2013
Electronics and
Telecommunications
Trends

사이버 보안 기술 특집

부채널 분석 시스템 기술 동향

Technical Trends of Side Channel Analysis System

Ⅰ. 머리말
Ⅱ. 부채널 분석 기술
Ⅲ. 부채널 분석 시스템 기술 동향
Ⅳ. 부채널 분석 시스템 구조
Ⅴ. 맺음말

김주한(J.H. Kim) 디바이스보안분석연구실 선임연구원
오경희(K.H. Oh) 디바이스보안분석연구실 선임연구원
최용제(Y.J. Choi) 디바이스보안분석연구실 선임연구원
김태성(T.S. Kim) 디바이스보안분석연구실 선임연구원
최두호(D.H. Choi) 디바이스보안분석연구실 실장

* 본 연구는 ETRI의 연구개발 과제인 KLA-SCARF 프로젝트로 수행하였음(암호키 누출 검증 및 방지 원천 기술 연구).

부채널 분석은 암호 알고리즘이 장치 내에서 동작하는 동안에 장치의 전력이나 전자파 등의 부가 정보의 수집, 가공 및 통계적인 분석을 통해 키 정보를 추출해 내는 매우 강력한 공격 방법이다. 부채널 분석 시스템은 암호 모듈이 탑재되는 장치가 부채널 공격에 대해 안전한지를 사전 검증 및 시험할 수 있는 방법들을 제공한다. 본고에서는 다양한 부채널 분석 방법 및 이를 제공하는 부채널 분석 시스템에 대한 현황 및 전망을 기술한다.

Ⅰ. 머리말

1. 부채널 분석 정의

부채널 분석(side channel analysis)은 암호 모듈이 탑재된 전자장치에서 암호 알고리즘이 수행되는 순간에 발생되는 전력소모 및 전자기파 등의 누수 정보를 획득 및 가공, 분석하여 암호키 등의 비밀 정보를 획득하는 분석법이다.

전통적인 암호 분석 방법은 입력인 평문과 출력인 암호문을 비교 분석하여 키 정보를 획득하는 방식으로 암호 알고리즘 자체의 보안 취약성을 이용한다. 그러나 부채널 분석은 암호 알고리즘이 구현된 암호 모듈이 키 정보를 연산하며 발생되는 전력 소모량, 전자기파 등의 부채널 정보를 통계적으로 분석한다.

따라서 암호 알고리즘 자체가 고도의 암호학적 이론을 갖더라도 실제 그 알고리즘이 구현된 암호 모듈 내부에서 사용되는 키 정보와 같이 연산되는 과정에서 발생되는 부가 정보들을 이용한 부채널 분석 방법에서는 안전하다고 볼 수 없다.

부채널 분석 공격을 막기 위해서는 암호 알고리즘 구현 시에 부채널 분석 공격에 대한 대응 기법들을 적용해야 한다. 하지만, 이런 대응 기법들에 대한 새로운 공격 방법들도 계속 논문 등으로 발표되고 있다. 대응 기법이 적용된 암호 모듈은 적용 안된 것에 비해 분석에 상대적으로 훨씬 많은 파형들이 필요하게 되고 분석의 난이도가 증가함으로 암호 모듈 제작 시에는 반드시 부채널 분석 대응 기법을 적용해야 한다.

부채널 분석 시스템은 부채널 분석 방법을 통해 암호 모듈이 탑재되어 있는 장치의 부채널 취약성을 검증하고 이에 대한 대응 기법을 적용한 암호 모듈을 다시 검증할 수 있어 부채널 분석에 대한 안전성 시험 및 대응 기술에 대한 효율성을 평가할 수 있는 방법을 제공한다.

2. 부채널 분석 배경

부채널 분석은 1996년 P. Kocher의 시차분석 공격(Timing Attack: TA)[1]에 대한 연구를 발표한 이후로 시작되었으며 전력분석 공격(Power Analysis Attack: PA)[2], 전자기파분석 공격(Electromagnetic Emission Attack: EM)[3] 및 오류주입 공격(Fault-Injection Attack: FA) 등의 다양한 형태로 제안되었으며 최근에는 이러한 부채널 분석 공격에 대한 대응책과 이런 대응책에 대한 공격 방법들에 대한 연구가 활발히 진행되고 있다.

부채널 분석 공격에 대한 암호 모듈이 탑재된 전자장치에 대한 취약성이 노출됨에 따라 부채널 분석 공격에 대한 보안성 평가가 필요하게 되었으며 이에 따라 CC (Common Criteria) 인증, EMV(Electromagnetic Vulnerability) 인증, FIPS140-3(Cryptographic Module Validation Program: CMVP) 등에 부채널 분석 공격에 대한 보안 하드웨어 안전성 평가가 포함되었다.

