# 비접촉 암호 분석용 루프 프로브 설계 및 전자파 신호 측정

# Loop Probe Design and Measurement of Electromagnetic Wave Signal for Contactless Cryptographic Analysis

최종균 · 김채영 · 박제훈 · 문상재

Jong-Kyun Choi · Che-Young Kim · Jea-Hoon Park · Sang-Jae Moon

## 요 약

본 논문은 스마트카드에서 방사되는 전자파를 이용한 암호 분석용 소형 루프 프로브 설계와 프로브에 유기된 전자파 신호의 분석에 관한 연구이다. 암호 분석용 프로브는 일반적인 전자장 측정용 프로브와는 다르다. 그 이유는 제시된 프로브의 목적은 암호 장비의 비밀 키 해독에 필요한 정보를 얻기 위함이기 때문이다. 스마트카드에서 발생된 파형을 분석하여서 전자파 공격을 시도하기 때문에 프로브에 유기된 전압의 파형과 IC 칩에서 발생된 파형은 가능한 한 서로 동일해야 한다. 그 목적을 위해서 전자파를 이용한 암호 분석, 신호원의 근사 모델링, 암호 분석용 프로브의 특징, 전자파 신호 측정 그리고 프로브의 교정에 대한 검토가 필요하다. 스마트카드 칩의 소비 전력 신호와 제안된 프로브를 이용한 전자파 신호를 측정하고 두 신호를 EMA의 관점에서 비교하였다. ARIA 알고리즘을 적용하여 제안된 비접촉 암호 분석용 프로브의 적합성 여부를 실험적으로 확인하였다.

## Abstract

In this paper, a study has been performed on the design of small loop probe and analysis of induced electromagnetic wave signal from a smartcard for contactless cryptographic analysis. Probes for cryptographic analysis are different from conventional EM probes, because the purpose of proposed probe is to obtain the information for secret key analysis of cryptographic system. The waveform of induced voltage on probe must be very close to radiated waveform from IC chip on smartcard because electromagnetic attack makes an attempt to analyze the radiated waveform from smartcard. In order to obtain secret key information, we need to study about cryptographic analysis using electromagnetic waves, an approximate model of source, characteristic of probe for cryptographic analysis, measurement of electromagnetic waves and calibration of probes. We measured power consumption signal on a smartcard chip and electromagnetic wave signal using proposed probe and compared with two signals of EMA point of view. We verified experimently the suitability of the proposed small loop probe for contactless cryptographic analysis by applying ARIA algorithm.

Key words : Loop Probe, Electromagnetic Wave, Cryptographic Analysis, Smartcard, Secret Key

## Ⅰ. 서 론

정보 통신의 발달로 인해 스마트카드, 센서 시스템 및 RFID 시스템 등의 중요도가 증가되고 있다. 이러한 시스템들의 여러 특징 중 하나는 정해진 시스템 내에서만 정보를 전달할 수 있도록 보안용 비밀 키를 사용한다는 점이다. 보안용 비밀 키는 다양한 방법으로 분석이 가능하기 때문에 정보 보호를 위해서는 분석 방법을 파악하고, 이에 대한 대처 방안을 마련해야 한다. 부 채널 공격(Side Channel

「이 논문은 BK21에서 지원하였음.」

경북대학교 전자전기컴퓨터학부(School of Electrical Engineering and Computer Science, Kyungpook National University)

· 논 문 번 호 : 20070612-063

· 수정완료일자 : 2007년 8월 24일

Attacks)은 저 전력형 정보 보호 관점에서 최근에 도입된 강력한 공격 방법이며, 미국 FIPS 140-1, 2, 3 CMVP 암호 모듈에서 중요한 평가 요소로 분류되어 있고, 공격/방어 기술의 발전에 따라 평가기준이 지속적으로 개선되고 있는 중이다. 부 채널 공격 기법으로는 시차분석, 전력 분석, 오류 주입, 전자파 분석 등이 있다[1],[2]. 부 채널 공격의 일종인 EMA(ElectroMagnetic Analysis)는 전자파 분석을 통해 비밀 키를 분석하는 방법으로 2001년 Gemplus팀에 의해 처음 소개되었다[3]. EMA는 크게 Simple EMA와 Differential EMA로 분류된다. Simple EMA(SEMA)는 측정된 전자파를 직접 분석하여 공격 대상 암호 장치의 비밀 정보를 알아내는 공격법이며, Differential EMA(DEMA)는 공격 대상으로부터 측정된 전자파 신호를 통계적인 방법과 에러 정정 기법 등을 사용해서 분석하며, 공격 대상 내부에서 연산되는 암호 알고리즘의 비밀 키를 유추하는 공격 방법이다. 저 전력 보안 장치에 대한 EMA는 대상물을 분해하지 않고도 암호 분석이 가능하기 때문에 보안 시스템이 고려된 설계가 필요하지만, 보안이 고려되지 않은 대다수의 장비는 전자파 분석 공격에 노출되어 있는 실정이다. EMA는 근거리와 원거리 측정을 통해 할 수 있다. 근거리 측정은 미소 루프나 다이폴 형태의 소형 프로브를 사용하고 원거리 측정은 지향성과 이득이 큰 안테나를 사용한다. 일반적인 전자장 측정용 프로브는 전자파 신호의 물리적인 방사량 측정이 주요 목적이지만, 암호 분석용 프로브는 방사된 전자파의 파형이 프로브 성능 평가의 기준이 된다. EMA는 비접촉식 방법으로 암호를 해독할 수 있으므로 보안 시스템에서 치명적인 정보가 유출될 수 있다. 국내에서는 최근 전력 분석 공격이나 오류 분석 공격 등에 대한 연구가 일부에서 진행되고 있으나, EMA에 대한 연구 결과는 드문 실정이다. 본 연구에서는 스마트카드에서 방출되는 전자파 신호의 특성을 이해하고 이에 적합한 루프 프로브를 제작하였으며, 측정된 신호가 EMA에 사용 가능한지를 알아보기 위해 스마트카드에서 방사되는 전자파를 측정을 통해 분석하였다.

