웨이블릿 잡음 제거 방법을 이용한 전력 분석 공격 성능 개선

정회원 김 완 진*, 송 경 원**, 준회원 이 유 리*, 종신회원 김 호 원***, 김 형 남*

Performance Improvement of Power Analysis Attacks based on Wavelet De-noising

Wan-Jin Kim*, Kyoung-Won Song** *Regular Members*, Yu-Ri Lee** *Associate Member*,
Ho Won Kim***, Hyoung-Nam Kim* *Lifelong Members*

요 약

전력 분석 (Power Analysis, PA) 공격은 정보보안 영역에서 매우 효과적인 물리적 공격방법으로 알려져 있다. 이 공격방법은 보안 장치로부터 누설된 전력 소비 신호의 통계적인 특성을 분석하여 비밀 키 (secret keys)를 찾아낸다. 그러나 누설된 전력 신호의 값이 크지 않기 때문에, 잡음에 의해 PA 공격 성능이 저하될 수 있다. 이런 PA 공격의 잡음 민감성을 극복하기 위해, 본 논문에서는 웨이블릿 잡음 제거 (wavelet de-noising)에 기반한 공격 성능 향상 방법을 제안한다. 모의실험을 통해, 제안된 잡음 제거 방법이 공격 성공에 필요한 신호의 개수와 공격 결과의 신뢰도 측면에서 공격 효율을 향상시킴을 보인다.

Key Words : SCA, DPA, CPA, power analysis, wavelet de-noising, security

ABSTRACT

Power analysis (PA) is known as a powerful physical attack method in the field of information security. This method uses the statistical characteristics of leaked power consumption signals measured from security devices to reveal the secret keys. However, when measuring a leakage power signal, it may be easily distorted by the noise due to its low magnitude values, and thus the PA attack shows different performances depending on the noise level of the measured signal. To overcome this vulnerability of the PA attack, we propose a noise-reduction method based on wavelet de-noising. Experimental results show that the proposed de-noising method improves the attack efficiency in terms of the number of signals required for the successful attack as well as the reliability on the guessing key.

Ⅰ. 서 론

정보보안을 위해 널리 사용되는 암호화 알고리즘들은 암호화된 정보를 해독하기 위한 다양한 공격 방법들과 경쟁하며 발전해 왔다. 그러나 암호화 알고리즘이 H/W에서 동작할 때 발생하는 물리적 누설신호를 이용해 공격을 수행하는 부채널 공격 (side channel attack, SCA) 방법이 등장하면서, 암호화 알고리즘의 보안 위협수준이 크게 증가하였다 [1]. 대표적인 SCA 방법으로는 연산 시간을 이용하는 시차 공격 (timing

※ 이 논문은 2008년 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No.2008-0061842)
* 부산대학교 전자전기공학과 통신 및 신호처리 연구실 (hnkim@pusan.ac.kr), ** SK C&C 금융사업본부,
*** 부산대학교 정보컴퓨터공학부 정보보호 및 임베디드 보안 연구실
논문번호 : KICS2010-03-134, 접수일자 : 2010년 3월 31일, 최종논문접수일자 : 2010년 9월 7일

attack, TA)과, 전력 소비를 이용하는 전력 분석 공격 (power analysis attack, PA), 방사되는 전자기를 이용하는 전자기파 분석 공격 (electromagnetic analysis attack, EMA)이 있다. 현재는 다른 SCA 방법에 비해 공격 효과가 낮은 시차 공격을 제외하고 PA와 EMA에 관한 연구가 활발하게 진행되고 있으며[1-6], 이 중에서도 PA는 현재까지 개발된 대부분의 암호 알고리즘에 대해 가장 효과적이고 위협적인 공격 방법으로 알려져 있다.

전력 분석 공격에는 다양한 방법들이 존재하나, 크게 분류하면 단순 전력 분석 (simple power analysis, SPA) 공격과 차분 전력 분석 (differential power analysis, DPA) 공격, 그리고 상관계수를 이용하는 DPA 공격인 상관도 분석 (correlation power analysis, CPA) 공격으로 나뉜다[2-4]. SPA 공격은 암호화 과정과 일치하는 전력 소비 변화를 직접 관찰하면서 비밀 키 (secret key)를 찾아내는 방법으로, 공격 절차가 매우 단순하나 암호화 절차가 순차적으로 수행될 때에만 비밀 키를 찾을 수 있는 단점이 있다. 이러한 SPA 공격의 문제점을 극복하기 위해 암호화 장치가 0과 1의 신호를 처리할 때 누설되는 소비 전력의 차를 통계적으로 분석하는 DPA 공격이 등장하였으며[2,8], 이 후 DPA 공격의 성능 향상을 위해 비트 값에 따른 소비 전력 차 대신 공격자가 추정하는 모델과 소비 전력 간의 상관도를 이용하여 비밀 키를 찾아내는 CPA 공격이 등장하였다[4]. 통계적 분석에 기반한 PA 공격들은 전반적으로 우수한 공격 성능을 보이며, 특히 CPA는 매우 뛰어난 공격 성능을 보이는 것으로 알려져 있다[4].

일반적으로 최상의 PA 공격 성능을 얻기 위해서는 획득한 소비 전력 신호의 대부분이 암호화 장치의 동작에 기인하는 부분으로 구성되어 있어야 한다. 그러나 본 논문에서 타겟 디바이스로 사용한 Telos 모듈과 같이 소비 전력이 낮은 칩 (TI MSP430)을 사용할 경우, 측정되는 소비 전력은 주변 장치의 동작에 크게 영향을 받게 된다. 이런 경우 획득한 소비 전력 신호에서 암호화 장치에서 발생하는 신호의 기여도는 낮아지고, 암호화 장치와 관련이 없는 부분, 즉 잡음으로 간주될 수 있는 부분의 기여도는 크게 증가하게 되므로, 기존 PA 공격의 실패 가능성도 높아지게 된다. 이렇게 잡음으로 인해 PA 공격의 성능이 저하되는 경우, 해결책으로 측정된 신호를 평균해 잡음의 영향을 감소시키는 방법을 고려해 볼 수 있다[2]. 그러나 평균을 이용해 잡음을 제거하는 효과를 보기 위해서는 많은 수의 소비 전력 신호가 요구되고, 암호화 장치의 비선형성에 의해 발생하는 고조파로 인한 전력 신호의 피크 왜곡은 보상할 수 없는 단점이 있다.

이러한 난점을 극복하기 위해 다중해상도 분석 (multi-resolution analysis, MRA)를 이용하여 측정된 전력 신호에 포함된 잡음 성분을 제거할 수 있는 방법이 제안되었다[7]. MRA를 이용한 잡음 감소 방법은 높은 공격 성능 향상을 보여주었으나, 고주파 성분을 모두 잡음으로 간주하여 배제하므로 의미 있는 고주파 성분까지 모두 제거돼 신호의 모양이 왜곡되고 이로 인해 공격 성능이 저하될 가능성이 있다. 이러한 문제점을 해결하기 위해 본 논문에서는 웨이블릿 변환에 기반한 잡음 감소 방법 (denoising)을 사용하여, 신호에 포함된 왜곡요소를 효과적으로 제거할 수 있는 전처리 방법을 제안한다. 제안된 방법은 신호의 모양을 유지하면서 전력 신호와 관계없는 작은 피크 값을 억제해 PA 공격 성능을 향상시킨다.