3. 부채널 분석 시스템

부채널 분석 시스템은 보안 하드웨어에 대한 부채널 분석 안전성을 평가하는 장비로 안전성 검증 및 인증하는 인증기관에서 사용된다. 그리고 안전성 평가 전에 설계 또는 구현된 암호 모듈이 부채널 분석 공격에 안전한지 사전에 검증하기 위해 보안 하드웨어 제조업체 등에서도 사용한다.

부채널 분석 시스템은 통상적으로 암호 모듈을 탑재하는 검증 보드, 검증 보드에서 파형을 수집하는 파형수집 장치 및 수집된 파형을 가공 및 분석하는 분석 장비로 구성된다.

검증 보드는 소프트웨어 형태로 구성된 암호 모듈을 탑재하여 시험할 수 있는 소프트웨어 검증 보드, 하드웨어 형태의 암호 모듈을 시험할 수 있는 하드웨어 검증 보드, 스마트카드 내의 암호 모듈을 시험할 수 있는 접

촉식/비접촉식 스마트카드 검증 보드 및 오류주입을 검증할 수 있는 오류주입 검증 보드 등이 있으며 각각의 보드들은 암호 모듈이 동작할 때 전력소모 또는 방출되는 전자파를 측정 및 수집하여 부채널 분석이 용이하도록 개발된다.

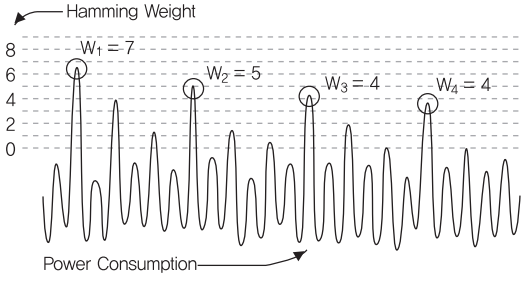
암호 모듈이 실제 탑재되는 장치의 프로세서는 다양하고 이에 따라 전력 소모량과 방출되는 전자파의 양 및 형태가 달라진다. 따라서 검증 보드의 설계 및 구현도 각 장치 프로세서를 고려하여 이루어지고 있다.

파형수집 장치는 기존의 오실로스코프 등을 이용하고 있으며 분석 장비는 검증 보드 및 파형수집 장치를 연결하여 암호 모듈이 동작할 때마다 전력소모 파형 또는 방출되는 전자파를 측정하여 수집하며, 이를 가공하고 분석하는 장비로 주로 소프트웨어로 이루어진다.

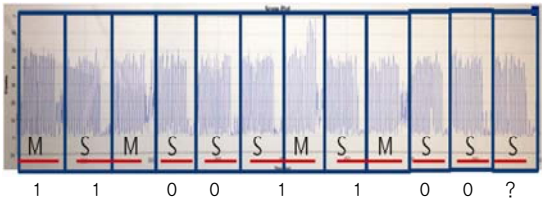
II. 부채널 분석 기술

부채널 분석은 암호 모듈이 동작하는 동안의 데이터의 변화를 통계적으로 분석하는 기술에 의존한다. 즉, 키와 관계된 데이터가 0과 1로 구성되고 전자장치에서 이런 0과 1을 처리하는 동안의 소모전력이 다른 특징을 이용한다. 전자장치에서 동작하는 동안의 0과 1의 변화량의 Hamming distance 또는 (그림 1)과 같이 1의 개수의 Hamming weight 등과 같은 전력/전자파 모델링을 통해 키를 분석해내는 방법이다.

위와 같은 분석 방식의 대표적인 것들로 DPA (Differential Power Analysis)와 CPA(Correlation Power Analysis)가 있다. 또한, 전력 또는 전자파 파형의 모습, 즉 전력 소모량을 관찰하여 중요 정보를 획득하는 SPA(Simple Power Analysis)가 있다. 그 외에 부채널 대응 기법이 포함된 암호 모듈을 분석할 수 HODPA (High Order Differential Power Analysis) 분석 방법 등 다양한 분석 방법이 존재한다.