## Ⅱ. 전자파를 이용한 암호 분석

### 2-1 DEMA 공격 방법

1. 공격 대상 알고리즘을 임의의 입력(Pi)과 추측한 비밀 키(K)를 이용해서 시뮬레이션한 후, 계산된 중간 값의 해밍웨이트를 바탕으로 Pi를 분류한다.
2. 분류된 Pi를 입력으로 대상 알고리즘을 수행하여 전자파를 측정한다.
3. 측정된 전자파 신호(Ti)들을 분류 함수 D를 이용하여 분류한다.
   T0={Ti|D(K, Pi)=Low Hamming weight}
   T1={Ti|D(K, Pi)=High Hamming weight}
4. 분류된 두 전자파 집합을 차분하여 추측한 비밀 키를 확인한다.

그림 1. DEMA 공격 과정
Fig. 1. Process of DEMA attacks.

DEMA 공격은 측정된 전자파 신호의 크기가 공격 대상 내부에서 연산되는 데이터의 해밍 웨이트(hamming weight)에 비례한다는 해밍 웨이트 가정을 바탕으로 한다. DEMA 공격은 그림 1의 순서대로 적용되며 추측한 비밀 키(key)가 틀린 경우에는 다른 키를 가정하여 공격 절차를 반복한다.

### 2-2 스마트카드의 EMA 특징

본 연구에서 전자파 공격은 스마트카드의 보안용 비밀 키 해독을 목적으로 실시되었다. 스마트카드는 집적 회로 기억 장치(IC memory)와 중앙 처리 장치(CPU)를 탑재한 반도체 칩을 이용해 은행이나 각종 인증 시설 그리고 보안 카드 등에 사용되고 있다. 스마트카드의 필수 요소들 중 하나인 보안 정보는 원하는 대상 이외에는 해독이 불가능하도록 설계가 되어야 하나, 정보 통신과 암호학 등의 발달로 인하여 보안을 위한 비밀 키가 해독되는 사례가 보고되고 있다[1]~[3]. 스마트카드에서 방사되는 전자파는 크게 신호(signal) 성분과 잡음(noise) 성분으로 구분할 수 있다. 여기서 신호 성분은 암호 알고리즘을 검출하기 위해 필요로 하는 정보가 담긴 신호인데, 스마트카드 칩 동작시 발생된 전류의 변화량이나 칩 구동에서 발생하는 신호 성분 등을 말한다. 관측된 정보를 신호와 잡음으로 구분하는 기준은 비밀 키를 풀기 위해 필요한 정보와 불필요한 정보로 나눌 수 있다. 스마트카드 칩 동작은 지속적인 자속의 변화를 가져오고 루프 프로브와 오실로스코프 등을 이용해 자장(magnetic field)에 기인된 유기 전압을 측정하면 암호 키를 분석할 수 있다. 따라서 칩에서 방사되는

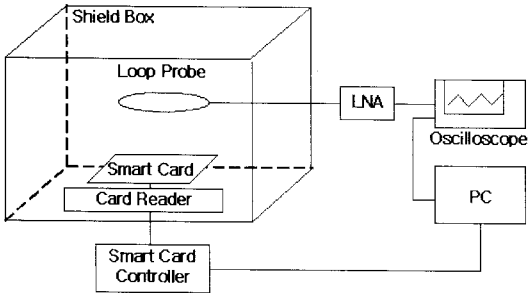



그림 2. EMA 측정 시스템
Fig. 2. EMA measurement system.

자장을 신호성분으로 정의하고, 전장(electric field) 및 인접 장비에서 방사되는 성분은 잡음으로 분류하였다.

### 2-3 측정 시스템

스마트카드에서 방사되는 전자파는 미약한 소신호이다. 따라서 측정은 정밀히 이루어져야 하고, 외부 전자파를 차단하는 쉴딩 박스 내에서 측정하는 것이 효과적이다. 측정 장비의 구성 및 연결은 그림 2와 같다. 루프 프로브에 유기된 미소한 전압은 저잡음 증폭기(low noise amplifier)를 통해 증폭되고 오실로스코프(oscilloscope)에 입력된다. 오실로스코프는 데이터 신호를 PC에 전송하고, PC 소프트웨어(software)를 이용하여 오실로스코프와 스마트카드의 주변 장치 제어 및 신호 분석을 수행한다.

