情 報 保 護 學 會 誌
第19卷 第2號, 2009. 4

정보보호 장치에 대한 부채널 공격 동향

박 제 훈*, 이 훈 재**, 하 재 철***, 문 상 재*

요 약

최근 금융권을 포함한 여러 분야에서 스마트카드의 활용이 급증함에 따라 IC 칩을 내장한 카드의 부채널 공격에 대한 안전성이 이슈가 되고 있다. 부채널 공격이란 IC 카드와 같은 저 전력의 정보보호 장치에 암호 알고리듬을 구현하였을 때 누출되는 연산 시간, 소비 전력, 전자파 등의 부채널 정보를 이용하여 구현된 암호 알고리듬의 비밀 정보를 알아내는 공격 방법이다. Kocher에 의해 부채널 공격이 소개된 이후, 많은 연구 그룹들에 의해 이론적인 연구와 실험적인 연구가 이루어져 왔다. 본 고에서는 시차 분석 공격, 전력 분석 공격, 전자파 분석 공격, 오류 분석 공격 등의 다양한 부채널 공격 방법들과 최근까지의 부채널 공격 실험 동향에 대해서 소개하고 국내외 연구 그룹들에 의해 진행된 실험 결과들을 고찰한다. 또한, 보유하고 있는 부채널 공격에 필요한 실험 장비와 지금까지의 부채널 공격 실험 결과들을 소개한다.

Ⅰ. 서 론

암호 알고리듬과 프로토콜 그 자체는 이론적으로 안전하더라도 구현 환경에 따라서 위협적인 공격이 노출될 수 있다. 스마트카드와 같이 IC 칩이 내장된 암호 장치에 구현된 암호 알고리듬에 대한 부채널 공격이 대표적인 경우로 이는 매우 현실적이고 위협적인 요소로서 국내외에서 활발히 연구가 진행되고 있다. 최근 금융 IC 카드, 전자주민증, 전자 여권 등의 여러 분야에서 IC 칩의 활용이 급증함에 따라 부채널 공격에 대한 안전성이 필수 요건으로 여겨지고 있다.

부채널 공격이란 IC 카드와 같은 저 전력의 정보보호 장치에 암호 알고리듬을 구현하였을 때 누출되는 연산 시간, 소비 전력, 전자기파, 오류 응답 등의 부채널 정보를 이용하여 구현된 암호 알고리듬의 비밀 정보를 알아내는 공격 방법이다. 부채널 공격 (Side Channel Analysis Attack, SCA)에는 크게 수동적 방법으로 시도하는 시차 공격 (Timing Attack, TA), 전력 분석 공격 (Power Analysis Attack, PA), 전자기파 분석 공격 (Electromagnetic Analysis Attack, EMA)이 있으며 능동적 공격 형태인 오류 분석 공격 (Fault Analysis Attack, FA)이 있다. 이와 같은 분류 외에도 부채널 공격은 공격에 사용되는 신호, 비밀키를 추출하는 방법, 공격 대상이 되는 암호 알고리듬, 구현 방식 등에 따라 매우 다양하게 분류할 수 있다. [그림 1]은 부채널 공격의 개념을 간단히 설명하고 있다.

[그림 1] 부채널 공격

본 고에서는 시차 분석 공격, 전력 분석 공격, 전자기파 분석 공격 그리고 오류 분석 공격 등의 다양한 부채널 공격 방법들의 적용 원리에 대해서 간단히 소개한다. 또한, 국내외 연구 그룹들에 의해 진행된 실험 결과들을 고찰하고, 본 연구센터에서 보유하고 있는 부채널 공격에 필요한 실험 장비와 지금까지의 부채널 공격 실험

* 경북대학교 전자전기컴퓨터공학부(jenoon65@ee.knu.ac.kr, sjmoon@knu.ac.kr)
** 동서대학교 컴퓨터정보공학부(hjlee@dongseo.ac.kr)
*** 호서대학교 정보보호학과(jcha@hoseo.edu)

결과들을 소개한다.

Ⅱ. 부채널 공격의 종류 및 소개

2.1 시차 분석 공격

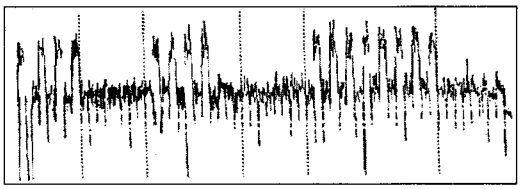
시차 분석 공격은 1996년 Kocher가 CRYPTO'96에서 처음으로 소개한 내용으로 비밀키에 따라서 암호장치가 수행하는 연산 시간을 분석하여 공격 방법이며, 주로 공개키 암호시스템에 적용되고 있다[1]. 이는 Diffie-Hellman, RSA, DSS와 같은 공개키 암호시스템에서 곱셈연산의 수행 시간과 제곱연산의 수행시간이 차이가 나기 때문에 가능하다.

시차 분석 공격을 위해서 공격자는 공격 대상 암호 알고리듬의 연산 시간을 측정한 후, 비밀키에 따른 연산 시간 차이를 분석한다. Dhem 등은 RSA가 구현된 스마트카드에 시차 분석 공격을 적용하였고, Hevia 등은 DES에 대한 시차 분석 공격 방법을 제안하였다[2,3]. 이외에도 수행시간 분석을 통한 몇 가지의 시차 분석 공격 시도가 있었으나 다른 부채널 공격에 비해 공격효과가 낮은 측면이 있어서 최근에는 활발히 연구되고 있지 않다.

