http://dx.doi.org/10.3745/KTCCS.2013.2.9.393

New Type of Collision Attack on Power-Analysis Resistant AES

HeeSeok Kim† · Hark-Soo Park†† · Seokhie Hong†††

ABSTRACT

This paper introduces a new collision attack on first-order masked AES. This attack is a known plaintext attack, while the existing collision attacks are a chosen plaintext attack. In addition, our method is more efficient than the second-order power analysis and requires about 1/27.5 power measurements by comparison with the last collision attack. Some experiment results of this paper support this fact. In this paper, we also introduce a simple countermeasure, which can protect against our attack.

Keywords : Side-Channel Attack, Power Analysis, Collision Attack, Masking Method, Second-Order Power Analysis, AES

전력 분석에 안전한 AES에 대한 새로운 종류의 충돌쌍 공격

김 희 석† · 박 학 수†† · 홍 석 희†††

요 약

본 논문에서는 일차 전력 분석에 안전한 AES의 마스킹 기법을 분석할 수 있는 새로운 충돌쌍 공격을 제안한다. 제안하는 충돌쌍 공격은 기존 충돌쌍 공격의 단점인 선택 평문 공격의 단점을 극복하고 기지 평문 공격이 가능하도록 구성되어진다. 또한 제안하는 분석기법은 이차 전력 분석보다 효율적이며 최근 제안된 충돌쌍 공격에 요구되는 파형 개수에 비해 약 1/27.5배의 파형만을 요구한다. 논문에 포함된 실험 결과들은 이러한 사실을 뒷받침한다. 본 논문에서는 또한 새로운 분석 기법과 함께 이 방법을 방어할 수 있는 간단한 대응방법을 소개하도록 한다.

키워드 : 부채널 공격, 전력 분석 공격, 충돌쌍 공격, 마스킹 기법, 이차 전력 분석, AES

1. 서 론

수학적으로 안전한 것으로 알려진 알고리즘조차도 구현 단계에서 고려되지 못한 부가적인 정보의 누출이 있다는 것이 알려졌고, 이로부터 비밀 키의 값을 알아낼 수 있는 부채널 공격(Side Channel Attack)이 소개되었다[1]. 이러한 부채널 공격이 소개되면서 많은 암호시스템 설계자들은 효율적인 대응법들을 연구하기 시작했고, 부채널 공격 중 하나인 차분 전력 분석(Differential Power Analysis, DPA)[1]에 대한 대응법으로는 마스킹 대응법(masking method)이 활발히 연구되어지고 있다[2, 3, 4, 5, 6, 7, 8]. 하지만 이러한 마스킹 대응법은 암호 연산 시, 임의의 두 중간 값이 같은 마스킹 값을 사용했을 경우 분석이 가능한 것으로 알려져 있으며 이러한 분석 기법을 이차 전력 분석이라 한다[9]. 이차 전력 분석이 처음 소개된 이후로, 최근 이차 전력 분석의 성능 향상을 위한 연구가 활발히 진행되어지고 있다[10, 11, 12, 13].

마스킹 기법에 대한 또다른 전력 분석방법은 충돌쌍 공격이다[14,15,16,17]. 이 충돌쌍 공격은 두 파형을 조합하는 이차 전력 분석과 임의의 두 중간 값이 충돌이 나도록 평문을 선택해서 입력하여 키를 찾아내는 방법이다. 하지만 이러한 충돌쌍 공격은 선택 평문 입력 공격이 불가능한 환경에서 사용이 불가능하며 충돌이 나기 위해 다수의 평문을 입력해야만 하는 단점이 있다. 하지만 최초의 충돌쌍 공격은 이차 전력 분석 공격보다 좀 더 많은 파형을 필요로 했으나 최근의 충돌쌍 공격[17]은 이보다 적은 파형의 개수를 요구한다고 보고되고 있다.