## Ⅲ. 근거리 자계 프로브

### 3-1 신호원의 근사 모델링

도체 루프는 자장의 발생원과 탐침용으로 각각 사용된다. 원형 루프는 루프 면을 관통하는 자속의 변화량을 유기된 전압의 형태로 관측할 수 있도록 해 준다.

그림 3은 스마트카드에서 파장에 비해 대단히 작은 루프에 의한 방사로서 간주한 모델이다. 그림 3에서 $\overline{R}$은 신호원과 관측점 사이의 거리 벡터이다. 그리고 $b$는 원형 루프의 반지름이며, 점 $P$는 관측점이고, 원점에서 관측점까지의 거리는 $z$이다. 루프는 Biot-Savart의 법칙을 사용하면 관측점 $P$에서의 자속

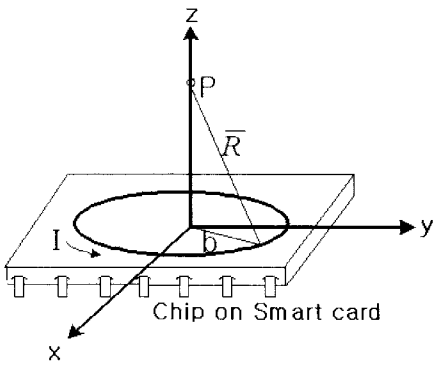



그림 3. 신호원 근사 모델
Fig. 3. An approximate model of source.

밀도인 벡터 $\overline{B}$를 구할 수 있다[4]. 신호원으로부터 관측점 $P$가 먼 지점에 위치할 경우에는 근사식 (1)이 얻어진다.

$$\overline{B} = \frac{\mu_0 I b^2}{2z^3}\hat{z} \tag{1}$$

루프가 아닌 선 전류원의 경우에는 거리에 반비례하게 된다. 스마트카드에서 발생되는 자장은 다양한 형태로 방사되기 때문에 배선의 위치, 길이, 크기 그리고 모양 등이 가변적이고 얼마나 많은 신호 발생원이 존재하는지는 추측하기 어렵다. 하지만 식 (1)을 통해서 관측점과의 거리와 측정 위치가 중요함을 알 수 있다.

### 3-2 자장과 전장의 비(比)

수신 프로브로 사용되는 루프에는 자장(magnetic field)만 유기되는 것이 아니라 전장(electric field)도 동시에 유기된다. 루프에 유기된 자장 성분이 전장 성분보다 크기 때문에 종종 전장 성분에 대한 응답은 무시된다. 하지만, 루프 프로브의 크기가 일정할 경우에는 주파수가 높아짐에 따라 루프에 유기된 자장과 전장의 상대적인 차이는 감소하게 된다. EMA를 수행함에 있어서 전장 성분은 2-2절에서 정의된 바와 같이 잡음으로 분류하였으므로 측정된 신호 중 전장으로 인해 유기된 전압은 제거되어야 한다.

그림 4는 수신을 위한 소형 루프 안테나이다. 전기적으로 소형 수신 루프는 $2\pi b \leq \lambda$이며, $b$는 루프의 반지름이고, $\lambda$는 자유 공간에서의 파장이다. $a$는 원

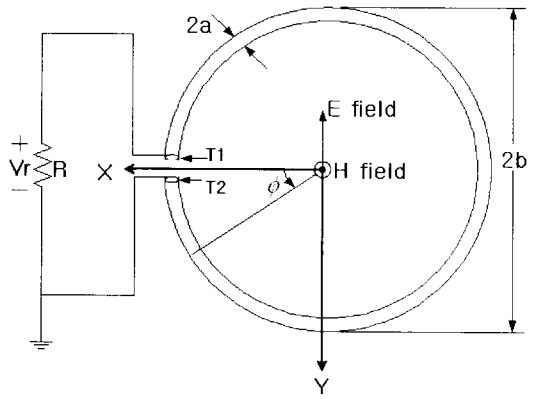



그림 4. 수신 소형 루프 안테나
Fig. 4. Receiving small loop antenna.

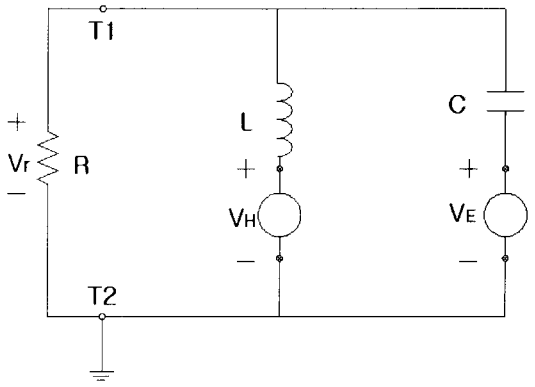



그림 5. 수신 소형 루프 안테나의 등가 회로
Fig. 5. Equivalent circuit of receiving small loop antenna.

