피크 매칭을 이용한 향상된 부채널 신호 정렬 방법

이 유 리, 김 완 진, 김 형 남
부산대학교 전자전기공학과

An improved alignment method for side-channel signals using peak matching

Yu-Ri Lee, Wan-Jin Kim, and Hyoung-Nam Kim
School of Electrical Engineering, Pusan National University
hnkim@pusan.ac.kr

Abstract: 부채널 공격 방법 중 전력 분석 공격은 매우 효과적이고 강력한 공격 방법으로 알려져 있으나, 공격 성능을 보장하기 위해서는 잘 정렬된 전력 신호가 요구된다. 그러나 실제 전력 신호를 측정할 때는 측정 오차나 랜덤 클럭과 같은 부채널 공격 대응 방법 등으로 인해 시간 왜곡이 발생하게 되고, 이로 인해 오정렬(misalignment) 문제가 야기된다. 오정렬 문제를 해결하기 위해 다양한 정렬 방법이 제안되었으나, 기존 방법들은 많은 계산량이 요구되며, 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, 제안한 방법이 다른 정렬방법보다 DPA 공격에 있어서 더 효과적임을 보인다.

Keywords: Power Analysis, Misalignment, DPA, Peak detection

Ⅰ. 서 론

스마트 카드나 RFID와 같은 장치에서는 데이터의 기밀성을 보장하기 위해 이론적인 안정성이 입증된 AES, DES 등의 다양한 암호화 알고리즘들이 사용되고 있으나, H/W상에서 암호화 알고리즘이 동작하며 발생되는 누설 정보들을 이용하여 비밀 키를 알아내는 부채널 공격(Side Cannel Attacks, SCA)이 등장하면서 정보보안은 큰 위협에 직면하게 되었다. SCA 공격방법에는 다양한 방식이 존재하나, 그 중에서도 전력 분석 (Power Analysis, PA) 공격은 대부분의 암호화 알고리즘에 대해 가장 위협적이고 효과적인 공격방법으로 알려져 있다. 대표적인 PA 공격방법으로는 차분 전력 분석(Differential Power Analysis, DPA) 공격과 상관도 전력 분석(Correlation Power analysis, CPA) 공격이 있다 [1],[2].

PA 공격은 암호화 과정에서 발생하는 정보의 통계적 특성에 근간한 방법이므로, 수집된 전력 신호들 간의 정렬 상태가 양호해야 하나, 현실적으로는 측정 시의 오차나 H/W의 불안정성으로 인해 정렬이 완벽하지 못하므로 PA 공격 성능이 저하되는 문제가 상존한다. 게다가, SCA 공격에 대한 방어책으로 랜덤 지연 시간을 삽입하거나 랜덤 클럭을 이용하여 의도적으로 전력 신호에 시간왜곡을 발생시키는 경우도 있으므로 [3],[4], PA 공격의 성능을 보장하기 위해서는 수집된 전력 신호를 잘 정렬하기 위한 방법이 요구된다.

전력 신호 정렬방법에는 전력 신호들 간의 상관관계를 이용해 정렬하는 방법과 수집된 전력 신호들을 퓨리에 변환한 후 위상 차를 이용해 신호를 정렬하는 방법이 있다. 이러한 정렬 방법들은 전력 신호 내에서 시간 지연이 균일한 경우에는 효과적이나, 클럭이 임의적으로 변하거나 의도적으로 시간 왜곡을 발생시킨 경우에는 효과적으로 대처할 수 없는 단점이 있다 [5],[6]. 이러한 기존 정렬 방법의 단점을 극복하기 위해 보간과 추출을 이용해 전력 신호를 변형시킨 후 신호간의 상관관계를 이용해 신호를 정렬하는 방법이 제안되었으나 [6], 상관연산을 이용해 신호를 정렬하므로 많은 계산량이 요구되는 단점이 있다. 계산량이 낮으면서도 임의적인 클럭 변화와 의도적인 시간왜곡에 효과적으로 대처하기 위해, 본 논문에서는 전력 신호의 피크 점을 기준으로 신호를 보간 또는 추출함으로써 신호를 정렬하는 방법을 제안한다. 제안된 방법은 반복적인 상관관계를 이용하여 신호를 정렬하지 않으므로 상대적으로 계산량이 적고, 피크를 기준으로 신호를 정렬한 후에 보간 또는 추출을 이용해 피크간의 샘플 수를 동일하게 조정하므로 전력 신호 내에서 지연이 균일하지 않더라도 정렬이 가능한 장점이 있다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 신호 정렬 방법에 대해 간단히 설명하고, 3장에서는 제안하는 신호 정렬 방법에 대해 소개한다. 4장에서는 제안된 방법과 기존의 신호 정렬 방법을 이용해 정렬한 후, DPA 공격을 수행해 각 정렬 방법들의 성능을 평가한다. 마지막으로 5장에서 본 논문의 결론을 맺는다.

