情報保護學會論文誌
第19卷 第3號, 2009. 6

CRT-RSA 암호시스템에 대한 광학적 오류 주입 공격의 실험적 연구

박 제 훈,[1†] 문 상 재,[1‡] 하 재 철[2]
[1]경북대학교, [2]호서대학교

Experimental Analysis of Optical Fault Injection Attack for CRT-RSA Cryptosystem

JeaHoon Park,[1†] SangJae Moon,[1‡] JaeCheol Ha[2]
[1]Kyungpook National University, [2]Hoseo University

요 약

중국인의 나머지 정리(Chinese Remainder Theorem, CRT)를 이용하는 RSA 암호시스템을 암호 칩에 구현할 경우, 암호 칩에서 동작하는 과정 중에 한 번의 오류 주입으로 모듈러스 N의 비밀 소인수 p, q 값이 노출될 수 있다. 본 논문에서는 상용 마이크로컨트롤러에 CRT-RSA 암호 시스템을 구현한 후, 레이저 빔과 플래시를 이용한 광학적 오류 주입 방법으로 공격을 시도하고 실험 결과를 분석하였다. 레이저 빔과 플래시를 이용한 오류 주입 공격 실험 결과, 일부 상용 마이크로 컨트롤러는 광학적 오류 주입 공격에 대해 취약한 특성으로 인해 CRT-RSA 암호 시스템에 소인수 분해 공격이 적용됨을 확인하였다.

ABSTRACT

The CRT-RSA cryptosystem is very vulnerable to fault insertion attacks in which an attacker can extract the secret prime factors p, q of modulus N by inserting an error during the computational operation on the cryptographic chip. In this paper, after implementing the CRT-RSA cryptosystem, we try to extract the secret key embedded in commercial microcontroller using optical injection tools such as laser beam or camera flash. As a result, we make sure that the commercial microcontroller is very vulnerable to fault insertion attacks using laser beam and camera flash, and can apply the prime factorization attack on CRT-RSA Cryptosystem.

Keywords: CRT-RSA, Fault Analysis Attack, Optical Fault Injection, Side-channel Attack

I. 서 론

RSA 공개 키 암호 시스템은 그 안전성과 효율성이 오랫동안 증명되어 가장 많이 사용되는 암호 시스템 중 하나이다. 한편, RSA 암호 시스템에서는 암호 처리를 위해 멱승(exponentiation) 연산이 필요하고 이에 대한 계산 속도를 높이기 위해 비밀 키에 대한 멱승시에는 중국인의 나머지 정리 (Chinese Remainder Theorem, CRT)를 이용하기도 한다[1]. 이론적으로 CRT에 기반한 RSA는 일반 RSA보다 계산 속도가 약 4배 정도 빠른 특성을 보인다.

하지만 최근 CRT-RSA는 오류 분석 공격(fault analysis attack) 혹은 오류 주입 공격(fault injection attack)이라 불리는 물리적 공격에 매우 위험한 것으로 밝혀졌다[2,3]. 오류 주입 공격은 1996년 처음 소개되었는데 암호 시스템이 탑재된 암호용 칩에 공격자가 임의의 오류를 주입하여 내부에서

접수일(2009년 1월 31일), 게재확정일(2009년 5월 14일)
† 주저자, jenoon65@ee.knu.ac.kr
‡ 교신저자, sjmoon@ee.knu.ac.kr

오동작을 유발한 후, 출력되는 연산 결과를 분석하여 공격 대상 칩 내부에 저장된 비밀키를 추출해 내는 능동적 공격 방법이다[4,5]. 그 동안의 연구 결과 암호 칩에 주입되는 오류들은 하드웨어 칩의 특정 부분에 전압 글리치(glitch)를 넣거나 전자파 방사 그리고 레이저 빔과 같은 빛 종류에 의해 오류가 주입될 수 있다. 특히, 공격자는 CRT-RSA 알고리즘에 단 한 번의 오류 주입만으로도 RSA 알고리즘의 모듈러스 N의 비밀 소인수 p, q를 알아낼 수 있어 CRT-RSA 알고리즘은 오류 주입 공격에 매우 취약하다.

