情報保護學會論文誌
第18卷 第5號, 2008. 10

차분 전력 분석 공격을 위한 향상되고 실제적인 신호 정렬 방법*

박 제 훈[1†], 문 상 재[1‡], 하 재 철[2], 이 훈 재[3]
[1]경북대학교, [2]호서대학교, [3]동서대학교

Enhanced and Practical Alignment Method for Differential Power Analysis*

JeaHoon Park[1†], SangJae Moon[1‡], JaeCheol Ha[2], HoonJae Lee[3]
[1]Kyungpook National University, [2]Hoseo University, [3]Dongseo University

요 약

스마트카드, USB token과 같은 저 전력 정보보호장치의 가장 큰 위협요소인 부채널 공격은 장치 내부에 구현된 암호 알고리즘의 이론적인 안전도와는 무관하게 적용될 수 있다. 특히, 부채널 공격들 중에서 차분 전력분석 공격은 적용이 쉽고 근본적인 방어가 어려워서 매우 위협적인 공격이지만 공격을 적용하기 위해서는 측정된 모든 신호가 시간축 상에서 매우 잘 정렬된 신호라는 전제조건이 필요하기 때문에, 트리거 지터링, 잡음, 차분 전력 분석 공격 방어책 등 여러 요인들에 의해 시간축 상에 정렬되지 않은 측정된 신호를 정렬하기 위한 여러 가지 방법들이 제안되어 왔다. 기존의 신호 정렬 방법들은 측정된 신호의 시간축 상의 위치만을 정렬하는 방법들이어서, 랜덤 클럭을 이용하여 알고리즘의 수행 시간(시간축 상의 신호 크기)을 변화시키는 차분 전력 분석 대응 방법에는 적용이 되지 않는다. 본 논문에서는 측정된 소비 전력 신호를 보간(interpolation)과 추출(decimation) 과정을 통해서 시간축 상에서 위치뿐만 아니라 크기도 동시에 정렬시키는 향상된 신호 정렬 방법을 제안하였다. 또한 랜덤 클럭 방식의 차분 전력 분석 공격 방어대책이 구현된 스마트카드 칩에 개선된 신호 정렬 방법을 적용하여 차분 전력 분석 공격이 효과적으로 적용됨을 실험적으로 확인하였다.

ABSTRACT

Side channel attacks are well known as one of the most powerful physical attacks against low-power cryptographic devices and do not take into account of the target's theoretical security. As an important succeeding factor in side channel attacks (specifically in DPAs), exact time-axis alignment methods are used to overcome misalignments caused by trigger jittering, noise and even some countermeasures intentionally applied to defend against side channel attacks such as random clock generation. However, the currently existing alignment methods consider only on the position of signals on time-axis, which is ineffective for certain countermeasures based on time-axis misalignments. This paper proposes a new signal alignment method based on interpolation and decimation techniques. Our proposal can align the size as well as the signals' position on time-axis. The validity of our proposed method is then evaluated experimentally with a smart card chip, and the results demonstrated that the proposed method is more efficient than the existing alignment methods.

Keywords : Side-ChannelAttack, Signal Alignment Method, Random Clock Countermeasure, Interpolation, Decimation

Ⅰ. 서 론

Kocher에 의해 차분 전력 분석 공격 방법이 제안된 이 후, 저 전력 정보보호장치들의 안전도를 논의할 때에 내부에 구현된 암호 알고리즘들은 암호 알고리즘의 이론적인 안전성 외에도 차분 전력 분석공격에 대한 안전성을 추가 검토할 필요가 있다[1]. 차분 전력 분석 공격은 저 전력 정보보호장치 내부에서 암호 알고리즘이 수행되는 동안에, 그 소비 전력이 암호 알고리즘의 연산 중간 값에 대한 해밍웨이트에 비례한다는 사실을 바탕으로 측정된 소비 전력을 분석하는 방법이다. 따라서 스마트카드, USB token, RFID 등에 암호 알고리즘을 구현할 때 이론적 안전성과는 별도로 암호 알고리즘에 대한 구현 측면의 대응책이 필요하게 된다.

차분 전력 분석 공격을 방어하기위한 기존의 방법들은 크게 두 가지로 나눌 수 있다. 첫 번째는 랜덤 값을 사용하여 암호 알고리즘 자체를 수정하거나 dual-rail logic 등을 사용해서 해서 연산중에 누출되는 소비 전력 정보가 연산중에 나타나는 중간 값과 연관이 없도록 하는 것이다[2-7]. 두 번째는 암호 알고리즘에 랜덤 지연 시간을 삽입하거나 랜덤 클럭을 이용하여 차분 전력 분석 공격이 적용되는 지점이 어긋나도록 하는 방법이다[8,9]. 전자의 경우 차분 전력 분석 공격 지점을 늘려서 랜덤 값의 영향을 상쇄되도록 하는 고차 차분 전력 분석 공격 방법에 취약할 수 있고, dual-rail logic의 경우 구현상의 문제점과 가격 면에서 효율성이 떨어진다. 후자의 경우에도 측정된 신호를 정렬하는 방법을 이용하여 어느 정도 극복이 가능하지만, 랜덤 클럭을 사용하는 경우에는 측정된 소비 전력 신호가 시간축 상에서 어긋나는 것은 물론이고 알고리즘의 수행 시간도 달라져서 기존의 신호 정렬 방법을 이용해서는 극복할 수 없다. 또한 가격 경쟁력을 위해 저가의 클럭 발생기를 사용하는 암호 장치에서 측정된 불안정한 클럭으로 인해 흐트러진 소비 전력 파형의 경우도 기존의 신호 정렬 방법은 적용되기 어려울 수 있다.

