Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.1, Feb. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.1.229

KLA-SCARF 부채널 검증 보드 구현*

최 용 제,[1†] 최 두 호,[1] 류 재 철[2‡]
[1]한국전자통신연구원, [2]충남대학교

Implementing Side Channel Analysis Evaluation Boards of KLA-SCARF system*

YongJe Choi,[1†] DooHo Choi,[1] JeaCheol Ryou[2‡]
[1]Electronics and Telecommunications Research Institute, [2]ChungNam University

요 약

암호 알고리즘에 대한 부채널 검증 필요성 증가로 인하여 이를 수행할 수 있는 부채널 검증 시스템이 여러 국내외 연구소에서 개발되고 있으며, 보안 제품의 인증 평가 수단을 목적으로 한 상용 제품도 판매되고 있다. 하지만, 스마트 카드와 같은 특정 보안 디바이스가 아닌 경우, 다양한 구동 환경으로 인하여 보안 디바이스에 대한 부채널 검증 보드 구현에 어려움이 있다. 본 논문에서는 국내 부채널 분석 시스템 개발을 목표로 진행된 KLA-SCARF 프로젝트의 부채널 검증 보드들의 구현과 특징에 대하여 기술하고자 한다. 이는 다양한 보안 디바이스 환경에서 부채널 분석 장비를 개발하고자 하는 연구자에게 방향을 제시할 수 있으리라 본다.

ABSTRACT

With increasing demands for security evaluation of side-channel resistance for crypto algorithm implementations, many equipments are developed at various research institutes. Indeed, commercial products came out for the purpose of evaluation and certification tool of security products. However, various types of security products exclusive a smart card make it difficult to implement a security evaluation system for them. In this paper, we describe implementation and characteristic of the side-channel evaluation boards of the KLA-SCARF, which is the project to develop domestic side-channel evaluation system. This report would be helpful for following researchers who intend to develop side-channel evaluation boards for other security devices.

Keywords: Side Channel Analysis, KLA-SCARF, Security Evaluation Board

I. 서 론

수학적으로 안전한 암호 알고리즘이라도 암호화 과정에서 발생하는 전력/전자파 신호 등의 부채널 정보에 의해 암호키가 분석될 수 있음이 Paul Kocher[1]에 의해 발표된 이후로 부채널(side channel) 분석 기법은 가장 강력한 암호 시스템 공격 기법으로 인정받고 있다. 특히 스마트 카드와 같은 보안 디바이스는 부채널 분석에 대한 안전성 검증이 필수 항목으로 되었으며, 이는 점차 암호모듈을 탑재

접수일(2013년 12월 26일), 수정일(2014년 2월 3일), 게재확정일(2014년 2월 3일)
* 본 연구는 ETRI의 연구개발 과제인 KLA-SCARF(프로젝트로 수행하였음(암호키 누출 검증 및 방지 원천 기술 연구), www.k-scarf.or.kr, KLA-SCARF(Key Leakage Analysis - Side Channel Analysis Resistant Framework)
† 주저자, choiyj@etri.re.kr
‡ 교신저자, jcryou@home.cnu.ac.kr (Corresponding author)

하는 모든 보안 디바이스로 확대될 것으로 보인다.

부채널 평가 장비로는 CRI사의 DPA workstation[2], Riscure사의 Inspector[3], Bright-Sight사의 Sideways[4] 등이 상용 제품으로 사용되고 있다. 이들 장비들은 파형 수집부터 분석까지 모두 수행할 수 있지만, 대부분 스마트 카드의 부채널 분석을 목적으로 하고 있다.

일본의 SASEBO 프로젝트[5]에서는 보안 하드웨어 모듈을 FPGA를 이용하여 부채널 검증을 수행할 수 있도록 하는 SASEBO 시리즈의 보드를 개발·배포하였다. SASEBO 보드는 보드 사용을 위한 인터페이스만 제공하며, 수집과 분석을 위해 별도의 프로그램 구현이 필요하다.

국내에서는 KLA-SCARF 프로젝트를 통하여 스마트 카드 뿐만 아니라 다양한 보안 디바이스에 적용 가능한 부채널 분석 시스템 개발을 목표로 부채널 분석용 보드 및 분석 시스템 개발이 진행 중에 있다.

본 논문에서는 이러한 KLA-SCARF에서 개발된 부채널 분석 보드 구현과 특징 등에 대하여 기술하고자 하며, 이를 통하여 부채널 분석 장비 개발의 방향을 제시하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 부채널 분석 기술 및 보안성 분석 시스템에 대하여 살펴본다. 3장에서 KLA-SCARF 시스템용 부채널 검증 보드 구현에 대하여 기술하고, 4장에서는 이들 보드의 기능 및 성능에 대하여 언급하며, 5장에서 결론을 맺는다.

II. 부채널 분석 기술 및 시스템

본 장에서는 부채널 분석/측정 기술과 대표적인 분석 시스템에 대하여 살펴본다.

2.1 부채널 분석 및 측정

암호 알고리즘의 연산 과정에서 누설되는 타이밍 정보, 전력소모, 전자파 신호등을 이용하여 암호키와 같은 중요 데이터를 찾아내는 부채널 분석 기술은 암호 알고리즘 안전성 분석 기술 중 가장 강력한 분석기법으로 인정받고 있다. 현재까지 연구된 부채널 분석 기법에는 시차분석 (TA: Timing Attack) 기법[6], 전력분석 (PA: Power Analysis) 기법[7], 전자파 분석 (Electromagnetic Analysis) 기법[8] 및 상관전력분석 (CPA: Correlation Power Analysis) 기법[9] 등이 있다. 이중에서 전력 소모 모델을 이용하는 CPA는 효율적이면서 가장 강력한 분석기법으로 알려져 있다. 이러한 분석기법이외에 암호 알고리즘 수행 시 오류를 발생시켜 암호키를 추출해내는 오류주입 분석기법[10]과 일차적인 부채널 방지기법을 공격하기 위한 고차(higher order) 분석기법[11] 등이 있다.