본 논문의 구성은 다음과 같다. II절에서는 DPA 공격과 CPA 공격의 기본적인 개념을 설명하고, III절에서는 웨이블릿 변환을 이용하여 신호의 특성을 유지하면서 측정된 신호에 포함된 왜곡 요소인 잡음을 감소시킬 수 있는 전처리 방법을 제안한다. IV절에서는 MSP430을 사용하는 센서모듈에서 측정된 소비 전력 신호와 이를 제안된 전처리 방법으로 처리한 신호를 각각 DPA와 CPA로 공격해 성능을 평가한 후, 그 결과를 분석하였다. 마지막으로 V절에서는 결론을 맺는다.

Ⅱ. 전력 분석 공격

현재 사용되고 있는 전력 분석 공격에는 P. Kocher 등에 의해 소개된 차분 전력 분석 (DPA) 공격[2],[3]과 Brier 등에 의해 제안된 DPA 공격인 상관도 분석 공격 (CPA)이 있다[4]. DPA 공격은 전력 소비 신호의 통계적인 특성, 즉 0의 비트 값일 때와 1의 비트 값인 경우의 전력 소비가 다르다는 점을 이용해 암호화 시스템의 비밀 키 (secret key)를 찾는 방법으로, 공격 시 암호화 알고리즘 구조에 대한 자세한 지식이 없이도 비밀 키를 얻을 수 있는 이점을 가지고 있다[2,8]. 이에 반해 CPA는 공격자가 Hamming weight model이나 Hamming distance model과 같은 소비 전력 모델을 만들고, 측정된 소비 전력신호와의 상관계수를 구한 후 이를 분석하여 비밀 키를 찾는 방법이다[4]. 본 절에서는 위에서 언급한 DPA와 CPA 공격방법에 대해 자세히 살펴볼 것이며, 설명의 편의를 위해 실험에 사용한 AES (Advanced Encryption Standard)를[9] 공

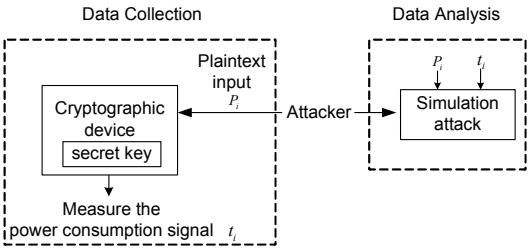

그림 1. 전력 분석 공격 과정[2].

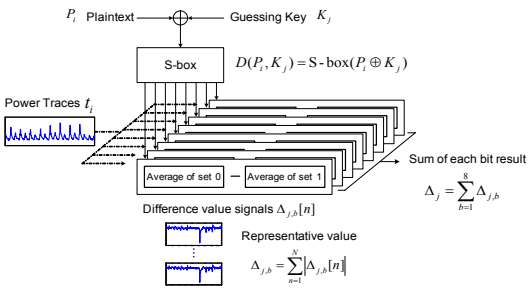

그림 2. 차분 전력 분석 (DPA) 공격의 블록 다이어그램.

격 대상 암호화 알고리즘으로 선택해 사용한다.

2.1 차분 전력 분석 (DPA) 공격

DPA 공격은 그림 1과 같이 데이터 수집과 데이터 분석 과정으로 나눌 수 있다. 우선 데이터 수집 단계에서 공격자는 임의의 평문 P_i (i=1,2,⋯,M)를 입력으로 하여, 암호화 알고리즘이 동작할 때 발생하는 누설 전력 신호를 수집하며, 이 때 M은 수집한 전력 신호의 개수가 된다. 실제 타겟 보드에서 데이터 수집이 끝나면 데이터 분석에 들어가게 되는데, 데이터 분석 과정에 대한 블럭도는 그림 2에 도시되어 있다.

데이터 분석 과정의 첫 단계는 데이터 수집 단계에서 사용한 평문 P_i와 추정 가능한 비밀 키 K_j (0h00～0hFF)를 exclusive-OR하여 S-box에 입력하는 것이다. 여기서 S-box는 AES 알고리즘에 포함된 substitution box를 의미하고, j는 추정 키의 인덱스로 0에서 255 사이의 값을 가진다. S-box의 입력 $P_i \oplus K_j$는 치환과정을 거쳐 출력되며, 이 결과는 분류함수를 거쳐 '0' 또는 '1'의 값으로 출력된다. 이 때 분류함수 $D(P_i, K_j)$는 다음과 같이 정의된다[10].

$$D(P_i, K_j) = \text{S-box}(P_i \oplus K_j) \tag{1}$$

여기서 분류함수의 출력 즉, S-box의 출력 1 byte에 해당하는 8개의 bit는 그 결과가 '0'인지 '1'인지에 따라 평문과 쌍을 이루는 전력 신호를 '0' set 또는 '1' set으로 분류한다. 이 과정은 하나의 추정 키에 대해 모든 평문이 연산될 때 까지 수행되며, 이 과정이 끝나면 각 set의 평균을 구하고 최종적으로 '0' set과 '1' set의 차분 값을 구하게 된다. 이 때 차분 값 $\Delta_{j,b}$는 다음과 같이 구할 수 있다.

$$\Delta_{j,b} = \frac{\sum_{i=1}^{M} D(P_i, K_j) t_i[n]}{\max[1, \sum_{i=1}^{M} D(P_i, K_j)]} - \frac{\sum_{i=1}^{M} (1 - D(P_i, K_j)) t_i[n]}{\max[1, \sum_{i=1}^{M} (1 - D(P_i, K_j))]} \tag{2}$$

여기서 b와 n은 각각 S-box 출력의 bit 인덱스와 소비 전력 신호의 샘플 인덱스를 의미한다.

상기에서 언급한 과정을 추정 키의 값을 변경시켜 가며 수행하면 각 추정키에 해당 하는 차분 값들을 얻을 수 있는데, 정확한 키 값을 찾아내기 위해서는 이 차분 값들의 크기를 비교해 최대 크기를 가지는 차분 값을 찾아야 한다. 그러나 차분 값들은 상이한 피크 지점을 가지고 있어 비교 지점을 결정하는 것이 쉽지 않으므로, 이를 극복하기 위해 다음과 같은 대푯값을 도입한다[8].

$$\Delta_j = \sum_{b=1}^{8} \sum_{n=1}^{N} |\Delta_{j,b}[n]| \tag{3}$$

여기서 N은 데이터 수집 단계에서 측정한 소비 전력 신호열의 길이를 의미한다.

차분 전력 분석 (DPA) 공격의 기본 개념에 따르면 정확한 비밀 키가 선택 함수의 입력으로 사용된다면, 전력 소모가 높은 신호는 '1' set으로 반대의 경우에는 '0' set으로 구분되어 저장될 것이다. 이 경우 두 set 차분 값 Δ_j는 DPA 피크라고 불리는 의미 있는 피크를 가지게 될 것이다[3,10]. 반면에 잘못된 추정 키가 입력으로 사용된다면 전력 신호는 각 set에 무작위하게 분포되므로, 각 set의 부분집합 평균이 비슷한 값을 가지게 되어 그 차분 값은 매우 작게 되어 의미 있는 피크가 나타나지 않을 것이다. 따라서 DPA 공격에서는 각 추정 키에 대한 차분 값들 중에서 가장 큰 DPA 피크를 검출함으로써 비밀 키를 찾을 수 있다.