(그림 1) Hamming Weight에 따른 전력소비량[4]



*M은 곱셈연산, S는 지수연산

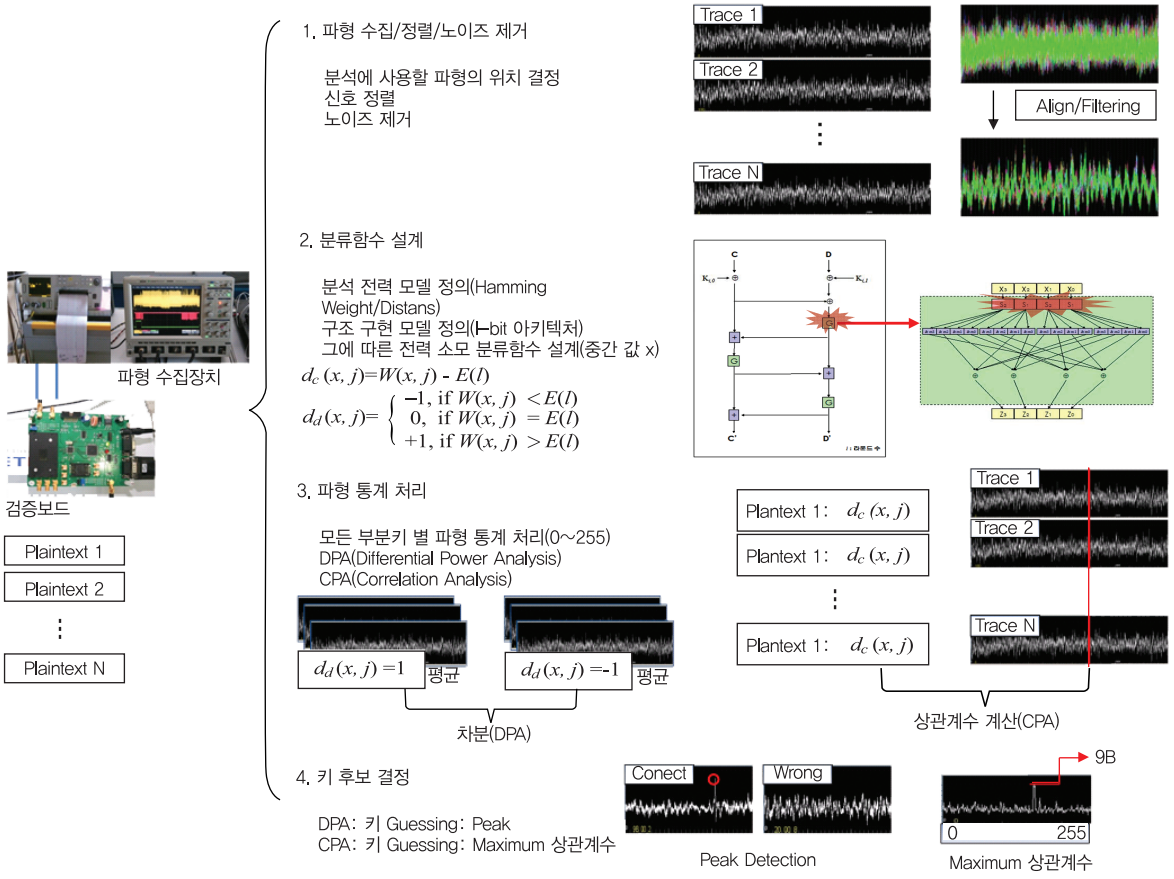
(그림 2) RSA 연산에 대한 SPA

1. SPA

(그림 2)는 RSA(Rivest-Shamir-Adleman) 알고리즘이 동작할 때 수집한 파형의 일부로 파형에서 RSA가 동작할 때 하는 곱셈연산과 지수연산의 패턴이 명확하게 보인다. RSA 알고리즘은 개인키의 한 비트가 0일 때는 지수연산만 동작하고 1일때는 지수연산과 곱셈연산이 순서대로 나온다. 따라서 (그림 2)와 파형을 통해 RSA 알고리즘에서 사용된 개인키를 계산할 수 있다. 이와 같이 단순히 파형의 모습을 관찰하여 키와 관계된 정보를 얻을 수 있는 분석 방법을 SPA라 한다.

2. DPA와 CPA

DPA와 CPA는 (그림 3)과 같이 암호 모듈을 계속 동작시키고 고정된 비밀키에 다른 평문을 입력으로 넣어 암호문을 얻고 동시에 파형수집 장치를 통해 파형들을 수집한다. 평문, 암호문 및 수집된 파형을 통해 설계된 분류함수를 기준으로 파형 통계 처리를 하여 분석하는 방식이다.



(그림 3) DPA와 CPA 분석절차

DPA의 분류 함수는 평문과 분석 부분의 출력 비트 그리고 비밀 정보를 입력으로 갖는 함수로, 이 세 가지 입력에 따라 결과가 0 또는 1이 되는 함수이다. 이를 통해 출력이 0이 되는 파형과 1이 되는 파형을 분류한다. 분류된 0 그룹의 파형과 1 그룹의 파형을 각각 평균을 내고 그룹 간 평균의 차를 구할 경우, 정확한 키에서는 평균의 차가 크고 그렇지 않을 경우에는 피크가 보이지 않게 되어 정확한 키를 추측할 수 있게 된다.