전력신호나 전자파신호를 이용한 부채널 분석 기법은 암호 알고리즘이 수행되는 범용 프로세서나 하드웨어의 연산장치의 정적/동적 전력 소모량이 입력 데이터에 따라 다른 특성을 이용한다. Fig.2.는 Fig.1.의 AES의 연산 중 한 바이트의 AddRoundKey와 ByteSub의 S-box 연산을 [12]에서와 같이 게이트로 구현하고, 이를 Nanosim 툴을 이용하여 전력 시뮬레이션한 결과이다. Fig.2.의 아래 파형은 시뮬레이션 결과를 파형하나로 겹쳐놓은 결과이다. AddRoundKey에 사용된 키값을 0xA8로 고정하고 8비트 입력값을 0x00 ~ 0xFF로 변화시키며 입력하였을 때, 전력 파형 변화량과 연산 시간이 미세하게 차이가 남을 확인할 수 있다.

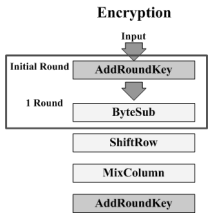


Fig.1. AES operation

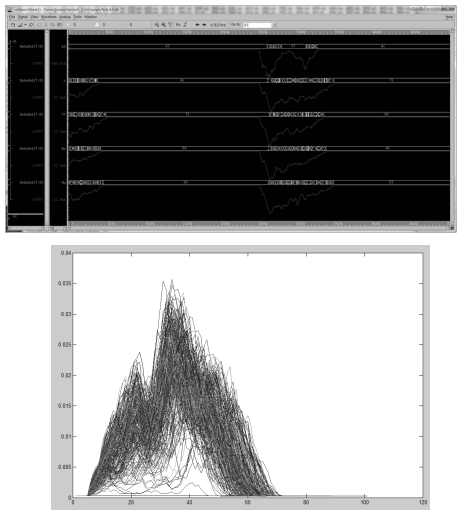


Fig.2. AES S-box power simulation result

Fig.3.은 키를 모른다는 가정 하에 Fig.2.의 결과에 대하여 AES-CPA 분석을 수행한 결과이다. Fig.2.와 같이 노이즈가 없는 파형의 경우 256개의 파형으로도 키 위치(168:0xA8)에서 피크가 검출됨을 확인할 수 있다.

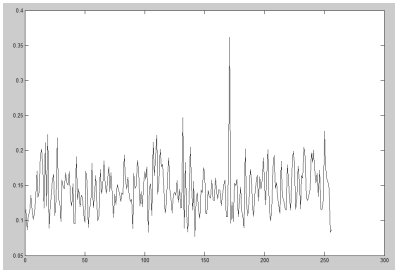


Fig.3. AES CPA result

시뮬레이션이 아닌 실제 보안 디바이스에 대한 부채널 분석기법을 적용하기 위해서는 암호 알고리즘 수행 시 발생하는 전력신호나 전자파신호 등의 부채널 신호 수집이 선행되어야 한다. 전력신호 측정은 전원(VDD)이나 그라운드(GND)에 작은 저항을 삽입하여 전위차를 생성하고, 전위차로 인한 전압신호를 측정함으로써 이루어진다. 이때 삽입되는 저항값이 크면 클수록 측정되는 전압신호가 커지지만, 이로 인하여 안정적인 VDD/GND 동작 범위를 벗어나 보안 디바이스가 동작하지 않을 수 있다. 따라서 암호 알고리즘 동작 검증을 위해서는 저항없이 동작하도록 하고, 동작 검증이 완료된 후 저항에 의한 부채널 신호 측정이 가능하도록 하는 것이 좋다. Fig.4.는 이와 같은 구조의 VDD/GND 전력신호 측정 모듈 그림이다. Fig.4.와 같이 가변저항을 사용하면 부채널 신호의 세기를 조절가능한 장점이 있다. 이러한 전력신호 측정 기법은 KLA-SCARF 부채널 검증 보드에 공통적으로 적용되었다.

Fig.4. Power measurement circuit

전자파신호는 EM(Electronic Magnetic) 프로브를 사용한다. 무선으로 동작하지 않는 보안 디바이스에 대한 전자파신호 측정에서는 EM 프로브를 코일로 직접 제작하여 사용가능하나, 매우 약한 신호를 증폭할 때 신호 왜곡은 최소가 되도록 하기 위해서는 EM 프로브와 매칭(matching)이 잘 이루어진 고속·고성능 증폭기를 사용할 필요가 있다. 이와 같은 문제를 해결하기 위해서 고성능 증폭기가 포함된 상용 EM 프로브를 많이 사용한다. 무선으로 동작하는 보안 디바이스의 전자파신호 측정에서는 EM 프로브와 무선 디바이스 매칭이 이루어지지 않으면 EM 프로브가 무선 통신을 방해할 수 있다. 따라서 EM 프로브가 무선 통신에 주는 영향은 최소가 되면서 측정하고자 하는 부채널 신호는 최대가 되도록 하는 기술이 필요하다. 잘 수집된 전자파신호에 대한 분석 기법은 기본적으로 전력신호 분석 기법과 동일하게 수행한다.

전력/전자파 신호수집은 신호수집장치를 통해서 수행된다. 신호수집장치로는 sampling rate와 bandwidth가 수백 MHz의 성능을 가지는 오실로스코프를 많이 사용한다. 이때, 부채널 신호의 반복적인 수집과 분석을 위해서는 오실로스코프에서의 파형수집 기준 신호인 트리거(trigger) 신호가 필요하다.

한편, 부채널 분석을 효과적으로 수행하기 위해서는 측정된 신호에 존재하는 잡음 성분이 효과적으로 제거되어야 하며 부채널 신호들 사이의 동기가 맞아야 한다. 만약 신호들 사이의 동기가 맞지 않으면 차분 공격 시, 평균에 의해서 각 신호들의 피크 성분이 서로 상쇄되어 분석 성능이 크게 저하된다. 이러한 문제를 해결하기 위해 주파수 영역 부채널 분석기법 (Frequency-domain SCA) [13]과 에너지신호 기반 분석기법 (Energy-based SCA) [14] 등이 제안되었다.

