情 報 保 護 學 會 誌
第22卷 第8號, 2012. 12

# 금융IC카드에 대한 부채널분석 도구 비교 연구

최 찬 영*, 정 재 철**, 신 휴 근***

요 약

기존 마그네틱 카드의 보안성을 강화하기 위해 집적회로칩이 부착된 IC카드의 사용이 날로 증가하고 있으나 IC카드에 대한 보안 위협 또한 발생하고 있는 실정이다. 그 중에서도 암호화에 사용된 키를 찾기 위해서 암호 알고리즘의 이론적인 취약점이 아닌 암호화 과정에서 누설되는 수행시간, 소비전력, 전자기 방사 등을 이용하는 물리적 공격 방법인 부채널분석 공격이 대표적인 보안 위협이다. 본 논문에서는 부채널분석 공격 기법을 구현한 국내·외 시험 도구의 차이점 및 시험방법의 유효성을 확인하기 위해, 각 도구별 시험 결과를 전력분석 관점에서 비교·분석해 보았다. 시험 결과, 각 도구별 특징을 파악할 수 있었고, 시험 도구의 동작 방식에 다소 차이가 있으나 모두 동일한 결과를 도출해 낼 수 있었다.

## Ⅰ. 서 론

Kocher의 부채널분석 관련 논문 [1] 이 발표된 이후 부채널분석에 대한 관심이 증가하였고 국내·외에서 여러 시험 도구들이 개발되어 사용되고 있다. 본 논문에서는 현재 국내·외에서 사용되고 있는 부채널분석 도구들의 시험 방법 및 결과를 비교·분석하여 각 도구별 특징과 결과의 유효성에 대한 사례 검증을 하고자 한다.

부채널분석에는 전력분석, 전자기분석 및 오류주입 분석 등 여러 세부분야가 있으며 본 논문에서는 전력분석에 국한하여 시험하였다. DES, AES, SEED 등 여러 암호화 알고리즘이 부채널분석이 가능하다고 알려져 있으며 본 논문에서는 그 중 SEED에 국한하여 시험하였다.

본 논문의 구성은 다음과 같다. 2장에서는 부채널분석 기법 중 전력분석 방법에 대한 연구 방향을 살펴보고 3장에서는 국내·외에서 개발된 다양한 부채널분석 도구에 대해 살펴본다. 4장, 5장에서는 각각 국내·외 부채널분석 도구를 이용한 SEED 알고리즘 기반 금융IC카드 시험 방법 및 결과를 기술하고 마지막장에서는 시험 결과 요약 및 향후 과제를 기술하였다.

## Ⅱ. 이론적 배경

부채널분석 중 전력분석은 하드웨어로 구현된 암호 모듈의 동작 과정에서 누설된 전력 소비 신호의 통계적인 특성을 분석하여 비밀키를 알아내는 공격 방법으로, 1999년 Kocher의 연구 [2] 가 시초라 여겨지고 있다. Kocher의 연구 이후 여러 연구들이 부채널분석의 이론적 보완을 시도하였다. 이 후 2008년 SEED 알고리즘을 이용하여 구현된 금융IC카드를 대상으로 전력분석을 시험하여 취약성을 조사한 연구 [3] 가 있다.

이러한 이론적 배경 아래 개발한 암호화 알고리즘별 세부적인 시험방법은 다를 수 있으나 기본적인 시험 방법은 동일하다고 할 수 있다.

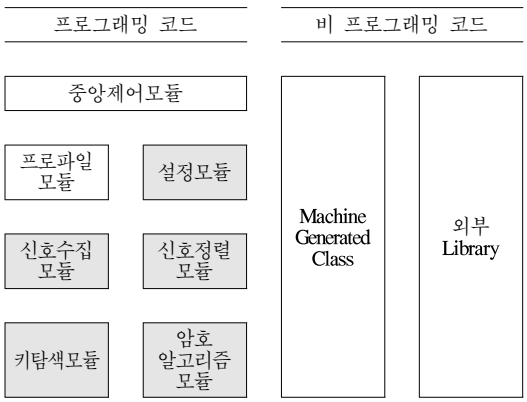
## Ⅲ. 시험도구 소개

본 논문에서 시험한 부채널분석 시험 도구는 아래와 같이 총 3개이다. 첫 번째 도구는 국가보안기술연구소(NSRI)에서 개발한 SCAP이며, 두 번째 도구는 한국전자통신연구원(ETRI)에서 개발한 SCARF, 마지막으로 네덜란드 Riscure社에서 개발한 Inspector이다.