본 논문에서는 새로운 종류의 충돌쌍 공격을 제안한다. 제안하는 공격은 기존 충돌쌍 공격의 최대 단점인 선택 평문 공격(Chosen-Plaintext Attack)[18]이 아닌 기지 평문 공격(Known-Plaintext Attack)[18]의 형태이다. 이는 선택 평문 공격이 불가능한 환경, 즉 평문이 임의의 난수로 선택되어지는 환경에서 유용하게 사용되어질 수 있다. 또한 기존

※ 본 연구는 미래창조과학부 및 정보통신산업진흥원의 IT융합 고급인력과정 지원사업의 연구결과로 수행되었음(NIPA-2013-H0301-13-3007).
† 정 회 원 : 한국과학기술정보연구원 과학기술정보보호실 선임연구원
†† 비 회 원 : 한국과학기술정보연구원 과학기술정보보호실 책임연구원
††† 정 회 원 : 고려대학교 정보보호대학원 교수
논문접수 : 2013년 4월 16일
수 정 일 : 1차 2013년 7월 26일
심사완료 : 2013년 8월 6일
* Corresponding Author : Seokhie Hong(shhong@korea.ac.kr)

방법보다 요구되어지는 전력 파형 개수를 대폭 감소시킨다. 이 목적을 달성하기 위해 본 논문에서는 두 마스킹 S-box의 출력 사이의 충돌쌍을 찾았던 기존 분석과 달리 하나의 S-box 출력과 마스킹 S-box 생성 시 나타나는 중간 값들 사이의 충돌쌍을 이용한다. 제안 기법의 성능의 우수성을 증명하기 위해 본 논문에서는 Message의 전력 소비 모델[19]에 기반한 시뮬레이션 결과를 보인다. 또한 제안하는 분석 기법을 방어하기 위한 간략한 대응 기법을 소개한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구로 AES[20]의 마스킹 기법과 이차 전력 분석, 충돌쌍 공격 등을 설명한다. 3장에서는 본 논문에서 제안하는 새로운 충돌쌍 공격을 소개하며 4장에서는 제안하는 공격의 성능을 기존의 다양한 이차 전력 분석과 비교한다. 5장에서는 제안하는 충돌쌍 공격을 포함해 기존의 충돌쌍 공격을 방어할 수 있는 간략한 대응 기법을 제안하며 6장에서 본 논문을 결론 맺는다.

2. 관련 연구

2.1 AES에 대한 마스킹 기법

마스킹 기법은 블록 암호를 차분 전력 분석으로부터 보호하기 위해 제안된 대응기법으로 비용이 저렴하며 기존 시스템에 쉽게 적용이 가능해 현재 가장 널리 사용되고 있다. 마스킹 기법은 평문 x에 대하여 암호문 y를 얻기 위해 마스킹 난수 r을 이용, $x \oplus r$($\oplus$: Excusive-Or, XOR)의 암호문 y'(=$y \oplus r'$)을 구한 후, 최종적으로 y를 얻기 위해 $y' \oplus r'$의 연산을 수행한다 (경우에 따라 마스킹 기법은 다르게 구성된다.). 따라서 암호화 중 중간 값을 알 수 없기 때문에 일반적인 차분 전력 분석 공격은 성공할 수 없다. 이러한 마스킹 기법을 사용한 경우, $x \oplus r$의 암호문 y'(=$y \oplus r'$)에서 r'을 알아야 실제 원하는 암호문 y를 얻을 수 있다. 하지만 블록암호 알고리즘은 비선형 연산을 수행하므로 수정되지 않은 블록 암호 시스템에서 r'값은 x에 따라 다르며 이 값을 중간 값의 누출 없이 아는 것도 상당한 연산을 필요로 한다. 따라서 마스킹 대응법은 이 비선형 연산에 대한 고려가 불가피하다. 블록 암호 AES의 비선형 연산은 S-box 연산으로 그 값이 $S(x \oplus m) = S(x) \oplus m_x$의 형태이며 m_x의 값이 x의 값마다 다르다. 따라서 일반적인 마스킹 방법에서는 이 m_x의 값이 모든 x에 대해 같은 값이 되게끔 암호 알고리즘의 최초 수행시마다 새로운 마스킹 S-box(MS)를 만든다. 즉, AES의 암호 연산 수행 전 생성된 임의의 두 난수 m, m'과 모든 x에 대해 $MS(x \oplus m) = S(x) \oplus m'$을 만족하는 마스킹 테이블 MS를 생성한다. 다음은 가장 널리 사용되고 있는 AES의 마스킹 기법을 알고리즘화한 것이다.

