情報保護學會論文誌
第16卷 第4號, 2006. 8

사이드 채널 공격에 대한 스마트카드 안전성의 실험적 분석*

한 동 호,[1†] 박 제 훈,[1] 하 재 철,[2] 이 성 재,[3] 문 상 재[1‡]
[1]경북대학교, [2]나사렛대학교, [3]한국정보보호진흥원

Development of Side Channel Attack Analysis Tool on Smart Card*

DongHo Han,[1†] JeaHoon Park,[1] JaeCheol Ha,[2] SungJae Lee,[3] SangJae Moon[1‡]
[1]Kyungpook National University, [2]Korea Nazarene University,
[3]Korea Information Security Agency

요 약

스마트카드에 내재된 암호 알고리즘이 이론적으로 안전하더라도 실제 구현 환경에 따라 사이드 채널 공격에 취약하다는 사실이 근래에 알려졌다. 본 논문에서는 스마트카드에 구현된 암호 알고리즘의 안전성을 분석할 수 있는 툴을 직접 개발하여 현재 상용 중인 칩을 탑재한 스마트카드에 사이드 채널 공격 중 가장 강력한 공격 방법으로 알려진 전력분석공격과 오류주입공격을 적용하여 안전성 분석을 하였다. 전력분석공격은 대칭키 암호 시스템에 적용하기 쉬운 차분전력분석 공격을 SEED와 ARIA에 대해서 적용하였고, 오류주입공격은 스마트카드의 동작 클럭과 전원을 차단하는 방법으로 CRT기반의 RSA에 적용하였다. 공격 결과 대상 대응책이 없는 경우의 전력분석공격은 가능하지만 오류주입공격은 칩 내부에 사전 방어대책이 마련되어 있어 사이드 채널 공격에 안전했다.

ABSTRACT

Although the cryptographic algorithms in IC chip such as smart card are secure against mathematical analysis attack, they are susceptible to side channel attacks in real implementation. In this paper, we analyze the security of smart card using a developed experimental tool which can perform power analysis attacks and fault insertion attacks. As a result, raw smart card implemented SEED and ARIA without any countermeasure is vulnerable against differential power analysis(DPA) attack. However, in fault attack about voltage and clock on RSA with CRT, the card is secure due to its physical countermeasures.

Keywords : *Fault Insertion Attacks, Differential Power Analysis(DPA), Side Channel Attack*

Ⅰ. 서 론

현재까지 많은 암호 시스템들이 수학적 안전도에 기반하여 개발되었다. 비록 설계된 암호 시스템이 수학적으로 안전하더라고, 각각의 구현 환경에 따라 물리적인 공격들에 취약함이 밝혀졌다. 특히, IC칩에 탑재된 암호 알고리즘에 대한 사이드 채널 공격[1,2]이 그 예이며, 그 중 전력분석공격과 오류주입공격이 대표적인 공격법으로 많은 학자들에 의해서 공격법과

접수일: 2006년 4월 18일 ; 채택일: 2006년 7월 26일
* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 지원사업과 한국정보보호진흥원에서 지원하는 위탁과제의 연구결과로 수행되었음.
† 주저자, dh1007@ee.knu.ac.kr
‡ 교신저자, sjmoon@ee.knu.ac.kr

대응책들이 연구되었다. 특히, 대칭키 암호 중에서는 국제 표준인 AES에 대한 공격과 이를 방어할 수 있는 안전한 설계 방법이 많이 연구되었다[3-5]. 또한 국내 표준 암호인 SEED와 ARIA에 대한 전력분석 공격이 가능함을 보였고[7,9], SEED의 경우에는 오류주입공격도 이론적으로 가능함을 증명한 바 있다[7]. 그러나 국내 표준 알고리듬에 대해서는 공격에 비해 대응책으로 구체화되어 제시된 것은 많지 않다. 단지 AES에서 제시된 일반적인 방법은 ARIA에, DES 방어책으로 제시된 마스킹 기법들은 SEED에 응용하여 사용할 수 있다. 특히, 전력분석공격이 오류주입공격보다 공격이 용이하여 많이 연구되고 있으며 오류주입공격은 블록 암호보다는 CRT를 이용한 RSA 등과 같은 공개키 암호 알고리듬[11]에서 그 공격의 현실성을 높이는 방법[13-15]으로 연구가 진행되고 있다. 물론 현재까지 국내에서 실제 스마트카드에 대한 오류주입공격 실험은 대칭키 암호 알고리듬이든 공개 키 암호 알고리듬이든 시도된 적은 없다.

따라서 본 논문에서는 개별 구현 모듈에 대한 사이드 채널 공격에 대한 안전성을 신속하고, 정확하게 판단할 수 있는 현실적인 대안으로, 전력분석공격뿐 만 아니라, 칩의 동작 클럭 및 전원을 차단하여 생성한 오류 신호로 실제 오류주입공격을 수행할 수 있는 하이브리드 형태의 사이드 채널 공격 분석 도구를 개발하였다. 그리고 이 도구를 이용하여 사이드 채널 공격을 현재 상용 중인 칩(실험에는 특정회사의 칩을 사용하였으나 칩은 제조사마다 다른 물리적 특성과 개발 환경을 가지므로 특정 제조사명은 기술하지 않았음)을 탑재한 스마트카드에 적용하여 안전성 분석을 하였다. 본 논문의 구성은 다음과 같다. Ⅱ장에서는 사이드 채널 공격 실험에 사용된 암호 알고리즘에 따른 사이드 채널 공격 방법에 대해서 살펴본다. 그리고 AES나 RSA 그리고 최근의 ARIA에 적용되었던 방어 대책에 대해 간략하게 살펴본다. Ⅲ장에서는 개발된 사이드 채널 공격 분석 도구를 소개하겠다. Ⅳ장에서는 상용 중인 칩을 탑재한 스마트카드의 안전성 분석을 하고, 마지막으로 Ⅴ장에서 결론을 논하겠다.