2.2 전력 분석 공격

2.2.1 전력 분석 공격의 종류

전력 분석 공격은 1999년 Kocher에 의해 CRYPTO'99에서 DES에 적용된 결과가 처음 소개되었다[4]. 여러 부채널 공격 방법들 중에서 가장 효과적이고 위협적인 공격 방법이라고 알려져 있으며, 현재까지 개발된 대부분의 암호 알고리듬들이 전력 분석 공격에 취약하다고 알려져 있다. 전력 분석 공격은 해밍무게(Hamming weight) 가정과 해밍거리(Hamming Distance) 가정에 기반하고 있다. 이들은 공격 대상 암호 장치의 소비 전력이 연산중에 처리하는 데이터 비트의 해밍무게와 해밍거리에 높은 상관도를 가진다는 것이다. 전력 분석 공격은 크게 단순 전력 분석 공격(Simple Power Analysis Attack, SPA)과 차분 전력 분석 공격(Differential Power Analysis Attack, DPA)으로 나눌 수 있다. 단순 전력 분석 공격은 하나의 측정된 소비 전력 신호의 패턴을 분석하여 비밀 정보를 알아내는 공격 방법이다. RSA 암호 알고리듬의 곱셈 연산과 제곱 연산의 소비 전력 차이나 비밀키에 따른 분기 연산에 의한 소비 전력 차이를 분석한다. [그림 2]는 RSA 암호 알고리듬에 대한 단순 전력 분석 결과를 보여주고 있다.



〔그림 2〕 이진 멱승 알고리듬에 대한 단순전력분석 결과

이진 멱승 알고리듬을 이용하여 RSA 암호 알고리듬을 구현하면 비밀키의 비트가 '1'인 경우에는 제곱 연산과 곱셈 연산이 이루어지고 비밀키의 비트가 '0'인 경우에는 제곱 연산만 이루어지게 된다. 따라서 [그림 2]와 같은 소비 전력 패턴이 나타나고 비밀키를 노출하게 된다.

차분 전력 분석 공격은 단순 전력 분석 공격이 단순히 소비 전력을 관찰하는 것에 더하여 비밀키와 높은 상관관계(correlation)를 가지는 정보를 추출하기 위해 통계적인 분석(statistical analysis)과 에러 정정(error correction) 기술을 사용한다.

전력 분석 공격자는 먼저 암호 장치에 구현된 암호 알고리듬이 수행될 때 소비되는 전력을 표본화(sampling)하여 그 데이터를 수집한다. 다음으로 공격자가 추측한 키를 사용하여 만들어진 소비 전력 모델과 실제 측정된 소비 전력간의 상관도를 분석한다. 공격자의 추정 모델과 실제 소비 전력 사이에 높은 상관도를 가지면 공격자의 추측한 키가 실제 암호 장치에서 사용된 비밀키라고 판단한다. 차분 전력 분석에서는 공격자 추정 모델의 옳고 그름을 판단하기 위해 추정 모델에 의해 분류된 소비 전력 사이의 전력 차이를 관찰하고, 상관도 분석 공격(Correlation Power Analysis, CPA)은 공격자 추정 모델과 측정된 소비 전력간의 상관도를 직접 계산한다[4,5]. 분할 전력 분석 공격(Partioning Power Analysis, PPA)은 기존의 차분 전력 분석 공격과 상관도 분석 공격 방법 등을 일반화하였다[6]. 또한 템플릿 공격(Template Attack), 확률 모델 기반 공격(Stochastic Model for

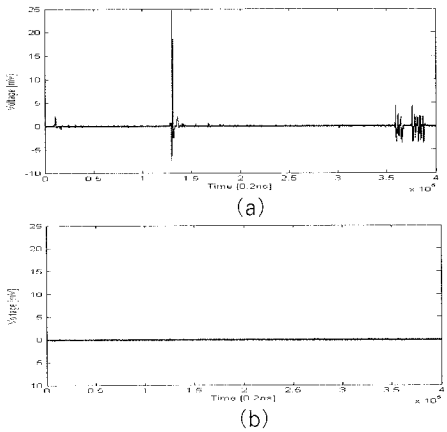
DPA) 들은 전력 분석 공격을 적용하기 전에 측정된 소비 전력과 잡음들을 모델링하여 공격의 효율성을 높이고 있다[7,8]. 이 외에도 마스킹 방어 대책을 무력화 할 수 있는 2차 차분 전력 분석 공격(2nd-order DPA)[9], 타원곡선 암호시스템에서 비밀키에 따른 특이점 계산 유무를 소비 전력 신호로 확인하는 공격(Refined Power Analysis, RPA, Zero-value Point Attack, ZPA)[10,11], 선택된 입력 메시지에 따라 나타나는 전력 파형의 패턴을 분석하는 공격(Doubling Attack, 2-torsion Point Attack)[12,13] 등의 공격 방법들은 전력 분석 공격의 특정 암호 알고리듬에 최적화된 형태로 볼 수 있다.

앞서 소개한 공격 방법들에 의해 DES, AES, SEED, ARIA, RSA, DSA, ECDSA, ElGamal 등의 대부분의 암호 알고리듬들이 전력 분석 공격의 위험에 노출되어 있다.

2.2.2 전력 분석 공격 실험

전력 분석 공격을 적용하기 위해서는 크게 공격 대상 암호 장치와 소비 전력 측정을 위한 오실로스코프, 측정된 소비 전력 분석을 위한 컴퓨터가 기본적으로 필요하다. 또한 공격 대상 암호 장치의 소비 전력을 측정하기 위해 일반적으로 공격 대상 암호 장치의 전원단이나 접지단에 수십 오옴(Ω)의 저항을 삽입하여 저항에 걸리는 전압 변화를 측정한다. [그림 3]은 전력 분석 공격을 위해 본 연구 센터에서 구성한 실험 환경과 소비 전력 측정을 위해 저항이 삽입된 모습들을 보여주고 있다.