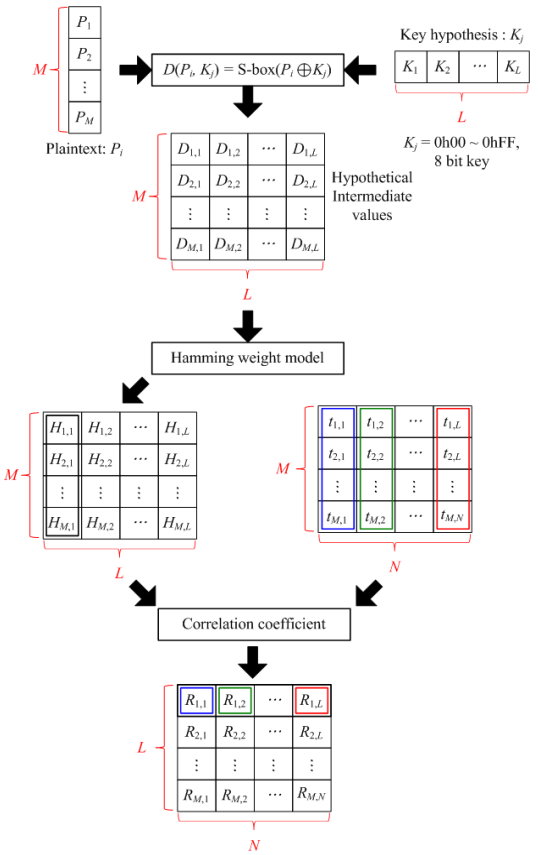

그림 3. Hamming weight 모델에 기반한 CPA 공격.

2.2 상관도 분석 (CPA) 공격

CPA 공격은 DPA 공격의 성능 향상을 위해 제안된 방법이므로 DPA 공격과 동일한 데이터 수집 방법을 사용하며, 자세한 공격 방법은 그림 3에 도시되어 있다. 데이터 분석 단계에서는 그림 3에서 보는 바와 같이 II-1절에서 설명한 분류함수 $D(P_i, K_j)$를 이용하여[10] S-box의 출력 bit를 얻고, 각 분류함수의 값을 Hamming weight 모델로 맵핑하여 소비 전력 모델을 만든다. 이 때, 분류함수의 출력에 포함된 '1'의 개수가 소비 전력을 나타낸다고 가정하고 $D(P_i, K_j)$에 대응하는 Hamming weight $H_{i,j}$를 계산한다. 모든 평문과 추정 키에 대한 $H_{i,j}$가 구해지면, 다음 식을 사용하여 $H_{i,j}$와 측정된 소비 전력 신호 간의 상관계수를 구한다.

$$R_{j,n} = \frac{\sum_{i=1}^{M}(H_{i,j}-\overline{H_j})\cdot(T_{i,n}-\overline{T_n})}{\sqrt{\sum_{i=1}^{M}(H_{i,j}-\overline{H_j})^2\cdot\sum_{i=1}^{M}(T_{i,n}-\overline{T_n})^2}} \quad (4)$$

여기서 $R_{j,n}$은 j번째 추정 키에 대한 Hamming weight와 n번째 소비 전력 샘플과의 상관계수를 의미한다. 그리고 $\overline{H_j}$와 $\overline{T_n}$는 각각 모든 평문에 대한 j번째 추정 키의 평균과 n번째 소비 전력 샘플의 평균을 의미한다. 열 벡터 (column vector) H_j와 T_n의 선형관계를 결정하기 위해 상관계수를 사용하는 이유는, 소비 전력 신호 $T_{i,n}$과 추정하는 소비 전력 모델 $H_{i,j}$가 모두 S-box의 출력, 즉 선택함수 $D_{i,j}$에 의존하기 때문이다. 만약 정확한 키가 선택함수의 입력으로 들어온다면 H_j와 T_n은 매우 높은 상관관계를 가질 것이고, 그렇지 않은 경우라면 두 열 벡터는 낮은 상관관계를 가지게 된다. 따라서 CPA 공격에서 정확한 키를 찾는 방법은 다음 식과 같이 가장 높은 상관계수 값을 가지는 추정 키를 선택하는 것이다.

$$K_j = \max_j(\max_n(R_{j,n})) \quad (5)$$

Ⅲ. 웨이블릿에 기반한 잡음 감소 방법

전력 분석 (PA) 공격의 성능은 정확한 키를 찾아내는 데 필요한 소비 전력 신호의 개수와 관계가 있으므로, 높은 공격 성능을 얻기 위해서는 원치 않는 왜곡이 제거된 순수한 전력 소비 신호를 획득하는 것이 필요하다. 그러나 잡음과 같은 왜곡 요소는 측정된 소비 전력 신호에 필연적으로 포함되므로, 이를 식으로 표현하면 다음과 같다.

$$t_{i,n} = s_i[n] + w_i[n],\ n = 1,2,..,N \quad (6)$$

여기서 $s_i[n]$과 $w_i[n]$은 각각 i번째 평문 입력 시 암호화 장치에서 발생되는 순수한 전력 신호와, 측정된 전력 신호에 포함된 왜곡요소를 나타낸다. 이 경우 우리는 다음과 같은 두 가지 가설을 고려해 볼 수 있다.

$$\begin{cases} H_1 : t_{i,n} = s_i[n] + w_i[n] \\ H_0 : t_{i,n} = w_i[n] \end{cases} \quad (7)$$

식 (7)은 전력 소비가 발생했을 때 측정된 신호에 암호화 장치에 의한 전력 소비 신호와 다른 잡음이 포함되어 있는 경우인 H_1과, 암호화 장치에 의한 전력 소비가 발생하지 않아 왜곡요소만이 존재하는 경우인 H_0를 식으로 나타내고 있다. 만약 그림 4에서 보는 바와 같이 두 가정에 대한 확률 $p_0(t)$와 $p_1(t)$를 알 수 있다면, 우리는 사후 최대 확률 (maximum a posteriori)

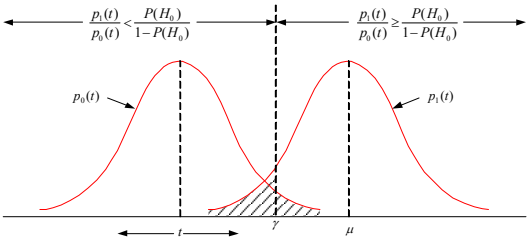

그림 4. MAP 우도함수를 이용한 가설 검증 방법.

을 이용해 최적화된 문턱 값 (threshold value) γ를 구해낸 다음 왜곡요소와 소비 전력 신호를 구분해 낼 수 있을 것이다[11]. 그러나 측정된 소비 전력 신호만을 이용해 $p_0(t)$와 $p_1(t)$를 알아낼 수 없으므로 잡음을 억제하기 위해서는 γ를 정해야 한다.