이후에도 많은 연구자들에 의해 CRT-RSA 알고리즘에 적용 가능한 오류 주입 공격 방법이 개발되었고, 이에 대한 방어 방법도 제안되었다[6-14]. 하지만, 대부분의 연구 결과들은 공격 대상 칩에 대한 실제적인 실험결과가 아닌 이론적으로 이루어진 것이 대부분이다. 보다 현실적인 공격 방법과 방어 방법 연구를 위해 오류 주입 공격을 구현하는 것이 중요하지만, 국내·외적으로 실제 CRT-RSA 알고리즘에 오류 주입 공격을 실험한 연구 결과들은 많지 않다. 많은 연구 그룹 중에서 영국의 Cambridge 대학[15], 벨기에의 Louvain 대학[16], 오스트리아의 Graz 대학[17] 연구 그룹 정도만 실제로 오류 주입 공격을 실험하여 연구한 결과들을 발표하였다. 오류 주입 공격 실험 환경을 갖춘 연구팀들의 연구 결과들에서는 레이저, 전압 글리치, EM 펄스 등을 이용하여 오류 주입 공격에 성공한 것으로 보고되어 있다. 국내에서는 아직까지 오류 주입 실험과 관련한 연구가 미흡한 실정으로, 오류 주입 공격을 실제 실험하거나 구체적인 실험 환경을 구축과 관련해서 보고된 문헌은 아직 없다.

본 논문에서는 국내에서도 오류 주입 공격의 실제적인 가능성을 검증하기 위해 해외 연구 기관들의 연구 결과들을 분석하여 오류 주입을 위한 실험 환경을 구성하고 광학적 오류 주입 도구를 이용한 오류 주입 공격을 시도하였다. 이를 위해 상용으로 많이 사용되고 있는 ATmega128 마이크로컨트롤러 칩[18]에 CRT-RSA 알고리즘을 구현한 후 공격 실험을 하였다. 실험을 위해 칩을 디캡핑하여 내부의 회로가 노출되도록 하였고, 레이저 빔이나 카메라 플래시와 같은 광학 오류를 회로에 주사하여 오류 연산을 유도하였다. 실험에서는 레이저와 플래시를 이용하여 칩에 구현된 CRT-RSA 알고리즘의 오류 결과를 출력하게 하여, Bellcore사에서 제안한 오류 결과 분석 방법으로 RSA 알고리즘의 모듈러스 N의 비밀 소인수 p, q를 알아낼 수 있음을 확인하였다. 오류 주입 공격을 실험적으로 성공함에 따라 물리적 오류 주입 공격에 대한 대응책이 마련되지 않은 일반 칩에 비밀 키를 내장하여 CRT-RSA 암호 시스템을 구현할 경우에는 비밀 키 노출에 주의하여야 한다.

II. CRT-RSA 암호 시스템에 대한 오류 주입 공격

2.1 CRT-RSA 암호 알고리즘

RSA 암호 알고리즘은 대표적인 공개키 암호 알고리즘으로서, 메시지를 암호하기 위해 상대방의 공개키를 사용하여 암호하고, 암호문을 복호하기 위해 공개된 값에 대응되는 자신의 비밀 키를 사용한다. 이와 반대로 RSA 서명에서는 메시지를 서명하기 위해 사용자 자신의 비밀 키 값을 이용하여 서명하고, 서명값을 검증하기 위해서는 공개 키를 이용한다.

따라서 RSA 암호 시스템에서 공개 키 e와 모듈러스 $N(=p \cdot q)$은 공개 키이고, 비밀 키 d와 모듈러스 N의 소인수 p, q는 비밀 정보이다. 비밀 키 d는 공개 키 e와 모듈러스 $\Phi(N)$에서 역수 관계를 가진다 ($d = e^{-1} \bmod \Phi(N)$). 여기서 $\Phi(N)$은 N보다 작은 정수 중에서 N과 서로 소인 정수의 개수를 나타낸다. RSA 암호 시스템의 안전도는 큰 길이의 합성수 N를 소인수 분해하여 비밀 소수 p나 q를 알아내는 것인데 이 문제는 아직까지 수학적으로 매우 어려운 문제로 알려져 있다. 비밀 정보는 보통 1024비트 정도의 큰 정수를 사용하므로 대부분 스마트카드와 같은 암호 칩 내부에 저장하여 메시지에 대한 서명이나 복호를 할 경우에 사용한다. 그리고 메시지 m에 대한 서명은 $S = m^d \bmod N$과 같이 메시지에 대해 비밀 키로 멱승을 수행하게 된다. 이러한 멱승은 보통 이진(binary) 방식을 많이 사용하게 되는데 [그림 1]은 이진 멱승 방법을 이용한 일반적인 RSA 서명 알고리즘을 보여 주고 있다. [그림 1]에서 비밀 키 d는 n 비트의 이진 정수로

```
입력 : d, N, m
출력 : S = m^d mod N
1. S = 1;
2. For i from n-1 to 0 {
2.1     S = S×S mod N;
2.2     if (d_i == 1) S = S×m mod N;
   }
3. Return S
```

[그림 1] 일반적인 RSA 서명 알고리즘

표현할 수 있으며, d_i는 d의 i 번째 비트를 의미한다.

