부채널 공격에 대한 대응기술 분석

강영진* · 조정복**· 이훈재**
*동서대학교 정보통신공학전공
**동서대학교 컴퓨터정보공학부

Analysis in Technological Responses to Side-channel Attack

Young-Jin d* · JungBok Jo**· HoonJae Lee**
*Dept. of information and Communication Engineering, Dongseo University
**Div. Computer and Information Engineering, Dongseo University
E-mail : rkddudwls55@gmail.com, {jobok, hjlee}@dongseo.ac.kr

요 약

현재 부채널 공격은 P. Kocher에 의해 제안된 공격 방법으로 암호 알고리즘 자체의 안전성이 높다고 하더라도 암호 알고리즘이 구현된 방법이나 구현된 환경에 따라 적용이 가능한 공격법이다. 이러한 부채널 공격은 정보보호 장치의 전력(전압), 실행시간, 오류 출력, 소리 등의 변화를 측정해 각종 정보의 이진코드를 읽어내어 통계적인 방법으로 중요한 정보를 분석함은 물론 위·변조까지 가능하다. 따라서 본 논문에서는 부채널 공격 기법 중에 하나인 SPA 공격 기법과 DPA공격 기법을 살펴보고 현재까지 나온 최신 대응 기술들을 분석하고자 한다.

ABSTRACT

The Side Channel attack methods proposed by P.Kocher are mainly used for cryptanalysis different cipher algorithms even though they are claimed to be strongly secured. Those kinds of attacks depend on environment implementation especially on the hardware implementation of the algorithm to the crypto module. side-channel attacks are a type of attack introduced by P.Kocher and is applicable according to each environment or method that is designed. This kind of attack can analyze and also extract important information by reading the binary code data via measurement of changes in electricity(voltage) consumption, running time, error output and sounds. Thus, in this paper, we discuss recent SPA and DPA attacks as well as recent countermeasure techniques.

키워드

부채널 공격, Masking Countermeasure, DPA 공격기법, SPA 공격기법, Software Based Countermeasure

Ⅰ. 서 론

부채널 공격(SCA: Side Channel Attack)은 P. Kocher에 의해 제안된 공격 방법으로 암호 알고리즘 자체의 안전성이 높다고 하더라도 암호 알고리즘이 구현된 방법이나 구현된 환경에 따라 적용이 가능한 공격법이며 암호화에 사용된 키를 찾기 위해서 암호 알고리즘의 이론적인 취약점이 아닌 암호화 과정에서 누설되는 타이밍 정보, 전력, 전자파 신호등을 이용하는 물리적인 공격방법이다. 부채널 공격에는 크게 수동적 공격 (passive attacks)과 능동적 공격(active attacks) 두 가지 종류로 나눌 수 있다. 수동적 방법에는 시차 공격(Timing Attack, TA), 전력 분석 공격 (Power Analysis Attack, PA), 전자기파 분석 공격(Electromagnetic Analysis Attack, EMA)이 있으며 능동적 공격에는 오류 분석 공격(Fault Analysis Attack, FA)이 있다. 이러한 공격 기법들은 알고리즘이 구현된 방법 또는 환경에 따라 적용이 가능한 공격기법이다.

아래의 [그림1]은 부채널 분석 공격(Side Channel Analysis Attack, SCA Attack)의 간단

한 개념을 나타내고 있다.

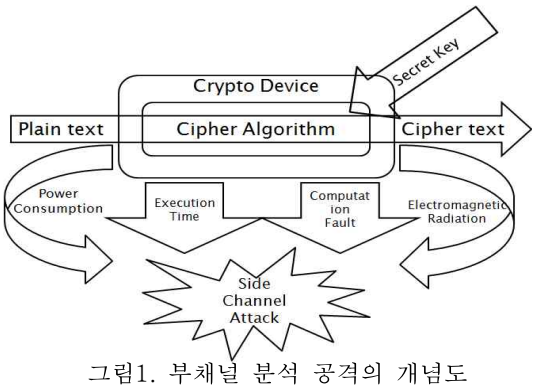

그림1. 부채널 분석 공격의 개념도

이에 본 논문에서는 수동적 공격 중에 전력 분석 공격에 해당하는 SPA(Simple Power Analysis) 공격 기법과 DPA(Differential Power Analysis)공격 기법을 살펴보고 현재까지 나온 최신 대응 기술들을 분석하고자 한다.