접수일 : 2008년 4월 8일; 수정일 : 2008년 7월 4일;
채택일 : 2008년 7월 21일
* 본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음(IITA-2008-C1090-0801-0026)
† 주저자, jenoon65@ee.knu.ac.kr
‡ 교신저자, sjmoon@ee.knu.ac.kr

본 논문에서 제안하는 신호 정렬 방법은 측정된 소비 전력 신호를 시간축 상에서 이동시켜 정렬하는 것은 물론이고, 보간(interpolation)과 추출(decimation) 과정을 통하여 기존의 신호 정렬 방법들이 고려하지 않았던 측정된 소비 전력 신호의 시간축 상의 크기도 변화시켜 정렬한다. 따라서 제안하는 부채널 신호 정렬 방법은 랜덤 클럭을 사용하거나 여러 가지 요인들에 의해 공격이 적용되는 지점이 어긋나 있고 암호 알고리즘의 수행 시간이 변화되어 있는 신호의 경우에도 효과적으로 적용될 수 있는 정렬 방법이다.

2장에서는 기존의 신호 정렬 방법에 대해 간단히 언급하고, 3장에서는 제안하는 신호 정렬 방법을 설명한다. 4장에서 랜덤 출력 대응책에 대한 차분 전력 분석 공격 실험을 통하여 제안하는 신호 정렬법의 효용성을 검증 한 후, 5장에서 결론을 맺도록 한다.

Ⅱ. 관련 연구

차분 전력 분석 공격의 경우 저 전력 정보보호장치에 대한 매우 위협적인 공격 방법이지만 측정되는 소비 전력 신호가 시간축 상에서 잘 정렬된 신호여야 하는 단점이 있다. 즉, 차분 전력 분석 공격자는 암호 알고리즘 수행 중에 예측하는 중간 값이 연산되는 시점에서의 소비 전력 차이를 비교하기 때문에 측정된 모든 소비 전력 신호들에서 예측하는 중간값이 연산되는 시점이 동일하여야 한다. 예를 들어 A XOR B를 계산한 결과값 C를 예측한다면 C가 레지스터에 저장되기 위해 LOAD 연산이 수행되는 지점들이 모든 측정된 소비 전력 파형에서 일치하여야 한다. 하지만 오실로스코프 트리거의 지터링이나 잡음 등의 영향으로 측정된 소비 전력 신호들이 시간축 상에서 정렬되지 않는 경우가 발생한다.

이 후로 설명하는 정렬 방법들은 시간축 상에서 정렬되지 않은 신호를 시간축 상에서 이동시켜가면서 정렬하여 차분 전력 분석 공격이 적용 가능하도록 하고 있다.

2.1 상관 계수를 이용한 정렬 방법

상관 계수는 두 변량 사이의 상관관계를 나타내는 값이다. 다음의 식은 상관 계수를 구하는 식을 나타내고 있다.

$$\frac{E((X-E(X))(Y-E(Y)))}{\sigma_X \sigma_Y} \quad (1)$$

여기서, $E()$는 평균값을 나타내고 σ_X, σ_Y는 각각 X, Y의 표준편차를 나타내고 있다.

측정된 소비 전력 신호들 중에 기준이 되는 임의의 신호를 선택한 후 측정된 소비 전력 신호들을 시간축 상에서 이동시켜 가면서 상관 계수를 계산하여 기준이 되는 신호와의 상관 계수 값이 최대가 되도록 측정된 소비 전력 신호들을 정렬한다.

2.2 POC(Phase-Only Correlation) 방법을 이용한 정렬 방법

시간 영역의 신호를 퓨리에 변환하면 신호의 모양에 의존하는 진폭 신호와 신호의 위치에 의존하는 위상신호로 구분할 수 있다. 다음의 수식은 두개의 소비 전력 신호의 이산시간 퓨리에 변환된 값을 나타내고 있다.

$$S_1(k) = \sum_{n=-M}^{M} s_1(n) W_N^{kn} = A_{S_1} e^{j\theta_{S_1}(k)} \qquad (2)$$
$$S_2(k) = \sum_{n=-M}^{M} s_2(n) W_N^{kn} = A_{S_2} e^{j\theta_{S_2}(k)}$$

여기서, $s_1(n)$, $s_2(n)$은 측정된 소비 전력 신호이고, N은 $2M+1$로서 소비 전력 신호의 크기를 나타내고, $W_N^{kn} = e^{-j\frac{2\pi}{N}}$이다. 위의 식에서와 값이 이산시간 퓨리에 변환된 신호는 진폭 성분인 A_{S_1}, A_{S_2}과 위상 성분인 $e^{j\theta_{S_1}(k)}$, $e^{j\theta_{S_2}(k)}$으로 구분할 수 있다. CHES 2006에 발표된 POC(Phase-Only Correlation) 정렬 방법은 측정된 소비 전력 신호를 이산시간 퓨리에 변환하여 신호의 위치에 의존하는 위상 성분의 값들만을 정렬한 다음 이산시간 퓨리에 역변환 하여 차분 전력 분석 공격을 적용한다[10]. POC 정렬 방법은 기존의 상관 계수를 이용한 정렬 방법과 비교하였을 때, 잘 정렬된 신호와 그렇지 않은 신호들 사이의 차이를 확실히 구분할 수 있어서 두 신호사이의 구분을 정확하게 할 수 있도록 한다.