2.2 부채널 분석 시스템

부채널 분석 시스템은 분석에 파형수집부터 전처리 기술 및 다양한 분석 기술 등을 체계적인 방법으로 제공하여야 한다. 현재 인증 장비로 활용되고 있는 대표적인 부채널 분석 시스템으로는 CRI (Cryptography Research Inc)사의 DPA workstation, Brightsight 사의 Sideways, Riscure 사의 Inspector 등이 있다[15].

2.2.1 CRI - DPA Workstation

CRI는 P. Kocher가 설립한 회사로 부채널 분석 기술 및 방지 기술에 대한 원천 특허를 보유한 회사이다. 스마트 카드의 부채널 분석 시스템인 DPA

workstation을 상용 장비로 가장 먼저 출시하였으며, 원천 기술을 바탕으로 세계적인 카드 제조 회사들의 부채널 방지 기술 관련 협력회사로 주된 영업을 하고 있다

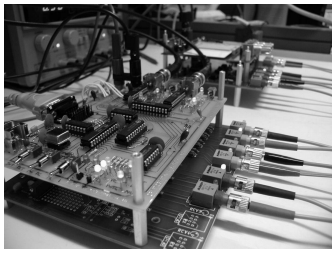


Fig.5. DPA Workstation board

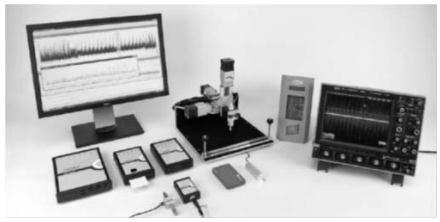
DPA workstation은 파형 수집 기능, 파형 분석 전처리를 위한 신호처리 기능과 SPA 및 DPA 등의 분석 기능을 제공하고 있다. 검증 보드는 Fig.5.의 자체 개발 보드이 외에 SASEBO-G와 SASEBO-W 등을 지원한다. 파형수집장치로는 Tektronics DPO 7104 오실로스코프를 지원하며, 최근에는 Signatec의 PX1440 내장형 파형수집장치를 포함하여 수집 시 바로 주파수 필터링한 데이터 수집이 가능하다. AES, DES, RSA, ECC 등의 암호 알고리즘의 분석이 가능하며, Matlab을 지원하여 이를 이용한 신호처리 등을 사용자가 직접 수행할 수 있다.

2.2.2 Riscure - Inspector

Riscure의 Inspector는 Fig.6.과 같이 전력/전자파 부채널 분석을 위한 Inspector SCA와 오류 주입 분석을 위한 Inspector FI로 구성된다.

Inspector SCA는 전력 및 전자파 파형을 수집하는 기능, 신호처리 기능 및 SPA, DPA 및 CPA 분석 방법 등을 제공한다. 비접촉식 시험 방법도 지원하며, 전자파 파형 수집 및 비접촉식 시험에는 자체 제작한 EM 프로브를 사용하여 신호를 수집한다. DES, AES, RSA, ECC, SEED, DSA, 및 EC-DSA 등의 암호 알고리즘에 대한 분석이 가능하다.

Inspector FI를 이용하여 전압, 클럭 및 레이저 장비를 통한 오류 주입을 통해 AES, DES 및 RSA에 대한 오류 주입 부채널 분석이 가능하다. 레이저 오류 주입 장치는 공격 위치에 따라 두 가지 다른 파장의 레이저로 오류를 주입할 수 있으며, 서로 다른



(a)

(b)

Fig.6. Inspector SCA system(a) and Inspector FI system(b)

두 위치에 오류주입도 가능하도록 구현되었다.

2.2.3 BrightSight - Sideways

BrightSight사의 부채널분석 시스템인 Sideways는 파형 수집과 데이터 분석을 위한 소프트웨어를 포함하고 전력 소모에 대한 SPA와 DPA 분석과 전자파 방출에 대한 SEMA (Simple Electro-Magnetic Analysis)와 DEMA (Differential ElectroMagnetic Analysis) 분석 방법 등을 포함하고 있다. 또한 비접촉식 인터페이스를 통해 비접촉식으로 DPA 분석이 가능하다. Sideways는 MDI (Multi-Document Interface)기반의 GUI를 제공하고 있다.

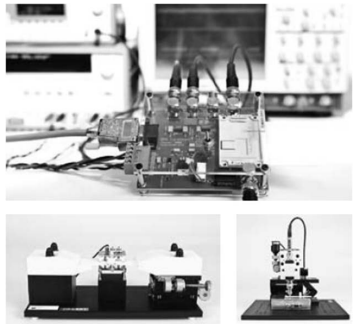


Fig.7. Sideways system

III. KLA-SCARF 부채널 검증 보드

KLA-SCARF 부채널 분석 보드는 접촉형 카드 부채널 분석 보드, 비접촉형 카드 부채널 분석 보드, 소프트웨어 부채널 분석용 보드, 하드웨어 부채널 분석용 보드, 접촉형 카드 오류주입 부채널 분석 보드, 소프트웨어 오류주입 부채널 분석 보드로 구분되며, 본 장에서는 이러한 보드들의 구조 및 기능, 부채널 분석을 위한 모듈에 대해 기술한다.

3.1 접촉형 카드 부채널 분석 보드

접촉형 카드 부채널 분석 보드(KLA-SCARF CEB)는 카드 타입 디바이스의 부채널 분석을 위한 테스트 보드로서 스마트 카드 타입과 USIM 타입 두 가지 디바이스를 테스트할 수 있도록 구성한다. 또한 각각의 IO, RST, CLK 신호 등도 측정이 가능하도록 하여 카드 동작 상태를 확인이 가능하다.

