전력분석공격에 대한 대응기술 분석

강영진* · 조정복** · 이훈재**

*동서대학교 유비쿼터스 IT

**동서대학교 컴퓨터정보공학부

Countermeasure Techniques Analysis for Power Analysis Attack

Young-Jin Kang* · Jung-Bok Jo** · HoonJae Lee**

*Department of Ubiquitous IT, Graduate School of Dongseo University

**Division of Computer and Information Engineering, Dongseo University

E-mail : rkddudwls55@gmail.com, hjlee@dongseo.ac.kr

요 약

P. Kocher 등이 제안한 전력분석공격에는 단순전력분석(SPA), 차분전력분석(DPA), 상관전력분석(CPA)이 있으며, 이러한 공격기법은 암호 알고리즘의 이론적인 취약점이 아닌 암호화 과정에서 누설되는 소모전력을 이용하여 공격한다. 또한 알고리즘이 구현된 방법 또는 환경에 따라 적용이 가능한 공격기법이기에 많은 대응기술들이 연구되고 있다. 본 논문에서는 전력분석공격에 대해 살펴보고 최근까지 연구된 대응기술들을 분석하고자 한다.

ABSTRACT

Power analysis attack on cryptographic hardware device aims to study the power consumption while performing operations using secrets keys. Power analysis is a form of side channel attack which allow an attacker to compute the key encryption from algorithm using Simple Power Analysis (SPA), Differential Power Analysis (DPA) or Correlation Power Analysis (CPA). The theoretical weaknesses in algorithms or leaked informations from physical implementation of a cryptosystem are usually used to break the system. This paper describes how power analysis work and we provide an overview of countermeasures against power analysis attacks.

키워드

전력분석공격, Software Based Countermeasure, 부채널 공격, Masking

Ⅰ. 서 론

부 채널 공격은 암/복호화 서명 등 하드웨어에서 어떠한 동작을 수행할 때 누출되는 정보를 말하며, 이 때 누출되는 정보를 이용해 공격하는 기법을 부채널 공격이라고 한다. 아래의 (그림 1)은 일반적인 암호화 프로세싱에 대한 부 채널 공격이다.

누출된 정보 중 소모 전력을 이용한 공격은 P. Kocher 등이 제안한 전력분석공격[1]이 있다. 암호 알고리즘의 이론적인 취약점이 아닌 암호화 과정에서 누설되는 소모 전력을 이용하여 공격하기 때문에 알고리즘이 구현된 방법 또는 환경에 따라 적용이 가능한 공격이며, 이에 따라 대응기술들이 많이 연구가 되고 있는 실정이다.

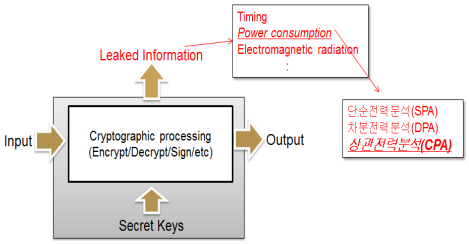

그림 1. 일반적인 암호화 프로세싱에 대한 부 채널

따라서 본 논문에서는 전력분석공격에 대한 최근까지의 대응기술들을 분석 하고자한다.

Ⅱ. 본 론

본장에서는 전력분석공격에 대한 대응기술 적용 사례들을 분석하기 전에 Goubin이 소개한 일반적인 대응방법을 소개하고자 한다[2].

- 실행시간을 무작위로 옮기고, 기다리는 상태를 넣고, 가짜 명령어를 삽입하고, 연산 실행을 무작위로 하는 등을 하여 암호 알고리즘의 실행에 따른 출력 추적 값의 상관관계를 제거한다.
- 중요한 어셈블러 명령어를 분석하기 어렵도록 다른 명령어로 대치하고, 셈이나 메모리를 옮기는 중요한 회로를 재설계한다.
- 자료나 키가 사용될 때 마다 다른 값을 갖도록 사용되는 암호 프리미티브의 알고리즘을 수정하여 공격이 어렵도록 만든다.

2.1 은닉(Hiding)기법

은닉(Hiding)을 이용한 설계 기법은 소비전력과 데이터 사이의 연결 관계를 끊음으로써 소비전력이 데이터에 의존하는 것을 방지한다. 그 방법은 두 가지가 있는데, 하나는 소비전력이 무작위로 발생하게 만드는 방법이다. 첫째로 매 클럭 사이클(clock cycle) 마다 소비되는 전력의 양을 무작위 값으로 만드는 것을 의미하고, 두 번째로 일정한 소비전력이 발생하도록 회로를 설계하는 것이다. 결국 어떤 데이터가 입력되더라도 항상 같은 양의 전력이 소비되도록 방어회로를 구성하는 것을 의미한다[3].