앞서 언급한 기존의 신호 정렬 방법들은 측정된 소비 전력 신호들이 시간축 상의 흔들림으로 인해 정렬되지 않았을 경우에는 효과적으로 적용될 수 있지만, 신호의 시간축 상으로의 이동만을 고려하는 방법들이라서 신호의 모양이 바뀌는 경우에는 적용되지 않는다. 즉, 트리거 지터링이나 잡음 등의 영향으로 측정된 소비 전력 신호가 시간축 상에서 잘 정렬되지 않았을 경우에는 앞서 언급한 방법들로 신호 정렬이 가능하지만, 랜덤 클럭을 사용하는 차분 전력 분석 공격 대응책이 구현된 장치에서 측정된 소비 전력 신호는 시간축 상에서 잘 정렬되지 있지 않음은 물론이고 알고리즘 수행 시간이 변화되어 측정된 소비 전력 신호의 모양이 바뀌는 경우에는 적용되지 못한다.

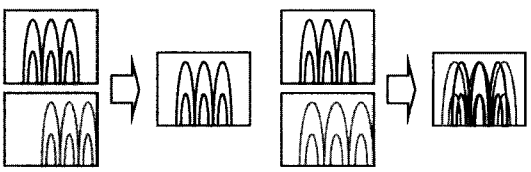
Ⅲ. 보간과 추출 방법을 이용한 향상된 신호 정렬 방법

차분 전력 분석 공격을 적용하기위해서 측정된 소비 전력 신호가 정렬되지 않았을 경우의 문제점을 해결하는 기존의 방법들은 측정된 소비 전력 신호의 시간축 상의 이동만을 고려하였다. 다시 말하면 암호 알고리즘의 수행 시간이 변화하여 측정된 소비 전력 신호의 모양이 바뀔 경우에는 적용되지 않는 신호 정렬 방법들이었다. 따라서 랜덤 클럭을 이용하는 차분 전력 분석 공격 대응방법을 사용하였거나 저가의 클럭 발생기 등의 여러 요인으로 인해 암호 알고리즘의 수행 시간이 변화하게 되는 경우에는 지금까지의 신호 정렬 방법으로는 차분 전력 분석 공격을 적용할 수 없다.

[그림 1(a)]와 같이 시간축 상의 위치가 어긋나서 측정된 신호들 간에 정렬이 이루어지지 않은 경우에는 시간축 상의 이동만을 고려하여 기존의 신호 정렬 방법으로 신호 정렬이 가능하지만, [그림 1(b)]와 같이 시간축 상의 위치가 어긋나 있고, 시간축 상의 크기 또한 어긋나 있는 신호들은 기존의 신호 정렬 방법으로는 신호를 정확히 정렬할 수 없다.

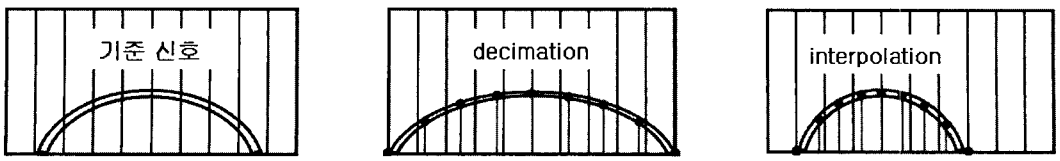
이와 같은 문제점을 해결하기 위해서 측정된 소비 전력 파형이 시간축 상의 이동에 의해 신호가 정렬되지 않았을 경우에는 물론이고 측정된 소비 전력 신호의 시간축 상의 크기가 변화하는 경우(즉, 랜덤 클럭을 사용하는 경우)에도 적용이 가능한 신호 정렬 방법을 제안한다.

보간과 추출 방법은 샘플링된 신호에 적용하는 방법



(a) 시간축 상의 이동만으로 정렬이 가능한 경우 (b) 시간축 상의 이동만으로 정렬이 불가능한 경우

〔그림 1〕 기존 신호 정렬 방법의 신호의 어긋난 성분에 따른 정렬 가능성



(a) 기준 신호 (b) 신호의 크기가 큰 경우 (샘플 개수가 많은 경우) (c) 신호의 크기가 작은 경우 (샘플 개수가 적은 경우)

〔그림 2〕 신호 샘플 개수의 변동 효과로 인한 신호 크기 변동 효과

으로, 샘플링 지점 외의 신호 값을 주변의 샘플링된 신호 값을 이용하여 추정해서 신호의 샘플수를 늘리거나 줄이는 방법이다. 따라서 본 논문에서는 보간과 추출 방법을 이용하여 측정된 소비 전력 신호의 샘플 수를 조정한다. 보간 방법을 이용하여 신호의 샘플 수를 적절히 늘려서 시간축 상의 신호의 크기가 작은 경우를 정렬하고, 추출 방법을 이용하여 신호의 샘플 수를 적절히 줄여서 시간 축 상의 신호의 크기가 큰 경우를 정렬한다.

[그림 2]는 샘플 개수의 변동으로 시간축 상의 신호의 크기를 변동시키는 효과는 볼 수 있다는 것을 보여주고 있다. [그림 2]의 가로축은 샘플을 나타내고 세로축은 신호의 진폭을 나타낸다.