형 루프를 만든 도선의 반지름이다. 안테나에 입사되는 평면파의 자장과 전장은 수신 루프에 최대 전류를 흐르게 하는 상태라고 가정하였다. 이때 입사된 자장 $H$는 루프가 놓여 있는 면에 수직이고, 입사된 전장 $E$는 루프의 면과 평형하고 파의 벡터 방향은 루프의 직경을 따라서 T1 점과 T2 점을 지나게 된다. 루프 안테나는 2가지 모드로 동작한다. 안테나를 다루는 방법은 먼저 전기적 응답(다이폴 응답)을 고려하고, 다음으로 파장에 비해 대단히 작은 루프 안테나($2\pi b \ll \lambda$)의 경우에 적용되는 것처럼 이상적인 자기적 응답만을 고려한다. 루프 안테나에 흐르는 총 전류 $I(\phi)$는 근사적으로 다이폴 모드의 전류 $I_d$와 루프 모드의 전류 $I_l$의 합과 같다. 다이폴 모드의 전류 $I_d$는 $\phi = \pm \pi/2$ 지점에서 상쇄된다. 예를 들어 $-\pi/2 \le \phi \le \pi/2$의 구간에서 반시계 방향으로 전류가 흐르는 경우에 $\pi/2 \le \phi \le 3\pi/2$의 구간에서는 시계 방향으로 전류가 흐르게 된다. 이는 동일한 위상(phase)을 가진 전류가 루프에 대칭하여 흐르는 것을 의미하고, 병렬 구조로 이루어진 두 개의 배열 다이폴과 같다. 반면에 루프 모드의 전류 $I_l$은 $\phi$와는 무관하게 시계 방향이나 반시계 방향인 단 방향으로 전류가 흐르게 된다. 이때, 루프의 등가 회로는 그림 5와 같이 나타낼 수 있고, 등가 회로의 $L$, $C$ 성분은 다음과 같다[5],[6].

$$L = \mu_0 b[\ln(8b/a) - 2] \tag{2}$$

$$C = \frac{2\varepsilon_0 b}{[\ln(8b/a) - 2]} \tag{3}$$

그림 5에서 $V_E$는 전장으로 인해 유기된 전압이고, $V_H$는 자장으로 인해 유기된 전압이며, $V_r$는 부하 저항 $R$ 양단의 전압이다. 저 주파수에서 동작하는 루프 안테나는 용량 성분이 매우 작기 때문에 다음 식이 성립한다.

$$\frac{1}{\omega C} \gg \omega L \tag{4}$$

식 (5)은 전장에 의해 유기된 등가 전압원이고[5], 식 (6)은 자장에 의해 유기된 등가 전압원이다.

$$V_E = -\pi b E \tag{5}$$

$$V_H = -j\omega\mu_0 H \cdot \pi b^2 \tag{6}$$

여기서 $E$와 $H$는 입사된 전장과 자장이다.

부하 저항 $R$ 양단의 전압은 $V_{rH}$와 $V_{rE}$이고, 비를 취하면 다음과 같다[5].

$$\frac{V_{rH}}{V_{rE}} = \frac{-j}{4\pi\varepsilon_0} \cdot \frac{1}{bf} \cdot \frac{H}{E} \tag{7}$$

여기서 $V_{rH}$는 자장으로 인해 유기된 등가 전압원에 의한 부하 저항 $R$ 양단의 전압이고, $V_{rE}$는 전장으로 인해 유기된 등가 전압원에 의한 부하 저항 $R$ 양단의 전압이다. 전장과 자장의 응답의 비는 부하 저항 $R$의 값과 무관하다[5]. 그 이유는 부하 저항인 $R$의 값이 변하면 $R$ 양단의 전압 $V_{rE}$와 $V_{rH}$도 변하게 되지만 비를 취하게 되면 상대적인 두 성분의 비는 일정하게 유지되기 때문이다. 자유 공간에서 특성 임피던스는

$$\frac{E}{H}=\sqrt{\frac{\mu_0}{\varepsilon_0}}=377\Omega \tag{8}$$

이고, 식 (8)에 의해 식 (7)은 다음과 같다[5].

$$\left|\frac{V_{rH}}{V_{rE}}\right|=\frac{c}{4\pi}\cdot\frac{1}{bf} \tag{9}$$

여기서 $c$는 진공에서의 빛의 속도이다. 측정에 사용된 루프는 계측 장비에 연결되고, 이는 그림 4와 5에서처럼 안테나의 T1 점 또는 T2 점이 접지(ground)된 것을 의미한다. 루프와 접지가 연결된 경우에는 접지로 인한 영향을 고려해야 한다. 따라서 평형 모드(balanced mode)와 불평형 모드(unbalance mode)의 개념을 도입하였다. 평형 모드는 접지와 분리된 루프만으로 구성된 모드이고, 불평형 모드는 루프로 구성된 하나의 도체와 접지가 결합된 모드이며, 두 모드를 중첩하면 원문제로 귀착된다[7]. 그림 5에서 루프 자체의 등가 회로는 평형 모드 하에서 추출된다. 반면 접지와 연결된 루프는 불평형 모드이다. 평형 모드의 등가 회로에서 불평형 모드를 적용하고자 한다면, 평형 모드에서 얻어진 용량 $C$의 두 배로 가정된 용량 $C$에 의해 등가로 처리할 수 있다. 루프만을 고려하였을 경우, 원하는 전장의 제거 비를 20 [dB]로 가정하면 주파수 범위는 식 (10)으로 주어진다[5].

$$f_{MHz}\leq 120/b_{cm} \tag{10}$$

단, $f$는 [MHz] 단위이고, $b$는 [cm] 단위이다.

