Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.2, Apr. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.2.285

오류주입공격 실험 정밀도 분석 및 개선지표*

김 현 호,[1†] 강 영 진,[1] 이 영 실,[1] 박 제 훈,[2] 김 창 균,[2] 이 훈 재[1‡]
[1]동서대학교, [2]한국전자통신연구원 부설연구소

The Study on Fault Injection Attack: The analysis and improvement of the experimental precision indicators*

HyunHo Kim,[1†] Young-Jin Kang,[1] Young-Sil Lee,[1] Jae-Hoon Park,[2]
Chang-Kyun Kim,[2] HoonJae Lee[1‡]
[1]Dongseo University, [2]Electronics and Telecommunications Research Institute

요 약

스마트기기 활용도가 높아지면서 스마트기기의 다양한 애플리케이션들이 개발되고 있다. 이 애플리케이션들은 디지털 포렌식 조사 관점에서 사용자의 행동과 관련된 중요한 데이터가 존재할 수 있기 때문에 애플리케이션에 대해 사전 분석이 진행되어야 한다. 하지만 애플리케이션들이 업데이트되면서 분석된 데이터 포맷이 변경되거나 새로운 형태로 생성되는 경우가 빈번히 발생하고 있다. 그래서 사전 분석된 모든 애플리케이션에 대하여 업데이트가 진행되었는지 일일이 확인하여야하고, 업데이트가 진행되었다면 변경된 데이터가 있는지에 대해서도 분석이 꼭 필요하다. 하지만 분석된 데이터를 지속적으로 반복 확인하는 작업은 많은 시간이 소요되므로 이를 효율적으로 대응할 수 있는 방법이 필요하다.

본 논문에서는 애플리케이션의 정보를 수집하여 업데이트 정보를 확인하고, 변경된 데이터에 대한 정보를 효율적으로 확인할 수 있는 자동화된 시스템을 제안한다.

ABSTRACT

As the utilization rate of smart device increases, various applications for smart device have been developed. Since these applications can contain important data related to user behaviors in digital forensic perspective, the analysis of them should be conducted in advance. However, lots of applications get to have new data format or type when they are updated. Therefore, whether the applications are updated or not should be checked one by one, and if they are, whether their data are changed should be also analyzed. But observing application data repeatedly is a time-consuming task, and that is why the effective method for dealing with this problem is needed.

This paper suggests the automatic system which gets updated information and checks changed data by collecting application information.

Keywords: Digital Forensics, Smartphone Forensics, Android Forensics, Android Application, Android Data Acquisition

I. 서 론

부 채널 공격(SCA: Side Channel Attack)은 암호 알고리즘의 연산 시 누출 되는 전력, 전자파 신호, 타이밍 정보 등을 이용하는 공격이다. 부 채널 공

접수일(2013년 12월 31일), 수정일(2014년 3월 4일), 게재확정일(2014년 3월 4일)
* 본 연구는 2013년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(과제번호: 2013-071188). 또한 부산광역시에서 지원하는 BB21과제에서 지원받았음.
† 주저자, feei_@naver.com
‡ 교신저자, hjlee@dongseo.ac.kr(Corresponding author)

격 중에서도 오류주입공격(FA: Fault-Injection Attack)은 1996년 Bellcore사에 의해 RSA 암호 방식에 대한 공격방법으로 처음 소개되었다[2]. 오류주입 공격은 암호 연산을 위한 칩이나 메모리 등 하드웨어에 인위적으로 오류를 주입함으로써 예상치 못한 결함을 유발시켜 발생된 잘못된 출력 값을 분석함으로써 내부의 비밀 정보를 알아내는 공격 방법이다. 이러한 오류는 인증기관의 서버와 같은 중량급의 장치뿐만 아니라 소형 정보보호 하드웨어 장치에서도 발생할 수 있다.

아래 그림 1은 캠브리지 대학의 연구[3]에 따라 암호 공격의 분류를 나눈 것이며, 하드웨어에 관련된 암호 공격은 공격 형태에 따라 침투형·준침투형·비침투형으로 나눌 수 있다.