보간과 추출 방법을 이용하여 새로운 위치에 샘플 값을 만드는 방법에는 Linear interpolation, Nearest neighbor interpolation, Cubic Spline interpolation 등의 여러 가지 방법이 있다. 본 논문의 실험에서는 보간과 추출 방법을 이용한 신호 정렬 가능성에 중점을 두고 실험을 하였으며, Linear interpolation 방법을 사용하였다. 다음의 수식은 *x0*와 *x1* 사이의 x축의 좌표가 주어졌을 경우, *(x0,y0)*와 *(x1,y1)* 사이의 y 점을 Linear interpolation 알고리즘을 나타내고 있다.

$$y=(1-\alpha)\cdot y_0+\alpha\cdot y_1,\ \text{여기서}\ \alpha=\frac{x-x_0}{x_1-x_0} \qquad (3)$$

요즘 일반적으로 사용하고 있는 디지털 오실로스코프는 측정된 신호의 샘플된 데이터를 사용자에게 제공한다. 따라서 스마트카드가 동작할 때 소비되는 전력 신호를 오실로스코프로 측정하여 컴퓨터에 저장한 후, 샘플의 개수를 조절할 수 있는 보간과 추출 방법을 이용하여 샘플의 개수를 조정함으로써 측정된 소비 전력 신호의 수행 시간(시간축 상의 크기)을 변화시키는 효과를 얻을 수 있었다. 다음의 [그림 3]은 제안하는 정렬 방법의 수행 절차를 나타내고 있다.

여기서, Smeasure 측정된 소비 전력 신호이며, Sref

Input : S_{ref}, $S_{measure}$, *dec*, *inter*, *cor*
Output : S_{align}

1. Max_{cor} = 0, $align_{cor}$ = 0, $align_{inter}$ = 0;
2. for *i* = *dec* to *inter* {
   S_{inter} = *INTER*(*i* , $S_{measure}$);
3. for *j* = *-cor* to *cor* {
   S_{shift} = *SHIFT*(*j* , S_{inter});
   S_{cor} = COR(S_{ref}, S_{shift});
   if (Max ≤ S_{cor})
   Max = S_{cor};
   $align_{inter}$ = *i*, $align_{cor}$ = *j*;
   }
   }
4. S_{align} = *SHIFT*($align_{cor}$, *INTER*($align_{inter}$, $S_{measure}$)
5. Return S_{align}

〔그림 3〕 제안하는 신호 정렬 알고리즘

는 측정된 소비 전력 신호 중에서 임의로 선택된 기준 신호 이다. *INTER*() 함수는 *dec*와 *inter* 범위 내의 비율 값에 따라 샘플 간격을 재조정하여 신호를 보간하고 추출하는 함수이다, 예를 들어, *INTER*(*i* , Smeasure)에서 *i* 값이 1.01일 경우에는 *x*축을 1.01 간격으로해서 0, 1.01, 2.02, 3.03,... 에 해당하는 *y*축의 값을 Linear interpolation 알고리즘을 사용하여 계산한다. *SHIFT*() 함수는 cor 값의 범위 내에서 이동 값에 신호를 좌/우 이동시키는 함수 이다. *COR(x,y)* 함수는 x와 y의 상관 계수를 구하는 함수이다.

[그림 3]의 제안하는 정렬 알고리즘에서는 보간/추출 방법을 이용하여 신호의 시간축 상의 크기를 변화 시킨 후, 시간축 상에서 이동을 시켜가면서 상관 계수를 계산한다. 이 때 상관 계수가 최대가 되도록 하는 *INTER*() 함수의 비율 값 *i*와 *SHIFT*() 함수의 이동 값 *j*를 저장하고, *SHIFT*(*i* , *INTER*(*j* , Smeasure)) 함수의 결과를 알고리즘의 출력 값으로 출력한다.

Ⅳ. 차분 전력 분석 공격을 이용한 제안된 신호 정렬 방법 검증

현재까지 DES, AES, RSA, ARIA 등 많은 암호 알

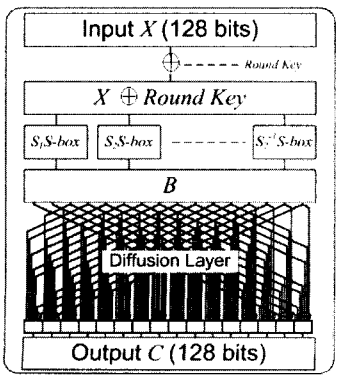
고리즘들이 차분 전력 분석 공격에 취약함이 밝혀졌다. 제안하는 신호 정렬 방법은 차분 전력 분석 공격의 공격 절차와는 별개로 측정된 신호만을 정렬하는 방법으로써, 공격 방법이나 타겟 암호 알고리즘에 영향을 받지 않는다. 다만 랜덤 클럭 등을 사용하여 기존의 차분 전력 분석 공격이 적용되지 않도록 한 암호 장치에서 측정된 소비 전력 신호를 정렬하여 차분 전력 분석 공격이 적용 가능하도록 한다. 본 논문의 실험에서는 국내 표준 알고리즘인 ARIA 알고리즘에 제안된 차분 전력 분석 공격 적용을 위해 J. Ha 등이 제안한 실험 환경을 구성하였다. 또한 부가적으로 랜덤 클럭을 사용하도록 하여 기존 공격이 적용되지 않는 환경을 만들어 제안하는 신호 정렬 방법의 효율성을 검증하였다.

4.1 ARIA 알고리즘에 대한 공격 실험

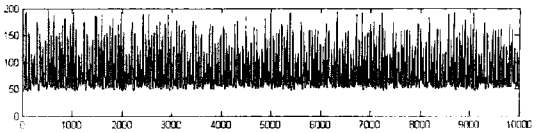
ARIA 블록 암호 알고리즘은 128 비트 입력과 128, 192, 256 비트 비밀키를 사용하는 암호 알고리즘으로써 각 라운드 함수는 AddRoundKey, Substitution Layer, Diffusion Layer의 세 가지 하위 함수들로 구성된다 [11,12]. ARIA 알고리즘 라운드 함수의 간단한 구조는 아래의 [그림 4]와 같다.