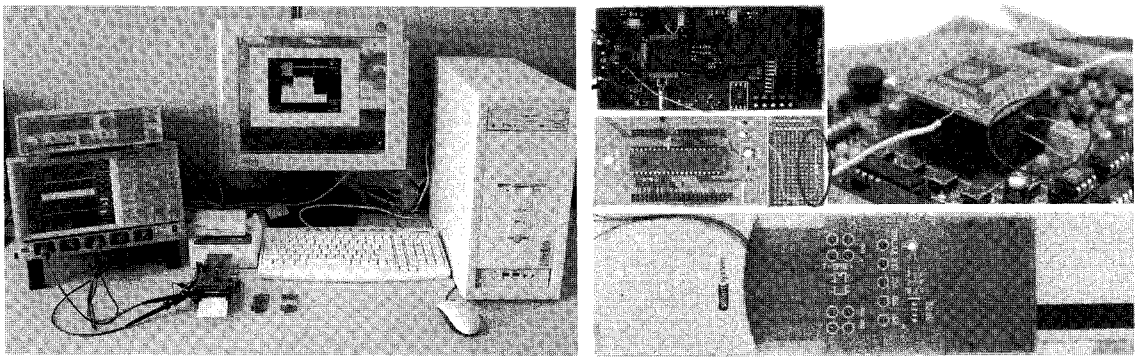
차분 전력 분석 공격 공격자는 추측한 비밀키를 이용하여 추정 소비 전력 모델을 만들고 이를 바탕으로 수집된 소비 전력 파형을 높은 전력을 소비한 그룹과 낮은 전력을 소비한 그룹으로 분류한다. [그림 4]는 국내 표준 알고리듬인 ARIA에 적용된 차분 전력 분석 공격 결과를 보여주고 있다[14,15].



(a) 추측한 키가 맞는 경우, (b) 추측한 키가 틀린 경우

[그림 4] 차분 전력 분석 공격 실험 결과

[그림 4(a)]와 같이 공격자의 추측한 비밀키가 맞다면, 소비 전력 모델이 올바르게 추정되었고, 이를 바탕으로 분류한 실제 소비 전력 파형 그룹들 간에 소비 전력 차이가 나타나게 된다. 반면, [그림 4(b)]와 같이 공격자의 추측한 비밀키가 틀리다면, 소비 전력 모델이 올바르게 추정되지 않았고, 실제 소비 전력 파형 그룹들이 제대로 분류되지 않아 분류된 그룹들 간의 소비 전력 차이가 크게 나지 않는다는 것을 확인할 수 있다.



(a) 전력 분석 공격 실험 환경 (b) 소비 전력 측정을 위한 저항 삽입

[그림 3] 전력 분석 공격 실험 환경

2.3 전자기파 분석 공격

2.3.1 전자기파 분석 공격 종류

공격 대상 암호 장치로부터 방사되는 전자기파(Electromagnetic radiation) 신호에 의해 누출되는 정보에 대한 전자기파 분석 공격(Electromagnetic Analysis Attack, EMA) 결과는 2001년 Quisquater 등의 Gemplus 연구 그룹에 의하여 처음 소개되었다[16]. 전자기파 분석 공격은 전력 분석 공격과 달리 원거리에서 부채널 정보의 습득이 가능하다는 장점과 다중 채널(multiple channels)로 구성되고 있어서 전혀 측정 불가능 하도록 방어대책이 있는 전력 분석 공격 대응 장치에서도 전자기파 정보의 분석이 가능할 수 있다는 장점이 있다.

전자기파 분석 공격도 크게 단순 전자기파 분석 공격(Simple Electromagnetic Analysis Attack, SEMA)과 차분 전자기파 분석 공격(Differential Electro-magnetic Analysis Attack, DEMA)으로 나눌 수 있다.

전자기파 분석 공격은 전력 분석 공격 기법을 거의 그대로 사용할 수 있을 뿐만 아니라, 원거리에서 전자기파 측정이 가능하다는 장점이 있다. Hutter는 [17]에서 지향성 안테나를 사용하여 약 1m 거리에서 측정된 전자기파를 이용하여 전자기파 분석 공격을 성공하였다.

C. Gebotys 등에 의해서는 측정된 전자기파 신호를 이용한 차분 주파수 분석 공격(Differential Frequency Analysis Attack) 방법이 소개 되었다[18]. 차분 주파수 분석 공격은 측정된 전자기파 신호를 주파수 영역으로 변환하여 처리함으로써 측정된 전자기파 신호가 시간 영역에서 가지는 문제점을 해결할 수 있다.

2.3.2 전자기파 분석 공격 실험

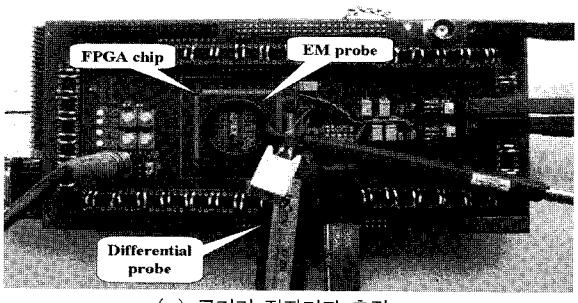
전자기파 분석 공격을 적용하기 위해서는 공격 대상 암호 장치에서 방사되는 전자기파를 측정하기 위한 프로브가 필요하다. [그림 5]는 전자기파 분석 공격을 위한 실험 환경과 여러 형태의 전자기파 측정 프로브를 보여주고 있다. 전자기파 분석 공격은 칩과 근접한 측정도 가능하지만 [그림 5(b)]와 같이 원거리에서도 전자기파 측정이 가능하다. 또한, 외부에서 전자기파 차폐 장치(shielding)를 이용하거나 스펙트럼 분석기, 기타 신호처리 등의 방법을 이용하여 공격 효과를 높일 수 있다.

