마스킹된 ARIA에 대한 2차 DPA 공격

유형소*, 김창균**, 박일환*, 문상재**

*경북대학교 전자공학과

**국가보안기술연구소

Second-order DPA attack against masked ARIA

HyungSo Yoo*, ChangKyun Kim**, IlHwan Park*, SangJae Moon**

*Department of Elec. Eng., Kyungpook National University.

**National Security Research Institute.

요 약

1999년 P.Kocher에 의해 전력분석공격에 대한 연구결과가 발표된 이후, 부채널 공격에 의한 많은 암호장치들의 취약성 및 대응방법들에 대한 연구가 이루어지고 있다. 지금까지 제안된 대응방법중 마스킹 기법이 소프트웨어적으로 구현하는데 가장 효율적이다. 하지만, 최근 마스킹이 적용된 AES에 대한 효율적인 2차 DPA 공격결과가 발표되었다. 본 논문에서는 마스킹이 적용된 국가표준암호 ARIA를 대상으로 2차 DPA 공격을 성공적으로 수행하였다.

Ⅰ. 서 론

최근 국내에서는 금융IC카드, 행정기관 IC카드 등이 스마트카드로 대체되고 있으며, 차세대 주민등록증으로 스마트카드로의 대체가 진행되고 있다. 또한, RFID, PDA 등 다양한 형태의 무선정보통신기기들의 사용이 증가하고 있다. 하지만, 1999년 Kocher에 의해 전력분석공격이[1] 처음으로 제안된 이후, 많은 연구자들에 의해 대응방법을 고려하지 않고 암호알고리즘을 구현한 스마트카드가 전력분석공격에 취약함이 밝혀졌으며. 따라서 전력분석공격에 안전하기 위한 대응방법이 활발히 연구되고 있다. 지금까지의 연구결과로 암호알고리즘의 수행도중 생성되는 중간값과 전력소모량간의 의존성을 제거하기 위하여 마스킹[4, 5], 랜덤 지연시간 삽입[5], 새로운 하드웨어 논리 스타일 사용[6, 7] 등이 있다. 본 논문에서는 전력분석공격에 대한 대응방법으로 가장 활발히 연구가 되고 있는 마스킹을 적용한 ARIA를 스마트카드에 구현하여 2차 DPA 공격을 수행하였다. 공격결과 약 1,000개의 전력파형을 이용하여 성공적으로 암호키를 찾아낼 수 있었다. 본 논문의 구성은 다음과 같다. II장에서 ARIA에 대한 마스킹 적

용기법 및 2차 DPA 공격의 이론에 대해 살펴본 후 III장에서 마스킹이 적용된 ARIA에 대한 2차 DPA 공격을 수행하였으며, IV장에서 결론을 맺는다.

II. 마스킹 기반 ARIA에 대한 2차 DPA 공격 이론

1차 DPA 공격은 측정된 전력파형의 시간축에서 한 시점에서의 전력정보를 이용하여 공격을 수행하는 반면, 2차 이상의 고차 DPA 공격은 2개 이상의 시점에서의 전력정보를 이용하여 공격을 수행한다. 마스킹이 적용된 AES에 대한 2차 DPA 공격에 대한 연구결과가 최근 활성화되고 있으나 [5,6,7,8], 본 논문에서는 가장 효율적인 방법으로 알려진 [8]에서 제안한 2차 DPA 공격이론을 사용하였다. [8]에서는 다음과 같은 기본적인 가정 및 사실을 바탕으로 2차 DPA 공격을 수행하였다.

가정 : $a \in \{0,1\}^n$ 이고 $P(a)$를 a를 처리할 때의 전력소모량, $HW(a)$ a의 해밍웨이트라고 했을 때, $P(a) \approx HW(a)$이라고 가정한다. 위 가정은 CMOS의 전력 소모특성에서 충분히 알 수 있는 것으로, 타당한 가정이다.