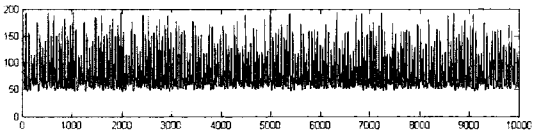
본 논문에서는 차분 전력 분석 공격을 적용하기 위해서 ARIA 알고리즘의 1라운드 첫번째 S-box를 공격 대상으로 하였고, 추측한 비밀키 이용하여 시뮬레이션한 1라운드 첫번째 S-box 결과 값의 해밍웨이트를 기준으로 임의로 생성된 입력 메시지를 높은 해밍웨이트를 가지는 그룹과 낮은 해밍웨이트를 가지는 그룹으로 분류하였다[13].

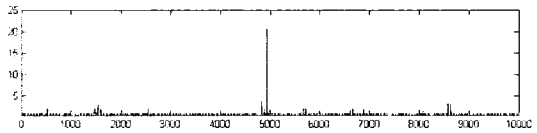
[그림 5]는 차분 전력 분석 공격 대응책이 구현되지



[그림 4] ARIA 알고리즘.


(a) 높은 해밍웨이트 평균 파형


(b) 낮은 해밍웨이트 평균 파형


(c) 차분 결과 파형

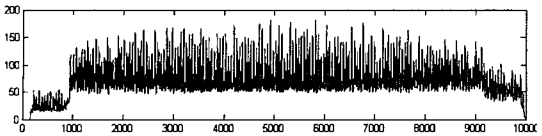
[그림 5] ARIA 알고리즘에 대한 차분 전력 분석 공격 결과

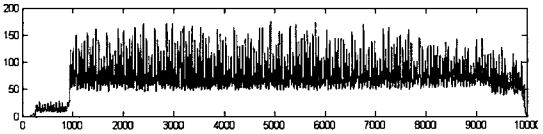
않은 공격 대상으로부터 측정된 소비 전력 파형을 이용한 차분 전력 분석 공격 실험 결과를 보여주고 있다. 실험을 위해서 ARIA 알고리즘을 소프트웨어로 스마트카드 칩의 EEPROM 영역에 구현하였고, 차분 전력 분석 공격이 용이 하도록 알고리즘 전/후로 트리거 신호를 삽입하였다. [그림 5]의 결과와 같이 잘 정렬된 신호의 경우 별도의 정렬 방법을 사용하지 않고도 차분 전력 분석 공격이 쉽게 적용된다는 것을 알 수 있다.

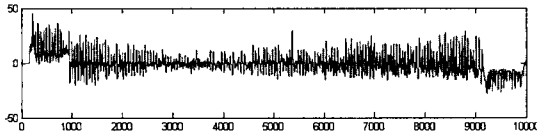
4.2 랜덤 클럭 대응 방법에 대한 기존의 신호 정렬 방법을 이용한 공격 실험

앞선 실험의 결과로 공격 대상 스마트카드에 전력 분석 공격을 적용할 수 있다는 것을 알 수 있었다. 따라서 이번 실험에서는 차분 전력 분석 공격을 방어하기위해서 스마트카드 칩이 3.579545MHz의 외부 함수발생기 클럭을 사용하도록 하였고, 함수 발생기의 sweep 기능을 이용하여 20kHz 범위 내에서 클럭이 변하도록 구현하였다. 즉, 스마트카드의 동작주파수는 3.569545MHz와 3.589545 사이에서 가변된다. 측정된 소비 전력 신호를 기존의 신호 정렬 방법 중의 하나인 상관 계수를 이용하는 신호 정렬 방법을 이용하여 정렬한 후 차분 전력 분석 공격을 적용하였다. 다음의 [그림 6]은 상관 계수를 이용하여 측정된 신호를 정렬한 후 차부전력분석 공격을 적용한 결과를 보여주고 있다.

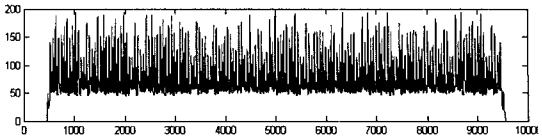
[그림 6]의 결과에서는 측정된 소비 전력 신호를 시

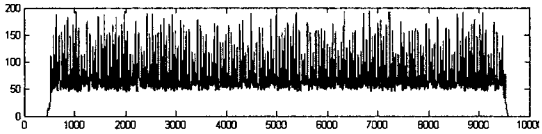

(a) 높은 해밍웨이트 평균 파형

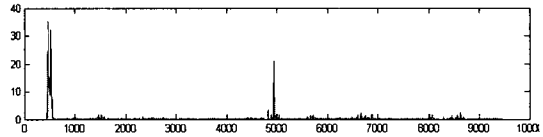

(b) 낮은 해밍웨이트 평균 파형


(c) 차분 결과 파형

〔그림 6〕 랜덤 클럭을 이용하는 차분 전력 분석 공격 대응 방법에 대한 상관 계수 신호 정렬 방법 적용 결과


(a) 높은 해밍웨이트 평균 파형


(b) 낮은 해밍웨이트 평균 파형


(c) 차분 결과 파형

〔그림 7〕 랜덤 클럭을 이용하는 차분 전력 분석 공격 대응 방법에 대한 제안된 신호 정렬 방법 적용 결과

간축 상에서 정렬하기 위해서 기존의 상관 계수를 이용하는 정렬 방법을 사용하였지만, 랜덤 클럭을 사용하는 대응방법에는 차분 전력 분석 공격이 적용되지 않는다는 것을 알 수 있었다. [그림 6(a)(b)] 평균 파형의 앞/뒤 모양이 [그림 5(a)(b)]와 다른 것은 시간 축 상에서 파형을 좌우로 이동시키면서 상관 계수를 계산하기 위해 *SHIFT*() 함수를 사용한 영향이다.