CRT-RSA 알고리즘은 RSA 알고리즘이 모듈러스 N에서 연산하는 것과 달리, 모듈러스 p, q상에서 각각 계산된 결과를 재결합(recombination)한다. CRT-RSA에서 사용되는 p나 q의 길이는 일반적으로 N의 1/2 정도이므로 일반 RSA보다 약 4배 정도의 연산 속도를 가지는 것으로 알려져 있다. 즉, n 비트 크기의 N상에서의 멱승 연산 한번을 $n/2$비트 크기의 두 번의 멱승 연산으로 대체하는 효과를 얻을 수 있다. [그림 2]는 가우스(Gauss) 재결합 방법을 사용하는 CRT 기반 RSA 알고리즘을 나타낸 것이다. 그림에서 단계 1과 2는 각각의 소수 p나 q에 대한 메시지에 대한 멱승을 수행하며 단계 3에서는 모듈러스 N에 대한 재결합을 수행한다. 또한, CRT 기반 RSA는 사용하는 모듈러스 p, q 자체가 비밀이므로 계산되는 중간 값을 예측하기가 어려워 전력 분석 공격과 같은 부채널 공격에 강인한 면을 가지고 있다[19].

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 2] 가우스 방법을 이용한 CRT 기반 RSA 서명

[그림 2]에서 사용한 가우스의 재결합 방법 외에도 가너(Garner)가 제안한 재결합 방법을 사용하여 RSA 암호 시스템을 구성하기도 한다. 다음의 식은 가너의 재결합 방법을 나타내고 있다. 일반적으로 가너 재결합 방식이 가우스 재결합 방식에 비해 사전 역수 계산이 한번 적은 특징이 있어 흔히 이용되기도 한다. 그러나 다음 절에 설명하는 오류 주입 공격은 두 가지 재결합 과정에 모두 적용됨을 주의해야 한다.

$$S = S_q + [(S_p - S_q) \cdot q_I) \bmod p] \bmod N \quad (1)$$

2.2 오류 주입 공격

Bellcore사에서 제안한 CRT 기반 RSA 알고리즘에 대한 오류 주입 공격 방법은 가장 쉽게 적용할 수 있는 오류 주입 공격 기술로서 RSA 알고리즘의 비밀 소인수인 p와 q를 알아낼 수 있다[2,3]. 공격 과정을 간단히 설명하면 다음과 같다.

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

단계 2 : 다시 메시지 m을 이용하여 [그림 2]의 알고리즘을 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 서명값을 S'라 한다.

단계 3 : 위의 두 단계에서 생성된 서명의 차를 구한 후 $GCD(S-S', N)$을 계산하여 비밀값 q(또는 p)를 추출해 낸다. 여기서, $GCD()$는 Great Common Divisor를 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 서명값의 재결합식 :
  $S = (S_p \cdot q \cdot q_I) + (S_q \cdot p \cdot p_I) \bmod N$
- 정오류 서명값의 재결합식 :
  $S' = (S_p' \cdot q \cdot q_I) + (S_q \cdot p \cdot p_I) \bmod N$
  $\therefore S - S' = (S_p \cdot q \cdot q_I) - (S_p' \cdot q \cdot q_I) \bmod N$
  $\therefore GCD(q(S_p \cdot q_I - S_p' \cdot q_I), p \cdot q) = q$

또한, Joye 등은 정상 서명 값이 없다고 하더라도 단 한 개의 오류 서명을 이용하여 CRT-RSA 알고리즘의 비밀 키 p, q를 알아낼 수 있는 방법을 제안하였다[4]. 이 공격에서는 위의 단계 2와 같이 오류 서명 S' 하나만 추출하면 된다. 그리고 다음 식을 이용하면 정상 서명 값이 없이도 CRT-RSA의 비밀 값 q를 알아낼 수 있다.

$$GCD(((S')^e - m), N) = q \quad (2)$$

이 후 많은 연구자들에 의해 오류 주입 공격에 안전한 새로운 CRT-RSA 알고리즘들이 제시되었다. 그러나 제안된 대응책들은 이론적 내용이 대부분이었고 이것들도 추후 더욱 정교한 공격 방법에 의해 다시 공격될 수 있음이 밝혀졌다. 한편 오류 주입 공격을 위해서는 칩에 대한 세밀한 오류 주입이 필요하므로 고

가의 오류 주입 장치가 필요할 뿐만 아니라 칩 표면을 모두 디캡핑할 수 있는 기술도 필요하게 되었다.

