情 報 保 護 學 會 誌
第 16 卷 第 4 號, 2006. 8

부채널 공격법과 이의 대응법에 대한 연구 동향*

정 석 원†

요 약

전통적인 암호시스템의 분석방법은 암호 프리미티브들로 구성된 부분을 블랙박스로 생각하고 이들을 구성하는 수학적 함수를 분석하여 이론적인 안전성을 정량화 했다. 그러나 암호 프리미티브가 이론적으로 안전하다고 해도 이들을 적용한 암호시스템을 구축할 때 구현 방법에 따라 비밀정보와 연관된 내부 함수가 실행되면서 연산시간, 소모전력, 전자복사, 오류결과 등의 부가적인 정보를 밖으로 누출하는 경우가 있다. 최근 들어 이런 부채널 정보를 통해 비밀정보를 유추하는 기술이 발전하였는데 시차공격법, 전력분석법, 전자복사 공격법, 오류 공격법, 오류 메시지 공격법 등 여러 가지 공격법이 알려지고 있다. 부채널 공격법을 통해 비밀키 암호 알고리즘, 공개키 암호 알고리즘, 해쉬함수 등을 프리미티브로 사용하여 구현한 암호 메카니즘의 취약점이 분석되었으며, 이를 막을 수 있는 대응법도 다양하게 제안되고 있다. 본 고에서는 부채널 공격법과 이의 대응법에 대한 최근 동향을 살펴본다.

Ⅰ. 서 론

비밀키 알고리즘, 공개키 알고리즘, 해쉬함수 등 암호학적 알고리즘들은 컴퓨팅 시스템, 네트워크 시스템이나 통신시스템에 인증, 무결성, 비밀성, 전자서명 등의 보안 기술을 제공하는 메카니즘을 만드는 기본 프리미티브로 사용되고 있다.

이러한 보안 메카니즘을 구성하기 위해서 어떤 함수를 사용하여야 하는가는 명시되어 있으나 이들 함수들이 어떻게 구현되어야 하는가는 명시되어 있지 않다. 즉, 보안 프로토콜 명세는 암호 알고리즘이 범용 프로세서에서 구동되는 소프트웨어로 구현되든지 특정 하드웨어로 구현되는지 상관없이 정의되어 있다. 이러한 보안 메카니즘과 구현 방법을 분리하여 생각하는 것은 암호 시스템과 암호 프로토콜을 이론적으로 분석하는 것을 가능하게 한다. 이 경우 일반적으로 암호 함수가 구현된 것을 블랙박스로 생각하고 그 내부를 관찰할 수도 없고, 악의적인 의도를 가진 객체에 의해 조작될 수도 없다고 가정한다. 이러한 가정 아래에 암호 알고리즘의 안전성을 키의 크기로 정량화한다.

그러나 현실적으로는 보안 메카니즘만이 완벽한 보안 솔루션을 제공하는 것과는 거리가 있다.[4] 공격자가 암호 시스템을 공격하기 위해 계산 복잡도 측면에서 암호 프리미티브를 분석한다는 가정은 실현성이 없다. 공격자는 공격하기 어려운 이론적인 공격법을 택하기 전에 암호 프리미티브를 구현하며 생긴 약점, 암호 메카니즘을 배치하면서 생긴 약점 등을 찾아 공격을 하는 것이 일반적이다.

암호 알고리즘은 항상 물리적인 디바이스 위에 소프트웨어나 하드웨어로 구현되며, 알고리즘이 동작할 때 물리적인 디바이스 환경과 상호작용을 하고 물리적인 디바이스에 영향을 미친다. 공격자는 이러한 물리적인 상호작용을 관찰하는 것이 가능하며, 이로부터 발생하는 정보는 암호분석에 유용하게 사용될 수 있다. 이 정보를 부채널 정보라고 하며 부채널 정보를 이용하여 공격하는 방법을 부채널 공격법(Side-Channel Attacks: SCA)이라고 한다. 전통적인 암호분석법은 암호 알고리즘을 수학적인 대상으로 보는 반면 부채널 공격법에서는 알고리즘이 구현된 방법에 초점을 둔다.

1965년 Wright가 쓴 책에 최초의 공식적인 부채널 공격법으로 영국의 비밀 정보부인 MI5가 영국 내 이집트 대사관에서 사용하던 암호기의 회전자가 돌아가는 소리를 듣고 암호기법을 분석하였음을 소개하고 있다.[46] 그러나 1996년에 Kocher가 제안한 부채널

* 본 연구는 정보통신부 대학 IT연구센터 육성·지원 사업의 연구결과로 수행 되었습니다.
† 목포대학교 정보보호전공 (jsw@mokpo.ac.kr)

공격법이[27] 학문적인 연구의 태동이 되었으며, 이후 다양한 부채널 공격법과 이의 대응법이 소개되었다. 부채널 공격법은 비밀키을 가지고 있는 디바이스의 내부 상태와 연산과정에서 발생하는 소비전력량, 계산시간, 전자복사 등의 물리적인 정보 사이의 연관성을 이용하여 비밀키 값을 알아내는 방법이다.

본 고에서는 최근 들어 암호시스템의 안전성을 측정하는 새로운 도구인 부채널 공격법에 대해서 알아본다. 먼저 부채널 공격법이 전통적인 안전성 분석 모델과 어떻게 다른지를 살펴보고, 부채널 공격법을 분류해 본다. 그리고 지금까지 알려진 시차공격법, 오류공격법, 전력분석법, 전자복사공격법, 오류 메시지 공격법 등에 대한 부채널 공격법에 대한 동향에 대해서 살펴보고, 끝으로 이들 공격법에 대한 대응방법을 알아본다.

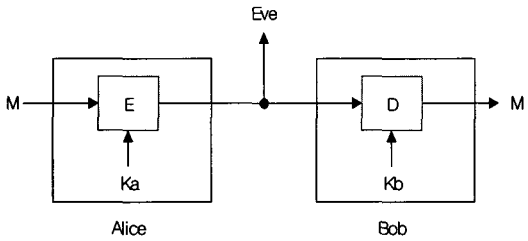
Ⅱ. 부채널 공격법의 모델

암호 프리미티브는 추상화된 수학적 대상으로 보는 입장과 특정 프로세서나 특정 환경에서 구동되는 프로그램 내에 구현된 대상으로 보는 입장이 있다. 수학적 대상으로 보는 입장에서는 전통적인 암호분석법을 통해 프리미티브의 안전성을 분석하고, 구현의 대상으로 보는 입장에서는 부채널 암호분석법에 의해 프리미티브의 안전성을 분석한다. 부채널 암호분석법은 구현에 의존된 특성을 통해 계산과정에서 나타나는 비밀 정보를 찾아내는 것이다. 따라서 이 방법은 일반적인 경우에 적용되지는 않지만 종종 전통적인 암호분석법보다 강력할 때가 있어서 암호 디바이스를 구현하는 사람은 이 분석법에 대응하도록 구현을 하도록 해야 한다.