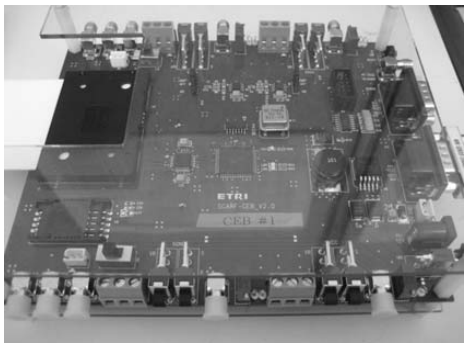


Fig.8. KLA-SCARF CEB

분석 보드의 부채널 신호는 위에 언급한 바와 같이 저항 연결없이 동작하거나, 가변저항/고정저항을 연결하여 부채널 신호를 측정할 수 있도록 한다. 가변저항은 0~200Ω내에 변경이 가능하며, 고정저항은 터미널 블록을 이용하여 특정 저항소자를 고정할 수 있다. 설정은 스위치 조작을 통하여 수행한다. Fig.9.은 GND쪽의 부채널 측정 회로도이다. 그림에 보는 바와 같이 스위치를 통하여 가변저항과 고정저항, 단락회로 중에 선택한다. 단락회로는 단순히 카드의 동작 검증을 수행할 때 사용하며, 동작 검증이 완료된 카드는 가변저항이나 고정저항을 통하여 부채널 신호를 측정한다. 또한 2단 연산증폭기(op-amp)를 사용하여 신호를 증폭하여 측정할 수 있도록 구성한다. 증폭회로는 앞뒤로 스위치를 두어 저항에 의한 신호 측정회로와 완전히 분리할 수 있도록 한다.

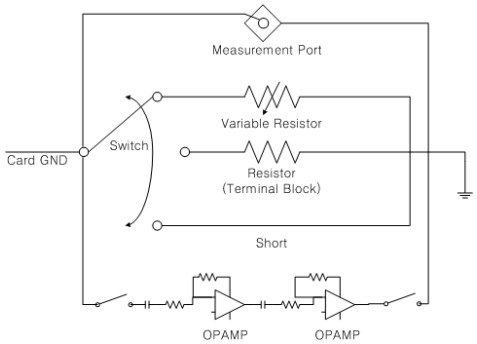


Fig.9. Power measurement circuit of KLA-SCARF CEB

ISO7816 제어를 위해 TDA8007 프로세서를 사용한다. TDA8007 프로세서는 두 개의 ISO7816 통신 포트를 지원하며, 이를 이용하여 스마트 카드 모듈과 USIM 모듈 각각 제어가 가능하다. 분석 보드 전반적인 제어는 ATmega128 프로세서를 사용하여 수행한다. 프로세서의 주된 동작은 다음과 같다.

- TDA8007 모듈 제어
- PC단의 제어 프로그램과의 데이터 송수신
- 파형 수집을 위한 트리거 신호 생성
- 디버깅용 메시지 출력

보드의 전원 공급은 범용적으로 사용되는 어댑터를 이용한다. 보드 내부의 레귤레이터를 이용하여 안정적인 전원이 공급이 가능하지만, 어댑터 전원이 안정적이지 못한 경우 부채널 측정 신호에 영향을 줄 수 있다. 이러한 경우에는 Sideway나 DPA workstation 보드와 같이 power supply에서 전원 공급을 받을 수 있도록 구성한다.

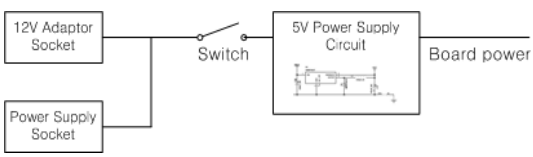


Fig.10. Power supply block

KLA-SCARF CEB 보드 구현에서는 보드 전원이 카드로 공급될 때 안정적인 전원 공급을 위하여 다시 한 번 콘덴서를 거쳐 카드에 입력된다. 이때 사용

되는 콘덴서 용량은 측정하고자 하는 부채널 신호의 패턴 및 분석에 크게 영향을 미치며, 보드에 맞는 콘덴서 용량을 찾을 필요가 있다. KLA-SCARF CEB 보드 구현에서는 콘덴서 용량을 다양하게 바꾸면서 분석 테스트를 수행하여 최적의 값을 도출하였다. 또한, 부채널 측정 신호의 노이즈 감소를 위하여 부채널 신호 측정을 위한 모듈과 그 외의 회로들은 PCB 상에서 각각 분리된 영역과 패턴으로 구현하였다.

3.2 비접촉형 카드 부채널 분석 보드

비접촉형 카드 부채널 분석 보드(KLA-SCARF C2EB)는 비접촉식 카드 디바이스의 부채널 분석을 위한 테스트 보드이다.

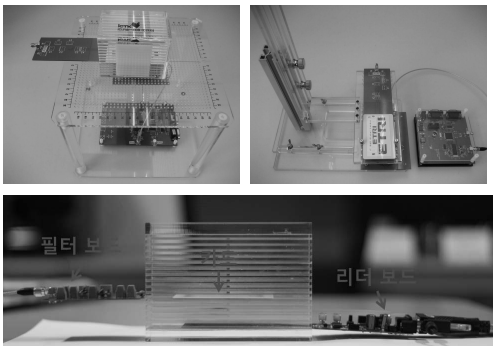


Fig.11. KLA-SCARF C2EB

비접촉형 카드 부채널 분석 보드는 ISO 14443 제어를 위한 NXP MFRC531 프로세서를 사용하는 리더보드와 카드 고정 장치, 그리고 부채널 신호 측정을 위한 필터 보드로 구성된다. Fig.11.에서 보는 바와 같이 비접촉형 카드 부채널 분석 보드는 동일한 리더보드에 안테나와 고정 장치에 따라 3가지 버전이 있다.

리더 보드는 비접촉형 카드와의 통신 데이터 처리 이외에 부채널 신호 측정을 위한 트리거 신호를 생성한다. 부채널 신호 측정을 위한 필터 보드는 Fig.12. 와 같이 구성된다. Card calibration coil은 비접촉식 리더 보드 테스트 시 사용되는 것과 동일하며, matching filter와 low pass filter는 카드 RF 특성에 맞추어 소자값들을 조정하여 구현한다.