III. 상용 마이크로컨트롤러에 대한 광학 오류 주입 공격 실험

3.1 주요 실험 장비

3.1.1 공격 대상 칩

오류 주입 공격은 어떠한 알고리듬을 사용하는가와 어떠한 칩을 사용하는가에 따라 결과는 달라질 수 있다. 예를 들면 금융이나 출입 통제 시스템에는 스마트카드와 같은 보안 전용 칩을 사용하지만 스마트카드를 사용할 수 없는 환경에서는 일반 마이크로프로세서를 이용하여 정보보호 서비스를 제공하기도 한다. 즉, 홈 네트워크 보안 서비스나 USN 등에서 사용되는 마이크로프로세서가 정보보호용으로 사용될 경우에는 직접적인 위협 대상이 될 수 있다. 본 논문에서는 센서 네트워크 시스템에서 많이 사용되는 상용 8비트 마이크로프로세서인 ATmega128칩에 오류 주입을 시도하여 그 결과를 분석하였다[18]. [표 1]은 ATmega128의 주요 제원을 나타낸 것이다.

[표 1] ATmega128 주요 제원

Program Memory	Bytes	128K
	# Optional External memory	up to 64K
Data SRAM (Bytes)		4K
EEPROM (Bytes)		4K
주 클럭		16MHz
구동 전압		4.5V ~ 5.5V

3.1.2 오실로스코프

암호용 칩이 동작하는 과정에 오류를 주입하기 위해서는 무엇보다도 오류 주입 시점이 중요하다. 이를 위해서는 칩이 동작하는 과정을 측정할 수 있는 고성능의 오실로스코프 장비가 필요하다. 논문에서는 오류 주입 시점을 결정하고 오류 주입에 의한 공격 대상 칩의 동작 변화를 관측/분석하기 위해서 LeCroy사의 LT374M 모델을 사용하였다. 이 오실로스코프는 4채널을 가지고 있으며, 500MHz의 대역폭과 2G/s의 성능을 가지고 있다[20].

3.1.3 고배율 현미경

오류 주입 공격에서 중요한 요소 중 다른 하나는 칩 내부의 어느 부분에, 어느 정도의 강도로, 어느 정도의 범위에 오류를 주입할 것인지 하는 것이다. 논문에서는 암호 칩 내부를 확대해서 관측할 수 있고 오류 주입 위치를 정확하게 판독하기 위해 전자 현미경을 이용하여 칩을 확대하여 볼 수 있도록 설치하였다. 즉, 공격 대상 칩을 디캡핑한 후 내부 회로의 SRAM, DRAM, flash 메모리, CPU 등의 특정 영역에 레이저 오류주입 공격을 시험해 보기 위해서 사용하였다. 사용된 현미경의 배율은 *20에서 *1000까지 확대할 수 있다.

3.1.4 레이저

오류 주입의 핵심이 되는 장비로서 공격 대상 칩의 내부 회로에 직접 레이저 오류를 주입하여 오류 결과값이나 이상 동작을 유도하기 위해 사용된다. 논문에서는 EzLaze 3 모델을 사용하였다[21]. 이 레이저 장비는 펄스 폭을 4ns, 그리고 전력 에너지를 3.0mJ까지 조절하여 레이저 빔을 주입할 수 있다.

3.2 레이저 오류 주입 공격 실험

본 논문의 실험에 사용한 공격 대상 마이크로컨트롤러에는 1024비트의 이상의 알고리즘을 구현할 수 없었고, 논문에서 이용한 오류 주입 공격은 CRT-RSA 알고리즘의 비트 크기에 상관없이 적용되는 공격 방법이다. 따라서 오류 주입 공격의 가능성을 확인하기 위해 256비트의 CRT-RSA 알고리즘을 ATmega128 칩에 소프트웨어로 구현하여 실험하였다. 공격 대상 칩에서 동작하는 CRT-RSA의 주요 파라미터들은 다음과 같다. [표 2]는 256비트용 CRT-RSA 암호 시스템에 사용된 파라미터를 16진수로 정리한 것이다.

레이저 오류 주입을 위해서는 먼저 칩의 외관을 디캡핑을 해야 하는데 칩 디캡핑은 다음과 같은 절차에 의해 이루어진다.

(a) Hot Plate에 디캡핑 하고자 하는 칩을 적당하게 가열해 준다.

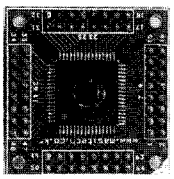
(b) 제거하고자 하는 패키지 부분에 스포이드를 이용하여 발연질산이나 황산과 같은 화학 약품을 적당량 살포한다.