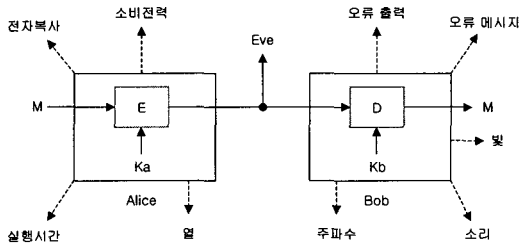
전통적인 암호분석법으로 암호 프로토콜의 안전성을 분석할 때 공격자는 프로토콜의 구조를 완벽하게 알고 있고 모든 공개키를 가지고 있지만 비밀키에 대한 정보를 모른다고 가정한다. 또한 공격자는 정당한 사용자들 사이에 오고가는 자료를 가로챌 수 있으며, 필요에 따라 자료를 선택하여 암호 시스템 내에 투입하여 결과를 얻을 수도 있다. 공격자는 이러한 자료를 바탕으로 풀기 어렵다고 여겨지는 기반 문제를 풀거나 프로토콜의 특정 부분의 흐름을 이용하여 프로토콜의 안전성을 와해시킨다. 이러한 과정에서 수학적인 추상화는 암호 프리미티브를 분석하는데 아주 유용한 도구이다. 암호 설계자는 암호 알고리즘의 안전성을 평가할 때 암호 알고리즘을 수학적 함수로 보고 [그림 1]과 같은 시나리오를 사용한다.

알고리즘의 안전성은 정당한 사용자의 비밀정보를 가지고 있는 암호 시스템을 블랙박스 형태로 보고 이에 접근할 수 있는 공격자의 능력을 측정한다. 그러나 이러한 가정이 항상 충분한 것은 아니다. 암호 알고리즘이 전통적인 분석법에 대해서 안전하다고 해도 비밀키가 저장된 장치의 불법적인 침입에 의해 비밀키의 누출이 가능하여 암호 시스템의 붕괴를 가지고 올 수 있다. 최근에 암호 디바이스의 구현 방법이나 구현 환경 조건을 이용한 공격이 가능해짐이 알려지고 있다. 이러한 공격법은 전통적인 분석법에서 고려되지 않았던 프로토콜의 실행 중에 발생하는 부가적인 정보를 이용한다. 예를 들면, 공격자는 스마트카드 내에서 개인키와 연관된 연산을 수행할 때 발생하는 소비전력이나 전자복사 방출을 이용할 수 있다. 또한 공격자는 암호 연산이 수행될 때 걸리는 시간을 측정할 수도 있고, 암호 디바이스가 오류를 일으킬 때 어떻게 행동하는지를 분석할 수도 있다. [그림 2]의 시나리오에서 보듯이 소비전력, 실행시간, 전자복사, 오류 출력 등의 부채널 정보는 현실적으로 수집이 쉬우며, 이를 이용한 분석법인 부채널 공격법은 시스템의 전체 안전성을 분석하는데 중요한 방법이 되고 있다.

부채널은 시스템으로부터 발생하는 의도적이지 않은 채널을 의미한다. 1996년 Kocher는 [27]에서 암호 알고리즘의 연산시간의 차이가 키에 대한 정보를



[그림 1] 전통적인 암호학적 모델



[그림 2] 부채널을 포함한 암호학적 모델

누출한다는 사실을 이용하여 Diffie-Hellman, RSA, DSS 등의 공개키 암호 시스템이 공격 가능함을 보였다. 이 논문이 발표될 당시에는 암호 알고리즘을 구현할 때 효율성에 초점이 맞추어져 있었는데 이러한 사실이 공격을 가능하게 하였다.

부채널 공격법은 일반적인 구현 환경에 모두 적용되는 것은 아니다. 스마트카드와 같이 신뢰할 수 없는 외부로부터 전력을 공급받는 에는 암호 모듈의 연산 시 발생하는 소비전력량을 측정하여 공격이 가능하다. 그러나 안전한 장소에 위치하고 있는 워크스테이션의 경우에는 소비전력을 측정하여 공격하는 방법은 위협이 되지 않는다.

Kocher에 의해 시차분석법이 제시된 이후 전력분석법, 오류공격법, 전자복사분석법 등 다양한 부채널 공격법이 연구되었으며, 이들 공격법에 대한 대응법도 활발히 제안되고 있는 중이다.

Ⅲ. 부채널 공격의 분류

부채널 공격은 계산과정의 제어와 관련된 분류, 모듈에 접근하는 방법에 따른 분류, 분석과정에 사용된 방법에 따른 분류로 그 종류를 나눌 수 있다.[48]

1. 계산과정의 제어와 관련된 분류

공격자가 계산과정의 제어를 어떻게 하느냐에 따라 부채널 공격은 크게 수동적 공격(passive attacks)과 능동적 공격(active attacks) 두 가지 종류로 나눌 수 있다. 수동적 공격은 공격자가 목표 시스템의 동작과정 중에 어떤 정보를 얻지만 목표 시스템의 동작에 영향을 주지 않는 것이다. 즉, 목표 시스템은 수동적 공격이 일어날 때나 공격이 일어나지 않을 때 모두 똑같이 정상적인 동작을 한다. 그러나 능동적 공격은 공격자가 목표 시스템의 동작에 영향을 미쳐서 동작 결과를 관찰할 수 있는 것이다.

2. 모듈에 접근하는 방법에 따른 분류

공격자가 접근할 수 있는 보안 하드웨어 모듈의 물리적, 전기적, 논리적 인터페이스를 점검하는 것은 모듈의 안전성을 분석하는 데 유용하다. Anderson 등은[5] 이런한 점을 바탕으로 침입 공격(invasive attacks), 준 침입 공격(semi-invasive attacks) 그리고 불 침입 공격(non-invasive attacks)으로 공격법을 구분하였다.

2.1. 침입 공격

침입 공격은 보안 모듈 또는 장치의 내부 성분에 직접적으로 접근할 수 있도록 패키징을 분해하는 것을 포함한다. 예를 들면 보안 모듈의 보호막 층에 구멍을 뚫고 데이터 버스에 탐사 침(probe needle)을 직접대서 전송되는 데이터를 알아내는 것이 있다. 이러한 침입 공격을 막는 방법으로는 변형방지(temper-resistant) 기법이나 침입반응 메카니즘을 하드웨어 모듈에 장착하는 방법이 주로 사용된다.

2.2. 준 침입 공격

준 침입공격의 개념은 Skorobogatov와 Anderson에 의해 제안된 것으로[41] 보호막 층의 손상이나 전기적 접촉 없이 디바이스에 접근을 하는 방법이다. 이러한 방법에는 레이저 광선을 디바이스에 쬐여 메모리 값을 바꾸어 디바이스의 출력 값을 바꾸는 것이 있다.

2.3. 불 침입 공격

불 침입 공격은 디바이스의 연산과정을 관찰하거나 조작하는 것으로 자연발생적으로 외부로 누출되는 정보를 관찰하여 디바이스 내의 비밀정보를 유추하는 방법이다. 이러한 방법에는 디바이스의 특정 연산시간을 측정하거나 특정 연산을 수행할 때 소모되는 전력량 등을 측정하여 이와 연관된 비밀정보를 얻는 시차분석법, 전력분석법 등이 있다. 이러한 침입이 아닌 공격의 중요한 특징은 디바이스가 공격이 되고 있어도 전혀 인지 없이 정상적으로 작동을 한다는 것이다.