* 금융결제원 금융정보보호부 (cchany@kftc.or.kr)
** 금융결제원 금융정보보호부 (vinbero@kftc.or.kr)
*** 금융결제원 금융정보보호부 (hkshin@kftc.or.kr)

### 3.1. 국가보안기술연구소의 SCAP

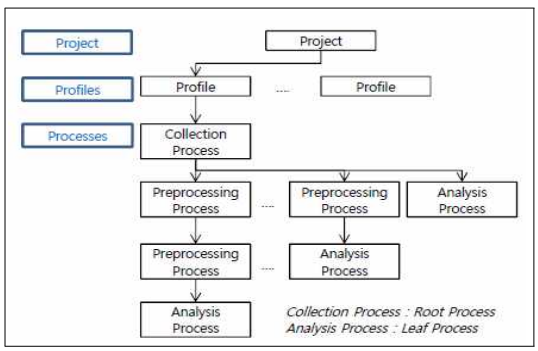
SCAP은 2008년 국가보안기술연구소 수행 연구[3]를 토대로 개발된 국산 부채널분석 도구로, DES, AES, ARIA, SEED등의 알고리즘들에 대한 전력분석(SPA/DPA)이 가능하다.




〔그림 1〕 SCAP 구성도

### 3.2. ETRI의 SCARF [4]

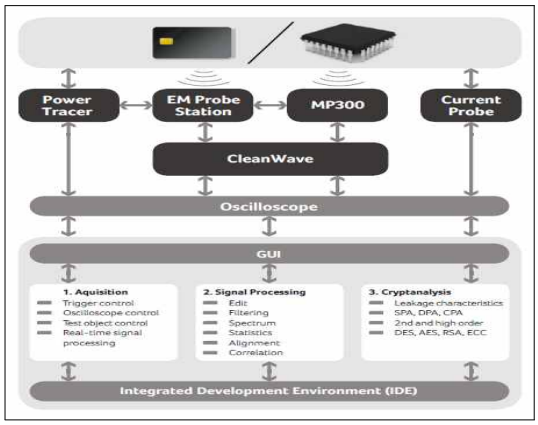
SCARF는 2009년 ETRI에서 개발한 프로파일 기반의 국산 부채널분석 도구로, 프로파일 정보(시험 단계 구성, 단계별 설정 등)를 기반으로 부채널분석이 수행되기 때문에 시험기관간 정보 공유에 유리한 측면이 있다.




〔그림 2〕 SCARF 프로파일 구조

### 3.3. Riscure社의 Inspector [5]

Inspector는 네덜란드 Riscure社에서 개발한 외산 부채널분석 도구로, 3-DES, AES, RSA, ECC, SEED등의 알고리즘들에 대한 전력분석(SPA/DPA)이 가능하다.




〔그림 3〕 Inspector 동작 구조

## Ⅳ. 도구별 시험분석

### 4.1. 시험 환경

각 도구의 시험방법은 신호수집, 신호정렬, 신호분석(중간값 계산, 키탐색)의 3단계로 구성되어 있어 기본적인 시험방법은 동일하다고 볼 수 있으나, 각 단계별 세부 설정사항에 일부 차이가 존재한다.

〔표 1〕 부채널분석 도구 시험단계

| | |
|---|---|
| 신호수집 | 소비전력신호 측정 |
| 신호정렬 | Pearson Correlation 기법을 이용한 신호정렬 |
| 신호분석 | S-box 출력의 해밍수를 고려한 행렬 계산, 수집한 소비전력신호와 S-box 출력간 상관계수 계산 및 키탐색 기능 수행 |

동 시험은 전력분석(SPA, DPA)을 통해 금융IC카드에 저장된 중요정보(암호화키)의 누출여부를 테스트하였으며, 동 시험을 위해 사용된 명령어는 표2, 표3과 같다.