〔표 2〕 256비트 CRT-RSA 알고리즘의 주요 파라미터

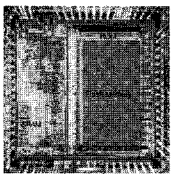
비밀키 d	6C43BAB4AF57BAA8911297A3719E28D8F45BF97285C7FDCFAFC4A18314A488FB
공개키 e	3
비밀값 p	D771E51EF0C69395770F7B868F06C775
비밀값 q	C0F75BE21615BCA7ACF1C10C2EC5DDF7
모듈러스 N	A265980F070397FCD99BE3752A6D3D4706F3372CCF884CF4ABA82ED75CC372E3

Wavelength
532nm
Pulse width
4ns
Power
~ 3.0mJ

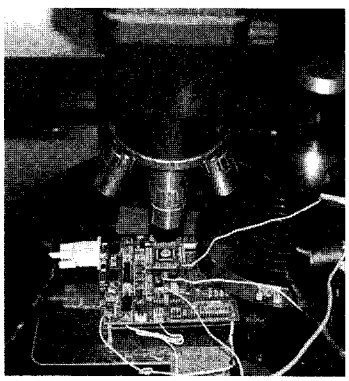
〔그림 3〕 레이저 오류 주입 장치 및 주요 제원



(a) 디캡 된 칩



(b) 내부 회로



(c) 실험을 위한 장치 구성

〔그림 4〕 레이저 오류 주입을 위한 실험 환경

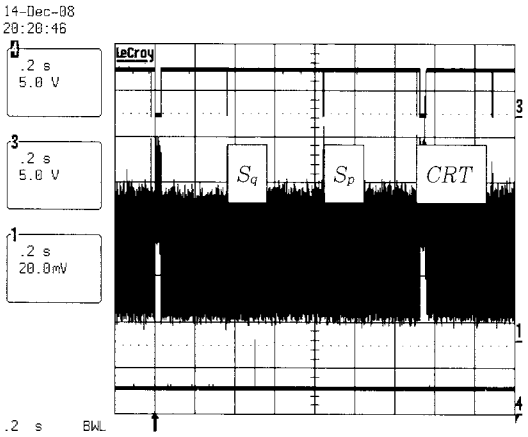
(c) 화학 반응을 일으킨 칩에 원하는 부위가 드러나면 아세톤을 이용하여 클리닝 후 건조한다.

위의 절차를 반복하여 ATmega128 칩을 디캡핑한 후 칩에 레이저 빔을 이용한 오류를 주입하기 위해서는 파형 측정용 오실로스코프와 칩의 내부를 확대하여 오류의 위치를 선정하기 위한 전자 현미경이 사용된다. 〔그림 4〕는 디캡된 ATmega128 칩과 레이저 오류 주입 공격을 위한 실험 환경을 보여주고 있다.

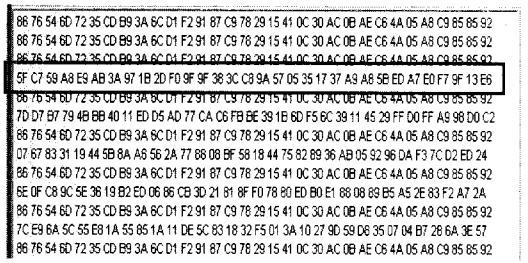
실험에서는 현미경을 통하여 디캡핑된 칩의 내부를 관찰하고, CPU, RAM, ROM, Flash memory 등의 여러 영역에 레이저 오류를 주입하였다. 실험에서 레이저를 이용한 오류 주입 시점이 중요한데 이를 위해서는 ATmega128 칩의 I/O 신호를 이용하여 이를 레이저 주입의 트리거 신호로 사용하였다. 그리고 PC와의 시리얼 통신을 통해 256 비트 CRT-RSA 알고리즘의 결과를 출력하도록 하였다. 〔그림 5〕는 오실로스코프로 측정된 CRT-RSA 알고리즘의 소비 전력 파형과 수행 과정을 나타낸 것이다.

〔그림 5〕에서 제일 상단의 신호는 CRT-RSA 알고리즘의 세부 연산을 구분하기 위한 I/O 신호이고, 두 번째 중간에 위치한 신호는 소비 전력 파형이다. 세 번째 하단에 위치한 신호는 레이저 오류가 주입되는 시점을 나타내고 있다. 첫 번째 I/O 신호를 함수 발생기의 트리거 신호로 인가하여 출력되는 펄스 신호의 지연시간을 조종해서 레이저 오류 주입 위치를 조정하였다.

