DOI: 10.3745/KIPSTC.2011.18C.1.007

전력분석 공격에서 랜덤클럭 전력신호에 대한 일정피치 기반의 시간적 정렬 방법

박 영 구[†] · 이 훈 재[††] · 문 상 재[†††]

요 약

전력분석공격은 스마트카드와 같은 저전력 보안장치에 대한 매우 강력한 공격방법이나, 측정된 전력신호와 암호알고리듬 실행 시 추정되는 중간 값과의 상관도를 연산하는 시점이 시간적으로 일치되어야 가능하다. 보안장치에 랜덤클럭을 적용하면 측정된 전력신호 분석 시점이 서로 일치하지 않게 되므로 랜덤클럭이 전력분석 공격에 대한 방어대책으로 사용된다.

본 논문에서는 전력분석공격에서 랜덤클럭 전력신호에 대한 일정피치 기반의 시간적 정렬 방법을 제안한다. 제안방법은 랜덤클럭이 적용된 보안 장치로부터 측정된 전력신호를 일정한 크기를 갖는 기준피치에 맞추어 시간 축 상의 위치와 크기를 정렬하므로 랜덤 클럭 방어대책을 공격할 수 있는 새로운 방법이다. 마지막으로, 랜덤클럭이 적용된 스마트카드 환경에서 실행된 AES 블럭 암호화 알고리듬에 대하여 제안된 방법을 적용하여 그 공격 가능성을 검토한다.

키워드 : 전력분석, 시간 정렬, 일정 피치, 제로통과율, 보간법, 랜덤클럭

A Constant Pitch Based Time Alignment for Power Analysis with Random Clock Power Trace

YoungGoo Park[†] · HoonJae Lee[††] · SangJae Moon[†††]

ABSTRACT

Power analysis attack on low-power consumed security devices such as smart cards is very powerful, but it is required that the correlation between the measured power signal and the mid-term estimated signal should be consistent in a time instant while running encryption algorithm. The power signals measured from the security device applying the random clock do not match the timing point of analysis, therefore random clock is used as counter measures against power analysis attacks.

This paper propose a new constant pitch based time alignment for power analysis with random clock power trace. The proposed method neutralize the effects of random clock used to counter measure by aligning the irregular power signals with the time location and size using the constant pitch. Finally, we apply the proposed one to AES algorithm within randomly clocked environments to evaluate our method.

Keywords : Power Analysis, Time Alignment, Constant Pitch, Zero-Crossing Rate, Interpolation and Decimation, Random Clock

1. 서 론

P. Kocher 등[1]에 의해 제안된 전력 분석 공격은 보안장치로 부터 비밀 키를 추출할 수 있는 매우 강력한 방법이다. 보안장치가 암호알고리듬 실행 시 소모하는 전력은 보안장치 내에서 실행되는 암호 알고리듬 연산의 중간 추정 값과 높은 상관도를 가진다. 비밀 키에 따라서 암호알고리듬의 중간 값을 추정하고, 추정된 중간 값의 해밍 값과 측정된 전력신호의 상관도를 계산하면, 올바른 키 추정에 대해서는

※ 본 연구는 2010년도 한국연구재단 과제 지원에 의한 결과로 수행되었음.
† 정 회 원 : 예스테크 연구개발 이사
†† 정 회 원 : 동서대학교 컴퓨터정보공학부 부교수
††† 정 회 원 : 경북대학교 전자전기컴퓨터공학부 교수
논문접수 : 2010년 10월 28일
수 정 일 : 1차 2010년 12월 15일
심사완료 : 2010년 12월 16일

높은 상관도를 가지고, 틀린 추정 비밀 키에 대해서는 낮은 상관도를 갖게 된다.

전력분석공격 시 측정된 전력신호와 중간 값을 추정하는 시점이 이 시간적으로 일치하도록 전력신호들을 정렬할 필요가 있다. 일정 클럭을 적용한 보안장치로 부터 측정된 전력신호가 시간적으로 정렬되지 않으면, 전력신호를 시간적으로 이동하면서 상관도가 최대가 되는 시점을 선택하여 전력신호를 정렬한 후 전력분석 공격을 한다.

한편, 전력분석공격의 방어대책 중의 하나로 보안장치에 랜덤클럭을 사용하고, 알고리듬 실행 시 랜덤 지연시간을 삽입하여 측정된 전력신호들 사이에 시간적으로 불일치가 일어나도록 하여 전력분석 공격을 어렵게 한다[2,3]. Park 등[4]이 랜덤클럭이 적용된 보안장치로 부터 측정된 전력신호들 중에서 임의로 기준 전력신호를 선택하고, 기준 전력신호의 시간적 변화에 맞추어 전력신호들을 시간적으로 이동하면서 보간법을 적용하여 상관도가 최대가 되도록 정렬한 후 차분전력분석으로 공격하였으나, 정렬한 한 전력신호 내에서는 여전히 시간적으로 랜덤클럭에 의한 성질을 가지고 있어, 전력신호 간에 동기를 잘 맞추어 정렬하여야 전력분석 공격이 가능하다.