Algorithm 1. First-order masked AES

Input : 16 바이트의 평문 x ($(x_0 x_1 ... x_{15})_{2^8}$), 마스터키 K, 라운드 수 Nr
Output : 16 바이트의 암호문 y ($(y_0 y_1 ... y_{15})_{2^8}$)

1. 여섯 개의 난수 m, m', m_1, m_2, m_3, m_4 생성
2. 마스킹 S-box 테이블 생성
   For i=0 to 255 do $MS(i \oplus m) = S(i) \oplus m'$;
3. $(m_1', m_2', m_3', m_4') \leftarrow$ Mixcolumns(m_1, m_2, m_3, m_4);
4. 마스터키 K와 함께 마스킹된 AES 키 스케쥴링을 수행 (각 16 바이트의 라운드키 k_i' ($0 \le i \le Nr$)은 16 바이트의 $(m_1' \oplus m' \| m_2' \oplus m' \| m_3' \oplus m' \| m_4' \oplus m')^4$로 마스킹 됨[4])
5. $s(= s_0 s_1 ... s_{15}) \leftarrow (x \oplus (m_1' \| m_2' \| m_3' \| m_4')^4) \oplus k_0'$
6. For j=1 to $Nr-1$
   For i=0 to 15 do $s_i = MS(s_i)$;
   s=Shiftrow(s); s=Mixcolumns(s);
   $s \leftarrow s \oplus k_j'$;
7. For i=0 to 15 do $s_i = MS(s_i)$;
8. s=Shiftrow(s);
   $s \leftarrow s \oplus k_{Nr}'$; $s \leftarrow s \oplus (m_1' \| m_2' \| m_3' \| m_4')^4$;
9. Return $y \leftarrow s$

2.2 이차 전력 분석

이차 전력 분석은 일차 마스킹이 적용된 암호 알고리즘에 대한 분석 방법으로서, 마스킹된 암호 연산의 중간 값에 의해 소비된 전력과 이 중간 값을 블라인딩하고 있는 마스킹 값에 의해 소비된 전력을 이용해 분석을 수행한다. 마스킹된 AES를 분석하는 일반적인 이차 전력 분석은 마스킹 S-box의 출력 값 $S(x \oplus k) \oplus m'$에 해당하는 전력과 이 값을 블라인딩하고 있는 마스킹 난수 m'에 해당하는 전력을 이용하는 방법이다. 이 두 전력을 조합한 값은 실제 키 값 k에 의해 연산되는 $S(x \oplus k)$와 밀접한 연관성을 갖게 된다. 이 것은 m'과 $S(x \oplus k) \oplus m'$의 두 바이트 중간 값이 한 바이트의 난수 m'에 의해 마스킹되기 때문이다. Messerges가 제안한 해밍웨이트 모델에 기초한 두 시점의 소비 전력은 다음과 같이 정의될 수 있다.

$$P(t_1) = offset + \varepsilon H(m') + N_1$$
$$P(t_2) = offset + \varepsilon H(S(x \oplus k) \oplus m') + N_2$$

이때, $offset$, ε, $Noise$는 각각 상수, 해밍웨이트 1당 소비하는 전력량, $N(0,\sigma^2)$의 정규 분포를 따르는 노이즈 값을 의미한다. 또한 $H(\bullet)$는 데이터 $\bullet$의 해밍웨이트를 나타내는 함수이다.

이 두 시점의 전력을 조합하는 방법은 이차 전력 분석 기법에 따라 다르다. 가장 효율적으로 알려진 세 종류의 이차 전력 분석 기법은 abs-diff, diff-square, norm-mult이며, 각 기법에 따라 두 전력을 조합하는 방식은 다음과 같다.