Ⅱ. 기존의 신호 정렬 연구

* 이 논문은 2008년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2008-0061842)

PA 공격을 효과적으로 수행하기 위해서는 측정된 모든 신호가 시간 축 상에서 잘 정렬된 상태여야 한다 [6]. 그러나 부채널 공격에서 신호의 정렬 문제는 측정된 전력 신호의 시작 시점이 상이하여 생기는 단순한 시간 지연뿐만 아니라, 클럭의 불균일성이나 잡음, 지터 (jitter)와 같은 H/W의 문제, 그리고 부채널 공격에 대한 방어책으로 사용되는 랜덤 클럭과 같은 다양한 요소에 의해 발생할 수 있다. 이러한 오정렬 (misalignment) 문제를 해결하기 위해 다양한 방법들이 제시되었으며, 본 절에서는 기존의 정렬 방법들에 대해 살펴본다.

1. 상관 계수를 이용한 정렬방법

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

$$C = \frac{E[(x(n) - E[x(n)])(y(n) - E[y(n)])]}{\sigma_x \sigma_y} \quad (1)$$

여기서 $E[]$는 평균값을 나타내고 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 인덱스 n을 증가시켜가면서 각 인덱스마다 두 신호의 상관도를 구한다. 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 높은 상관관계를 가지는 경우, 즉 단순히 시간 지연된 경우에는 매우 효과적이나 각 신호들이 임의의 클럭을 가지거나 신호 내에서 지연이 변하는 경우에는 정렬 성능이 떨어진다.

2. POC (Phase-Only Correlation)를 이용한 정렬방법

POC 방법은 정렬하고자 하는 신호를 퓨리에 변환 (Fourier transform)하여 두 신호의 위상 성분을 추출하고, 위상 성분의 차로부터 시간 지연을 찾아내는 방법이다 [5]. 임의의 두 신호 $x(n)$과 $y(n)$을 퓨리에 변환하면 다음과 같고

$$X(k) = \sum_{n=0}^{N-1} x(n) W_N^{kn} = A_X(k) e^{j\theta_X(k)} \quad , \quad (2)$$
$$Y(k) = \sum_{n=0}^{N-1} y(n) W_N^{kn} = A_Y(k) e^{j\theta_Y(k)}$$

여기서 W_N^{kn}은 $e^{j2\pi n/N}$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 [5].

$$R_{XY}(k) = \frac{X(k)\,Y^*(k)}{|X(k)\,Y^*(k)|} = e^{j\theta_{XY}(k)} \quad . \quad (3)$$

여기서 *는 복소 켤레 (complex conjugate)를 의미한다. 식 (3)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 [5].

$$R_{XY}(k) = \frac{X(k)\,Y^*(k)}{|X(k)\,Y^*(k)|} \simeq e^{j\frac{2\pi}{N}kn_0} . \quad (4)$$

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.

$$r_{xy}(n) = \frac{1}{N}\sum_{k=0}^{N-1} R_{XY}(k)\, W_N^{-kn} \quad (5)$$
$$\simeq \frac{\alpha}{N}\frac{\sin\pi(n+n_0)}{\sin\frac{\pi}{N}(n+n_0)}$$

식 (5)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. 보간과 추출을 이용한 정렬방법

보간 (interpolation)과 추출 (decimation)을 이용한 신호 정렬 방법은 부채널 공격 대응 방법 중 하나인 랜덤 클럭을 극복하기 위한 방법이다 [6]. 이 방법은 샘플링 지점 외의 신호 값을 주변의 측정된 신호 값을 이용하여 추정하고, 보간 및 추출 방법을 이용해 측정된 신호의 시간 간격을 조절하여 샘플수를 늘리거나 줄여 샘플수가 바뀐 여러 개의 신호를 만들어 낸다. 이렇게 만들어진 신호들을 시간 축 상에서 이동시켜가면서 기준신호와의 상관계수를 구하고, 가장 큰 상관계수를 가진 신호를 기준 신호와 정렬된 신호로 판단한다. 이 방법은 신호를 적절히 변형시켜 정렬하므로 랜덤 클럭으로 인해 측정된 신호들 간에 상관도가 떨어지는 경우에도 효과적으로 대처할 수 있다. 그러나 보간과 추출, 그리고 상관계수를 구하기 위해 많은 반복 연산이 요구되고, 한 파형 내에서 지연이 변화하는 경우에 대처하지 못하는 단점이 있다.

