Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.23, NO.6, Dec. 2013 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2013.23.6.1017

안드로이드 기반 스마트폰 어플리케이션의 전자기파분석 공격 취약성

박 제 훈,†‡ 김 수 현, 한 대 완
한국전자통신연구원 부설 연구소

Weakness of Andriod Smartphone Applications against Electromagnetic Analsysis

JeaHoon Park,†‡ Soo Hyeon Kim, Daewan Han
The Attached Institute of ETRI

요 약

스마트폰의 사용이 증가하고 사용처가 다양해지면서 뱅킹, 결제, 인증을 위한 보안 어플리케이션이 스마트폰에 구동되고 있다. 보안 서비스를 제공하기 위해 RSA, AES, ECC 등의 암호 알고리즘을 스마트폰 CPU로 연산하고 있지만 스마트폰 CPU는 전자기파분석 공격과 같은 부채널분석 공격에 대한 안전도를 고려하지 않고 있다. G. Kenworthy는 2012년 DesignCon에서 스마트폰에서 동작하는 암호 알고리즘의 전자기파분석 공격에 대한 취약성을 발표하였다. 본 논문에서는 G. Kenworthy의 전자기파분석 실험 환경을 개선하여 안드로이드 기반 스마트폰 상에서 동작하는 상용 보안 어플리케이션의 전자기파분석 공격에 대한 취약성 분석 실험을 수행하였다. 실험 결과 상용 보안 어플리케이션 내에서 동작하는 암호 알고리즘의 전자기파분석 공격에 대한 취약점을 확인하였다. 실험 장비 설정값에 따라 Google의 Play 스토어 동작 중에 방사되는 전자기파 신호에서 w-NAF 스칼라곱셈 연산 구간 구분이 가능하였으며, w-NAF 스칼라곱셈의 스칼라값이 '0'인지 '0'이 아닌지도 구분 가능하였다.

ABSTRACT

With the growing use of smartphones, many secure applications are performed on smartphones such as banking, payment, authentication. To provide security services, cryptographic algorithms are performed on smartphones' CPU. However, smartphone's CPU has no considerations against side-channel attacks including Electromagnetic Analysis (EMA). In DesignCon 2012, G. Kenworthy introduced the risk of cryptographic algorithms operated on smartphone against EMA. In this paper, using improved experimental setups, we performed EMA experiments on androin smartphones' commercial secure applications. As a result, we show that the weakness of real application. According to the experimental setups, we picked up the operation of w-NAF scalar multiplication from the operation of Google's Play Store application using radiated EM signal. Also, we distinguished scalar values (0 or not) of w-NAF scalar multiplication.

Keywords: Smartphone, Electromagnetic Analysis, SSL, ECC

I. 서 론

스마트카드, RFID, USB 토큰 등의 저 전력 장치에서 암호 알고리즘이 동작하는 경우에는 부채널분석 공격에 취약할 수 있다[1,2,3]. 따라서 부채널분석 공

접수일(2013년 9월 9일), 수정일(2013년 10월 14일), 게재확정일(2013년 10월 14일)
† 주저자, jenoon65@ensec.re.kr
‡ 교신저자, jenoon65@ensec.re.kr(Corresponding author)