4.3 랜덤 클럭 대응 방법에 대한 제안된 신호 정렬 방법을 이용한 공격 실험

기존의 상관 계수를 이용한 정렬 방법은 측정된 소비 전력 신호를 시간축 상의 이동만을 고려하여 정렬하므로 랜덤 클럭 대응책이 사용되어 알고리즘의 수행 시간이 변화하는 경우에는 적용되지 않는다.

이번 실험에서는 제안하는 신호 정렬 방법을 사용하여 측정된 소비 전력 신호를 시간축 상에서 이동과 수행 시간의 변화가 모두 정렬되도록 하였다. [그림 7]은 제안하는 정렬 방법을 이용한 차분 전력 분석 공격 결과를 보여주고 있다. 실험을 위해 오실로스코프에 측정된 50us 구간의 파형을 200Msps로 샘플한 10000개의 샘플 데이터를 사용하였다. 실험에 사용되는 스마트카드는 3.569545MHz~3.589545MHz의 외부 클럭을 사용한다. 따라서, 3.579545MHz에서의 10000샘플이 포함하는 연산을 기준으로 3.569545MHz에서는 10028샘플, 3.589545MHz에서는 9972샘플이 포함하는 연산이 동일하게 된다. [그림 2]의 알고리즘을 위하여 ±30 샘플이 보간/추출될 수 있도록 *dec*=0.997, *inter*=1.003으로 두고 *i*는 0.0001씩 증가하도록 하였다. 상관 계수 계산 전에 신호의 시간축 이동 값은 오실로스코프의 트리거 지터링과 실험 환경에서의 잡음 등에 크게 의존한다. 실험에서는 측정된 소비 전력 파형의 10% 정도의 시간축 이동을 고려하여 *cor*=1000으로 두고 *j*는 1씩 증가하도록 하였다. 물론 [그림 2]의 알고리즘을 적용하는 환경을 고려하여 임의의 기준 신호와 예상되는 클럭의 변동 범위에 따라 정렬을 위한 세 가지 변수를 적절히 변화시켜야 한다. *i, j* 변수의 변화 범위가 클수록 더 심한 클럭 변동을 교정할 수 있지만, 연산량이 많아지는 단점이 있다. 신호를 정렬하기 전에 주파수 성분 분석 등을 통하여 클럭 변동 범위를 효과적으로 설정할 수 있을 것이다.

[그림 7]의 결과를 통해서 제안하는 신호 정렬 방법은 랜덤 클럭을 사용한 차분 전력 분석 공격을 방어법이 사용된 암호 장치에도 적용이 된다는 것을 알 수 있다. 즉, 제안하는 정렬 방법은 측정된 소비 전력 신호의 시간축 상의 이동에 의한 신호의 정렬되지 않음과 알고리즘 수행 시간 변화에 의한 신호의 정렬되지 않음을 모두 해결하는 정렬 방법이라는 것을 알 수 있으며, 이를 실험적으로 확인하였다. [그림 7(c)]에서 관찰할 수 있는 500포인트 부근의 피크 파형은 [그림 6]의 결과와

마찬가지로 상관 계수를 계산하기 위해 *SHIFT*() 함수를 사용한 영향이다.

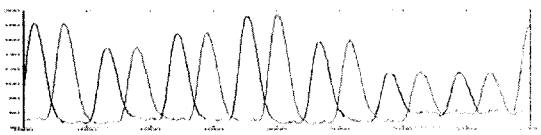
4.4 실험 결과 분석

제안 하는 정렬 방법과 기존의 정렬 방법을 비교하기 위해서 랜덤 클럭을 사용하는 암호 장치에서 측정된 소비 전력 신호를 정렬한 후 분석하였다. [그림 8]은 랜덤 클럭을 사용하는 암호 장치에서 측정된 소비 전력 신호와 이를 상관 계수를 사용하여 정렬된 신호, 이를 제안하는 정렬 방법을 사용하여 정렬된 신호를 보여주고 있다.

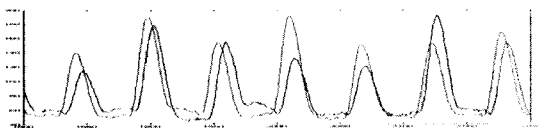
[그림 8(b)]에서와 같이 상관 계수를 사용하여 정렬된 신호는 정렬되지 않은 [그림 8(a)]에 비해서는 좀 더 정렬된 듯 보이지만 완전히 정렬되지 않았고, 또한 두 신호의 수행 시간이 다르기 때문에 정렬된 신호가 같은 연산에 대한 소비 전력 파형이라는 것을 확신할 수 없다.

하지만 제안하는 정렬 방법을 사용하여 정렬된 신호는 측정된 소비 전력 신호의 수행 시간까지 조정하여 [그림 8(c)]에서와 같이 두 신호가 완전히 정렬된다는 것을 알 수 있다.