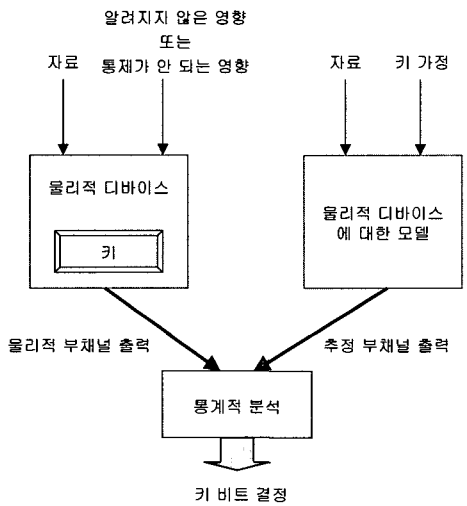
Ⅳ. 부채널 공격법

부채널 공격법은 표본 자료의 분석과정에 사용된 방법에 따라 단순 부채널 공격법(Simple Side Channel Attacks: SSCA)과 차분 부채널 공격법(Differential Side Channel Attacks: DSCA)으로 나눌 수 있다.

SSCA는 연산의 수행과정에서 발생하는 한 개의 추적정보(trace)를 이용하여 비밀정보를 유추하는 방법이다. 이는 공격 대상의 연산에서 발생하는 신호(signal) 부채널 정보가 대상 연산과 상관없이 발생하는 잡음(noise) 부채널 정보 보다 아주 클 때 사용

이 가능하다. DSCA는 연산결과 자료와 연산과정에서 발생한 부채널 정보의 상관성을 관찰하여 비밀 정보를 알아내는 방법으로 많은 추적정보와 통계적인 방법을 사용한다. 이러한 특징으로 인해 SSCA가 잡음이 많을 때 사용하기 어려운 반면 DSCA는 잡음이 많은 경우에도 적용이 가능하다. 따라서 DSCA가 SSCA보다 강력한 공격법이라 할 수 있다.

DSCA는 암호 모듈의 자료와 이와 동시에 발생하는 부채널 누출 사이의 상관성을 이용하는 것인데, 일반적으로 이들의 상관성은 매우 작다. 그래서 통계적인 방법을 사용하여 이들 사이의 상관성을 효과적으로 알아내는 방법이다.([그림 3]) DSCA 공격법에서 공격자는 공격대상 모듈에 대한 가설 모델을 설정한다. 이 모델의 특성은 공격자의 능력에 따라 달라진다.



[그림 3] DSCA의 일반적인 분석방법

가설 모델은 디바이스의 부채널 출력 값을 추정하는데 사용된다. 이는 여러 시간대에 대한 한 가지 형태의 부가정보일 수도 있고, 여러 부채널을 통해 누출되는 정보일 수도 있다. 공격법에 한 개의 출력 값이 사용될 때 일계 공격법(first-order attack)이라 하고, 두 개나 그 이상의 출력 값을 사용할 때 이계 공격법(second-order attack) 또는 고계 공격법(higher-order attack)이라 한다.

1. 알려진 공격법들

이 절에서는 지금까지 알려진 부채널 공격법에 대해서 살펴보겠다. 부채널 공격법은 블록 암호알고리즘(DES, AES, Camellia 등), 스트림 암호알고리즘(RC4, RC6, A5/1 등) 또는 공개키 알고리즘(RSA ElGamal, ECC, XTR 등)을 소프트웨어나 하드웨어로 구현하여 구축한 서명기법, 메시지 인증코드, 암호 프로토콜, 암호시스템 그리고 네트워킹 시스템에 적용되어 공격에 성공을 거두었다.

많은 전문가들은 좋은 암호 알고리즘을 사용한다고 해서 응용시스템의 안전성을 보장받는 것은 아니라고 얘기한다. 또한 시스템의 각 요소가 안전하다고 해도 전체 시스템이 안전한 것은 아니다. 복잡한 시스템 일수록 이의 안전성은 여러 각도에서 다양한 공격법을 대상으로 진단되어야 한다. 부채널 공격법은 안전성 분석 방법 중 중요한 한 가지로 여겨지고 있다.

부채널 공격은 암호 프리미티브나 프로토콜이 구현된 암호 모듈의 부채널로부터 발생되는 연산시간, 소비전력, 전자파 등을 분석하여 특정 정보를 알아내는 방법이다. 또한 하드웨어나 소프트웨어의 장애, 계산상의 오류 등을 유발하거나 주파수, 온도 등의 변화를 발생시켜 부채널 정보를 얻어 특정정보를 알아내는 방법이다. 이렇듯이 부채널 공격법은 암호 프리미티브의 구현 구조뿐만 아니라 하드웨어나 소프트웨어 요소의 특성을 시스템 공격에 이용하는 기법이다. 따라서 수학적 구조를 바탕으로 암호 프리미티브를 분석하는 것과는 달리 부채널 분석법은 구현을 포함하고 있다. 이러한 관점에서 암호시스템의 안전성은 구현의 완벽성에 을 좌우되며, 구현상 약간의 차이가 안전성에 큰 차이를 나타내게 됨을 뜻한다.

1.1. 시차공격법(Timing Attack)

시간의 최적화를 목적으로 구현된 암호 알고리즘은 때때로 내부 연산 시간이 다른 경우가 있다. 이런 연산이 비밀정보를 처리한다면 처리 시간에 대한 차이가 정보를 제공하게 되고, 얻은 정보들에 대한 통계적인 분석을 통해 비밀정보를 획득할 수 있게 된다. 이러한 개념은 Kocher에 의해 처음으로 제시되었다.[27]

시차공격법은 암호 연산을 수행하는 시간을 측정하여 사용자의 비밀정보를 얻어내는 방법이다. 기본적인 원리는 연산이 수행될 때의 시간 차이를 이용하는 것으로 다음과 같은 가정을 따른다.

- 암호 연산의 실행 시간은 키와 연관된 정보에 의존한다.(현재 구현된 하드웨어 중 일부는 이런 조건을 만족하기도 하지만 잡음을 넣음으로써 시차공격이 가능하지 않도록 하는 효율적인 하드웨어가 다양하

게 제안되고 있다. 소프트웨어의 경우 조건문 분기 때 같은 시간이 걸리도록 연산을 구성하여 시차공격에 대응하고 있다.)
- 키가 바뀌지 않는 동안에 충분한 양의 암호화를 수행할 수 있다. (시도와 응답 프로토콜(challenge-response protocol)이 좋은 예이다.)
- 알려진 오류에 대한 시간 측정이 가능하다. (오류가 적으면 적을수록 더 적은 시간 측정량이 필요하다.)

1996년 Kocher에 의해 시차공격법이 제안된 이후 Dhem 등이 RSA가 구현된 스마트카드에 적용하였고[16], Hevia 등이 DES에 대해 시차공격법을 적용하여 비밀키 정보를 얻는데 성공하였다.[23]

OpenSSL은 아파치 웹 서버에 SSL 기능을 제공하는 암호 라이브러리로 잘 알려져 있다. Brumley와 Boneh는 시차공격법을 원격으로 이용하여 지역 네트워트에 있는 OpenSSL 기반의 웹 서버로부터 RSA의 개인키를 찾는 방법을 설명하였다.[10] 이들은 약 2시간 동안 약 3,000만개의 쿼리를 이용하여 RSA 용 1024비트 법의 소인수를 찾았다.