Ⅱ. 암호 알고리즘에 따른 사이드 채널 공격 방법 및 대응방법

본 장에서는 사이드 채널 공격 실험에 사용된 SEED와 ARIA에 대한 차분전력분석 공격과 CRT 기반 RSA 암호 알고리즘에 대한 오류주입공격 방법에 대해서 설명하겠다. 그리고 현재까지 대칭키 암호 알고리듬 등에 적용된 차분전력분석공격의 대응 방법과 오류주입공격에 대한 대응 방법을 간략히 살펴본다.

2.1 SEED와 ARIA에 대한 차분전력분석공격

2.1.1 SEED에 대한 차분전력분석공격 방법[7]

SEED[6]에 대한 차분전력분석공격은 해밍웨이트 모델을 기본 가정으로 하고 있으며, 각 라운드의 결과 값이 저장되는 시점을 알고 있다고 가정한다. SEED는 그림 1의 R_1계산과정에서 공격자가 F 함수의 입력과 출력을 알고 있으면 라운드 키를 구할 수 있으므로 차분전력분석공격에 취약하다. 공격 수행 방법은 다음과 같은 단계를 거친다. 다음에서 사용되는 F함수의 출력을 F_1이라고 하겠다.

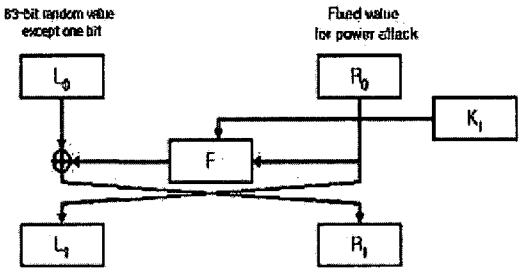


그림 1. 1라운드 SEED에 대한 차분전력분석공격

□ 1단계 : F함수의 출력 64비트를 $F_1(f_0,f_1,f_2,...,f_{63})$ 이라 정의하고 F_1의 t번째 비트를 공격한다고 가정한다.

□ 2단계 : 임의의 128비트 평문 $M_i(m_0,m_1,m_2,...,m_{127})$을 선택한다. 이 때, L_0에 들어갈 $(m_0,m_1,m_2,...,m_{63})$ 중에서 t번째 비트를 제외하고는 랜덤한 값으로 정하고 R_0에 들어갈$(m_{64},m_{65},m_{66},...,m_{127})$는 임의의 어떤 값으로 고정시킨다.

□ 3단계 : L_0에서 t번째 비트 값 "0" 과 "1" 에 따라 R_1에 저장되는 시점(t^*)의 소비 전력 신호를 분류한다. 이 때, $T_i[t]$는 샘플링 시간 t의 소비 전력신호를 나타낸다.

$$T_0 = \{T_i[t] | L_0\text{의 } t\text{번째 비트의 값} = \text{"0"}\}$$
$$T_1 = \{T_i[t] | L_0\text{의 } t\text{번째 비트의 값} = \text{"1"}\}$$

□ 4단계 : 양분한 소비 전력 신호 데이터를 각각 평균하여 차분 신호를 구한다.

$$\triangle D_t = \frac{1}{|T_0|}\sum_{T_i[t]\in T_0} T_i[t] - \frac{1}{|T_1|}\sum_{T_i[t]\in T_1} T_i[t]$$

□ 5단계 : L_0에 대한 소비 전력 신호가 충분히 많을 시 다음과 같은 차분신호를 얻을 수 있다.

$$\lim_{N\to\infty}\triangle_{D_t} = \begin{cases} 0 & \text{if } t \neq t^* \\ \epsilon & \text{if } t = t^* \end{cases}$$

R_1이 저장되는 시점이 t^*이고, t와 t^*이 같다고 가정한다. 만약 차분신호에서 ε보다 큰 피크가 형성된다면 F_1의 t번째 값은 1이다. 이는 비트 "1"에 대한 소비 전력이 "0"에 대한 소비 전력보다 크기 때문이다. 만약 차분신호에서 $\epsilon < 0$ 인 피크가 형성된다면 F_1의 t번째 값은 0이다. 여기서 기본 가정인 t와 t^*이 다르면, 메시지와 소비전력신호는 무관하므로 피크가 발생하지 않는다.

위 과정을 계속 반복하여 64비트 F_1을 알아낼 수 있으며, 결국 이를 이용해서 라운드 키 K_1을 찾을 수 있다.

2.1.2 ARIA에 대한 차분전력분석공격 방법[9]

ARIA [8] 에 대한 차분전력분석공격은 SEED와 마찬가지로 해밍웨이트 모델을 기본 가정으로 하고, 공격자는 각 라운드의 결과 값이 저장되는 시점을 알고 있다고 가정한다. ARIA는 각 라운드마다 메시지와 라운드 키를 XOR 연산 후 수행되는 S-Box 연산 부분이 차분전력분석공격에 취약하다. 먼저 공격자는 분류함수 $D(P, b, rk_8)$을 정의한다. P와 rk_8은 각각 S-Box의 입력인 8비트 평문과 라운드 키이며, b는 S-Box의 출력 중 공격하고자 하는 1비트 값이다. 공격자는 N개의 평문 P_i와 각 라운드에 대한 소비 전력 신호 T_{it}을 구하고 그 값을 다음과 같이 나타낸다.