이를 위해 다양한 방법을 고려해 볼 수 있으나, 왜곡요소를 제거하는 과정에서 가능한 측정된 신호의 특성을 왜곡시키거나 제거시키지 않는 방법을 사용하는 것이 바람직하다. 만약 저대역 통과 필터 (lowpass filter)와 같은 방법을 사용하면 특정 주파수 대역 이상의 모든 정보가 제거되므로, 높은 주파수 대역에서 포함된 유용한 정보까지 같이 사라지게 된다. 이러한 난점을 극복하기 위해서는 신호와 왜곡요소를 분리하기 위해 지정된 대역을 더 정확하게 나눌 수 있는 방법이 요구되며, 이를 위해 현재 영상처리 등에서 널리 활용되고 있는 다중 해상도 분석 (multi-resolution analysis, MRA)을 기반으로 하는 웨이블릿 잡음 제거 (wavelet de-noising) 방법이 좋은 해결방안이 될 수 있다.

웨이블릿 잡음 제거 방법을 이용해 소비 전력 신호를 전처리한 후 PA 공격을 수행하는 제안된 방법은 그림 5에 도시되어 있다. 제안된 방법의 첫 번째 단계로 잡음이 있는 소비 전력 신호를 이산 웨이블릿 변환 (discrete wavelet transform, DWT)하는 것으로, 다음과 같은 디지털 필터를 이용해 수행된다[12].

$$f(n) = \sum_{k=-\infty}^{\infty} \sum_{l=-\infty}^{\infty} d(k,l) 2^{k/2} \Psi\left(\frac{n-2^k l}{2^k}\right) \quad (8)$$

여기서 2^k와 $2^k l$은 각각 MRA를 가능하게 하는 팽창 (dilation)과 이동 (translation) 매개 변수이다[13]. MRA란 그림 6에서 보는 바와 같이 입력신호를 저대역 통과 필터 $h[n]$과 고대역 통과 필터(high-pass filter) $g[n]$에 통과시켜 다운 샘플링 (down- sampling)한 후 근사성분 (approximation)과 세부성분 (detail)으로 나누는 과정이다. 이 과정은 우리가 원하는 주파수 대역을 얻을 때까지 반복된다. 입력신호를 웨이블

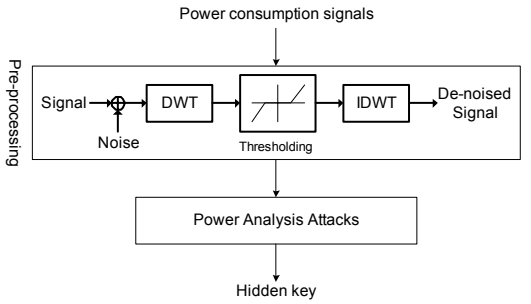

그림 5. 제안된 웨이블릿 잡음 제거 방법을 이용한 전력 분석 공격 방법.

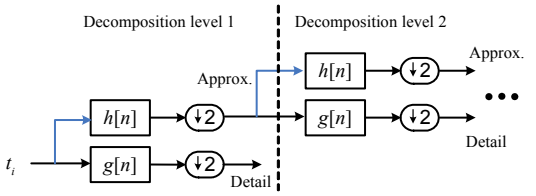

그림 6. 웨이블릿 분해의 블록 다이어그램.

릿 분해한 후에는 왜곡요소를 제거하기 위한 과정을 수행하게 되는데, 이 때 문턱 값 γ가 필요하며 다음과 같이 계산된다[14].

$$\gamma_d = \sqrt{2 \ln N_d} \cdot \sigma_d \quad (9)$$

여기서 d는 분해 수준 (decomposition level)을 의미하며, N_d, σ_d와 γ_d는 각각 d에 해당하는 신호의 길이와 분산 값, 그리고 문턱 값을 의미한다. 식 (9)에서 γ_d는 d에 의해 결정되는 값이므로, 어떻게 d를 선택할 것인지 신중하게 고려해야 한다.

d를 선택하는 방법을 결정하기 위해 우선 입력신호가 그림 7과 같이 보안 장치의 내부 클럭 (internal clock) c_1과 c_1의 고조파로 구성되어 있다고 가정하자. 암호화는 매 클럭마다 수행되므로, 전력 소비에 의해 발생하는 높은 피크가 측정된 신호에 나타나게 될 것이다. 그러나 측정된 신호에는 c_1에 의한 성분뿐만 아

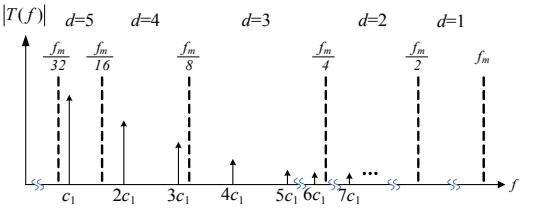

그림 7. 입력 신호 특성의 예.

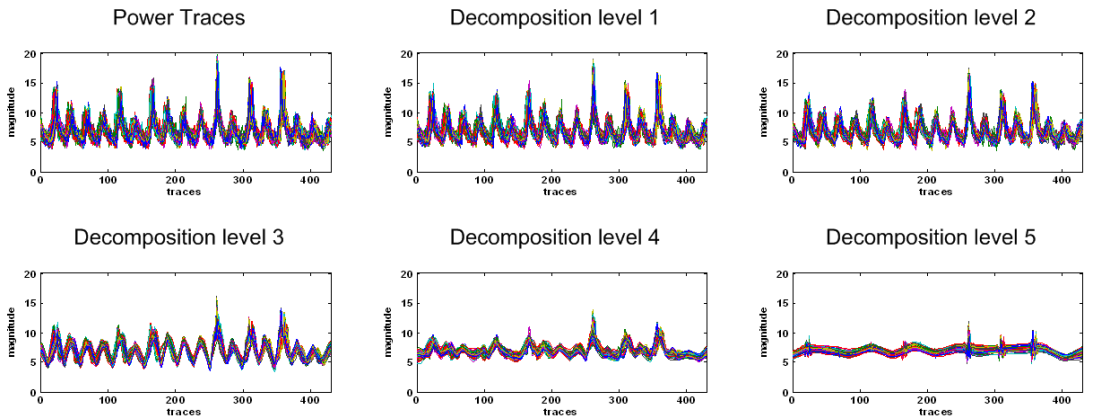

그림 8. 기본 전력 신호와 각 분해 레벨에 따라 재구성된 신호.