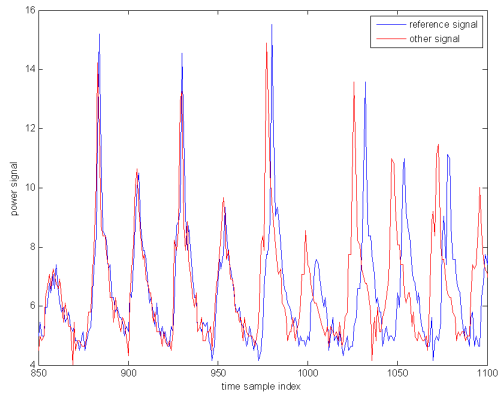

그림 1. 시간 왜곡이 발생한 전력 신호 파형 예.

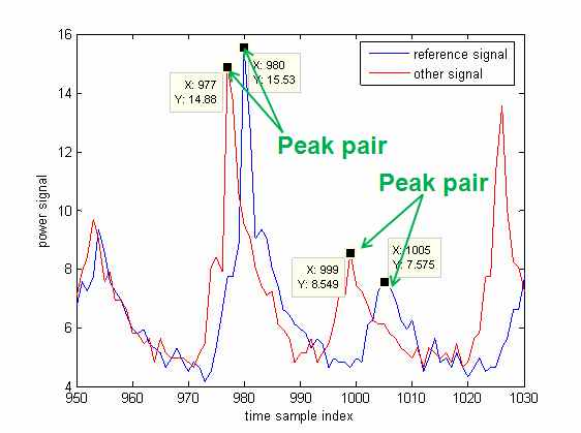

그림 2. 정렬 전 전력 신호 파형의 예.

III. 피크 매칭을 이용한 신호 정렬 방법

기존의 정렬 방법들은 단순히 측정된 전력 신호들의 시간 축 상에서의 위치가 어긋나 있거나, 파형이 압축 또는 확장된 경우에 대해 신호를 정렬하는 방법을 제시하였다 [5],[6]. 그러나 그림 1과 같이 한 파형 내에서 시간지연이 변화하는 경우에는 효과적으로 대처할 수 없는 한계가 있다. 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 있으며 구체적인 정렬 방법은 다음과 같다.

먼저 기준 신호와 정렬할 전력 신호의 피크 인덱스를 구하기 위해 측정된 전력 신호를 저대역 통과 필터(lowpass filter, LPF)에 통과 시켜 고주파에 의해 발생할 수 있는 작은 피크들을 없앤다. LPF를 통과한 신호로부터 의미 있는 피크 지점에 해당하는 인덱스의 근사치를 구할 수 있고, 원 전력신호에서 근사치 값 주변의 피크 지점을 탐색해 매핑 (mapping)한다. 다음으로 측정된 전력 신호들 중에서 임의로 기준 신호를 정한 후 그림 2와 같이 기준 신호의 피크에 대응하는 정렬할 신호들의 피크(peak pair)를 찾는다. 이 때, 피크 사이의 샘플 수가 일치하면 피크의 위치를 일치 시킨 후 그대로 저장하고, 만약 다르다면 보간 (interpolation) 또는 축소 (decimation)를 이용해 기준신호와 피크 사이의 샘플 수가 일치되도록 조절한다.

제안된 방법은 보간 또는 축소를 이용해 신호를 변형한 후 반복적인 상관연산을 통해 정렬을 수행하는 기존 방법과 달리 LPF와 부분적인 보간 및 축소 연산을 수행하므로 상대적으로 계산량이 낮다. 그리고 한 파형 내에서 지연이 변하는 경우에도 피크 지점을 일치시킨 후

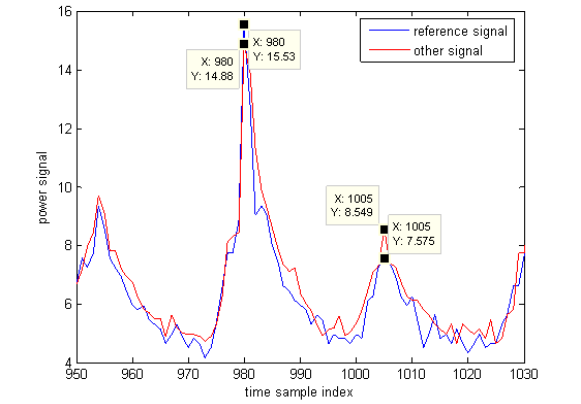

그림 3. 정렬 후 전력 신호 파형의 예.

축소 또는 보간을 이용해 신호를 적절히 변형시킴으로써 정렬이 가능한 장점이 있다. 제안된 방법을 이용하여 정렬을 수행한 결과는 그림 3에 제시되어 있으며, 그림 2에서 불규칙한 시간 지연을 보였던 신호가 잘 정렬되어 있음을 볼 수 있다.

