2001년 한국정보처리학회 추계 학술발표논문집 제8권 제2호

덧셈 연산에서 차분 전력 분석에 관한 연구

최희봉*, 박일환*, 윤이중*, 원동호**
*국가보안기술연구소
**성균관대학교 전전컴공학부
e-mail:hbchoi@etri.re.kr

On Differential Power Analysis On The Addition modular 2^N Operation

Hee-Bong Choi*, Il-Hwan Park*, Lee-Joong Yun*,
Dong-Ho Won**
*National Security Research Institute
**Dept of E.E.C Engineering, Sung-kyun-kwan University

요약

2000년 T.S.Messerges는 데이터와 키의 이원가산 연산에서 해밍 무게에 기초한 차분 전력 분석 기술을 제안하였다. 본 논문에서는 T.S.Messerges의 분석 기술이 데이터와 키의 덧셈 mod 2^N 연산에 대해서도 확대 적용할 수 있음을 제안하고 이에 대한 시뮬레이션 결과를 제시한다. 데이터와 키의 이원가산 연산은 Twofish와 같은 암호 알고리즘에서 사용되고 있으며 덧셈 mod 2^N 연산은 IDEA와 같은 암호 알고리즘에서 사용되고 있다. 따라서 본 논문에서 제안한 전력 분석 적용기술을 이용할 경우 IDEA의 키 128비트 중 덧셈 mod 2^N 연산에 들어가는 키 32비트를 분석해 낼 수 있다.

1. 서론

과거 몇 년 사이에 암호 학자들은 암호 장치의 분석 방법을 발전시켜 왔으며 타이밍 분석 및 단순 전력 분석, 차분 전력 분석 공격 기술 그리고 기타 관련된 기술들을 이용하여 암호 분석 분야에 적용시켜 왔다. 이것은 공격자가 암호장치에서 비밀키를 탈취할 수 있는 기술로서 정교하고 아주 강력한 해독 도구이다. 그 결과 누출 공격에 대한 암호 알고리즘의 취약성에 대한 관심이 더욱 높아지고 있다.[1] 이들 공격들은 하드웨어 장치가 암호 알고리즘을 구동할 때 정보를 누출할 수 있는 사실에서 시작하였다. 누출 정보원의 한 예는 암호 알고리즘을 실행시키는 장치의 시간_변동 전력 소모 신호라고 말할 수 있다. 1998년 Kocher 등은 DPA(Differential Power Analysis)라 불리는 방법을 사용한 전력 누출 공격법을 제안했다.[2] 많은 학자들은 암호 알고리즘에 대한 전력 분석 공격법을 제안하였고[3] 이들 공격에 방어할 수 있는 보호대책을 개발하였다.[4]

2000년 T.S. Messerges는 이원가산 연산에서 데이터와 키의 상관특성을 이용하여 해밍 무게에 기초한 1차 DPA 공격을 이론적으로 입증할 수 있음을 제안하였다.[5]

본 논문에서는 덧셈 mod 2^N 연산에서 데이터와 키의 상관특성을 유도하여 T.S. Messerges의 DPA 공격 방법이 이론적으로 덧셈 mod 2^N 연산으로 확대 적용될 수 있음을 제안한다. 또한 여기서도 1차 DPA 공격으로부터 보호할 수 있는 대책도 설계될 수 있음을 보인다. 덧셈 mod 2^N 연산에서 DPA 공격에 대한 시뮬레이션을 수행한 결과도 보인다. 이원가산 연산은 Twofish 같은 암호 알고리즘에 사용되고 있는 반면에 mod 2^N 연산은 IDEA에서 데이터와 키를 연산하는 데 사용되고 있으며 전력 분석 기술을 이용할 경우 IDEA의 키 128비트 중 덧셈 mod 2^N 연산에 들어가는 키 32비트를 해독해 낼 수 있다.