본 논문에서는 제로통과율로 전력신호의 기준 피치를 결정하고, 전력신호를 기준피치에 맞추어 보간법으로 정렬하므로, 시간 축 상의 위치와 크기를 정렬 할 뿐 아니라, 피치도 일정하게 정렬하여 방어대책으로 사용된 랜덤클럭에 의한 영향을 무력화 시키는 개선된 정렬 방법을 제안하고자한다.

랜덤클럭이 적용된 스마트카드에 AES 블럭 암호화 알고리듬을 실행하여 전력신호를 측정하고 제안된 방법으로 정렬한 후 정렬된 전력신호간의 상관계수 추정 값을 계산하여 정렬한 정도를 측정하였고, 정렬한 전력신호와 암호알고리듬의 추정 중간 값과의 상관계수 추정치를 구하여 실제로 공격하고자 한다.

본 논문의 구성은 2장에서 정렬되지 않은 전력신호와 랜덤클럭이 적용된 전력신호에 대한 기존의 정렬 방식을 간단히 살펴보고, 3장에서는 제안된 랜덤클럭 전력신호의 정렬방식에 대해서 설명하며, 4장에서는 랜덤클럭이 적용된 전력신호에 대하여 제안된 정렬 방식을 적용하여 정렬하고, 정렬한 정도와 공격 결과를 보여주고, 5장에서 결론을 맺는다.

2. 관련 연구

전력분석에 의한 공격은 측정된 전력신호와 추정된 중간 값의 계산시점이 시간적으로 일치 되어야 가능하므로, 시간적으로 불일치한 전력신호의 정렬 방법에 대해서 알아본다.

2.1 상관계수를 이용한 정렬 방법

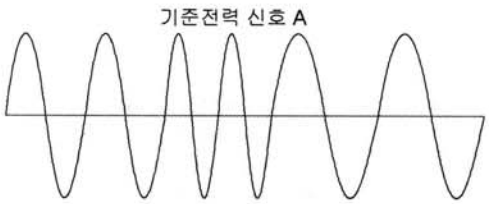
보안장치에 일정 클럭이 적용되었으나 추정된 중간 값과 측정된 전력신호와 비교 시점이 불일치하면 기준 전력신호를 선택하고 전력신호를 시간적으로 이동시켜 가면서 상관계수를 구하여, 상관계수가 최대가 되는 위치로 정렬한다. 식(1)은 기준신호(X)와 전력신호(Y)간의 상관계수를 구한다.

$$\rho(X,Y)=\frac{E(XY)-E(X)E(Y)}{\sqrt{Var(X)Var(Y)}} \quad (1)$$

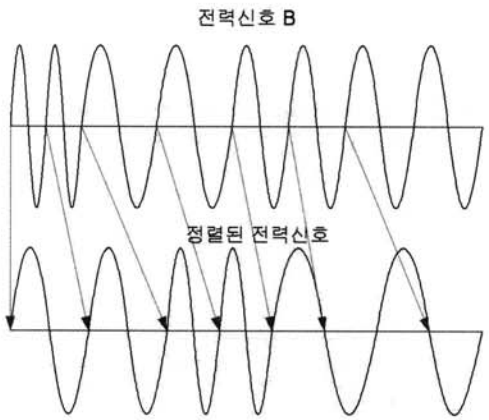
여기서 $\rho(X,Y)$는 X와 Y의 상관 계수이고, $E(\cdot)$는 평균값을, $Var(\cdot)$은 표준 편차를 나타낸다.

2.2 기준 전력신호를 이용한 정렬방법[4]

Park 등[4]은 랜덤클럭이 적용된 보호 장치를 공격하기 위하여 기준 전력신호를 선택하고, 기준 전력신호와 상관도가 최대가 되도록 기준 전력신호의 각 피치마다 보간법을 적용하여 전력신호를 정렬한다. 즉 한 피치 동안에 전력신호의 샘플수를 증가하면서 보간법을 적용하여 기준 전력신호와 최고의 상관계수 값을 갖도록 정렬하고, 다음 피치로 이동하여 동일한 방법으로 정렬하게 된다. 이러한 정렬 방법은 신호에 랜덤클럭의 성질을 그대로 둔 채 최대 상관도를 이용하여 공격하는 방법으로, 정렬된 전력신호들의 시작 시점이 일치하지 않으면 공격이 매우 어렵다. (그림 2)는 (그림 1)의 기준 전력신호와 최대의 상관도를 갖도록 피치마다 보간법과 상관계수를 적용하여 정렬하는 과정을 보여준다.