2.4 오류 분석 공격

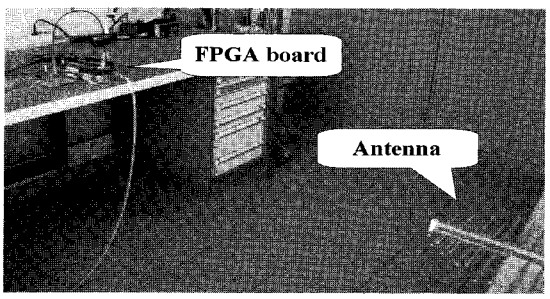
2.4.1 오류 분석 공격의 종류

오류 분석 공격이라 불리는 부채널 공격은 1996년 Bellcore사에 의해 RSA 암호 방식에 대한 공격방법으로 처음 소개되었다[19]. 오류 주입 공격은 암호 연산을 위한 칩이나 하드웨어에 예상치 못한 결함을 유발시켜 발생된 잘못된 출력 값을 분석함으로써 내부의 비밀 정보를 알아내는 공격 방법이다. 일반적으로 오류는 인증기관의 서버와 같은 중량급의 장치로부터 소형 정보보호 하드웨어 장치에서도 발생할 수 있다.

오류 분석 공격에 대한 연구는 DES[20,21], AES[22-26], SEED[27,28], ARIA[29,55], RSA[30-36], ECC[37-42] 등 대부분의 암호 알고리듬에 대해 이루어지고 있으며, 특히 CRT(Chinese Remainder Theorem)에 기반을 둔 RSA 시스템에 대한 연구 결과가 많이 발표 되고 있다[43-54]. 오류 분석 공격의 강력함을 설명하기 위해 오류 분석



(a) 근거리 전자기파 측정



(b) 원거리 전자기파 측정

[그림 5] 전자기파 분석 공격 실험 환경[55]

공격에 매우 취약한 CRT-RSA 알고리듬의 예를 들면 다음과 같다. [그림 6]은 Gauss 재결합 방식을 사용하는 CRT-RSA 알고리듬이다.

입력 : p, q, d, p_I, q_I, N, m
여기서, $p_I = p^{-1} \bmod q$, $q_I = q^{-1} \bmod p$.
출력 : $S = m^d \bmod N$

1. $S_p = m^{d_p} \bmod p$, 여기서, $d_p = d \bmod (p-1)$
2. $S_q = m^{d_q} \bmod q$, 여기서, $d_q = d \bmod (q-1)$
3. $S = (S_p \cdot q \cdot q_I) + (S_q \cdot p \cdot p_I) \bmod N$
4. **Return** S

〔그림 6〕 Gauss 방법을 이용한 CRT 기반 RSA 서명

[그림 6]에서 모듈러스 $N(=p \cdot q)$은 공개키이고, 비밀키 d와 모듈러스 N의 소인수 p, q는 비밀 정보이다. CRT-RSA 알고리듬에 대한 오류 주입 공격 절차는 다음과 같다.

단계 1 : 메시지 m을 입력으로 하여 [그림 2]의 알고리듬을 정상적으로 수행한 결과 서명값 S를 계산한다.

단계 2 : 다시 메시지 m을 이용하여 [그림 2]의 알고리듬을 수행하는 중, $S_p = m^{d_p} \bmod p$ (또는 $S_q = m^{d_q} \bmod q$)가 계산되는 과정에 오류를 주입한다. 오류가 주입된 후 출력되는 오류 서명 값 S'이라 한다.

단계 3 : 위의 두 단계에서 생성된 서명 값의 차를 구한 후 $GCD(S-S', N)$을 계산하여 비밀 값 q (또는 p)를 추출해 낸다. 여기서, $GCD()$는 최대공약수를 구하는 함수이다.

$S_p = m^{d_p} \bmod p$가 계산되는 과정에 오류가 주입된 경우를 예로 들어, 오류 주입 공격이 적용되는 원리를 설명하면 다음과 같다.

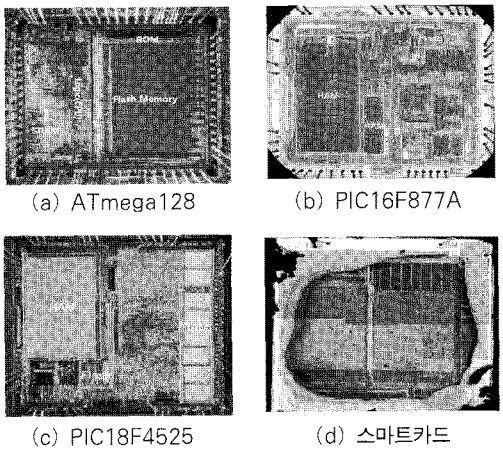
정상 서명 값의 재결합식 :
$S = (S_p \cdot q \cdot q_I) + (S_q \cdot p \cdot p_I) \bmod N$
오류 서명 값의 재결합식 :
$S' = (S_p' \cdot q \cdot q_I) + (S_q \cdot p \cdot p_I) \bmod N$
$\therefore S - S' = (S_p \cdot q \cdot q_I) - (S_p' \cdot q \cdot q_I) \bmod N$
$\therefore GCD(q(S_p \cdot q_I - S_p' \cdot q_I), p \cdot q) = q$

이와 같이 CRT-RSA 알고리듬은 단 한 번의 오류 주입으로도 비밀 소인수인 p, q를 노출할 수 있어 매우 위협적인 공격 방법이다.

2.4.2 오류 분석 공격 실험

오류 분석 공격을 위해서는 공격 대상 칩에 오류 연산을 유도할 수 있는 오류를 주입하여야 한다. 가능한 오류 주입 기술들로는 내부 회로에 직접 주입하는 것이 효과적인 레이저, 전자기파, 이온 빔, X-ray 등과 칩 외부에서도 오류를 유발할 수 있는 전압 글리치, 클럭 글리치, 온도 변화 등 다양한 기술들이 소개되고 있다.