- abs-diff: $C=|P(t_1)-P(t_2)|$
- diff-square: $C=(P(t_1)-P(t_2))^2$
- norm-mult: $C=(P(t_1)-E(P(t_1)))(P(t_2)-E(P(t_2)))$

공격자는 이 조합된 전력 C와 추측한 키 값에 따라 결정된 $H(S(x\oplus k))$의 헤밍웨이트 사이의 상관계수를 통해 실제 키를 찾아낼 수 있다. [13]의 논문에서는 헤밍웨이트 모델일 경우, norm-mult 기법을 사용한 이차 전력 분석의 상관계수가 가장 높다는 것을 이론적으로 증명하였다.

2.3 충돌 쌍 공격

마스킹된 AES에 대한 또 다른 분석법은 충돌쌍 공격이다. 이 충돌쌍 공격은 입력값을 조절하여 고정된 입력 값에 대해 다수의 파형을 모은 후 분석이 수행되어진다. 예를 들어 [14]의 논문에서, AES의 1 라운드 두 바이트의 키 값이 k_1, k_2라면 공격자가 입력 평문의 처음 두 바이트를 0, $k_1\oplus k_2$로 선택해서 입력했을 때, 이에 대한 S-box 출력 값들은 둘 다 $S(k_1\oplus k_2)\oplus m'$이 된다. 즉, 동일한 입력에 대해 다수의 파형을 얻는다면 두 시점 사이의 상관계수 값은 1에 근사하게 된다. 공격자는 이 두 바이트의 입력 값을 (0, 0), (0, 1), ..., (0, 255)로 조절하며 입력하면서 이 충돌 쌍을 찾음에 의해 가장 높은 상관계수 값을 갖는 쌍 (0, ζ)에 대해 $k_1\oplus k_2$의 값을 ζ로 결정할 수 있다. 또한 이러한 과정을 나머지 바이트에 대해서도 되풀이하여 수행한다면 1 라운드의 모든 키 바이트 값을 알아낼 수 있다. 최근에는 이러한 분석을 좀 더 향상시켜 이차 전력 분석보다 충돌 쌍 공격이 더 적은 파형 개수를 필요로 할 수 있다는 것이 보고되었다 [17]. 하지만, 충돌 쌍 공격이 여전히 가지고 있는 문제점은 공격자가 선택 평문을 이용해 공격을 수행해야 한다는 것이며, 여전히 많은 파형 개수를 필요로 한다는 데에 있다.

3. AES에 대한 새로운 종류의 충돌쌍 공격

기존의 충돌쌍 공격은 입력 값을 조절하며 두 S-box 연산 사이의 충돌쌍을 찾는 분석 기법이었다. 하지만 이러한 분석 기법은 같은 평문을 여러 번 입력하여 충돌이 있는지 확인하고 다른 평문에 대해서도 동일한 작업을 해야 한다는 단점이 있다. 즉, 이 공격 기법이 이차 전력 분석에 비해 필요 되어지는 평문 수는 적을 수 있지만 공격자가 선택한 입력을 넣어야 한다는 단점이 따른다. 사실, 이차 전력 분석 시에 없던 이러한 제약은 선택 평문 공격이 불가능한 특정 환경에서 공격자의 이러한 분석을 불가능하게 할 수 있다.

본 논문에서는 두 S-box 연산 사이의 충돌이 아닌 하나의 S-box 연산과 마스킹 테이블 생성 시 소비되는 전력 간의 충돌쌍을 이용한 새로운 종류의 충돌 쌍 공격을 제안한다. 본 논문의 방법은 공격자가 평문을 선택할 필요가 없으며 기존 충돌 쌍 공격에 비해 훨씬 적은 량의 파형 개수를 필요로 한다.

제안하는 공격의 시나리오는 다음과 같다.

