情報保護學會論文誌
第19卷 第3號, 2009. 6

웨이블릿 기반의 차분전력분석 기법 제안*

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]국민대학교

A Proposal of Wavelet-based Differential Power Analysis Method*

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]Kookmin University

요 약

수집신호의 통계적 특성을 기반으로 하는 차분전력분석(Differential Power Analysis, DPA) 방법은 암호시스템의 키를 해독하는 데 아주 효과적인 방법으로 알려져 있다. 그러나 이 방법은 수집신호의 시간적인 동기와 잡음에 따라 공격 성능에 상당한 영향을 받는다. 본 논문에서는 DPA에서 시간적인 동기와 잡음에 의한 영향을 동시에 효과적으로 극복하는 웨이블릿(Wavelet) 기반의 신호처리 방법을 제안한다. 제안된 방법의 성능은 DES 연산중인 마이크로 컨트롤러 칩의 전력소비 신호를 이용해서 측정한다. 실험을 통해 제안된 웨이블릿 기반의 전처리 시스템의 성능은 키 해독에 필요한 필요 평문의 수가 기존의 방법들이 필요로 하는 25%의 평문의 수로도 충분함을 보여주고 있다.

ABSTRACT

Differential Power Analysis (DPA) based on the statistical characteristics of collected signals has been known as an efficient attack for uncovering secret key of crypto-systems. However, the attack performance of this method is affected very much by the temporal misalignment and the noise of collected side channel signals. In this paper, we propose a new method based on wavelet analysis to surmount the temporal misalignment and the noise problem simultaneously 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. The experimental results show that our proposed method based on wavelet analysis requires only 25% traces compared with those of the previous preprocessing methods to uncover the secret key.

Keywords: Side Channel Attack, Differential Power Analysis, Correlation Power Analysis, Wavelet Transform, Multi-Resolution Analysis

I. 소 개

부채널 분석은 암호시스템의 물리적인 구현으로부터 나오는 암호연산의 시간, 소비전력 및 전자장과 같은 정보를 이용하는 공격법이다. 지금까지 알려진 소비전력을 이용한 공격법으로는 단순전력분석(Simple Power Analysis, SPA), 차분전력분석(DPA)[1,2]과 상관전력분석(Correlation Power Analysis, CPA)[3] 및 템플릿(Template)[4,5] 분석 등이 있다.

이와 같은 다양한 공격법을 수행할 때 부채널 신호로 함께 나오는 잡음 및 시간 불일치는 공격의 효율성을 저하시키는 주된 요소였다. 지금까지 공격 효율성의 저하를 극복하기 위해, Gobotys[6]의 주파수 변환과 T-H Le의 잡음의 고차 통계적 특성을 이용한 잡음 감소법[7]등이 제안되었다. 그러나 부채

접수일(2008년 9월 24일), 게재확정일(2009년 5월 15일)
* 이 연구에 참여한 연구자(의 일부)는 '2단계 BK21사업'의 지원비를 받았음.
† 주저자, jcwillow@naver.com
‡ 교신저자, sangjin@korea.ac.kr

널 신호를 통하여 나타나는 암호연산의 시간 국부성(Locality) 및 시간 불일치(Misalignment)에 의한 위상 잡음과 기타 다양한 잡음의 특성을 동시에 고려하여 DPA 공격의 성능을 높이는 방법에 대한 연구는 없었다.

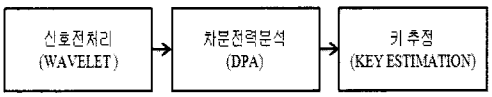
본 논문에서는 수집 신호의 전 처리를 통하여 DPA 공격 성능을 향상시키는 새로운 개념의 부채널 신호처리 기법인 웨이블릿(Wavelet) 기반의 다중해상도 분석(Multi-resolution Analysis, MRA) 방법을 제안한다. 본 논문의 구성은 다음과 같다. 우선 2장에서는 DPA 공격법을 소개하고, 3장에서는 웨이블릿 및 다중해상도 분석의 개념을 살펴보고, 4장에서는 제안된 신호처리 기법의 부채널 분석에의 적용 등을 설명하고, 5장에서는 기존 기법과 제안된 신호처리 기법을 키를 찾기 위해 필요한 트레이스의 수를 평가 기준으로 각 공격법의 성능을 비교하였다. 마지막으로 6장에서는 향후의 연구 계획 및 결론으로 마무리하였다.