Ⅱ. 전력 분석 공격

전력 분석 공격은 1999년 Kocher에 의해 CRYPTO'99에서 DES에 적용된 결과가 처음 소개되었다. 여러 부채널 공격 방법들 중에서 가장 효과적이며 위협적인 공격 방법이라고 알려져 있으며, 현재까지 개발된 대부분의 암호 알고리즘들이 전력 분석 공격에 취약하다고 알려져 있다[1]. 아래의 [그림2]는 전력 분석 공격을 하기 위한 구성도이며 공격을 하기 위해서는 크게 공격대상과 소비 전력을 측정하기 위한 오실로스코프, 측정한 전력을 분석하기 위해 컴퓨터가 필요하다.

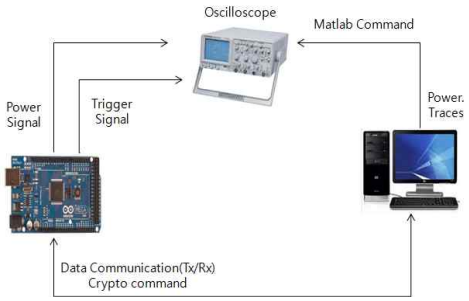

그림2. 전력 분석 공격을 위한 구성도

2.1 SPA(Simple Power Analysis)

전력 분석 공격에 해당하는 SPA공격은 특정 명령어가 수행되는 한 시점에서 입력과 출력의 값이 가지는 소비전력을 통해 비밀정보를 유추하는 방법이다[2]. 스마트카드는 대부분 트랜지스터를 이용한 논리회로로 구성되므로 게이트에 전압이 가해지면 전류가 흐르게 되고 전력이 소비되게 된다. [그림3]은 16라운드 DES(Data Encryption Standard)알고리즘 동작에 의한 소비전력 신호 변화를 확인 할 수 있으며 파형을 관찰함으로써 암호화 동작에 대한 다양한 정보를 얻어낼 수 있다[3].

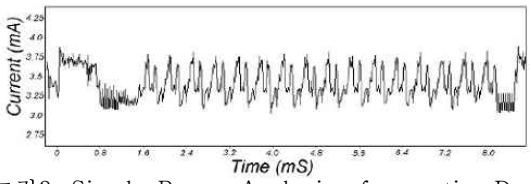

그림3. Simple Power Analysis of an entire Des

2.2 DPA(Differential Power Analysis)

DPA공격은 위에서 언급한 부채널 공격법 중 가장 강력한 공격법 중 하나이며 아주 작은 자원을 사용해서 공격을 할 수 있는 방법이다. SPA가 소비 전력을 관찰하는 것에 반하여 DPA는 비밀키와 정확히 상관관계(correlation)를 가지는 정보를 추출하기 위해 통계적인 분석(statistical analysis)과 에러정정(error correction)기술을 사용한다[4]. DPA는 다음과 같이 세분화 할 수 있다.

1) 구하려는 Device의 n비트 비밀키 k를 $(K_{n-1}, K_{n-2}, \cdots K_1, K_0)$라 정의하고 최상위 혹은 최하의 비트의 순서를 순차적으로 키의 일부가 입력되어 연산한다고 가정한다.

2) 먼저 키의 일부인 K_i 또는 $(K_i, \cdots K_j)$를 미리 가능한 키 영역에서 추측한다.

3) 추측한 키와 전력신호 데이터를 구할 때 쓴 평문을 입력으로 연산을 수행한 후 분류함수를 이용하여 전력신호 데이터를 분류한다.

$$S_0 = \{S_i[j] \mid D(key, data) = 0 \text{ or } low\,hamming\,weight\}$$
$$S_1 = \{S_i[j] \mid D(key, data) = 0 \text{ or } low\,hamming\,weight\}$$

4) 양분한 데이터를 각각 평균하여 차분 신호(Differential Signal)를 구한다.

$$\triangle_D[j] = \frac{1}{S_0}\sum_{S_{i[j]} \in S_0} S_i[j] - \frac{1}{S_1}\sum_{S_{i[j]} \in S_1} S_i[j]$$

5) 평문과 전력소비신호의 샘플 수 t 값이 크고, 추측한 키가 옳지 않다면 $\triangle_D[j]$ 신호가 거의0에 수렴한다. 키가 반응하는 지점에서 non-zero이고 추측한 키가 맞으면

$$\lim_{t \to \infty} \triangle_D[j] \approx nonzero \quad \text{if } guess\,is\,correct$$

$$\lim_{t \to \infty} \triangle_D[j] \approx 0 \quad \text{if } guess\ is \in correct$$

6) 추측이 올지 않다면 다시 2)로 돌아간다.

