스마트카드에 대한 전자파 분석 공격†

한동호*, 박제훈*, 하재철**, 이훈재***, 문상재*, 김창균****, 박일환****

*경북대학교 전자공학과

**나사렛대학교 정보통신학과

***동서대학교 인터넷공학부

****국가보안기술연구소

Electromagnetic Analysis Attacks against Smartcards

*DongHo Han, *JeaHoon Park, **JaeCheol Ha, ***HoonJae Lee, *SangJae Moon,

****ChangKyun Kim and ****IlHwan Park

*Dept. of Electronics, Kyungpook National Univ.

**Dept. of Information and Communication, Korea Nazarene Univ.

***School of Internet Engineering, Dongseo Univ.

****National Security Research Institute

요 약

스마트카드에 대한 전자파 분석 공격은 스마트카드 내의 마이크로프로세서가 연산될 때, 방사하는 의도되지 않은 전자파를 수집하여 비밀정보를 알아내는 공격이다. 이 경우에는 스마트카드에 어떤 훼손도 가하지 않고 비밀정보를 알아낼 수 있어, 기존에 국내외적으로 활발히 연구된 전력 분석 공격보다 더욱 현실적이고, 강력한 공격이다. 본 논문은 국내에서는 처음으로 스마트카드에 대한 전자파 분석 공격인 SEMA와 DEMA 공격 실험을 하였다. 그 결과 공개키 알고리즘인 RSA에 SEMA 공격을 성공하였고, 이에 대한 방어대책을 적용하여 방어를 하였다. 그리고, 국내 표준 블록 암호 알고리즘인 ARIA에 DEMA 공격을 적용하여, 비밀키를 알아냈다.

I. 서론

부채널 공격[1]은 암호 시스템의 구현 환경에 따라 의도되지 않은 채널을 통해 누설되는 정보를 분석하여 암호시스템을 공격하는 방법이다. 지금까지 국내외적으로는 스마트카드에 대한 전력 분석 공격[2-4]이 활발히 연구되었다. 그러나 전력 분석 공격은 공격 대상이 되는 스마트카드를 직접 획득한 후 스마트카드 접지와 리더기 접지 사이에 저항을 연결하여 측정된 전력 소비 파형을 분석하는 공격법이다. 전력 분석 공격은 획득한 스마트카드에 대해서는 충분히 강력한 공격이지만, 공격대상인 카드를 획득하는 것은 다소 현실적이지 않다.

이에 반해, 전자파 분석 공격은 스마트카드의 마이크로프로세서가 연산될 때, 마이크로프로세서 내부의 회로소자에 의해서 의도되

† 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음.

지 않은 전자파가 발생하게 된다. 이 때, 발생하는 전자파 역시 비밀정보를 가지고 있는데, 이 경우는 스마트카드를 획득하거나 저항을 연결할 필요없이 원거리에서 안테나를 통해서 수집된 파형을 분석하여 비밀정보를 알아낼 수 있는 좀 더 현실적이고, 강력한 공격 방법이다.

전자파 분석 공격은 국외적으로는 CHES '01에서 Gandolfi[5]등이 처음 암호 알고리즘에 대한 공격 사례를 발표하였고, Quisquater[6]는 EM 공격 방법을 Simple ElectroMagnetic Analysis(SEMA)와 Differential ElectroMagnetic Analysis(DEMA)로 나누어 구분하였다. SEMA는 전력 분석 공격의 SPA와 유사한 개념으로 신호의 특성을 파악하여 내부에 있는 비밀정보를 알아내는 방법이고, DEMA는 DPA와 유사한 개념으로 통계적인 분석방법과 에러 정정 기술을 이용하는 방법이다.

현재 국내에서는 아직 스마트카드에 대한 전자파 분석 공격을 적용한 사례는 없었다. 따라서 본 논문에서는 상용화 이전의 칩 형태 스마트카드에 RSA 알고리즘[7]과 ARIA 알고리즘[8]을 탑재하여, 각각 SEMA와 DEMA 공격 실험을 하였고, 그 결과를 보이겠다. 논문의 구성은 2장에서 전자파 분석 공격 실험에 사용된 실험 장비 소개, RSA 알고리즘에 대한 SEMA 공격 실험과 ARIA 알고리즘에 대한 DEMA 공격 실험을 보이겠다. 그리고, 3장에서 결론을 맺겠다.