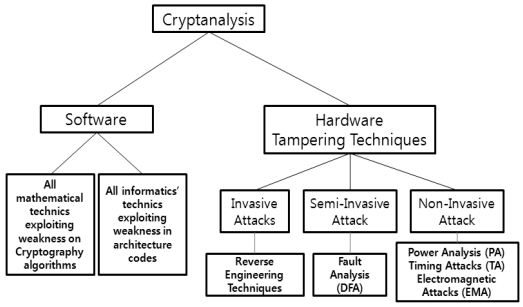


Fig. 1. Classification of cryptographic attacks

비침투형 공격은 암호 장치나 암호 칩에 대하여 물리적인 침해 없이 오류를 주입하는 유형으로 비정상 온도 오류, 클럭 글리치, 전압 글리치, 저전압 인가 오류 등이 있다. 준침투형 공격은 하드웨어를 (또는 장치를) 디캡핑한 상태에서 동작시키며, 암호 장치나 암호 칩에 대하여 광원이나 전자기파 오류를 주입하는 유형이다. 침투형 공격은 디캡핑된 장치 내부의 칩 표면의 보호막층(passivation layer)을 제거한 후 마이크로 프로빙을 통해서 직접적으로 회로를 관측하여 조작하는 공격으로, 칩 내부 깊은 곳의 금속 층까지도 방사되는 이온 빔 장치 등과 같은 고가의 장비를 필요로 한다.

오류주입공격은 부 채널 공격 중 가장 최근에 알려진 공격기술이며, 국내에서는 2000년 초반부터 소수의 전문가들에 의해서 연구가 진행 되고 있으나, 실험환경의 제약(실험 장비의 부족, 전문 인력의 부족 등)의 이유로 극히 제한적인 연구가 이루어지고 있는 실정이다.

이에 본 논문의 목표는 다음과 같다.

1) 사례연구를 통한 실험환경을 비교·분석

2) 오류주입공격 실험을 위한 개선지표 제시

이를 위해 먼저, 기존 오류주입공격의 동향을 분석하고, 다양한 사례연구를 통한 실험환경을 비교·분석한다. 또한, 분석한 내용을 토대로 향후 오류주입공격 실험 환경 구성을 위한 개선 지표를 제시할 것이다.

II. 오류주입공격 동향

본 장에서는 오류주입공격기술의 동향을 살펴보기 위하여 비침투형·준침투형·침투형 공격 분류에 따른 다양한 오류주입공격 실험 사례들을 분석한다.

2.1 비침투형 오류주입공격

비침투형 오류주입공격 유형으로는 비정상 온도 오류, 클럭 글리치, 전압 글리치, 저전압 인가 오류가 있다. S. Skorobogatov[4]는 비정상 온도 오류를 유발시키기 위해 RAM의 온도를 -20℃ 근처에서 동작상태를 확인한 결과 데이터가 1분간 유지된다는 결과를 보였다. H. Bar-EL 등 [5]은 RAM을 가열하여 셀의 임의적인 변경을 유도하는 실험을 하였으며, 그 결과 반도체 결함유도 및 오류를 발생시켜 이를 악의적으로 사용할 수 있음을 증명하였다. Blömer 등 [6]의 연구에서 스마트카드를 대상으로 낮은 클럭을 사용하여 내부 상태를 확인한 결과 CPU의 실행 동작을 변경할 수 있음을 확인한 사례가 있다. 전압 글리치를 이용한 오류 주입 공격의 사례로 C. Aumüller 등 [7]은 스마트카드를 대상으로 전압 스파이크를 사용해 오류를 주입하여 스마트카드 침입 및 미묘한 계산오류를 발생할 수 있는 실험을 하였다. 또한 A. Barenghi 등 [8]은 저전압 인가 오류 실험을 위해 ARM 범용 CPU를 대상으로 전원 칩의 종류에 따라 수행되는 명령어의 OPCODE가 변형하여 비정상적인 명령어가 동작되는 실험을 한 사례가 있다.

2.2 준침투형 오류주입공격

준침투형 오류주입공격은 디캡핑된 상태에서 작동하는 암호 장치 또는 암호 칩에 대해 광(레이저)오류, 자외선(UV)오류, 외부 전자장/와전류 오류, X-선 마이크로파 오류를 주입하는 공격방법 등이 있다. 광(레이저)오류와 자외선(UV) 오류에서는

Skorobogatov와 Anderson[9]이 SRAM을 대상으로 섬광 전구(Photoflash)를 망원경을 통해 증폭해 강한 광원을 만들어 SRAM에 공격하여 SRAM의 셀 특정 영역의 비트 값을 변경한 사례가 있다. 또한 EEPROM이나 플래시 메모리를 대상으로 자외선을 조사하여 게이트 내부에 존재하는 전하의 집속도를 떨어뜨려 메모리 셀을 방전시키는 형태의 오류를 실험한 사례가 있다. 외부 전자장/와전류 오류에는 O. Kocar[10]이 트랜지스터를 대상으로 와전류를 이용해 내부의 산화 그리드의 상당수의 전자를 변형한 사례가 있다. X-Y선에는 S. Govindavajhala, A. Appel[11]이 메모리 오류는 NET 가상머신 또는 자바에서 심각한 보안 취약점이 생긴다고 말했으며, 이들은 고에너지의 X-선을 사용하여 메모리 비트 값을 바꾸는 실험을 한 사례가 있다.