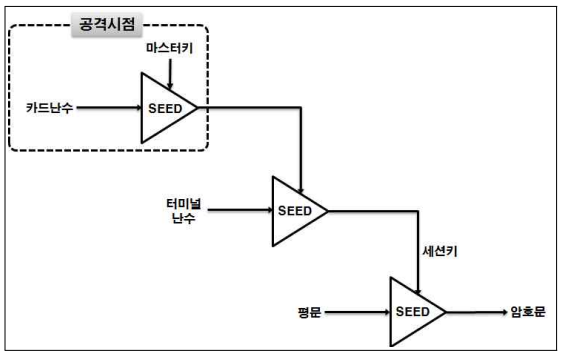
〔표 2〕 SELECT DF 명령어

| SELECT DF | | | | | | |
|---|---|---|---|---|---|---|
| CLA | INS | P1 | P2 | Lc | Data | Le |
| 00 | A4 | 04 | 00 | 07 | D4106509900010 | 변수 |

〔표 3〕 GET ENCIPHER 명령어

| GET ENCIPHER | | | | | | | |
|---|---|---|---|---|---|---|---|
| CLA | INS | P1 | P2 | Lc | Data | | Le |
| 90 | E4 | 00 | 81 | 변수 | 터미널난수 (16Byte) | 입 력 평 문 | 20 |

그림4는 금융IC카드에서 GET ENCIPHER 명령어를 이용한 세션키 및 암호문 생성과정을 설명하고 있으며, GET ENCIPHER 단계 중 첫 번째 SEED를 공격시점으로 한다.

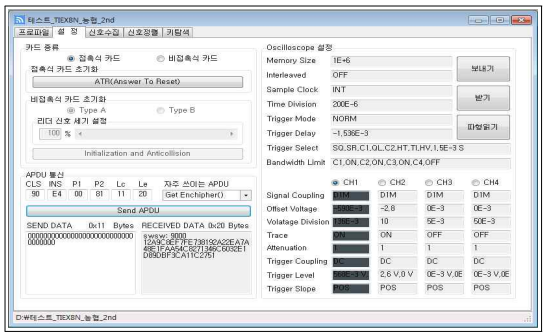



〔그림 4〕 GET ENCIPHER 명령어를 이용한 세션키 및 암호문 생성과정 [3]

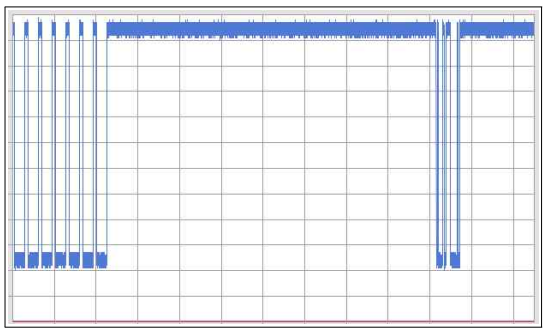
## 4.2. 도구별 시험방법

### 4.2.1 국가보안기술연구소의 SCAP

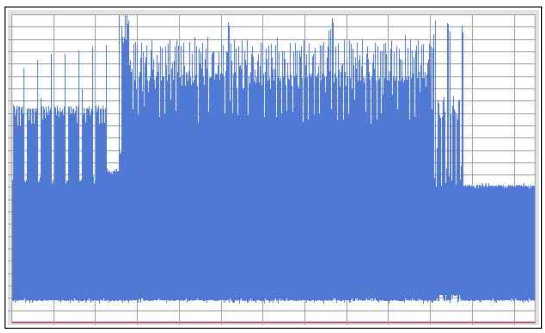
시험 단계별 설정화면이 그림5와 같이 탭으로 고정 구현되어 있다. 따라서 각 단계가 완료된 후 다음 단계로 진행이 가능하다. 신호수집시 수집범위 지정 기능을 제공하여 오실로스코프만으로 수집범위를 지정하는 것보다 편리하다. 수집신호는 신호별로 하나의 파일로 저장되며 신호정렬시 첫 번째 신호가 기준신호가 된다. 신호정렬시에 상관값이 낮은 신호는 분석 대상신호에서 제외할 수 있는 기능을 제공하여 보다 정확한 키탐색이 가능하다. 신호정렬시 정렬범위를 GUI로 정할 수 있어 직관적인 범위 지정이 가능하다. 키탐색시에도 키탐색범위를 다시 한 번 지정할 수 있게 하여 키탐색 시간을 단축할 수 있다.