II. 전자파 분석 공격 실험

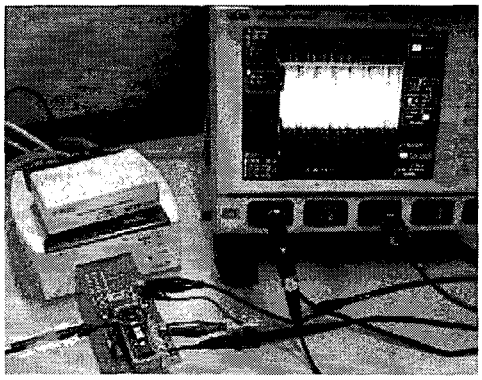
본 장에서는 전자파 분석 공격 실험에 사용된 실험장비 소개, SEMA 공격, DEMA 공격 실험결과에 대해서 소개하겠다.

1. 실험장비 소개

전자파 분석 공격 실험을 적용한 스마트카드는 상용화 이전의 칩 형태의 스마트카드로 32비트 ARM 프로세서가 내장되어 있고, 부채널 공격에 대비한 하드웨어적인 방어책은 없다. 실험에 적용한 알고리즘은 SEMA 공격 실험에 공개키 암호 알고리즘인 RSA를 사용했고, DEMA 공격 실험에 는 국내 표준 블록 암호 알고리즘인 ARIA을 사용하였다. 카드리더기는 Microprossa사의 제품으로 EEPROM에 알고리즘을 탑재하고, 스마트카드를 제어하는 기능을 가지고 있다. 스마트카드에 클럭신호를 입력하는 장비인 함수발생기는 최대 15MHz 신호를 생성 가능한 함수발생기를 사용했고, 파형측정을 위해서는 대역폭 500MHz 디지털 오실로스코프를 사용하였다.

그 외 스마트카드 칩에서 발생하는 전자파를 측정하기 위해서 EM Probe가 필요하다. 그러나, 전자파의 경우는 전력 분석 공격 시와 달리 측정된 신호의 크기가 전력 소비 신호보다 작고, 잡음의 영향이 크기 때문에 전압이득이 30dB인 증폭기를 이용해서 신호를 증폭하여 사용하였다. 실험의 마지막 단계로 수집한 신호분석 및 처리는 Matlab 7.1을 사용하였다.

(a) EM Probe



(b) 실험 요도

그림 1. 실험 장비

2. SEMA 공격 실험

SEMA 공격은 대표적인 공개키 암호 알고리즘인 RSA를 스마트카드에 탑재하여 실험하였다. RSA 알고리즘은 메시지 m에 $m^d \bmod N$과 같이 비밀키 d를 지수로 하는 멱승 연산을 한다. 그림 2는 실험에 사용한 제곱-곱셈을 이용한 멱승 알고리즘이다.

그림 3에서 보듯이, 비밀키 d의 비트 값에 따라서 연산이 달라진다. d의 비트 값이 '0'일 경우에는 제곱 연산만을 수행하고, '1'일 때는 제곱과 곱셈이 수행되게 된다. 따라서 공격자는 그림 3과 같이 비밀키의 공격 대상 해밍웨이트를 예측할 수 있고, 이를 이용해서 비밀키를 알아낼 수 있다. SEMA 공격은 비밀키의 비트 값에 따라 각각 다른 연산을 수행하기 때문에 가능하다. 이를 방어하기 위해서는 각 비트에 대해서 같은 연산을 수행하게 함으로써 SEMA 공격을 방어할 수 있다. 그림 4가 방어대책을 적용한 제곱-곱셈 알고리즘이다. 이 알고리즘을 적용하여 실험한 결과 그림 5와 같이 각 비트마다 동일한 연산을 수행함으로써 공격자는 그 비트가 '0' 인지 '1'인지를 알 수 없게 된다.

```
exp(M,d,N) ; LR  method
{   R = M
    for(i = n − 2  down to 0){
        R = R^2 mod N
        if (ith bit of d is a 1)
            R = R · M mod N }
    return R
}
```

그림 2. 제곱-곱셈을 이용한 멱승 알고리즘

```
exp(M,d,N) ; LR  method
{   R[0] = M
    for(i = n − 2  down to 0) {
        R[0] = R[0]^2 mod N
        R[1] = R[0] · M mod N
        R[0] = R[d[i]] }
    return R[0]
}
```