II. DPA 공격법

이 장에서는 간단히 DPA의 개념을 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. 이러한 분석 시, DPA는 서로 다른 선택 평문 P를 입력으로 일련의 소비전력 파형을 수집하고, 소비전력 파형에 상응하는 평문과 추정한 비밀 키 K 값을 기준으로 수집신호 파형을 구분하여, 분류함수 $D(P, b_i, K)$가 "1"인 트레이스의 평균과 "0"인 트레이스의 평균의 차이를 취한 값 $\triangle D(b_i)$를 계산한다. 만약 추정한 비밀 키 K 값이 옳으면 구분된 두 집단 간의 평균 소비전력의 차이는 비트 "b_i"를 계산하는 순간 τ에서 $\triangle D(b_i) \neq 0$이 되며 DPA 피크로 불리는 값이 일반적으로 나타난다. 그러나 올바르지 못한 키에 대해서는 두 집단 간의 평균 소비전력의 차이는 $\triangle D(b_i) \approx 0$이 되며 피크 값이 나타나지 않을 것이다. 이러한 공격 방식의 경우, 한 비트의 변화에 의한 전력치의 변화는 극도로 작으며 각 트레이스가 τ의 조그만 불일치와 주변 잡음에 의해서도 DPA 공격의 성능은 아주 저하된다. 따라서 DPA 공격의 성능 향상은 트레이스의 시간 불일치를 최소화하고 효율적으로 잡음을 제거하는 신호처리 방법에 의존한다고 볼 수 있다.

III. 웨이블릿 분석(Wavelet Analysis)

본 논문에서 제안하는 웨이블릿 기반의 다중해상도 분석을 통한 DPA 기법의 전체적인 흐름도는 다음 [그림 1]과 같다.

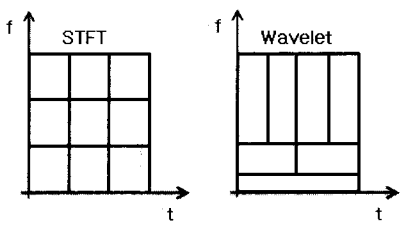


[그림 1] 부채널 분석 흐름도

[그림 1]에서 신호처리 분야는 구체적으로 다음의 세 부분으로 크게 나누어 볼 수 있다. 첫째 수집한 부채널 신호를 선택한 웨이블릿의 다양한 척도(Scale)로 표현하는 다중해상도 분석, 둘째 다중해상도로 분석된 신호로부터 잡음 등을 감소시키는 부분, 셋째 잡음 감소된 신호로부터 DPA 공격에 이용할 부채널 신호를 복원하는 부분으로 구성되어 있다. 제안하는 신호처리 기법은 부채널 분야에서는 DPA 공격의 성능 향상을 위해 최초로 적용되는 개념임으로, 먼저 제안기법의 물리적인 의미와 기초이론 등을 살펴보고 본 논문에서 사용하는 다중해상도분석 기법과 부채널 신호 분석에의 적용 개념을 설명하고자 한다.

3.1 웨이블릿 변환(Wavelet Transform)

신호처리에 많이 이용된 방법인 푸리에 변환[8](Fourier Transform)은 그 특성상 주파수 영역에서만 신호를 분석할 수 있어 시간 및 주파수 정보를 동시에 파악할 수 없다는 단점이 있다. 이러한 한계를 극복하기 위해 국소 푸리에 변환(Short Time Fourier Transform, STFT)이 도입되었는데, 그 대표적인 것이 가우시안 함수를 이용한 가보변환(Gabor's Transform)이다. 이 방법도 시간에 따라 특성이 변하는 정보의 분석을 효율적으로 할 수 없다는 단점을 가지고 있다. 그러나 웨이블릿 변환은 이러



[그림 2] 시간-주파수 분석 특성 개념도

한 단점을 보완하여 국소 푸리에 변환보다 더 효율적인 시간-주파수 분석을 가능하게 한다.

[그림 2]에서와 같이 푸리에 변환의 단점을 극복하기 위한 국소 푸리에 변환도 고정된 크기의 창문함수(Windowing Function)를 이용함으로 주파수 영역의 변화와는 관계없이 일정한 주파수 해상도를 가진다. 이는 부채널 정보와 같이 주파수 의존성(Dependency) 및 시간 국부성(Locality)을 동시에 갖는 신호의 분석에는 한계를 가지고 있다는 것을 의미한다. 그러나 본 논문에서 제안하는 웨이블릿 변환은 선택한 분석 웨이블릿의 특성에 따라 조금의 차이는 있으나, 앞의 [그림 2]를 통해서도 알 수 있는 바와 같이 고주파수 영역에서는 좋은 시간 해상도와 나쁜 주파수 해상도를 나타내고 저주파수 영역에서는 좋은 주파수 해상도와 나쁜 시간 해상도를 나타내는 특징이 있다.

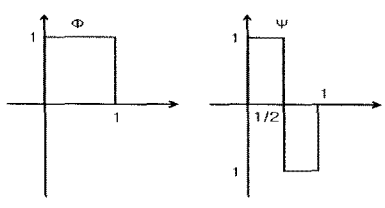
S웨이블릿 변환은 적절히 선택된 직교기저함수(Orthogonal Basis Function)를 척도(Scaling) 성하고 팽창(Dilation) 또는 이동(Translation)한 결과로 생기는 함수를 기저(Basis)로 이용하여 얻는다. 이를 수식으로 표현하면 다음과 같다.

$$\begin{aligned}\phi_{k,j}(t) &= 2^{k/2}\phi(2^k t-j)\\ \psi_{k,j}(t) &= 2^{k/2}\psi(2^k t-j)\end{aligned},\quad k,j\in Z \tag{1}$$