Cathalo 등은 유럽의 NESSIE 프로젝트의 GPS 식별기법에 대해 시차공격법을 적용하였다.[11] 이들은 PC에서 800개의 시간 측정 값을 사용하여 80%의 성공확률로 수 초 만에 개인키를 찾았다. 이들이 제안한 방법은 일반적인 대응책이 적용된 기법에도 공격 가능하며, 중국인의 나머지 정리(Chinese Remainder Theorem)의 사용 유무와 관계없이 적용 가능하다.

1.2. 오류 공격법(Fault Attack)

대부분의 디바이스는 여러 가지 암호 연산을 수행하는데 이러한 연산이 안정적으로 수행된다고 믿고 사용하고 있다. 그러나 암호 모듈이 암호 연산을 하는 동안 하드웨어의 장애나 오류가 발생하면 안전성에 치명적일 수 있다. 이러한 장애 작용 또는 장애로 인한 결과는 중요한 부채널 정보가 된다. 장애 공격은 스마트카드와 같은 하드웨어 기반의 암호 모듈을 공격하는 실질적이고 효율적인 방법이다.

오류 공격은 1996년 Boneh 등에 의해 제안된[8] 이후 대부분의 암호 알고리즘이 이러한 방법에 의해 공격을 받았다. 오류 공격은 공격자에게 암호 시스템을 공격할 수 있는 많은 가능성을 제공한다. 오류 결과를 얻는 방법은 알고리즘에 따라 다르다. 오류 공격의 성공 가능성은 공격자의 능력과 공격자가 유도할 수 있는 오류의 종류에 의존된다. 일반적으로 오류 공격의 모델은 다음과 같은 정보에 의존한다.

- 암호 모듈이 실행되는 동안 공격자가 오류를 발생시킬 정밀한 시점이나 위치
- 오류에 의해 영향을 받는 자료의 길이, 예를 들어 한 비트 또는 한 바이트 등
- 일시적인지 지속적인지에 대한 오류 결과의 내구력
- 한 비트를 바꾸거나 한 바이트를 임의의 값으로 바꾸는 등의 오류의 형태

오류 공격법에는 크게 두 가지로 나누어진다. 하나는 암호 연산 과정에서 발생하는 계산상의 오류를 사용하는 것이고, 다른 하나는 암호 모듈에 고의적으로 충돌되는 입력 자료를 보냄으로써 발생되는 오류를 이용하는 것이다. 전자는 계산과정에 정밀한 전압의 조절 등을 통해 얻을 수 있는 임의적이거나 의도적인 오류를 이용하는 공격법으로 거의 대부분의 암호 메카니즘에 적용될 수 있어 아주 효과적인 부채널 공격법으로 여겨지고 있다. 후자는 모듈에 일반적이지 않은 상황을 발생시켜 계산과정을 중지시키고 모듈이 사용자에게 오류 메시지를 알려주는 경우에 사용하는 공격방법이다. 이 경우 모듈은 정상적인 사용자에 의한 오류 발생인지 의도적인 공격자에 의한 오류인지 구별하기 어렵다.

오류 공격법은 오류 주입과 오류 이용 두 단계로 이루어진다. 첫 번째 단계는 연산과정의 적당한 시간에 오류를 주입하는 과정으로 디바이스의 하드웨어 특성에 의존한다. 비정상적인 저전압 또는 고전압, 클럭, 온도, 복사에너지, 빛 등을 스마트카드에 주입하는 것이 한 예이다. 두 번째 단계는 오류의 결과나 의외의 동작을 이용하는 것으로 소프트웨어 디자인이나 구현 방법에 의존된다. 알고리즘의 경우 오류의 이용법은 알고리즘의 사양에 의존하며 암호분석기법과 결합되어 사용된다.

1996년 Boneh 등이 RSA 서명기법, Fiat- Shamir와 Schnorr 식별 프로토콜에 오류 공격법을 처음 적용한 이후 ElGamal, DSA 서명기법, 타원곡선 암호기법, DES 등에 적용됨이 발표되었다.

2002년에 Skorobogatov와 Anderson은 광학적 오류 공격이라는 실현 가능한 방법으로 스마트카드의 특정 트랜지스터에 빛을 쬐어 오류를 발생시키는 방법을 제안하였다.[41] 이들은 이에 대한 대응책도 제시했는데, 이로 인해 오류 주입이 보안시스템이나 디바이스의 설계 및 테스트에서 고려해야 할 요소임을 보였다.

차분 오류 공격(Differential Fault Attack:

DFA)은 같은 입력에 대해 정상적인 조건에서의 알고리즘의 결과와 비정상적인 조건에서의 알고리즘의 결과를 분석하는 것이다. 비정상적인 조건은 연산 이전에 오류를 주입하여 얻거나 연산과정에 오류를 주입하여 얻을 수 있다. DFA는 이론적인 관점에서 많이 연구되었으며, 대부분의 대칭키 암호 시스템에 적용될 것으로 여겨지고 있다.

1.3. 전력분석 공격법(Power Analysis Attack)

암호 디바이스의 실행시간, 오동작 이외에 전력소비량은 내부에 저장하고 있는 파라미터의 정보를 간접적으로 알려줄 수 있는 아주 좋은 부채널 정보이다. 그러나 전력분석 공격은 하드웨어 구현물에 국한하여 적용이 가능하며, 특히 스마트카드나 비밀키를 저장하는 용도로 사용되는 보안토큰과 같은 장치에 성공적으로 적용되고 있다.

전력분석 공격법은 단순전력분석(Simple Power Analysis: SPA)과 차분전력분석(Differential Power Analysis: DPA)으로 나누어진다. SPA 공격법은 특정 명령어가 수행되는 한 시점에서 입력과 출력의 값이 가지는 소비전력을 통해 비밀정보를 유추하는 방법이다. 따라서 공격자는 공격하고자 하는 시점의 구현방법을 정확히 알고 있어야 한다. 반면 DPA 공격법은 구현에 대한 정확한 방법을 몰라도 분석과정에서 통계적인 처리를 통해 비밀정보를 유추할 수 있는 방법이다. DPA 공격법은 부채널 공격법 중 가장 강력한 공격법 중 하나이며 아주 작은 자원을 사용해서 공격을 할 수 있는 방법이기도 하다.

SPA 공격법은 암호화가 한 번 실행될 때 소비되는 전력에 대한 정보를 분석하여 키 비트를 직접적으로 알아낸다. 공격자가 어떤 명령어가 수행되는가를 알면 유용한 정보를 추출해 내는 것이 가능하다. RSA 암호를 square-multiply 방법으로 구현한 경우 키 비트의 값이 0인 경우와 1인 경우 분기 제어문에 따라 제곱연산만 하는 경우와 제곱연산과 곱셈연산을 하는 경우로 구분되며, 곱셈과 제곱 연산 사이의 전력소비량이 달라 키의 비트 정보를 쉽게 알아낼 수 있다.

DPA 공격법은 비밀정보 비트와 소비전력의 통계적인 상관관계를 적용하는 강력한 공격법이지만 아직까지는 스마트카드와 같은 몇 가지 경우에만 적용이 가능하다. 공격자는 전력추적(power trace)과 암호문 쌍에 대한 집합 $\{T_i, C_i\}$를 모으고, 암호문과 비밀키의 추정 값을 입력으로 받아 한 비트의 결과를 출력하는 분류함수(selection function) D를 선택한다. 만약 키에 대한 추정이 맞으면 분류함수의 분류가 어떤 의미를 갖게 되지만 키에 대한 추정이 틀리면 D는 암호문에 대해 난수함수처럼 작용할 것이다.