그림 4. SEMA 방어대책을 적용한 제곱-곱셈 알고리즘

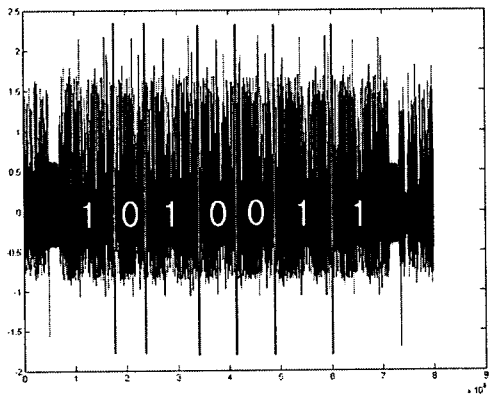


그림 3. 제곱-곱셈 알고리즘을 이용한 멱승 결과 파형 (SEMA)

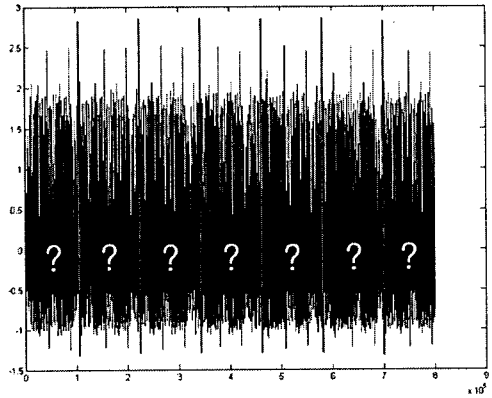


그림 5. SEMA 방어대책을 적용한 제곱-곱셈 알고리즘 파형

3. DEMA 공격 실험

DEMA 공격은 국내 표준 블록 암호 알고리즘인 ARIA를 스마트카드에 탑재하여 실험하였다. 공격 방법은 기존의 차분 전력 분석 공격방법[9]과 동일한 방법으로 1라운드 S-Box의 출력에 ZEMD 공격을 적용하였다. 그림 6는 공격 대상인ARIA 알고리즘의 1라운드를 평균한 파형이다.

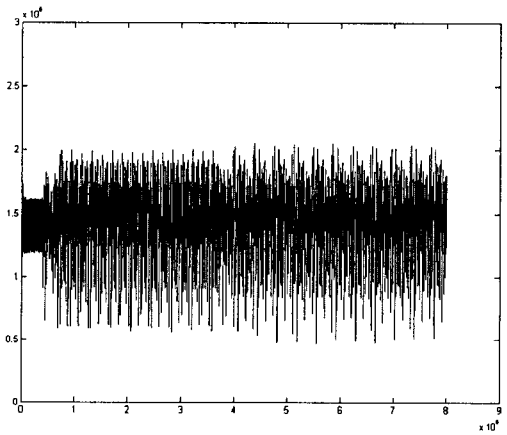
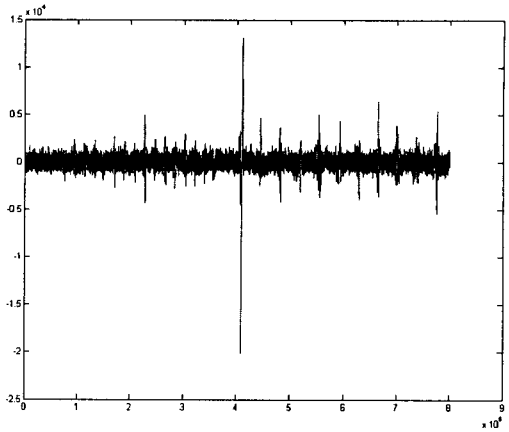