$P_1, \ldots, P_N$, $T_{1t}, \ldots, T_{Nl}$ (t : 샘플링 시간)

공격 수행 방법은 다음과 같은 단계를 거친다.

□ 1단계 : S-box의 출력 값을 다음과 같이 분류한다.

$$T_0 = \{T_{it} | D(P, b, rk_8) = 0\}$$

$$T_1 = \{T_{it} | D(P, b, rk_8) = 1\}$$

□ 2단계 : 양분한 소비 전력 신호 데이터를 각각 평균하여 차분 신호를 구한다.

$$\triangle D[t] = \frac{1}{|T_0|}\sum_{T_{it}\in T_0} T_{it} - \frac{1}{|T_1|}\sum_{T_{it}\in T_1} T_{it}$$

만약 rk_8가 잘못된 키이면 S-Box의 연산 후 계산된 분류함수 $D(P,b,rk_8)$의 값이 난수발생기 (random generator)와 같은 동작을 하게 된다. 이는 b비트의 값과 실제 비밀 키가 어떤 상관관계도 갖고 있지 않기 때문이다. 따라서 $\triangle D[t]$는 N의 수가 커질수록 0으로 접근할 것이다. 반면에 rk_8가 올바른 키라면, 분류함수를 통해서 계산된 값이 b와 일치하게 된다. 따라서 분류함수는 S-Box후 레지스터에서 처리된 값과 상관이 있으며, 그 결과 power trace의 차분파형은 어떤 값 ϵ보다 큰 피크가 형성된다. 위 과정을 반복하여 1라운드의 나머지 키를 모두 구할 수 있으며, 결국 모든 라운드 키를 구할 수 있다.

2.2 차분전력분석공격에 대한 대응 방법[7,10,3]

차분전력분석공격에 대한 대응 방법들에는 여러 가지 방법들이 있는데, 여기서는 그 중 몇 가지 방법들에 대해서 알아보겠다.

Dual Rail/Logic은 암호 알고리즘이 수행되는 동안에 유출되는 소비 전력을 일정하게 해주는 active component로 이로 회로를 구현하면, 전력분석공격에 대한 방어를 할 수 있다. 또한, 암호 알고리즘이 시작할 때, 랜덤 지연시간을 삽입하여 전력 파형에 변화를 주어 방어하는 방법, 회로에 잡음 생성기를 통해 생성한 잡음을 추가하여, 비밀정보를 가진 신호와 잡음 신호의 구분을 모호하게 함으로써 방어하는 방법과 암호 알고리즘의 수행 중 생성되는 중간 값과 전력 소모량간의 의존성을 제거하기 위해서 각 연산의 입출력에 가변 마스크를 사용하여 방어하는 마스킹 기법이 있다.

추가적으로 랜덤화 기법이 있는데, ARIA는 Add RoundKey와 S-Box의 연산 순서를 바꿔도 동일한 결과 값이 나온다. 이와 같은 특징을 이용하여 공격자가 전력 파형을 통해서 연산 시점을 예측하지 못하게 함으로써, 전력분석공격에 방어를 할 수 있다.

2.3 CRT 기반 RSA 암호 알고리즘에 대한 오류주입공격 및 대응방법

2.3.1 오류 주입 방법[17-19]

오류를 주입하는 방법은 여러 가지가 있는데, 여기서는 전압, 클럭, 빛을 이용한 방법 등에 대해서 알아보겠다.

첫 번째 전원전압에 오류를 발생하는 방법으로 IC 카드의 전원전압은 ISO 표준에서 4.5V와 5.5V사이로 규정하고 있다. 따라서 전압을 강제적으로 차단하거나, spike에 의해 범위를 벗어나게 하여 잘못된 연산을 유도하는 방법이다. 두 번째 클럭에 오류를 발생하는 방법으로 카드의 동작 클럭을 강제적으로 차단하거나, 동작 범위를 벗어난 클럭을 사용하여 데이터 처리 시 CPU가 명령어를 생략하거나 하는 오류를 유도하는 방법이다. 세 번째 반도체 칩에 강한 빛을 입사하여 SRAM의 특정 비트에 오류를 주입하는 공격 방법이다. 그 외에는 높은 온도나 자장에 의해 유도된 와상 전류 등을 이용하여 메모리 값을 변경시키는 방법들이 있다.

2.3.2 공격 방법

중국인 나머지 정리 (Chinese Remainder Theorem : CRT)는 RSA 암호시스템에 대하여 서명 생성 시에 속도의 향상을 위해 많은 표준들에 의해 권장되고 있다[11]. 하지만 CRT-RSA를 암호시스템에 사용할 경우 연산에서 오류가 발생했을 때, 가장 강력한 오류 공격으로 알려진 CRT 기반 오류 공격이 가능하다[12].

먼저 공격의 대상인 CRT를 이용한 RSA 암호시스템을 간략히 설명하면 그림 2와 같다. 이러한 CRT 기반의 RSA 서명 생성 과정에서 S_p, S_q 둘 중 하나만 오류가 발생하여 잘못된 값이 될 경우, 그림 3처럼 공격자가 N을 소인수 분해하는 공격이 가능해진다.

2.3.3 대응 방법[13-15]

오류 주입 공격에 대한 대응 방법들에는 여러 가지 방법들이 있는데, 여기서는 그 중 몇 가지 방법들에 대해서 알아보겠다.