2.3 침투형 오류주입공격

침투형 오류주입공격의 유형으로는 이온 오류, 능동 프로브, 집속 이온빔(FIB) 오류가 있다. 이온 오류 분야에는 O.Kömmerling 등 [12]이 스마트카드를 대상으로 레이저 절단과 이온 빔을 사용하여 오류를 주입하여 공격하는 사례가 있다. 능동 프로브 분야에는 S. H. Weingart[13]가 활성화된 시스템에 신호 및 정보를 삽입하는 사례가 있다. Trichina 등[26]은 SRAM을 대상으로 YAG 레이저 시스템을 사용하여 오류를 주입하고, LeCroy 오실로스코프를 통해서 SRAM의 변화를 관측한 결과 연산오류가 가능한 오류주입 지점을 찾아내는 사례가 있다.

III. 오류주입공격 실험환경 비교 분석

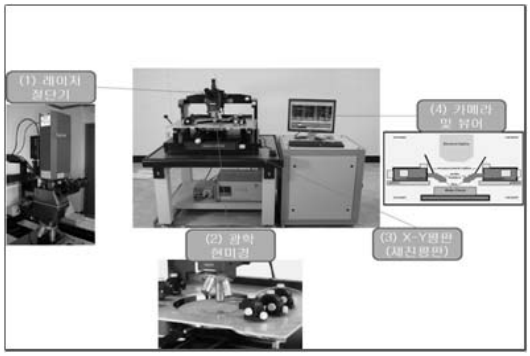


Fig. 2. A Proposed generalization model for FA tools

지금까지 공격된 다양한 사례를 종합하여 그림 2는 오류주입장치의 일반화된 모델로서 그림 2와 같이 제안한다. 일반화된 모델은 레이저를 이용한 절단/공격 부분과, 대상 칩의 공격부분에 대한 확대/축소를 위한 전자현미경, 대상 칩의 정확한 공격 위치를 x-y-z축으로 맞추기 위한 X-Y평판 그리고 공격 대상을 카메라와 뷰어로 확인하는 부분으로 구성되어 있다.

Table 1.은 실험 환경을 비교하기 위한 매개변수들의 정의와 이를 선정한 이유를 나타내고 있으며, Table 2.는 앞서 정의한 매개변수들을 기준으로 최근 오류주입공격 연구 시 구성한 실험 환경을 보여준다.

Table 1. Comparison parameters

Parameters	Description
공격 대상 소자	오류주입공격 실험을 위해 어떤 칩(Smartcard, Atmega128, SRAM, 등)을 대상으로 선정 하였는가를 나타낸다.
공격 대상 및 암호 알고리즘	공격대상은 암호 알고리즘(AES, DES, ARIA 등)과 대상 소자 칩의 EEPROM, Flash memory등으로 나눌 수 있다.
공격 대상 함수	일반적으로 암호 알고리즘의 대표적인 함수는 S-BOX, XOR, AddRoundKey 등을 들 수 있으며, 암호 칩에 오류주입공격을 실험하기 위해 어느 부분을 대상으로 공격 하였는가를 나타낸다.
공간 정밀도	얼마만큼의 레이저 면적으로 공격 가능한지를 나타낸다.
시간 정밀도	얼마만큼의 레이저 지연시간으로 공격 가능한지를 나타낸다.
에너지	오류를 주입한 에너지양을 의미한다.
레이저 원/파장	레이저 원(Laser source)은 레이저의 매질(고체, 액체, 기체, 등)을 의미하고, 레이저를 발생하는 매질에 따라 고유 파장을 가진다. 그리고 오류를 주입하기 위해 사용한 레이저 장비의 레이저 원, 파장 등의 상세 정보를 나타낸다.
X-Y 평판	오류주입공격을 ㎛단위로 정밀하게 X축과 Y축을 움직이기 위한 평판을 의미하며, 오류를 주입할 때 정밀하게 움직이기 위해 X-Y 평판을 사용하였는가를 나타낸다.
관찰 기기	CCD카메라, 광학현미경, 오실로스코프 등이 있으며, 오류주입공격을 위한 관찰 기기로 사용된다.