식 (10)을 이용하면 제한된 주파수내에서 전장 성분에 의해 유기된 전압을 제거하기 위한 루프 프로브의 반지름을 결정할 수 있다.

### 3-3 암호 분석용 루프 프로브 설계시의 고려사항

암호 분석을 위한 프로브는 일반적인 전자장 측정용 프로브와는 다르다. 예를 들어 EMI/EMC 측정용 프로브는 측정 대상에서 방사되는 전자파의 신호 레벨이 중요한 의미를 갖는데, 이는 방사된 전자파의 양이 측정의 기준이 되기 때문이다. 반면에 암호 분석용 프로브는 암호 장비에서 방사되는 신호의 물리적 양보다는 암호 키 해독을 위한 정보를 제공하는 파의 형상을 관측하기 위한 용도로 사용된다. 전자 장비에서 의도적으로 방사되거나 누설되는 전자파의 근거리 측정을 위해 다양한 형상을 가진 루프 프로브가 많은 연구자들에 의해 개발되었으며, 여러 분야에 사용되고 있다. 4장의 실험을 통해 보이겠지만 제작된 다수 개의 루프 프로브를 사용한 결과, 본 연구의 목적인 스마트카드의 암호분석을 위한 전자파 측정에는 한계를 보였다. 그 이유는 DEMA 공격 시 측정된 전자파 신호의 크기는 데이터의 해밍 웨이트(Hamming weight)에 비례하여야 하나, 신호의 정확도가 낮아서 추측한 비밀 키가 올바른 키인지 확인하기 어렵기 때문이다. 암호 분석용 프로브는 측정 대상물에서 직접 접촉하여 얻는 소비 전력 신호(power consumption signal)를 대신하여 유기된 전압 형태의 전자파 신호(electromagnetic wave signal)를 제공하는 매개체 역할을 한다. 그러므로 소비 전력 신호와 전자파 신호 사이의 상관성(相關性)을 높이기 위한 연구가 수행되어야 한다.

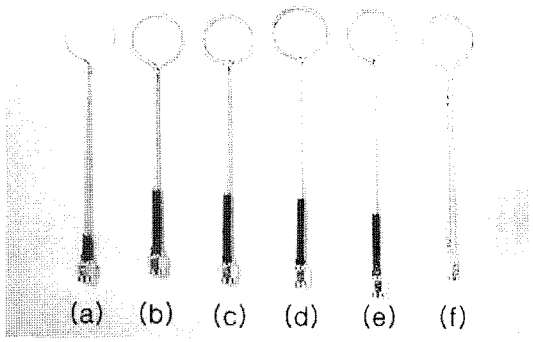
## Ⅳ. 프로브 제작 및 전자파 신호 측정

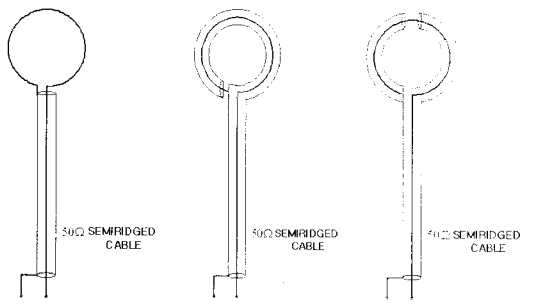
### 4-1 프로브 제작 및 측정

프로브는 그림 6과 같이 모두 여섯 가지 종류로 제작하였다. 이때 50 [Ω] SMA 세미리지드(semi-rigid) 케이블을 사용하였고, 안테나는 스마트카드 칩의 크기와 주파수에 따른 전장과 자장의 비를 고려해 전장으로 인해 유기된 전압을 제거하기 위하여 루프 직경을 약 2.5 [cm]가 되도록 제작하였다. 쉴드 구조의 루프는 전장을 비롯한 잡음 성분의 차단을 위해 사용하였다.

그림 2와 동일한 측정 환경을 구축한 다음, 제작된 다수 개의 루프 프로브를 사용하여 스마트카드 칩에 대한 측정을 수행하였다.

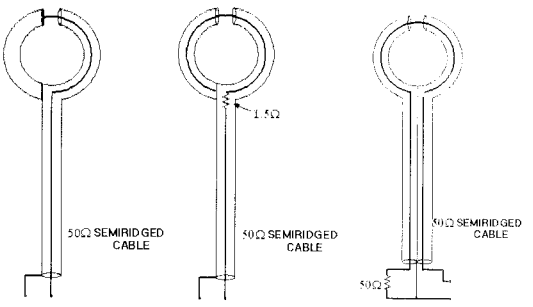
그림 7은 쉴딩 박스 내부의 실제 측정 모습이다. 오실로스코프는 LeCroy사의 LT374M 모델이며, LNA의 이득(gain)은 30 [dB], 잡음지수(noise figure)는 4.5 [dB]이다. 측정용 스마트카드는 32 bit CPU, 160 K bytes ROM, 64 K bytes EEPROM, 6.5 K bytes ststic RAM 그리고 데이터 보안을 위한 하드웨어와 소프트웨어 등으로 구성되어 있다. 오실로스코프의 한 채널은 스마트카드에 직접 연결되어 소비 전력을 측정하고, 다른 채널은 루프 프로브에 유기된 전자파 신호를 관측한다. 측정 시 루프의 위치는 결과에