1. N개의 16 바이트 평문 $P_i(=p_{i0}p_{i1}\cdots p_{i15})(1\le i\le N)$에 대해 N개의 파형 S_i를 얻음
2. S_i의 파형에서 마스킹 테이블 생성 시 소비된 전력을 256 개의 부분 파형 SS_{ij} $(0\le j\le 255,$ $MS(j\oplus m)=S(j)\oplus m'$에 대한 파형)으로 분할
3. 평문의 첫 번째 바이트 p_{i0}에 대해 각 파형에서 부분 파형 SS_{ij}를 재정렬: $SS_{ij}' \leftarrow SS_{i(j\oplus p_{i0})}$ $(1\le i\le N,\ 0\le j\le 255)$, SS_{ij}'은 $S(p_{i0}\oplus j)\oplus m'$ 연산에 대한 파형.
4. 암호 연산 시 첫 번째 S-box 연산 $S(p_{i0}\oplus k_0)\oplus m'$의 전력 소비 S_{i0}와 SS_{ij}'과의 충돌을 조사. 즉, 256 개의 상관 계수 신호 $\delta_j=\rho_{mat}(\{S_{10},S_{20},....S_{N0}\},\{SS_{1j}',SS_{2j}',....SS_{Nj}'\})(0\le j\le 255)$으로부터 최대 값을 갖는 $\delta_{\bar{j}}$를 찾음.

Algorithm 2. The function ρ_{mat}

Input : $\{S_1(t),S_2(t),....S_N(t)\}(1\le t\le l_1)$,
$\{S_1'(u),S_2'(u),....S_N'(u)\}(1\le u\le l_2)$
Output : $\delta(j)(1\le j\le l_1\times l_2)$
1. For t=1 to l_1 do
  For u=1 to l_2 do
    $\delta((t-1)l_2+u)=\rho(\{S_1(t),S_2(t),....S_N(t)\},$
    $\{S_1'(u),S_2'(u),....S_N'(u)\})$
2. Return $\delta(j)(1\le j\le l_1\times l_2)$

5. 첫 번째 바이트의 키 k_0를 $\bar{j}$로 선택
6. 나머지 바이트의 평문에 대해서도 단계 3-5를 반복 수행

마스킹 S-box를 생성하는 연산은 크게 두 가지의 종류의 알고리즘으로 구분된다.

Algorithm 3. Generation of *MS* table-1

Input : 난수 m, m'
Output : MS
1. For u=0 to 255 do
  $MS(u\oplus m)=S(u)\oplus m'$;
2. Return MS

Algorithm 4. Generation of *MS* table-2

Input : 난수 m, m'
Output : MS
1. For u=0 to 255 do
  $MS(u)=S(u\oplus m)\oplus m'$;
2. Return MS

공격 시나리오의 단계 3과 단계 4에서 SS_{ij}'과 S_{i0}의 전력 소비 파형이 $j=k_0$일 때 충돌됨을 확인하기 위해 두 마스킹 S-box 생성 알고리즘에서 $u=k_0\oplus p_{i0}$일 때 나타날 수 있는 모든 중간 값들을 확인할 필요가 있다. 이 중간 값들에 의해 소비된 전력 파형이 바로 $SS_{i(k_0\oplus p_{i0})}$, 즉 파형 SS_{ik_0}'이다. 또한 첫 번째 마스킹 S-box 연산에 의해 소비되는 전력 파형 S_{i0}는 마스킹된 입력 $p_{i0}\oplus k_0\oplus m$과 마스킹된 출력 $S(p_{i0}\oplus k_0)\oplus m'$에 의해 영향 받는 파형이다. 다음 표는 각 파형에 연관된 중간 값들을 나타낸 것이다.

	SS_{ik_0}' in Algorithm 3	SS_{ik_0}' in Algorithm 4	S_{i0}
중간 값	$p_{i0}\oplus k_0$	$p_{i0}\oplus k_0$	$p_{i0}\oplus k_0\oplus m$
	m	m	
	$p_{i0}\oplus k_0\oplus m$	$p_{i0}\oplus k_0\oplus m$	
	$S(p_{i0}\oplus k_0)$	$S(p_{i0}\oplus k_0\oplus m)$	$S(p_{i0}\oplus k_0)\oplus m'$
	m'	m'	
	$S(p_{i0}\oplus k_0)\oplus m'$	$S(p_{i0}\oplus k_0\oplus m)\oplus m'$	