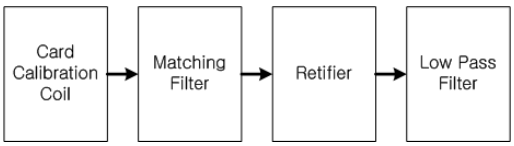


Fig.12. Components of Filter board

3.3 소프트웨어 부채널 분석 보드

소프트웨어 부채널 분석 보드는 부채널 분석을 쉽게 수행할 수 없는 소형 보안 디바이스의 보안 프로그램에 대한 1차적인 부채널 검증을 위한 보드이다. 이를 위해서 소형 보안 디바이스에 많이 사용되는 8비트 2종, 16비트 1종, 32비트 1종의 프로세서를 선정하고, 이들 프로세서들에 대한 부채널 분석을 쉽게 수행할 수 있도록 보드를 구현하였다. 다음은 이러한 소프트웨어 부채널 분석 보드의 형상과 특징이다.

Fig.13. Software side-channel evaluation boards

이들 보드의 부채널 신호 측정 모듈 구현 시 측정하고자 하는 프로세서의 VDD/GND 신호를 보드의 VDD/GND 신호를 분리하여 측정 모듈을 구현하여야 하며, 프로세서 내에 여러 개의 VDD/GND 신호가 있는 경우 이들 신호들을 하나로 통합하여 부채널

신호 측정 모듈에 연결하여야 한다. Fig.14.는 KLA-SCARF SW 보드 프로세서의 GND 신호 연결과 GND 신호 측정 모듈 구성도이다. VDD도 이와 유사한 방식으로 구성되며, 측정 모듈이 프로세서 입력 전에 있는 점만 다르다. 신호 측정 시 필요한 트리거 신호는 보안 프로그램 수행 시 특정 포트 로 직접 출력하고 이를 측정하는 방식으로 구현한다.

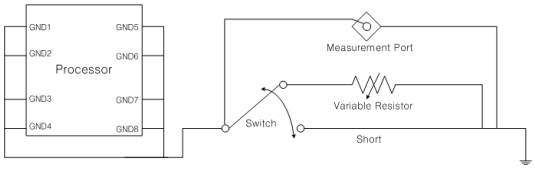


Fig.14. GND signal measurement circuit of KLA-SCARF SW board

3.4 하드웨어 부채널 분석 보드

하드웨어 부채널 분석 보드(KLA-SCARF HEB)는 하드웨어 IP(Intellectual Property)로 설계된 보안 모듈에 대한 부채널 분석을 수행할 수 있도록 하는 보드로서 SASEBO 보드와 유사한 기능을 수행한다.

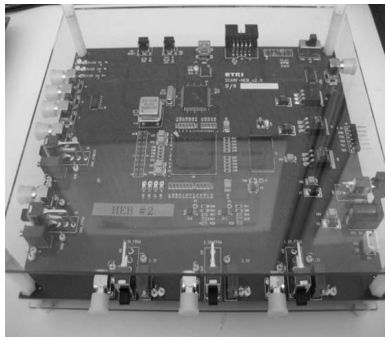


Fig.15. KLA-SCARF HEB

Fig.16.은 하드웨어 부채널 분석 보드의 구조를 보인 그림이다. 보드 제어 및 사용자 PC와의 통신은 ATmega128 프로세서를 사용하며, 하드웨어 구현을 위한 FPGA는 Xilinx spartan3 1500이 사용되었다. FPGA와 ATmega128 프로세서와의 인터페이스를 위한 I/O 모듈이 별도로 구성된다. 프로세서용 코드와 I/O 모듈의 샘플 코드를 이용하여 테스트하고자하는 보안 HW 모듈 인터페이스의 간단한 수정으로

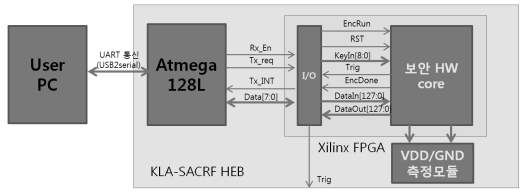


Fig.16. Component block diagram of KLA-SCARF HEB

안전성 검증을 수행할 수 있다.

부채널 신호 측정을 위하여 Xilinx spartan3 FPGA의 3.3V, 2.5V, 1.8V의 3가지 전원 신호와 GND 신호는 각각 분리하여 측정 모듈을 구성한다. 트리거 신호는 보안 HW 모듈에서 측정하고자 하는 부분의 신호를 측정 포트로 바로 출력할 수 있으며, 별다른 트리거 신호가 없는 경우 보안 HW 모듈 시작 신호를 트리거 신호로 사용할 수 있다.

3.5 접촉형 카드 오류주입 분석 보드

접촉형 카드 오류주입 분석 보드(KLA-SCARF CFEB)는 접촉형 카드 부채널 분석 보드의 확장형으로 스마트 카드의 전원과 클럭(CLK) 신호에 오류주입 분석이 가능하도록 한다.

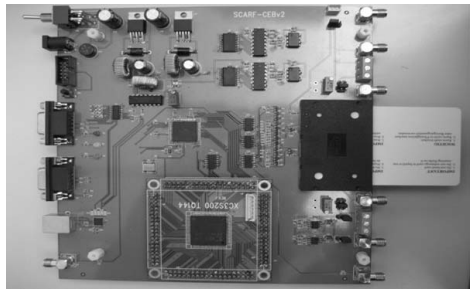


Fig.17. KLA-SCARF CFEB

접촉형 카드 오류주입 분석 보드는 별도의 외부장비없이 오류주입 테스트가 가능하며, Fig.18.과 같이 카드에 입력되는 전원을 0V~25V 내로 가변하여 입력할 수 있으며, CLK는 클럭의 상승과 하향 신호에서 고주파 클럭을 주입할 수 있다.

전원 오류를 위한 가변전압은 Fig.19.와 같이 연산증폭기(op-amp)를 통하여 생성하며, 생성된 가변 전압은 트랜지스터(TR : Transistor) 스위치를 통하여 선택적으로 카드에 입력된다. 그림의 아래쪽 트랜

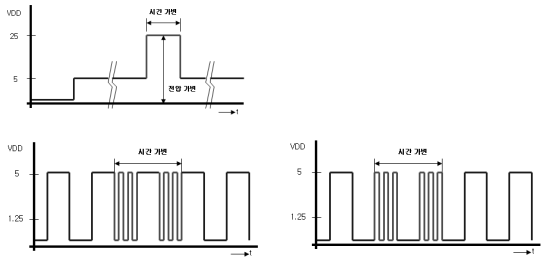


Fig.18. VDD/CLK fault-injection of KLA-SCARF CFEB

지스터 스위치는 공급되는 전압을 순간적으로 GND로 낮추는 동작 수행에 사용된다. 이들 동작을 위한 제어 데이터(Control data)와 오류 제어 신호(Fault control) 신호는 보드 내의 FPGA에 구현되는 하드웨어 로직을 통하여 수행한다. FPGA에서는 카드에 공급되는 클럭 생성 동작도 수행하며, 클럭 오류 주입 동작 시에는 고주파 클럭 신호를 생성하여 카드에 공급한다.