CPA는 암호 알고리즘의 특정 부분을 분석하는 것으로 분석 부분의 데이터에 대해서 모든 키가 가질 수 있는 경우의 수와 동일한 데이터 셋을 이용하여 중간값의 추정치를 생성한다. 추정치를 이용하여 모든 키와 특정 데이터 셋에 대한 전력소모 모델을 설계한다. 해당 데이터 셋을 이용하여 전력소모 정보를 수집하고 각 파형과 키에 대응하는 전력소모 모델을 비교하여 가장 상관 계수가 높은 추정하여 키를 찾는 방식이다.

CPA는 중간값과 암호 모듈 동작 시에 수집한 파형 간에 연관성 정도를 통계적으로 계산하여 가장 연관이 높은 경우를 이용해 분석한다. 따라서, 입력에 따라 어떤 중간값이 나오는지 미리 계산해야 한다.

3. 오류주입

오류주입은 암호 모듈을 탑재하고 있는 칩과 같은 전자장치에 외부로부터 전압, 클록, 온도 및 레이저 빛 등을 가해서 암호 알고리즘의 연산 과정의 특정 위치에서 오류를 일으키도록 하는 부채널 분석 방법이다.

분석 위치에서 정확하게 발생되는 오류를 통해 원래

나와야 할 정상적인 암호문과 오류가 발생되어 나오는 암호문을 연속적으로 수집한 후 이를 비교 분석하면 비밀키를 얻어낼 수 있다.

오류주입 방식은 전압, 클록, 온도 등의 변화를 통해 오류주입하는 방식의 비침투형, 레이저 빛이나 외부의 전자장 등을 이용하는 방식을 준침투형 및 칩의 패키지를 벗겨내어 분석하는 침투형 방식으로 구분할 수 있다.

Ⅲ. 부채널 분석 시스템 기술 동향

부채널 분석 시스템은 분석에 필요한 절차, 파형수집, 여러 가지 전처리 기술 및 분석 기술 등을 체계적인 방법으로 제공하고 다양한 암호 알고리즘 및 분석 방법 등을 사용자가 쉽게 사용할 수 있도록 지원하는 역할을 한다. 대표적인 부채널 분석 시스템으로는 CRI (Cryptography Research Inc)사의 DPA workstation[5], Brightsight사의 Sideways[6], Riscure사의 Inspector[7] 및 ETRI의 SCARF(Side Channel Analysis Resistant Framework)[7] 등이 있다. 각 부채널 분석 시스템은 각각의 특징이 있지만 부채널 취약성 검증에 대한 신뢰성 있는 방법을 제공하고 있다.

1. CRI – DPA Workstation

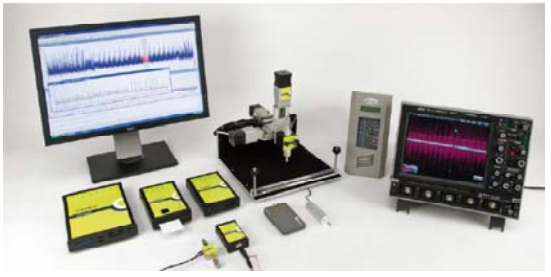
P. Kocher가 설립한 회사로 부채널 분석 시스템에 대한 원천 특허(미국 및 네덜란드) 및 다수의 부채널 대응 기술에 대한 특허를 보유한 회사이다. CRI는 부채널 분석 시스템에 대한 사업보다는 부채널 대응 기술에 대한 IP(Intellectual Property)에 대한 사업을 중점적으로 진행하고 있다.

DPA workstation은 파형수집 기능, 파형 분석 전처리를 위한 신호처리 기능과 SPA 및 DPA 등의 분석 기능을 제공하고 있다. 파형수집을 위해서 Tektronics DPO7104 오실로스코프를 지원하고 있으며 검증 보드는 SASEBO(Side-channel Attack Standard Evaluation Board) FPGA 보드와 스마트카드 검증 보드 등을 지원한다. AES(Advanced Encryption Standard), DES(Data Encryption Standard), RSA, ECC(Elliptic Curve Cryptography) 등의 암호 알고리즘 등에 분석할 수 있다. DPA workstation은 Matlab을 지원하여 이를 이용한 신호처리 등을 사용자가 직접 실험을 해볼 수 있는 것이 특징이다.

2. Riscure – Inspector

Inspector는 (그림 4)와 같이 전력/전자파 부채널 분석을 위한 Inspector SCA(Side Channel Attack)와 오류주입 분석을 위한 Inspector FI(Fault Injection)로 구성된다.