여기서, $\phi(t)$는 척도구성 함수, $\psi(t)$는 웨이블릿 함수이고, k는 척도, j는 이동을 나타내는 인자이다. 가장 기본적인 웨이블릿의 형태는 1910년에 Haar에 의해 소개된 것으로 다음과 같다.

$$\phi(t)=\begin{cases}1 & 0\le t<1\\ 0 & elsewhere\end{cases}$$
$$\psi(t)=\begin{cases}1 & 0\le t<1/2\\ -1 & 1/2\le t<1\\ 0 & elsewhere\end{cases} \tag{2}$$

Haar 함수는 [그림 3]과 같이 불연속적인 까닭으로 영상 신호와 같은 매끄러운 신호의 직접적인 처리



[그림 3] Haar 웨이블릿의 척도구성함수 $\phi(t)$와 웨이블릿 $\psi(t)$

에는 적당하지 못하나 웨이블릿의 개념을 이해하는 데에는 아주 좋은 함수이고, 암호연산에 의해 생성된 부채널 신호가 구동 클럭에 의존하기 때문에 Haar 함수적인 특성을 많이 가지고 있다고 생각할 수 있다.

따라서 본 논문에서는 분석 웨이블릿으로 Haar 함수를 선택하여 부채널 신호를 분석하였다.

3.2 다중해상도 분석(Multi-Resolution Analysis, MRA)

Mallat[9]은 직교기저 웨이블릿과 다중해상도 분석에 대한 이론과 구현 가능한 고속 웨이블릿 변환 방법을 1980년대 후반에 발표하였다. 유한 에너지 공간 $L^2(R)$에 속하는 임의의 함수 f를 구간별 상수함수(Box Function)로 근사할 수 있다는 사실은 잘 알려져 있다. 즉, 각각의 정수 k에 대하여

$$P_k f=\sum_{k\in Z}<f,\phi_{k,j}>\phi_{k,j} \tag{3}$$

라 정의하면, $P_k: L^2(R)\rightarrow V_k$는 정사영 (Orthogonal Projection) 이고, V_k는 $L^2(R)$의 닫힌 부공간(Closed Subspace)이다. 여기서 $<\bullet,\bullet>$는 내적(Inner Product)으로 다음 수식과 같이 정의한다.

$$<g_1,g_2>=\int_R g_1(t)g_2(t)dt \tag{4}$$

식 (3)에서 $P_k f$를 f의 다중해상도 근사(Multi-resolution Approximation)라 하고, V_k를 $L^2(R)$에서의 다중해상도 분석(Multi-resolution Analysis)이라 한다.

다중해상도 분석에서는 두 개의 연속하는 해상도 레벨에서 근사신호들의 차이를 이용하여 주어진 신호를 재구성할 수 있다. 해상도 레벨 V_{k+1}는 V_k와 직교여공간(Orthogonal Compliment Space) W_k= $V_{k+1}-V_k$로 정의할 수 있고, 이는 V_{k+1}의 근사신호가 V_k와 V_k 공간으로 사영(Projection)될 때 없어지는 세부정보 W_k로 구성됨을 보여준다. 공간 W_k를 해상도 수준 k에서의 웨이블릿 공간(Wavelet Space)이라고 정의한다. 만약 W_0의 생성원 ψ가 존재하여

$$\{\psi_{k,j}(t):=2^{k/2}\psi(2^k t-j)\,|\,j\in Z\} \tag{5}$$

가 W_k의 정규직교기저가 되면, 정사영 $P_k: V_{k+1}\rightarrow V_k$

와 같이 $Q_k : V_{k+1} \rightarrow W_k$가 존재하여 유한 에너지 공간 $L^2(R)$에 속하는 함수 f는 다음의 수식과 같이 표현할 수 있다.

$$\begin{aligned} P_{K+1}f(t) &= P_k f(t) + Q_k f(t) \\ &= \sum_j < f, \phi_{k,j} > \phi_{k,j}(t) \\ &\quad + \sum_j < f, \psi_{k,j} > \psi_{k,j}(t) \end{aligned} \tag{6}$$

식 (6)에서 척도구성 함수 $\phi_{k,j}$ 및 웨이블릿 $\psi_{k,j}$와 f의 내적을 구하면

$$\begin{aligned} c_{k,j} &= < f, \phi_{k,j} > = \sum_{l \in Z} h_{l-2j} c_{k+1,l} \\ d_{k,j} &= < f, \psi_{k,j} > = \sum_{l \in Z} g_{l-2j} c_{k+1,l} \end{aligned} \tag{7}$$

이 되고, 해상도수준 $k+1$에서 f의 이산근사 신호 c_{k+1}은 해상도수준 k에서의 이산근사 신호 c_k와 이산세부 신호 d_k로 분해됨을 알 수 있다. 여기서 $h_n = < \phi, \phi_{1,n} >$ 및 $g_n = < \psi, \phi_{1,n} >$으로 정의하고 척도구성 계수 $(h_n)_{n \in Z}$와 웨이블릿 계수 $(g_n)_{n \in Z}$는 Mallat의 공식에 의해 $g_n = (-1)^n h_{1-n}$의 관계에 있다.