첫 번째 Shamir의 대응 방법은 $S_p \equiv m^d \bmod p$에 대해 $S_{p1} \equiv m^d \bmod pr$와 $S_{q1} \equiv m^d \bmod qr$ (여기서 r은 적당한 정수이고, 보안 파라메터)를 계산해 놓고, $S_{p1} \equiv S_{q1} \bmod r$이면 오류가 없는 것이고, $S_{p1} \neq S_{q1} \bmod r$이면 오류가 발생하였으므로 새로운 서명을 생성하도록 하는 방법이다.

두 번째 단계적인 결과 값 검사법를 사용한 방법은 오류가 주입되는 것을 방어하기 위해 작은 소수를 발생하고, 이를 이용하여 단계적으로 중간 결과 값을 유도하고 이를 검사함하는 방법이다. 즉, 오류가 발생하면 중간에 동작을 멈추게 함으로써 최종 결과에는 오류가 주입되지 않도록 하여 공격을 방어하는 방법이다.

세 번째 오류 확산을 이용한 방법은 오류가 주입되면 서명 계산 과정에서 에러가 넓게 확산되게 함으로써 공격자가 비밀키를 공격할 수 있는 계산식을 유도하지 못하도록 하는 방법이다.

단계 1 : 서명자가 서명하려는 메시지 $M \in Z_N$을 선택. 여기서 N은 소수 p와 q를 곱한 수이다.

단계 2 : 서명자는 p와 q를 이용하여 서명 생성

① $S_p = M^{d_p} \bmod p$, where $d_p = d \bmod (p-1)$

② $S_q = M^{d_q} \bmod q$, where $d_q = d \bmod (q-1)$

③ 서명 S 는

$S = u_p S_p + u_q S_q \bmod N$

, where $u_p = \begin{cases} 1 \bmod p \\ 0 \bmod q \end{cases}$ and $u_q = \begin{cases} 0 \bmod p \\ 1 \bmod q \end{cases}$

그림 2. CRT 기반의 RSA 서명 생성 과정

단계 1 : $S_q = M^{d_q} \bmod q$의 계산 과정 중 오류를 발생하여 $S_q N \neq S_q' \bmod q$가 되게 함.

단계 2 : 올바른 서명 값은 $S = u_p S_p + u_q S_q \bmod N$ 오류 서명은 $S' = u_p S_p + u_q S_q' \bmod N$

단계 3 : 공격자는 $gcd(N, M - S'^e) = p$를 구함.

공격 근거 : $M - S'^e$값의 특성

$M - S'^e \bmod p = M - S_p^e \bmod p = 0 \bmod p$ and $M - S'^e \bmod q = M - S_q'^e \bmod q \neq 0 \bmod q$

$M - S'^e$는 p 의 배수이지만 q 의 배수는 아님.

그림 3. CRT 기반의 RSA에 대한 오류 공격

Ⅲ. 사이드 채널 공격 분석 도구 개발

본 장에서는 개별 모듈에 대한 사이드 채널 공격 여부를 판단할 수 있는 사이드 채널 공격 분석 도구에 대해서 소개하겠다. 이 도구는 기존의 연구를 통해서 강력한 사이드 채널 공격으로 알려진 전력분석 공격과 오류주입공격을 수행할 수 있다.

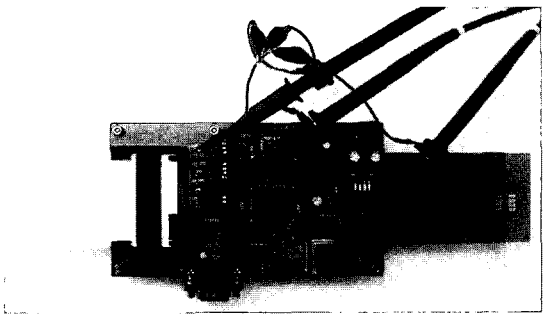


그림 4. 사이드 채널 공격 분석 도구

전력분석공격을 위해서 스마트카드 접지와 카드리더기 접지 사이에 저항을 연결하여 암호 알고리즘 연산 시 누출되는 전력을 측정할 수 있게 설계되어 있다. 입력 클럭은 기본적으로 카드리더기를 통한 내부 클럭과 암호 알고리즘의 연산시간을 조절하기 위해서 외부 단자를 통해 받는 외부 클럭을 사용할 수 있다. 이는 내부 클럭보다 느린 외부 클럭을 입력함으로써, 알고리즘의 연산 시간을 길게 만들어 오류주입 시점을 정밀하게 조절하기 위함이다. 뿐만 아니라, 표 1에 나타낸 것처럼 딥 스위치를 이용해 카드의 공급 전원 및 동작 클럭 차단과 같은 다양한 방법으로 오류 신호를 생성하여 오류주입공격을 수행할 수 있도록 설계했다. 오류 신호 생성 원리는 분석자가 PC의 COM포트(RS232)를 통해서 마이크로프로세서를 제어한다. 마이크로프로세서는 PLD(Prog-rammable Logic Device)를 제어하여 원하는 공격 시점에 임의의 시간동안 스마트카드에 입력되는 전원(Vcc)과 주 클럭(CLK)를 차단하여 전원 오류 신호와 클럭 오류 신호를 생성한다.

그림 5는 오실로스코프를 통해서 사이드 채널 공격 분석 도구에 의해 생성된 오류 신호를 캡쳐한 것이다.