〔그림 5〕 APDU 명령어 전송 UI

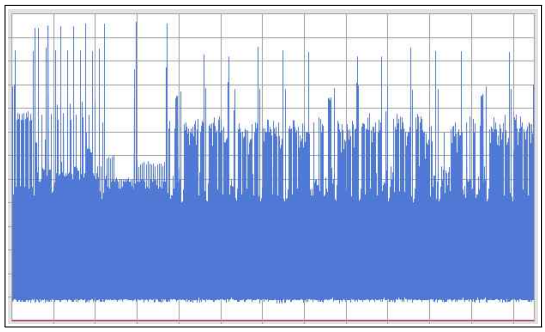


〔그림 6〕 입력 전력 신호



〔그림 7〕 SEED 알고리즘 전력 신호(3회)

〔그림 8〕 SEED 알고리즘 16라운드 전력 신호

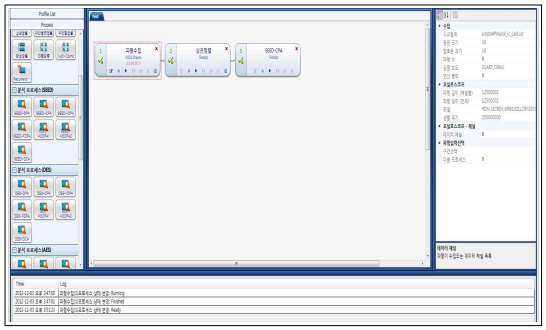


〔그림 9〕 SEED 알고리즘 1라운드 전력 신호

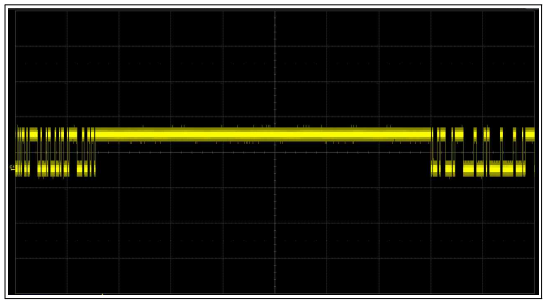
#### 4.2.2 ETRI의 SCARF

그림10과 같이 모듈별 시험단계 설정, 사용자 정의 모듈 추가를 통해 단계별 설정의 커스터마이징이 용이하다. 각 작업의 순서를 미리 지정하여 시험자 개입없이 신호수집부터 키탐색까지 가능하다.

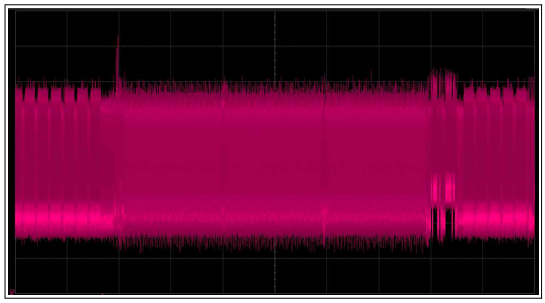
수집신호는 수집 중에는 메모리에 저장되며 수집 완료후 파일에 저장하여 수집시간을 단축하였다. 각 작업 단계가 병렬로 처리되는 기능이 제공되어 전체 분석시간을 단축할 수 있다. 다만, 신호정렬 결과를 시험자가 확인하지 않은 경우 키탐색 결과가 정확하지 않을 수 있다.



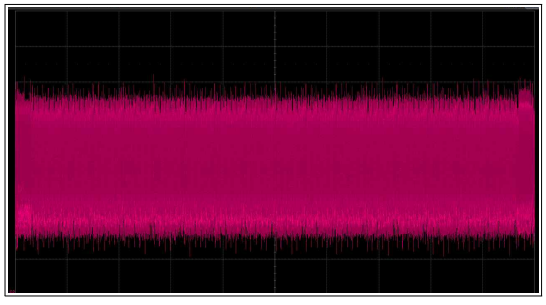
〔그림 10〕 프로파일 설정 UI



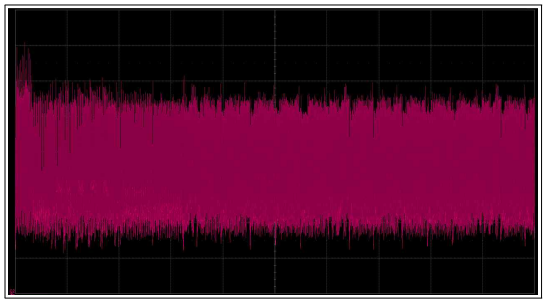
〔그림 11〕 입력 전력 신호



〔그림 12〕 SEED 알고리즘 전력 신호(3회)