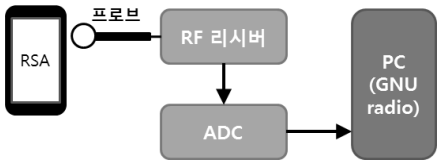

Fig.1. Block Diagram of Electromagnetic Analysis

격이 소개된 이후 많은 대응방안들이 개발되어 사용되고 있다. 최근 스마트폰의 사용이 증가하고 사용처가 다양해지면서 뱅킹, 결제, 인증을 위한 보안 어플리케이션이 스마트폰에 구동되고 있다. 보안 서비스를 제공하기 위해 RSA, AES, ECC 등의 암호 알고리즘을 스마트폰 CPU로 연산하고 있지만 스마트폰 CPU는 스마트카드 EMV 인증과 같이 부채널분석에 대한 안전도 평가를 수행하지 않고 있다. DesignCon 2012에서 G. Kenworthy는 스마트폰에서 동작하는 암호 알고리즘의 전자기파분석 공격에 대한 취약성을 발표하였다[4]. [4]에서 그는 스마트폰과 PDA에 2048-bit RSA와 8-bit ECC를 구현하여 반복 동작시킨 후 전자기파를 측정하여 RSA의 멱승값과 ECC의 스칼라값을 추출하였다. 본 논문에서는 스마트폰에서 동작하는 상용 어플리케이션의 취약성을 분석하기 위해 G. Kenworthy의 실험 환경을 스펙트럼분석기와 오실로스코프를 이용하여 개선하였다. 그 결과 상용 보안 어플리케이션 내에서 동작하는 암호 알고리즘에 대한 전자기파분석 공격 적용 가능성을 확인하였다. Android 스마트폰 사용자의 필수 어플리케이션인 Google의 Play 스토어 어플리케이션은 사용자 인증과 암호 통신을 위해 SSL 통신을 사용하며, SSL(Secure Socket Layer) 통신을 위한 키 설정 과정에서 스마트폰은 w-NAF 스칼라곱셈을 연산한다. 전자기파분석 실험 결과 SSL 통신 설정 과정 중 연산되는 w-NAF 스칼라곱셈을 구분할 수 있었으며, w-NAF 스칼라곱셈의 스칼라값이 '0'인지 '0'이 아닌지도 구분 가능하였다.

본 논문의 구성은 다음과 같다. 2장에서 전자기파분석 공격과 SSL 통신에 대해 설명한 후 3장에서 전자기파분석 실험 환경에 대해 설명한다. 4장에서 Google의 Play 스토어 어플리케이션에 대한 전자기파분석 실험 결과를 설명하고 5장에서 결론을 맺는다.

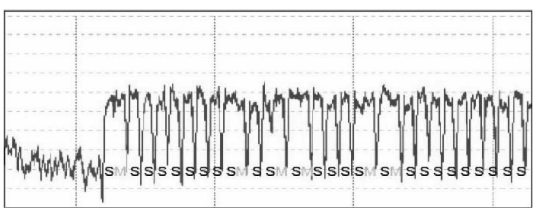

Fig.2. EM Trace of RSA Algorithm

II. 배경 연구

2.1 전자기파분석 공격

전자기파분석 공격(Electromagnetic analysis, EMA)은 공격 대상 장치에서 암호 알고리즘이 동작할 때 방사되는 전자기파를 측정하여 암호 알고리즘의 비밀키 정보를 알아내는 공격 방법으로 부채널분석 공격의 한 종류로 분류된다[5,6,7]. 특히 암호 모듈에 대한 직접적인 변경이나 침입을 하지 않고 공격을 적용할 수 있어서 매우 위협적이다. DesignCon 2012에서 G. Kenworthy는 스마트폰에 전자기파분석 공격을 적용하여 스마트폰 CPU에서 연산되는 암호 알고리즘의 취약성을 실험으로 확인하였다[4]. 스마트폰 전자기파분석 공격 실험을 위해 IC-R7000 RF 리시버, EM 프로브, USRP N200 ADC, GNU radio 프로그램을 이용하여 Fig.1.과 같이 실험 환경을 구성하였다[8,9,10].

EM 프로브로 측정된 전자기파 신호는 RF 리시버의 대역통과필터를 거쳐 PC로 전달되고 전달된 신호는 PC의 GNU 프로그램을 통해 AM 복조 된다. G. Kenworthy는 실험을 위해 RSA 알고리즘을 스마트폰 어플리케이션으로 직접 구현 하였으며, 부채널분석 대응 방안을 고려하지 않은 일반적인 이진 멱승 알고리즘을 사용하였다. Fig.2.는 스마트폰에서 RSA 알고리즘이 동작될 때 측정한 전자기파 신호이다.