사실 : $a,b \in \{0,1\}$이고, $\oplus$를 배타적 논리합 연산, $HW(x)$를 x의 해밍웨이트라고 표기했을 때 다음의 관계가 확률 1로 성립한다.

$$HW(a \oplus b) = |HW(a) - HW(b)|$$

위의 가정과 사실을 기반으로 $a,b \in \{0,1\}$인 경우 두 지점에서의 전력소모량 차이 $|P(a) - P(b)| \approx |HW(a) - HW(b)| = HW(a \oplus b)$를 정확하게 예측할 수 있다.

디지털 오실로스코프를 통해 측정한 전력파형의 집합을 T, 마스크가 적용된 평문 $P \oplus M$에 대한 라운드 함수 연산을 F(P)^M이라고 했을 때, 2차 DPA 공격은 다음과 같이 2단계로 이루어진다.

단계 1 : 디지털 오실로스코프로 측정한 전력소모파형 $T \in T$ 에 대해 공격대상이 되는 구간 I를 설정한다. 이 구간은 공격의 관심이 대는 두 연산 $F_1(P_i) \oplus M_i$와 $F_2(P_i) \oplus M_i$가 처리되는 시간구간으로 경험에 의해 결정할 수 있다. 각 전력파형 T에 대해 $|I_a - I_b|, \forall I_a, I_b \in I \subseteq T$를 계산한다.

단계 2 : 단계 1에서의 계산 결과를 이용하여 1차 DPA공격을 수행한다. 즉 디지털 오실로스코프로 측정한 전력소모파형을 이용해 단계1에서 계산한 $|I_a - I_b|, \forall I_a, I_b \in I \subseteq T$와 공격자의 추정모델 $HW(F_1(P_i) \oplus F_2(P_i))$사이의 상관관계를 계산한다. 두 시점에서의 XOR 연산으로 마스크가 제거된 형태의 추정모델 설정이 가능하다.

III. 마스킹 기반 ARIA에 대한 2차 DPA 공격 결과

본 논문에서는 마스킹을 적용한 ARIA를 AVR 기반의 8비트 마이크로프로세서에 구현하여 2차 DPA 공격을 수행하였다. DPA 공격에 가장 효율적인 1라운드의 SBOX 연산결과의 8비트를 추정모델로 사용하였다. 마스킹된 SBOX 연산은 $x \oplus k \oplus m$을 입력으로 한 테이블 참조 연산으로 이루어진다. 즉, $out = MaskedSBOX(x \oplus m \oplus k) = SBOX(x \oplus k) \oplus m'$ 가 된다. 이 때 입력 마스크 m과 출력 마스크 m'은 동일한 경우와 서로 다른 경우로 구분이 된다. 입출력 마스크가 동일한 경우에는 SBOX의 입력 $x \oplus k \oplus m$과 출력 $SBOX(x \oplus k) \oplus m$을 XOR하면 마스크가 제거된 상태의 추정모델을 만들 수 있다. 이를 이용하여 2차 DPA 공격이 가능하다. 입출

력 마스크가 서로 다른 경우에는 두 개의 SBOX의 출력을 사용하면 마스크가 제거된 상태의 추정모델을 만들 수 있다. 이 경우에는 2개의 SBOX에 대한 라운드키를 추측해야 하므로, 추측 가능한 키는 216=65536가 된다. III장에서 설명한 2차 DPA공격 이론을 실제 ARIA에 적용하면 다음과 같다. 본 논문에서는 SBOX의 입출력 마스크가 동일한 경우에 대한 실험결과만을 기술한다.

단계 1 : SBOX의 입력 $x\oplus k\oplus m$가 처리될 때의 전력소모량을 P_{in}, SBOX의 출력 $SBOX(x\oplus k)\oplus m$이 처리될 때의 전력소모량을 P_{out} 라고 하자. 디지털 오실로스코프에서 측정한 전체 전력파형 T에서 P_{in}과 P_{out}의 위치를 추정할 수 있다. 따라서, 두 전력파형의 차이의 절대값 $|P_{in}-P_{out}|$를 계산할 수 있다.