공격자는 키에 대한 추정 K_g를 선택하고, 선택함수 D를 이용하여 전력추적을 $D(C_i, K_g)=0$인 것과 $D(C_i, K_g)=1$인 것 두 집합으로 나눈다. 이렇게 나눈 각 집합에 대해 평균을 낸 후 그 값에 대한 차를 계산한다. 추정 키가 잘못되었으면 선택함수 D에 대해 분류된 두 집합은 연관성이 없을 것이고 따라서 평균의 차는 표본의 크기가 커짐에 따라 0에 가까워 질 것이다. 그러나 추정 키가 맞으면 선택함수 D에 대해 분류된 두 집합은 연관성이 있어 평균의 차이는 큰 값을 가지게 될 것이다.

SPA와 DPA 공격법은 1999년에 Kocher 등에 의해 제안되었다.[28] Kocher 등은 DES의 하드웨어 구현물에 대한 실현가능한 전력분석 공격법을 보여주었다. Coron은 전력분석공격법을 처음으로 타원곡선 암호시스템에 적용하였으며 SPA 공격법에 대한 대응법과 무작위 사영좌표(randomized projective coordinates)를 사용한 DPA 대응법을 제안하였다.[15] Akkar 등, Messerges 등은 스마트카드에 대한 전력분석 공격법의 실험적 결과를 제시했으며[2, 34], Gebotys 등은 DSP 프로세서 코어에 대한 전력분석 공격법의 실험적 결과를 제시했다.[18] Chari 등은 SPA와 DPA에 대한 일반적인 대응법과 대응법의 효율성을 측정할 수 있는 형식론적 방법(formal methodology)을 제시하였다.[12]

전력분석법에 대한 하드웨어 기반의 대응법으로는 내부 전력 자원의 사용, 실행되는 명령어 순서의 무작위 사용, 사용되는 레지스터 이름의 무작위 사용, 두 개의 축전기 사용 등이 제안되고 있다.

AES 알고리즘에 대한 DPA 대응법으로는 모든 중간값을 무작위로 만드는 방법이 일반적으로 적용되고 있다. Akkar 등이 AES에 대한 마스킹 기법을 처음 소개하였고[3], 최근에 다양한 마스킹 기법이 제안되었다.[19, 37, 43]

타원곡선 알고리즘의 점 곱셈(point multiplication)에 대한 효과적인 SPA 방어법은 타원곡선 덧셈공식과 두 배 공식을 같게 만드는 것이다. Liardet 등[31]은 자코비 형식(Jacobi form)을, Joye 등[24]은 헤시안 형식(Hessian form)을 Brier와 Joye[9]는 일반적인 바이어스트라스 형식(Weierstrass form)을 사용하였다. Hasan은 코브리츠 곡선 위에서의 점 곱셈에 대한 공격법을 제안하고 이에 대한 대

응법을 제시하였다.[22] 또 다른 타원곡선 점 곱셈에 대한 SPA 대응법은 덧셈과 두 배 연산 패턴을 곱셈기에 독립적으로 구성하는 것이 있고[15], 몽고메리 점 곱셈 알고리즘을 사용하는 방법[35]과 덧셈과 두 배 연산에 사용되는 유한체 연산을에 대해 같은 공식을 사용하는 것도 제안되었다[18].

Joye 등은 주어진 타원곡선과 동형이 되는 임의의 타원곡선을 택하고, 유한체의 표현을 무작위로 택하여 타원곡선 알고리즘에 대한 DPA 대응법을 제시하였다.[25] Goubin은 점 곱셈 알고리즘의 SPA 공격법에 대한 대응법으로 Coron의 방법[15]을 사용하고, 무작위 사영좌표 사용, 무작위 타원곡선 사용, 무작위 유한체 표현 사용 등으로 DPA에 대응법을 적용하였다고 하여도 공격자가 타원곡선 위의 특이점을 선택함으로써 DPA 공격이 가능함을 보였다.[20]

암호 알고리즘을 하드웨어에 구현할 때 공격자가 얻을 수 있는 신호를 감소시키는 것은 가능하나 일반적으로 완전히 제거하는 것은 어렵다. 이러한 이유 때문에 소비전력에 대한 통계적인 방법을 사용하는 차분전력분석법이 가능하게 한다. 따라서 차분전력 공격법은 막기 어려운 공격법으로 인식되며 많은 연구가 진행되고 있다.

1.4. EM 공격법(Electromagnetic Attack)

컴퓨터의 요소인 전자장치들은 연산을 수행하는 동안 전자복사(electromagnetic radiation)를 발생한다. 공격자는 전자복사 방출을 관찰하여 전자장치의 연산과 내부 자료의 연관성을 알 수 있다. 전력분석법과 비슷하게 전자파분석법(ElectroMagnetic Analysis: EMA)도 단순 전자파분석법(Simple ElectroMagnetic Analysis: SEMA)와 차분 전자파분석법(Differential ElectroMagnetic Analysis: DEMA)으로 나뉜다.

전자파 방출을 이용하는 기술은 오랜 동안 국방 분야에서 사용되어 왔다. 최근에 공개된 NSA (National Security Agency)의 TEMPEST 문서에는 전자복사 방출, 선 전도, 음향 방출 등에 대한 기술이 다루어져 있다. Kuhn 등은 모니터에서 방출되는 전자복사 방출을 통해 비디오 스크린의 정보를 알아내는 공격법에 대한 소프트웨어 기반 대응기법을 소개하였다.[29] Quisquater 등은 스마트카드와 같은 암호 디바이스에 전자파분석법을 적용한 실험결과를 처음으로 소개하였고, 전자파분석법과 전력분석법을 비교하였다.[38] Agrawal 등은 EM 방출이 부채널공격이 적용되지 않는 암호 디바이스에 적용가능할 뿐만 아니라 부채널공격에 대한 대응책이 적용된 디바이스에도 적용이 가능함을 보였다.[1]

EMA 공격에 대한 대응법은 신호 강도 감소(signal strength reduction)와 신호 정보 감소(signal information reduction)로 나눌 수 있다. 신호 강도 감소 기술은 회로 재설계를 통해 의도적이지 않은 방출을 줄이는 기법과 물리적으로 안전한 구역이나 보호막을 만들어 주변 열잡음과 대비해서 공격자에게 유용한 신호의 강도를 줄여주는 것이 포함된다. 신호 정보 감소 기술은 연산 도중에 난수성의 삽입이나 키의 재설정 등을 통해 공격 가능한 신호에 대한 통계적 특성을 줄여주는 것이 포함된다.

1.5. 오류 메시지 공격법(Error Message Attack)

SSL, TLS, IPSEC, WTLS 등의 표준에서는 메시지를 먼저 형식화한 후 블록 암호 알고리즘을 이용하여 CBC 모드로 암호화한다. 복호화할 때에 메시지 형식의 유효성을 확인하게 되는데, 형식의 유효성을 확인하기 위해 프로토콜의 통신과정에서 승인이나 오류 메시지를 보내주는 경우 선택 암호문 공격에 의해 형식의 유효성에 대한 부가정보가 누출될 수 있다. 이것은 암호분석을 위한 유용한 부채널이 되며, 이 부채널을 이용하여 공격하는 방법을 오류 메시지 공격법이라고 한다.