Inspector SCA는 전력 및 전자파 파형을 수집하는 기



(a)

(b)

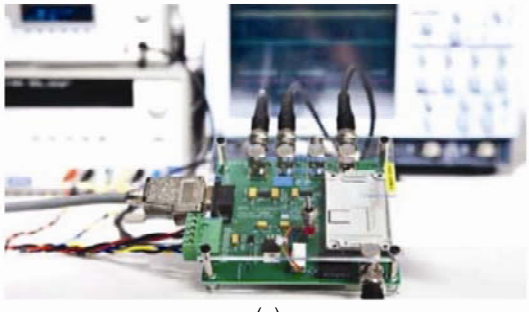
(그림 4) Inspector SCA 시스템 구성(a)과 Inspector FI 시스템 구성(b)[6]

능, 신호처리 기능 및 SPA, DPA 및 CPA 분석 방법 등을 제공한다. 비접촉식 시험 방법도 지원한다. DES, AES, RSA, ECC, SEED, DSA(Digital Signature Algorithm), 및 ECDSA 등의 암호 알고리즘에 대한 분석이 가능하다.

Inspector FI를 이용하여 전압, 클록 및 광학 장비를 통한 오류주입을 통해 AES, DES 및 RSA에 대한 오류주입 부채널 분석이 가능하다.

3. BrightSight – Sideways

BrightSight사의 부채널 분석 시스템인 Sideways는 (그림 5)와 같이 파형수집과 데이터 분석을 위한 소프트웨어를 포함하고 전력소모에 대한 SPA와 DPA 분석과 전자파 방출에 대한 SEMA(Simple Electromagnetic 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.



(a)

(b)

(c)

(그림 5) Sideways 검증보드(a), 비접촉식 DPA 분석을 위한 측정장비(b), EM 측정장비(c)[7]

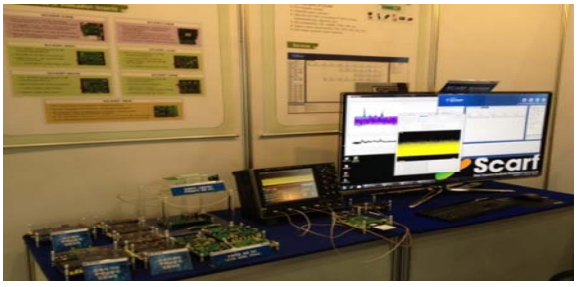
4. ETRI – SCARF

(그림 6)은 ETRI에서 개발한 SCARF로 전력 및 전자파에 대한 파형수집, 전처리 및 분석에 이르는 모든 과정이 병렬처리 및 분산처리가 가능한 구조로 되어 있고 수집부터 분석까지 일괄처리가 가능하다.

SEED, AES, DES, ARIA(Academy-Research Institute-Agency) 및 RSA 등의 암호 알고리즘에 대한 분석이 가능하며 사용자가 새로운 분석 방법이나 전처리 기능을 프로세스로 생성하여 추가하는 가능한 구조로 되어 있다.

검증 보드는 소프트웨어 검증 보드 4종, 하드웨어 검증 보드, 접촉식 카드 검증 보드, 비접촉식 카드 검증 보드 및 오류주입 검증 보드 3종을 지원하고 있다.

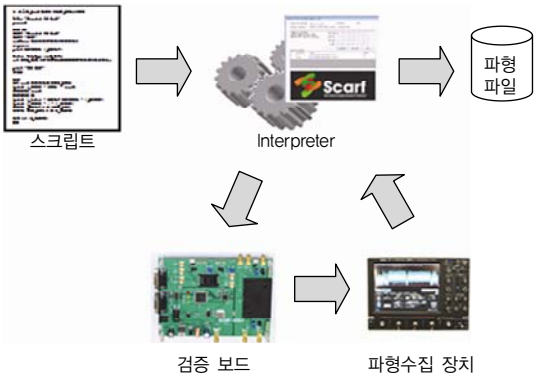
SCARF는 한번 분석된 결과를 프로파일 구조로 저장이 가능하고 읽어올 수 있는 구조로 되어 있어 하나의 프로파일을 보면 파형수집부터 전처리 및 결과에 이르는 모든 과정에 대한 내용을 쉽게 알 수 있어 쉽게 분석 기술의 전수 및 전달이 용이한 구조이다.



(a)

(b)

(그림 6) SCARF 구성(a)와 SCARF 분석 시스템 GUI(b)



(그림 7) SCARF 파형수집 과정

Ⅳ. 부채널 분석 시스템 구조

부채널 분석 시스템의 구조 및 상세 설계 내용 등은 논문으로 잘 발표되지 않는 관계로 ETRI에서 개발한 SCARF의 시스템 구조 및 설계 내용을 위주로 설명한다.