7) 추측이 옳다면 그 키가 Device의 실제 내부 키의 일부가 된다.

위의 과정을 반복하여 전체 사용되는 내부의 비밀 키를 같은 방법으로 구할 수 있다. DPA 공격에서 중요한 기술은 분류함수인 D(key, data)를 어떻게 설정 하는가 하는 것이다. 아래의 [그림4]는 DPA기법에서 비밀 키값에 따른 차분 전력 신호에 대한 그림이다.

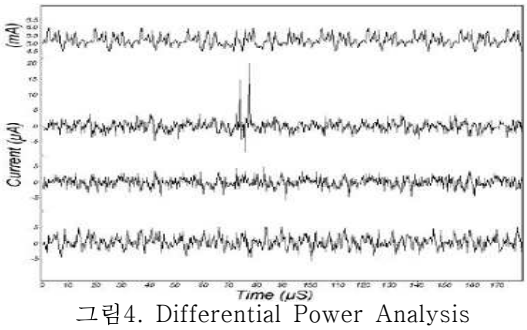

그림4. Differential Power Analysis

Ⅲ. 부채널 공격에 대한 대응 기술

최근까지 연구된 대응기법은 암호장치에서 처리 되는 데이터와 부채널 신호간의 상관관계를 제거하기 위한 방안이며 부채널 공격에 대한 대응 기술로는 대표적으로 마스킹(Masking)기법, 블라인딩(Blinding)기법, 무작위성(Randomization)기법, 은닉(Hiding)기법 이 있다.

3.1 마스킹 기법

마스킹 기법은 랜덤 한 값을 집어넣어 공격자가 원하는 전력 소모 값을 얻지 못하게 하는 기술이다. 즉, 공격자는 마스킹 된 암호 장치로부터 랜덤 한 전력 소모 값을 얻게 되기 때문에, 자신이 얻은 전력 소모 값을 통해 분석해 내고자 하는 정보를 얻지 못 한다. 결국 마스킹은 처리되는 데이터와 전력 소모 값 사이의 의존성을 제거하는 기법이다. 마스킹은 주로 알고리즘 수준의 소프트웨어에 많이 적용되며, 하드웨어에서의 적용은 주로 셀 수준에서 이루어진다.

아래의 [그림5]는 하드웨어에서의 일반 게이트와 마스킹 된 게이트를 비교하여 보여주는 그림이다.

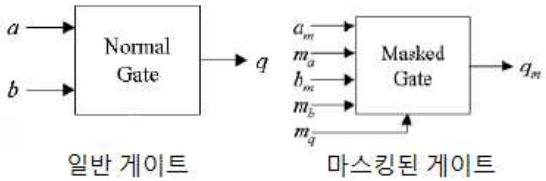

그림5. 일반게이트와 마스킹 된 게이트

그리고 위에서 언급한 소프트웨어 구현에 가장 적합한 방법으로는 암호알고리즘 수행 시에 발생하는 중간 값 i를 랜덤 마스크 m을 이용하여 공격자가 알 수 없는 값 r =i⊕m 로 대체하는 가산 마스킹 방법이다[5]. 아래의 [그림6] 은 가산 마스킹을 이용한 마스킹 된 Sbox 테이블 생성을 위한 일반적인 알고리즘 코드이다.

```
입력 : m, m'
출력 : MaskedSBOX(x⊕m) = SBOX(x)⊕m'
1 : for i = 0 to 255 do
2 :     MaskedSBOX(x⊕m) = SBOX(x)⊕m'
3 : end
4 : Return(MaskedSBOX)
```

그림 6. 마스킹 된 Sbox 생성을 위한 알고리즘

3.2 블라인딩 기법

블라인딩 기법은 클라이언트가 입력 xdp 대해 수학적 함수 f를 이용하여 출력 y를 얻을 때, x와 y의 값을 모르면서 값을 계산해 주는 공급자를 갖는 암호 설계 개념이다. 이는 클라이언트가 수학적 함수를 계산할 수 없을 때 유용한 방법이다.