Vaudenay는 비밀키 암호시스템에서 메시지가 덧붙임(padding)에 의해 형식화된 후 CBC 모드로 암호화된 경우 오류 메시지 공격법에 의해 공격 가능함을 보였다.[45] 복호화 후 덧붙임이 올바르지 않으면 SSL/TLS는 세션을 닫고, IPSec의 ESP 프로토콜은 오류에 대한 로그를 남기고 WTLS는 오류 메시지를 전송한다. 공격자는 덧붙임에 대한 오류 상태를 알아내어 선택암호문 공격에 사용한다.

오류 메시지 기반의 공격법은 대칭키 알고리즘뿐만 아니라 공개키 알고리즘에도 적용이 가능하다. 공격자가 암호문이 PKCS #1 v.1.5에 따라 암호화가 되었는지에 대한 정보 비트를 알려주는 오라클에 접근이 가능하다는 가정 하에 백만개의 선택 암호문을 사용하여 RSA 암호 시스템이 깨질 수 있음이 보여졌다.[7] 이후 Shoup[40]과 Fujisaki 등은[17] Bellare와 Rogaway[6]가 1994년에 제안한 RSA-OAEP 암호화 기법이 랜덤 오라클 모델에 대해 안전함을 증명하였으며, 그 결과 RSA-OAEP 암호화 기법은 여러 표준에 적용되고 있다.

Klima 등은 EME-OAEP PKCS #1 v.2.1에 의해 암호화된 평문에 대한 새로운 부채널 공격법을 제안하였다.[26] 이들은 또한 RSA PKCS #1 v.1.5의 RSA 암호화 기법에 대한 Bleichenbacher의 공격법과 EME-OAEP PKCS #1 v.2.1의 RSA 암호화 기법에 대한 Manger[33]의 공격법이 어떠한 메시지 인코딩을 적용한 RSA 서명기법에 대한 공격법으로 변환이 가능함을 보였다.

선택암호문 공격에 대응하기 위해서는 덧붙임 한 후 해쉬함수를 이용한 암호학적 CRC(checkable redundancy code) 코드를 삽입하고 이를 암호화하는 방법이 제안되고 있다.

1.6. 기타 공격법

부채널 공격법 중 가장 오래된 것 중 하나가 음향 방출에 관한 것이다. 금고털이는 금고 다이얼을 돌리면서 소리를 들으며 날름쇠가 올바른 자리에 위치하는가를 알아내는 방법을 사용해 왔다. 최근에 Shamir 등은 프로세서의 소리와 연산 사이에 관계가 있다는 가능성을 보였다.[39]

Kuhn은 CRT의 빛이 벽으로 반사되는 광도를 수집하여 CRT에 나타나는 신호를 재구성할 수 있음을 보였다.[30] 이 공격법의 특징은 물리적인 접근이 필요하지 않다는 것이다. Kuhn은 이 공격법이 LCD 신호에도 적용 가능함을 설명하였다. Loughry 등은 LED로부터 방출된 빛의 정보가 디바이스 내에서 처리되는 내부 자료를 분석하는데 사용될 수 있음을 설명하고, 재설계가 이런 종류의 광학적 공격법을 막을 수 있음을 보였다.[32]

오늘날 대부분의 컴퓨터는 프로그램의 실행시간을 평균적으로 증가시키기 위해 CPU와 주기억장치 사이에 캐쉬를 사용한다. 그러나 CPU가 캐쉬에 저장되지 않은 자료에 접근할 때 목표 자료가 주기억장치로부터 캐쉬로 옮겨지는 일이 발생하여 시간 지연이 발생하게 된다. 암호 알고리즘이 실행될 때 캐쉬 메모리를 사용하면 CPU 지연이라는 부가 정보가 발생하게 된다. 소프트웨어로 구현된 DES, AES, Camellia 등의 알고리즘이 이 부가 정보를 이용해 공격을 당하였다.[44] 캐쉬 제거, S-box를 캐쉬에 저장하는 방법, 캐쉬 플러쉬(flush), 시간 또는 캐쉬 미스 왜곡, 응용에 특화된 알고리즘 적용, 분할된 캐쉬 하드웨어의 적용 등이 캐쉬 기반 공격법에 대한 대응법으로 제시되고 있다.

Tiu는 PDA, 핸드폰 등의 모바일 디바이스에 주파수 기반의 부채널 공격법을 제안하였다.[42] 이 방법은 차분전력분석과 비슷한 것으로 관찰 시간대에서 신호의 차분을 계산하는 대신에 주파수대의 전력 스펙트럼 밀도 신호의 차분을 계산하여 분석하는 기법이다. 차분전력분석법이나 차분전자파분석법을 실제 실험에 적용할 때 관찰시점에 전력 추적값이나 EM 추적값이 정렬이 안 되는 경우가 있어 분석이 실패하는 경우가 있다. Tiu의 방법은 추적값들이 정렬이 안 되는 경우에도 적용이 가능할 뿐만 아니라 무작위로 시간 지연을 삽입한 대응법에도 적용이 가능하다.[42]

스캔 기반의 테스트는 순차회로의 제작과정에서 디자인을 검증하는 방법으로 널리 사용되고 있다. Yang 등은 스캔 기반의 테스트에서 사용되는 스캔 사슬(scan chain)을 부채널로 사용하여 DES가 구현된 하드웨어에서 비밀정보를 복원하였다.[47] 그러나 이미 FIPS 140-1에서는 BIST(Built In Self-Test) 방법을 권고하고 있어 FIPS 140-1 기준을 만족하는 암호 칩의 내부 상태는 스캔되지 않아 스캔 기반의 공격이 적용되지 않는다.

2. 부채널 공격에 대한 대응방법

부채널 공격에 대한 많은 대응방법과 대응전략이 제안되고 있는데, 이들 중 Goubin은 다음과 같은 일반적인 전략을 소개하였다.[21]

- 실행시간을 무작위로 옮기고, 기다리는 상태를 넣고, 가짜 명령어를 삽입하고, 연산 실행을 무작위로 하는 등을 하여 암호 알고리즘의 실행에 따른 출력 추적값의 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.

이러한 전략 중에서 알고리즘을 수정하는 대응법이 가장 강력하며 효과적인 것으로 여겨지고 있다.

소프트웨어 기반의 대응법에는 가짜 명령어 사용, 실행 명령 순서의 무작위, 내부 자료에 대한 해밍 무게의 균형, 비트의 분할 등이 사용된다. 하드웨어 기반의 대응법에는 무작위 클럭 사용, 소비 전력의 무작위성, 실행되는 명령어 집합이나 사용 레지스터의 무작위성 등의 기법이 사용되고 있다. 그러나 다양한 신호 처리 기술이 이러한 대응법을 무력화시키고 있다.[14] 소프트

웨어 기반의 대응법은 메모리나 실행시간 면에서 알고리즘의 효율성을 떨어뜨리는 결과를 초래한다. 따라서 가능한 효율성을 적게 떨어뜨리면서 부채널 공격에 대응할 수 있는 방법의 모색이 중요한 과제이다.