위의 표에서 보는 바와 같이 Algorithm 3에서의 부분 파형 SS_{ik_0}'는 S_{i0}와 두 번의 충돌 쌍을 가지며, Algorithm 4에서의 부분 파형 SS_{ik_0}'는 S_{i0}와 한 번의 충돌 쌍을 가진다. 하지만 $u\neq k_0$인 모든 u에 대해 SS_{iu}'와 연관된 중간 값들은 S_{i0}와 연관된 $p_{i0}\oplus k_0\oplus m$, $S(p_{i0}\oplus k_0)\oplus m'$의 값들과 충돌 쌍을 가질 수 없다. 따라서 위의 공격 시나리오에 따라 공격자는 모든 키 바이트를 찾아낼 수 있다.

4. 이차 전력 분석과의 성능 비교

본 절에서는 Message가 제안한 전력 소비 모델[19]을 이용해 새로운 충돌쌍 공격의 성능을 이차 전력 분석과 비교한다. 앞에서 설명한 바와 같이 이차 전력 분석은 다음의 두 시점에서의 전력 소비를 이용한다.

$$P(t_1)=offset+\varepsilon H(m')+N_1$$
$$P(t_2)=offset+\varepsilon H(S(x\oplus k)\oplus m')+N_2$$

또한 이 두 시점에서의 노이즈 값 N_i는 가우시안 분포 $(0,\sigma^2)$를 따른다고 가정하였으며 사용되는 평문은 랜덤하게 매번 생성하였다. 한편, 제안하는 충돌 쌍 공격은 마스킹 테이블 생성 시 소비되는 전력파형을 이용하여야 한다. 본 논문에서는 많은 논문들에서 기술된 Algorithm 3을 이용해 마스킹 테이블이 생성되었다고 가정한다. 이 때 연산되는 $S(u)\oplus m'(0\le u\le 255)$에 의해 소비된 전력 파형과 S-box 출력 값에 의해 소비된 전력파형 S_x를 다음과 같이 정의한다.

$$SS_u=offset+\varepsilon H(S(u)\oplus m')+N_{(u)}(0\le u\le 255)$$
$$S_x=offset+\varepsilon H(S(x\oplus k)\oplus m')+N_x$$

Algorithm 5. Generation of MS table to prevent the new collision attack

Input : 난수 m, m'
Output : MS
1. 난수 r 생성
2. For u=r to 255+r do
   $MS((u \bmod 256)\oplus m)=S(u \bmod 256)\oplus m'$;
3. Return MS

위의 식에서도 $N_{(u)}$와 N_x의 노이즈는 가우시안 분포 $(0,\sigma^2)$를 따른다고 가정하였다. 비교되어지는 세 종류의 이차 전력 분석과 충돌쌍 공격의 성능은 상수인 $offset$ 값에 무관하다. 이는 파형끼리의 차분을 낼 경우 이 상수 값이 사라지거나 상관계수 연산 시 상수 값은 영향을 미치지 않기 때문이다. 본 논문에서는 σ/ε이 1인 경우와 2인 두 가지 경우에 대해 [13]의 방법을 따라 실험을 수행하였다.

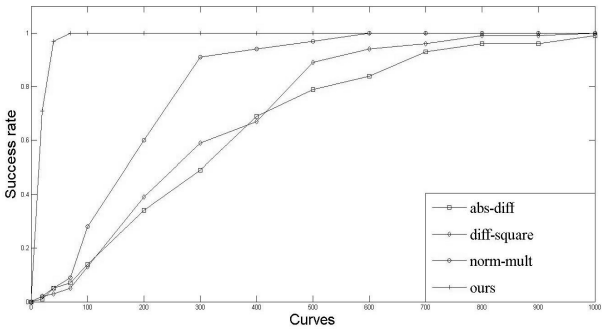


Fig. 1. Success rate of the attacks on the first-order masked AES (σ/ε=1)