단계 2 : 단계 1에서의 계산 결과를 이용하여 1차 DPA공격을 수행한다. 즉 단계 1에서 계산된 측정값 $|P_{in}-P_{out}|, \forall P_{in}, P_{out}\in I\subseteq T$와 추정모델 $HW(x\oplus k\oplus SBOX(x\oplus k))$사이의 상관관계를 계산한다. 이 때 공격자는 $HW(x\oplus m\oplus k\oplus SBOX(x\oplus k)\oplus m)$에서 마스크 m이 제거되므로 $HW(x\oplus k\oplus SBOX(x\oplus k))$를 예측할 수 있다. $|P_{in}-P_{out}|\approx HW(x\oplus m\oplus k\oplus SBOX(x\oplus k)\oplus m)=HW(x\oplus k\oplus SBOX(x\oplus k))$이므로, 공격자는 올바른 키를 추측했을 경우 높은 상관관계를 가지게 된다. 그림 2는 마스킹된 ARIA의 1라운드 수행시의 전력소모량 파형으로, AddRoundKey연산은 0~160클럭싸이클 사이에서 수행되며, 마스킹된 SBOX 연산은 160~5400클럭싸이클, Diffusion 연산은 5400~5800클럭싸이클 사이에서 수행된다. 마스킹된 SBOX 연산은 16번의 동일한 연산으로 구성되며, 이는 그림에서 쉽게 확인할 수 있다. 본 논문에서는 첫 번째 SBOX를 대상으로 공격을 수행하였다. SBOX의 입력이 수행되는 시간구간은 대략 160~180, SBOX의 출력이 수행되는 시간구간은 대략 181~215으로 추정하였다. 따라서, 단계1을 통해 처리된 전력파형은 전체 550개의 점들로 구성된다. 단계1에서 처리된 전력파형을 사용하여 DPA 공격을 수행한 결과 그림 2, 3과 같은 결과를 얻을 수 있었다. 그림 2, 3은 각각 올바른 키 추측 및 가능한 모든 키에 대한 상관계수이다. 그림에서 확인할 수 있는 바와 같이 올바른 키 추측시 상관계수가 가장 높음을 알 수 있다. 그림 5는 성공적인 공격을 위해 필요한 전력파형의 수를 나타내고 있는데, 약 1,000개의 파형으로 올바른 키와 틀린 키를 구별할 수 있음을 알 수 있다.