IV. 모의실험 결과 및 성능분석

제안된 방법의 신호 정렬 성능을 확인하기 위해, “mote IV”라는 무선센서 네트워크 장치를 이용하여 AES 암호화 알고리즘이 동작할 때 측정된 총 4,000개의 전력 소비 파형을 이용하여 DPA 공격을 수행하였다 [1],[7]. 암호화 장치의 내부 클럭과 측정 장치의 샘플링 주파수는 각각 8 MHz 와 200 MHz였다. 피크 신호 사이를 보간하는 방법으로는 여러 보간법의 이용이 가능하나, 계산량이 적고 구현이 간단한 선형 보간법을 사용하였다. 제안된 신호 정렬의 성능을 확인하기 위해서 정렬이 되지 않은 원 신호에 대해 DPA 공격을 수행했을 때 필요한 최소 전력 신호 개수를 표 1에 제시하였다. 여기서 'Fail'은 주어진 4,000 개의 신호 내에서 비밀 키를 찾아내는데 실

표 1. 정렬 전 신호를 이용한 DPA 공격 시 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. POC를 이용한 신호 정렬 후 DPA 공격을 수행했을 때 요구되는 최소 신호 개수

key No.	# of traces	key No.	# of traces
1	1288	9	2498
2	788	10	835
3	1054	11	2694
4	1402	12	1513
5	1576	13	1459
6	1169	14	3137
7	**Fail**	15	1366
8	3378	16	1371

표 3. 제안된 방법을 이용한 신호 정렬한 후 DPA 공격을 수행했을 때 요구되는 최소 신호 개수

key No.	# of traces	key No.	# of traces
1	712	9	1,879
2	770	10	588
3	868	11	1,732
4	853	12	1,192
5	1,321	13	917
6	933	14	849
7	1,772	15	1,215
8	1,063	16	757

패했다는 것을 의미한다. 표 1에서 보듯이 정렬되지 않은 신호를 공격하였을 때는 대부분의 경우에 공격에 실패하는 것을 볼 수 있다. 이러한 결과는 H/W 또는 측정 시의 오차에 의한 영향이 크게 나타나 측정된 전력 신호 파형이 시간 축 상에서 제대로 정렬되지 않았기 때문이다.

다음으로 기존의 정렬 방법의 성능을 알아보기 위해 POC 정렬 방법을 이용해 신호를 정렬한 후 DPA 공격을 수행하였으며, 그 결과는 표 2에 제시되어 있다. 표 2에서 보듯이 POC 정렬을 이용할 경우 대부분의 공격이 성공함을 볼 수 있으며, 요구되는 최소 전력 신호의 수도 1,700개 정도로 감소했음을 알 수 있다. 그러나 8번이나 14번 비밀 키와 같이 요구되는 전력 신호의 수가 3,000개를 넘어가는 경우가 존재하는데, 그 원인은 한 파형 내에서 지연의 변동이 발생할 경우에 위상 차를 이용하는 POC 방법으로는 정렬이 불가능하기 때문이다.

마지막으로 제안된 방법의 성능을 검증하기 위해 제안된 정렬 방법을 이용해 신호를 정렬한 후 DPA 공격을 수행하였으며, 그 결과는 표 3에 제시되어 있다. 표 3에서 보듯이 제안된 방법을 이용할 경우 모든 비밀 키에 대해 공격에 성공하였음을 볼 수 있으며, 요구되는 최소 전력 신호의 수도 1,060개로 POC 정렬 방법에 비해 약 38% 정도 감소하였음을 확인할 수 있다. 이러한 성능 향상은 제안된 방법이 신호의 시간적 이동을 이용하여 정렬을 수행하는 것이 아니라, 같은 암호화 동작에 의해 발생하는 전력 피크를 매칭시켜 정렬을 수행하기 때문이다.

V. 결 론

본 논문에서는 PA 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 있다. 이것은 부채널 공격에서 오정렬 문제로 인한 PA 공격 성능의 불안정성을 해결할 수 있음을 의미한다. 그리고 제안된 방법은 DPA 공격에만 한정되는 것이 아니므로, 다른 부채널 공격의 성능 향상에도 크게 이바지할 수 있을 것으로 기대된다.

참고문헌

[1] P. Kocher, J. Jaffe and B. Jun, "Differential Power Analysis," *in proceedings of CRYPTO 1999*, LNCS 1666, pp. 388-397, *Springer-Verlag*, 1999.

[2] 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.

[3] 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.

[4] O. Kömmerling, and M. G. Kuhn, "Design Principles for Tamper-Resistant Smartcard Processors", *The Proceeding of the USENIX Workshop on Smartcard Technology-Smartcard'99*, pp. 9-20, 1999.

[5] 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.

[6] 박제훈, 문상재, 하재철, 이훈재, "차분 전력 분석 공격을 위한 향상되고 실제적인 신호 정렬 방법", *정보보호학회논문지*, 제 18권, 5호, pp. 93-101, 2008.10.

[7] Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, 2001.