情報保護學會論文誌
第 21 卷 第 1 號, 2011. 2

모바일 기기에서의 전력 분석 공격을 위한 새로운 전력 신호 정렬 방법*

이 유 리,† 김 완 진, 이 영 준, 김 형 남‡
부산대학교

A novel power trace aligning method for power analysis attacks in mobile devices*

Yu-Ri Lee† , Wan-Jin Kim, Young-Jun Lee, Hyoung-Nam Kim‡
Pusan National University

요 약

최근 모바일 기기를 통한 인터넷 접속이 급격하게 증가함에 따라 모바일 보안의 중요성이 크게 대두되고 있다. 특히 무선 인터넷을 통해 개인정보나 금융정보와 같은 중요한 정보가 전달되는 경우 정보 노출의 우려가 크게 증가하므로 이를 방지하기 위해 다양한 암호화 알고리즘들이 개발되어 사용되고 있다. 그러나 이론적으로는 매우 안전한 것으로 알려진 암호화 알고리즘들도 암호화가 수행되는 동안 기기에서 누설되는 물리적 신호를 이용하는 부채널 공격에는 취약성을 드러내는 경우들이 많다. 이러한 문제를 해결하기 위해서는 부채널 공격에 대한 분석 및 예상되는 성능 개선안 등에 대한 연구가 선행되어야 한다. 부채널 공격 방법 중에서 전력 분석 공격은 매우 효과적이고 강력한 방법으로 알려져 있다. 그러나 전력 분석 공격의 성능을 보장하기 위해서는 수집된 전력 신호가 잘 정렬되어야 하나, 실제 전력 신호 측정 시 측정오차나 랜덤 클럭과 같은 부채널 공격 대응 방법 등으로 인해 시간 왜곡이 빈번하게 발생하므로 전력 분석 공격 성능이 저하되는 문제가 있다. 이러한 오정렬 문제를 해결하기 위해 다양한 정렬 방법이 제안되었으나, 기존 방법들은 많은 연산량이 요구되고 한 파형 내에서 시간 지연이 변화하는 경우에 효과적으로 대처하지 못하는 단점이 있다. 이러한 문제를 극복하기 위해 본 논문에서는 기준 신호의 피크 (peak)를 이용해 신호를 정렬하는 방법을 제안한다. 모의실험을 통해, 제안하는 정렬 방법이 기존의 정렬 방법보다 전력 분석 공격에서 매우 효과적임을 보인다.

ABSTRACT

Recent trends in mobile device market whose services are rapidly expanding to provide wireless internet access are drawing people's attention to mobile security. Especially, since threats to information leakage are reaching to the critical level due to the frequent interchange of important data such as personal and financial information through wireless internet, various encryption algorithms has been developed to protect them. The encryption algorithms confront the serious threats by the appearance of side channel attack (SCA) which uses the physical leakage information such as timing, and power consumption, though the their robustness to threats is theoretically verified. Against the threats of SCA, researches including the performance and development direction of SCA should precede. Among the SCA methods, the power analysis (PA) attack overcome this misalignment problem. The conventional methods require large computational power and they do not effectively deal with the delay changes in a power trace. To overcome the limitation of the conventional methods, we proposed a novel alignment method using peak matching. By computer simulations, we show the advantages of the proposed method compared to the conventional alignment methods.

Keywords: Power analysis attack, alignment method, peak matching

접수일(2010년 12월 03일), 게재확정일(2011년 02월 07일)
* 이 논문은 2008년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2008-0061842)

† 주저자, leeyuri@pusan.ac.kr
‡ 교신저자, hnkim@pusan.ac.kr

I. 서 론

최근 모바일 기기의 발달로 인해 스마트폰이나 태블릿 PC의 사용자가 급격하게 증가함에 따라 무선 인터넷 서비스도 급격하게 확대되고 있으며, 무선 인터넷 환경에서 제공되는 다양하고 유용한 서비스를 이용하기 위해 개인정보나 금융정보와 같은 민감한 정보의 저장과 교환도 빈번하게 발생하고 있다. 그러나 이러한 정보가 제대로 보호되지 못할 경우 정보 유출에 따른 피해가 필연적으로 발생하게 되므로, 이를 방지하기 위한 모바일 보안의 필요성이 점차적으로 증가하고 있다. 모바일 보안은 스마트폰과 같은 모바일 기기에서 뿐만 아니라, 무선 인터넷 환경을 구축하기 위해 사용되는 무선공유기 (Wireless Access Point)에서도 요구되며, 대표적인 무선 데이터 통신 시스템인 와이파이 (Wi-Fi)와 와이브로 (Wibro)는 무선 통신 중에 발생할 수 있는 정보 유출을 막기 위해 IEEE 802.11-2007 표준과 IEEE 802.16e-2009 표준을 각각 제정하였다[1],[2]. 이러한 표준들에서는 데이터 교환 방식에 따라 다양한 방법의 암호화 알고리즘이 사용되는데, 데이터의 양방향 통신인 경우에는 암호화를 위해 AES (Advanced Encryption Standard)[3], DES (Data Encryption Standard)[4], SEED (128-bit Symmetric Block Cipher)[5] 등과 같은 대칭형 암호화 알고리즘을 사용한다[6]. 데이터의 기밀성을 보장하기 위한 대칭형 암호화 알고리즘들은 비밀 키를 이용해 입력되는 정보를 복잡한 연산을 통해 암호화시켜 뛰어난 안정성을 가지므로, 모바일 보안뿐만이 아니라 RFID나 USB 보안 token 등 다양한 곳에서 활용되고 있다. 그러나 이러한 암호화 알고리즘의 안전성이 매우 뛰어나다 할지라도 H/W상에서 암호화 알고리즘이 동작하면서 누설되는 물리적 정보들은 보호되지 않으므로, 이러한 허점을 이용해 비밀 키를 알아내는 부채널 공격 (Side Channel Attacks, SCA) 방법이 등장하게 되었다. 대표적인 SCA 방법에는 시차 공격 (Timing Attack, TA), 전력 분석 (Power Analysis, PA) 공격, 전자기파 분석 (ElectroMagnetic Analysis, EMA) 공격이 있으며[7]-[11], 다양한 SCA 방법 중에서도 PA 공격은 대부분의 암호화 알고리즘에 대해 가장 위협적이고 효과적인 공격 방법으로 널리 알려져 있다. 이런 PA 공격의 성능 향상을 위해 수집한 전력 신호의 잡음을 제거는 방법과 전처리 방법이 제안되어[12]-[15], 정보보안은 큰 위협에 직면하게 되었다.

대표적인 PA 공격 방법으로는 차분 전력 분석 (Differential Power Analysis, DPA) 공격[8]과 상관도 전력 분석 (Correlation Power Analysis, CPA) 공격[9]이 있다. PA 공격은 암호화 과정에서 누설되는 전력 신호의 통계적 특성을 이용한 방법이므로, 수집된 전력 신호들은 높은 상관관계를 가져야 한다. 그러나 현실적으로는 측정 시의 오차나 H/W의 불안정성으로 인해 수집된 전력 신호간의 정렬이 완벽하지 못하므로, 파형간의 상관관계가 떨어져 PA 공격 성능이 저하되는 문제가 상존하며 이를 오정렬 (misalignment) 문제라고 한다. 최근에는 SCA 공격에 대한 방어책으로 랜덤 지연 시간을 삽입하거나 랜덤 클럭을 이용하여 의도적으로 전력 신호에 시간왜곡을 발생시켜 의도적으로 오정렬 문제를 발생시키는 경우도 있으므로 [16],[17], PA 공격의 성능을 보장하기 위해서는 수집된 전력 신호를 잘 정렬하기 위한 방법이 요구된다.

전력 신호 정렬 방법에는 전력 신호들 간의 상관관계를 이용해 정렬하는 방법과 수집된 전력 신호들을 퓨리에 변환한 후 위상 차를 이용해 신호를 정렬하는 방법[18]이 있다. 이러한 정렬 방법들은 수집된 전력 신호들의 오정렬이 단순히 시간 지연으로만 나타난다는 가정을 포함하고 있으므로 측정 타이밍 에러 등에 의해 전력 신호간의 오정렬이 발생하는 경우에는 효과적이나, 클럭이 임의적으로 변하거나 의도적으로 시간 왜곡을 발생시킨 경우에는 정렬 성능이 떨어지는 단점이 있다. 이러한 기존 정렬 방법의 단점을 극복하기 위해 보간과 추출을 이용해 전력 신호를 변형시킨 후 신호간의 상관관계를 이용해 신호를 정렬하는 방법이 제안되었으나[19], 상관연산을 이용해 신호를 정렬하므로 연산량이 증가하는 단점이 있다.