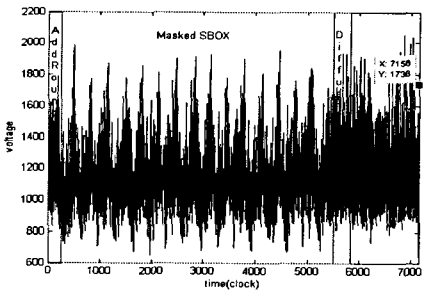

그림 1. 마스킹된 ARIA 1라운드 전력파형

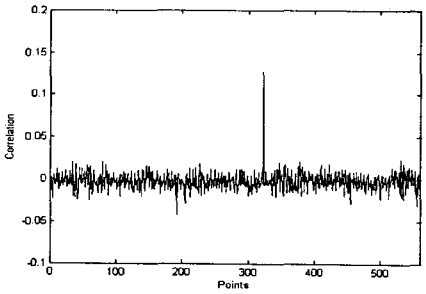

그림 2. 올바른 키

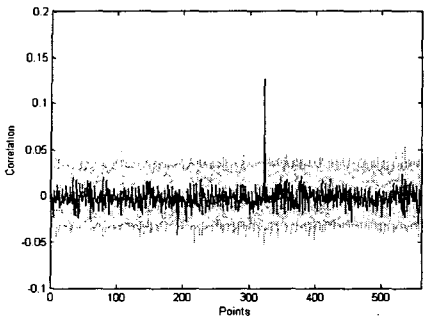

그림 3. 가능한 모든 키

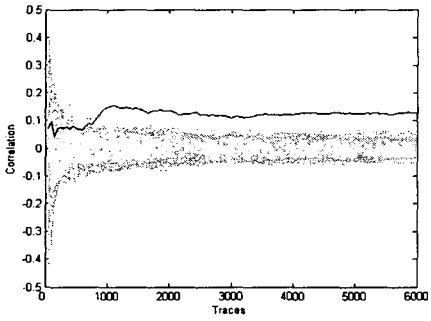

그림 4. 성공적인 공격에 필요한 전력파형 수

IV. 결 론

1999년 DPA에 대한 연구결과가 처음으로 발표된 이후, 효율적인 DPA 공격법, 대응방법 등에 대한 다양한 연구가 이루어졌다. 마스킹 기법은 소프트웨어로 쉽게 구현할 수 있는 대응방법으로, 가장 활발히 연구가 이루어지고 있는 분야이다. 하지만, 마스킹 기법을 적용한 AES에 대한 효율적인 2차 DPA 공격결과가 발표되었다. 본 논문에서는 마스킹이 적용된 ARIA에 대한 2차 DPA 공격을 수행하였다. 공격결과 약1,000개의 전력파형만으로 스마트카드 내부에 저장된 암호키를 찾아낼 수 있었다. 따라서, 마스킹 기법만으로는 전력분석공격에 안전하지 않으며, 추가적인 대응방법에 대한 연구가 필요하다. 소프트웨어에서 효율적으로 적용할 수 있는 대응방법으로 알고리즘 수행순서의 랜덤화, 랜덤 지연 삽입 등의 방법이 있다.

[참고문헌]

[1] Paul Kocher, Joshua Jaffe, and Benjamin Jun, "Differential Power Analysis," in proceedings of Advances in Cryptology -CRYPTO '99, Springer-Verlag, 1999, pp.388-397

[2] Daesung Kwon et al., "New Block Cipher ARIA," in proceedings of ICISC 2002, Springer-Verlag, 2002, pp.541-548

[3] JaeCheol Ha, ChangKyun Kim, SangJae Moon, IlHwan Park, and HyungSo Yoo, "Differential Power Analysis on Block Cipher ARIA," in proceedings of HPCC 2005, Springer-Verlag, 2005, pp.541-548

[4] Thomas S. Messerges, "Power Analysis Attacks and Countermeasures for Cryptographic Algorithms," Ph.D Thesis 2000, pp.541-548

[5] Thomas S. Messerges. "Using Second-Order Power Analysis to Attack DPA Resistant Software," in proceedings of CHES 2000, LNCS 1965, pp.238-251, Springer, 2000

[6] Marc Joye, Pascal Paillier, and Berry Schoenmaker. "On Second-Order Differential Power Analysis," in

proceedings of CHES 2005, LNCS 1717, pp.158-172, Springer, 2005

[7] Eric Peeters, Francois-Xavier Standaert, Nicolas Donckers, and Jean Jacques Quisquater. "Improved Higher Order Side-Channel Attacks with FPGA experiments," in proceedings of CHES 2005, LNCS 1717, pp.158-172, Springer, 2005

[8] Elisabeth Oswald, Stefan Mangard, Christoph Herbst, and Stefan Tillich. "Practical Second-Order DPA Attacks for Masked Smart Card Implementations of Block Ciphers," in proceedings of CT-RSA2006, LNCS 3860, pp.192-207, Springer, 2006

[9] K.Tiri, M.Akmal, and I.Verbauwhede, "A Dynamic and Differential CMOS Logic with Signal Independent Power Consumption to Withsatand Differential Power Analysis on Smart Cards," in proceedings of ESSCIRC2002, 2002

[10] K.Tiri and I.Verbauwhede, "Securing Encryption Algorithms against DPA at the Logic Level:Next Generation Smart Card Technology," in proceedings of CHES2003, LNCS 2779, pp.125-136, Springer, 2003