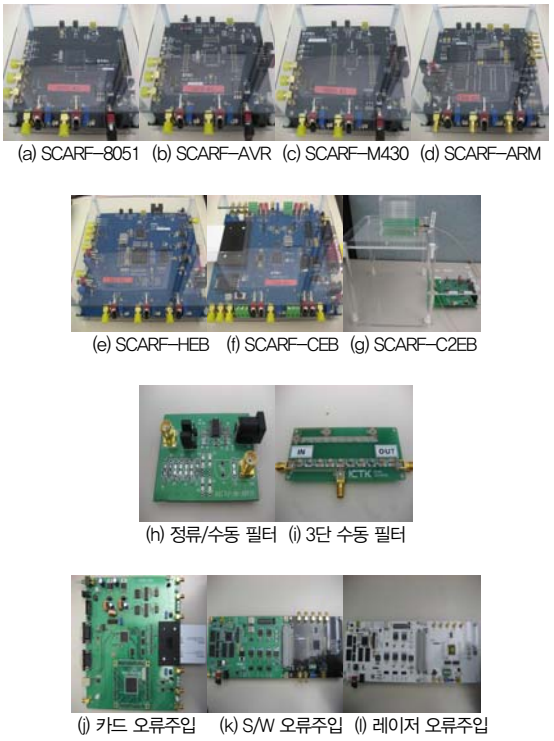
1. 파형수집 기능

파형수집은 부채널 분석에서 가장 기초적인 기능으로 SCARF에서는 (그림 7)과 같은 스크립트를 통해 파형수집 과정을 진행한다.

스크립트 기반의 파형수집 방식은 암호 모듈이 탑재되는 다양한 장치에 대한 접근 프로토콜이 다른 환경에서 매우 유용하다. SCARF 내부의 코드를 수정하는 것이 아니라 정해진 규칙대로 작성된 스크립트를 SCARF가 해석하고 동작시키면서 파형을 수집하는 방식이기 때문이다.

2. 검증 보드

암호 모듈이 탑재되거나 암호 모듈과 접촉/비접촉식으로 연결되어 검증 가능한 검증 보드는 수집되는 파형의 질에 중요한 영향을 끼친다. 검증 보드의 성능에 따라 수집되는 파형의 형태나 질이 다르며 이는 부채널 분석에 필요하게 되는 파형의 개수와 직결된다. 경우에 따라서는 분석이 안되거나 훨씬 많은 파형이 필요하게 될 때도 있다. 따라서, 부채널 분석이 용이하게 검증 보드를 제작할 수 있어야 한다. (그림 8)은 SCARF의 검증 보드들이다.

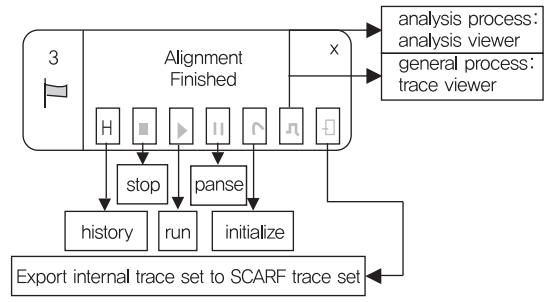

(a) SCARF-8051 (b) SCARF-AVR (c) SCARF-M430 (d) SCARF-ARM
(e) SCARF-HEB (f) SCARF-CEB (g) SCARF-C2EB
(h) 정류/수동 필터 (i) 3단 수동 필터
(j) 카드 오류주입 (k) S/W 오류주입 (l) 레이저 오류주입

(그림 8) SCARF의 부채널 검증보드

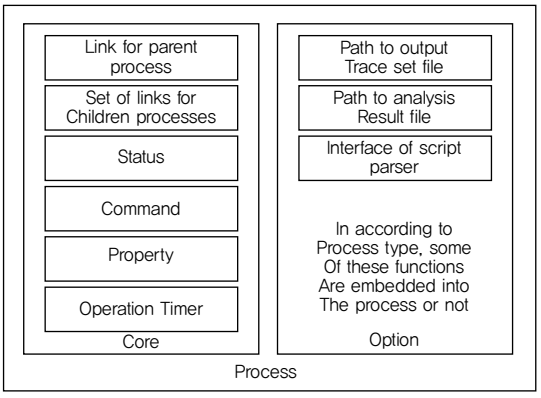
(그림 8)의 SCARF-8051, SCARF-AVR, SCARF-M430, SCARF-ARM(Advanced RISC Machine)은 소프트웨어 검증 보드로 소프트웨어로 개발된 암호 모듈이 각 프로세스에서 연산될 때 부채널 분석을 하기 위한 검증 보드들이다. SCARF-HEB는 하드웨어 개발되는 암호 모듈을 검증하기 위한 하드웨어 검증 보드다. 카드 오류주입 및 S/W 오류주입 검증 보드는 전압 및 클록을 가변시켜 오류를 주입할 수 있는 검증 보드들이다. 레이저 오류주입은 SCARF 레이저 장치를 이용하여 검증할 수 있다.