(a) 일반 루프 (b) 아래쪽 중앙에 갭이 있는 쉴드 루프 (c) 위쪽 중앙에 갭이 있는 쉴드 루프

(a) Bare loop (b) Shielded loop with gap of below center (c) Shielded loop with gap of upper center




(d) 루프의 반이 도체로 구성된 쉴드 루프 (e) 갭의 반대편에 1.5 [Ω] 저항을 가진 쉴드 루프 (f) 발란스 쉴드 루프

(d) Shielded loop with conductor of half the loop (e) Shielded loop with 1.5 [Ω] resistor opposite gap (f) Balanced shielded loop

그림 6. 시험한 루프 프로브
Fig. 6. Tested loop probes.

큰 영향을 주므로 파형을 관측하여 가장 적합한 위치를 선정하였다. 위치선정 후에는 루프가 움직이지 않도록 루프 지지대를 단단히 고정하였다.

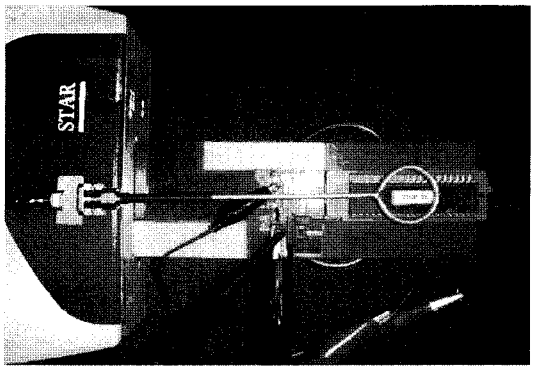



그림 7. 루프 프로브를 이용한 전자파 신호 측정
Fig. 7. Measurement of electromagnetic wave signal using a loop probe.

### 4-2 프로브의 교정

아래 순서대로 루프 프로브를 교정하였다.

① 신호 측정을 통해 소비 전력 신호와 전자파 신호 비교
② 파형의 일치 여부 확인
③ 만약 파형이 일치한다면 종료, 일치하지 않는다면 다음 방법을 수행
④ 그림 4의 프로브로 ①~③번 과정 수행
⑤ 루프의 임피던스 측정을 통한 공진 회로 구성 후 파형 확인
⑥ 부하를 이용한 low Q 회로 구성 후 파형 확인

본 실험에서 스마트카드 칩에 대한 EMA는 ①~④번 과정까지 만족할 만한 결과를 얻지 못하였다. ④번 과정에서 그림 5에서 보인 6개의 프로브를 사용하였지만, 프로브의 형상만으로는 소비 전력 신호와 유사한 전자파 신호의 파형을 얻을 수 없었다. 따라서 암호 분석에 적합한 파형을 얻기 위해서 제작된 프로브에 ⑤번 과정의 공진 회로와 ⑥번 과정의 low Q 회로를 추가하였다. 그림 8에서 소비 전력 신호는 전력 분석 공격시 사용하는 파형으로 스마트카드 칩에 직접 접촉하여 얻은 신호이며, 전자파 신호는 제작된 루프 프로브를 이용하여 측정된 신호이다. 그림 8의 가장 위쪽에 위치한 신호는 오실로스코프로 관측한 파형으로 ④번 과정까지의 결과이다.

그림 8의 교정 전 파형의 측정은 그림 6의 (c)번 안테나를 이용한 것이지만 (a)번, (b)번 그리고 (d)~(f)번 안테나에 유사한 파형이 관측되었다. 따라서 실험에 사용된 스마트카드 칩은 3.5 [MHz]의 동작 주파수이므로, 특정 주파수의 신호를 측정하고자 루프의 $L$을 실험적으로 구하였다. 그 후 식 (11)로 계산된 용량 $C$를 루프 프로브의 후단에 병렬로 연결하여 ⑤번 과정을 수행하였다.

$$C = \frac{1}{4\pi^2 f^2 L} \tag{11}$$

3-2절에서 언급한 것과 같이 저 주파수에서 소형 루프 안테나는 용량 성분이 대단히 작기 때문에 안테나 자체의 인덕턴스 성분으로 인한 위상차는 발생하게 된다. 따라서 식 (11)를 이용한 용량 $C$를 추가함으로써 ①~④번까지 수행된 결과보다 위상이 앞선 부분을 개선할 수 있었다. 실험에 사용된 스마트카드는 동작 주파수뿐만이 아니라 넓은 대역에 걸쳐 전자파가 방사되는데, 그림 8의 교정 전 전자파 파형을 분석해 보면 특정 주기에서 측정된 신호의 레벨이 낮아지는 것을 통하여 확인할 수 있다. ⑤번 과정에서 제작된 회로의 후단에 직렬로 부하를 추가로 구성하여 부하 값을 가변한 ⑥번 과정의 실험은 Low Q 회로를 이용하여 프로브의 측정 대역폭을 넓히는 역할을 한다. 실험 결과 ⑥번 과정을 통하여 부분적인 파형의 보정이 가능하였다.