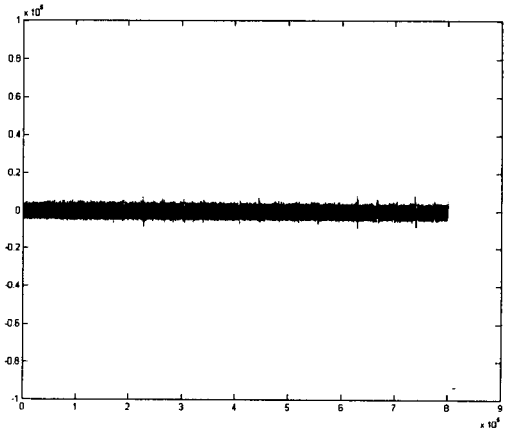
그림 6. ARIA 1라운드 평균파형

공격자는 오프라인 시뮬레이션을 다음과 같이 수행한다. 타겟 S-Box 출력 값의 해밍 웨이트에 따라 하이 해밍웨이트와 로우 해밍 웨이트로 메시지를 분류한다. 이렇게 분류한 메시지를 ARIA 알고리즘의 입력에 넣으면, 첫 번째 라운드 키와 XOR 연산 후에 S-Box에 들어가게 된다. 만약 시뮬레이션에 사용된 키가 옳은 키라면, 메시지 분류가 제대로 수행되어 파형에 피크가 발생하게 된다. 만약, 추측한 키가 잘못된 키라면 메시지 분류가 정상적으로 수행되지 않고 랜덤하게 분류되었으므로, 피크는 발생하지 않는다.

그림 7 (a)는 라운드 키 추측이 맞을 경우, 타겟인 첫 번째 S-Box에서 피크가 발생한 것을 확인할 수 있다. 그에 반해 (b)는 라운드 키 추측이 틀렸을 경우이다. 이 때는 메시지가 잘못 분류되어 타겟인 S-Box 출력 값이 랜덤하게 되어 피크가 발생하지 않는다.



(a) 추측이 맞을 경우



(b) 추측이 틀릴 경우

그림 7. ARIA 차분 파형

III. 결론

본 논문에서는 지금까지 알려진 전력 분석 공격보다 더욱 현실적이고, 강력한 공격인 전자파 분석 공격 실험을 국내에서는 처음으로 실제 스마트카드에 SEMA 공격과 DEMA 공격을 실험하였다. SEMA 공격 실험은 공개키 암호 알고리즘인 RSA 알고리즘에 적용하여 공격에 성공하여 비밀키를 알아냈으며, SEMA에 대한 방어대책을 RSA 알고리즘에 적용하여 공격에 방어가 됨을 확인하였다. DEMA 공격 실험은 국내 표준 알고리즘인 ARIA 알고리즘의 S-Box에 공격을 적용하여 비밀키를 알아냈다. ARIA의 DEMA 공격에

대한 방어대책은 기 발표된 전력 분석 공격에 대한 방어대책인 마스킹 기법[10]을 사용하면 방어가 가능하다.

결론적으로, 방어대책이 마련되어 있지 않은 스마트카드는 전력 분석 공격 및 전자파 분석 공격에 취약하다. 그러므로, 실제 구현 시에는 방어대책을 적용한 알고리즘을 사용해야 한다.

참고문헌

[1] J. Keley, B. Schneier, D. Wagner and C. Hall, "Side Channel Cryptanalysis of Product Cipher", *in Proceedings ESORICS '98*, pp.97-100, Springer-Verlag, Sep. 1998.

[2] P. Kocher, J. Jaffe and B. Jun, "Introduction to differential power analysis and related attacks", *http://www.cryptography.com/dpa/technical*, 1998.

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

[4] T. S. Messerges, E. A. Dabbish and R. H. Sloan, "Power Analysis Attacks on Modular Exponentiation in Smart Cards", *in Proc. of CHES 1999*, pp.144-157, Springer-Verlag, 1999.

[5] K. Gandolifi, C. Mourtel and F. Olivier, "Electromagnetic Analysis : Concrete Results", *CHES'01*, LNCS 2162, pp.251-261, 2001.

[6] J-J. Quisquater and D. Samyde, "A new tool for non-intrusive analysis of smartcards based on electro-magnetic emissions, the sema and dema methods", Presented at the rump session of eurocrypt'2000.

[7] R. L. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communication of the ACM, Vol 21, pp. 120-128, 1978

[8] D. Kwon, J. Kim, S. Park, S. Sung, Y. Sohn, J. Song, Y. Yeom, E. Yoon, S. Lee, J. Lee, S. Chee, D. Han and J. Hong, "New block cipher : ARIA", *ICISC '03*, LNCS 2971, pp. 432-445, 2003.

[9] J. Ha, C. Kim, , S. Moon, I. Park and H. Yoo, "Differential Power Analysis on Block Cipher ARIA", HPCC' 05, LNCS 3726, pp.541-548, 2005.

[10] 유형소, 하재철, 김창균, 박일환, 문상재, "랜덤 마스킹 기법을 이용한 DPA 공격에 안전한 ARIA 구현", 정보보호학회논문지, 제16권 제2호, pp.129-139, 2006.