3. 프로세스

SCARF는 파형수집, 전처리 및 분석의 모든 기능들이 (그림 9)와 같은 프로세스 단위로 구성된다. 사용자는



(a)



(b)

(그림 9) SCARF 프로세스 GUI(a)와 프로세스 구조(b)[8]

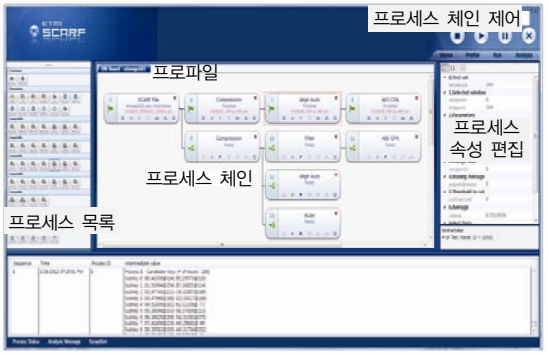
GUI상에 있는 프로세스 리스트에서 필요한 프로세스를 끌어다 프로파일 편집기에 놓고 해당 프로세스의 속성값들을 편집하고 구동시킬 수 있다.

4. 프로파일

SCARF의 프로파일은 프로세스 체인으로 보통 하나의 파형수집 프로세서와 다수의 전처리 프로세스 및 분석 프로세스 구성된다. 프로세스 안에 이미 각 속성값, 결과 파형, 분석 결과 등이 다 포함되어 있어 프로파일은 이런 프로세스의 연결 및 상태만 관리하면 된다.

(그림 10)과 같이 SCARF GUI에는 프로파일 창에 프로세스들로 구성된 프로세스들이 포함되어 있다. 한 프로세스를 클릭하면 우측에 해당 프로세스의 속성값들이 표시되어 속성값을 편집할 수 있다.

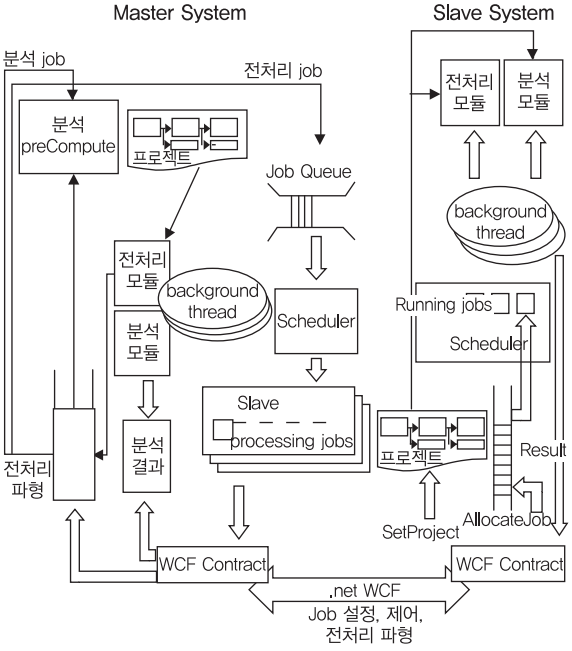
SCARF는 기존의 다른 부채널 분석 시스템과 다르게 부채널 분석이 프로세스로 구성된 프로파일 안에서 모두 이루어지고 프로파일이 복사 및 이동이 된다. 따라서 부채널 분석 노하우의 저장 및 전수에 장점이 있다.



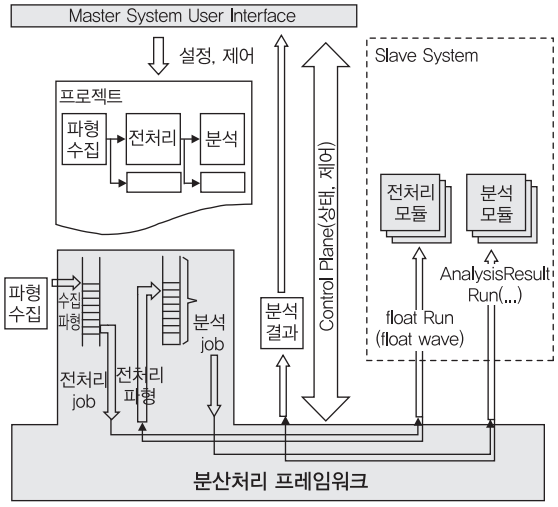
(그림 10) SCARF 프로파일 및 GUI 환경[8]

5. 분산처리 및 병렬처리

SCARF는 (그림 11)과 (그림 12)와 같은 구조로 한 프로파일 내의 다수의 프로세스가 동시에 구동하거나 또는 모든 프로세스를 구동시킬 수 있다. (그림 11)은 동시에 각 프로세스의 작업을 진행시키는 데 필요한 병렬처리의 구조를 (그림 12)는 빠른 병렬처리를 위한 분산



(그림 11) SCARF 분산처리 구조[9]



(그림 12) SCARF 병렬처리 구조[9]

처리 구조를 보여준다.

