계없이 약 250개의 신호가 필요함을 알 수 있다. 이는 전 처리를 통하여 주파

수 영역의 DPA 공격 성능을 키 해독에 필요한 신호 관점에서 계산하면 약 50%의 성능 개선 효과가 있음을 보여주고 있다.

### 4.3. 성능 평가

앞의 성능 비교 시 압신 계수가 시간 영역에서는 A=2.0을 주파수 영역에서는 A=17.5를 기준으로 전 처리의 이득이 DPA 공격 성능에 미치는 영향이 수렴함을 알 수 있다. 압신 계수 값은 압축과 신장 두 영역간의 상대적인 신호처리 이득을 나타내는 값으로 이는 시간 영역 대비 주파수 영역의 분석이 압신 계수에 더욱 민감함을 나타낸다. 또한, 압신 계수 값은 대상 암호연산 디바이스 특성에 의존하는 값으로 실험을 통하여 결정할 수 있을 것이다.

다음 [표 1]은 원 신호 및 전처리 신호를 이용하여 시간영역과 주파수 영역에서의 처리 및 변환 이득을 비밀키 해독에 필요한 트레이스의 수를 기준으로 종합하여 비교한 표이다.

[표 1]을 살펴보면 시간과 주파수영역에서 단순 전처리 이득이 각각 33%, 50%가 됨을 알 수 있고, 또한 원 신호와 전 처리 신호의 단순 주파수 변환으로 17%, 38%의 이득을 얻을 수 있음을 알 수 있다. 이렇게 신호 변환 이득과 신호처리 이득이 원 신호와 전 처리 신호의 경우에 시간영역과 주파수영역에서 차이가 생기는 것을 볼 수 있다. 이는 신호의 전 처리를 통하여 수집신호의 시간 불일치 요소가 DPA 공격 성능에 미치는 영향을 상대적으로 줄일 수 있음을 보여주고 있다. 또한 본 논문에서 제안한 전 처리를 기법을 통하여 신호처리 및 변환에 의한 이득을 동시에 상승적으로 얻을 수 있음을 알 수 있고 신호처리와 변환에 의한 전체 이득은 신호처리를 하지 않았을 경우의 단순 주파수 변환에 의한 이득 17% 대비 58%에 달함을 알 수 있다.

결론적으로, 원 신호를 통한 비밀 키의 해독 시에는 600개의 트레이스가 필요하나 전 처리를 통하여 주파수 영역에서 분석함으로 약 250개의 트레이스 만으로도 비밀 키의 해독이 가능함을 알 수 있다. 이는 신호처리 이득뿐만 아니라 앞에서 언급한 시간 불일치에 의한 요인이 DPA 성능에 미치는 영향을 본 논문에서 제안한 신호 전처리 기법을 통하여 더욱 더 줄일 수 있음을 보여 주고 있다.

〔표 1〕 시간영역과 주파수영역에서의 전처리 이득

| 항목 | 시간영역 | 주파수영역 | 변환이득 |
|---|---|---|---|
| 원신호 | 600 | 500 | 17% |
| 전처리 | 400 | 250 | 38% |
| 처리이득 | 33% | 50% | 58% |

## V. 결 론

본 논문에서는 부채널 공격에 많이 사용되는 DPA의 성능을 획기적으로 개선할 수 있는 새로운 개념의 전처리 방법을 제시하였다. 본 논문에서 제시한 방법은 실제 DPA 공격 시 구현하기가 아주 쉽고 또한 전처리 이득이 시간 영역 및 주파수 영역에서도 그대로 나타남을 알 수 있다. 본 논문에서는 DES를 기준으로 제안한 방법의 성능을 시간 및 주파수 영역에서 비교 분석하였다. 향후 제안한 전처리 방식을 다른 보안장비, 예를 들어 스마트카드, 등에 적용하여 DPA의 공격성능 개선효과를 연구할 것이다. 또한 제안한 전처리 방식이 CPA (Correlation Power Analysis)[3]와 같이 두 개 이상의 수집 신호간의 상관관계를 이용하여 분석하는 부채널 공격법에는 어떠한 효과를 나타내는지도 연구해 볼 것이며, DPA 및 CPA 방식에 가장 적절한 신호 전처리 함수에 대한 연구도 함께 진행할 것이다.

## 참고문헌

[1] P.Kocher, J.Jaffe, and B. Jun, “Introduction to differential power analysis and related attacks,” 1998, White Paper, Cryptography Research.

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

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

[4] K. Gandolfi, C. Mourtel, and F. Olivier, “Electromagnetic Analysis: Concrete Results,” CHES 2001, LNCS 2162, pp. 251-261, Springer-Verlag, 2001.

[5] J.J Quisquater and D. Samyde, “Electromagnetic Analysis(EMA): Measures and Countermeasures

for Smart Cards," in In proceedings of e-Smart 2001.

[6] C. Gebotys, S. Ho, and A. Tiu, "EM Analysis of Rijndael and ECC on a Wireless Java-Based PDA," CHES 2005, LNCS 3659, pp. 250-264, Springer-Verlag, 2005.

[7] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," Journal of IEEE Trans. on Computers, vol.51, Issue 5, pp.541-552, 2002.

[8] R. Bevan and E. Knudsen, "Ways to Enhance DPA," ICISC 2002. LNCS 2587, pp. 327-342, Springer-Verlag, 2003.