니라 고조파에 의한 영향도 함께 나타나게 되므로, 측정된 신호의 피크는 왜곡된다. DPA 공격과 같이 피크 정보가 중요한 경우에는 피크의 왜곡을 최대한 방지하여야 하므로, 고조파의 영향을 배제하기 위해서는 d=4를 선택하는 것이 타당하다. 그러나 그림 8에서 보듯이 큰 피크들을 제외하고는 많은 정보들이 유실되므로, 소비 전력 모델과 상관계수를 구하는 CPA 공격에는 d=4가 적합하지 않을 것임을 예상할 수 있다. 따라서 CPA 공격의 경우에는 소비 전력 파형을 왜곡시키지 않도록 낮은 수준의 d를 선택하는 것이 좋다. d가 결정되면, 문턱 값 γ_d가 결정되므로 이를 이용해 다음과 같이 입력신호에서 잡음을 제거한다.

$$T_d[f] = \begin{cases} T[f] - \gamma_d, & T[f] > \gamma_d \\ 0, & T[f] < \gamma_d \end{cases} \quad (10)$$

제안된 시스템의 마지막 단계는 복원이다. 복원을 위해서 역 이산 웨이블릿 변환 (inverse DWT) 과정이 수행되며, 완벽한 복원을 위해 복원 필터 (reconstruction filters)로 $h[n]$과 $g[n]$의 직교 미러 여파기 (quadrature mirror filter)를 사용한다[12]. 제안된 왜곡요소 제거 과정을 통해 고조파와 잡음과 같은 오류 요소들을 억제할 수 있으므로, 전처리 블럭의 출력 신호는 원래 입력 신호보다 높은 순도를 가질 것이다. 이러한 순도의 증가는 전력 분석 (PA) 공격 시 더 적은 수의 전력 신호로 비밀 키를 찾아낼 수 있도록 해준다.

Ⅳ. 실험결과 및 분석

웨이블릿 잡음 제거에 기반한 제안된 전처리 방법의 성능을 확인하기 위해, AES 암호화 알고리즘이 1 round 동작할 때 "mote IV"라는 무선센서 네트워크 장치의 전력 소비를 측정하였다[9]. 실험에 사용된 타겟 디바이스와 측정 장비는 그림 9, 10과 같고, 총 4천 개의 전력 신호를 측정하였다. 차분 전력 분석

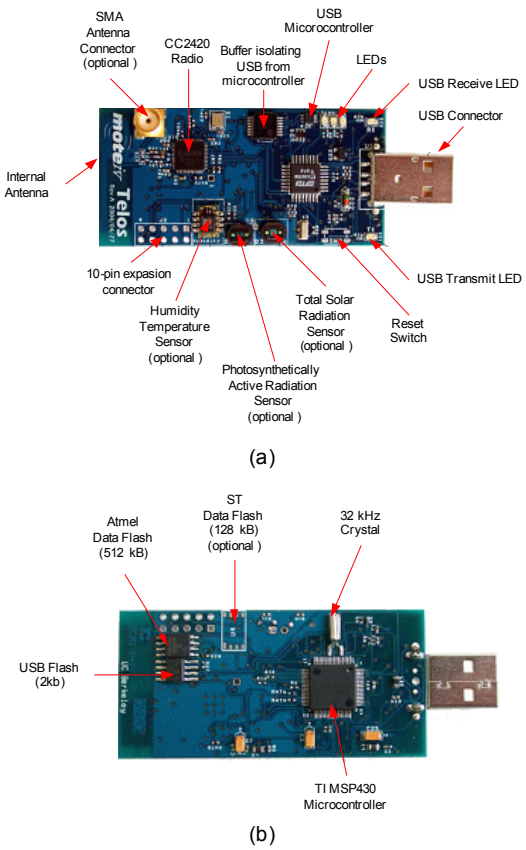

그림 9. 타겟 디바이스인 "mote IV": (a) 전면, (b) 후면.

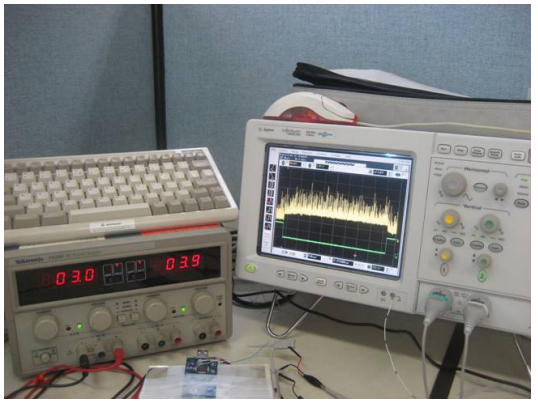

그림 10. 무선 센스 네트워크 장치 "mote IV", 전력공급기, 오실로스코프를 갖춘 실험환경.

(DPA) 공격 및 상관도 분석 (CPA) 공격은 16개의 S-box에 대해 각각 수행되었다. 타겟 디바이스의 내부 클럭과 측정 장치의 샘플링 주파수 (sampling frequency)는 각각 8 MHz와 200 MHz였다. 왜곡 요소 제거를 위해 모 웨이블릿 (mother wavelet)으로 Haar, Symlet, 그리고 Daubechies를 사용하여 전력 분석 (PA) 공격의 성능을 평가하였다[16]-[18]. 공격의 성능은 4천 개의 전력 신호 내에서 비밀 키를 찾아내는 데 요구되는 최소 신호의 수를 기준으로 평가하였으며, 4천 개의 전력 신호 내에서 비밀 키를 찾지 못할 경우 공격 실패로 간주하고 'Fail'이라고 표시하였다.

Ⅲ절에서 언급한 분해 수준 d 값의 결정에 대한 타당성과 제안된 전처리 방법의 성능을 입증하기 위해, 우선 측정된 파형을 이용하여 기존 DPA와 CPA의 성능을 평가하였으며, 그 결과는 표 1과 2에 제시하였다. 표 1과 2에서 보듯이 DPA의 경우 대부분 공격에 실패하며, CPA의 경우에도 상당히 많은 수의 신호를 요구하는 것을 볼 수 있는데 이는 저전력 칩을 사용하는 타겟 디바이스의 특성상 측정된 신호의 품질이 양호하지 못하기 때문이다. 그럼에도 불구하고 CPA 공격이 가능한 것은 DPA에 사용되는 평균과는 달리 상관도 분석에 사용되는 연산이 왜곡요소에 보다 강인하기 때문이다.

다음으로 제안된 방법을 사용한 전력 분석 공격의 성능을 평가하기 위해, 6차 Symlet 웨이블릿을 이용하여 제안된 전처리방법을 수행한 후 DPA 공격을 시도하였다. 전처리를 위해서는 분해 수준 d를 선택해야 하는데, 실험조건에서 입력 신호의 내부 클럭과 최고 주파수가 각각 8 MHz와 200 MHz로 주어졌으므로 Ⅲ절에서 설명한 바와 같이 고조파와 잡음을 제거할 수 있도록 d를 4로 결정하였다. 분해 수준 d에 따른

표 1. 기존 DPA 공격에 요구되는 최소 신호 개수

Key No.	# of traces	Key No.	# of traces
1	3,997	9	3,841
2	3,420	10	Fail
3	3,805	11	Fail
4	3,921	12	Fail
5	3,999	13	1,547
6	Fail	14	Fail
7	2,850	15	Fail
8	3,130	16	1,400

표 2. 기존 CPA 공격에 요구되는 최소 신호 개수

Key No.	# of traces	Key No.	# of traces
1	402	9	437
2	157	10	934
3	122	11	1021
4	1292	12	3701
5	1156	13	1095
6	1461	14	1495
7	1763	15	3083
8	1493	16	1470