앞서 소개된 오류 주입 방법들 중에서 내부 회로에 직접 주입하는 것이 효과적인 경우에는 공격 대상 칩을 디캡하여 내부 회로가 보이도록 한다. 디캡 방법에는 완전 디캡(Full Decapsulation), 부분 디캡(Hole Decapsulation), 그라인딩 디캡(Grinding Decapsulation) 등이 있다. [그림 7]은 공격 대상 칩의 내부 회로를 관찰하고 레이저 등의 오류를 직접 주입하기 위해 부분 디캡된 칩을 보여주고 있다.



(a) ATmega128 (b) PIC16F877A
(c) PIC18F4525 (d) 스마트카드

〔그림 7〕 부분 디캡된 공격 대상 칩

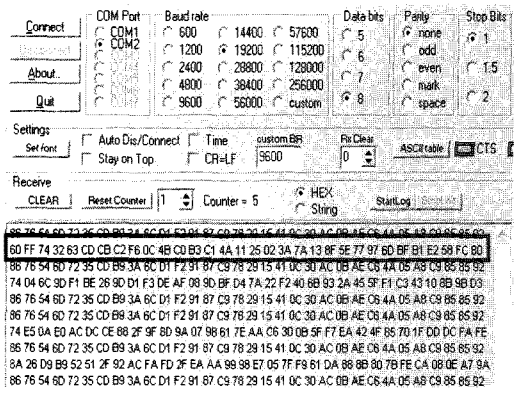
또한 오류 주입 기술들로 주입된 오류의 형태를 간단히 분류하면 다음과 같다.

- 영구적 오류, 일시적 오류
- 비트 크기 오류, 바이트 크기 오류, 임의의 크기 오류
- 특정 값을 유도하는 오류, 임의의 값을 유도하는 오류

예를 들어, CRT-RSA 알고리듬에 적용 가능한 오류 주입 형태는 일시적이고 임의의 크기를 가지면서 임의의 값을 유도하는 오류로 가장 적용하기 쉬운 오류 주입 형태이다. [그림 8]은 본 연구 센터에서 보유한 레이저 오류 주입 환경과 전압 글리치 오류 주입 환경을 보여주고 있다.

본 센터에서는 오류 주입의 가능성을 확인해 보기 위해 256비트의 CRT-RSA 알고리듬을 8비트 범용 마이크로프로세서에 구현하여 사용할 경우 오류 주입 공격 가능 여부를 검증해 보았다. 그리고 서명 결과는 PC와의 시리얼 통신을 통해 출력하도록 하였다. 먼저 전원 전압을 단절하여 칩의 오류 연산을 유도하는 실험을 하였다. 함수 발생기 펄스 출력을 전력 증폭기를 이용하여 증폭하고 반전시켜 전압 단절의 효과를 얻을 수 있었다. CRT-RSA 서명 연산시 원 전압을 일정 시간동안 단절하여 칩의 오류 동작을 유도하는 실험 결과, 전압 단절 시점에 따라 약간의 차이는 있었지만 일정 시간 동안 전원 전압을 단절하면 칩의 오류 동작이 유도되어 오류 결과를 출력하는 것을 확인할 수 있었다.

[그림 9]는 전원 전압 단절로 인한 오류 출력 결과들을 보여주고 있다. 따라서 이러한 오류 서명은 위에서 언급한 바와 같이 정상 서명과의 차를 구하여 비밀 정보를 추출하는데 사용되므로 실제로 CRT-RSA 시스템의 비밀 정보 전체를 공격할 수 있다. 이러한 공격은 전압 단절뿐만 아니라 전압 글리치를 주입하거나 위와 같이 칩을 디캡한후 레이저 장비를 이용하여 오류를 주입해도 같은 결과를 얻을 수 있다.

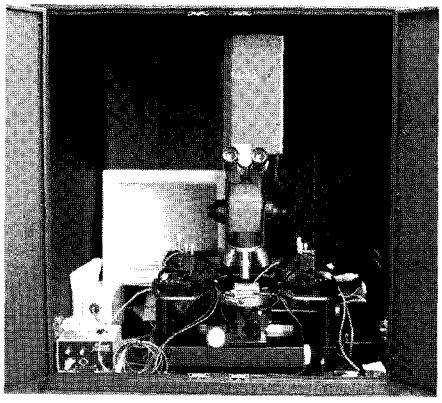


[그림 9] 전압 단절에 의한 오류 서명 출력

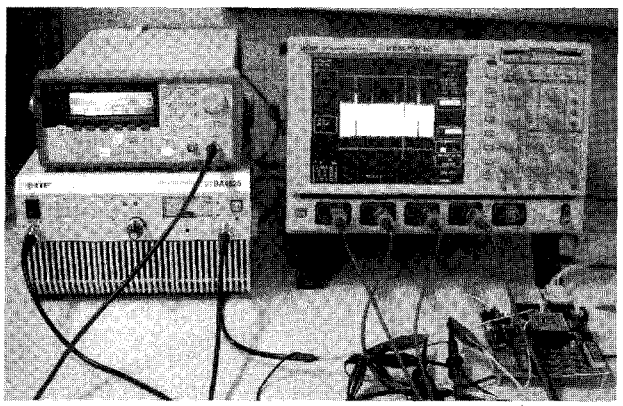
Ⅲ. 부채널 공격 대응 방안

앞서 설명한 바와 같이 대부분의 암호 알고리듬들은 방어대책이 없을 경우 부채널공격으로 쉽게 공격될 수 있다. 따라서 스마트카드와 같은 저 전력 암호 장치의 안전한 사용을 위해서 는 반드시 부채널 공격 대응 방안을 함께 적용하여야 한다.