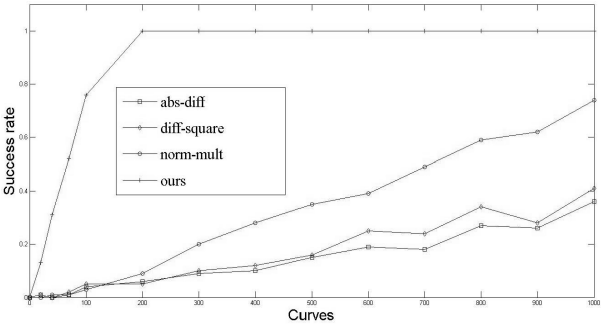


Fig. 2. Success rate of the attacks on the first-order masked AES (σ/ε=2)

본 논문에서는 기존의 충돌쌍 공격과 직접적인 실험 결과를 비교하지는 않았다. 이는 기존 충돌쌍 공격들이 임의의 평문을 사용할 수 있는 분석법이 아니기 때문이다. 또한, 공격자가 선택 평문 공격을 시도하는 것이 가능하다 하더라도 [14]의 논문의 경우는 고정된 평문을 N번씩 총 256회, [17]의 논문의 경우 고정된 평문을 N번씩 근사적으로 27.5회 입력하여야 한다. 따라서 제안하는 분석 기법보다 [14]의 방법은 256배의 평문 쌍이, [17]의 방법은 27.5 배의 평문 쌍이 요구되어질 것이다.

5. 대응 기법

제안하는 충돌 쌍 공격은 마스킹 테이블 생성 연산을 랜덤화함에 의해 쉽게 방어되어질 수 있다. 즉, 공격 시나리오의 단계 3에서 공격자가 신호를 재정렬할 때 공격자가 원하는대로 정렬이 되지 않도록 하는 것이다.

이 대응 기법과 더불어 공격자는 기존의 충돌쌍 공격을 방어하기 위해 이론적으로 안전성을 제공할 수는 없다 하더라도, S-box 연산의 위치를 랜덤화하는 셔플링 기법[7]도 추가적으로 적용하여야만 한다.

6. 결 론

본 논문에서는 일차 전력 분석에 안전한 AES의 마스킹 기법에 대한 새로운 충돌쌍 공격을 제안하였다. 제안하는 분석 기법은 기존의 충돌쌍 공격의 최대 단점인 선택 평문 공격을 기지 평문 공격으로 변화시켰다. 또한 본 논문에서는 제안하는 충돌쌍 공격 기법이 기존 충돌쌍 공격과 이차 전력 분석 공격보다 상당히 소수의 전력 파형을 요구하는 것을 실험적으로 증명하였다.

참 고 문 헌

[1] P. Kocher, J. Jaffe, B. Jun, “Differential Power Analysis”, Crypto 1999, LNCS 1666, pp.388-397, Springer-Verlag, 1999.

[2] M.-L. Akkar, C. Giraud, “An Implementation of DES and AES, Secure against Some Attacks”, CHES 2001, LNCS 2162, pp. 309-318, Springer-Verlag, 2001.

[3] J. Blömer, J. Guajardo, V. Krummel, “Provably Secure Masking of AES”, SEC 2005, LNCS 3357, pp.69-83, Springer-Verlag, 2005.

[4] C. Herbst, E. Oswald, S. Mangard, “An AES Smart Card Implementation Resistant to Power Analysis Attacks”, ACNS 2006, LNCS 3989, pp.239-252, Springer-Verlag, 2006.

[5] H. Kim, T.H. Kim, D.-G. Han, S. Hong, “Efficient Masking Methods Appropriate for the Block Ciphers ARIA and AES”, ETRI Journal. Vol.32, No.3. 2010, pp.370-379.

[6] E. Oswald, S. Mangard, N. Pramstaller, “A Side-Channel Analysis Resistant Description of the AES S-Box”, FSE 2005, LNCS 3557, pp.199-228, Springer-Verlag, 2005.

[7] E. Oswald, K. Schramm, “An Efficient Masking Scheme for AES Software Implementations”, WISA 2005, LNCS 3786, pp. 292-305, Springer-Verlag, 2006.

[8] H. Kim, Y.I. Cho, D. Choi, D.-G. Han, S. Hong, "Efficient Masked Implementation for SEED Based on Combined Masking," ETRI Journal. Vol.33, No.2, 2011, pp.267-274.