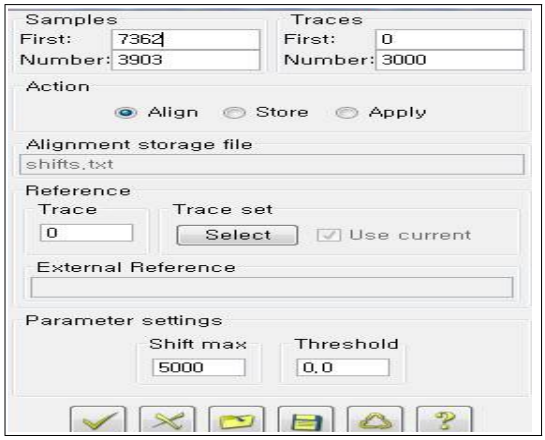
〔그림 13〕 SEED 알고리즘 16라운드 전력 신호



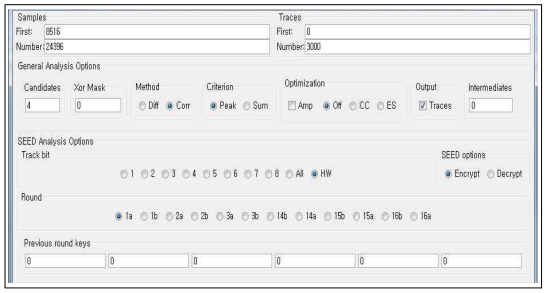
〔그림 14〕 SEED 알고리즘 1라운드 전력 신호

#### 4.2.3 Riscure社의 Inspector

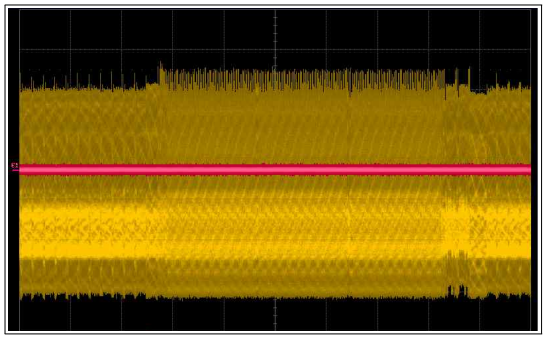
오실로스코프를 직접 제어할 수 있는 기능을 제공하며, 일부 설정(신호정렬, 신호분석 등)을 제외한 시험 전단계가 스크립트 형태로 구동되는 차이점이 있다.



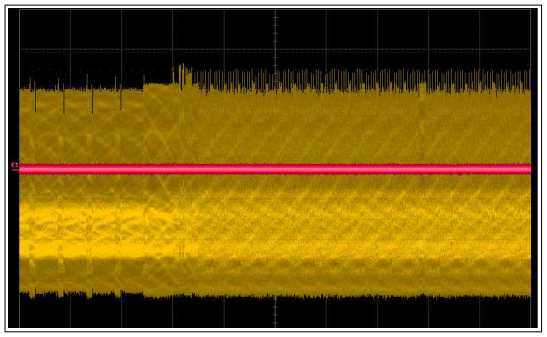

〔그림 15〕 신호정렬 UI



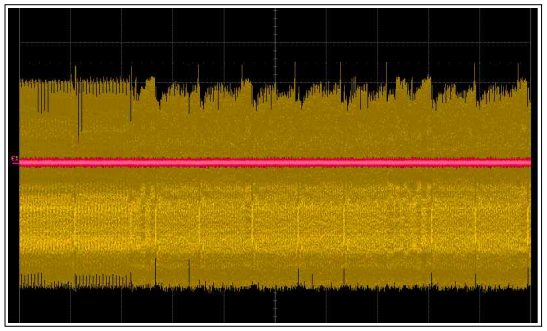
〔그림 16〕 신호분석 UI



〔그림 17〕 SEED 알고리즘 전력 신호(3회)