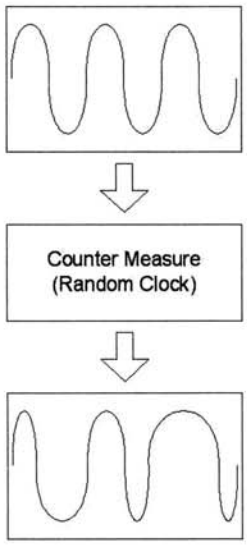


(그림 1) 선정된 기준 전력신호

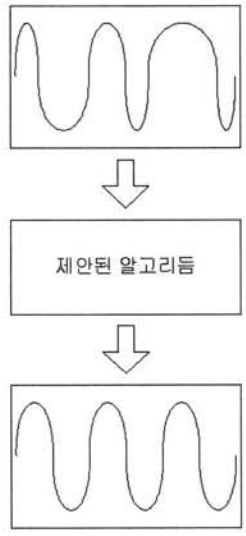


(그림 2) 기준 전력신호에 맞추어 정렬한 전력신호

모든 전력신호에 대하여 동일한 피치를 적용하면 랜덤 클럭이 적용된 전력신호가 일정한 클럭이 적용된 전력신호로 변환되기 때문에 기존의 일정클럭에 대한 공격방법을 그대로 적용할 수 있게 된다. (그림 3)은 랜덤클럭 방어대책이 적용되어 일정 클럭 전력신호가 랜덤클럭 전력신호로 변화되는 과정이고, (그림 4)는 제안된 방법을 적용하여 랜덤클럭 전력신호를 일정클럭의 전력신호로 변환하는 과정을 보여준다.



(그림 3) 방어대책이 적용되어 랜덤클럭 전력신호로 변환과정

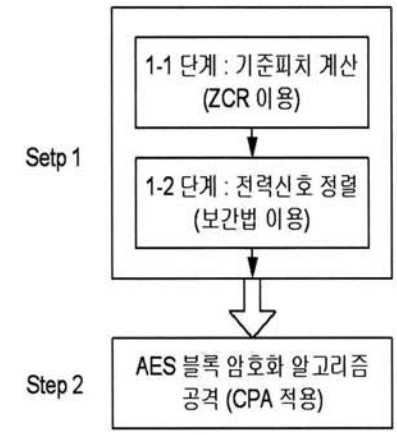


(그림 4) 제안된 알고리듬이 적용되어 일정클럭 전력신호로 변환과정

3. 제안된 전력신호 정렬 방법 및 AES 공격

본 연구에서는 랜덤클럭 방어대책 적용회로에서 랜덤클럭의 효과를 근본적으로 원상 복귀시킨 정렬을 이룬 후 상관 전력분석공격을 적용하는 개선된 방법을 제안하고 그 성능을 분석한다.

제안된 전력신호 정렬 방법을 이용하여 AES 블록 암호 알고리듬에 대한 공격은 (그림 5)와 같이 2 단계로 구성된다. 1단계는 제로통과율(zero-crossing rate)을 이용하여 기준 피치를 정하고, 기준피치와 보간법을 이용하여 전력신호를 정렬한다. 제로통과율은 신호가 제로를 통과한 비율이며, 신호가 양의 값에서 음의 값으로, 음의 값에서 양의 값으로 변화하는 비율을 말한다. 피치는 신호의 마루에서 마루까지 또는 골에서 골까지의 시간적 길이 이며, 기준 피치는 전력신호 정렬 시 보간법이 적용되는 피치이다. 2단계는 정렬된 전력신호와 암호화 알고리듬 추정 중간 값의 상관계수 추정치를 구하여 암호화 알고리듬에 사용된 키를 찾아내는 상관분석(CPA : Correlation Power Analysis) 공격하는 단계이다.



(그림 5) 제안된 전력신호의 정렬과 암호화 알고리듬의 공격단계

3.1 제안된 랜덤클럭 전력신호 정렬 방법

제안된 정렬방법은 방어대책으로 랜덤클럭이 적용되어 시간적으로 흔들린 전력파형을 적절히 추정된 일정크기의 기준피치와 보간법을 적용하여 일정한 크기의 피치를 갖는 전력신호로 정렬하는 것이다. 기준 피치의 크기가 너무 작으면 전력신호가 가지고 있는 정보의 일부분을 잃어버리고, 기준 피치가 너무 크면 정렬하는데 시간이 많이 걸리므로, 전력신호의 평균 피치를 기준 피치로 정하고, 매 신호의 각 피치마다 보간법을 적용하여 전력신호를 정렬하며, 제안된 정렬 방법은 다음과 같다.

3.1.1 기준피치 계산

기준피치를 잘못 선정하면 2단계의 전력분석 공격이 실패할 수 있으므로, 적절한 기준피치를 선택하는 것이 중요한 시작 단계에 해당한다. 본 제안에서는 다음과 같이 기준피치를 계산한다.