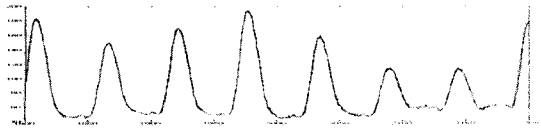
[그림 9]는 신호 정렬법을 적용하지 않은 랜덤 클럭 방어책을 적용한 스마트카드로부터 측정된 전력 소비 신호 그룹과 측정된 전력 소비 신호에 상관 계수를 이용한 신호 정렬법을 적용한 그룹, 측정된 전력 소비 신호에 제안하는 신호 정렬법을 적용한 그룹의 세 가지 그룹별로 그룹 내의 임의의 한 신호를 기준으로 기준



(a) 측정된 정렬되지 않은 전력 소비 파형

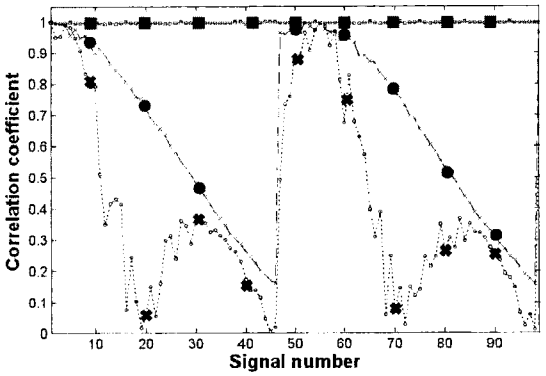


(b) 상관 계수 정렬 방법으로 정렬된 전력 소비 파형



(c) 제안하는 정렬 방법으로 정렬된 전력 소비 파형

〔그림 8〕 신호 정렬 전/후의 소비 전력 파형 비교



■ 제안하는 신호 정렬법을 사용하여 정렬된 그룹.
● 상관 계수 정렬법을 사용하여 정렬된 그룹.
X 신호 정렬법을 사용하지 않은 그룹.

〔그림 9〕 측정 신호 그룹별로 계산된 그룹내의 신호들 간의 상관 계수

〔표 1〕 기존 정렬 방법과 제안 정렬 방법 비교.

항목	정렬 항목	랜덤 클럭 방어책 공격 여부
상관 계수 정렬법	시간 축 상의 위치	공격 적용 불가능
POC 정렬법	시간 축 상의 위치	공격 적용 불가능
제안 방법	시간 축 상의 위치 시간 축 상의 크기	공격 적용가능 (랜덤 클럭 대응책 무력화)

신호와의 상관 계수를 계산하여 보여주고 있다. [그림 9]의 결과와 같이 제안하는 신호 정렬법을 적용한 그룹의 그룹 내의 신호들 간의 상관 계수들은 모두가 거의 1에 가까운 값을 가지므로 랜덤 클럭을 사용하는 스마트카드로부터 측정된 소비 전력 신호도 제안하는 신호 정렬법을 이용하면 잘 정렬될 수 있다는 것을 알 수 있다.

다음의 [표 1]은 앞선 실험 결과들과 비교 결과들을 종합하여 나타내고 있다. 제안하는 신호 정렬법은 랜덤 클럭 대응책이 구현된 암호 장치로부터 측정한 정렬되지 않은 신호의 시간축 상의 위치 변화와 시간축 상의 크기 변화 모두를 정렬하여 기존의 차분 전력 분석 공격 방법이 적용 가능하도록 한다. 본 논문에서는 이를 스마트카드에 대한 실험을 통하여 제안하는 신호 정렬법의 효용성을 검증하였다.

V. 결 론

차분 전력 분석 공격은 적용이 용이하고 근본적으로 방어하는 것이 어려워 저 전력 암호장치들에 대해 매우

위협적인 공격이지만 측정된 신호가 시간축 상에서 매우 잘 정렬된 신호여야 하는 단점이 있다. 본 논문에서는 소비 전력 신호를 시간축 상에서 이동시켜 정렬하는 것은 물론이고 오실로스코프를 통해 측정된 소비 전력 신호가 이산 시간 신호라는 것에 착안하여 보간과 추출 방법을 이용해서 측정된 소비 전력 신호의 시간축 상의 크기를 변화시키는 향상된 부채널 신호 정렬 방법을 제안하였다. 또한 랜덤 클럭을 사용하여 차분 전력 분석 공격을 방어하는 상황을 구현하여 제안하는 신호 정렬 방법과 기존의 정렬 방법을 비교하였다. 실험 결과 예상과 마찬가지로 시간축 상의 이동만을 고려하는 기존의 신호 정렬 방법은 랜덤 클럭을 사용하는 방어책에 적용되지 않았지만, 제안하는 정렬 방법은 랜덤 클럭을 사용하거나 여러 가지 요인들에 의해 측정된 소비 전력 신호에서 차분 전력 분석 공격을 적용하려는 지점이 어긋나있고 암호 알고리즘의 수행 시간이 변화되어 있는 신호의 경우에도 효과적으로 적용되어 차분 전력 분석 공격이 적용 가능하도록 하였다.

참고문헌

[1] P. Kocher, J. Jae, and B. Jun, "Differential power analysis", *Springer-Verlag*, In Advances in Cryptology-CRYPTO'99, LNCS 1666, pp. 388-397, 1999.

[2] M. Akkar, and C. Giraud, "An Implementation of DES and AES, Secure against Some Attacks", *Springer-Verlag*, Workshop on Cryptographic Hardware and Embedded Systems-CHES'01, LNCS 2162, pp. 309-318, 2001.