2.2 이중선로방식(DRL, Dual-rail Logic)

이중선로방식을 사용한 키에 따른 전력소모 랜덤화 기술은 매 클럭 사이클에서 디바이스에 일정 전력을 소모하도록 만드는 암호학적으로 적용하기 위한 논리 장치이다.

2.3 마스킹(Masking)기법

마스킹 기법은 랜덤 한 값을 집어넣어 공격자가 원하는 전력 소모 값을 얻지 못하게 하는 기법이다. 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 못한다. 결국 마스킹은 처리되는 데이터와 전력 소모 값 사이의 의존성을 제거하는 기법이며, 구현 방법에 따라 게이트 수준의 마스킹과 알고리즘 수준의 마스킹으로 구분된다. 아래의 (그림2)는 일반 게이트와 마스킹된 게이트를 보여주며, (그림3)은 가산 마스킹을 이용한 마스킹된 Sbox 테이블 생성을 위한 일반적인 알고리즘 코드이다[4].

게이트 수준의 마스킹은 회로에서 처리되는 실제 데이터 a를 두 개의 값 a_m, m_a로 표현하는 것이다. 따라서 디지털 회로에서 실제 처리되는 데이터와 전력소모량간의 상관관계가 존재하지 않는다. 이때 m_a는 a와는 통계적으로 독립적이고 균일한 분포를 가지는 랜덤 값으로 마스크라고 부르며, 마스킹된 값 a_m은 a와 m_a의 배타적 논리합 연산(XOR): $a_m = a \oplus m_a$을 통해 계산된다. 마스킹된 디지털회로에서, 논리 게이트는 a대신에 a_m, m_a를 입력으로 받아들인다[5].

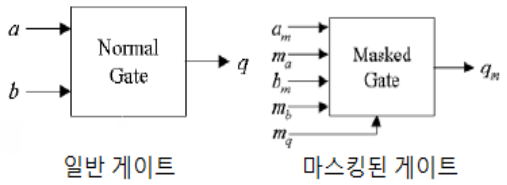

그림 2. 일반게이트와 마스킹된 게이트

그리고 소프트웨어 구현에 가장 적합한 방법으로는 암호알고리즘 수행 시에 발생하는 중간 값 I를 랜덤 마스크 m으로 이용하여 공격자가 알 수 없는 값 r = i⊕m 으로 대체하는 가산 마스킹 방법이다.

입력 : m, m'
출력 : $MaskedSBOX(x \oplus m) = SBOX(x) \oplus m'$

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

그림 3. 마스킹된 Sbox 생성을 위한 알고리즘

2.4 연구사례 분석

본 절에서는 앞에서 설명한 기법들을 가지고 전력분석공격에 대응책을 가지는 연구사례들을 분석하고자 한다.

사례 1)은 LFSR(Linear Feedback Shift Register)을 이용하여 마스킹 과 은닉 기법을 구현하였다. 전력분석공격의 주요 목표가 되는 S-box와 확산계층에 대한 이중 마스킹을 수행하였으며, S-box와 확산계층에 대해 이루어지는 부분 마스킹은 매 라운드 마다 랜덤수 생성기에서 새로운 값을 생성하여 마스킹을 강화하였다. 이 결과 동일한 평문과 같은 키를 사용하여 암호화를 하더라도 중간 연산 값은 다르게 나타나며, 전력분석공격을 시도하더라도 중간 값 데이터에 대한 상관관계를 파악할 수 없어 공격이 어렵다[6].

사례 2)는 비밀 중간키를 이용한 방어대책을 제안하였다. 암호 알고리즘은 비밀 중간키로부터 마스터키의 추정이 가능하고, 알고리즘의 실행 연산(연산자와 알려진 연산값)이 알려져 있으면 전

력분석으로 비밀 중간키를 찾아서 마스터키를 알아내는 것이 가능함으로써 가능한 조건을 바꾸어 알려진 연산값과 연산자를 숨기거나, 마스터키를 비밀 중간키로부터 추정이 불가능하게 하면 전력분석공격에 대한 방어대책이 된다고 제안하였다[7].