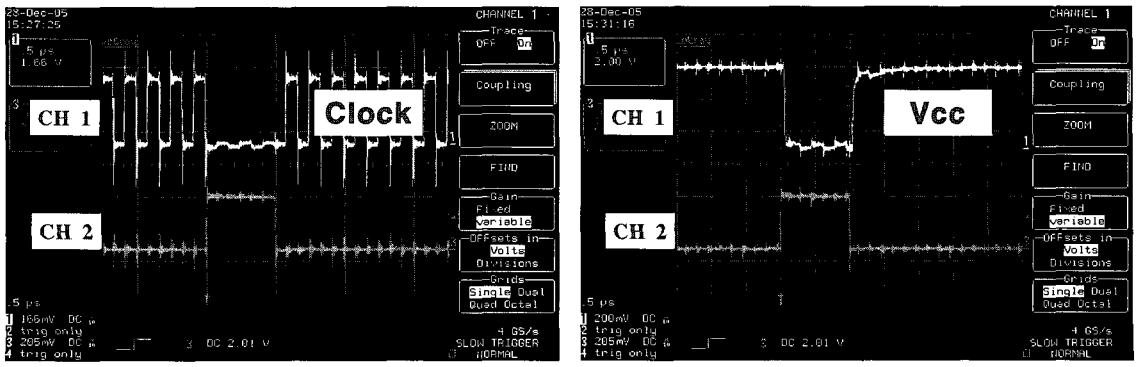
표 1. 딥 스위치를 이용한 모드 설정 방법

	1	2	3	4
카드 리더 파워 입력	ON	OFF	OFF	OFF
컷팅 파워 입력	OFF	ON	ON	OFF

	1	2	3	4
카드 리더 클럭 입력	ON	OFF	OFF	OFF
컷팅 클럭 출력	OFF	ON	ON	OFF
외부 클럭 입력	OFF	OFF	ON	ON
외부 컷팅클럭 입력	OFF	OFF	ON	OFF

	1	2	3	4
RESET 입력	OFF	OFF	ON	OFF
카드 DATA 입력	OFF	OFF	OFF	ON

그림 5 (a)는 스마트카드의 CLK 단자의 파형으로 4Mhz로 동작하는 스마트카드를 1㎲동안 클럭 신호를 차단한 것이다. 채널 1은 스마트카드의 클럭 신호이며, 채널 2는 오류 신호 생성 시점을 나타내는 신호 파형이다. 그림 5 (b)는 스마트카드의 Vcc단자의 파형을 측정한 것으로, 채널 2에 나타난 오류 신호 생성 시점에 5V인 Vcc가 1㎲동안 0V로 전원이 차단된 것이다.



(a) 클럭 차단 파형 (b) 파워 차단 파형

그림 5. 사이드 채널 분석 도구의 동작 방법

Ⅳ. 스마트카드 안전성 분석

본 장에서는 앞서 살펴본 사이드 채널 공격 분석 도구를 사용하여, 개별 모듈에 대한 안전성 분석을 수행하였다. 우선 실험에 사용된 장비에 대한 설명을 하겠고, 다음으로 이 도구를 이용하여 SEED와 ARIA에 차분전력분석공격을 적용해 보겠다. 마지막으로는 지금까지 실제 구현이 힘들었던 오류주입공격을 사이드 채널 분석 도구를 사용하여 오류주입공격 중 가장 강력하다고 알려져 있는 CRT 기반의 RSA 암호시스템에 대한 오류 공격을 적용하겠다.

4.1 실험 장비

실험의 대상이 되는 스마트카드는 국내에서 상용중인 칩을 탑재한 스마트카드를 사용하였다. 실험에 사용한 회사의 칩은 기본적으로 8비트 연산을 수행하며, DES, AES와 RSA는 하드웨어로 구현되어 있다. 그 외 알고리즘은 8, 16비트 임베디드 시스템 컴파일러인 Metrowerks사의 CodeWarrior를 사용하여, 소프트웨어로 구현이 가능하다. 그리고 칩 내부에 전력분석공격에 대비한 잡음 생성기와 오류주입공격에 대비한 사전 탐지기능 등이 내장되어 있는데, 이는 실험 결과를 통해서 확인해 볼 수 있다. 카드리더기는 EEPROM에 암호 알고리즘 탑재와 연산 결과 값을 확인할 수 있는 Smart System사의 SSR-120과 차분전력분석공격과 같이 여러 번 같은 연산을 반복 수행하는 기능을 가진 Microprossa사의 Star265를 사용했다. 기본적으로 스마트카드는 내부 클럭으로 동작하지만, 알고리즘 수행시간을 조절하기 위해서 외부 클럭을 입력할 필요가 있다. 이 때는 HAMEG 8131-2 함수발생기를 사용했다. 그리고, 소비 전력 파형을 관찰하기 위해서 LeCroy사의 LT372M 디지털 오실로스코프를 사용하였으며, 측정한 파형 분석은 MATLAB 7.0을 이용하였다.