[9] T-H. Le, J. Clediere, C. Serviere, and J-L. Lacoume, "Efficient solution for misalignment of signal in side channel analysis," ICASSP 2007, pp.257-260.

[10] K. Tiri, I.Verbauwhede, "Simulation Models for side-channel information leaks," Annual ACM IEEE Design Automation Conference 2005, pp. 228 - 233, 2005.

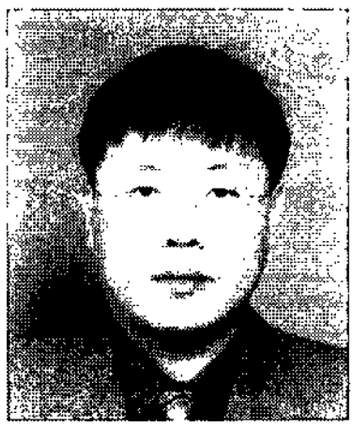
[11] FIPS PUB 46-3, "Data Encryption Standard (DES)," National Institute of Standards and Technology, 1999.

[12] Microchip Technology Inc., PIC16F8X-18 pin Flash EEPROM 8-bit Microcontrollers, 1998.

[13] N.S. Jayant, Peter Noll Digital Coding of Waveforms : Principles and Applications to Speech and Video, Prentice Hall, 1984.

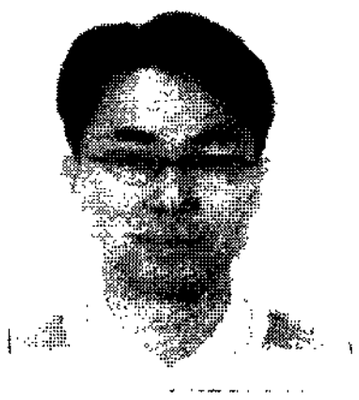
[14] Richard G. Lyons Understanding Digital Signal Processing Second Edition, Prentice Hall, 2004.

## 〈著者紹介〉



**류 정 춘 (JeongChoon Ryoo) 학생회원**

1988년 2월 : 경북대학교 전자공학과 졸업(학사)
1990년 2월 : 경북대학교 전자공학과 석사(공학석사)
1990년 1월~1995년 4월 : LG정보통신 연구소 근무
1996년 1월~1999년 11월 : 대우그룹 해외통신사업본부 근무
2005년 3월 ~ 현재 : 고려대학교 정보경영공학전문대학원 박사과정
<관심분야> 부채널 공격, 이동통신 암호프로토콜, 대칭키 암호의 분석 및 설계

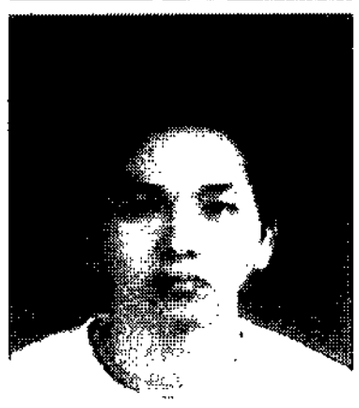


**한 동 국 (Dong-Guk Han) 일반회원**

1999년 : 고려대학교 수학과 졸업(학사)
2002년 : 고려대학교 수학과 석사 (이학석사)
2005년 : 고려대학교 정보보호대학원 박사 (공학박사)
2004년 4월 ~ 2005년 4월 : 일본 Kyushu Univ., 방문연구원
2005년 4월 ~ 2006년 4월 : 일본 Future Univ.-Hakodate, Post.Doc.
2006년 6월 ~현재 : 한국전자통신연구원 정보보호연구단 선임연구원
<관심분야> 공개키암호 안전성분석 및 고속구현, 부채널분석, RFID/USN 정보보호 기술

**김 성 경 (Sung-Kyoung Kim) 학생회원**

2005년 2월 : 동의대학교 수학과 학사
2007년 8월 : 고려대학교 정보경영공학전문대학원 석사
2007년 9월 ~ 현재 : 고려대학교 정보경영공학전문대학원 박사과정
<관심분야> 부채널 공격, 공개키 암호, 암호칩 설계 기술



**김 희 석 (HeeSeok Kim) 학생회원**

2006년 2월 : 연세대학교 수학과 졸업(학사)
2006년 3월 ~ 현재 : 고려대학교 정보경영공학전문대학원 석사과정
<관심분야> 부채널 공격, 공개키 암호시스템 안전성 분석 및 고속구현, 타원곡선

**김 태 현 (Tae Hyun KIM) 학생회원**

2002년 2월 : 서울 시립대학교 수학과 이학사
2004년 8월 : 고려대학교 정보보호 대학원 공학석사
2005년 3월~현재 : 고려대학교 정보경영공학전문대학원 박사과정
<관심분야> 부채널 공격, 공개키 암호 알고리즘, 암호칩 설계 기술

**이 상 진 (Sangjin Lee) 종신회원**

1987년 2월: 고려대학교 수학과 이학사
1989년 2월: 고려대학교 수학과 이학석사
1994년 2월: 고려대학교 수학과 이학박사
1989년 2월~1999년 2월: 한국전자통신연구원 선임 연구원
1999년 2월~2001년 8월: 고려대학교 자연과학대학 조교수
2001년 9월~현 재: 고려대학교 정보경영공학전문대학원 부교수
<관심분야> 부채널 공격, 대칭키 암호의 분석 및 설계, 정보은닉이론, 컴퓨터 포렌식