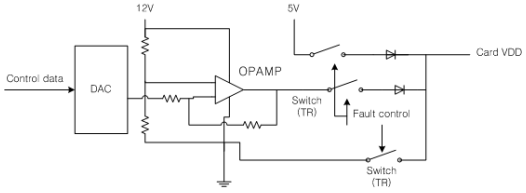


Fig.19. Power fault generation circuit

3.6 소프트웨어 오류주입 분석 보드

소프트웨어 오류주입 분석 보드(KLA-SCARF SFEB)는 소프트웨어로 구현된 암호 알고리즘에 대한 오류주입 분석을 위한 보드이다. 카드 오류주입 보드와 같이 전원과 CLK 오류 주입이 가능하다.

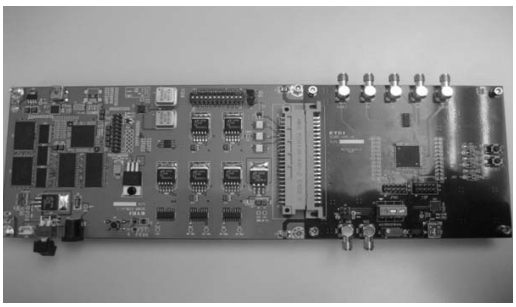


Fig.20. KLA-SCARF SFEB

소프트웨어 오류주입 분석 보드는 오류주입 제어 보드(왼쪽)와 오류주입 타겟 보드(오른쪽)로 구분된다. 오류주입 제어보드는 ARM 프로세서를 통하여 오류 생성 및 주입 동작을 수행하며, 타겟 보드는 ATmega128 프로세서를 통하여 오류주입 시 상태를 확인할 수 있도록 한다. 전원 오류는 Fig.21.과 같이 0V~12V 사이의 오류전원을 주입할 수 있으며, 클럭 오류는 정상 클럭과 고주파 클럭을 순간적으로 스위칭 시키는 방식으로 오류 CLK을 주입한다.

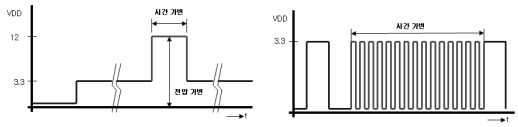


Fig.21. VDD/CLK fault-injection of KLA-SCARF SFEB

IV. KLA-SCARF 부채널 검증 보드 성능

이 장에서는 구현된 KLA-SCARF 부채널 분석 보드들의 기능 및 성능에 대해 기술한다.

4.1 접촉형 카드 부채널 분석 보드

접촉형 카드 부채널 분석 보드는 2장에서 언급한 바와 같이 상용 시스템들이 존재한다. 이들과의 비교 테스트가 국민대학교와 금융결제원에서 수행되었으며, 상용 시스템과 비교하여 성능차이는 거의 없는 것으로 평가되었다[16].

알고리즘	SCA Tool	카드작동	SPA 분석	CPA분석(키분석 유무)
SEED	SCARF	○	○	○
	Inspector	○	○	○
	Sideways	○	○	○
AES	SCARF	○	○	○
	Inspector	○	○	○
	Sideways	○	○	○
DES	SCARF	○	○	○
	Inspector	X	-	-
	Sideways	X	-	-

Fig.22. Testing result of the KLA-SCARF and commercial equipments

4.2 비접촉형 카드 부채널 분석 보드

KLA-SCARF C2EB 비접촉형 카드 부채널 분석 장비는 카드 파형 수집 시 SPA(Simple Power

Analysis)로 암호 연산 파형을 구분할 수 있으며, 이를 통하여 접촉식 카드 분석과 유사한 방식으로 테스트를 수행할 수 있다. Fig.23.은 상용 금융IC 카드에 대한 테스트 시 3번의 SEED가 수행되고 있음을 확인할 수 있는 SPA 파형이며, Fig.24.는 수집된 파형에 대한 첫 번째 SEED의 1라운드 부분키 분석 결과이다. Fig.24.결과를 보면 필터로부터 수집된 파형으로 4개의 부분 키들이 분석됨을 확인할 수 있다.

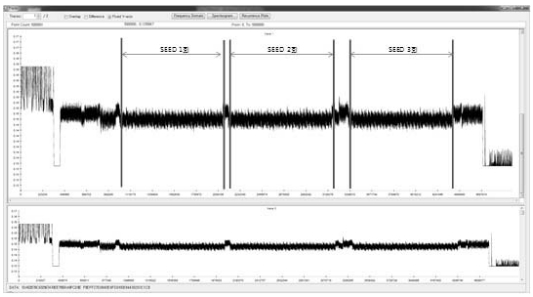


Fig.23. SPA result of a contactless financial IC card

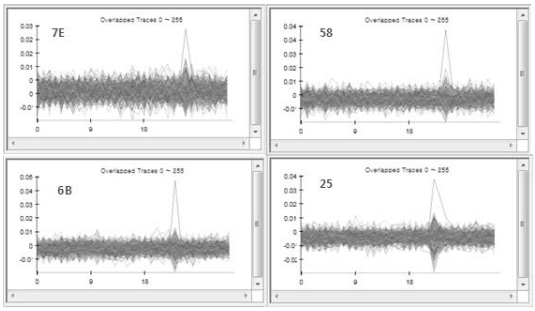


Fig.24. SEED-CPA result

4.3 소프트웨어/하드웨어 부채널 분석 보드

KLA-SCARF 소프트웨어와 하드웨어 부채널 분석 보드들은 부채널 분석을 필요한 로직들만으로 구성하였으며, 트리거 신호가 측정하고자 하는 연산단계에서 바로 출력된다는 점에서 부채널 분석을 매우 쉽고 정확하게 수행할 수 있다. 이러한 이유로 각 보드마다 특성이 존재하지만, 방지 기법이 없는 암호 알고리즘에 대하여 거의 백여 개 파형으로 키 검출이 가능하다. Fig.25.는 ARM 보드에서 AES를 구현하여, 이에 대한 AES-CPA를 분석한 결과이다. 500개 파형에 대한 분석 결과로서, 첫 번째 결과 그림에서 모든 키들이 분석되었음을 확인할 수 있으며, 50개 단위로 분석 결과를 출력한 세 번째의 추세 그래프를 보면, 거의 수십 개의 파형부터 키가 검출되기 시작함을 확인할 수 있다.