2.1. 무작위성 기법(Randomization)

SPA 공격에 대한 일반적인 대응법은 소비전력, 전자복사 방출, 실행 시간등의 다양한 부채널을 통해 누출될 수 있는 자료를 무작위로 만드는 것이다. 공격자는 난수성을 띤 정보만을 얻게 됨으로써 계산과정 중에 포함된 실제 초기값이나 중간 값을 알 수 없다.

타원곡선 암호시스템의 경우 무작위 사영좌표를 사용하는 방법이 SPA 공격에 실질적인 대응법으로 소개되고 있다. 이 경우 공격자는 좌표가 무작위로 변하기 때문에 특정한 값이 나타나는 것을 예측할 수 없다. Okeya 등은 사전 계산된 점들이 나타나지 않는 SPA에 대응하는 스칼라 곱셈 방법을 제안하였다.[35] 이 방법은 단순전력분석에는 효과적으로 대응하지만 차분전력분석에는 대응하지 못한다.

DPA 공격법은 관찰되는 연산과 연관된 비밀정보의 특정 비트를 분류할 수 있는 연관 함수를 사용한다. 이러한 DPA 공격에 대응하기 위해서는 타원곡선의 파라미터를 무작위호 만드는 것이 필요하다. 이를 위해 세 가지 무작위 방법이 소개되고 있다.[15] 첫째는 무작위 점을 사용하여 기저 점(base point)를 마스킹하는 것이고, 둘째는 타원곡선 위수의 임의의 배수를 사용해 비밀 스칼라 값을 난수화 하는 것이고, 셋째는 사영좌표를 이용하여 기저 점을 무작위로 만드는 것이다. 이러한 대응법이 부분적으로 약하게 적용된 몇 가지 경우에 대해 공격이 가능함이 제안되었다.[20, 36] 그러나 아직까지 위에서 언급한 무작위 방법을 모두 사용한 경우에 대한 공격법은 알려지지 않고 있다. SPA 대응법을 적용한 기법은 무작위성을 사용하여 쉽게 DPA 대응 기법으로 변환이 가능하다. 그러나 이러한 대응법의 적용에 따른 연산의 효율성 감소를 최소로 하는 연구가 필요하다.

2.2. 블라인딩 기법(Blinding)

블라인딩은 클라이언트가 입력 x에 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.[13] 블라인드 기법은 웹 서버에 대한 원격 시간 분석법에 효과적인 대응법이며[9], 하드웨어 암호 모듈에 대한 전력분석과 시간분석에 대응하는 기법이다.

2.3. 마스킹 기법(Masking)

자료의 마스킹 기법은 전력분석법과 시차분석법에 널리 사용되는 소프트웨어 수준의 대응법이다. 마스킹 기법은 알고리즘의 연산과정 중에 나타난 중간 값을 감추는 것을 의미한다. 메시지와 키는 연산의 시작 단계에서 임의의 마스크 값으로 감추어진 후 알고리즘을 정상적으로 수행한다. 마스크 된 값은 각 라운드의 끝이나 선형 계산이 끝나는 부분 등 어떤 특정 단계에서 원래 예정된 값으로 되돌려진다.

AES의 경우 알고리즘의 수행 중간의 상태 바이트 값 x에 대해서 임의의 마스크 값 m과 마스킹으로 불리는 함수 f를 선택해서 $f(x, m) = x \circ m$로 마스킹을 하는 것이다. 여기에서 연산 $\circ$은 비트 단위의 XOR 연산이거나 유한체 위의 덧셈연산 +(additive masking) 또는 유한체 위의 곱셈연산 x(multiplicative masking)로 정의된다. Trichina 등은 AES 블록 암호 알고리즘의 비선형 함수인 바이트 대치(Byte Substitution) 연산 전에 부울 마스크(boolean mask)를 곱셈 마스크(multiplicative mask)로 바꾸는 효율적인 방법을 제시하여 전력분석 공격에 대응하였다.[43]

V. 결 론

부채널 공격법은 암호 알고리즘 자체의 안전성이 높다고 하더라도 암호 알고리즘이 구현된 방법이나 구현된 환경에 따라 적용이 가능한 공격법이다. 암호 알고리즘은 특정 디바이스에 소프트웨어나 하드웨어로 구현이 되며, 암호 알고리즘이 동작할 때 디바이스는 실행시간, 소비전력, 전자복사, 오류 출력, 소리 등의 부채널 정보를 누출하며, 이러한 부채널 정보는 공격자에게 좋은 정보가 될 수 있다. 이러한 부채널 분석법은 전체 암호 시스템의 약점을 찾아 공격하는 현실적인 공격법으로 인식되고 있으며, 이러한 점이 안전한 암호 시스템을 구축하는데 좋은 도구로 이용되고 있다.

본 고에서는 지금까지 알려진 부채널 공격법과 이의 대응법에 대해서 알아보았다. 여러 가지 구현 환경에 대한 공격법과 이의 대응법이 개별적으로 소개되었으

나 아직까지 암호 시스템에 대한 일반적인 대응법이 제시된 적은 없다. 또한 부채널 공격법이 형식론적 기술이나 계산 복잡도 이론의 적용이 가능할 수도 있으며, 지금까지 알려지지 않은 공격법이 조만간 나타날 수도 있다. 암호학은 암호설계와 암호분석의 지속적인 싸움의 과정으로 발전하고 있는 학문이다. 부채널 공격법도 암호학의 큰 틀에 속하여 새로운 공격법과 이의 대응법이 계속 나타날 것을 여겨진다. 암호 알고리즘이 구현되는 환경에 적용 가능한 부채널 공격법에 대한 정확한 이해와 이의 대응법을 적절히 배치시켜 구현하는 것이 안전한 시스템을 개발하는 중요한 요소이므로 부채널 공격법과 이의 대응법에 대한 연구는 앞으로도 중요한 과제이다.

참 고 문 헌

[1] D. Agrawal, B. Archambeault, J. R. Rao, P. Rohatgi, "The EM Side-Channel(s)", CHES 2002, LNCS 2523, pp.29-45, 2003.

[2] M. Akkar, R. Bevan, P. Dischmp, and D. Moyart, "Power Analysis, what is now possible...", ASIACRYPT 2000, LNCS 1976, pp.489-502, 2000.

[3] M. Akkar, C. Girard, "An Implemetation of DES and AES, Secure against Some Attacks", CHES 2001, LNCS 2162, pp.309-318, 2001.

[4] R. Anderson, *Security Engineering: A guide to Building Dependable Distributed Systems*, John Wiley & Sons, 2001.

[5] R. Anderson, M. Bond, J. Clulow, and S. Skorobogatov, "Cryptographic Processors-A Survey", Proc. of IEEE, Vol. 94, No.2, pp.357-369, 2005.

[6] M. Bellare, P. Rogaway, "Optimal Asymmetric Encryption", Eurocrypt'94, LNCS 950, pp.92-111, 1994.

[7] D. Bleichenbacher, "Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS #1", CRYPTO'98, LNCS 1462, pp.1-12, 1998.

[8] D. Boneh, R. A. DeMillo, R. J. Lipton, "On the importance of checking cryptographic protocols for faults", EUROCRYPT'97, LNCS 1233, pp.37-51, 1997.

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

[10] D. Brumley, D. Boneh, "Remote Timing Attacks are Practical", Proc. of 12th Usenix Security Symposium, 2003.