① 기준 전력신호를 정한다.
② 기준 전력신호에서 평균값(DC)을 뺀다.
③ 상승 (또는 하강) 제로통과율(zero-crossing rate)을 구한다.
④ 기준 전력신호의 전체 샘플 수를 상승(또는 하강) 제로통과율로 나눈 값을 기준 피치로 정한다.

3.1.2 보간법의 적용

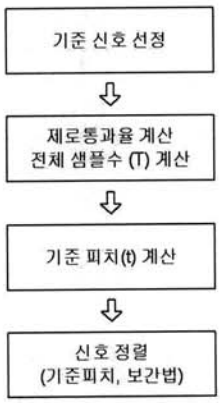
수집된 전력신호의 매 신호마다 피치단위로 보간법을 적용하여야 하며, 제안된 방법에서는 선형보간(linear interpolation and decimation)법을 이용하였으며, 식(2)을 이용하여 (x_0, y_0)와 (x_1, y_1) 사이에서 임의의 x 위치의 y값을 구한다.

$$y = (1-\alpha)y_0 + \alpha y_1 \tag{2}$$

여기서 $\alpha = \dfrac{x - x_0}{x_1 - x_0}$ 이다.

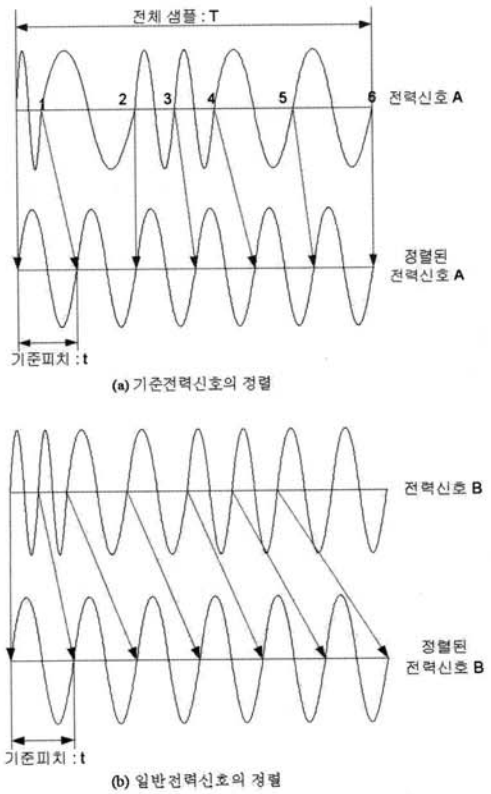
3.1.3 기준피치와 보간법을 적용한 전력신호의 정렬

앞에서 정한 기준피치를 전체 전력신호에 동일하게 적용하여 정렬하므로, 정렬된 전력신호의 피치의 크기는 기준피치와 같게 된다. 전력신호에 동일한 기준피치와 보간법을 사용하여 정렬하는 과정은 (그림 6) 및 (그림 7)과 같다.



(그림 6) 기준피치와 보간법을 이용한 정렬 과정

랜덤클럭이 적용된 전력신호에서 기준 신호를 선정하고, 기준신호의 상승(또는 하강)제로통과율과 전체 샘플수를 계산한다. 전체 샘플수를 상승(또는 하강)제로통과율로 나누어 기준 피치로 정한다. 기준피치와 보간법을 적용하여 전력신호를 정렬한다.



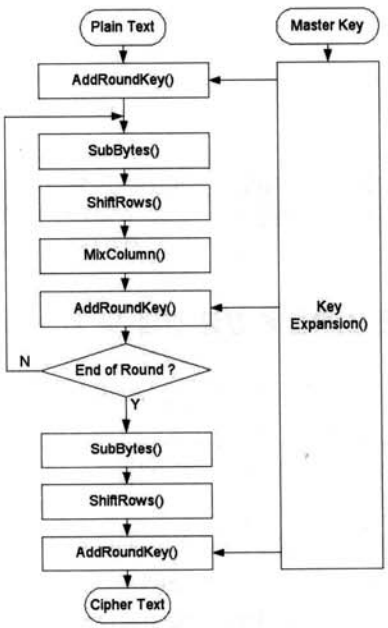
(그림 7) 일정피치와 보간법 적용 방법 예시

전력신호 A를 기준 전력신호로 정하고, 기준 전력신호A의 상승 제로 통과율을 구한 후 기준 전력신호A의 전체 샘플 수(T)를 상승 제로통과율에 해당하는 단위 파형수(그림에서는 6이 됨)로 나누어 기준 피치(t)로 하고, 기준 전력신호 A에 기준 피치와 보간법을 적용하여 정렬한다. 전력신호 B를 기준전력신호 A에서 구한 기준 피치와 보간법을 적용하여 정렬한다.