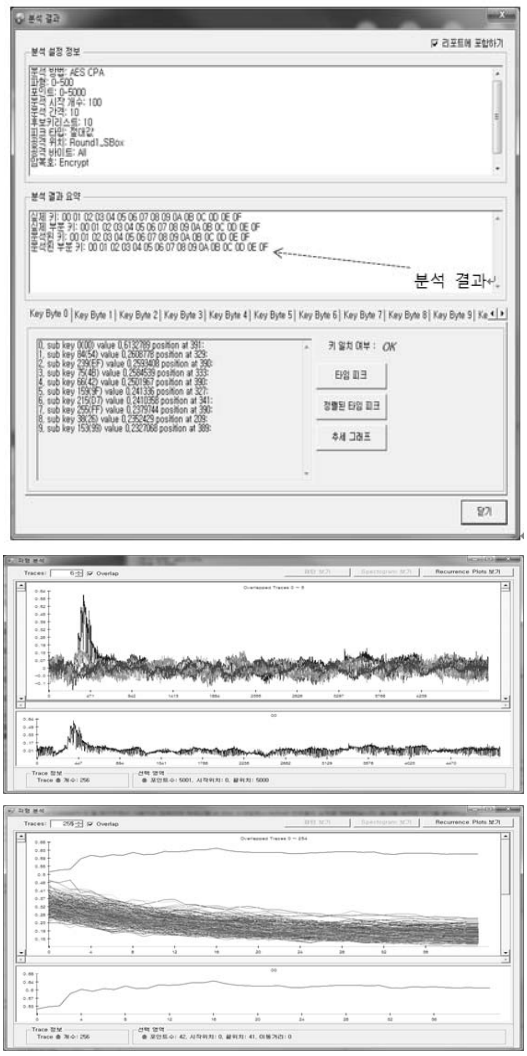


Fig.25. AES-CPA result of KLA-SCARF ARM

4.4 접촉형 카드/소프트웨어 오류주입 분석 보드

접촉형 카드 오류주입 분석 보드에서 생성되는 전원 오류와 CLK 오류는 Fig.26.과 같다. 각 그림들의 원으로 표시되어 있는 곳에서 보는 바와 같이 VDD 전원이 순간적으로 떨어졌다가 다시 정상적인 값으로 돌아가며, CLK 신호가 고주파 클럭으로 바뀌었다가 다시 정상 클럭으로 변함을 확인할 수 있다. 소프트웨어 오류주입 분석 보드에서 생성되는 전원 오류와 CLK 오류도 이와 거의 유사하다.

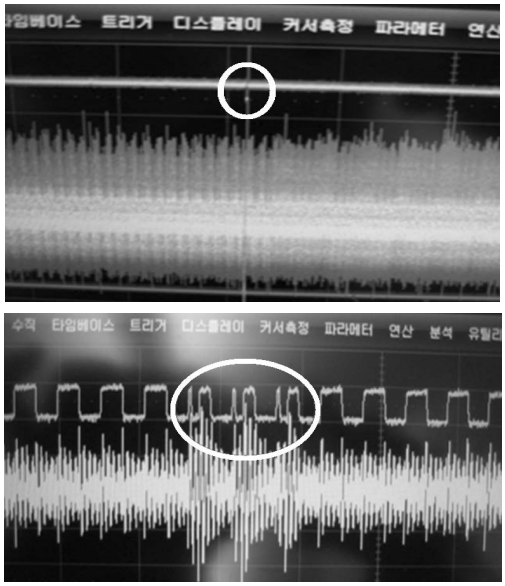


Fig.26. Waveforms of VDD/CLK fault

위와 같은 오류가 주입되었을 때 테스트 디바이스는 동작을 멈추거나, 오류에 영향없이 정상적으로 동작하거나, 오류 결과를 출력한다. 오류주입 분석을 위해서는 오류 결과가 출력되는 경우가 필요하다. Fig.27.은 AES가 구현된 카드의 9라운드에 전원 오류를 삽입했을 때 분석에 필요한 4개의 오류가 발생하는 결과들만 출력한 데이터이다.

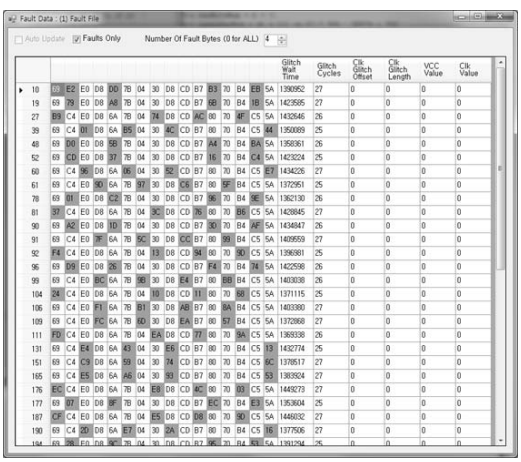


Fig.27. Fault-injection test result of an AES card

그림에서 보는 바와 같이 동일한 위치에 오류가 발생하더라도 오류의 미세한 차이로 다른 오류값들을 얻을 수 있으며, 이를 통해 키를 분석할 수 있다. Fig.28.은 수집된 오류 데이터를 이용하여 SCARF 툴에서 오류분석을 수행한 결과로서, 모든 키가 분석됨을 확인할 수 있다.