표 3. d에 따른 DPA 공격의 최소 요구 신호 개수

Key No.	Level 1	Level 2	Level 3	Level 4	Level 5
1	Fail	Fail	3,634	1,665	3,360
2	3,419	3,194	2,904	1,973	2,102
3	3,772	3,612	2,462	1,645	1,935
4	2,612	2,701	2,553	1,518	3,680
5	Fail	Fail	Fail	1,606	Fail
6	Fail	Fail	3,562	1,227	Fail
7	2,784	2,742	2,676	2,159	Fail
8	2,897	2,819	2,408	2,106	3,199
9	Fail	Fail	Fail	2,541	3,871
10	Fail	Fail	3,678	923	1,415
11	Fail	Fail	Fail	2,930	3,788
12	Fail	Fail	3,867	1,101	2,375
13	1,531	1,522	1,443	842	1,382
14	Fail	Fail	Fail	1,553	1,585
15	Fail	Fail	Fail	1,250	1,871
16	1,430	1,429	1,260	1,009	1,529

결과는 표 3에 제시되어 있으며, d=4인 경우를 제외하고 모두 공격에 실패하는 것을 볼 수 있다. d가 1, 2, 3인 경우에는 고조파 성분이 충분히 제거되지 않았기 때문에 공격에 실패하는 경우가 많이 발생하게 되고, d가 5인 경우에는 내부 클럭에 의해 발생하는 신호까지 억압하기 때문에 오히려 성능이 열화 됨을 볼 수 있다. 이러한 현상은 그림 8에서도 관찰할 수 있는데, d=1, 2, 3인 경우에는 원 신호 파형과 유사함을 관찰할 수 있으나, d=4인 경우에는 의미 있는 피크를 제

표 4. Symlet 웨이블릿 사용 시 차수 별로 요구되는 최소 신호의 개수

Key No.	Symlet 4	Symlet 6	Symlet 8
1	2,099	1,665	1,648
2	1,419	1,973	1,859
3	1,717	1,645	2,075
4	1,520	1,518	1,428
5	1,762	1,606	2,648
6	1,331	1,227	1,332
7	1,909	2,159	2,158
8	2,018	2,106	1,799
9	2,518	2,541	2,584
10	1,036	923	923
11	2,814	2,930	2,814
12	1,101	1,101	1,222
13	845	842	833
14	1,541	1,553	1,553
15	1,249	1,250	1,290
16	1,121	1,009	1,096

표 5. Daubechies 웨이블릿 사용 시 차수 별로 요구되는 최소 신호의 개수

Key No.	Daubechies 4	Daubechies 6	Daubechies 8
1	1,713	1,821	1,812
2	1,421	1,338	1,340
3	1,592	1,437	1,584
4	1,430	1,107	1,413
5	1,797	2,279	2,394
6	3,258	1,227	1,246
7	2,281	1,875	1,871
8	2,662	2,626	2,654
9	2,683	2,574	1,953
10	930	901	913
11	2,988	3,264	3,193
12	1,222	1,107	1,423
13	839	842	959
14	1,551	1,551	1,551
15	1,708	1,556	1,512
16	1,120	1,263	968

외하고 작은 피크들은 대부분 억압된 것을 볼 수 있다. 그리고 d=5인 경우에는 대부분의 신호를 억압하여 신호가 심하게 뭉개지는 것을 볼 수 있다.

그러나 이 결과는 6차 Symlet 웨이블릿을 이용한 결과에 국한되므로, 제안된 방법의 강인성을 보이기 위해 Daubechies 웨이블릿을 추가로 채택하고 차수를 변경하면서 모의실험을 수행하였으며 그 결과를 표 4와 5에 정리하였다. 이 때 모의실험에 사용된 d는 4였다. 웨이블릿 차수가 커지면 필터 특성이 달라져 복잡한 신호를 좀 더 정확하게 표현할 수 있는 장점이 있으나[19], 필터를 통과하는 신호도 번하게 되므로 문턱

표 6. Haar 웨이블릿 사용 시 d에 따른 기존 잡음 감소 방법의 성능

Key No.	Level 1	Level 2	Level 3	Level 4	Level 5
1	Fail	Fail	Fail	2,352	2,886
2	3,418	3,290	2,136	1,338	2,101
3	3,809	3,585	2,386	1,574	2,282
4	2,731	2,612	2,254	1,548	3,594
5	Fail	3,995	3,995	2,376	Fail
6	Fail	Fail	1,364	3,754	Fail
7	2,784	2,680	2,342	2,329	3,691
8	3,119	2,402	2,485	3,134	3,547
9	3,842	Fail	2,998	Fail	Fail
10	Fail	Fail	3,455	1,424	1,705
11	Fail	Fail	Fail	3,055	3,946
12	Fail	Fail	Fail	2,306	2,375
13	1,547	1,531	870	811	1,459
14	Fail	Fail	Fail	2,843	3,379
15	Fail	Fail	1,571	1,567	3,221
16	1,399	1,373	1,282	1,296	1,413

표 7. Haar 웨이블릿 사용 시 d에 따른 제안된 잡음 감소 방법의 성능

Key No.	Level 1	Level 2	Level 3	Level 4	Level 5
1	Fail	Fail	Fail	2,369	2,884
2	3,417	3,293	2,133	1,850	2,100
3	3,809	3,586	2,384	1,471	2,190
4	2,731	2,612	2,254	1,548	1,807
5	Fail	3,995	3,559	2,274	Fail
6	Fail	Fail	1,347	3,954	Fail
7	2,784	2,680	2,341	2,322	3,950
8	3,118	2,404	2,485	2,662	3,434
9	3,842	Fail	2,995	3,297	Fail
10	Fail	Fail	3,484	1,416	1,705
11	Fail	Fail	Fail	2,997	Fail
12	Fail	Fail	Fail	2,300	2,375
13	1,547	1,531	860	805	1,407
14	Fail	Fail	Fail	2,857	3,383
15	Fail	Fail	1,571	1,571	3,270
16	1,399	1,373	1,282	1,282	1,455

값 역시 바뀌게 된다. 문턱 값이 변경되면 최종적으로 획득되는 신호도 바뀌게 되므로 공격 성능 역시 영향을 받게 되나, 표 4와 5에서 보듯이 평균적인 공격 성능은 웨이블릿의 종류와 차수에 크게 영향을 받지 않음을 알 수 있다.