Fig.2.에서 'S'는 제곱연산, 'M'은 곱셈연산을 나타낸다. Fig.2.의 전자기파 신호에서 공격자는 'SM'과 'S' 신호 형태를 구분할 수 있다. 따라서 공격자는 이진 멱승 알고리즘의 동작 방식으로부터 'SM'과 'S'의 신호 패턴을 유도하는 RSA 비밀 키 비트값('1' 또는 '0')을 알아낼 수 있다.

2.2 SSL(Secure Socket Layer) 통신

SSL은 TCP/IP 통신에서 기밀성, 무결성, 상호 인증 서비스를 제공하기 위해 Netscape사가 제안한 통신 방식이다[11]. 현재는 TLS(Transport Layer Security)로 개명되어 사용되고 있다. 최근에는 스마

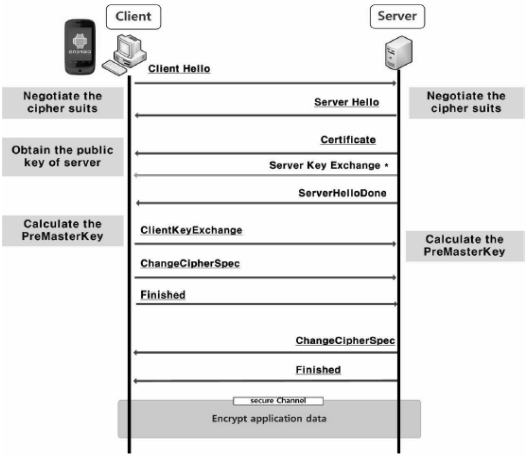

Fig.3. SSL Handshake Protocol

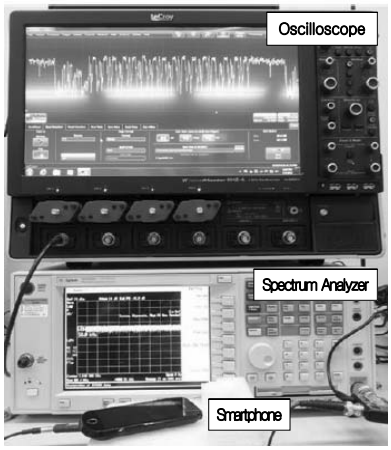

Fig.4. Experimental Environment

트폰을 이용한 보안 어플리케이션의 사용이 증가함에 따라 보안이 취약한 무선 환경에서 데이터 보호를 위해 SSL 통신을 사용하기도 한다. Fig.3.은 SSL handshake 프로토콜을 보여주고 있다.

SSL handshake 프로토콜에서는 상호 인증과 암호화 통신을 위한 키(PreMasterKey)를 생성한다. PreMasterKey 생성을 위해 Server와 Client는 구현 방식에 따라 RSA, DH(Diffie-Hellman), ECDH(Elliptic Curve Diffie-Hellman) 키 교환 프로토콜을 수행한다.

III. 스마트폰에 대한 전자기파분석 공격 실험

본 논문에서는 G. Kenworthy의 실험 환경을 개선한 후, 실제 상용 어플리케이션에 대한 전자기파분석 적용 결과를 3장과 4장에서 설명한다.

3.1 실험 환경

전자기파 신호의 보다 정교한 분석을 위해 애질런트 사의 E4440A 스팩트럼분석기와 텔레다인르크로이 사의 804Zi-A 오실로스코프를 활용하여 스마트폰 전자기파분석 공격 실험 환경을 구성하였다[12,13]. 스팩트럼분석기를 이용하여 AM 복조 효과를 만들어 내기 위해 zero span 모드를 활용하였다. Zero span 모드는 중심 주파수의 일정 대역 신호를 시간영역에 나타내는 기능이다. 또한 RBW(Resolution BandWidth, 분해능대역폭)를 조절하여 대역통과필터의 대역폭을 조절할 수 있었고, VBW(Video BandWidth, 비디오대역폭)를 조절하여 출력 신호의 잡음 수준을 조절할 수 있었다. Fig.4.는 논문의 실험을 위해 구성된 전자기파분석 공격 실험 환경을 보여주고 있다.