반대로 낮은 해상도수준에서 f의 이산근사 신호와 이산세부 신호로부터 높은 해상도수준에서 f의 이산근사 신호를 복구할 수 있다. 척도구성 함수 및 웨이블릿 f의 내적을 구하고 이를 각각의 계수로 표시하면

$$\begin{aligned} < f, \phi_{k+1,l} > &= \sum_j h_{l-2j} < f, \phi_{k,j} > \\ &\quad + \sum_j g_{l-2j} < f, \psi_{k,j} > \\ c_{k+1,l} &= \sum_j h_{l-2j} c_{k,j} + \sum_j g_{l-2j} d_{k,j} \end{aligned} \tag{8}$$

이 되며, $k_0 \le k < K$에서 식 (8)을 반복 적용하여 적당한 해상도수준 K에서 주어진 신호 f_K를 다음과 같이 재구성할 수 있다.

$$f_K = \sum_j c_{k_0,j} \phi_{k_0,j} + \sum_{k=k_0}^{K-1} \sum_j d_{k,j} \psi_{k,j} \tag{9}$$

이와 같이 척도구성 계수 $c_{k_0,j}$의 k_0를 기준으로 선정하고 적당한 해상도수준 K를 정하여 세부신호의 계수 $d_{k,j}$를 이용하여 신호를 표현하는 기법을 다중해상도 분석이라 한다.

IV. 부채널 신호 분석에의 적용

4.1 부채널 신호의 구성[10]

먼저 웨이블릿 관점의 분석을 위해 일반적으로 암호연산 시 출현하는 부채널 신호의 구성을 살펴보면, 다음의 식과 같이 4가지 부분으로 크게 정의할 수 있다.

$$S_t = S_d + S_c + N_p + N_g \tag{10}$$

여기에서 S_t는 수집된 부채널 신호, S_d는 암호연산을 수행하는 프로세스와 관련된 신호, S_c는 암호연산 데이터와 관련된 신호, N_p는 신호의 시간 불일치에 의해 생기는 위상잡음, N_g는 디바이스 내부잡음 등의 다양한 잡음원에 의해 발생하는 가우시안(Gaussian) 잡음이다. 각각의 부채널 구성 신호의 특성을 나열하면 다음과 같다.

첫 번째, S_d는 암호연산 하드웨어에 의존하는 신호로 선택된 디바이스의 특성에 따라 이미 알려진 신호로 DPA와 같이 통계적 기법에 기반한 부채널 분석에는 거의 영향을 미치지 않는 신호로 판단할 수 있다.

두 번째, S_c는 암호연산 순간 데이터의 해밍 웨이트(Hamming Weight) 값에 따라 변하는 신호로 $S_c = \epsilon \cdot H(w)$와 같이 표현할 수 있다. 여기서 $H(w)$는 처리하고자 하는 정보의 해밍 웨이트를 나타내고, ϵ는 단위 해밍 웨이트의 변화에 따른 신호의 변화량을 나타낸다. 이 신호는 암호연산의 시간적인 특성으로 수집한 부채널 신호에서 주파수만으로는 정확한 표현이 어려운 신호이다.

세 번째, N_p는 주로 디바이스 구동 클럭의 위상 불일치 등과 같은 원인에 의해 발생하는 잡음으로 부채널 공격의 성능에 결정적인 영향을 미치는 잡음이다. 위상 불일치에 의한 영향을 최소화하기 위한 기법으로 각 수집 부채널 신호간의 상관도(Correlation)를 이용한 기법이 사용되기도 하지만 위상 불일치의 원인이 구동 클럭의 지터(Jitter)와 같이 시간에 따라 변화(Time Variant)하는 특성을 가지는 경우에는 신호 정렬법(Signal Alignment) 및 주파수 변환 기법도 부채널 공격 기법의 성능 향상에 크게 도움이 되지 못한다.

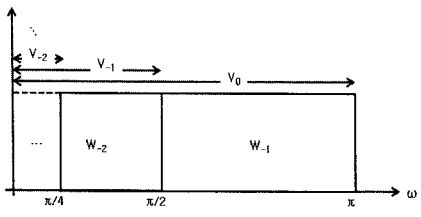
네 번째, N_g는 다양한 잡음원의 합에 의한 가우시안적인 특성을 가지고 있는 잡음으로 $N(0,\sigma)$와 같이 모델링할 수 있는 신호로 통계적인 기법을 이용하여 부채널 공격에 미치는 영향을 많이 줄일 수 있는 잡음이다.

여기서 부채널 공격의 성능 향상을 위해 효율적인 신호처리가 필요한 주요 성분은 S_c, N_p 및 N_g로 판단할 수 있다.