표 1을 보면 16개의 S-box 중 6개에서는 4천 개의 신호를 사용했음에도 공격에 실패하는 것을 볼 수 있으며, 나머지 7개의 경우에도 대부분 4천 개의 신호에 근접한 결과를 보이고 있어 결과의 신뢰도가 크게 떨어진다. 반면에 제안된 전처리 기법을 사용한 경우 편차는 있으나 공격에 필요한 최소 신호의 개수가 평균

표 8. 6차 Daubechies 웨이블릿 사용 시 d에 따른 기존 잡음 감소 방법의 성능

Key No.	Level 1	Level 2	Level 3	Level 4	Level 5
1	Fail	Fail	3,571	1,831	2,470
2	3,422	3,642	3,420	1,407	2,100
3	3,772	3,616	3,585	1,447	1,965
4	2,731	2,697	2,590	1,095	3,683
5	Fail	3,995	Fail	2,376	2,843
6	Fail	Fail	Fail	1,238	Fail
7	2,784	2,784	2,411	1,929	3,765
8	2,878	2,830	2,190	2,919	3,252
9	Fail	Fail	Fail	2,574	3,871
10	Fail	Fail	Fail	912	923
11	Fail	Fail	Fail	3,272	3,836
12	Fail	Fail	3,819	1,411	2,053
13	1,531	1,522	1,531	839	1,461
14	Fail	Fail	Fail	1,552	1,606
15	Fail	Fail	3,928	1,565	1,517
16	1,432	1,400	1,278	1,270	1,523

표 9. 6차 Daubechies 웨이블릿 사용 시 d에 따른 제안된 잡음 감소 방법의 성능

Key No.	Level 1	Level 2	Level 3	Level 4	Level 5
1	Fail	Fail	3,565	1,821	2,470
2	3,419	3,422	3,418	1,338	2,100
3	3,772	3,616	3,586	1,437	1,935
4	2,612	2,603	2,580	1,107	3,693
5	Fail	3,995	Fail	2,279	3,072
6	Fail	Fail	Fail	1,227	Fail
7	2,784	2,747	2,411	1,875	3,716
8	2,880	2,830	2,192	2,626	3,197
9	Fail	Fail	Fail	2,574	3,957
10	Fail	Fail	Fail	901	923
11	Fail	Fail	Fail	3,264	3,824
12	Fail	Fail	3,789	1,107	2,053
13	1,531	1,522	1,531	842	1,459
14	Fail	Fail	Fail	1,551	1,605
15	Fail	Fail	3,929	1,556	2,364
16	1,431	1,416	1,282	1,263	1,523

1,600개 정도로 크게 감소했음을 볼 수 있다. 그림 11과 12는 각각 기존 DPA 공격과 제안된 전처리 방법(6차 Symlet, d=4)을 이용해 DPA 공격에 대한 16번째 S-box의 차분 곡선 (difference curves, Δ_j)이다. 그림에서 빨간 세로선은 정확한 키 (0h0F)를 나타내는 차분 값이 가장 커진 시점을 의미하며, 그림 11에 제시된 기존 DPA 결과와 비교할 때 그림 12에 제시된 제안된 방법을 적용해 얻은 결과가 다른 키들에 비해 높은 차분 값을 유지하는 것을 볼 수 있다. 이상의 결과들을 볼 때 제안된 방법은 명백하게 기존 DPA 공격의 성능을 향상시킨다고 볼 수 있다.

표 10. 6차 Symlet 웨이블릿 사용 시 d에 따른 기존 잡음 감소 방법의 성능

Key No.	Level 1	Level 2	Level 3	Level 4	Level 5
1	Fail	Fail	3,642	1,831	2,385
2	3,419	3,378	2,953	1,412	2,100
3	3,773	3,590	2,463	1,466	1,980
4	2,731	2,743	2,586	1,109	3,649
5	Fail	Fail	Fail	2,380	2,846
6	Fail	Fail	3,552	1,238	Fail
7	2,784	2,747	2,680	1,929	Fail
8	2,897	2,815	2,404	3,055	3,330
9	Fail	Fail	Fail	2,574	3,870
10	Fail	Fail	3,657	914	1,124
11	Fail	Fail	Fail	3,495	3,839
12	Fail	Fail	3,861	1,232	2,375
13	1,531	1,522	1,444	798	1,429
14	Fail	Fail	Fail	1,552	1,543
15	Fail	Fail	3,931	1,704	1,783
16	1,431	1,429	1,271	1,275	1,529

본 논문에서 제안된 방법과 기존에 제안된 잡음 감소 방법의 성능을 비교하기 위해[7], Haar 웨이블릿을 이용하여 시뮬레이션을 수행한 결과는 표 6과 7에 제시되어 있다. 기존 방법과 제안된 방법 모두 level 4에서 가장 높은 성능을 보이나, 기존의 방법의 경우 주어진 4천개 이내에서 공격에 성공하지 못함을 볼 수 있다. Daubechies와 Symlet 웨이블릿을 이용한 결과는 표 8부터 10과 표 3에 제시되어 있으며, 제안된 방법의 경우 기존 방법에 비해 공격 성공을 위해 요구되는 최소 요구 신호의 수가 평균적으로 각각 50, 100 정도 낮음을 확인할 수 있다. 따라서 본 논문에서 사용한 환경에서는 제안된 방법이 기존 MRA를 이용한 잡음 감소 방법보다 조금 더 나은 성능을 가짐을 알 수 있다.

다음으로 제안된 방법이 CPA 공격에서 효과가 있는지 살펴보기 위해 6차 Symlet 웨이블릿을 사용하고 d를 1에서 5까지 변경시키면서 모의실험을 수행하였다. 수행한 모의실험의 결과는 표 6에 나타나 있으며, DPA 공격과는 달리 d가 2일 때 기존 CPA에 비해 비교적 나은 성능을 보임을 확인할 수 있다. d가 2일 때 성능이 향상되는 원인은 고조파 성분을 제거해 피크 값만을 보존하는 DPA 공격과는 달리, 고조파 성분을 모두 제거하면 소비 전력 추정 모델과 높은 상관도를 유지할 수 없기 때문이다. 즉, 에너지 밀도가 낮은 고주파 대역 성분만을 제거하면 크기가 매우 작은 고조파 성분과 잡음 성분이 제거되므로 소비 전력 추정 모델과 상관도가 크게 감소하지는 않으나, d가 커지면 제거되는 신호의 양도 증가하므로 오히려 추정모델과

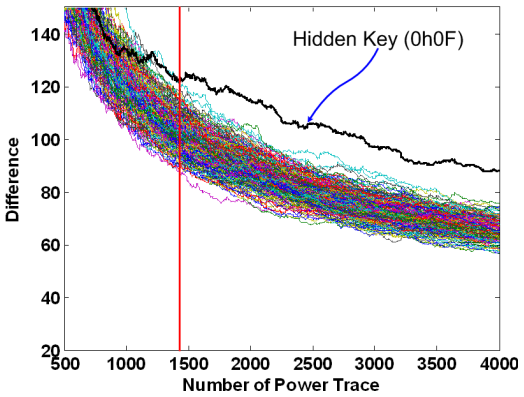

그림 11. 기존 DPA 공격의 차분 곡선.

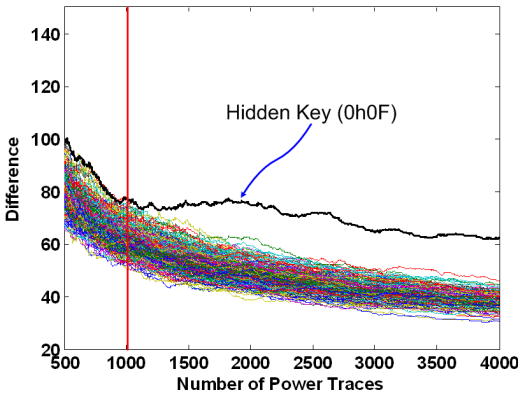

그림 12. 제안된 전처리 기법을 적용한 DPA 공격의 차분 곡선 (Symlet 6, d=4).