그림 8의 가장 아래쪽에 위치한 파형은 그림 6의 (c)번 프로브를 이용하여 제안된 교정 절차를 수행한 결과이다.

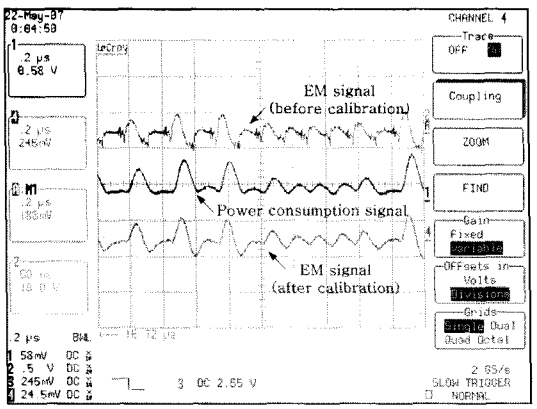


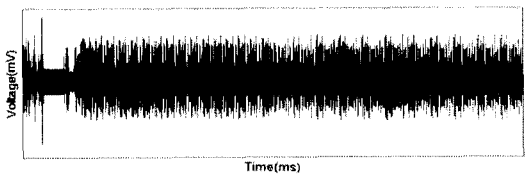

그림 8. 소비 전력 신호와 비교한 교정 전·후의 전자파 신호

Fig. 8. Power consumption signal vs. EM signal of before and after calibration.

두 변량 사이의 상관관계의 정도를 나타내는 수치인 상관 계수(correlation coefficient)를 $r$로 표현하였을 경우에 양의 상관관계인 $0 \leq r \leq 1$의 범위에서 1은 완전 상관, 0은 무상관이 된다. 소비 전력 신호와 전자파 신호의 상관 계수는 오실로스코프에 측정된 수치를 이용하여 산출하였다. 그림 8의 교정 전파형의 상관 계수는 $r=0.18$이고 교정 후, 파형의 상관계수는 $r=0.68$이다. 따라서 교정 전에 비해 교정후의 루프 프로브는 EMA의 관점에서 약 3.7배 정도의 성능이 향상되었음을 확인할 수 있다. 제시된 교정 절차를 그림 8에서 소비 전력 신호와 루프 프로브의 교정 후 측정된 전자파 신호의 파형을 비교해 보면 두 신호는 상호 유사한 것을 관측할 수 있고, 소비 전력 신호를 대신하여 전자파 신호를 이용한 암호 분석이 가능한 것을 확인할 수 있다. 또한, 스마트카드의 종류와 구조에 따라서 측정값의 변화를 예측할 수 있지만, 제시된 교정 절차를 수행한다면 암호 분석을 위한 전자파 신호의 측정이 가능함을 알 수 있다.

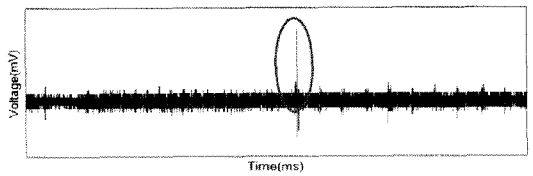
### 4-3 제작된 프로브를 이용한 DEMA 공격 결과

국내 표준 알고리즘인 ARIA(Academy, Reserch In-




(a) ARIA 알고리즘 평균 전자파 신호(1,000개)

(a) ARIA algorithm mean electromagnetic wave signal (signal of 1,000)




(b) 올바른 키에 대한 차분 전자파 신호

(b) Differential electromagnetic wave signal of correct key

그림 9. ARIA 알고리즘의 EMA 적용 결과

Fig. 9. EMA application result of ARIA algorithm.

stitute, Agency) 블록 암호 알고리즘을 공격 대상으로 하였으며, 2-1절에서 언급한 순서에 의해 기존의 소비 전력 신호를 이용한 공격 방법을 동일하게 사용하였다[8],[9]. 그림 9는 제작된 프로브를 이용한 DEMA 공격 적용 결과를 보여주고 있다.

측정된 전자파 신호를 이용한 암호 해독은 추측한 비밀 키가 맞을 경우, 차분 전자파 신호에서 피크(peak) 신호를 관측할 수 있다. 교정 전 프로브를 사용하였을 경우에는 피크 신호의 레벨이 낮으나 교정 후의 프로브를 사용할 경우에는 피크 신호가 높아지게 된다. 이는 추측한 비밀 키에 대한 신뢰도가 높아진 것을 의미한다. 그림 9의 (b)에서 확인할 수 있듯이 올바른 키에 대한 피크 신호가 관측되었고, 제작된 루프 프로브가 암호 분석용으로 적합함을 알 수 있다.