3.2 AES 블록 암호화 알고리듬에 대한 공격

3.2.1 AES 블록 암호 알고리듬

AES는 128비트의 비트열 입력과 128, 192 또는 256 비트의 비트열 암호화 키로 구성된 블록암호화 알고리듬이며, 각각을 AES-128, AES-192, AES-256이라 한다[7]. AES는 기본적으로 8비트 비트열인 바이트 단위로 실행된다. AES 블럭 암호화 알고리듬은 SubBytes(), ShfiRow(), Mix Column(), AddRoundKey()의 함수로 구성되어있으며, 암호화 키 비트열의 크기가 128, 192, 256이면 반복되는 라운드 수는 각각 10, 12, 14 이며, AES 블록암호화 알고리듬의 블록다이어그램은 (그림 8)과 같다.



(그림 8) AES 암호화 알고리듬

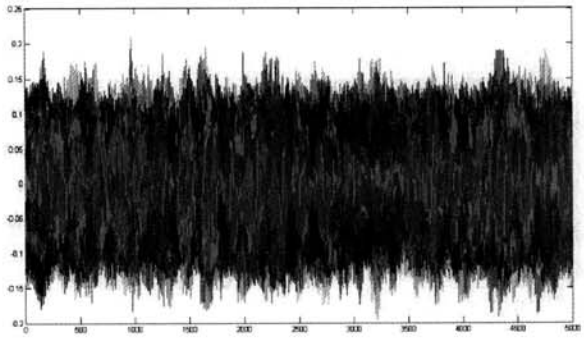
3.2.2 AES 블록 암호화 알고리듬에 대한 공격 [5,6]

첫 번째 AddRoundKey()함수는 평문과 마스터키와 동일한 비밀 키를 이용하여 연산한다. 첫 번째 라운드의 SubBytes()함수의 출력 값을 비밀 키 값에 따라 추정하고, 추정된 중간 값과 측정된 전력신호간의 상관계수를 구하는 상관계수 추정 방법으로 공격하여 비밀 키를 바이트 단위로 찾는다. 식(3)은 추정된 중간 값(X)과 전력신호(Y)의 상관계수 추정 값(r)을 구하는 계산식이다.

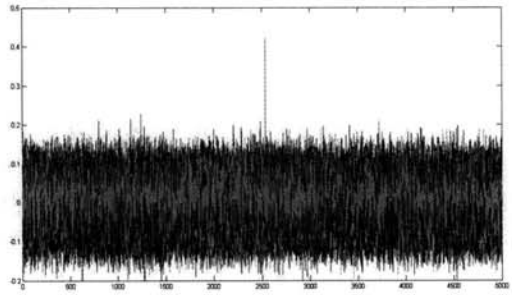
$$r_{k,s} = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2 \sum_{i=1}^{n}(y_i - \bar{y})^2}} \quad (3)$$

여기서 $r_{k,s}$는 k 번째 비밀 키에 대한 s번째 샘플의 상관계수 추정 값, x_i는 i 번째 전력신호의 샘플 값, $\bar{x}$ 는 s 번째 샘플들의 평균값, y_i는 i 번째 추정된 중간 값, $\bar{y}$는 추정된 중간 값들의 평균값이고, $0 \le k \le 255$, s는 전력신호의 샘플 수, n 측정된 전력신호의 수이다.

모든 비밀키에 대하여 추정된 중간값 구하고, 추정된 중간값과 랜덤 클럭이 적용된 전력신호간의 상관계수 추정값을 (그림 9)에, 추정된 중간값과 제안된 방법으로 정렬한 전력신호간의 상관계수 추정값을 (그림 10)에 비교하여 나타내었다. 제안된 알고리듬을 적용하여 정렬한 전력신호 상관계수 추정값에서만 알고리듬 실행 중 추정된 중간 값이 계산 시점에서 큰값을 나타냄을 볼 수 있다.