[9] T. Messerges, “Using Second-Order Power Analysis to Attack DPA Resistant Software”, CHES 2000, LNCS 1965, pp. 238-251, Springer-Verlag, 2000.

[10] M. Joye, P. Paillier, B. Schoenmakers, “On Second-Order Differential Power Analysis”, CHES 2005, LNCS 3659, pp. 293-308, Springer-Verlag, 2005.

[11] E. Oswald, S. Mangard, C. Herbst, and S. Tillich, “Practical second-order DPA attacks for masked smart card implementations of block ciphers”, CT-RSA 2006, LNCS 3860, pp.192-207, Springer-Verlag, 2006.

[12] K. Schramm, C. Paar, and D. Pointcheval, “Higher Order Masking of the AES”, CT-RSA 2006, LNCS 3860, pp. 208-225, Springer-Verlag, 2006.

[13] E. Prouff, M. Rivain, and R. Bevan, “Statistical Analysis of Second Order Differential Power Analysis”, IEEE Transactions on Computers, Vol.58, No.6. 2009, pp.799-811.

[14] K. Schramm, G. Leander, P. Felke, C. Paar, “A Collision Attack on AES: Combining Side Channel and Differential Attack”, CHES 2004, LNCS 3156, pp.163-175, Springer-Verlag, 2004.

[15] A. Bogdanov, “Improved Side-Channel Collision Attacks on AES”, SAC 2007, LNCS 4876, pp.84 - 95. Springer-Verlag, 2007.

[16] A. Moradi, O. Mischke, and T. Eisenbarth, “Correlation-Enhanced Power Analysis Collision Attack”, CHES 2010, LNCS 6225, pp.125 - 139. Springer-Verlag, 2010.

[17] C. Clavier, B. Feix, G. Gagnerot, M. Roussellet, and V. Verneuil, “Improved Collision-Correlation Power Analysis on First Order Protected AES”, CHES 2011, LNCS 6917, pp.49-62, Springer-Verlag, 2011.

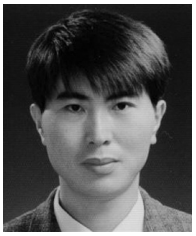
[18] G. Welchman, “The Hut Six Story: Breaking the Enigma Codes”, New York, McGraw-Hill, 1982.

[19] S. Mangard, E. Oswald, and T. Popp, “Power Analysis Attack: Revealing the Secrets of Smart Cards”, Springer, 2007.

[20] J. Daemen and V. Rijmen, “AES Proposal: Rijndael.” 1998.

김 희 석

e-mail : hs@kisti.re.kr
2006년 연세대학교 수학과(학사)
2008년 고려대학교 정보보호대학원 (공학석사)
2011년 고려대학교 정보보호대학원 (공학박사)
2011년~2012년 Bristol University 박사후 연구원
2013년~현 재 한국과학기술정보연구원 과학기술정보보호실 선임연구원
관심분야 : 부채널 공격, 암호시스템 안전성 분석 및 고속구현, 암호칩 설계 기술, 보안관제, 네트워크 보안



박 학 수

e-mail : hspark@kisti.re.kr
1989년 한남대학교 전자계산학과(학사)
1991년 한남대학교 컴퓨터공학과(공학석사)
2003년 한남대학교 컴퓨터공학과(공학박사)
1991년~현 재 한국과학기술정보연구원 과학기술정보보호실 책임연구원
관심분야 : 보안관제, 침해사고 대응, 네트워크 보안

홍 석 희

e-mail : shhong@korea.ac.kr
1995년 고려대학교 수학과(학사)
1997년 고려대학교 수학과(이학석사)
2001년 고려대학교 수학과(이학박사)
1999년~2004년 (주)시큐리티 테크놀로지스 선임연구원
2003년~2004년 고려대학교 시간강사
2004년~2005년 K.U. Leuven 박사후 연구원
2005년~현 재 고려대학교 정보보호대학원 교수
관심분야 : 대칭키 암호 알고리즘, 공개키 암호 알고리즘, 포렌식