의 상관도를 하락시키기 때문이다. 따라서 CPA 공격의 경우는 고주파 대역에 존재하는 잡음의 에너지를 추정하여 신호에서 제거해야 공격 성능을 향상시킬 수 있다.

V. 결 론

전력 분석 (PA) 공격의 효율성을 높이기 위해서 본 논문에서는 웨이블릿 잡음 제거를 기반으로 하는 전처리 방법을 제안했다. 제안된 전처리 방법은 잡음뿐만 아니라 장치의 비선형성에 의해 발생하는 고조파 성분과 같은 오류 요소를 줄일 수 있고, 공격 성공에 요구되는 전력 신호의 수를 감소시킬 수 있었다. 이러한 결과는 잡음이 많이 포함되거나, 저전력 환경에서 측정된 소비 전력 신호에 대해서도 보다 효율적인 공격이 가능하게 되었음을 의미하므로, PA 공격의 범위를 다양한 타겟 디바이스로 확장시키는 데 기여할 수 있을 것으로 기대된다. 그리고 제안된 전처리 방법은 PA 공격과 독립적으로 작동할 수 있으므로, 주파수영역 차분 전력 분석 (DPA)[15]과 같은 다른 공격 방법에서도 활용될 수 있을 것으로 기대된다.

참 고 문 헌

〔1〕 P. Kocher, “Timing Attack on Implementation of Diffe-Hellman, RSA, DSS and other Systems”, *Advances in Cryptology - Crypto’96*, LNCS 1109, NewYork1996.

〔2〕 P. Kocher, J. Jaffe, and B. Jun, “Introduction to differential power analysis and related attacks,” 1998, White Paper, Cryptography Research.

〔3〕 P. Kocher, J. Jaffe and B. Jun, “Differential Power Analysis,” in *proceedings of CRYPTO 1999*, LNCS 1666, pp.388-397, Springer-Verlag, 1999.

〔4〕 E. Brier, C. Clavier, and F. Olivier, “Correlation power analysis with a leakage model,” in *Proceedings of CHES 2004*, LNCS 3156, pp. 16-29, 2004.

〔5〕 K. Gandolfi, C. Mourtel, and F. Oliver, “Electromagnetic Attacks: Concrete Results,” in *Proceedings of CHES 2001*.

〔6〕 J.J. Quisquater and D. Samyde, “Electromagnetic Analysis (EMA): Measures and Countermeasures for Smart Cards,” in *Proceedings of e-Smart 2001*.

〔7〕 류정춘, 한동국, 김성경, 김희석, 김태현, 이상진, “웨이블릿 기반의 차분전력분석 기법 제안,” *정보보호학회 논문지*, 제19권, 제3호, pp.27-35, 2009년 06월.

〔8〕 R. Bevan, E. Knudsen “Ways to Enhance Differential Power Analysis,” in *proceedings of ICISC 2002*, LNCS 2587, pp.327-342, Springer-Verlag, 2003.

〔9〕 Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, 2001.

〔10〕 T. S. Messerges, E. A. Dabbish and R. H. Sloan, “Examining Smart-Card Security under the Threat of Power Analysis Attacks,” *IEEE Trans. on Computers*, Vol.51, No.5, pp.541-

552, May 2002.
〔11〕 S. M. Kay, Fundamentals of Statistical Signal Processing Estimation Theory Vol.1, pp.351-359, Prentice Hall Inc., 1993.
〔12〕 I. Daubechies, "Where do wavelets come from? – A personal point of view," in *Proc. of the IEEE*, Vol.84, No.4, April, 1996.
〔13〕 S. Mallat, "A Theory for Multiresolution Signal Decomposition: The Wavelet Representation," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 11(7):674-693, 1989.
〔14〕 D. L. Donoho, I.M. Johnstone, G. Kerkyacharian, and D. Picardi, "Wavelet Shrinkage: Asymptopia?" *Journal of the Royal Statistical Society*, B, Vol.57, pp.301-369, 1995
〔15〕 C. Gebotys, S. Ho. And C.C. Tiu, "EM Analysis of Rijndael and ECC on a Wireless Java-Based PDA," in *Proceedings of CHES 2005*, LNCS 3659, pp.350-264, Springer-Verlag, 2005.
〔16〕 R. M. Rao, and A. S. Bopardikar, Wavelet Transforms Introduction to Theory and Applications, pp.41-46, Addison-Wesley Longman, Inc., 1998.
〔17〕 I. Daubechies, Ten Lectures on Wavelets, CBMS-NSF Regional Conf. Ser. in *Appl. Math.*, Vol.61, SIAM, Philadelphia, 1992.
〔18〕 I. Daubechies, "Orthonormal bases of compactly supported wavelets," *Conirnun. Purr Appl. Math.*, Vol.41, pp.909-996. Nov. 1988.
〔19〕 S. Mallat, A Wavelet Tour of Signal Processing 2nd Ed., pp.241-254. Academic Press, 1998.

김 완 진 (Wan-Jin Kim) 정회원

2005년 2월 부산대학교 전자전기통신공학부 공학사
2007년 2월 부산대학교 전자공학과 공학석사
2007년 3월~현재 부산대학교 전자공학과 박사과정
<관심분야> 적응신호처리, 디지털 통신, RFID, OFDM, SCA, 레이더 및 소나 신호처리

송 경 원 (Kyoung-Won Song) 정회원

2008년 2월 부산대학교 전자전기통신공학부 공학사
2010년 2월 부산대학교 전자공학과 공학석사
2010년 3월~현재 SK C&C 금융사업본부
<관심분야> 부채널 공격, 적응신호처리, 디지털 통신

이 유 리 (Yu-Ri Lee) 준회원

2010년 2월부산대학교 전자전기통신공학부 공학사
2010년 3월~현재 부산대학교 전자공학과 공학석사과정
<관심분야> 부채널 공격, 디지털 방송신호처리

김 호 원 (Ho Won Kim) 종신회원

1993년 2월경북대학교 전자공학과
1995년 2월 포항공과대학교 전자전기공학과 석사
1999년 2월 포항공과대학교 전자전기공학과 박사
2003년 7월~2004년 6월 : 독일 Ruhr University Bochum Post Doctorial
1998년 12월~2008년 2월 한국전자통신연구원 정보보호연구본부 팀장/선임연구원
2008년 3월~현재 부산대학교 정보컴퓨터공학부 조교수
<관심분야> 센서네트워크 보안, RFID 보안, 프라이버시 보호, 공개키 암호, 저전력 기술, 스마트 그리드 보안

김 형 남 (Hyoung-Nam Kim) 종신회원

1993년 2월 포항공과대학교 전자전기공학과 공학사
1995년 2월 포항공과대학교 전자전기공학과 공학석사
2000년 2월 포항공과대학교 전자전기공학과 공학박사
2000년 4월 포항공과대학교 전자컴퓨터공학부 박사후 연구원
2003년 3월 한국전자통신연구원 무선방송연구소 선임연구원
2007년 2월 부산대학교 전자공학과 조교수
2007년 3월~현재 부산대학교 전자공학과 부교수
<관심분야> 적응신호처리, 레이더 신호처리, 디지털 방송신호처리, BCI