본 실험에서는 〔그림 5〕에서와 같이 $S_q = m^{d_q} \bmod q$ 가 계산되는 도중에 레이저 오류를 주입하였다. 공격은 S_q를 계산하는 과정의 어느 시점이든 상관이 없고 이 계산 구간은 전체 연산 시간의 약 절반을 차지하는 넓은 구간이므로 비교적 오류 주입을 위한 정교한 시점을 필요로 하지는 않는다. 〔그림 5〕에서와 같이 ATmega128 칩에 구현한 256 비트의 CRT-RSA 알고리즘의 수행 시간은 약 1300ms이고, S_q가 연산되는 도중에 레이저 오류를 주입하기 위해서 〔그림 5〕의 세 번째 신호와 같이 칩의 I/O가 발생한 후 약 500ms 후에 함수 발생기에서 레이저 주입을 위한 트리거 신호가 발생하도록 하였다. 실제로는 레이저 주입을 위한 트리거 신호가 발생한 뒤 약 23ms의 지연시간 후 칩에 레이저가 주입되므로 ATmega128 칩의 I/O 신호가 발생한 후 약 523ms 후에 칩에 레이저가 주입된다.



〔그림 5〕 S_q 연산중에 오류를 주입하는 경우



〔그림 6〕 레이저 오류 주입에 의한 오류 출력 결과

〔그림 6〕은 ATmega128 칩에서 CRT-RSA 알고리즘을 정상적으로 수행하는 경우와 오류가 주입되었을 경우의 PC로 출력된 서명 값을 보여 주고 있다. 〔그림 6〕에서와 같이 정상 서명이 이루어진 경우에는 그 서명 값이 반복하여 잘 나타나지만 레이저 오류 주입 공격을 시도하면 비정상적인 값들이 출력됨을 볼 수 있다.

- 정상 서명값 :
8676546D7235CDB93A6CD1F29187C9782915410C30AC0BAEC64A05A8C9858592
- 오류 서명값 :
5FC759A8E9AB3A971B2DF09F9F383CC89A5705351737A9A85BEDA7E0F79F13E6

여기에서 〔그림 6〕의 오류 출력들 중 하나를 이용하여 Bellcore 공격을 적용하여 CRT-RSA의 비밀 소인수를 알아내는 방법은 다음과 같다. 먼저 정상 서명 값과 오류 서명 값의 차를 구한다.

- 정상 서명값 - 오류 서명값 :
26AEFAC4888A93221F3EE152F24F8CAF8EBE3BD7197462066A5C5DC7D1E671AC

그리고 이 차분 값과 모듈러스 N과의 최대 공약수를 계산한다.

- GCD(정상 서명값 - 서명값, 모듈러스 N) =
D771E51EF0C69395770F7B868F06C775

최종적인 결과를 보면 이 결과가 비밀 키 p임을 알 수 있다. 물론 2장에서 언급한 Joye 등에 의한 오류 주입 공격처럼 오류 서명에 공개 키를 멱승하여 최대 공약수를 구하는 방법으로도 비밀 키를 찾을 수 있다.

$$GCD(((S')^e - m), N) = p \tag{3}$$

뿐만 아니라 $S_p = m^{d_p} \bmod p$에 레이저 오류를 주입했을 경우에는 GCD(Great Common Divisor)를 구하는 함수의 결과로 q값을 알아낼 수도 있다. 따라서 오류 주입 공격을 통해 공격에 대한 대응책이 마련되지 않은 암호 칩의 경우는 공격자가 칩 내부의 비밀 키를 추출할 수 있음을 실험적으로 확인하였다.

이러한 공격은 원래 소인수분해 문제인 합성수 N으로부터 비밀 소수 p나 q를 직접 찾아내는 접근 방법과는 약간 차이가 있다. 즉, 식 (3)과 같이 N에도 비밀 성분인 p가 포함되어 있으며 오류 서명으로부터 유도된 $(S')^e - m$에도 비밀 성분 p가 공통으로 포함되어 있을 경우 최대 공약수를 찾는 알고리듬을 이용하여 소수 p 를 찾아내는 것이다. 결론적으로 광학적 오류 주입 실험을 통해 RSA 암호 시스템에서 N의 소인수를 찾아낼 수 있으므로 소인수분해 문제를 푸는 것과 동일한 결과를 얻을 수 있었다.

3.3 플래시 오류 주입 공격 실험

ATmega128 칩에 일반 광학 오류를 주입하기 위해서 일반 디지털 카메라의 플래시를 이용하는 실험도 수행하였다. 실험 결과, 카메라의 플래시를 이용한 오류 주입 공격도 레이저 오류 공격과 동일하게 출력되는 오류 출력값을 얻을 수 있었고 이를 이용하여 Bellcore 공격을 적용하여 CRT-RSA 암호시스템의 비밀 소인수 p, q를 구할 수 있었다. 다만, 일반 디지털 카메라를 이용한 플래시 오류 주입 실험의 경우에는 레이저 오류

주입 실험과 달리 ATmega128 칩의 I/O 신호를 이용하여 플래시 오류 주입 시점을 정확하게 조정하지 못하는 단점이 있었다. 따라서, 플래시 주입 시점을 정교하게 조정하지 못하기 때문에 CRT-RSA 알고리즘을 반복 수행시켜 놓고 S_p나 S_q 연산중에 플래시 오류가 주입되도록 실험을 반복하였다. 플래시 오류가 S_p 연산에 주입되는지 S_q 연산에 주입되는지는 알 수 없었지만, 오류 연산에 의해 출력되는 오류 서명값을 이용하여 p 또는 q를 알아낼 수 있었다.