논문 구성은 다음과 같다. 2장에서는 일반적인 정의와 전력 누출 모델에 대하여 설명하고, 3장에서는 T. S. Messerges가 제안한 이원가산 연산에서의 DPA 공격방법을 설명하고, 4장에서는 덧셈 mod 2^N 연산에서 1차 DPA 공격방법을 제안하고 이에 대한 보호 대책도 제안한다. 5장에서는 덧셈 mod 2^N 연산에서 1차 DPA 공격을 수행한 시뮬레이션 결과를 설명하고 6장에서 결론을 맺는다.

2. 전력 누출 모델

2.1 정의

이 논문에서 설명된 공격은 Sound로 설명한다.

Sound DPA 공격의 정의는 다음과 같다.

[정의 2]
공격자가 전력 소모 정보를 이용하여 비밀키의 모든 정보를 이론적으로 구할 수 있을 때 알고리즘의 비밀키에 대한 DPA 공격은 Sound 이다 라고 정의한다.

2.2 전력누출모델

이 논문에서 언급하는 공격에 대하여, 처리 데이터의 해밍 무게에 대한 정보를 누출한다고 가정한다. 높은 해밍 무게를 갖는 데이터 처리는 낮은 해밍 무게를 갖는 데이터 처리보다 더 많은 전력을 소모한다고 가정한다. 이 관계는 선형이라 가정한다.

$P[j]$를 시간 j에서 전력 소모라 하면 전력 소모 값은 세 부분으로 나눈다. 첫번째 처리되고 있는 데이터의 해밍 무게에 따라 변하는 전력 부분, 두번째 일정하게 추가되는 상수 부분, 세번째 잡음으로 나누어진다.

$$P[j]=\varepsilon \cdot d[j]+L+n \qquad (1)$$

여기서 $d[j]$는 시간 j에서 중간 데이터 결과의 해밍 무게이고, ε은 해밍 무게에서 각 특정 1에 대한 전력 증가분이고, L은 전체 전력 중에 추가되어야 할 상수 부분이고, n은 잡음이다. 잡음 n은 평균이 0이라고 가정한다. 충분한 통계적 평균치가 사용될 때 잡음은 무시한다.

3. T. S. Messerges DPA 공격방법

이 절에서는 이원가산 연산에서 T.S. Messerges가 제안한 1차 DPA 공격 방법을 설명한다.

1차 DPA 공격 방법을 설명하기 위해 알고리즘 코드의 일부분으로써 [그림1]에 나타내었다.이들 알고리즘은 입력 PTI 데이터와 비밀키를 결합하는 것으로 수행된다. 이원가산 연산이 첫번째 단계에서 사용되는 암호 알고리즘이 존재한다. 이러한 알고리즘의 예로서 Twofish 암호 알고리즘이 있다. 입력 데이터와 비밀키는 서로 이원가산 연산을 사용하여 수행된다. W_1 알고리즘은 명령 라인 A에서 이 이원가산 연산을 수행한다. 명령 라인 A에서 이원가산 연산으로 인해 비밀키에 대한 정보를 누출 시킬 수 있다. 다음에서 W_1 알고리즘은 1차 DPA 공격에 취약함을 이론적으로 설명한다.

```
W1(PTI)
{
        A: Result = PTI ⊕SecretKey
        .....
        other operation·
        return CTO
}
```

[그림 1] 1차 DPA 공격에 취약한 이원 가산 연산 알고리즘 W_1

W_1 알고리즘에 대한 가능한 DPA 공격은 아래와 같이 설명될 수 있다.

j^*를 W_1 루틴 내에 있는 명령 라인 A의 결과를 계산하는 시간과 같은 샘플 시간이라 둔다. 또한 이 시간에서 전력 소모는 P로 표시한다. 따라서 방정식 (1)의 모델을 사용하여 $P = d\varepsilon + L + n$를 얻는다. 여기서 d는 W_1의 명령라인 A에서 변수 결과값의 해밍 무게를 나타낸다.