4.2 전력분석공격

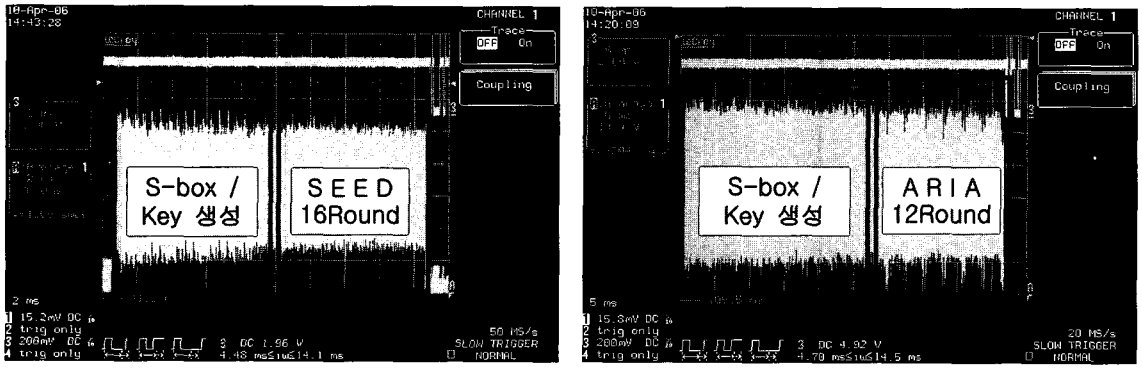
여기서는 사이드채널 공격 분석 도구를 이용한 전력분석공격에 대해서 설명하겠다. 사이드채널 공격 분석 도구는 스마트카드 접지와 리더기 접지 사이의 저항을 통해서 암호 알고리즘 연산 시 소모되는 전력을 측정할 수 있다. 그림 6은 SEED와 ARIA 알고리즘을 자체 개발하여 EEPROM에 탑재한 후 각각 1,000번씩 수행하여 측정한 평균 소비 전력 파형이다. 여기서 얻은 평균 파형을 이용하여 Ⅱ장에서 살펴본 SEED와 ARIA의 전력분석공격을 적용하여 스마트카드 내의 비밀정보를 알아낼 수 있다.

4.3 클럭오류공격

클럭오류공격은 스마트카드가 오류 공격 시점을 정밀하게 조절하기 위해서, 외부 클럭으로 동작하도록 프로그램 한 다음, 클럭을 일정 시간동안 차단하였다.

이 스마트카드는 클럭 차단 시간의 임계치 초과 유무에 따라 2가지 상태로 분류할 수 있다.

첫 번째는 클럭 차단 시간이 임계치 이하일 경우이다. 그림 7 (a)가 이 경우에 해당되는데 그림에서처럼 스마트카드는 정상적인 동작을 한다. 채널 3가 IO 신호인데, IO신호의 변화는 암호 알고리즘의

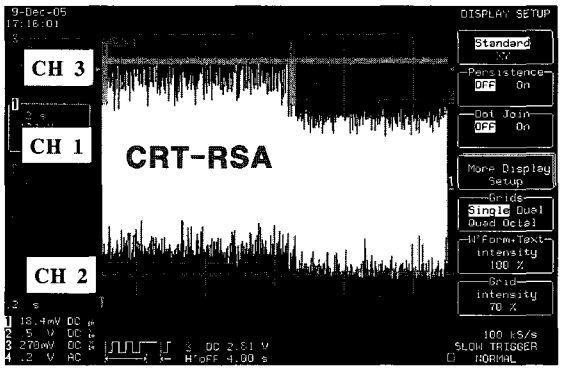


(a) ARIA 평균 파형 (b) SEED 평균 파형

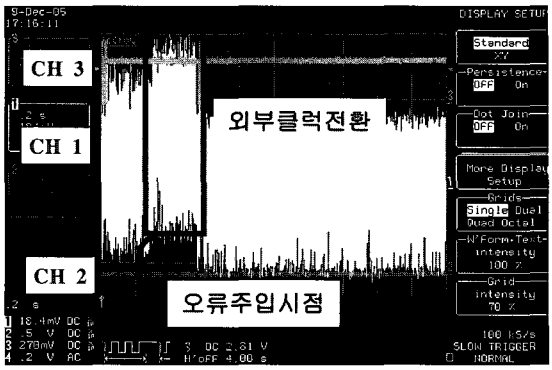
그림 6. ARIA 및 SEED 알고리즘 평균 소비 전력 파형

시작과 종료를 나타낸다. 즉, IO 신호가 변화하는 두 시점 사이가 암호 알고리즘이 수행되는 시점이다. 채널 1은 스마트카드의 전력소비를 나타내는 파형인데, 암호 알고리즘이 수행되는 동안에 전력소비가 다른 구간보다 많은 것을 알 수 있다. 채널 2는 오류 신호 생성 시점을 나타내는데, 차단 시간이 짧아서, 오류 생성 시점이 화면에 나타나지 않았다.

두 번째는 클럭 차단 시간이 임계치를 초과했을 경우이다. 그림 7 (b)가 이 경우에 해당된다. 채널 2에 나타난 오류 생성 시점부터 스마트카드의 소비 전력이 급격히 증가하고, 암호 알고리즘의 수행 속도가 빨라지는데, 이것은 내부 클럭으로 동작 시의 스마트카드의 소비 전력량과 연산 시간이 정확히 일치한다. 이 현상으로 미루어 볼 때, 이 회사의 칩을 탑재한 스마

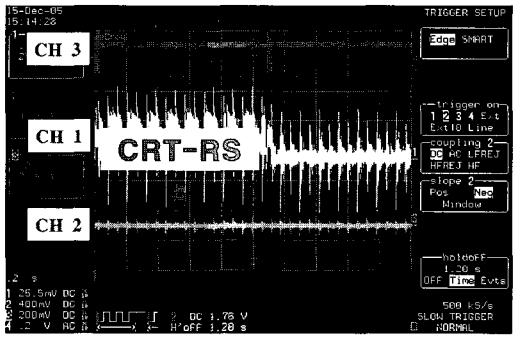


(a) 동작 클럭을 임계치 이하로 차단시



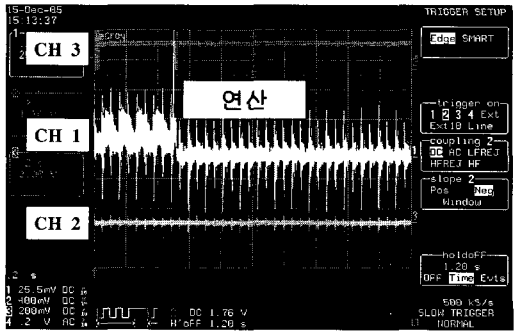
(b) 동작 클럭을 임계치 초과 차단시

그림 7. 클럭오류공격 파형



(a) 정상 동작 파형

(b) 전원 전압이 임계치까지 강하 됐을시



(c) 전원 전압이 임계치 이하일 때

그림 8. 전원오류공격 파형

트카드는 칩 내부에 사전 탐지기능이 있어 클럭 이상을 감지하고, 외부 클럭으로 동작 중이던 스마트카드를 강제적으로 안전한 내부 클럭으로 전환하여 연산을 정상적으로 종료한 것으로 보인다. 채널 3의 IO 신호를 통해서 역시 연산의 정상 종료를 확인 가능하다.