SCARF는 분산처리 없이 마스터 시스템만으로도 구성이 가능하며, 분산처리 시에는 하나의 마스터 시스템과 여러 대의 슬레이브 시스템으로 구성된다. 슬레이브 수가 증가할수록 각 프로세스의 동작이 고속화됨으로 가능하면 다수의 슬레이브 시스템을 연결하는 것이 좋음을 알 수 있다[10].

V. 맺음말

앞에서 설명한 바와 같이 부채널 분석 기술은 암호 모듈이 전자장치에 탑재되어 동작할 때 발생되는 전력 및 전자파 등을 통해 비밀키를 알 수 있는 매우 강력한 공격이다.

최근 몇 년 동안 급격히 증가하고 있는 스마트폰 및 스마트 센서 등의 스마트기기의 증가와 맞물려 인터넷 뱅킹 및 지급 결제 등 보안이 필요한 많은 부분이 생겨나고 있다. 하지만, 기존의 암호 및 보안 시스템이 이런 환경의 변화를 따라가지 못하면서 키 누출 위협성이 증대되고 있다.

이러한 스마트기기를 대상으로 키 누출 위협을 검증할 수 있는 부채널 분석 기술과 키 누출을 차단할 수 있는 부채널 분석 대응 기술의 개발이 시급하다.

용어해설

부채널 분석 암호 알고리즘이 장치 내에서 동작하는 동안에 장치의 전력이나 전자파 등의 부가 정보의 수집, 가공 및 통계적인 분석을 통해 키 정보를 추출해내는 매우 강력한 공격 방법 중 하나

부채널 분석 시스템 암호 모듈이 탑재되는 장치가 부채널 공격에 대해 안전한지를 사전 검증 및 시험할 수 있는 방법들을 제공

약어 정리

AES	Advanced Encryption Standard
ARIA	Academy-Research Institute-Agency
ARM	Advanced RISC Machine
CC	Common Criteria
CMVP	Cryptographic Module Validation Program
CPA	Correlation Power Analysis
CRI	Cryptography Research Inc
DEMA	Differential Electromagnetic Analysis
DES	Data Encryption Standard
DPA	Differential Power Analysis
DSA	Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
EM	Electromagnetic waves
EM	Electromagnetic Emission Attack
EMV	Electromagnetic Vulnerability
FA	Fault-injection attack
FIPS	Federal Information Processing Standard
HODPA	High Order Differential Power Analysis
IP	Intellectual Property
MDI	Multi-Document Interface
PA	Power Analysis Attack
RSA	Rivest-Shamir-Adleman
SASEBO	Side-channel Attack Standard Evaluation Board
SCA	Side Channel Attack

SCARF	Side Channel Analysis Resistant Framework
SEMA	Simple ElectroMagnetic Analysis
SPA	Simple Power Analysis
TA	Timing Attack

참고문헌

[1] P.C. Kocher, "Timing Attacks on Implementation of Diffe-Hellman, RSA, DSS and Other Systems," Proc. Adv. Cryptology, 1996, pp. 104-113.

[2] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," Proc. CRYPTO, 1999, pp. 388-397.

[3] J. Quisquater and D. Samyde, "Electromagnetic Analysis (EMA): Measures and Countermeasures for Smart Cards," Proc. e-Smart, 2001, pp. 200-210.

[4] Thomas S. Messerges, Ezzat A. Dabbish, Robert H. Sloan, "Examing Smart-Card Security under the Threat of Power Analysis Attacks," IEEE transactions on computer, vol. 51, no. 5, 2002.

[5] Cryptography Research. DPA Workstation TM. http://www.cryptography.com/technology/dpa-workstation.html

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

[7] Brightsight. Unique Tools from the Security Lab. http://www.brightsight.com/documents/marcom-materials/Brightsight_Tools.pdf

[8] J. Kim et al., "SCARF: Profile-based Side Channel Analysis Resistant Framework," Int. Conf. Security Manag., 2012, pp. 359-364.

[9] 김주한 , "사용자 중심의 부채널 분석 시스템 설계," 정보과학회논문지, vol. 19, no. 1, 2013.

[10] 오경희, "부채널 분석 고속화를 위한 분산처리 시스템에 관한 연구," NCS, 2011.