신호 정렬을 위한 전처리 과정을 단축하기 위해서는 연산량이 작으면서도 임의적인 클럭 변화와 의도적인 시간 왜곡에 효과적으로 대처할 수 있는 방법의 개발이 요구되며, 이를 위해 본 논문에서는 전력 신호의 피크 점을 기준으로 하여 부분적으로 신호를 보간함으로써 신호를 정렬하는 방법을 제안한다. 제안된 방법은 상관 계수를 이용한 정렬 방법이나 보간과 추출을 이용한 정렬 방법과 같이 반복적으로 상관 계수를 구하지 않으므로 상대적으로 연산량이 작고, 신호의 피크를 정렬한 후에 보간법을 이용해 피크간의 샘플 수를 동일하게 조정하므로 전력 신호 내에서 지연이 균일하지 않더라도 정렬이 가능한 장점이 있다.

본 논문의 구성은 다음과 같다. II장에서 PA 공격 방법에 대해 간단히 설명하고, 신호 정렬과 PA 공격 성능과의 관계에 대해 설명한다. III장을 통해 기존의 신호 정렬 방법들에 대해 간략히 살펴보고, IV장에서 제안하는 피크 매칭을 이용한 새로운 신호 정렬 방법에 대해 소개한다. V장에서는 각 신호 정렬 방법에 따른 PA 공격 성능을 비교하기 위해, 제안된 피크 매칭을 이용한 신호 정렬 방법과 기존의 신호 정렬 방법을 적용하여 수집된 전력 신호를 정렬한 후 PA 공격을 수행하여 각 정렬 방법들이 PA 공격 성능에 미치는 영향을 분석한다. 마지막으로 VI장에서 본 논문의 결론을 맺는다.

II. PA 공격 성능과 신호 정렬의 관계

PA 공격은 암호화 기기가 암호화 동작을 하는 동안 누설되는 전력 신호들의 통계적 특성을 이용해 암호화에 사용된 비밀 키를 알아내는 방법으로, 여기서 누설되는 전력 신호란 암호화 기기에 임의의 평문을 입력으로 넣었을 때 암호화 알고리즘이 H/W상에서 동작하면서 발생되는 전력신호를 말한다. 수집된 전력 신호의 정렬정도와 PA 공격 성능간의 관계를 알아보기 위해, 본 절에서는 우선 PA 공격 중 대표적인 방법인 DPA 공격과 CPA 공격들에 대해 간략하게 살펴본다. 아래에 제시된 PA 공격 방법의 이해를 돕기 위해, 현재 모바일 데이터 보안의 표준으로 사용되고 있는 128-bit AES 암호화 알고리즘을 공격 대상 암호화 알고리즘으로 가정하였다.

2.1 차분 전력 분석 (DPA) 공격[8]

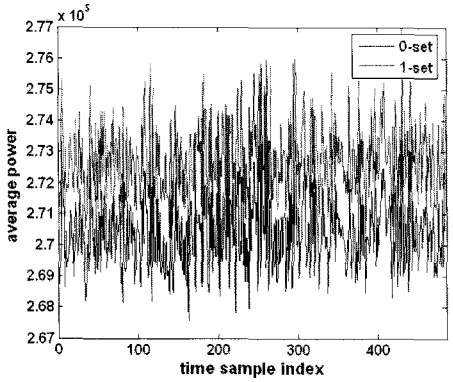
P. Kocher 등에 의해 제안된 DPA 공격은 임의의 평문을 암호화 알고리즘의 입력으로 넣었을 때 계산되는 중간 값과 전력 신호 사이의 관계를 이용하여 비밀 키를 알아내는 방법이다. 임의의 평문 P_i (i = 1,2,...,M)를 AES 암호화 알고리즘의 입력으로 넣으면, 각 평문 P_i와 0h00~0hFF인 256개의 값을 가지는 K_j (j = 0,1,...,255)를 XOR (Exclusive OR, ⊗) 연산하여 그 연산 결과를 분류함수인 S-Box (Substitution Box)의 입력으로 넣는다. 이 때 분류함수 $D_b(P_i, K_j)$는 다음과 같이 정의 된다 [20].

$$D_b(P_i, K_j) = SBOX(P_i \otimes K_j) \quad (1)$$

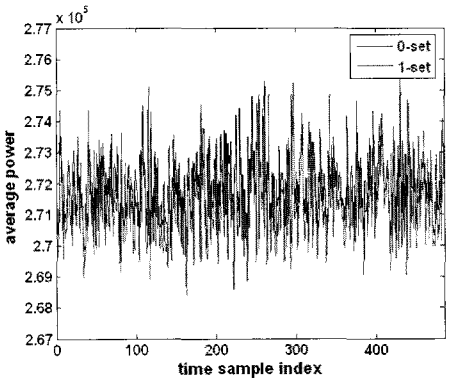
여기서 $D_b(P_i, K_j)$는 8-bit의 길이 (b=1,2,...,8)를 가지며, 각 bit의 값은 '1' 또는 '0'이다. DPA 공격은 $D_b(P_i, K_j)$의 값이 '1'의 값을 얻었을 때와 '0'의 값을 얻었을 때의 전력 소비 정도가 다르다는 가정에 기반해 '1'의 값을 가지는 경우에는 i번째 입력에 해당하는 전력 신호 $W_{i,n}$를 '1-set'으로 분류하고, '0'의 값을 가지는 경우에는 전력 신호 $W_{i,n}$를 '0-set'으로 분류한다. 여기서 n은 전력 신호 샘플 인덱스를 의미한다. 각 추정 키에 대해 모든 입력을 대입하여 XOR 연산을 수행하여 식 (1)과 같이 분류하고, 이렇게 얻은 각 'set'의 평균을 이용하여 다음과 같이 차분 값을 구한다.

$$\Delta_{j,n} = \sum_{b=1}^{8} \left\{ \frac{\sum_{i=1}^{M} D_b(P_i, K_j) W_{i,n}}{\sum_{i=1}^{M} D_b(P_i, K_j)} - \frac{\sum_{i=1}^{M} (1 - D_b(P_i, K_j)) W_{i,n}}{\sum_{i=1}^{M} (1 - D_b(P_i, K_j))} \right\} \quad (2)$$

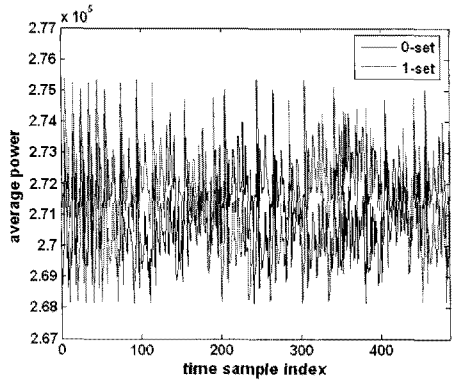
이 차분 값 $\Delta_{j,n}$의 크기를 모든 n에 대하여 합하면, 각 추정 키에 대한 DPA 공격 연산의 대푯값 Δ_j를 계산할 수 있다[21]. DPA 공격에서는 bit의 값이 '1' 또는 '0'일 경우 소비되는 전력이 다르다고 가정하였으므로 각 추정 키 별로 DPA 공격 연산의 대푯값을 살펴보면 추정 키가 비밀 키일 경우에는 큰 대푯값이 나타나고, 그 반대의 경우에는 작은 대푯값이 나타날 것임을 추측할 수 있다. [그림 1].(a)와 같이 비밀 키가 사용된 경우에는 2.08×10^3의 큰 대푯값을 가지며, [그림 1].(b)와 같이 잘못된 추정 키가 사용된 경우에는 0.66×10^3의 작은 대푯값을 가지는 것을 볼 수 있다. 이 경우 비밀 키와 잘못된 추정 키의 대푯값 차이가 크므로 추정 키가 비밀 키임을 신뢰할 수 있다. 그러나 신호 간에 정렬이 되지 않은 경우에는 [그림 1].(c)에서처럼 비밀 키를 사용하는 경우에도 대푯값이 1.78×10^3으로 감소하고, [그림 1].(d)에서 보는 바와 같이 잘못된 추정 키를 사용하는 경우에는 대푯값이 1.26×10^3으로 오히려 커지는 현상이 나타나게 된다. 이렇게 정렬되지 않은 신호를 사용하는 경우에는 비밀 키와 잘못된 추정 키 사이의 편차가 감소하게 되므로, 올바른 비밀 키를 추정하였다 하더라도 DPA 공격 결과를 신뢰하기 어렵게 된다.