시차 분석 공격, 전력 분석 공격, 전자기파 분석 공격이 적용되는 근본적인 이유는 암호 장치 내부에서 연산되는 도중에 누출되는 부채널 정보가 암호 장치 내부의 비밀 정보와 상관성을 가지기 때문이다. 이를 방어하는 방법들을 크게 분류하면 크게 두 가지로 나눌 수 있다. 첫 번째는 랜덤 값을 사용하여 암호 알고리듬의 연산 중간 값을 마스킹하거나 이중-레일 회로(dual-rail logic) 등의 별도의 회로를 사용하여 연산중에 누출되는



(a) 레이저 오류 주입 도구



(b) 전압 글리치 오류 주입 도구

[그림 8] 오류 분석 공격 실험 환경

부채널 정보와 연산중에 나타나는 중간 값들의 상관도를 줄이는 방법이다[56-61].

두 번째는 암호 알고리듬에 랜덤 지연시간을 삽입하거나 알고리듬의 수행 순서를 랜덤하게 바꾸는 방법, 랜덤 클럭을 이용하여 부채널 공격의 통계적인 분석 방법이 적용되지 않도록 공격 지점이 시간 축 상에서 어긋나도록 하는 방법이다[62,63].

또한 오류 분석 공격을 방어하기 위해서도 별도의 대응 방안이 필요하다. 오류 분석 공격을 방어하기 위해 오류 주입 여부를 알고리듬 출력 전에 확인하는 방법[45-47,50-53]과 오류가 주입되면 오류가 연산과정 전반으로 확산되어 공격자가 의도하지 않은 임의의 값을 출력하는 방법[33,54], 에러 검출 코드를 이용하는 방법[35]등이 있다.

Ⅳ. 결 론

부채널 공격은 공격 대상 암호 장치에서 암호 알고리듬이 구현되어 연산되는 동안에 누출되는 연산 시간, 소비 전력, 전자기파, 오류 출력 등의 부채널 정보를 이용하기 때문에 암호 알고리듬과 프로토콜 그 자체의 이론적 안전성과는 무관하게 이들의 구현 환경에 따라 쉽게 공격될 수 있다. 따라서 암호 알고리듬을 금융 IC 카드, 전자주민증, 전자여권 등과 같은 암호 장치에 안전하게 구현하기위해서 부채널 공격 방어법이 반드시 고려되어야 한다.

현재까지도 부채널 공격 기법과 방어 방법들은 많은 연구 그룹들에 의해서 연구되고 있는 중이며, 본 연구센터에서도 국내외 부채널 공격 관련 연구를 선도하기 위해 이론적인 연구 활동뿐만 아니라 전력 분석 공격, 전자기파 분석 공격, 오류 분석 공격을 위한 실험 환경을 구성하여 실제 상용 암호 장치들의 부채널 공격에 대한 안전도를 분석하고 있다.

참고문헌

[1] P. Kocher, "Timing attacks on implementations of Diffie-Hellmann," *Crypto'96, LNCS 1109*, pp. 104-113, 1996.

[2] J. Dhem, F. Koeune, P. Leroux, P. Mestre, J. Quisquater, and J. Williems, "A practical implementation of the timing attack," *CARDIS'00, LNCS 1820*, pp. 167-182, 2000.

[3] 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.

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

[5] E. Brier, C. Clavier, and F. Olivier, "Correlation Power Analysis with a Leakage Model," *CHES'04, LNCS 3156,* pp. 16-29, 2004.

[6] T. Le, J. Clédière, C. Canovas, B. Robisson, C. Servière, and J. Lacoume, "A proposition for correlation power analysis enhancement," *CHES'06, LNCS 4249*, pp. 174-186, 2006.

[7] C. Rechberger, E. Oswald, "Practical Template Attacks," *WISA'04, LNCS 3325,* pp. 443-457, 2004.

[8] W. Schindler, K. Lemke, and C. Paar, "A Stochastic Model for Differential Side Channel Cryptanalysis," *CHES'05, LNCS 3659,* pp. 30-46, 2005.

[9] E. Oswald, S. Mangard, C. Herbst, and S. Tillich, "Practical Second-Order DPA Attacks for Masked Smart Card Implementations of Block Ciphers," *CT-RSA'06, LNCS 3860*, pp. 192-207, 2006.

[10] L. Goubin, "A Refined Power-Analysis Attack on Elliptic curve cryptosystems," *PKC'03, LNCS 2567*, pp. 199-211, 2003.

[11] T. Akishita and T. Takagi, "Zero-Value Point Attacks on Elliptic cryptosystem," *ISC'03, LNCS 2851,* pp. 218-233, 2003.

[12] P. Alain and F. Valette, "The Doubling Attack Why Upwards is better than Downwards," *CHES'03, LNCS 2779*, pp. 269-280, 2003.

[13] S. Yen, W. Lien, S. Moon, and J. Ha, "Power Analysis by Exploiting Chosen Message and Internal Collisions Vulnerability of Checking Mechanism for RSA-Decryption," *Mycrypt'05, LNCS 3715,* pp. 183-195, 2005.

[14] 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.

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

[16] J. Quisquater, D. Samyde, "Electromagnetic analysis (ema): Measures and counter-measures for smart cards," *E-smart 2001, LNCS 2140,* pp. 200-210, 2001.

[17] M. Hutter, "EM Side-Channel Attacks on Cryptographic Devices," Master thesis, Graz University of Technology, 2006.

[18] C. Gebotys, S. Ho, C. Tiu, "EM Analysis of Rijndael and ECC on a Wireless Java-Based PDA," *CHES'05, LNCS 3659,* pp. 250-264, 2005.

[19] Bellcore Press Release, *"New threat model breaks crypto codes,"* Sept. 1996.

[20] C. Moratelli, E. Cota, and M. Lubaszawski, "A Cryptography Core Tolerant to DFA Fault Attacks," *Proceedings of the 19th annual symposium on Integrated circuits and systems design-SBCCI'06, ACM,* pp. 190-195, 2006.