〔그림 18〕 SEED 알고리즘 16라운드 전력 신호



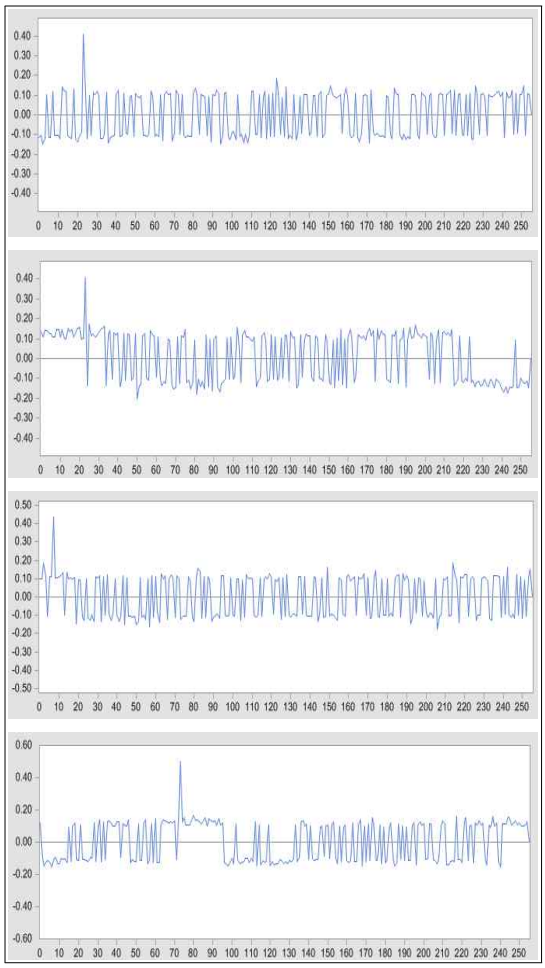
〔그림 19〕 SEED 알고리즘 1라운드 전력 신호

## Ⅴ. 도구별 시험결과

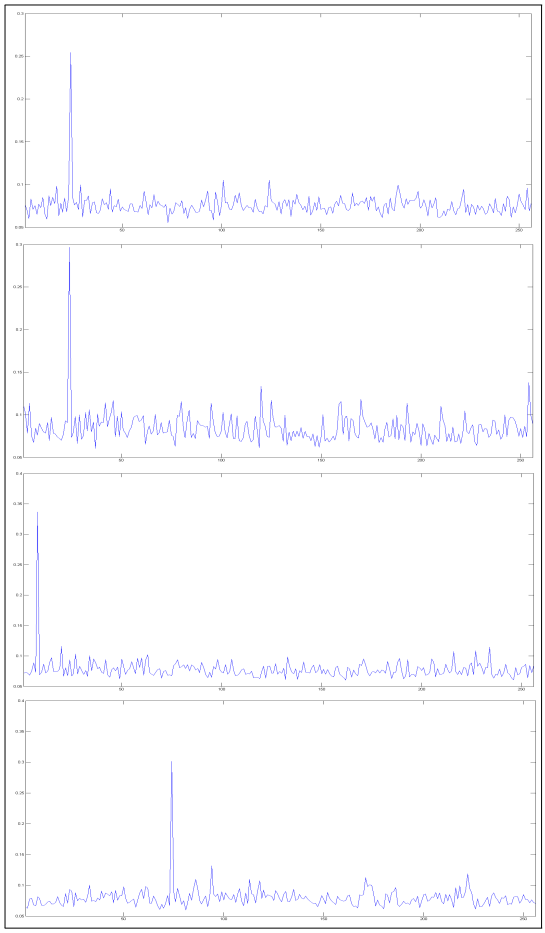
256개 Key값에 대한 전력신호값과 수집된 전력신호의 상관계수값 중 유일한 Peak값이 존재하면 키탐색이 성공한 것이다. 그림20, 21, 22와 같이 유일한 Peak값이 존재하므로 Key탐색이 성공했음을 알 수 있다.

다만, 상관계수값(Peak값)은 각 도구마다 조금씩 차이가 있었으며, 각 도구별 신호정렬의 정확성과 시험자의 능력과 숙련도에 따라 차이가 발생되었다고 추측되나 보다 많은 반복 시험과 분석이 있어야 정확한 원인을 파악할 수 있을 것이라 생각된다.