Table. 2를 분석해보면 CPU나 메모리의 오작동 유도를 목적으로 한 오류주입공격과 암호칩에 내장된 암호의 비밀키를 알아내기 위한 목적으로 나눠 볼 수 있다.

먼저 CPU나 메모리의 오작동을 유도할 목적으로 오류주입공격을 시도했던 사례는 (2), (3), (6), (7)이 있다. 사례 (2)는 오류 마스킹 공격 기법에 대해 소개하였으며, PIC 마이크로컨트롤러 내부 EEPROM과 플래시 메모리를 대상으로 메모리 내용 변경을 방지하는 것을 목표로 연구가 진행 되었다. 사용된 실험장비 환경은 테스트보드 구성과 CCD카메라 장착, XYZ스테이지, 광학현미경, 650nm 파장을 가진 레이저와 25mW 전력을 사용하였다. 사례 (3)은 메모리 실행을 방해하기 위한 오류 주입 공격에 초점을 맞추었으며 실험 구성은 공간정밀도 3㎛ x 2㎛, 시간정밀도 2 hours 30 minutes (read the memory every 5 minute), 약 4000uW/cm2의 표준 자외선 소거기와 피시험 장치(DUT)로 16KB의 EEPROM, 0.35㎛ 기술로 제조된 간단한 APDU 명령(메모리 프로그램, 읽기, 삭제 등)의 해석이 가능한 기본 OS를 가진 스마트카드 칩을 사용 하였다. 사례 (6)은 레이저를 이용하여 EEPROM과 플래시 메모리 장치에 내용을 수정하는 공격 방법을 보여준다. 그 결과 메모리셀을 파장 650㎚와 전력 50㎽으로 약 300초 동안 가열하면 1bit의 메모리가 지워지는 것을 확인할 수 있고, 파장650㎚와 전력 100㎽를 사용했을 때는 약170초 시점에 1bit메모리가 지워지는 것을 증명하였다. 그리고 사례 (2)와 같이 이미징을 위해서 CCD카메라를 장착하여 사용했다. 사례 (7)은 40㎛와 8㎛의 레이저 스팟 사이즈를 이용하여 레이저 직경에 대한 영향을 설명한다. 그리고 오류를 분석하기 위해 개발된 CAD tool을 이용한다.

위 사례와 달리 비밀키를 알아내기 위한 목적의 오류주입공격 실험 사례는 (1), (4), (5), (8), (9), (10), (11), (12) 가 있다. 사례 (1)은 의료 장비, PC 주변 장치, 산업 장비, 알람 장치 등에 주로 사용되는 32비트 ARM Cortex M3 core의 CPU 기반인 마이크로컨트롤러에 CRT 방식의 RSA 암호 알고리즘을 적용하여 구현한 이중 오류 공격을 수행하였다.

사례 (4)의 첫 번째 실험은 오직 CPU만 해당되며 1MHz의 외부 클록으로 이중 PIN 인증을 수행한다. 실험의 목표는 PIN 인증의 수행을 강제로 건너뛰도록(생략)하며, 칩의 뒷면에 오류를 주입하였고 칩의 중요한 위치 및 공격을 위한 정확한 타이밍을 찾기 위한 시도를 하였다. 실험을 위해 사용한 레이저 사양과 장비는 파장 808㎚, 전력 14W와 파장1064㎚, 전력 20W, 펄스 주파수 25㎒, 트리거 지연 50ns, X-Y스테이지, 2ns 시간 정밀도를 갖는 FPGA-기반 목표물 조정 & 트리거, FPGA-기반 실시간 패턴 매칭 기술, 오실로 스코프, 동작 소프트웨어(Inspector)이다.

사례 (5)는 비동기 방식의 DES에 적용된 오류주입 방어대책에 대한 실질적인 평가를 제안하였으며, 두 개의 DES 암호화 프로세서는 특정 기술을 사용하여 강화된 130nm STMicroelectronics CMOS 프로세서를 사용하여 제작되었다. 또한 증명을 위해 오류를 주입하여 두 회로의 저항을 비교하고 제안된 방어법의 유효성을 검사하였다.

사례 (8)은 AES 암호 연산을 수행하는 동안 라운드 함수를 반복적으로 사용하는 경우, 반복하는 구문에 오류를 넣어 한 라운드를 생략하면 쉽게 비밀 키를 추출할 수 있음을 확인하였다. 그리고 라운드의 시간 측정을 위해 오실로스코프 장비를 사용하였으며, 칩은 디캡핑(decapping)하였다.

사례 (9)는 Miller 알고리즘의 루프 횟수를 판별하는 분기 구문에 오류를 주입하여 원하는 루프 시점에서 연산을 단번에 종료 시키는 방법으로 검증하였다. 실험결과 확인을 위해 오실로스코프를 이용하여 파형을 관찰하였다.