[3] M. Akkar, and L. Goubin, "A Generic Protection against High-Order Differential Power Analysis", *Springer-Verlag*, The 10th annual Fast Software Encryption workshop-FSE'03, LNCS 2887, pp. 192-205, 2003.

[4] J. Bl¨omer, J. Guajardo, and V. Krummel, "Provably Secure Masking of AES", *Springer-Verlag*, The 11th International Workshop on Selected Areas in Cryptography-SAC'04, LNCS 3357, pp. 69-83, 2005.

[5] E. Oswald, S. Mangard, N. Pramstaller, and V. Rijmen, "A Side-Channel Analysis Resistant Description of the AES S-box", *Springer-Verlag*, The 12th Fast Software Encryption workshop-FSE'05, LNCS 3557, pp. 413-423, 2005.

[6] M. Bucci1, L. Giancane, R. Luzzi, and A. Trifiletti, "Three-Phase Dual-Rail Pre-charge Logic", *Springer-Verlag*, Workshop on Cryptographic Hardware and Embedded Systems-CHES'06, LNCS 4249, pp. 232-241, 2006.

[7] Z. Chen, and Y. Zhou, "Dual-Rail Random Switching Logic : A Countermeasure to Reduce Side Channel Leakage", *Springer-Verlag*, Workshop on Cryptographic Hardware and Embedded Systems-CHES'06, LNCS 4249, pp. 242-254, 2006.

[8] C. Herbst, E. Oswald, and S. MangardAn, "AES Smart Card Implementation Resistant to Power Analysis Attacks", *Springer-Verlag*, The 4th International Conference on Applied Cryptography and Network Security-ACNS'06, LNCS 3989, pp. 239-252, 2006.

[9] O. K¨ommerling, and M. G. Kuhn, "Design Principles for Tamper-Resistant Samrtcard Processors", The Proceedings of the USENIX Workshop on Smartcard Technology-Smartcard'99, pp. 9-20, 1999.

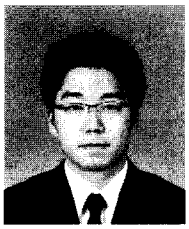
[10] N. Homma, S. Nagashima, Y. Imai, T. Aoki, and A. Satoh, "High-Resolution Side-Channel Attack Using Phase-Based Waveform Matching", *Springer-Verlag*, Workshop on Cryptographic Hardware and Embedded Systems-CHES'06, LNCS 4249, pp. 187-200, 2006.

[11] NSRI, NSRI anounces that ARIA v. 1.0 has been presented as a standard block cipher in Korea. June, 2004, Available from http : //www.nsri.re.kr/ARIA/.

[12] D. Kwon, J. Kim, S. Park, S. Sung, Y. Sohn, J. Song, Y. Yeom, E. Yoon, S. Lee, J. Lee, S. Chee, D. Han, and J. Hong, "New Block Cipher : ARIA", *Springer-Verlag*, In Information Security and Cryptology-ICISC'03, LNCS 2971, pp. 432-445, 2003.

[13] J. Ha, C. Kim, S. Moon, I. Park, and H. Yoo, "Differential Power Analysis on Block Cipher ARIA", *Springer-Verlag*, In the International Conference on High Performance Computing and Communications-HPCC'05, LNCS 3726, pp. 541-548, 2005.

〈著者紹介〉



박 제 훈 (JeaHoon Park) 학생회원
2004년 2월 : 경북대학교 전자·전기공학부 졸업
2006년 2월 : 경북대학교 전자공학과 석사
2006년 3월~현재 : 경북대학교 전자전기컴퓨터학부 박사과정
<관심분야> 정보보호, 네트워크 보안 스마트카드 보안

문 상 재 (SangJae Moon) 종신회원
1972년 2월 : 서울대학교 공업교육(전자전공)과 학사
1974년 2월 : 서울대학교 전자공학과 석사
1984년 6월 : 미국 UCLA 전기공학과 박사
1984년 7월~1985년 6월 : UCLA Postdoctor 근무
1997년 9월~1998년 8월 : 경북대학교 전자전기공학부 학부장
2001년 1월~2001년 12월 : 한국정보보호학회 회장
1974년 12월~현재 : 경북대학교 전자전기컴퓨터공학부 교수
2000년 8월~현재 : 경북대학교 이동네트워크 정보보호기술 연구센터장
2002년 2월~현재 : 한국정보보호학회 명예회장
<관심분야> 정보보호, 디지털 통신, 이동 네트워크

하 재 철 (JaeCheol Ha) 종신회원
1989년 2월 : 경북대학교 전자공학과 졸업
1993년 8월 : 경북대학교 전자공학과 석사
1998년 2월 : 경북대학교 전자공학과 박사
1998년 3월~2006년 1월 : 나사렛대학교 전자계산소장, 학술정보관장, 입시학생처장
1998년 3월~2007년 2월 : 나사렛대학교 정보통신학과 부교수
2006년 7월~2006년 12월 : QUT in Australia 연구 교수
2007년 3월~현재 : 호서대학교 정보보호학과 부교수
2002년 3월~현재 : 한국정보보호학회 이사
<관심분야> 정보보호, 네트워크 보안, 스마트카드 보안

이 훈 재 (HoonJae Lee) 종신회원
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~현재 : 동서대학교 컴퓨터정보공학부 부교수
2007년 6월~현재 : 동서대학교 유비쿼터스 IT전문인력양성사업단장(NURI)
<관심분야> 암호이론, 정보통신/네트워크, u-네트워크 보안, 부채널 공격