k_i 와 p_i는 각각 SecretKey 및 PTI의 i번째 비트를 나타낸다. 해밍 무게 d의 기대값은 아래와 같이 k_i 와 p_i의 값에 의한다.

$$E[d|k_i \oplus p_i=0]=\frac{N-1}{2}$$
$$E[d|k_i \oplus p_i=0]=\frac{N+1}{2}$$

$k_i=0$일때 $A_0[j^*]$ 및 $A_1[j^*]$에 대한 방정식은 전력 소모 P의 기대값으로 표시될 수 있다.

$$\begin{aligned} A_0[j^*] &\approx E[P|k_i=0, p_i=0] \\ &= E[d\varepsilon+L+n|k_i=0, p_i=0] \\ &= \frac{N-1}{2}\varepsilon+L \end{aligned} \qquad (2)$$

$$\begin{aligned} A_1[j^*] &\approx E[P|k_i=0, p_i=1] \\ &= E[d\varepsilon+L+n|k_i=0, p_i=1] \\ &= \frac{N+1}{2}\varepsilon+L \end{aligned} \qquad (3)$$

방정식 (2)에서 방정식 (3)을 빼면

$$T[j^*]=A_0[j^*]-A_1[j^*]\approx -\varepsilon \ (k_i=0\text{일때}) \qquad (4)$$

유사하게 $k_i=1$일 때 $A_0[j^*]$ 및 $A_1[j^*]$에 대한 방정식은 P의 기대값으로 표시될 수 있다.

$$T[j^*]=A_0[j^*]-A_1[j^*]\approx \varepsilon \ (k_i=1\text{일때}) \qquad (5)$$

식 (4)와 (5)에서 $k_i=1$일 때 양의 펄스신호가 있으며, $k_i=0$일 때 음의 펄스신호가 있다. 따라서 Sound DPA 공격이 가능함을 입증할 수 있게 된다.

4. 덧셈 mod 2^N 에서 DPA 공격방법 제안

이 장에서는 Thomas S.M.의 DPA 공격 방법이 덧셈 mod 2^N 으로 확대되어 적용될 수 있음을 제안한다.

1차 DPA 공격 방법을 설명하기 위해 알고리즘 코드의 일부분으로써 [그림2]에 나타내었다.이들 알고리즘은 입력 PTI 데이터와 비밀키를 덧셈 mod 2^N 연산으로 결합하는 것으로 수행된다. 이러한 알고리즘의 예로서 IDEA 암호 알고리즘이 있다. $W_{1\text{-}1}$ 알고리즘은 명령 라인 A에서 이 덧셈 mod 2^N 연산을 수행한다. 명령 라인 A에서 덧셈 mod 2^N 연

산으로 인해 비밀키에 대한 정보를 누출 시킬 수 있다.

```
W1-1(PTI)
{
   A: Result = PTI+SecretKey (mod 2^N)
     .....
   other operation·
   return CTO
}
```

[그림 2] 1차 DPA 공격에 취약한 덧셈 mod 2^N 연산 알고리즘 W_{1-1}

W_{1-1} 알고리즘에 대한 가능한 DPA 공격은 아래와 같이 설명될 수 있다.

j^*를 W_{1-1} 루틴 내에 있는 명령 라인 A의 결과를 계산하는 시간과 같은 샘플 시간이라 둔다. 또한 이 시간에서 전력 소모는 P로 표시한다. 따라서 방정식 (1)의 모델을 사용하여 $P = d\varepsilon + L + n$를 얻는다. 여기서 d는 W_{1-1}의 명령라인 A에서 변수 결과값의 해밍 무게를 나타낸다. k_i 와 p_i는 각각 SecretKey 및 PTI의 i번째 비트를 나타낸다. 덧셈 mod 2^N 연산의 결과값의 해밍 무게 d의 기대값은 아래와 같이 k_i 와 p_i의 값에 의한다.