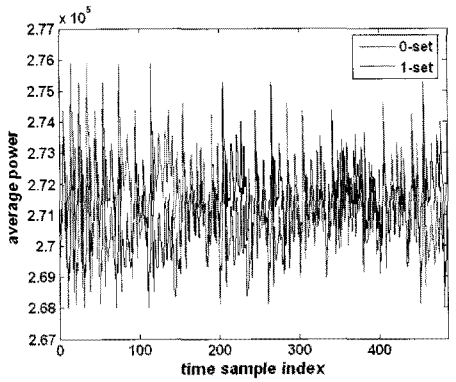
(a) 정렬된 전력 신호로 옳은 추정 키를 사용해 DPA 공격을 수행한 경우 0-set과 1-set의 평균 ($\Delta_j \approx 2.08\times10^3$)



(b) 정렬된 전력 신호로 틀린 추정 키를 사용해 DPA 공격을 수행한 경우 0-set과 1-set의 평균 ($\Delta_j \approx 0.660\times10^3$)



(c) 정렬되지 않은 전력 신호로 옳은 추정 키를 사용해 DPA 공격을 수행한 경우 0-set과 1-set의 평균 ($\Delta_j \approx 1.78\times103$)



(d) 정렬되지 않은 전력 신호로 틀린 추정 키를 사용해 DPA 공격을 수행한 경우 0-set과 1-set의 평균 ($\Delta_j \approx 1.26\times103$)

〔그림 1〕 정렬이 된 경우와 아닌 경우의 DPA 공격 결과 차이

2.2 상관도 전력 분석 (CPA) 공격[9]

Brier 등에 의해 제안된 CPA 공격은 임의의 평문을 암호화 알고리즘의 입력으로 넣었을 때 생기는 중간 값을 이용해 소비 전력 모델을 생성한 후, 매 시간 샘플마다 소비 전력 모델 값과 측정된 소비 전력 신호들의 상관 계수를 구하여 비밀 키를 찾아내는 방법이다. CPA 공격을 수행하기 위해서는 우선 전력 신호 모델을 만들어야 하며, 이를 만드는 방법에는 Hamming distance를 이용하는 방법과 Hamming weight를 이용하는 방법 등이 있는데[22] 본 논문에서는 Hamming weight를 이용하는 방법을 기준으로 설명을 진행한다. Hamming weight 모델은 DPA 공격과 마찬가지로 먼저 분류함수 $D_b(P_i, K_j)$로부터 얻어진 8-bit의 결과에서, '1'의 값을 가지는 bit의 개수를 더하여 아래 식과 같이 얻어진다.

$$H_{i,j} = \sum_{b=1}^{8} D_b(P_i, K_j) \tag{3}$$

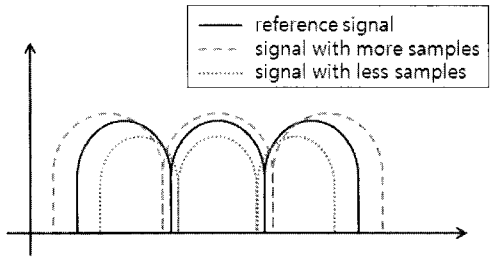
모든 평문과 추정 키에 대해 Hamming weight $H_{i,j}$가 구해지면, $H_{i,j}$와 n번째 시간 샘플에 해당하는 모든 소비 전력 값과의 상관 계수 $C_{j,n}$은 다음과 같이 계산된다.

$$C_{j,n}=\frac{\sum_{i=1}^{M}\{(H_{i,j}-E[H_j])\cdot(W_{i,n}-E[W_n])\}}{\sqrt{\sum_{i=1}^{M}(H_{i,j}-E[H_j])^2\cdot\sum_{i=1}^{M}(W_{i,n}-E[W_n])^2}}$$
$$where\begin{cases}E[H_j]=\frac{1}{M}\sum_{i=0}^{M}H_{i,j}\\E[W_n]=\frac{1}{M}\sum_{i=0}^{M}W_{i,n}\end{cases} \quad (4)$$

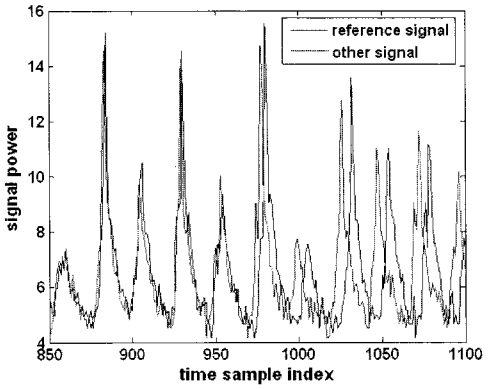
여기서 $E[H_j]$는 모든 평문에 대한 j번째 추정 키의 Hamming weight 값의 평균을 나타내고, $E[W_n]$는 모든 평문에 대한 n번째 소비 전력 샘플의 평균을 나타낸다. 앞에서의 가정에 따르면 비밀 키를 이용해 Hamming weight를 구한 경우에는 상관 계수 값이 크고, 다른 추정 키가 사용되었을 때는 작은 상관 계수 값을 가진다. 따라서 각 추정 키별로 구한 상관 계수 $C_{j,n}$중 가장 큰 값일 때, 그에 해당하는 추정 키를 비밀 키로 판단한다. 이러한 CPA 공격은 측정된 전력 신호간의 지연으로 인해 오정렬이 발생한 경우에도 소비 전력 모델과 소비 전력 신호간의 높은 상관관계가 유지되는 범위 내에서는 비교적 큰 상관 계수 값을 가질 수 있으므로 DPA보다 우수한 공격 성능을 보인다. 즉, CPA 공격은 DPA 공격에 비해 신호의 오정렬에 대해 상대적으로 영향을 덜 받으므로, 정렬이 되지 않은 전력 신호를 이용하더라도 DPA 공격보다 더 나은 성능을 보일 것이라 예상할 수 있다. 그러나 측정된 전력 신호 간에 오정렬이 발생하면 사용한 전력 신호 모델과 측정된 신호 간에 상관관계 손실이 발생하게 되어 공격 성능이 저하되므로, CPA 공격의 성능을 보장하기 위해서는 공격에 앞서 수집된 신호를 정렬하는 전처리 과정이 반드시 수행되어야 한다.

III. 기존의 신호 정렬 방법

II절에서 살펴본 바와 같이, PA 공격을 효과적으로 수행하기 위해서는 측정된 신호가 시간 축 상에서 잘 정렬된 상태여야 한다[19]. 그러나 부채널 공격에서 신호의 오정렬 (misalignment) 문제는 측정된 전력 신호의 시작 시점이 상이하여 생기는 단순한 시간 지연뿐만 아니라, [그림 2]와 같이 부채널 공격에 대한 방어책으로 사용되는 랜덤 클럭이나, [그림 3]과 같은 클럭의 불균일성이나 잡음, 지터 (jitter) 등의 H/W 문제로 인해서도 발생할 수 있다. 본 절에서는 이러한 신호의 오정렬 문제를 해결하기 위해 제안된 다양한 신호 정렬 방법에 대해서 살펴본다.



[그림 2] 랜덤 클럭으로 인해 각 신호들 간의 샘플수가 달라진 예.



[그림 3] 시간 왜곡이 발생한 전력 신호 파형 예.