4.4 전원오류공격

전원오류공격은 스마트카드에 공급되는 전원을 일정 시간동안 차단함으로써 비정상적인 연산을 유도하는 실험이다. 이 때, 전원이 차단되더라도 아주 짧은 시간동안 전원을 차단하기 때문에 전압이 0V까지 강하되지는 않는다. 실험 결과 이 스마트카드는 동작 전압이 임계치 이상일 때, 임계치 부근일 때와 임계치 이하일 때 3가지 상태로 분류할 수 있다.

첫 번째 상태는 그림 8 (a)의 경우로 60ns보다 짧은 시간동안 스마트카드 칩의 전원을 차단했을 때이다. 이 경우는 전원 차단 시간이 극히 짧아 칩의 동작 전압은 임계치(일반적으로 Vcc±10%)보다 높게 되며, 스마트카드는 정상적으로 암호 알고리즘을 수행하였다. 채널 3은 IO파형, 채널 1은 전력 소비 파형이고, 채널 2는 오류 신호 생성 시점을 나타내는 파형이다.

두 번째 상태는 그림 8 (b)에 해당하는 경우이며, 스마트카드 칩의 전원을 60~80ns동안 차단했을 때이다. 이 때는 칩의 동작 전원이 임계치까지 떨어지게 된다. 그림 8 (a)와 (b)의 채널 1의 신호를 비교해 보면, 암호 알고리즘이 종료되는 시점의 IO 신호가 달라졌음을 확인할 수 있다. 암호 알고리즘의 종료 시점에 나타나는 IO 신호는 연산 결과 값을 리턴해 주는 부분으로 전력 소비 파형에는 변화가 없고, IO 신호에만 변화가 생겼다는 것은 스마트카드가 연산은 정상적으로 수행하였지만, 도중에 비정상적인 전원을 감지하여 결과 값을 출력하지 않은 것으로 보인다.

마지막 상태는 스마트카드 칩의 전원을 80ns이상 차단하여, 칩의 동작 전원이 임계치 이하로 떨어진 상태이다. 그림 8 (c)가 마지막 상태일 때, 스마트카드의 소비 전력을 측정한 것이다. 클럭 오류 실험에서 확인했듯이, 스마트카드는 내부에 사전 탐지기능이 있어서 클럭 오류뿐만 아니라 전원 이상까지 감지할 수 있다. 연산 도중 전원 이상을 감지하면, 칩은 현재 진행 중인 모든 연산을 중단시키고, 에러 메시지를 출력한다. 채널 1의 전력 소비 파형을 보면

레벨의 변화 없이 단순히 시간만 짧아졌다. 이로써 암호 알고리즘이 연산 도중에 중단되었다는 것을 추측할 수 있다.

V. 결 론

지금까지의 사이드 채널 공격에 대한 연구를 통해서 전력분석공격과 오류주입공격은 스마트카드에 강력한 공격법으로 알려져 있다. 그러나 전력분석공격은 비교적 구현이 쉬워 실제적인 연구가 많이 이뤄진 반면에, 오류주입공격은 구현에 어려움이 있어 실제 적용한 사례는 드물었다. 따라서 본 논문에서는 전력분석공격뿐만 아니라, 오류주입공격까지 실제 적용이 가능하여 정보보호장치의 안전성을 효율적으로 검증하고 분석할 수 있는 하이브리드 형태의 사이드 채널 분석 도구를 직접 개발하였다. 개발된 툴은 암호 알고리즘 수행 시 발생하는 누수 전력을 스마트카드 칩과 리더기 접지 사이에 연결된 저항에서 측정하여 전력분석공격을 수행할 수 있다. 또한, 공격대상인 스마트카드를 훼손하지 않고 현실적으로 적용 가능한 오류인 칩의 동작 클럭과 전압을 차단하여 생성한 오류 신호로 오류주입공격까지 적용할 수 있다.

또한 논문에서는 사이드 채널 분석 도구를 이용하여 국내에서 상용 중인 칩을 탑재한 스마트카드에 SEED 및 ARIA를 탑재한 후 차분전력분석공격과 CRT 기반 RSA에 대한 오류주입공격을 적용하여 스마트카드의 안전성을 분석하였다. 단, 실험에서는 현재까지 국제 표준에 적용되었거나 국내에서 개발된 일부 소프트웨어적인 대응책은 적용하지 않았고 스마트카드가 제작 시 가지고 있는 물리적 방어 대책만 그대로 적용하였다. 공격결과 오류주입공격은 스마트카드의 자체 방어대책으로도 안전하였으나, 전력분석공격은 기존에 제시된 방어대책을 적용할 필요가 있음을 확인하였다. 본 논문에서 개발된 도구는 실험에 사용된 회사의 칩을 탑재한 스마트카드 외에 다른 제조사의 스마트카드에도 적용하여 안전성 분석이 가능하다. 이를 통해서 대응책이 적용되지 않은 스마트카드와 대응책이 잘 적용된 카드에 대한 사이드 채널 공격 여부를 신속하고, 정확하게 판단할 수 있게 되며, 사이드 채널 공격에 실질적인 대응 방법을 단계적으로 적용하여 보안성 평가 활용할 수 있다.