첫 번째로 알려진 블라인딩 기법은 Chaum이 제안한 RSA 서명함수에 대한 동형사상에 기반 한 블라인드 서명기법이다[6]. 블라인드 기법은 웹 서버에 대한 원격 시간 분석법에 효과적인 대응법이며, 하드웨어 암호 모듈에 대한 전력분석과 시간분석에 대응하는 기법이다.

3.3 은닉 기법

은닉 기법은 소비전력과 데이터 사이의 연결관계를 끊음으로써 소비전력이 데이터에 의존하는 것을 방지한다. 이 방법으로는 일정한 소비전력이 발생하도록 회로를 설계하는 방법이다. 어떤 데이터가 입력되더라도 항상 같은 양의 전력이 소비되도록 방어회로를 구성하는 방법이다. 이러한 방어회로는 국외에서 DRL, WDDL등의 기술을 들 수 있으며, 지속적으로 연구 개발이 계속되고 있는 기술이다.

3.4 무작위성 기법

현재 무작위성 기법은 부채널을 통해 누출되는 자료를 무작위로 만드는 것으로 공격자는 난수성을 띤 정보만을 얻게 됨으로 계산과정 중에 포함된 실제 초기 값이나 중간 값을 알 수 없다. 이러한 기법은 위에서 소개한 SPA공격 기법에 실질적인 대응기법으로 소개되며 DPA공격에는 효과적으로 대응하지 못한다[7].

이러한 DPA공격에 대응하기 위해서는 타원곡선의 파라미터를 무작위호 만드는 것이 필요하다.

1) 무작위 점을 사용하여 기저 점(Base Point)을 마스킹 한다.

2) 타원곡선 위수의 임의의 배수를 사용해 비밀 스칼라 값을 난수화 한다.

3) 사영좌표를 이용하여 기저 점을 무작위로 만든다.

이러한 대책은 부분적으로 적용된 몇 가지의 경우에는 공격이 가능함이 제시되었다. 하지만 위에서 언급한 무작위 방법을 모두 사용한 경우 대한 공격법은 알려지지 않은 상황이다.

Ⅳ. 결 론

부채널 공격은 P. Kocher에 의해 제안된 공격방법으로 암호화에 사용된 키를 찾기 위해서 암호 알고리즘의 이론적인 취약점이 아닌 암호화 과정에서 누설되는 타이밍 정보, 전력, 전자파 신호등을 이용하는 물리적인 공격방법이다. 현재 부채널 공격은 시스템의 취약점을 찾아 공격하는 현실적인 공격기법으로 인식되고 있으며, 이와 같은 기반으로 안전한 암호 시스템을 구축하는데 좋은 도구로 이용되고 있다.

본 논문에서는 부채널 공격 중에 가장 강력하다고 알려진 전력 분석 공격에서도 SPA공격 기법과 DAP공격 기법을 살펴보았고, 이러한 공격기법에 대응하는 마스킹 기법, 블라인딩 기법, 은닉기법, 무작위성 기법을 분석하였다. 부채널 공격은 현재까지도 활발하게 연구 중인 분야이지만 이렇다 할 대응책이 없으며, 연구에 투입되는 인력도 부족한 편이다. 앞으로의 연구를 위해서도 보다 낳은 정책지원과 활발한 교류가 필요하다 생각 된다.

참고문헌

[1] P. Kocher, J. Jae, and B.Jun, "Differential power analysis", CRYPTO'99, LNCS 1666, pp. 388-397, 1999.

[2] 정석원, “부채널 공격법과 이의 대응법에 대한 연구 동향”, 情報保護學會誌, 第 16 卷 第 4 號, 2006. 8

[3] Sinan Hanay, Tariq Bashir Ahmed Xiang Yun, Lang Lin, "Side-Channel Attack Tolerant Logic Styles", 03. 10. 2008

[4] 이훈재, 장익훈, 최희봉, 박일환, “스마트카드의 전력분석공격 실험 방법에 관한 연구”, 한국통신학회, vol.27, No.6A, pp.541, 02-6

[5] 김창균, 박일환, 유형소, “하드웨어 마스킹 대응기법에 대한 고차 차분부채널분석 공격”, 情報保護學會論文誌, 第17卷 第5號, pp.67, 2007, 10

[6] E. Brier, M. Joye, "Weierstrass Elliptic Curves and Side-Channel Attacks", PKC 2002, LNCS 2274, pp.335-345, 2002.

[7] 곽 진, 이동범, 황문영, “부채널 공격 취약성 평가방법론 및 기준개발”, 한국인터넷진흥원, pp28-29, 2009. 12