3.1 상관 계수를 이용한 정렬 방법

상관 계수는 두 신호 $x(n)$과 $y(n)$사이의 상관관계의 정도를 0과 1사이의 값으로 나타내며, 다음과 같이 계산된다.

$$C(n_0)=\frac{E\left[\begin{array}{c}(x(n-n_0)-E[x(n-n_0)])\\\cdot(y(n-n_0)-E[y(n-n_0)])\end{array}\right]}{\sigma_{x(n-n_0)}\sigma_{y(n-n_0)}} \quad (5)$$

여기서 $E[\,]$는 평균값을, n_0는 지연된 시간 인덱스를 나타내며, 그리고 σ_x와 σ_y는 각각 $x(n)$과 $y(n)$의 표준편차를 의미한다. $x(n)$과 $y(n)$이 서로 비슷하다면 상관도가 커져 '1' 근처의 큰 값을 가지게 되고, 두 신호의 차이가 커지면 상관도가 감소하여 '0' 근처의 작은 값을 가지게 된다. 상관 계수를 이용해 신호를 정렬하기 위해서는, 먼저 측정된 신호 중에서 기준 신호를 정하고, 나머지 신호들과 시간 지연 인덱스 n_0를 증가시켜가면서 각 인덱스마다 두 신호의 상관도를 구

한다. 모든 인덱스에 대해 상관도 값이 구해지면 그 중 가장 큰 값을 가질 때가 기준 신호와 가장 비슷하게 정렬되었다고 판단한다. 그러나 이러한 정렬 방법은 측정된 신호들이 단순히 시간 지연된 경우에는 매우 효과적이나, 각 신호들이 임의의 클럭을 가지거나 신호 내에서 지연이 변하는 경우에는 정렬 성능이 떨어진다.

3.2 POC (Phase-Only Correlation)를 이용한 정렬 방법

POC 를 이용한 신호 정렬 방법은 정렬하고자 하는 신호를 퓨리에 변환 (Fourier transform)하여 두 신호의 위상 성분을 추출하고, 위상 성분의 차로부터 시간 지연을 찾아내는 방법이다[18]. 임의의 두 신호 $x(n)$과 $y(n)$을 퓨리에 변환하면 다음과 같이 나타낼 수 있다.

$$X(k)=\sum_{n=0}^{N-1}x(n)W_N^{kn}=A_X(k)e^{j\theta_X(k)}$$
$$Y(k)=\sum_{n=0}^{N-1}y(n)W_N^{kn}=A_Y(k)e^{j\theta_Y(k)}, \quad (6)$$

여기서 W_N^{kn}은 $e^{j2\pi kn/N}$이다. $x(n)$과 $y(n)$의 주파수 응답 $X(k)$와 $Y(k)$은 위의 식과 같이 크기 성분 $A_X(k)$, $A_Y(k)$와 위상 성분$e^{j\theta_X(k)}$,$e^{j\theta_Y(k)}$의 곱으로 나타낼 수 있으며, 상호 위상 스펙트럼 (cross-phase spectrum) $R_{XY}(k)$는 다음과 같이 정의된다[18]

$$R_{XY}(k)=\frac{X(k)Y^*(k)}{|X(k)Y^*(k)|}=e^{j\theta_{XY}(k)}, \quad (7)$$

여기서 *는 복소 켤레 (complex conjugate)를 의미한다. 식 (7)에서 만약 $x(n) = y(n)$이라면 $R_{XY}(k)$는 크로네커 델타 (kronecker delta)이고, $y(n) = x(n-n_0)$, 즉 $y(n)$이 임의의 지연 n_0를 가지는 $x(n)$과 동일하다면 다음과 같은 결과를 얻을 수 있다[18]

$$R_{XY}(k)=\frac{X(k)Y^*(k)}{|X(k)Y^*(k)|}\simeq e^{j\frac{2\pi}{N}kn_0}. \quad (8)$$

즉, 두 신호가 시간 지연된 동일한 신호라면 $R_{XY}(k)$는 두 신호의 위상차와 같고, $R_{XY}(k)$를 역 퓨리에 변환 (inverse Fourier transform)하면 다음과 같은 결과를 얻을 수 있다.

$$r_{xy}(n)=\frac{1}{N}\sum_{k=0}^{N-1}R_{XY}(k)W_N^{-kn}$$
$$\simeq\frac{alR}{N}\frac{\sin\pi(n+n_0)}{\sin\frac{\pi}{N}(n+n_0)} \quad (9)$$

식 (9)에서 얻어지는 결과는 시간 영역에서 n_0만큼 지연된 sinc 함수를 의미하므로, $r_{XY}(n)$을 관찰하면 두 신호의 시간 지연 정도를 알 수 있다. 이 방법은 반복 계산을 하지 않고 두 신호의 시간 지연 정도를 쉽게 찾을 수 있는 장점이 있지만, 두 신호의 유사성이 높아야 하고 한 파형 내에서 지연이 균일해야 한다는 전제조건을 만족하는 경우에만 정렬 성능이 보장된다는 단점이 있다.

3.3 보간과 추출을 이용한 정렬 방법

보간 (interpolation)과 추출 (decimation)을 이용한 신호 정렬 방법은 부채널 공격 대응 방법 중 하나인 랜덤 클럭을 극복하기 위한 방법이다[19]. 이 방법은 측정된 신호의 시간 간격을 조절하여 보간과 추출 방법을 이용해 샘플수를 늘리거나 줄여 샘플수가 바뀐 여러 개의 신호를 만들어 낸다. 이렇게 만들어진 신호들을 시간 축 상에서 이동시켜 가면서 기준신호와의 상관 계수를 구하고, 가장 큰 상관 계수를 가진 신호를 기준 신호와 정렬된 신호로 판단한다. 이 방법은 [그림 2]와 같이 랜덤 클럭으로 인해 측정된 신호들 간에 상관도가 떨어지는 경우에도 효과적으로 대처할 수 있다. 그러나 [그림 3]과 같이 한 파형 내에서 시간지연이 변화하는 경우에는 효과적으로 대처할 수 없는 한계가 있다.

IV. 피크 매칭을 이용한 제안된 신호 정렬 방법

PA 공격의 성능을 보장하기 위해서는 가능한 모든 시간 왜곡에 대응해야 하므로, 본 논문에서는 기준 신호와 정렬할 신호의 상관관계를 이용하지 않고 두 신호가 동일한 암호화 과정을 수행하였다는 사실에 입각하여 피크를 정렬하는 방법을 제안한다. 즉, 클럭이 변하더라도 동일한 암호화 과정이 수행되고 발생하는 피크의 수는 항상 동일하므로, 기준 신호의 피크에 정렬할 신호들의 피크를 일치시킴으로써 신호를 정렬시킬 수 있다. 구체적인 정렬 방법은 다음과 같은 순서

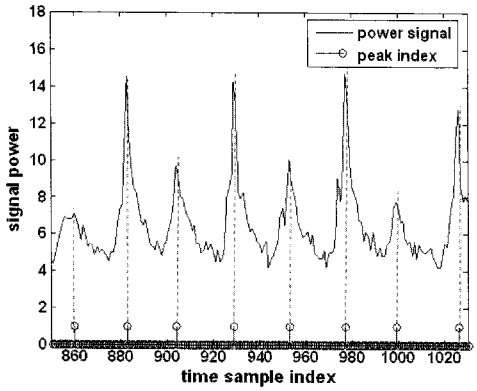
로 진행된다.

(1) 측정된 전력 신호에서 피크 인덱스를 구하기 위해, 측정된 전력 신호를 고주파에 의해 발생할 수 있는 작은 피크들을 없애고 암호화 동작의 클럭 주파수는 통과할 수 있는 저대역 통과 필터 (lowpass filter, LPF)에 통과시킨다.

(2) [그림 4]와 같이 LPF를 통과한 신호로부터 주요 피크 지점에 해당하는 인덱스의 근사치를 구할 수 있고, LPF를 통과하기 전의 원 전력 신호에서 근사치 값 주변의 피크 지점을 탐색한다.

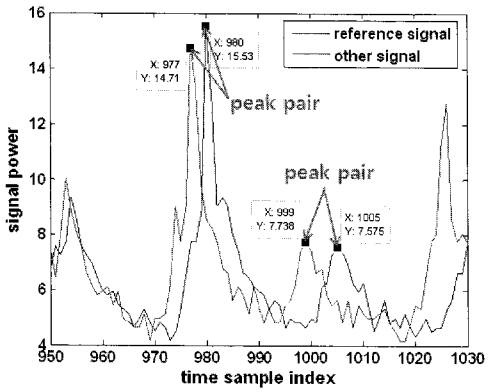
(3) 측정된 전력 신호들 중에서 임의로 기준 신호를 정한 후 [그림 5]와 같이 기준 신호의 피크에 대응하는 정렬할 신호들의 피크 (peak pair)를 찾아 매핑(mapping)한다.