사례 (10)은 Triple DES에서 수행되는 각각의 DES 알고리즘 중 마지막 라운드를 실행시키지 않도록 오류를 주입함으로써 비밀 키를 찾아내는 차분 오류 분석 공격을 제안 하였다. 제안한 공격 방법을 이용하여 시뮬레이션 결과, 9개 정도의 정상-오류 암호문 쌍을 얻을 수 있으며 224번의 비밀 키 전탐색을 통해 3개의 비밀 키를 모두 찾을 수 있었다. 실험결과 측정을 위해 고성능 오실로스코프를 사용하였다. 사례 (11)은 AES암호를 수행하는 동안 마지막 라운드의 키를 더하는 반복문(for statement)에 대한 오류 주입을 통해 비밀키 전체를 공격 할 수 있음을 확인하였다. 실험결과 확인을 위해 고성능 오실로스코프를 사용하였다.

사례 (12) 에서는 마스터 비밀키를 알아내기 위해 차분 오류 분석(DFA)공격을 이용하여 라운드 키를 복구하는 방법을 제안한다. 시뮬레이션 한 결과에 따르면 잘못된 33 암호문과 마스터 비밀 키를 검색 할 수 있었다. 실험결과를 측정하기 위해 오실로스코프를 이용하였다.

Table 2. Comparison of Fault Analysis Attacks

사례	공격 대상 소자	공격 대상 및 암호 알고리즘	공격 대상 함수	공간 정밀도	시간 정밀도	에너지
	레이저 원/ 파장		X-Y 평판		관찰 기기	
1[14]	32-bit ARM Cortex M3 core	CRT-RSA (512, 1024, 2048)	Modulus computation Mp or Mq	1~2 μm²	58 ms	Minimum energy
	YAG laser, 532nm green and 1064 nm infrared		1㎛		LeCroy oscilloscope	
2[15]	PIC16F84 fabricated with 1.2㎛	EEPROM and Flash memory	N/A	1㎛ spot size		25㎽
	PIC16F628 fabricated with 0.9㎛			1㎛ spot size		25㎽
	PIC16F628A built with 0.5㎛			10㎛		10㎽
				10㎛		25㎽
	MSP430 microcontroller-MSP430F112 built with 0.35㎛					Full laser power of 75㎽
	650㎚ (Class 1 laser, <1 mW)		Motorized XYZ-stage		20X objective (N.A=0.40) CCD cameras	
	650㎚ (Class 1 laser, <1 mW)					
	1065㎚					
3[16]	Smart card chip in 0.35㎛ with 16KB of embedded EEPROM(cell size is around 1.6㎛2)	EEPROM	N/A	3㎛ x 2㎛	2 hours 30 minutes (read the memory every 5 minute)	4000 ㎼cm-2
	UV radiation (lamp)				X500	
4[17]	Front side of the chip	DES	N/A	60 X 1.4㎛	Starting at time t=600㎲, k=72㎲	14W
	Back side of the chip					20W
	Jitter-free diode laser				5X ~ 50X objective	
	808㎚, 1064㎚ with 25㎒					
5[18]	Asynchronous DES coprocessor	DES	S-Box & XOR	220 μm²	200 ns for 16 round	0.8 pJ/μm²
	Gemalto Laser					

사례	공격 대상 소자	공격 대상 및 암호 알고리즘	공격 대상 함수	공간 정밀도	시간 정밀도	에너지
	레이저 원/ 파장		X-Y 평판		관찰 기기	
6[19]	PIC16F628	EEPROM, Flash memory devices				50㎽ - no more than 100㎽ (damaged)
	650㎚		0.1㎛ accuracy using the motorized stages		100X objective lens	
7[20]	FPGA-Xilinx Virtex-II XC2V1000	720Kbit block RAMs		30㎛		Few watts and several spot sizes
	900㎚		40㎛, 8㎛ diameters			
8[21]	ATmega 128 microcontroller	AES	1~8 round, 10round	반복문 (for statement)		
	EzLaze3 laser, 535㎚					
9[22]	ATmega 128 microcontroller	Miller	루프 연산 횟수를 변형하여 순환 구문의 연산 횟수 변형			
	EzLaze3 laser, 532㎚				LeCroy LT374M Oscilloscopes	
10[23]	ATmega 128 microcontroller	Triple DES	16round F function	반복문 (for statement)	10㎳ for 15round	35㎷
	EzLaze3 laser, 532㎚				LeCroy LT374M Oscilloscope, Optical Microscope	
11[24]	ATmega 128 microcontroller	AES	AddRoundKey		5.6㎲	
	EzLaze3 laser, 532㎚				High-performance Oscilloscope, Optical Microscope	
12[25]	ATmega 128 microcontroller	ARIA	Round key addition	0.78㎳~0.80㎳		
			Substitution layer	0.80㎳~0.82㎳		
			Diffusion layer	0.82㎳~0.84㎳		
	EzLaze3 laser, 532㎚, injection tool shoot after about 200㎲ delay					