(그림 9) 랜덤 클럭이 적용된 전력신호의 상관계수 추정 값



(그림 10) 제안된 방법으로 정렬된 전력신호의 상관계수 추정 값

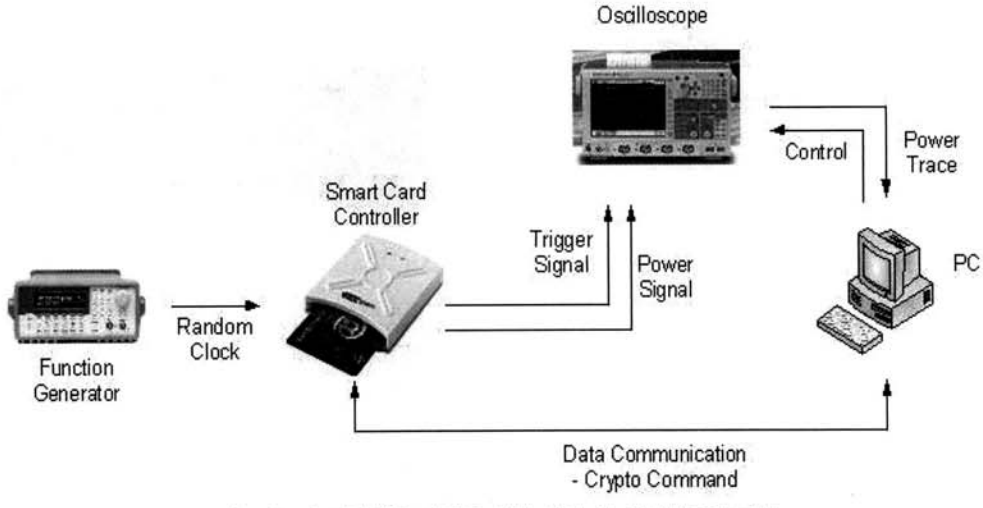
4. 실험 및 비교

랜덤클럭이 적용된 스마트카드에서 AES 블록 암호화 알고리듬을 실행하여 전력신호를 수집하고, 제안된 방법으로 정렬한 전력신호간의 상관도를 구하여 정렬된 정도를 검증하고, 중간 추정 값과 전력신호와의 상관계수 추정치를 구하여 AES 블록 암호화 알고리듬에 사용된 비밀 키를 찾는다.

4.1 실험환경

실험 장치를 (그림 11)과 같이 구성하고, 스마트카드 칩에 AES 블록 암호화 알고리듬을 탑재하고, 디지털 오실로스코프를 사용하여 알고리듬 실행 시 소모되는 전력을 측정하고, PC의 제어프로그램을 통하여 전력소모파형을 수집하고 저장한다. 외부 함수발생기에 sweep 기능이 동작하도록 설정하여 3.579545MHz±150KHz의 클럭이 스마트카드 칩에 인가되도록 한다.

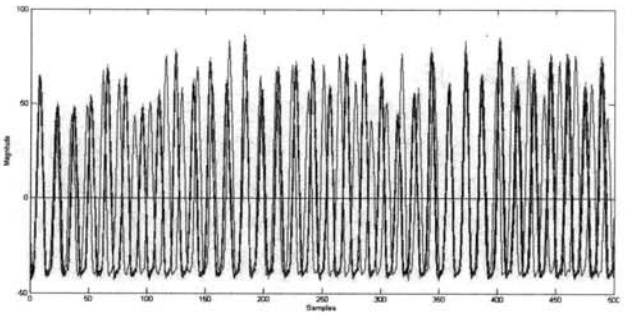
500개의 평문 입력에 대하여 500개의 전력신호를 수집하고, 수집된 전력신호의 샘플링 주파수는 50MHz, 측정 시간은 10msec로, 전력신호 당 획득된 샘플은 500,000개이다.



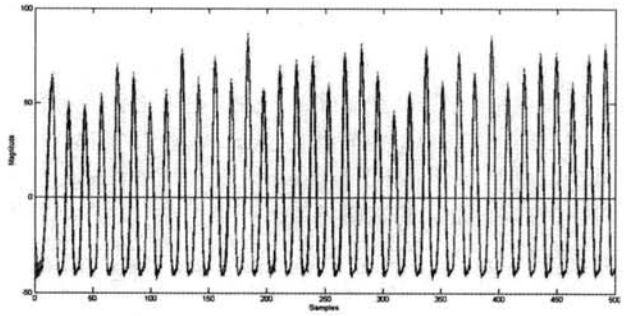
(그림 11) 전력신호 수집을 위한 장비 간 제어신호의 구성

4.2 제안된 방법으로 정렬한 전력신호상호간의 상관도

기준 전력신호를 선정하고, 선정된 기준 전력신호의 상승 제로 통과율을 구한 후 전체 샘플 수를 상승 제로 통과율로 나눈 값을 기준피치로 정하고, 기준피치와 보간법을 적용하여 기준전력신호를 정렬한다. 일반 전력신호에 대하여도 같은 방법으로 정렬한다. (그림 13)은 (그림 12)의 랜덤클럭 전력신호에 제안된 방법을 적용한 전력신호로 시간적으로 바르게 정렬되었음을 보여준다.

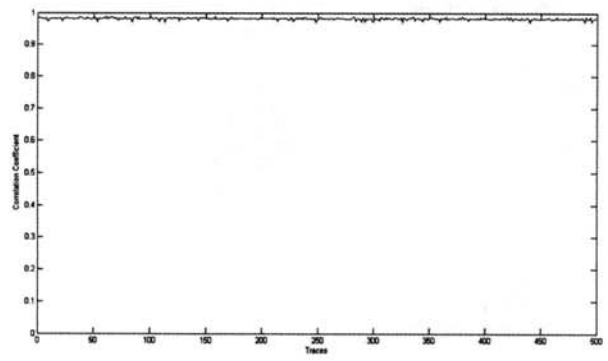


(그림 12) 랜덤클럭 전력신호 (10 trace)



(그림 13) 제안된 방법으로 정렬한 전력신호 (10 trace)

랜덤클럭 전력신호에 제안된 방식을 적용하여 정렬한 전력신호 중 기준 전력신호를 정하고, 기준 전력신호와 일반 전력신호간의 상관계수 추정치를 계산하였다. (그림 14)의 전력신호 상관계수가 거의 1에 가까우면서도 변화가 매우 적어 시간적으로 잘 정렬되었음을 보여준다.