3.4 오류 주입 실험 결과 분석

레이저와 플래시를 이용한 CRT-RSA 암호 시스템을 탑재한 ATmega128 칩에 대한 오류 주입 공격 실험 결과, 레이저와 플래시 모두 ATmega128 칩이 동작하는 중에 주입되면 오류 결과값을 출력하게 할 수 있는 효과적인 오류 주입 도구라는 것을 확인할 수 있었다.

레이저 오류 주입 실험의 경우, ATmega128 칩 내부의 CPU, RAM, ROM, Flash memory 등의 거의 모든 영역에서 오류 연산을 유도할 수 있었다. 다만 위치에 따라 주입되는 레이저의 세기가 달랐지만, 실험때마다 위치에 따른 레이저의 세기가 변하는 등 특정 영역에 특정 세기의 레이저를 주입해야만 오류 연산을 유도한다는 규칙은 발견할 수 없었다. 레이저의 세기가 약하면 오류 서명값을 출력하지 않고, 레이저의 세기가 강하면 레이저 주입 순간에 칩이 동작을 멈추기 때문에, 실험에서는 주입 위치를 먼저 정한 후 알고리즘의 출력을 관찰하면서 정상 동작하지만 오류 서명값이 출력될 수 있도록 레이저의 세기를 조절하였다. 향후에는 보다 정교한 오류 주입 공격을 위한 방법의 개발이 필요하며 일반 RSA와 같은 암호 시스템 등을 공격하기 위한 모듈라 곱셈 수준의 하위 단계까지 세밀한 분석이 필요하다.

IV. 결 론

현재 국내외적으로 가장 많이 사용하는 CRT-RSA 알고리즘은 한 번의 오류 주입으로 비밀 값인 소인수 p, q가 노출되는 치명적인 약점을 가지고 있다. 따라서 이에 관한 많은 이론적인 연구가 진행되었지만, 실제 실험을 통하여 오류 주입 공격을 시도하여 성공한 사례를 발표된 경우는 많지 않다. 본 논문에서는 광학 오류 주입 공격 환경의 구성을 설명하여, 공격 대상 칩의 광학 오류 주입 공격에 대한 취약성을 검증할 수 있도록 하였다. 또한, 국내에서는 처음으로 상용 ATmega128 칩에 CRT-RSA 암호시스템을 구현했을 경우 레이저나 플래시와 같은 광학 오류 주입 공격에 취약한지를 실제 비밀 소인수 p, q를 추출하는 실험을 통하여 검증하였다. 따라서 이에 대한 오류 주입 방어대책을 세우지 않은 채 이러한 종류의 칩을 암호용도로 사용한다면 비밀 키가 공격자에 의해 유출될 수 있으므로 주의를 해야 한다. 또한 어느 칩이든 비밀 정보가 담겨져 있거나 이를 정보보호용으로 사용하는 경우에는 오류 주입 공격과 같은 물리적 공격이 가능한지를 반드시 검사한 후 사용하여야 한다.

참 고 문 헌

[1] C. Couvreur and J. Quisquater, "Fast decipherment algorithm for RSA public-key cryptosystem," Institution of Engineering and Technology IET, Electronics Letters, vol. 18, no. 21, pp. 905-907, Oct. 1982.

[2] D. Boneh, R. DeMillo, and R. Lipton, "New Threat Model Breaks Crypto Codes," Bellcore Press Release, Sep. 1996.

[3] A. Lenstra, "Memo on RSA Signature Generation in the Presence of Faults," private communication(available from the author), Sep. 1996.

[4] M. Joye, A. Lenstra, and J. Quisquater, "Chinese remaindering based cryptosystems in the presence of faults," Journal of Cryptology, vol. 12, no. 4, pp. 241-245, Dec. 1999.

[5] D. Boneh, R. DeMillo, and R. Lipton, "One the importance of checking cryptographic protocols for faults," Eurocrypt Conference-EUROCRYPT'97, LNCS 1233, pp. 37-51, 1997.

[6] S. Yen, S. Kim, S. Lim, and S. Moon, "RSA speedup with residue number system immune against hardware fault cryptanalysis," International Conference on Information Security and Cryptology-ICISC'01, LNCS 2288, pp. 397-413, 2001.