IV. 고찰

본 장에서는 III장에서 사례를 분석한 내용으로 현재 상용화되어 많이 사용되는 기준으로 볼 때 오류주입 목적별로 매개변수를 Table 3과 같이 정리하였다.

Table 3. Optimized table of best parameters in FA Tools

	CPU, 메모리 오작동 유도를 목적으로 한 오류주입공격	알고리즘의 비밀키를 알아내기 위한 목적의 오류주입공격
공격 대상 소자	PIC 칩 시리즈	ATmega128
공격대상 및 암호 알고리즘	EEPROM	AES
공격 대상 함수	N.A	AddRoundKey
레이저 원/파장	650㎚ (Class 1 laser, 〈1 mW)	EzLaze3 laser/ 532㎚
공간 정밀도	1㎛ spot size	반복문(for statement)
시간 정밀도	N.A	5.6㎲
에너지	25㎽	N.A

CPU, 메모리 오작동을 유도한 목적의 오류주입에서 사용된 매개변수 중 대상 칩의 종류는 PIC16F84, PIC16F628, PIC16F628A, MSP430, MSP430F112, Smart card chip이 있다. 이 칩들은 EEPROM이 내장되어 있으며, 이 중 PIC16F84와 PIC16F628칩은 SRAM, EEPROM, 데이터 메모리, 플래시 프로그램 메모리가 포함되어 있는 것이 특징이다. 그리고 사용된 파장 650㎚ (Class 1 laser, 〈1 mW)와 25㎽의 에너지를 선택한 이유는 가능한 최대의 전력과 파장을 갖는 저가의 레이저 다이오드 모듈을 장착하기 위해서 이며, 레이저가 눈에 위험하지 않게 직접 관찰할 수 있는 가장 안전한 방법이기 때문이다. 마지막으로 1㎛ spot size에 초점을 맞추기 위해 마이크로스코프는 저해상도 20×objective를 사용하였다.

알고리즘의 비밀키를 알아내기 위한 목적 오류주입에서 대상 암호칩으로 ATmega128을 선택한 이유는 센서 네트워크 시스템에 많이 사용되어 지고 있기 때문이다. 대상 알고리즘은 국제표준인 AES 알고리즘을 선택하였으며, 차분 오류 분석(Differential Fault Analysis, DFA)에 대한 연구가 많이 있으며, 그 결과 비밀키를 알아내기 위한 방법이 많이 제안 되었다. 본 논문에서 조사한 사례들을 봤을 때 레이저장비는 EzLase3, 파장은 532㎚를 가장 많이 사용해서 연구되었으며, 또한 "for"문과 같이 반복적인 연산을 하는 과정에 오류를 주입하여 키를 찾는 방법과 암호 알고리즘의 일부 라운드를 수행하지 않도록 공격하는 라운드 축소와 같은 공격방법 등이 연구되었다.

V. 결론

현재 오류주입공격은 연구가 시작된 지 얼마 되지 않았기에 이에 따른 전문가가 부족한 실정이며, 또한 비용적인 측면에서도 실험장비가 고비용에 속하기 때문에 연구를 위한 환경을 만들기가 쉽지 않다.

본 논문은 오류주입공격에 관한 정의 및 분류 등 전반적인 내용을 소개하였고, 오류주입공격의 최근연구동향을 분석하였으며, 공격 장치에 대한 일반화된 모델을 제안하였다. 실험사례에서 사용했던 실험요소를 크게 실험을 위한 공격 대상 소자, 공격대상 및 암호 알고리즘, 공격 대상 함수, 공간 정밀도, 시간 정밀도, 에너지, 레이저 원, 파장, X-Y평판, 관찰기기로 분류 하였으며, 이를 통해 오류주입공격 대상에 따른 실험환경 및 공격방법과 동일한 칩을 공격한 실험에서도 실험 목적에 따라 레이저 에너지 및 정밀도 등의 변화에 따른 다양한 실험 결과를 비교 분석하였다.