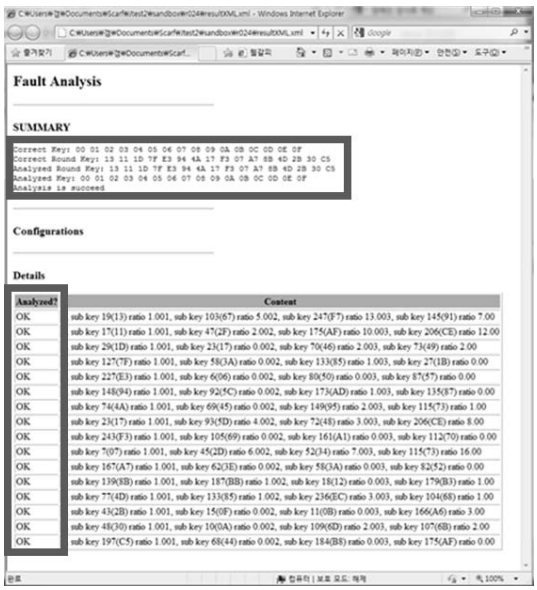


Fig.28. Fault analysis result of an AES card

V. 결론

본 논문에서는 KLA-SCARF 시스템의 부채널 분석 보드들의 구현 기법과 기능 및 특성 등에 대하여 기술하였다. KLA-SCARF 시스템은 현재 고가의 외산 부채널 분석 장비를 대체할 수 있는 장비로 평가받고 있으며, 이의 분석용 보드들의 구현 기법과 특징을 기술함으로써 추후 보안 디바이스의 부채널 분석 시스템을 구현하고자 하는 연구자에게 방향을 제시하고자 하였다.

KLA-SCARF 프로젝트에서는 위에서 언급된 분석용 보드 이외에 저가의 레이저를 이용한 레이저 오류 주입 시스템, EM 오류주입 보드, 소형 보안 디바이스 부채널 분석용 보드, 파형 검출 및 스마트 트리거 보드 등이 개발 중에 있으며, 구현된 보드들과 개발될 시스템의 연동은 보안 디바이스에 대한 보다 강력한 평가 툴을 제공할 수 있으리라 본다.

VI. References

[1] P. Kocher, J. Jaffe, and B. Jun, "Introduction to differential power analysis and related attacks," White Paper, Cryptography Research, pp. 1-5, 1998.

[2] Cryptography Research. DPA Workstation. Available online at http://www.cryptography.com/technology/dpa-workstation.html.

[3] Riscure. Inspector - The Side-Channel Test Tool. Available online at http://www.riscure.com/archive/Inspector_brochure.pdf

[4] BrightSight. Unique Tools from the Security Lab. Available online at http://www.brightsight.com/documents/marcom-materials/BrightSight_Tools.pdf

[5] SASEBO project. Available online at http://www.risec.aist.go.jp/project/sasebo

[6] Paul C. Kocher, "Timing attacks on implementations of diffie-hellman, RSA, DSS, and other systems," Advances in Cryptology-Crypto. LNCS 1109, pp 104-113, 1996.

[7] P. Kocher, J. Jaffe and B. Jun, "Differential power analysis," CRYPTO 1999, LNCS 1666, pp. 388-397, 1999.

[8] K. Gandolfi, C. Mourtel, and F. Oliveier, "Electromagnetic analysis: concrete results," CHES 2001, LNCS 2162, pp. 255-265, 2001.

[9] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," CHES 2004, LNCS 3156, pp. 16-29, 2004.

[10] Mei-Chen Hsueh, Timothy K. Tsai, Ravishankar K. Iyer, "Fault injection techniques and tools," IEEE Computer Vol. 30, no. 4, pp 75-82, 1997.

[11] Thomas S. Messerges "Using second-order power analysis to attack DPA resistant software" CHES 2000, LNCS 1965, pp 238-251, 2000.

[12] Wolkerstorfer J, Oswald E, Lamberger M. "An ASIC implementation of the AES S-Boxes" Cryptographer's Track at the RSA Conference, LNCS 2271. pp. 67-78, 2002.

[13] C. Gebotys, S. Ho. and C.C. Tiu, "EM analysis of Rijndael and ECC on a wireless java-based PDA," CHES 2005, LNCS 3659, pp. 350-264, 2005.

[14] T-H. Le, J. Clédière, C. Servière, J-L. Lacoume, "Efficient solution for misalignment of signal in side channel analysis," ICASSP 2007. vol. 2, pp. 257-260, April 2007.

[15] Juhan Kim, Kyunghee Oh, Yongje Choi, Taesung Kim, and Dooho Choi, "Technical Trends of Side Channel Analysis System", Electronics and Telecommunications Trends, 28(3), June 2013.

[16] Changyoung Choi, Jaechoel Jung, and Hyugun Shin, "Comparison of Side Channel Analysis Tools for the Financial IC Card", Journal of The Korea Institute of information Security & Cryptology, 22(8), pp 54-60, Dec. 2012.

〈저자소개〉

최 용 제 (Yong-Je Choi) 정회원
1996년 8월: 전남대학교 전자공학과 졸업
1999년 2월: 전남대학교 전자공학과 석사
1999년 2월~1999년 8월: 전남대학교 전자통신연구소 인턴연구원
1999년 8월~현재: 한국전자통신연구원 선임연구원
〈관심분야〉 보안프로세서 설계, 부채널 분석 시스템, RFID/USN 보안

최 두 호 (Doo-Ho Choi) 정회원
1994년 2월: 성균관대학교 수학과 졸업
1996년 2월: KAIST 수학과 석사
2002년 2월: KAIST 수학과 박사
2002년 1월~현재: 한국전자통신연구원 책임연구원
〈관심분야〉 암호학, 부채널 분석, RFID/USN 보안

류 재 철 (Jea-Cheol Ryou) 종신회원
1985년 2월: 한양대학교 산업공학과 졸업
1988년 2월: Iowa State University 전산학과 석사 졸업
1990년 2월: Northwestern University 전산학과 박사 졸업
1991년~현재: 충남대학교 전기정보통신공학부 교수
〈관심분야〉 인터넷 보안