[7] C. Aumüller, P. Bier, W. Fischer, P. Hofreiter, and J. Seifert, "Fault attacks on RSA with CRT: concrete results and practical countermeasures," Workshop on Cryptographic Hardware and Embedded Systems-CHES'02, LNCS 2523, pp. 260-275, 2002.

[8] S. Yen, S. Moon, and J. Ha, "Permanent fault attack on the parameters of RSA with CRT," Australasian Conference on Information Security and Privacy-ACISP'03, LNCS 2727, pp. 285-296, 2003.

[9] J. Blömer, M. Otto, and J. Seifert, "A new CRT RSA algorithm secure against Bellcore attacks," Proceedings of the 10th ACM conference on Computer and communications security, pp. 311-320, Oct. 2003.

[10] D. Wagner, "Cryptanalysis of a provably secure CRT-RSA algorithm," Proceedings of the 11th ACM conference on Computer and communications security, pp. 92-97, Oct. 2004.

[11] C. Giraud, "Fault resistant RSA implementation," Workshop on Fault Diagnosis and Tolerance-FDTC'05, LNCS 2779, pp. 142-151, 2005.

[12] F. Fumaroli and D. Vigilant, "Blinded fault resistant exponentiation," Workshop on Fault Diagnosis and Tolerance-FDTC'06, LNCS 4236, pp. 62-70, 2006.

[13] S. Yen, D. Kim, and S. Moon, "Cryptanalysis of two protocols for RSA with CRT based on fault infection," Workshop on Fault Diagnosis and Tolerance-FDTC'06, LNCS 4236, pp. 53-61, 2006.

[14] C. Kim and J. Quisquater, "How can we overcome both side channel analysis and fault attacks on RSA-CRT," Proceedings of the Workshop on Fault Diagnosis and Tolerance in Cryptography, pp. 21-29, Sep. 2007.

[15] S. Skorobogatov and R. Anderson, "Optical Fault Injection Attack," Workshop on Cryptographic Hardware and Embedded Systems-CHES'02, LNCS 2523, pp. 2-12, 2002.

[16] C. Kim and J. Quisquater, "Fault Attacks for CRT Based RSA: New Attacks, New Results, and New Countermeasures," Workshop in Information Security Theory and Practice-WISTP'07, LNCS 4462, pp. 215-228, 2007.

[17] M. Schmidt and M. Hutter, "Optical and EM Fault-Attacks on CRT-based RSA: Concrete Results," Proceedings of the 15th Austrian Workshop on Microelectronics, pp. 61-67, Oct. 2007.

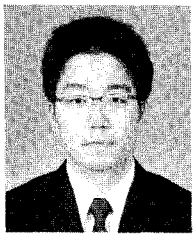
[18] Atmel, http://www.atmel.com/dyn/products/product_card.asp?part_id=2018

[19] T. Messerges, E. Dabbish, and R. Sloan, "Power Analysis Attacks of Modular Exponentiation in Smartcards," Workshop on Cryptographic Hardware and Embedded Systems-CHES'99, LNCS 1717, pp. 144-157, 1999.

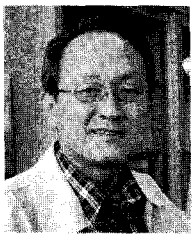
[20] LeCroy, http://www.lecroy.com/tm/products/scopes/waverunner2/brochure/page10.asp

[21] New Wave, http://www.new-wave.com/1nwrProducts/EZLaze3.htm

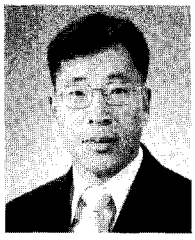
〈著者紹介〉



박 제 훈 (Jea Hoon Park) 정회원
2004년 2월: 경북대학교 전자·전기공학부 졸업
2006년 2월: 경북대학교 전자공학과 석사
2006년 3월~현재: 경북대학교 전자전기컴퓨터학부 박사과정
〈관심분야〉 정보보호, 네트워크 보안 스마트카드 보안



문 상 재 (Sang Jae 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 전자전기학부 학부장
2001년 1월~2001년 12월: 한국정보보호학회 회장
1974년 12월~현재: 경북대학교 전자전기컴퓨터공학부 교수
2000년 8월~현재: 경북대학교 이동네트워크 정보보호기술 연구센터장
2002년 2월~현재: 한국정보보호학회 명예회장
〈관심분야〉 정보보호, 디지털 통신, 이동 네트워크



하 재 철 (Jae Cheol 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 연구 교수
2007년 3월~현재: 호서대학교 정보보호학과 부교수
2002년 3월~현재: 한국정보보호학회 이사
〈관심분야〉 정보보호, 네트워크 보안, 스마트카드 보안