(그림 14) 제안된 방법으로 정렬된 전력신호의 상관계수 추정치

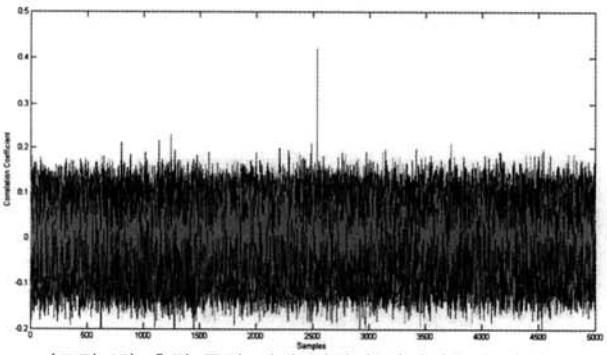
<표 1>은 기존의 전력신호 정렬방법과 제안된 방법을 비교하여 나타낸 것이다. <표 1>과 같이 기존의 정렬 방법에서는 측정된 전력신호의 정렬 시작시점이 시간적으로 일치하여야 공격이 가능하나, 제안된 방법은 측정된 전력신호의 정렬 시작시점이 시간적으로 일치하지 않아도, 제안된 방법으로 정렬 후 전력신호 상호간에 상관계수을 이용하여 시간적으로 동기를 일치 시켜 공격이 가능하다.

〈표 1〉 기존 정렬방법과 제안된 정렬 방법의 비교[4]

항목	정렬항목	랜덤클럭 방어책 공격적용 가능성	전제조건
상관계수 정렬법	- 시간 축 상의 위치	불가능	
기준 전력신호를 이용한 정렬법	- 시간 축 상의 위치 - 시간 축 상의 크기	가능	정렬 시작 시점에서 시간적 동기 요구
제안된 방법	- 시간 축 상의 위치 - 시간 축 상의 크기 - 전력신호 내 일정 주기	가능	없음

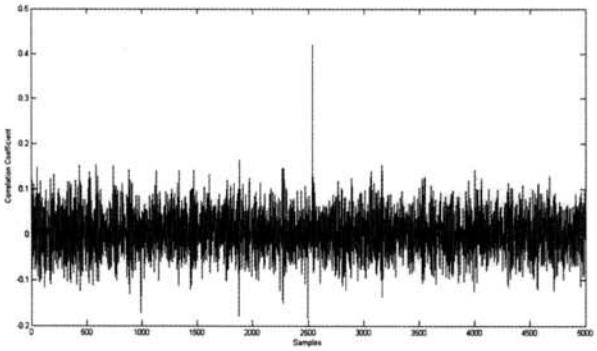
4.3 제안된 알고리듬을 적용한 공격 결과

램덤 클럭이 적용된 AES 블록 암호화 알고리듬 실행 중 측정된 전력신호를 제안된 방법으로 정렬하고, 추정된 중간 값과 정렬된 전력신호사이의 상관계수 추정 값을 구하여 사용된 비밀 키 값을 찾았다.



(그림 15) 추정 중간 값과 정렬된 전력신호의 상관계수 추정 값

AES 블록 암호화 알고리듬의 첫 번째 AddRoundKey() 함수에 사용된 256 가지의 비밀 키(0x00~0xFF) 각각에 대한 추정된 중간 값과 정렬된 전력신호 사이의 상관계수 추정 값들을 (그림 15)에 나타내었다. 최대의 상관계수 추정 값을 보여주는 비밀 키 값은 43(0x2B)이며, 비밀 키 값이 43(0x2B)일 때의 상관계수 추정 값을 (그림 16)에 나타낸다.



(그림 16) 키 값이 43(0x2B)일 때의 정렬된 전력신호의 상관계수 추정 값

(그림 15)와 (그림 16)을 비교하면 시간적으로 동일한 위치에 최대 값이 나타남을 관찰할 수 있으며, 이 시각에 AES 블록 암호화 알고리듬의 SubBytes()함수가 첫 번째 바이트에 대한 연산을 실행함을 보여준다.

5. 결 론

보안장치가 암호 알고리듬 실행 시 소모하는 전력에 대한 분석은 매우 강력한 공격방법이나, 측정된 전력신호와 암호 알고리듬 실행 시 추정되는 중간 값과의 상관도를 연산하는 시점이 시간적으로 일치되어야 전력신호 분석이 가능한 단점을 안고 있다. 전력분석 공격에 대한 방어대책으로 보안장치에 랜덤클럭을 사용하여 측정된 전력신호가 시간적으로 일치하지 않게 한다.