사례 3)은 기존의 마스킹 알고리즘의 시간 효율을 개선하여 전력분석공격에 대응할 수 있는 마스킹 알고리즘과 구현 방법을 제안하였다. 먼저 적응형 랜덤(Adaptive Random) 마스킹 알고리즘은 마스킹 중간에 입력 마스크를 역원 마스크로 변형 시켜 입력 바이트 마다 다른 마스크 값을 사용하는 경우에도 쉽게 마스킹 계산이 되도록 설계하였고, 아핀 테이블을 이용하여 연산 속도를 90%이상 줄였다. 이 결과 기존의 S-Box 테이블 생성 방법 보다는 메모리 효율이 높으며, RAM 메모리 사용이 적기 때문에 스마트카드와 같이 RAM이 작은 임베디드 시스템 환경에서는 효율적으로 이용 가능한 장점을 가진다[8].

사례 4)는 비동기회로 설계 기법을 이용하여 전력분석공격에 대응할 수 있는 방법을 제안하였다. 먼저 동작전력균등화(Operation Balancing)를 이용하여 입력데이터 1과 0을 처리할 때 나타나는 전력소모 패턴의 차이를 최소화 하였으며, 비동기회로로 인해 발생하는 DPA 동기 실패(DPA Synchronization Failure)는 전력분석공격을 하기 위해선 더 많은 개수의 입력샘플을 요구하게 되며, 결과적으로 공격을 더욱 어렵게 하였다[9].

Ⅲ. 결 론

현재 전력분석공격이 부 채널 공격 중에서 가장 강력한 공격이며, 알고리즘이 구현된 방법이나 환경에 따라 얼마든지 공격이 가능하다. 따라서 대응 기술들이 필요한 시점이다. 본 논문에서는 암/복호화 서명 등 하드웨어에서 어떠한 동작을 수행할 때 누출되는 정보 중 소모 전력을 이용한 전력분석공격의 대응기술과 최근 연구된 사례들을 분석하였다.

연구된 사례들을 분석하였을 때 크게 하드웨어 대응기술과 소프트웨어 대응기술로 나눌 수 있으며, 각각의 특징을 가지고 있다. 전력분석공격의 특성상 소비전력을 통해 공격을 시도하기 때문에 하드웨어 대응기술에서는 소비전력을 무작위로 하는 방법과 일정한 소비전력이 발생하도록 회로를 설계하는데 목적을 두고 있지만 비용이 비싸다는 단점을 가지고 있다. 그리고 소프트웨어적 대응기술은 알고리즘 자체에 대응기술을 적용하여 처리되는 데이터와 전력 소모 값 사이의 의존성을 제거하는데 목적을 두고 있다. 하지만 하나의 대응기술을 적용 하였을 때, 암호 알고리즘의 안전성에 대한 확신이 없다. 그러나 두 가지 이상의 대응기법을 적용하게 되면 기존의 암호 알고리즘 보다 성능저하 우려가 있어 사실상 사용이 불가능 하다. 이러한 결과를 볼 때 앞으로 전력분석공격에 대한 성능고도화를 위한 연구가 필요하다 생각된다.

감사의 글

이 논문은 2013년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행되었으며(과제번호:2013-071188), 부산광역시에서 지원하는 BB21 과제에서 지원받았음.

참고문헌

[1] P. Kocher, J. Jaffe, and B. Jun, “Differential power analysis,“ Advances in Cryptology, CRYPTO’99, LNCS 1666, pp. 388-397, 1999.

[2] L. Goubin, J. Paratin, “DES and differential power analysis“, CHES’99, LNCS 1717, pp.158-172, 1999.

[3] S. Mangard, O.Elisabeth, and Thomas Popp, “Power analysis attack: Revealing the secrets of smart cards, Springer, p.338, 2007.

[4] E. Oswald, S. Mangard, C. Herbst, and S. Tillich, “Practical Second-Order DPA Attacks for Masked Smart Card Implementations of Block Ciphers,” In CT-RSA’06, LNCS 3860, pp. 192-207, Springer-Verlag, 2006.

[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] 김용민, 김동규, 이문규 “전력분석공격 방지 기법을 적용한 ARIA 하드웨어 모듈 구현”, 대한전자공학회 하계학술대회 제33권, 1호, 2010

[7] 박영구 외, “비밀 중간키를 이용한 소프트웨어적 전력분석공격 방어대책”, 한국정보통신학회논문지, Vol. 17, No. 12, 2013, 12

[8] 강준기, 최두호, “이차차분전력분석공격에 안전한 효율적인 ARIA 마스킹 기법”, 대한전자공학회 하계종합학술대회, 제34권, 1호, 2011

[9] 이동욱, 이동익, “비동기회로 설계기술을 이용한 DPA(차분전력분석공격) 방어방법에 관한 연구”, 대한전자공학회 하계종합학술대회, 제26권, 1호, 2003