4.2 부채널 신호의 다중해상도 분석(MRA)

부채널 공격의 성능 향상은 S_c 값의 증폭과 N_p 및 N_g의 감쇄를 통하여 얻을 수 있다. 그러나 이 신호는 단순한 주파수 변환 및 필터 기법을 통하여 처리할 수 없다. 푸리에 기법은 S_c의 시간 국부성을 효과적으로 처리하지 못하고, 단순한 필터 기법은 N_p 및 N_g의 감소와 동시에 S_c 정보도 감소시키는 단점을 피할 수 없다. 따라서 암호연산 신호의 시간 국부성을 충실히 표현하고, 암호연산 정보에 미치는 영향을 최소화하는 기법의 개발은 부채널 공격의 성능 향상에 절대적이라 할 수 있다.

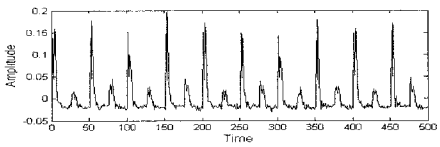
본 논문에서 제안하는 웨이블릿 기반 다중해상도 분석기법은 기본적으로 S_c와 같은 시간 국부성을 효율적으로 표현할 수 있고 N_p 및 N_g를 효율적으로 감쇄할 수 있다. Vetterli[11]는 다중해상도 분석기법을 필터와 관련한 대역분할부호화(Subband Coding) 기법으로 해석할 수 있음을 보여주고 있다. 다음 [그림 4]는 웨이블릿 기반의 다중해상도 분석의 대역분할 부호화 개념도이다.



[그림 4] 다중해상도 분석의 대역분할 부호화 개념도

다중해상도분석 기법을 대역분할 부호화 방식으로 해석하면, 해상도 레벨 1에서는 원 신호를 웨이블릿 계수로 표현하는 고주파 영역(W_{-1})과 척도구성 계수로 표현되는 저주파 영역(V_{-1}) 으로 분할하고, 레벨 2에서는 레벨 1에서 분할한 저주파 영역(V_{-1})을 다시 고주파 영역(W_{-2})과 저주파 영역(V_{-2})으로 반복하여 이분법적인(Dyadic) 기법으로 분할함을 알 수 있다.

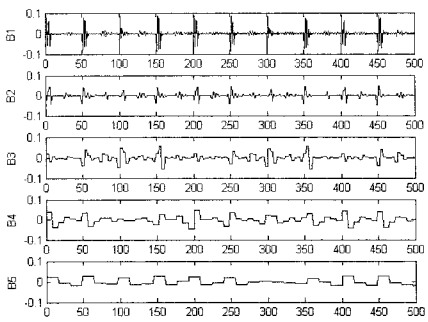
본 논문에서는 분석 대상으로 사용하는 DES 연산 시 수집된 부채널 신호를 지금까지 살펴본 웨이블릿의 다중해상도 분석기법과 대역분할 부호화의 개념을 적용하여 해석한다. 다음 [그림 5]는 암호연산 시 소비되는 전력신호의 일부분을 확대하여 표현한 그림이다.



[그림 5] 암호연산 시 소비되는 전력신호의 예

위의 소비전력 파형은 $S_t = S_d + S_c + N_p + N_g$로 구성된 신호이다. 파형에서 S_d는 전체적인 신호의 형태를 결정하고, N_p의 주요 성분은 주로 클럭 에지(Clock Edge)와 같은 신호의 변환(Transition)영역에 존재하며, N_g는 전 파형에 고루 분포한다고 추정할 수 있다.

[그림 6]은 [그림 5]의 원 수집 파형을 분석 웨이블릿 함수로 Haar를 선택하여, 분석 레벨이 4인 경우 각각의 해상도로 위의 소비전력 파형을 분석한 그림이다.



[그림 6] Haar 웨이블릿을 이용한 분석 레벨 4에 대한 다중해상도 신호

[그림 6]에서 B_1, B_2, B_3, B_4, B_5는 [그림 4]의 $W_{-1}, W_{-2}, W_{-3}, W_{-4}, V_{-4}$에 해당하며, B_1, B_2, B_3, B_4는 웨이블릿 계수를 나타내고 B_5는 척도구성 계수를 나타낸다. 즉, 앞 절의 식 (9)에서 B_5는 척도구성 계수 $c_{k_0,J}$로 B_1, B_2, B_3, B_4는 세부신호 계수 $d_{k,j}$로 표현된다.

[그림 6]의 다중해상도 신호를 부채널 신호의 구성

을 기준으로 분석하면 B_1,B_2는 신호의 변화가 급격하고 클럭 에지(Clock Edge) 부분에 집중하는 특성을 가지고 있으므로 주로 잡음과 관련된 N_p와 N_g로 구성된 신호로 볼 수 있고, B_3,B_4,B_5는 클럭에 따른 신호 파형의 구간별 변화를 나타내고 있으므로 주로 암호연산 및 프로세서와 관련된 S_c와 S_a로 구성된 신호로 추정할 수 있다.