$$E[d|k_i=0, p_i=0] = \frac{N-a_i}{2}$$
$$E[d|k_i=0, p_i=1] = \frac{N+a_i}{2}$$
$$E[d|k_i=1, p_i=0] = \frac{N+a_i}{2}$$
$$E[d|k_i=1, p_i=1] = \frac{N-a_i}{2} \qquad (6)$$

여기서 a_i는 임의의 양수이고 i=1인 경우이다. i=1인 경우 덧셈 mod 2^N 연산의 성질에 의해서 식 (8)을 얻을 수 있다. 아래에서는 i=1에 대해서 공격방법을 유도한다. 즉 키의 첫번째 LSB를 공격한다.

$k_1=0$일때 $A_0[j^*]$ 및 $A_1[j^*]$에 대한 방정식은 전력 소모 P의 기대값으로 표시될 수 있다.

$$A_0[j^*] \approx E[P|k_1=0, p_1=0]$$
$$= E[d\varepsilon + L + n|k_1=0, p_1=0]$$
$$= \frac{N-a_1}{2}\varepsilon + L \qquad (7)$$

$$A_1[j^*] \approx E[P|k_1=0, p_1=1]$$
$$= E[d\varepsilon + L + n|k_1=0, p_1=1]$$
$$= \frac{N+a_1}{2}\varepsilon + L \qquad (8)$$

방정식 (7)에서 방정식 (8)을 빼면

$$T[j^*] = A_0[j^*] - A_1[j^*] \approx -\varepsilon\frac{a_1+a_1}{2} = -\varepsilon a_1 \qquad (9)$$

유사하게 $k_1=1$일 때 $A_0[j^*]$ 및 $A_1[j^*]$에 대한 방정식은 P의 기대값으로 표시될 수 있다.

$$T[j^*] = A_0[j^*] - A_1[j^*] \approx \varepsilon\frac{a_1+a_1}{2} = \varepsilon a_1 \qquad (10)$$

식 (9)와 (10)에서 $k_1=1$일 때 양의 펄스신호가 있으며, $k_1=0$일 때 음의 펄스신호가 있다. 따라서 i=1에서 덧셈 mod 2^N 연산에 대하여 Sound DPA 공격임을 입증할 수 있게 된다. i=2인 경우p_1=0로 두면 (8)식을 구할 수 있으며 이 식으로 부터 위와 같이 i=2에서 덧셈 mod 2^N 연산에 대하여 Sound DPA 공격임을 입증할 수 있게 된다. 이와 같이 계속하면 모든 키를 공격할 수 있다.

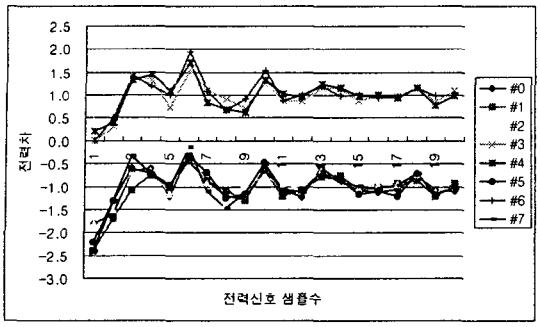
1차 DPA 공격에 보호하기 위한 대책으로 [그림 3]와 같이 덧셈 mod 2^N 연산에 간접 접근법을 취한다. 첫째 명령라인 B에서 랜덤 마스크를 생성한다. PTI데이터와 랜덤 마스크를 덧셈 mod 2^N 연산이원 가산하여 결과 mPTI를 얻는다. 다음에 명령라인 C에서 mPTI와 비밀키를 덧셈 mod 2^N 연산한다. 랜덤 마스크는 내부에서 발생하기 때문에 공격자에게 관측될 수 없다. 따라서 별개로 검토하면 명령라인 B와 C의 결과는 랜덤 정보만을 누출시키며 DPA 공격으로부터 방어할 수 있다.

```
W2-1 (PTI)
{
 B: RandomMask = rand()
 MPTI = PTI ⊕RandomMask
 C: Result = mPTI+SecretKey (mod
2^N)
        .....
 other operation
        .....
 return CTO
}
```