[21] E. Biham and A. Shamir, "Differential Fault Analysis of Secret Key Cryptosystems," *CRYPTO '97, LNCS 1294,* pp. 513-525, 1997.

[22] P. Dusart, G. Letourneux, and O. Vivolo, *"Differential Fault Analysis on A.E.S.,"* Technical Report, 2003.

[23] J. Takahashi, T. Fukunaga, and K. Yamakoshi, "DFA mechanism on the AES key schedule", *FDTC'07, IEEE Computer Society,* pp. 62-72, 2007.

[24] D. Peacham, B.Thomas, "A DFA atttack against the AES key schedule", *SiVenture White Paper 001,* available at http://www.siventure.com/pdfs/AES _keyschedule_DFA_whitepaper.pdf.

[25] C. Giraud, "DFA on AES", *Speringer-Verlag,* In Advanced Encryption Standard(AES): *AES'04, LNCS 3373,* pp. 27-41, 2005.

[26] B. Robisson, P.Manet, "Differential Behavioral Analysis", *CHES'07, LNCS 4727,* pp. 413-426, 2007.

[27] 하재철, 김창균, 문상재, 박일환, "SEED에 대한 오류 분석 공격," *한국정보보호학회, 한국정보보호학회 학술대회논문집,* pp. 39-44, 2003.

[28] H. Yoo, C. Kim, J. Ha, S. Moon, and I. Park, "Side Channel Cryptanalysis on SEED," *WISA'04, LNCS 3325,* pp. 411-424, 2005.

[29] W. Li, D. Gu, and J. Li, "Differential fault analysis on the ARIA algorithm", *Information Sciences, Elsevier,* Vol. 178, pp. 3727-3737, 2008.

[30] D. Boneh, R. DeMillo, and R. Lipton, "On the importance of checking cryptographic protocols for faults," *EUROCRYPT'97, LNCS 1233,* PP. 37-51, 1997.

[31] F. Bao, R. Deng, Y. Han, A. Jeng, A. Narasimbalu, and T. Ngair, "Breaking public key cryptosystems on tamper resistant devices in the presence of transient faults," *In Pre-proceedings of the 1997 Security Protocols Workshop, LNCS 1361,* pp. 115-124, 1998.

[32] S. Yen, M. Joye, "Checking before output may not be enough against faults-based cryptanalysis," *IEEE Computer Society, IEEE Trans. on Computers,* Vol. 49, No. 9, pp. 967-970, 2000.

[33] S. Yen, "A countermeasure against one physical cryptanalysis May Benefit Another Attack," *ICISC'01, LNCS 2288,* pp. 414-427, 2001.

[34] C. Girraud, E. Kundsen, "Fault Attacks on Signature Schemes,." *ACISP 2004, LNCS 3108,* pp. 478-491, 2004.

[35] R. Karri, K. Wu, P. Mishra, and Y. Kim, "Concurrent error detection of fault-based side-channel cryptanalysis of 128-bit symmetric block ciphers," *ACM, Proceedings, IEEE Design Automation Conference (DAC),* pp. 579-584, 2001.

[36] J. Schmidt, C. Herbst, "A Practical Fault attack on Square and Multiply", *FDTC'08, IEEE Computer Society,* pp. 53-58, 2008.

[37] P. Fouque, R. Lercier, "Fault Attack on Elliptic Curve with Montgomery Ladder Implementation", *FDTC'08, IEEE Computer Society,* pp. 92-98, 2008.

[38] I. Biehl, B. Meyer, and V. Müller. "Differential fault attacks on elliptic curve cryptosystems". *CRYPTO'00, LNCS 1880,* pp. 131-146, 2000.

[39] M. Ciet, M. Joye, "Elliptic curve cryptosystems in the presence of permanent and transient faults," *Cryptology ePrint Archive*, 2003. http://eprint.iacr.org/2003/028.

[40] J. Blömer, M. Otto, and J. Seifert, "Sign change fault attacks on elliptic curve cryptosystems," *Cryptology ePrint Archive,* 2004. http://eprint.iacr.org/2004/227.

[41] D. Page, F. Vercauteren, "A Fault Attack on Pairing Based Cryptography," *IEEE Computer Society, IEEE Transaction on Computers,* Vol. 55, No. 9, pp. 1075-1080, 2006.

[42] I. Duursma, H. Lee, "Tate Pairing Implementation for Hyperelliptic Curves $y^2 = x^p - x + d$," *ASIACRYPT, LNCS 2894,* pp. 111-123, 2003.

[43] A. Lenstra, "*Memo on RSA signature generation in the presence of faults,*" September 1996.

[44] M. Joye, J. Quisquater, F. Bao, and R. Deng, "RSA-type signatures in the presence of transient faults," In *Cryptography and Coding, LNCS 1355, Springer-Verlag*, pp. 109-121, 1997.

[45] A. Berzati, C. Canovas, and L. Goubin, "(In)security Against Fault Injection Attacks for CRT-RSA implementations," *FDTC'08, IEEE Computer Society,* pp. 101-107, 2008.

[46] S. Yen, S. Moon, and J. Ha, "Hardware Fault Attack on RSA with CRT Revisited," *ICISC 2002, LNCS 2587,* pp. 374-388, 2003.

[47] J. Blömer, M. Otto, and J. Seifert, "A new CRT-RSA algorithm secure against Bellcore attacks," *10th ACM conference on Computer and Communication Security, ACM,* pp. 311-320, 2003.

[48] C. Aumüller, P. Bier, W. Fischer, P. Hofreiter, and J. Seifert, "Fault Attacks on RSA with CRT: Concrete Results and Practical Countermeasures," *CHES 2002, LNCS 2523,* pp. 206-275, 2003.

[49] D. Wagner, "Cryptanalysis of a provably secure CRT-RSA algorithm," *11th ACM Conference on Computers and Communications Security, ACM,* pp. 92-97, 2004.