V. 실험 결과

5.1 실험 환경

본 실험에서는 DES[13] 알고리즘을 PIC16F84A [14]에 구현하였다. DES의 첫 번째 라운드를 공격 대상으로 선정하였고 실험 수행 방법은 먼저 임의로 선택한 1,000개의 평문을 입력으로 하여 공격 파형을 첫 번째 라운드를 기준으로 수집하였다. 수집한 신호는 본 논문에서 제안한 웨이블릿 기법으로 전처리하여 DES의 8개 S-Box 각각에 대하여 성능을 측정하여 DPA 공격의 효율성을 기존의 방법과 비교하였다. 구체적인 장비로는 DC Power Supply를 이용하여 +5V의 전력을 외부에서 공급하고, Function Generator를 이용하여 1MHz의 Sine Wave를 공급하게 된다. 그리고 소비전력 파형을 측정하기 위하여 Tektronix사의 TDS3032B의 디지털 오실로스코프(CRO)를 사용하여 50MHz로 표본화하였다. 그리고 실험을 수행한 환경은 일반적인 사무실 환경이다.

5.2 성능 분석

본 논문에서는 DPA 공격 방법으로 S-box의 각 비트에 대한 DPA 공격의 결과 값을 합하여 이 값을 기준으로 공격을 수행하였다. 비트 합 방식은 각 비트의 연산결과가 서로 거의 독립인 DES 공격법으로 아주 효율적인 방식이다. 실험에서는 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.

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.

$$\sum_i \triangle_D(b_i) \tag{11}$$

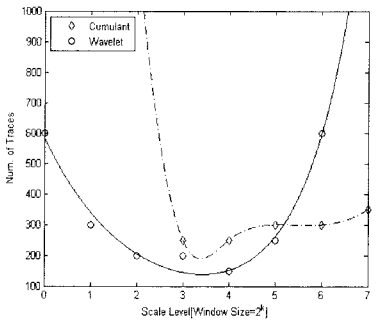
예를 들어 DES의 경우에는 각 S-box의 공격 시 i=1,2,3,4로 4 비트 합 방식을 사용하여 공격법을 구성할 수 있다. 비트 합 방식은 각 비트의 연산결과가 서로 거의 독립인 DES 공격법으로 아주 효율적인 방식이다. 이렇게 비트 합에 의한 성능 비교 분석법을 통해 본 논문에서는 1,000개의 신호를 이용하여 제안한 전처리 방법에 의한 DPA의 성능을 기존의 방법과 비교하였다.

본 논문에서는 가장 기초적인 웨이블릿이면서 부채널 신호의 특성을 효과적으로 표현할 수 있는 Haar 웨이블릿을 선정하여 해상도 각 레벨[또는 윈도우 크기]에서의 잡음 감소법[7]과 DPA 공격 성능을 비교 분석하고, 원 신호를 기준으로 기존의 신호처리 방식인 주파수 변환법[6], 잡음 감소법 및 신호 압신법[12]등과 DPA 공격에 필요한 트레이스의 수를 기준으로 S/N 비를 비교하였다.

5.2.1 해상도와 DPA 성능

[그림 7]은 다중해상도 분석의 해상도 각 레벨에서의 DPA 공격 성능과 기존에 제안된 잡음감소 분석법의 윈도우 크기에 따른 DPA 공격 성능을 올바른 키를 찾기 위해 필요한 트레이스(Trace)의 수를 기준으로 분석한 결과이다.

[그림 7]에서 잡음 감소법은 가우시안 잡음의 4차 큐물런트(Cumulant)의 통계적 특성을 이용함으로 통계처리에 필요한 윈도우의 최소 크기가 기본적으로



[그림 7] 레벨(또는 윈도우 크기) 별 DPA 성능

필요하다. 따라서 윈도우의 크기가 작을 경우에는 잡음 감소법이 원 신호를 단순히 이용하는 DPA 기법보다 성능이 더욱 열화 됨을 알 수 있다. 즉, 윈도우의 크기가 4보다 작은 경우에는 1,000개의 트레이스로도 정확한 키를 찾을 수 없었다.

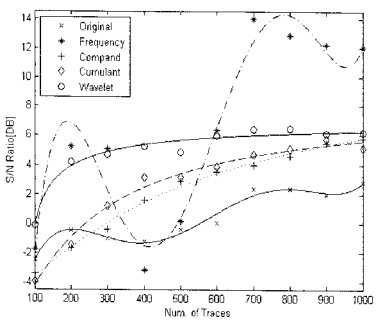
그러나 다중해상도 분석법은 부채널 신호의 통계적 처리에 기반한 잡음 감소법과는 다르게 신호를 다중해상도 각 레벨로 분석하고 해당 레벨 이하의 신호는 잡음으로 판단하여 필터링하는 웨이블릿 분석법을 기본으로 하고 있으므로 효율적인 DPA 공격이 가능함을 알 수 있다.