## V. 결 론

스마트카드 칩에서 물리적으로 접촉된 소비 전력 신호와 근거리에서 유기된 전자파 신호를 측정한 후에, 두 신호를 EMA의 관점에서 상호 비교하였다. 제작된 소형 루프 프로브는 잡음으로 분류한 전장 성분을 제거하고 방사된 자장 성분을 효과적으로 측정할 수 있었다. 스마트카드에서 방사되는 전자파 신호를 검출해 본 결과, 제안된 프로브는 비접촉 암호분석용으로 사용 가능함을 확인할 수 있었다. ARIA 알고리즘에 대한 EMA 적용 결과 올바른 키에 대한 차분 전자파 파형을 관측할 수 있었고, 스마트카드의 칩에서 발생되는 전자파를 이용한 암호 해독이 가능함을 보여주었다. 암호 분석용 프로브 제작 시 본 연구에서 제시된 교정 절차를 수행한다면 스마트카드뿐만이 아니라 RFID 장치, USB 그리고 PDA 등 다양한 암호 장비의 근거리 전자파 분석 공격에도 적용할 수 있으리라고 본다.

각종 암호 장비들은 전자파 공격 등 물리적인 공격에 취약점을 지니기 때문에, 차후 여러 종류의 암호 장비들에 대한 EMA 대비책이 연구되어야 할 것이다.

## 참 고 문 헌


[1] 문상재 외, 전자기 신호 분석 및 대응기술 동향, 국가보안연구소, 경북대학교, 2006년 10월.

[2] YongBin Zhou, DengGuo Feng, "Side-channel attacks: Ten years after its publication and the impacts on cryptographic module security testing", *NSA PST workshop*, Sep. 2005.

[3] K. Gandolfi, C. mourtel, and F. olivier, "Electromagnetic analysis: Concrete results", *CHES2001*, 2001.

[4] R. P. Feynman, *Lectures on Physics*, Addison-Wesley publishing company, vol. 2, pp. 15-17, 1972.

[5] Carlo F. M. Carobbi, L. M. Millanta, and L. Chiosi, "High-frequency behavior of the shield in the magnetic-field probes", *Electromagnetic Compatibility, 2000 IEEE International Symposium*, pp. 35-36, 2000.

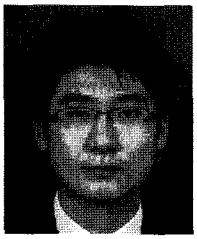
[6] R. W. P. King, "The loop antenna for transmission and reception", in R. E. Collin, F. J. Zucker, *Antenna Theory*, Part 1, Chapter 11, McGraw-Hill, 1969.

[7] 김채영, 전자파 공학, 경북대학교 산학협력단, pp. 364-368, 2007년 4월.

[8] NSRI, NSRI announces that ARIA v. 1.0 has been presented as a standard block cipher in Korea, June, 2004, Available from http://www.nsri.re.kr/ARIA/.

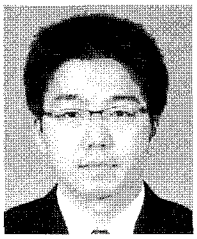
[9] J. C. Ha, C. K. Kim, S. J. Moon, I. H. Park, and H. S. Yoo, "Differential power analysis on block cipher ARIA", In *the 2005 International Conference on High Performance Computing and Communications-HPCC 05*, 2005.

최 종 균



2003년 2월: 영남대학교 전자공학과 (공학사)
2007년 8월: 경북대학교 전자공학과 (공학석사)
2007년 8월~현재: LG전자 연구원
[주 관심분야] 안테나 해석 및 설계, EMI/EMC

박 제 훈

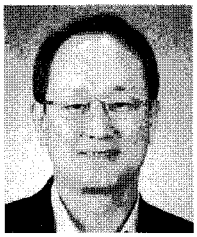


2004년 2월: 경북대학교 전자·전기공학부 (공학사)
2006년 8월: 경북대학교 전자공학과 (공학석사)
2006년 3월~현재: 경북대학교 전자공학과 박사과정
[주 관심분야] 정보 보호, 네트워크 보안, 스마트카드 보안

김 채 영

1976년 2월: 경북대학교 전자공학과 (공학사)
1978년 2월: 한국과학원 전기및전자공학과 (공학석사)
1990년 2월: 한국과학기술원 전기및 전자공학과 (공학박사)
1985년 9월~1986년 8월: 미국 Syracuse대학 방문연구원
1991년 9월~1993년 2월: 미국 MIT 공대 연구과학자
1979년 4월~1992년 9월: 경북대학교 공과대학 전자전기컴퓨터학부 전강, 조교수, 부교수
1992년 10월~현재: 경북대학교 전자전기컴퓨터학부 교수
[주 관심분야] 무선환경, 무선측정, 전자파 이론 및 응용

문 상 재



1972년 2월: 서울대학교 공업교육(전자)과 (공학사)
1974년 2월: 서울대학교 전자공학과 (공학석사)
1984년 6월: 미국 UCLA 전기공학과 (공학박사)
1984년 7월~1985년 6월: UCLA Post-Postdoctor 근무
1984년 7월~1985년 6월: 미국 OMNET 컨설턴트
1974년 12월~현재: 경북대학교 공과대학 전자전기컴퓨터학부 교수
2000년 8월~현재: 경북대학교 이동네트워크 정보 보호기술 연구센터 소장
2002년 2월~현재: 한국정보보호학회 명예회장
[주 관심분야] 정보 보호, 디지털 통신, 이동 네트워크