(4) 피크 사이의 샘플 수가 일치하면 피크의 위치를 일치 시킨 후 그대로 저장하고, 샘플 수가 일치하지 않으면 보간법(interpolation)을 이용해 기준신호와 같은 샘플 수를 가지고 그 샘플에서의 크기 값을 추정하여 저장한다.

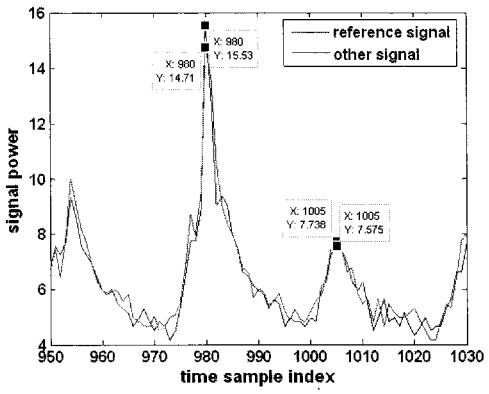


[그림 4] 의미 있는 피크 지점에 해당하는 인덱스.

제안된 방법은 한 파형 내에서 지연이 변하는 경우에도 피크 지점을 일치시킨 후 보간을 이용해 신호를 적절히 변형시킴으로써 동일한 암호화 시점을 맞추는 장점이 있다. 제안된 방법을 이용하여 정렬을 수행한 결과는 [그림 6]에 제시되어 있으며, [그림 5]에서 불규칙한 시간 지연을 보였던 신호가 잘 정렬되어 있음을 볼 수 있다. 제안된 방법은 보간법을 이용해 신호를



[그림 5] 정렬 전 전력 신호 파형의 예.



[그림 6] 정렬 후 전력 신호 파형의 예.

[표 1] 각 정렬 방법의 연산량 비교

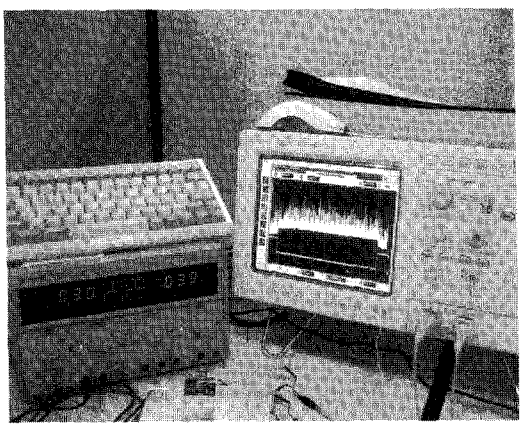
정렬 방법	연산량	모의실험에 사용된 변수 값	모의실험 연산량 결과
상관계수 정렬	$n[(7N+1)+(3N+19)]=n(10N+20)$	N=6,880 n=45 N'=8,192 l=7 m=30	3,096,900
POC 정렬	$[(2N'log_2N'+6N')+(N'log_2N'+15N')]=3N'log_2N'+21N'$		491,520
보간과 추출을 이용한 정렬	$[(nl(7N+1)+3N)+(nl(3N+19)+2N)]=nl(10N+20)+5N$		21,712,700
제안된 피크 매칭 정렬	$[((m-1)N+3N)+(mN+2N)]=(2m-1)N+5N$		440,320

변형한 후 반복적인 상관연산을 통해 정렬을 수행하는 기존 방법과 달리 LPF와 부분적인 보간법 연산을 수행하므로 상대적으로 연산량이 작은 이점이 있는데, 이를 확인하기 위해 기존 방법들과 제안된 방법의 연산량을 비교해 보면 다음과 같다. 우선 제안된 방법의 연산량을 구해보면 다음과 같다. 총 연산량은 대략적으로 합과 곱의 연산량의 합으로 볼 수 있으므로, 각 연산단계에서 필요한 연산량을 '[(합의 연산량)+(곱의 연산량)]=총 연산량'으로 표현해 구해보면 다음과 같다. 전력 신호의 길이를 N이라고 하고 LPF의 길이를 m이라고 하면, 신호를 LPF를 통과시키는 경우 $[(m-1)N+(m)N]=(2m-1)N$의 연산량이 필요하다. LPF를 통과한 신호로부터 피크 점을 찾아 피크 점 사이를 선형 보간법으로 정렬할 경우, 대략 신호의 총 길이만큼 보간 연산을 하게 된다고 가정하면 $[(3N)+(2N)]=5N$의 연산량이 요구된다. 따라서 제안된 피크 매칭 방법을 이용하여 신호를 정렬할 경우, 하나의 전력 신호를 정렬하기 위해 요구되는 총 연산량은 대략적으로 $[((m-1)N+3N)+(mN+2N)]=(2m-1)N+5N$ 이 된다.

상관 계수를 이용한 정렬 방법의 경우 길이 N인 전력 신호 하나를 정렬하는 데 필요한 연산량을 계산해 보면 다음과 같다. 우선 분자인 x, y 편차 곱의 평균에 대한 연산량은 $[(5N-3)+(N+3)]=6N$이고, 분모의 표준 편차는 편차 제곱의 평균의 제곱근을 나타내므로 앞에서 x, y의 편차 값과 평균 값은 저장되어 있는 경우 $[(2N+4)+(2N+16)]=4N+20$의 연산량을 가진다. 그리고 분모와 분자의 연산을 하게 되면 상관계수를 한 번 구하는데 $[(7N+1)+(3N+19)]=10N+20$의 연산이 필요하므로, 이를 시간축 상에서 이동 시켜 가면서 총 n번의 상관계수를 구할 경우 총 연산량은 $n[(7N+1)+(3N+19)]=n(10N+20)$이 된다.

다음으로 POC를 이용한 정렬 방법의 경우에 대해 구해보면, 이 정렬 방법의 연산량은 고속 퓨리에 변환 (Fast Fourier Transform, FFT)을 이용하여 줄일 수 있다. 길이 N의 신호를 FFT하기 위한 연산량은 $[(N'log_2N')+(\frac{N'}{2}log_2N')]=\frac{3N'}{2}log_2N'$ 이다. 여기서 N'은 N보다 작지 않은 가장 작은 2^k값이다. 퓨리에 변환 후에 식 (8)과 같이 $R_{XY}(k)$를 구하는데 복소수의 곱과 복소수 값의 크기를 계산하면 $[(6N')+(15N')]=21N'$의 연산량을 갖는다. IFFT와 FFT의 연산량은 같으므로 POC 정렬 방법은 하나의 전력 신호를 정렬하는 데, 총 $[N'(2log_2N'+6)+N'(log_2N'+15)]=3N'log_2N'+21N'$의 연산량이 필요하다.

보간과 추출을 이용한 정렬 방법의 경우 한 전력신호를 정렬하는 데 필요한 연산량을 계산해 보면, 시간을 확대/축소시켜 새로운 시간 인덱스에서의 값을 계산한 후, 총 전력 신호 길이만큼의 선형 보간 계산을 수행해야 하므로 시간을 확대/축소시킬 때 마다 $[(3N)+(2N)]=5N$ 의 연산을 한다. 이렇게 만든 신호를 지연 정도를 n번 바꿔가면서 상관계수를 구하는데 상관계수 정렬 방법에서 구한 총 연산량만큼 더 늘어나고, 시간을 확대/축소시키는 횟수만큼 앞의 연산을 반복해야 하므로, 시간의 확대/축소 횟수를 l이라고 하면 보간과 추출을 이용한 정렬의 총 연산량은 $[(nl(7N-5)+3N)+(nl(3N+7)+2N)]=nl(10N+2)+5N$ 이 된다. 이상의 결과를 정리하여 각 정렬 방법의 연산량을 비교해 보면 [표 1]과 같으며, [표 1]에서 보듯이 제안된 방법이 다른 정렬 방법에 비해 작은 연산량을 가짐을 알 수 있다.