특히, [그림 7]에서 본 논문의 분석 대상 DES 디바이스는 레벨 4에서는 150개의 트레이스로 정확한 키를 찾고, 레벨 7 이상의 경우에는 1,000개의 트레이스로는 정확한 키를 찾을 수 없었다. 이는 레벨 0 또는 1에서는 잡음에 의한 에너지가 많고, 레벨 7 이상에서는 암호연산 관련 에너지는 거의 존재하지 않음을 보여주고 있다. 즉, 본 논문에서 제안한 다중해상도 분석법을 통해 우리는 아주 효과적으로 디바이스에 따라 특성을 달리하는 암호연산 에너지의 시간적 분포 특성을 알 수 있다.

5.2.2 각 방식의 성능 비교

[그림 8]은 DES 연산 시 각각의 신호처리 방식에 따른 DPA의 성능을 S/N 비로 비교한 그림이다. S/N 비의 측정 방법은 올바른 키일 경우의 차분 값과 올바르지 못한 키일 경우의 차분 값 중 최고치를 데시벨(dB) 단위로 비교한 결과이다. 따라서 0[dB] 이상의 값을 가지는 경우에는 올바른 키를 찾는다고 판단할 수 있다

[그림 8]에서 주파수 변환에 의한 DPA 공격이 다른 방식에 비해 S/N 비의 변화 폭이 상당히 큰 천이



[그림 8] 전처리 방식별 DPA 성능 비교

영역이 존재함을 알 수 있다. 이는 각 트레이스 별 위상의 에러가 일정하지 않은 경우에는 주파수 변환에 의한 신호처리 기법은 제대로 성능을 발휘하기가 어려움을 나타낸다. 원 신호의 경우에도 주파수 변환 기법보다는 작지만 트레이스의 수의 증가에 따라 S/N 비의 변화가 단조 증가하지 않는 천이영역이 존재함을 알 수 있다. 따라서 두 가지 방식은 잡음의 감쇄 또는 신호의 증폭을 하지 않으므로 트레이스에 포함된 시간 불일치에 의한 위상잡음 또는 기타 잡음에 의한 영향에 아주 민감한 영역이 존재함을 알 수 있다.

그러나 압신법은 암호연산 관련 신호의 증폭을 통해 잡음의 영향을 줄이고, 잡음 감소법은 윈도우내 신호의 통계적 특성을 이용한 잡음의 제거 또는 감쇄에 의한 DPA 공격 성능 개선 방법이며, 본 논문에서 제안하는 방법은 부채널 신호를 적절히 선택한 웨이블릿 함수로 분석하고 다중해상도 각 레벨의 암호연산 및 잡음관련 신호 특성을 분석하여 DPA 공격 성능을 개선하는 방법이다. 그러므로 트레이스의 수가 증가함에 따라 S/N 비도 단조 증가함을 알 수 있다.

특히, 본 논문에서 제안한 다중해상도 분석기법은 작은 트레이스의 수에서도 충분한 S/N 비로 수렴하여 안정적인 값을 유지하고, 압신법 및 잡음 감소법에 의한 방식도 다중해상도 분석법 보다는 충분한 S/N 비로의 수렴은 늦지만 트레이스 수의 증가에 비례하여 안정적인 값으로 증가한다.

5.3 성능 평가

앞의 성능 분석에서 다중해상도 분석을 통해 본 실험에서 사용한 디바이스의 DES 암호연산 에너지는 해상도 레벨 4에 주로 집중함을 알 수 있다. 즉, 본 논문의 실험 환경은 디바이스 구동 클럭이 1MHz이고 오실로스코프의 트레이스 획득 표본화 주파수가 50MHz 임을 고려할 때 암호연산 관련 데이터는 약 $20[\eta\text{sec}/sample]\times 2^4[samples]=320[\eta\text{sec}]$의 지속 시간으로 주로 존재하는 특성이 있음을 알 수 있다.

[표 1]를 살펴보면 웨이블릿에 의한 다중해상도 분

[표 1] 각 신호처리 방식별 DES에 대한 DPA 성능 비교

신호처리방식 / 비교항목	원신호	주파수 변환	압신법	잡음 감소법	다중 해상도
트레이스의 수	600	500	400	250	150
성능 향상도	-	17%	33%	58%	75%

석법이 기존의 다른 방법인 주파수 변환, 압신법 및 잡음 감소법등에 비해 월등히 성능이 우수함을 알 수 있다.

특히, 본 논문에서 제안한 다중해상도 분석법을 적용할 경우 DPA 성능의 직접적인 개선뿐만 아니라 암호연산 프로세스의 부채널 신호 특성을 다중 해상도로 분석하여 암호와 관련된 에너지가 시간 축에서 어떠한 형태로 존재하는지를 함께 분석할 수 있다는 것이다. 이는 기존의 다른 신호처리 기법에서는 없는 본 제안 기법의 또 다른 특징이며 이점이다.