[11] J. Cathalo, F. Koeune, J. J. Quisquater, "A New Type of Timing Attack: Application to GPS", CHES 2003, LNCS 2779, pp.291-303, 2003.

[12] S. Chari, C. Jutla, J. Rao, P. Rohatgi, "Towards sound approaches to counteract power-analysis attacks", CRYPTO'99, LNCS 1666, pp.398-412, 1999.

[13] D. Chaum, "Blind Signatures for untraceable payments", CRYPTO'82, pp.199-203, 1983.

[14] C. Clavier, J. S. Coron, N. Dabbus, "Differential Power Analysis in the Presence of Hardware Countermeasures", CHES 2002, LNCS 1965, pp.252-263, 2002.

[15] J. S. Coron, "Resistance against Differential Power Analysis for Elliptic Curve Cryptosystems", CHES'99, LNCS 1717, pp.292-302, 1999.

[16] J. F. Dhem, F. Koeune, P. A. Leroux, P. Mestre, J. J. Quisquater, J. L. Williems, "A practical implementation of the timing attack", Proc. of CARDIS 1998, 1998.

[17] E. Fujisaki, T. Okamoto, D. Pointcheval, J. Stern, "RSA-OAEP is secure under the RSA assumption", CRYPTO 2001, LNCS 2139, pp.260-274, 2001.

[18] C. H. Gebotys, R. H. Gebotys, "Secure elliptic curve implementations: an analysis of resistance to power-attacks

in a DSP processor", CHES 2002, LNCS 2523, pp.114-128, 2003.

[19] J. Golic, C. Tymen, "Multiplicative Masking and Power Analysis of AES", CHES 2002, LNCS 2535, pp.198-212, 2003.

[20] L. Goubin, "A Refined Power-Analysis Attack on Elliptic Curve Cryptosystems", PKC 2003, LNCS 2567, pp.199-211, 2003.

[21] L. Goubin, J. Paratin, "DES and differential power analysis", CHES'99, LNCS 1717, pp.158-172, 1999.

[22] M. Hasan, "Power analysis attacks and algorithmic approaches to their countermeasures for Koblitz curve cryptosystems", IEEE Trans. on Computers, vol.50, pp.1071-1083, 2001.

[23] A. Hevia, M. Kiwi, "Strength of two data encryption standard implementations under timing attacks", ACM Trans. on Information and System Security, Vol. 2, pp.416-437, 1999.

[24] M. Joye, J. J. Quisquater, "Hessian elliptic curve and side-channel attacks", CHES 2001, LNCS 2162, pp.402-410, 2001.

[25] M. Joye, C. Tymen, "Protections against differential analysis for elliptic curve cryptography: An algebraic approach", CHES 2001, LNCS 2162, pp.377-390, 2001.

[26] V. Klima, T. Rosa, "Further results and considerations on side channel attacks on RSA", CHES 2002, LNCS 2523, pp.244-259, 2002.

[27] P. Kocher, "Timing attacks on implementations of Diffie-Hellmann, RSA, DSS, and other systems", Crypto'96, LNCS 1109, pp.104-113, 1996.

[28] P. Kocher, J. Jaffe, B. Jun, "Differential Power Analysis", CRYPTO'99, LNCS 1666, pp.388-397, 1999.

[29] M. G. Kuhn, R. J. Anderson, "Soft tempest: hidden data transmission using electromagnetic emanations", Information Hiding 1998, LNCS 2140, pp.200-210, 2001.

[30] M. G. Kuhn, "Optical Time-Domain Eavesdropping Risks of CRT Displays", Proc. of the 2002 Symposium on Security and Privacy, pp.3-18, 2002.

[31] P. Y. Liardet, N. P. Smart, "Preventing SPA/DPA in ECC systems using the Jacobi form", CHES 2001, LNCS 2162, pp.391-401, 2001.

[32] J. Loughry, D. Umphress, "Information leakage from optical emanations", ACM Trans. on Information and System Security, vol. 5, pp.262-289, 2002.

[33] J. Manger, "A Chosen Ciphertext Attack on RSA Optimal Asymmetric Encryption Padding(OAEP) as Standardized in PKCS #1 v2.0", CRYPTO 2001, LNCS 2139, pp.230-238, 2001.

[34] T. S. Messerges, E. A. Dabbish, R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks", IEEE Trans. Computers, 51(5), pp.541-552, 2002.

[35] K. Okeya, T. Takagi, "A More Flexible Countermeasure against Side Channel Attacks Using Window Method", CHES 2003, LNCS 2779, pp.397-410, 2003.

[36] K. Okeya, K. Sakurai, "Power Analysis Breadks Elliptic Curve Cryptosystems even Secure against the Timing Attack", INDOCRYPT 2000, LNCS 1977, pp.178-190, 2000.

[37] E. Osward, S. Mangard, N. Pramstaller, and Vincent Rijmen, "A Side-Channel Analysis Resistant Description of the AES S-box", FES 2005, LNCS 3557, 2005.

[38] J. J. Quisquater, D. Smayde, "Electromagnetic Analysis(EMA): measures and countermeasures for smart cards",

E-smart 2001, LNCS 2140, pp.200-210, 2001.
[39] A. Shamir, E. Tramer, "Acoustic cryptanalysis: on noisy people and noisy machines", Eurocrypt 2004 rump session, 2004.
[40] V. Shoup, "OAEP reconsidered", J. of Cryptology, vol.15, pp.223-249, 2002.
[41] S. Skorobogatov, R. Anderson, "Optical Fault Induction Attacks", CHES 2002, LNCS 2523, pp.2-12, 2003.
[42] C. C. Tiu, *A New Frequency-Based Side Channel Attack for Embedded Systems*, Master degree thesis, Department of Electrical and Computer Engineering, Univ. of Waterloo, 2005.
[43] E. Trichina, D. Seta, and L. Germani, "Simplified Adaptive Multiplicative Masking for AES", CHES 2002, LNCS 2535, pp.187-197, 2003.
[44] Y. Tsunoo, E. Tsujihara, K. Minematsu, h. Miyauchi, "Cryptanalysis of Block Ciphers Implemented on Computers with Cashe", ISITA 2002, 2002.
[45] S. Vaudenay, "Security Flaws Induced by CBC padding - Applications to SSL, IPSEC, STLS", Erutocrypt 2002, LNCS 2332, pp.534-545, 2002.
[46] P. Wright, *Spy Catcher: The Candid Autobiography of a Senior Intelligence Officer*, Viking Press, 1987.
[47] B. Yang, K. Wu, R. Karri, "Scan-Based Side-Channel Attack on Dedicated Hardware Implementations of Data Encryption Standard", ITC 2004, pp.339-344, 2004.
[48] Y. Zhou, D. Feng, "Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptography Module Security Testing", Cryptology ePrint Archive, Report 2005/388, 2005.

〈著 者 紹 介〉

정 석 원(Seok Won Jung)
평생회원

1991년 2월: 고려대학교 수학과 졸업
1993년 2월: 고려대학교 수학과 이학석사
1997년 3월: 고려대학교 수학과 이학박사
2002년 3월 ~ 2004년 2월: 고려대학교 정보보호기술연구센터 연구교수
2004년 3월 ~ 현재: 국립목포대학교 정보보호전공 조교수
〈관심분야〉 암호알고리즘 구현, 스마트카드보안, 방송보안