랜덤클럭이 적용된 전력신호는 시간적으로 동기화가 되지 않아 전력분석이 불가능하므로 측정된 전력신호를 일정 피치와 보간법을 적용하여 전력신호 분석이 가능하게 하는 향상된 정렬 방법을 제안하였고, 기존의 정렬방법과 비교 분석하였다. 실험결과 기존의 방법들은 랜덤클럭이 적용된 전력신호 정렬시 시간축의 위치와 크기를 정렬하여, 한 전력신호 내에서는 시간적으로 여전히 랜덤클럭에 대한 영향이 남아있어, 전력신호 측정 시 시간적 동기가 맞지 않으면 전력신호 분석이 어렵게 된다. 그러나 제안된 방법으로 정렬된 전력신호는 일정한 피치를 적용하여 전력신호를 정렬하므로, 한 전력신호 내에서 일정한 피치를 갖게 되어 랜덤클럭에 대한 영향이 없어져, 랜덤클럭을 사용하거나 원하지 않던 원인으로 측정신호가 변형되어 시간적인 위치가 랜덤한 성질을 갖는 전력신호에 효과적으로 적용되어 전력신호 분석공격이 용이하도록 하였다.

참 고 문 헌

[1] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," Proc. CRYPTO, LNCS 1666, pp. 388-397, 1999.

[2] C. Herbst, E. Osward, and S. Mangard, N. "An AES Smart Card Implementation Resistant to Power Analysis", Splinger-Verlag, The 4th International Conference onApplied Cryptography and Network Security-ACNS'06, LNCS 3989, pp. 239-252, 2006.

[3] O. Kömmerling and M. G Kuhn, "Design Principles for Tamper-Resistant Smart Card Processors", The Proceedings of USNIX Wrokshop on Smartcard Technology - Smartcard'99, pp.9-20, 1999.

[4] 박제훈, 문상재, 하재철, 이훈재, "차분 전력 분석 공격을 위한 향상되고 실제적인 신호 정렬 방법," 정보보호학회 논문지, pp.93-101, 제 18권 5호, 2008.

[5] J. Jaffe, "Introduction to Differential Power Analysis", Presented at ECRYPT Summer school on Cryptographic Hardware, Side Channel and Fault Analysis. Jun. 2006.

[6] E. Prouff, "DPA Attack and S-Boxes", In proceedings of FSE-2005, LNCS 3557, pp. 424-441, Springer-Verlag, 2005.

[7] NIST, "Announcing the ADVANCED ENCRYPTION STANDARDS(AES)", Federal Information Processing Standerds Publication 197, Nov. 26, 2001

박 영 구

e-mail : park09@empas.com

1986년 8월 경북대학교 전자공학과(공학사)

1989년 2월 경북대학교 전자공학과 (공학석사)

1998년 8월 경북대학교 전자공학과 (박사수료)

1989년 1월~1997년 2월 국방과학연구소 선임연구원

1997년 3월~2008년 2월 창신대학 모바일통신과 조교수

2010년 1월~현 재 예스테크 연구개발 이사

관심분야 : 정보보호, 정보통신, 부채널 공격 등

이 훈 재

e-mail : hjlee@dongseo.ac.kr

1985년 2월 경북대학교 전자공학과(공학사)

1987년 2월 경북대학교 전자공학과(공학석사)

1998년 2월 경북대학교 전자공학과(공학박사)

1987년 2월~1998년 1월 국방과학연구소 선임연구원(개발팀장)

1998년 3월~2002년 2월 경운대학교 컴퓨터공학과 조교수

2002년 3월~현 재 동서대학교 컴퓨터정보공학부 부교수

2007년 6월~현 재 동서대학교 유비쿼터스 IT전문인력양성 사업단장(NURI)

관심분야 : 암호이론, 정보통신/네트워크, u-네트워크 보안, 부채널 공격 등

문 상 재

e-mail : sjmoon@ee.knu.ac.kr

1972년 2월 서울대학교 공업교육(전자)과 (공학사)

1974년 2월 서울대학교 전자공학과(공학석사)

1984년 6월 미국 UCLA 전자공학과(공학박사)

1984년 7월~1985년 6월 UCLA Postdoctoral 근무

1984년 7월~1985년 6월 미국 OMNET 컨설턴트

1974년 12월~현 재 경북대학교 전자전기컴퓨터공학부 교수

2000년 8월~현 재 경북대학교 이동네트워크 정보보호기술 연구센터 소장

2002년 2월~현 재 한국정보보호학회 명예회장

관심분야 : 정보보호, 디지털 통신, 이동 네트워크 등