VI. 결 론

본 논문에서는 부채널 공격에 많이 사용되는 DPA의 성능을 획기적으로 개선할 수 있고 동시에 암호연산의 특성을 분석할 수 있는 새로운 개념의 전처리 방법을 제시하였다. 본 논문에서 제안한 웨이블릿 기반의 다중해상도 분석법은 기존의 방식 보다 DPA 성능이 아주 우수할 뿐만 아니라 암호연산 에너지의 시간적 분포 특성을 동시에 분석할 수 있었다. 향후 제안한 웨이블릿 기반의 다중해상도 분석 기법을 위상 잡음의 영향을 많이 받는 다양한 보안장비의 암호연산에 적용하여 DPA의 공격성능 개선에 미치는 영향을 연구할 것이다. 또한, 본 논문에서 제안한 다중해상도 분석법이 CPA 및 템플릿(Template) 공격과 같은 부채널 공격법에는 어떠한 효과를 나타내는지도 연구해 볼 것이다.

참 고 문 헌

[1] 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.

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

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

[4] S. Chari, J. Rao, and P. Rohatgi, "Template Attacks," CHES 2002, LNCS 2523, pp. 13-28, 2003.

[5] C. Rechberger and E. Oswald, "Practical Template Attacks," WISA 2004, LNCS 3325, pp. 443-457, 2004.

[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, 2005.

[7] 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.

[8] R. Lyons, Understanding Digital Signal Processing, Second Edition, Prentice Hall, 2004.

[9] S. Mallat, a Wavelet Tour of Signal Processing, Second Edition, Academic Press, 1999.

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

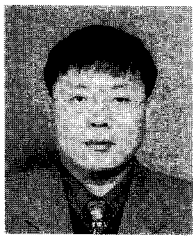
[11] M. Vetterli and J. Kovacevic, Wavelets and Subband Coding, Prentice Hall, 1995.

[12] 류정춘, 한동국, 김성경, 김희석, 김태현, 이상진, "신호 압신법을 이용한 차분전력분석 공격성능 향상," 정보보호학회논문지, 18(2), pp. 39-47, 2008년 4월.

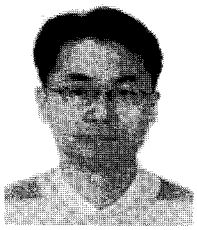
[13] U.S. DoC/NIST, "Data Encryption Standard(DES)," FIPS PUB 46-3, National Institute of Standards and Technology, Oct. 1999.

[14] Microchip Technology Inc., "PIC16F8X-18 pin Flash EEPROM 8-bit Microcontrollers," http://ww1.microchip.com/downloads/en/devicedoc/30430c.pdf, 1998.

〈著者紹介〉

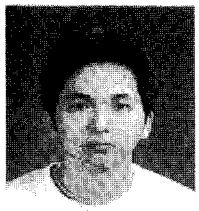


류 정 춘 (Jeong Choon Ryoo) 정회원
1988년 2월: 경북대학교 전자공학과 졸업(학사)
1990년 2월: 경북대학교 전자공학과 석사(공학석사)
1990년 1월~1995년 4월: LG정보통신 연구원 근무
1996년 1월~1999년 11월: 대우그룹 해외통신사업본부 근무
2005년 3월~현재: 고려대학교 정보경영공학전문대학원 박사과정
〈관심분야〉 부채널 공격, 대칭키 암호의 분석 및 설계, 이동통신 암호프로토콜

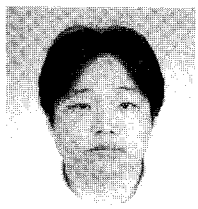


한 동 국 (Dong Guk Han) 정회원
1999년: 고려대학교 수학과 졸업(학사)
2002년: 고려대학교 수학과 석사(이학석사)
2005년: 고려대학교 정보보호대학원 박사(공학박사)
2004년 4월~2005년 4월: 일본 Kyushu Univ., 방문연구원
2005년 4월~2006년 4월: 일본 Future Univ.-Hakodate, Post.Doc.
2006년 6월~2009년 2월: 한국전자통신연구원 정보보호연구단 선임연구원
2009년 3월~현재: 국민대학교 수학과 조교수
〈관심분야〉 공개키암호 안전성분석 및 고속구현, 부채널분석, RFID/USN 정보보호 기술

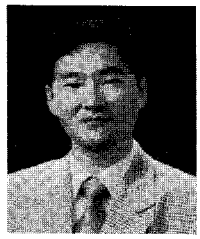
김 성 경 (Sung Kyoung Kim) 학생회원
2005년 2월: 동의대학교 수학과 학사
2007년 8월: 고려대학교 정보경영공학전문대학원 공학석사
2007년 9월~현재: 고려대학교 정보경영공학전문대학원 박사과정
〈관심분야〉 부채널 공격, 공개키 암호, 암호칩 설계 기술



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



김 태 현 (Tae Hyun KIM) 정회원
2002년 2월: 서울 시립대학교 수학과 이학사
2004년 8월: 고려대학교 정보보호 대학원 공학석사
2009년 2월: 고려대학교 정보경영공학전문대학원 공학박사
〈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~현재: 고려대학교 정보경영공학전문대학원 부교수
〈관심분야〉 부채널 공격, 대칭키 암호의 분석 및 설계, 정보은닉이론, 컴퓨터 포렌식