[50] J. Blömer, M. Otto, "Wagner's attack on a secure CRT-RSA algorithm reconsidered," *FDTC'06, LNCS 4236*, pp. 13-23, 2006.

[51] M. Ciet, M. Joye, "Practical fault countermeasures for Chinese Remaindering based RSA," *FDTC'05, IEEE Computer Society*, pp. 124-131, 2005.

[52] C. Giraud, "Fault resistant RSA implementation," *FDTC'05, IEEE Computer Society,* pp. 142-151, 2005.

[53] A. Boscher, R. Naciri, and E. Prouff, "CRT-RSA Algorithm Protected Against Fault Attacks," *WISTP'07, LNCS 4462*, pp. 237-252, 2007.

[54] C. Kim, J. Ha, S. Moon, S. Yen, and S. Kim, "A CRT-Based RSA Countermeasure Against Physical Cryptanalysis," *HPCC'05, LNCS 3726,* pp. 549-554, 2005.

[55] 김창균, 유형소, 박일환, "FPGA 기반 ARIA에 대한 차분부채널분석 공격," *한국정보보호학회, 한국정보보호학회논문지,* Vol. 17, No. 5, pp. 55-63, 2007.

[56] M. Akkar, C. Giraud, "An Implementation of DES and AES, Secure against Some Attacks", *CHES'01, LNCS 2162*, pp. 309-318, 2001.

[57] M. Akkar, L. Goubin, "A Generic Protection against High-Order Differential Power Analysis", *FSE'03, LNCS 2887,* pp. 192-205, 2003.

[58] J. Blömer, J. Guajardo, and V. Krummel, "Provably Secure Masking of AES", *SAC'04, LNCS 3357,* pp. 69-83, 2005.

[59] E. Oswald, S. Mangard, N. Pramstaller, and V. Rijmen, "A Side-Channel Analysis Resistant Description of the AES S-box", *FSE'05, LNCS 3557,* pp. 413-423, 2005.

[60] M. Bucci1, L. Giancane, R. Luzzi, and A. Trifiletti, "Three-Phase Dual-Rail Pre-charge Logic", *CHES'06, LNCS 4249,* pp. 232-241, 2006.

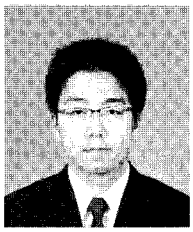
[61] Z. Chen, Y. Zhou, "Dual-Rail Random Switching Logic : A Countermeasure to Reduce Side Channel

Leakage", *CHES'06, LNCS 4249,* pp. 242-254, 2006.

[62] C. Herbst, E. Oswald, and S. MangardAn, "AES Smart Card Implementation Resistant to Power Analysis Attacks", *ACNS'06, LNCS 3989,* pp. 239-252, 2006.

[63] O. Kömmerling, M. G. Kuhn, "Design Principles for Tamper-Resistant Smartcard Processors", *The Proceedings of the USENIX Workshop on Smartcard Technology-Smartcard'99, USENIX Association,* pp. 9-20, 1999.

〈著者紹介〉



박 제 훈 (JeaHoon Park)
정회원

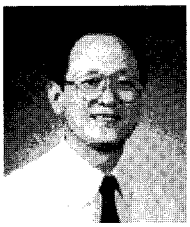
2004년 2월: 경북대학교 전자·전기공학부 졸업
2006년 2월: 경북대학교 전자공학과 석사
2006년 3월~현재: 경북대학교 전자전기컴퓨터학부 박사과정
<관심분야> 정보보호, 네트워크 보안, 스마트카드

이 훈 재 (HoonJae Lee)
종신회원

1985년 2월: 경북대학교 전자공학과 (공학사)
1987년 2월: 경북대학교 전자공학과 (공학석사)
1998년 2월: 경북대학교 전자공학과 (공학박사)
1987년 2월~1998년 1월: 국방과학연구소 선임연구원 (개발팀장)
1998년 3월~2002년 2월: 경운대학교 컴퓨터공학과 조교수
2002년 3월~현재: 동서대학교 컴퓨터정보공학부 부교수
2007년 6월~현재: 동서대학교 유비쿼터스 IT전문인력양성사업단장 (NURI), BK21 사업팀장
<관심분야> 암호이론, 정보통신/네트워크, u-네트보안

하 재 철 (JaeCheol Ha)
종신회원

1989년 2월: 경북대학교 전자공학과 졸업
1993년 8월: 경북대학교 전자공학과 석사
1998년 2월: 경북대학교 전자공학과 박사
1998년 3월~2006년 1월: 나사렛대학교 전자계산소장, 학술정보관장, 입시학생처장
1998년 3월~2007년 2월: 나사렛대학교 정보통신학과 부교수
2006년 7월~2006년 12월: QUT in Australia 연구교수
2007년 3월~현재: 호서대학교 정보보호학과 부교수
2002년 3월~현재: 한국정보보호학회 이사, 논문지 편집위원
<관심분야> 정보보호, 네트워크 보안, 스마트카드



문 상 재 (SangJae Moon)
종신회원

1972년 2월: 서울대학교 공업교육(전자전공)과 학사
1974년 2월: 서울대학교 전자공학과 석사
1984년 6월: 미국 UCLA 전기공학과 박사
1984년 7월~1985년 6월: UCLA Postdoctor 근무
1997년 9월~1998년 8월: 경북대학교 전자전기공학부 학부장
2001년 1월~2001년 12월: 한국정보보호학회 회장
1974년 12월~현재: 경북대학교 전자전기컴퓨터공학부 교수
2000년 8월~2008년 12월: 경북대학교 이동네트워크 정보보호기술연구센터장
2002년 2월~현재: 한국정보보호학회 명예회장
<관심분야> 정보보호, 디지털 통신, 이동 네트워크