[그림 7] 무선 센스 네트워크 장치 "mote Ⅳ", 전력 공급기, 오실로스코프를 간춘 실험 환경

Ⅴ. 모의실험 결과 및 성능 분석

제안된 신호 정렬 방법의 성능을 확인하기 위해, [그림 7]과 같이 "mote Ⅳ"라는 무선센서 네트워크 장치에서 AES 암호화 알고리즘이 동작할 때 측정된 총 4,000개의 전력 소비 파형을 이용하여 DPA와 CPA 공격을 각각 수행하였다. 암호화 장치의 내부 클럭과 측정 장치의 샘플링 주파수는 각각 8 MHz 와 200 MHz였다. 피크 신호 사이를 보간하는 방법으로는 여러 보간법의 이용이 가능하나, 연산량이 작고 구현이 간단한 선형 보간법을 사용하였다. 그리고 전력

신호들 중 피크 사이의 간격이 비교적 일정한 신호를 기준 신호로 하여 정렬에 대한 성능 확인을 하였다. PA 공격 결과의 신뢰도는 PA 공격 연산에서 비밀 키로 추측한 추정 키일 때의 대푯값과 이를 제외한 나머지 추정 키 중 가장 큰 대푯값의 차이 비율을 나타내는 MDR (Maximum Difference Ratio)[23]의 평균과 분산을 이용해 확인할 수 있다.

$$E[MDR_i] = \frac{\sum_{i=k}^{N} MDR_i}{N-k+1}$$
$$var[MDR_i] = \frac{\sum_{i=k}^{N} (MDR_i - E[MDR_i])^2}{N-k+1} \quad (10)$$
$$\left(MDR_i = \frac{\max_{tr}(X_i) - \max 2_{tr}(X_i)}{\max_{tr}(X_i)} \right)$$

비밀 키를 찾고 난 후에 사용되는 전력 신호의 수가 많아질수록 신호의 통계적 특성이 향상되므로 공격의 성공을 판단하기 위해서는, 비밀 키로 추측한 추정 키의 대푯값과 이를 제외한 추정 키의 대푯값이 확연히 구분되어야 하므로 MDR의 평균이 큰 값을 가질수록 신뢰도가 높다. 그리고 사용된 소비 전력 신호수에 따라 두 대푯값의 차이가 감소하는 경우는 신뢰도가 달라질 수 있음을 의미하므로 MDR의 분산이 작아야 추측한 키가 암호화에 사용된 비밀 키일 확률이 높아진다. 그러므로 MDR 값의 평균과 분산을 확인하여 정렬 방법들의 성능을 비교하였다.

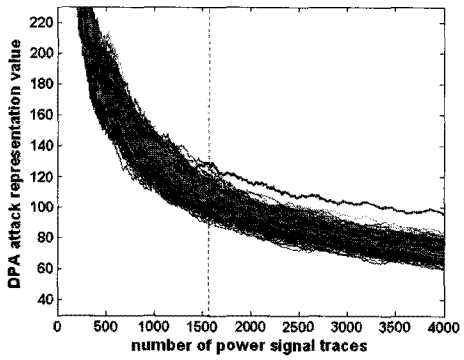
정렬이 되지 않은 원 신호, 기존의 정렬 방법으로 정렬된 신호, 그리고 제안된 피크 매칭 방법을 이용해 정렬된 신호에 대해 DPA 공격을 수행했을 때 필요한 최소 전력 신호 개수를 [표 2]에 나타내었고, CPA 공격을 수행했을 때 필요한 최소 전력 신호 개수는 [표 3]에 제시하였다. 여기서 'Fail'은 주어진 4,000개의 신호 내에서 비밀 키를 찾아내는데 실패했음을 의미한다. [표 2]에서 볼 수 있듯이 정렬되지 않은 신호를 이용해 DPA 공격을 하였을 때는 모든 경우에 공격에 실패하는 것을 볼 수 있다. 이러한 공격 실패의 이유는 H/W 또는 측정 시의 오차에 의한 영향이 크게 나타나 측정된 전력 신호 파형이 시간 축 상에서 제대로 정렬되지 않았기 때문이다. 다음으로 상관 계수 정렬 방법과 보간과 추출 방법을 이용한 정렬방법의 결과를 살펴보면 몇몇의 경우에서 4,000개 내의 신호에서 찾을 수 있는 경우를 볼 수 있으나, 대부분 4,000개 근처에서 공격에 성공하였으므로 신뢰도가 낮아 추정된 키가 비밀 키라고 보기 어렵다. 이러한 결과는 신호 전체의 상관관계를 이용하여 지연을 구하는 정렬방법의 특성상 파형들이 오로지 시간차의 함수로만 표현되는 경우를 제외하고는 파형 내에서 발생하는 지연 등을 제대로 보상할 수 없기 때문이다. POC 정렬을 이용한 경우도 상관 계수 또는 보간과 추출 방법을 이용한 정렬방법과 유사한 성능을 보이는데, 이는 소비 전력 신호 간에 높은 유사성이 보장되지 않아 위상정보로부터 도출되는 지연 정보가 부정확해지므로 신호를 제대로 정렬할 수 없기 때문이다. 이에 반해 제안된 방법을 이용한 경우를 살펴보면 모든 비밀 키에 대해 공격에 성공하였음을 볼 수 있으며, 요구되

[표 2] DPA 공격시 요구되는 최소 전력 신호 개수

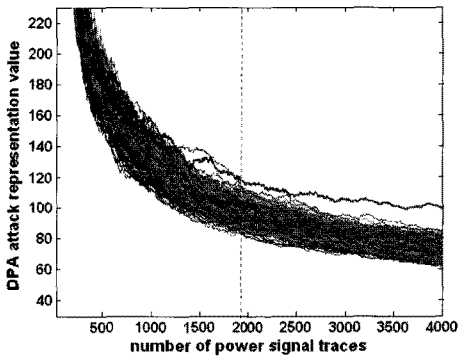
key No.	정렬 전 신호	상관계수 정렬	POC 정렬	보간과 추출을 이용한 정렬	제안된 피크 매칭 정렬
1	Fail	3,997	Fail	3,053	712
2	Fail	3,420	3,858	2,826	770
3	Fail	3,805	Fail	Fail	868
4	Fail	3,921	3,859	2,325	853
5	Fail	3,999	Fail	Fail	1,321
6	Fail	Fail	Fail	2,946	933
7	Fail	2,850	Fail	2,745	1,772
8	Fail	3,130	3,154	2,185	1,063
9	Fail	3,841	Fail	Fail	1,879
10	Fail	Fail	Fail	3,673	588
11	Fail	Fail	Fail	Fail	1,732
12	Fail	Fail	3,995	3,922	1,192
13	Fail	1,547	1,879	1,540	917
14	Fail	Fail	Fail	Fail	849
15	Fail	Fail	Fail	3,929	1,215
16	Fail	1,400	1,868	1,428	757

〔표 3〕 CPA 공격시 요구되는 최소 전력 신호 개수

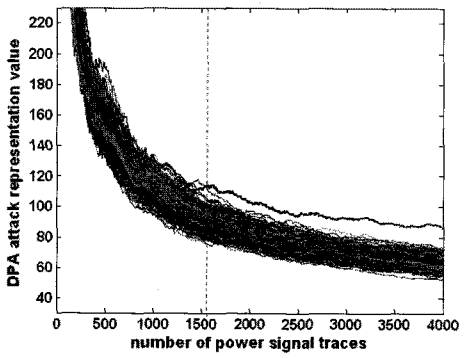
key No.	정렬 전 신호	상관계수 정렬	POC 정렬	보간과 추출을 이용한 정렬	제안된 피크 매칭 정렬
1	1,300	3,167	257	1,425	249
2	520	1,278	750	1,194	400
3	2,050	1,448	390	433	362
4	1,510	608	1,085	989	423
5	2,980	1,687	780	1,191	429
6	2,710	1,775	Fail	2,528	1,493
7	3,750	751	660	1,287	1,030
8	Fail	1,219	1,205	1,833	1,481
9	Fail	2,216	882	1,683	921
10	3,090	1,414	1,443	921	1,825
11	Fail	1,130	1,413	2,357	1,133
12	Fail	1,408	2,571	2,048	3,274
13	Fail	2,131	680	895	825
14	Fail	882	729	695	609
15	Fail	3,884	3,752	3,951	1,278
16	Fail	Fail	2,463	3,311	3,341