앞으로도 본 논문을 활용해서 오류주입공격 연구자들이 기존에 연구된 실험사례에서 사용했던 실험환경과 조건을 활용하여 연구발전에 필요한 정보가 될 것으로 사료된다.

향후 본 논문의 결과를 활용하여 오류주입공격 실험을 위한 효율적인 실험환경을 구성하기 위해서 최적의 매개변수를 도출하며, 실험을 통해 이를 증명할 예정이다.

References

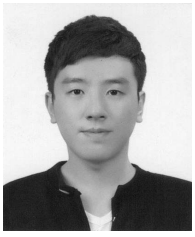
〔1〕 Young-Sil Lee, HyunHo Kim and HoonJae Lee, "A study on generalization of Fault-Injection Analysis tools", Dongseo University Industry-Academic Cooperation

Foundation, pp. 1-205, Otc. 2013.
〔2〕 D. Bonech, R. DeMillo and R. Lipton, "New threat model breaks crypto codes," Bellcore Press Release, Sep. 1996.
〔3〕 Sergei P. Skorobogatov, "Semi-invasive attacks: A new approach to hardware security analysis," Technical Report UCAM-CL-TR-630, University of Cambridge, Apl. 2005.
〔4〕 Sergei Skorobogatov, "Low temperature data remanence in static RAM," Technical Report UCAM-CL-TR-536, University of Cambridge, Jun. 2002.
〔5〕 H. Bar-El, H. Choukri, and C. Whelan, "The Sorcerer's Apprentice Guide to Fault Attacks," Proceedings of the IEEE, vol. 94, no. 2, pp. 371-382, Feb. 2006.
〔6〕 Johannes Blömer and Jean-Pierre Seifert, "Fault based cryptanalysis of the Advanced Encryption Standard (AES)," Financial Cryptography, pp. 162-181, 2003.
〔7〕 C. Aumüller, P. Bier, and J. P. Seifert, "Fault attacks on RSA with CRT: Concrete results and practical countermeasures," Workshop on Cryptographic Hardware and Embedded Systems, LNCS 2523, pp. 260-275, 2002.
〔8〕 A. Barenghi, G. Bertoni, and G. Pelosi, "Low Voltage Fault Attacks on the RSA cryptosystem," Workshop on Fault Diagnosis and Tolerance in Cryptography, pp.23-31, 2009.
〔9〕 Sergei P. Skorobogatov and Ross J. Anderson, "Optical Fault Induction Attacks," Workshop on Fault Diagnosis and Tolerance in Cryptography, LNCS 2523, pp. 2-12, 2003.
〔10〕 O. Kocar, "Hardwaresicherheit von Mikrochips in Chipkarten," Datenschutz and Datensicherheit, vol. 20, no. 7, pp. 421-424, 1996.
〔11〕 S. Govindavajhala and A. Appel, "Using memory errors to attack a virtual machine," In Proceedings of the IEEE symposium on Security and Privacy, pp. 154-164, May. 2003.
〔12〕 Oliver Kömmerling and Markus G. Kuhn, "Design principles for tamper-resistan smartcard processors," Proceedings of the USENIX Workshop on Smartcard Technology, pp.9-20, May. 1999.
〔13〕 S. H. Weingart, "Physical Security Devices for Computer Subsystems: A Survey of Attacks and Defenses," Workshop on Cryptographic Hardware and Embedded Systems, LNCS 1965, pp. 302-317, 2000.
〔14〕 Elena Trichina and Roman Korkikyan, "Multi Fault Laser Attacks on Protected CRT-RSA," Workshop on Fault diagnosis and Tolerance in Cryptography, pp. 75-86, Aug. 2010
〔15〕 Sergei Skorobogatov, "Optical Fault masking Attacks," Workshop on Fault diagnosis and Tolerance in Cryptography, pp. 23-29, Aug, 2010
〔16〕 Jacques J.A. Fournier and Philippe Loubet-Moundi, "Memory address Scrambling Revealed using Fault Attacks," Workshop on Fault diagnosis and Tolerance in Cryptography, pp. 30-36, Aug. 2010
〔17〕 J. G. J. van Woudenberg, M. F. Witteman and Federico Menarini, "Practical Optical Fault Injection on Secure Microcontrollers," Workshop on Fault Diagnosis and Tolerance in Cryptography, pp. 91-99, 2011
〔18〕 Y. Monnet, M. Renaudin, and F. M'Buwa Nzengust "Practical Evaluation of Fault Countermeasures on an Asynchronous DES Crypto Processor," Proceedings of the 12th IEEE International On-Line Testing Symposium, 2006
〔19〕 Sergei Skorobogatov, "Local Heating Attacks on Flash Memory Devices," International Workshop on