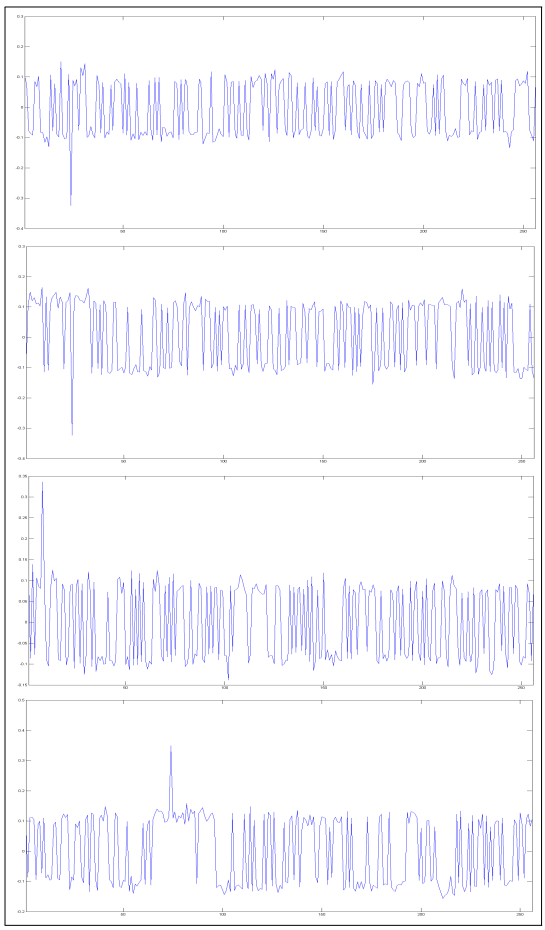
따라서 전력분석에 대한 각 도구의 시험성능은 크게 차이가 없음을 본 논문의 시험결과로 알 수 있다.



〔그림 20〕 SCAP Key 탐색 결과



〔그림 21〕 SCARF Key 탐색 결과



〔그림 22〕 Inspector Key 탐색 결과

## Ⅵ. 결론

본 논문에서는 SEED 알고리즘에 대한 부채널분석을 국내·외 여러 시험도구를 이용해 비교·분석하였다. 비교·분석한 결과 도구별 세부적인 시험방법에 차이가 있음에도 불구하고 3개의 시험도구 모두 동일한 결과를 산출하여 국내 도구들과 외산도구와의 성능에 차이가 없음을 알 수 있었다.

다만, 시험시 사용된 시료가 다양하지 않아 다양한 H/W, S/W 및 부채널분석 대응기법에 대한 성능은 검증되지 않았다. 따라서 향후 분석 시료, 암호화 알고리즘, 분석 및 대응기법 등을 다양화하여 성능을 비교한다면 보다 정확한 각 도구별 성능 비교 결과가 도출될 것으로 예상된다.

## 참 고 문 헌

[1] P.Kocher, “Timing Attacks on Implementations of Diffie-Hellman”, *CRYPTO'96*, pp. 104-113, 1996.

[2] P.Kocher, J.Jaffe, B.Jun, “Differential Power Analysis", *CRYPTO'99*, 1999.

[3] 김창균, 박일환, “금융IC카드에 대한 부채널분석공격 취약성 분석", *정보보호학회논문지 제18권 제1호*, pp. 31-39, 2008.2

[4] Juhan Kim, Kyunghee Oh, Dohoo Choi, Howon Kim, “SCARF: profile-based Side Channel Analysis Resistant Framework", *WorldComp2012*, 2012.7

[5] Riscure. Inspector - 부채널분석 도구 : http://www.riscure.com/benzine/documents/Inspector_brochure_screen.pdf

## 〈著者紹介〉

**최 찬 영 (Choi Chan Young)**
정회원
2002년 2월: 중앙대학교 컴퓨터공학과 졸업
2011년 5월: 카네기멜론대학교 정보보호학과 석사
2001년 12월~현재: 금융결제원 재직
<관심분야> 컴퓨터공학, 정보보호, 경영학

**정 재 철 (Jeong Jae Cheol)**
정회원
1995년 2월: 한양대학교 수학과 졸업
1995년 2월~현재 : 금융결제원 재직
<관심분야> 정보보호, 수학

**신 휴 근 (Shin Hyu Keun)**
정회원
2002년 2월: 아주대학교 정보및컴퓨터공학부 졸업
2004년 2월: 아주대학교 정보통신대학원 석사
2004년 3월~현재: 금융결제원 금융정보보호부 재직
<관심분야> 컴퓨터공학, 정보보호