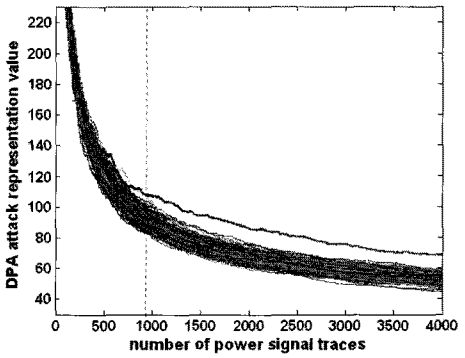
(a) 상관 계수를 이용한 정렬
($E[MDR_i] \approx 7.89 \times 10^{-2}$, $var[MDR_i] \approx 7.62 \times 10^{-4}$)



(b) POC 정렬
($E[MDR_i] \approx 8.61 \times 10^{-2}$, $var[MDR_i] \approx 16.0 \times 10^{-4}$)

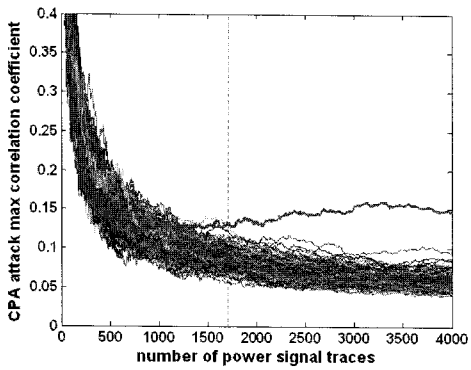


(c) 보간과 추출을 이용한 정렬
($E[MDR_i] \approx 9.36 \times 10^{-2}$, $var[MDR_i] \approx 12.0 \times 10^{-4}$)

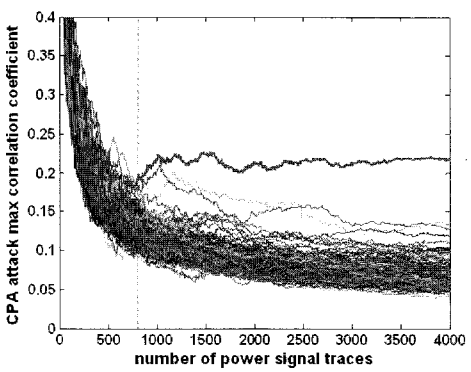


(d) 제안된 피크 매칭을 이용한 정렬
($E[MDR_i] \approx 11.4 \times 10^{-2}$, $var[MDR_i] \approx 6.50 \times 10^{-4}$)

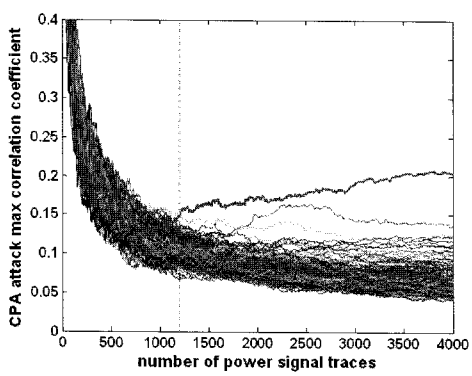
〔그림 8〕 각 정렬 방법으로 정렬된 신호를 이용하여 DPA 공격을 수행한 결과



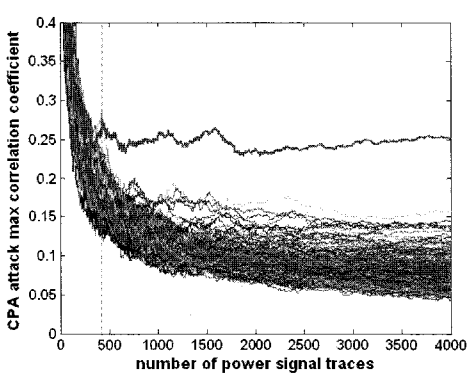
(a) 상관 계수를 이용한 정렬
($E[MDR_i] \approx 2.85 \times 10^{-1}$, $var[MDR_i] \approx 9.2 \times 10^{-3}$)



(b) POC 정렬
($E[MDR_i] \approx 2.56 \times 10^{-1}$, $var[MDR_i] \approx 11.2 \times 10^{-3}$)



(c) 보간과 추출을 이용한 정렬
($E[MDR_i] \approx 1.88 \times 10^{-1}$, $var[MDR_i] \approx 8.1 \times 10^{-3}$)



(d) 제안된 피크 매칭을 이용한 정렬
($E[MDR_i] \approx 3.14 \times 10^{-1}$, $var[MDR_i] \approx 4.7 \times 10^{-3}$)

[그림 9] 각 정렬 방법으로 정렬된 신호를 이용하여 CPA 공격을 수행한 결과

는 최소 전력 신호의 수도 다른 정렬 방법에 비해 크게 감소하였음을 확인할 수 있다. 이러한 성능 향상은 제안된 방법이 전력 신호를 단순히 시간적 이동을 시키는 다른 정렬 방법들과는 달리 같은 암호화 동작에 의해 발생하는 전력 피크를 일치시켜 정렬을 수행하기 때문에, 신호 내에서 발생하는 불규칙한 시간지연 등에도 잘 대처할 수 있기 때문이다.

DPA 공격 시 필요한 전력 신호 개수만이 아니라 추측한 비밀 키의 신뢰도도 커야 실제 비밀 키를 바르게 추정했다고 할 수 있다. 따라서 신뢰 정도를 확인할 수 있는 MDR의 비교를 위해 [표 2]에서 4가지 정렬방법이 모두 공격에 성공한 13번째 비밀 키에 대해, 사용된 전력 파형의 수에 대한 대푯값의 변화를 [그림 8]에 도시하였다. [그림 8]에서 256개의 결과는 사용된 전력 신호 개수 당 각 추정 키의 DPA 연산 결과 대푯값을 나타내고, 점선은 공격이 성공한 최소 전력 신호의 수를 나타낸다. [그림 8].(a)부터 (c)에서 보듯이 비밀 키를 찾은 후, 기존의 정렬 방법들은 비밀 키와 다른 추정 키의 대푯값 차이가 작아 제안된 정렬 방법에 비해 MDR의 평균이 작은 것을 알 수 있고, 대푯값 차이가 감소하는 경우를 볼 수 있으므로 MDR의 분산이 커져 신뢰도가 줄어든다. 이에 반해 [그림 8].(d)에서 보는바와 같이 제안된 방법은 공격에 성공한 이후 MDR의 평균이 비교적 크고 분산은 작으므로, 여타 방법들에 비해 제안된 방법이 신뢰도가 높음을 알 수 있다.

다음으로 CPA 공격을 수행했을 때의 결과는 [표 3]에 제시되어 있다. [표 3]에서 보듯이 CPA 공격을 수행한 경우에는 [표 2]에 제시된 DPA 공격 결과와는 달리 대부분의 정렬 방법이 공격에 성공을 하였음을 볼 수 있으며, 이는 II-2절에서 설명한 바와 같이 CPA 공격이 정렬 오차에 대해 상대적으로 강인하기

때문이다. 그러나 상관계수를 이용한 정렬방법과 POC 정렬을 이용한 방법의 경우에는 각각 하나의 비밀 키에 대해 공격에 실패하였으며, 보간과 추출 방법의 경우에는 모든 비밀 키에 대해 공격에 대해 성공하였으나 POC 정렬을 이용한 경우와 비교해 볼 때 사용된 신호의 개수는 큰 차이가 없음을 볼 수 있다. 이에 반해 제안된 방법을 이용했을 때는 모든 경우에서 공격이 성공하였고, 공격 성공에 필요한 신호의 개수가 보간과 추출을 이용한 정렬을 했을 때 평균 약 1,700개인 반면에 제안한 방법을 이용해 정렬을 했을 때 평균 약 1,200개로 30% 정도 줄어들었음을 확인할 수 있다.