참 고 문 헌

[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, "Differential power analysis", Advances in Cryptology - CRYPTO'99, LNCS 1666, pp.388-397, 1999.

[3] L. Goubin and J. Patarin, " DES and Differential Power Analysis - The Duplication Method," CHES 1999, LNCS 1717, pp.158-172, Springer, 1999

[4] M. Akkar and C. Giraud, "An implementation of DES and AES, secure against some attacks," in proceedings of CHES2001, LNCS 2162, pp.309-318, Springer-Verlag, 2001

[5] E. Oswald and K. Schramm, "An Efficient Masking Scheme for AES Software Implementation," WISA 2005, LNCS 3786, pp.292-305, 2006.

[6] Korea Information Security Agency, "Block Cipher Algorithm SEED", http://www.kisa.or.kr/seed/seed_eng.html

[7] HyungSo Yoo, ChangKyun Kim, Jae Cheol Ha, SangJae Moon and IlHwan Park, "Side Channel Cryptanalysis on SEED", WISA 2004, LNCS 3325, pp. 411-424, 2005.

[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, 제 16권 제 2호, pp129-139, 2006.

[11] M. Joye, A.K. Lenstra, and J.-J.Quisquater, "Chinese remaindering based cryptosystems in the presence of faults", Journal of Cryptology, 12(4), pp. 241-245, 1999.

[12] A. Lenstra, "Memo on RSA Signature Generation in the Presence of Faults," Sept. 28, 1996.

[13] A. Shamir, "How to check modular exponentiation," presented at the rump session of EUROCRYPT '97, 1997.

[14] C. Kim, J. Ha, S. Kim, S. Kim, S. Yen and S. Moon, "A Secure and Practical CRT-Based RSA to Resist Side Channel Attacks", ICCSA '04, LNCS 3043, pp.150~158, 2004.

[15] C. Aumuller, P. Bier, W. Fischer, P. Hofreiter, and J.-P. Seifert, "Fault attacks on RSA with CRT: Concrete results and practical countermeasures," CHES'02, LNCS 2523, pp.260-275, 2003.

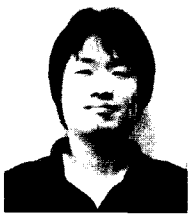
[16] J.F. Dhem and N. Feyt, "Hardware and software symbiosis helps smartcard evolution," In IEEE Micro 21, pp. 14-25, 2001.

[17] D. Boneh, R.A. DeMillo, and R.J. Lipton, "On the importance of checking cryptographic protocols for faults," In Advances in Cryptology - EUROCRYPT '97, LNCS 1233, PP. 37-51, Springer-Verlag, 1997.

[18] R. Anderson and M. Kuhn, "Low cost attacks on tamper resistant devices", LNCS 1361, pp.125-136, 1997.

[19] Sergei P. Skorobogatov, Ross J. Anderson "Optical Fault Induction Attacks", CHES '02, LNCS 2523, pp. 2-12, Springer-Verlag, 2002.

〈著者紹介〉



한 동 호 (DongHo Han) 학생회원
2005년 2월 : 경북대학교 전자전기공학부 졸업
2006년 현재 : 경북대학교 전자공학과 석사과정
〈관심분야〉 정보보호, 네트워크 보안, 스마트카드 보안

박 제 훈 (JeaHoon Park) 학생회원
2004년 2월 : 경북대학교 전자전기공학부 졸업
2006년 2월 : 경북대학교 전자공학과 석사
2006년 현재 : 경북대학교 전자공학과 박사과정
〈관심분야〉 정보보호, 네트워크 보안, 스마트카드 보안

하 재 철 (JaeCheol Ha) 종신회원
1989년 2월: 경북대학교 전자공학과 졸업
1993년 8월: 경북대학교 전자공학과 석사
1998년 2월: 경북대학교 전자공학과 박사
1998년 3월~2004년 12월: 나사렛대학교 전자계산소장, 학술정보관장
2005년 1월~2006년 1월: 나사렛대학교 입시학생처장
1998년 3월~현재: 나사렛대학교 정보통신학과 부교수
2002년 3월~현재 : 한국정보보호학회 이사
〈관심분야〉 정보보호, 네트워크 보안, 스마트카드 보안

이 성 재 (Sungjae Lee) 종신회원
1996년 2월 : 고려대학교 수학과 이학사
1999년 2월 : 고려대학교 수학과 이학석사
2002년 현재 : 고려대학교 정보보호대학원 박사수료
1999년 9월~현재 : 한국정보보호진흥원(KISA) 선임연구원

문 상 재 (SangJae Monn) 종신회원
1972년 2월: 서울대학교 공업교육(전자)과 졸업
1974년 2월: 서울대학교 전자공학과 석사
1984년 6월: 미국 UCLA 전자공학과 박사
1984년 7월~1985년 6월: UCLA Postdoctoral 근무
1984년 7월~1985년 6월: 미국 OMNET 컨설턴트
1974년 12월~현재: 경북대학교 공과대학 전자전기컴퓨터공학부 교수
2000년 8월~현재: 경북대학교 이동네트워크 정보보호기술 연구센터 소장
2002년 2월~현재: 한국정보보호학회 명예회장
〈관심분야〉 정보보호, 디지털 통신, 이동 네트워크