Hardware-Oriented Security and Trust, 2009
〔20〕 G. Canivet, J. Clediere, and R. Leveugle, "Detailed Analysises of Single laser Shot Effects in the Configuration of a Virtex-II FPGA," International On-Line Testing Symposium, pp. 289-294, 2008
〔21〕 Doo-sik Choi, Yong-Je Choi, and Jae-cheol Ha, "A Late-Round Reduction Attack on the AES Encryption Algorithm Using Fault Injection," Journal of The Korea Institute of information Security & Cryptology, 22(3), pp. 339-445, Jun. 2012
〔22〕 KiSeok Bae, JeaHoon Park, and SangJae Moon, "Efficient Fault Injection Attack to the Miller Algorithm in the Pairing Computation using Affine Coordinate System," Journal of The Korea Institute of information Security & Cryptology, 21(3), pp. 11-25, Jun. 2011
〔23〕 Doo-sik Choi, Doo-hwan Oh, and Jae-cheol Ha "A Round Reduction Attack on Triple DES Using Fault Injection", Journal of The Korea Institute of information Security & Cryptology, 21(2), pp. 91-100, Apl. 2011
〔24〕 JeaHoon Park, KiSeok Bae, and JaeCheol Ha, "A Fault Injection Attack on the For Statement in AES Implementation," Journal of The Korea Institute of information Security & Cryptology, 20(6), pp. 59-65, Dec. 2010
〔25〕 JeaHoon Park and JaeCheol Ha, "Improved Differential Fault Analysis on Block Cipher ARIA," International Workshop on Information Security Applications, LNCS 7690, pp. 82-95, 2012
〔26〕 E.Trichina. R. Korkikyan, "Multi Fault Laser Attacks on Protected CRT-RSA," Workshop on Fault diagnosis and Tolerance in Cryptography, pp. 75-86, 2010

〈저자소개〉

김 현 호 (HyunHo Kim) 정회원
2013년 2월: 동서대학교 정보통신공학과 졸업
2013년 2월: 동서대학교 일반대학원 유비쿼터스IT학과 석사과정
〈관심분야〉 부채널공격, 시스템보안, 디지털포렌식, 네트워크 보안



강 영 진 (Young-Jin Kang) 정회원
2013년 8월: 동서대학교 정보통신공학과 졸업
2013년 8월: 동서대학교 일반대학원 유비쿼터스IT학과 석사과정
〈관심분야〉 부채널공격, 네트워크 보안

이 영 실 (Young-Sil Lee) 정회원
2006년 2월: 동서대학교 정보네트워크학과 졸업
2010년 8월: 동서대학교 디자인&IT전문대학원 유비쿼터스IT학과 석사 졸업
2011년 3월 ~ 현재: 동서대학교 일반대학원 유비쿼터스ITgkr과 박사과정
2012년 1월 ~ 현재: University of Oulu, Dept. of Electrical Engineering, 박사과정
〈관심분야〉 부채널분석, 암호 알고리즘, 헬스케어 시스템 보안, 센서 네트워크 보안

박 제 훈 (Jae-Hoon Park) 정회원
2004년 2월: 경북대학교 전자·전기공학부 졸업
2006년 2월: 경북대학교 전자공학과 석사 졸업
2011년 2월: 경북대학교 전자공학과 박사 졸업
2011년 1월 ~ 2012년 1월: 국방기술품질원 선임연구원
2012년 2월 ~ 현재: 한국전자통신연구원 부설연구소
〈관심분야〉 부채널분석, 정보보호시스템 안전성 분석

김 창 균 (Chang-Kyun Kim) 정회원
2001년 2월: 경북대학교 전자·전기공학부 졸업
2003년 2월: 경북대학교 전자공학과 석사 졸업
2009년 8월: 경북대학교 전자공학과 박사 졸업
2004년 11월 ~ 현재: 한국전자통신연구원 부설연구소
〈관심분야〉 부채널분석, 임베디드시스템 보안, 암호알고리즘구현

이 훈 재 (HoonJae Lee) 정회원
1987년: 경북대학교 전자공학과 석사 졸업
1998년: 경북대학교 전자공학과 박사 졸업
1987년 ~ 1998년 국방과학연구소 선임연구원/ 팀장
1998년 ~ 2002년 경운대학교 조교수
2002년 ~ 현재: 동서대학교 컴퓨터정보공학부 교수
〈관심분야〉 암호이론, 네트워크보안, 부채널공격, 정보통신/정보네트워크