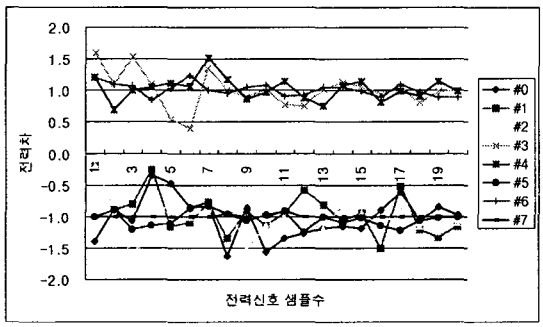
[그림 3] 1차 DPA 공격에 대응할 수 있는 알고리즘 W_{2-1}

5. 시뮬레이션 결과

이 장에서는 이원가산 연산에서 1차 DPA 공격에 대한 시뮬레이션과 덧셈 mod 2^N에 대한 1차 DPA 공격에 대한 시뮬레이션 결과를 설명한다. 랜덤한 입력 평문을 생성하기 위하여 분포 특성이 우수한 117 단 선형 귀환 시프트 레지스터를 사용하였다. [그림 4]와 [그림 5]는 키 8비트에 대한 DPA 공격을 시뮬레이션한 것이다. 전력차가 양이면 키는 1이고 음이면 0이다. 전력신호 샘플수가 많아지면 공격 성공률이 높아짐을 알 수 있다.



[그림 4] 이원가산 연산에서 DPA 공격 시뮬레이션 (전력샘플수: 5배수)



[그림 5] 덧셈 연산에서 DPA 공격 시뮬레이션 (전력샘플수 : 5배수)

6. 결론

본 논문에서는 덧셈 mod 2^N 연산에서 1차 DPA 공격 방법과 대응책을 제안하였다. 이것은 이원 가산 연산에서 T.S. Messerges.가 제안한 DPA 공격 방법을 확대 적용한 것이다. 덧셈 mod 2^N 연산은 데이터와 키 연산으로 IDEA 등에서 사용되고 있으며, 제안한 DPA 공격 방법을 사용하면 IDEA의 키 128비트 중 32비트를 분석할 수 있다. 그리고 다른 많은 논리 연산에 대해서도 DPA공격과 대응책 그리고 고차 DPA 공격 방법에 대한 연구가 필요하다.

본 논문에서 제안한 암호 장치의 전력 분석에 대한 이론적인 해석은 앞으로 암호 장치를 안전하게 설계하는데 많은 도움을 주리라 판단된다.

참고문헌

[1]J. Kelsey, B. Schneier, D. Wagner, and C. Hall, "Side Channel Cryptanalysis of Product Ciphers", in Proceedings of ESORICS98, Springer-Verlag, September, 1998, pp. 97-110.

[2]Paul Kocher, Joshua Jaffe, and Benjamin Jun, "Differential Power Analysis," in Proceedings of Advances in Cryptology-CRYPTO99, Springer-Verlag, 1999, pp. 388-397.

[3]Eli Biham and Adi Shamir, "Power Analysis of the Key Scheduling of the AES Candidates," Second Advanced Encryption Standard Candidate Conference, http://www.nist.gov/aes, March 1999.

[4]Louis Goubin and Jacques Patarin, "DES and Differential Power Analysis-The Duplication Method," in Proceedings of Workshop on Cryptographic Hardware and Embedded Systems, Springer-Verlag, August 1999, pp.158-172.

[5]T.S. Messerges, "Using Second-Order Power Analysis to Attack DPA Resistant Software," CHES'2000, pp.238-251.