공격의 효율성 측면이외에 제안된 방법의 신뢰성을 살펴보기 위해, 사용된 전력 신호에 대한 상관계수 값을 살펴보면 [그림 9]와 같다. [그림 9]는 [표 3]의 5번째 비밀 키에 대한 CPA 연산 결과를 도시한 것으로, 각 그림의 256개 결과는 사용된 전력 신호 개수당 각 추정 키의 CPA 연산 결과 상관 계수를 나타낸다. [그림 9]에서 보듯이 비밀 키일 경우에는 다른 추정 키들에 비해 높은 상관계수를 유지하는 것을 볼 수 있다. 특히 [그림 9].(d)의 제안된 방법의 상관계수를 보면 다른 정렬 방법들에 비해 MDR의 평균은 크고, 분산은 작아 신뢰도 측면에서도 우수함을 확인할 수 있다. 이렇게 제안된 방법이 다른 정렬 방법들에 비해 높은 신뢰도를 가지는 것은 파형을 단순히 시간이동 또는 축소/확대시키는 기존 방법과는 달리, 피크 점을 기준으로 하여 신호를 정렬함으로써 파형 내에서 발생하는 시간 지연에도 효과적으로 대처할 수 있기 때문이다.

VI. 결 론

본 논문에서는 모바일 보안에 사용되는 암호화 알고리즘의 부채널 공격법 중의 하나인 전력 분석 공격의 성능을 보장하기 위한 새로운 신호 정렬 방법을 제안하였다. 제안된 방법은 상관연산이나 위상 차를 이용하는 기존 방법과 달리 동일한 암호화 동작을 측정한 신호들의 피크 점을 찾아 신호를 정렬하므로, 랜덤 클럭이나 H/W의 불안정성 또는 측정 간에 발생할 수 있는 오차에 강건하게 대응할 수 있는 장점이 있어 전력 분석 공격의 효율성과 신뢰도를 향상시킬 수 있는 이점이 있다. 이러한 결과는 신호의 오정렬을 유발하여 전력 분석 공격을 막기 위한 대응 방법에 대해서도 공격이 가능해짐을 의미하므로, 전력 분석 공격이 가능한 범위의 확장뿐만 아니라 이에 대한 대응책 개발에도 크게 기여할 수 있을 것으로 기대된다.

참고문헌

[1] IEEE standard, "Part 11: Wireless LAN Medium Access Control(MAC) and PHysical Layer(PHL) specifications," IEEE Std. 802.11-2007.

[2] IEEE standard, "Part 16: Air interface for fixed broadband wireless access systems," IEEE Std. 802.16e-2009.

[3] National Institute of Standards and Technology, "Advanced Encryption Standard(AES)," Federal Information Processing Standards Publication 197, Nov. 2001.

[4] National Bureau of Standards, "Data Encryption Standard(DES)," Federal Information Processing Standards Publication 46-3, Oct. 1999.

[5] Korean Internet Security Agency, "The SEED encryption algorithm," IETF RFC 4269, Dec. 2005.

[6] 김종환, 신경욱, "AES 기반 와이브로 보안 프로세서 설계," 전자공학회논문지, 44(7), pp. 71-80, 2007년 7월.

[7] P.C. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," Advances in Cryptology, CRYPTO'96, LNCS 1109, pp. 104-113, 1996.

[8] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," Advances in Cryptology, CRYPTO'99, LNCS 1666, pp. 388-397, 1999.

[9] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," Proceedings of Cryptographic Hardware and Embedded Systems - CHES 2004, LNCS 3156, pp. 16-29, 2004.

[10] K. Gandolfi, C. Mourtel, and F. Oliver, "Electromagnetic analysis : Concrete

results," Proceedings of Cryptographic Hardware and Embedded Systems - CHES 2001, LNCS 2162, pp. 251-261, 2001.

[11] J.-J. Quisquater and D. Smyde, "Electro-Magnetic Analysis (EMA) : Measures and countermeasures for smart cards," Proceedings of Smart Card Programming and Security, LNCS 2140, pp. 200-210, 2001.

[12] 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.

[13] 류정춘, 한동국, 김성경, 김희석, 김태현, 이상진, "웨이블릿 기반의 차분전력분석 기법 제안," 정보보호학회논문지, 19(3), pp.27-34, 2009년 6월.

[14] 김완진, 송경원, 이유리, 김호원, 김형남, "웨이블릿 잡음 제거 방법을 이용한 전력 분석 공격 성능 개선," 한국통신학회논문지, 35(9), pp. 1330-1341, 2010년 9월.

[15] 이유석, 이유리, 이영준, 김형남, "차분 전력 분석 공격의 성능 향상을 위한 전처리 기법," 정보보호학회논문지, 20(4), pp. 3-9, 2010년 8월.

[16] C. Herbst, E. Oswald, and S. Mangard, "An AES smart card implementation resistant to power analysis attacks," Proceedings of Applied Cryptography and Network Security, LNCS 3989, pp. 239-252, 2006.

[17] O. Kömmerling and M.G. Kuhn, "Design principles for tamper-resistant smartcard processors," Proceedings of the USENIX Workshop on Smartcard Technology, Smartcard'99, pp. 9-20, May, 1999.

[18] N. Homma, S. Nagashima, Y. Imai, T. Aoki, and A. Satoh, "High-resolution side-channel attack using phase-based waveform matching," Proceedings of Cryptographic Hardware and Embedded Systems - CHES 2006, LNCS 4249, pp. 187-200, 2006.

[19] 박제훈, 문상재, 하재철, 이훈재, "차분 전력 분석 공격을 위한 향상되고 실제적인 신호 정렬 방법," 정보보호학회논문지, 18(5), pp. 93-101, 2008년 10월.

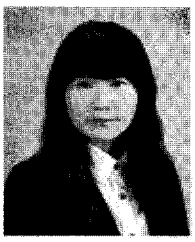
[20] T.S. Messerges, E.A. Dabbish, and R.H. Sloan, "Examining smart-card security under the threat of power analysis attacks," IEEE Transactions on Computers, vol. 51, no. 5, pp. 541-552, May 2002.

[21] R. Bevan and E. Knudsen "Ways to enhance differential power analysis," Proceedings of Information Security and Cryptology - ICISC 2002, LNCS 2587, pp. 327-342, 2003.

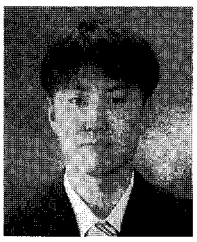
[22] S. Mangard, E. Oswald, and T. Popp, Power analysis attacks: Revealing the secrets of smart cards, Springer, pp. 123-136, Mar. 2007.

[23] Kyung-Won Song, You-Seok Lee, and Hyoung-Nam Kim, "Performance improvement of the DPA attack based on wavelet denoising," Proceedings of International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC), pp. 1312-1315, July. 2009.

〈著者紹介〉

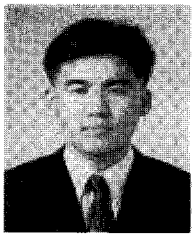


이 유 리 (Yu-Ri Lee) 학생회원
2010년 2월: 부산대학교 전자전기공학부 졸업
2010년 3월~현재: 부산대학교 전자전기공학과 석사과정
〈관심분야〉 부채널 공격, 디지털 방송신호처리



김 완 진 (Wan-Jin Kim) 학생회원
2005년 2월: 부산대학교 전자전기공학부 졸업
2007년 2월: 부산대학교 전자전기공학과 석사
2007년 3월~현재: 부산대학교 전자전기공학과 박사과정
〈관심분야〉 적응신호처리, 디지털 통신, SCA, 레이더 및 소나 신호처리

이 영 준 (Young-Jun Lee) 학생회원
2006년 2월: 부산대학교 전자전기공학부 졸업
2008년 2월: 부산대학교 전자전기공학과 석사
2008년 3월~현재: 부산대학교 전자전기공학과 박사과정
〈관심분야〉 디지털 방송신호처리, 적응신호처리, 부채널 공격



김 형 남 (Hyoung-Nam Kim) 정회원
1993년 2월: 포항공과대학교 전자전기공학과 졸업
1995년 2월: 포항공과대학교 전자전기공학과 석사
2000년 2월: 포항공과대학교 전자전기공학과 박사
2000년 3월~2003년 2월: 한국전자통신연구원 선임연구원
2003년 3월~2007년 2월: 부산대학교 전자전기통신공학부 조교수
2007년 3월~현재: 부산대학교 전자전기공학부 부교수
〈관심분야〉 적응신호처리, 레이더 신호처리, 디지털 방송신호처리, BCI