스팩트럼분석기의 AM 복조 결과는 오실로스코프 화면을 통해 관찰한다. 이 때 오실로스코프의 Time/Div와 Voltage/Div를 조절하면서 복조된 스마트폰 전자기파 신호를 세밀하게 분석할 수 있다. G. Kenworthy 실험 환경의 RF 수신기는 AM과 FM 통신에 사용되는 수신 신호 대역폭만을 제공하기 때문에 수신 신호의 대역폭 조절에 제한이 있다. 하지만, 스팩트럼분석기와 오실로스코프로 구성한 전자기파분석 공격 실험 환경에서는 수신 신호의 대역폭(RBW, 1Hz~8MHz) 조절이 용이하다. 또한 VBW를 조절하여 수신 신호의 잡음을 제거할 수 있어서 보다 정교한 신호에 대한 분석에 활용 가능하다.

3.2 스마트폰에 대한 전자기파분석 실험

구성된 실험 환경을 검증하기 위해 4종의 실험 대상 스마트폰에 2048-bit RSA 멱승 알고리즘을 반복하여 동작시킨 후, 스팩트럼분석기의 중심주파수, RBW, VBW를 변화시켜가면서 RSA 멱승 알고리즘의 멱승값이 구분 가능한 설정값을 탐색하였다. Table 1.은 실험에 사용된 스마트폰의 사용과 스팩트럼분석기의 설정값을 보여주고 있다.

Fig.5.는 RSA 멱승 알고리즘이 동작되는 동안 측정된 전자기파 신호이다.

실험 결과 4종의 실험 대상 스마트폰 모두에 전자

Table 1. Specifications of Target Smartphones & Experimental Settings

Type	CPU	OS ver.	Spectrum analyzer settings
(a)	Single 582MHz	2.2	- 중심주파수 : 12.96MHz RBW : 360KHz VBW : 51KHz
(b)	Dual 720MHz	2.3	- 중심주파수 : 34.96MHz RBW : 8MHz VBW : 30KHz
(c)	Single 1.2GHz	4.0	- 중심주파수 : 19.81MHz RBW : 8MHz VBW : 30KHz
(d)	Dual 1.5GHz	4.0	- 중심주파수 : 15.83MHz RBW : 300KHz VBW : 4.3KHz

기파분석 공격이 적용 가능함을 확인하였다. 스팩트럼 분석기의 설정값은 스마트폰 CPU의 사양에 따라 달랐으며, Table 1.에 나타난 설정값 외에도 Fig.5.와 같이 멱승 알고리즘의 비트값을 확인할 수 있는 중심주파수가 검색 구간(10MHz~2GHz) 내에 몇 군데 더 존재하였다.

IV. 스마트폰 상용 어플리케이션에 대한 전자기파분석 공격 실험

본 장에서는 개선된 실험 환경을 이용하여 상용 어플리케이션에 대한 전자기파분석 공격 적용 가능성 실험 결과를 설명한다.

4.1 Play 스토어 어플리케이션 전자기파분석을 위한 실험 장비 설정

Google의 Play 스토어 어플리케이션은 android 사용자라면 필요한 어플리케이션을 설치하기 위해 이용하는 필수 어플리케이션이다. 실험에서는 Play 스토어 어플리케이션이 사용자 인증과 암호 통신을 위해 SSL protocol을 수행하는 중에 연산되는 암호 알고리즘에 대해 전자기파분석 공격을 적용한다. 스마트폰은 SSL 통신을 위해 Google 서버와 SSL handshake protocol을 수행하며, 키 설정을 위해 android 버전에 따라 OpenSSL 라이브러리를 활용하여 DH나 ECDH를 수행한다[14]. 실험에서는 OS 버전, 생산년도, 전자기파 신호 품질 등을 고려하여 Table 1.의 (c) 모델을 이용하여 실험을 수행하였다. (c) 스마트폰에서 동작하는 Play 스토어 어플리케이션을 분석한 결과 (c) 스마트폰은 키 설정을 위해 $F_p(p$:256-bit)상에서 ECDH를 수행하고, 스칼라곱셈의 연산 효율을 높이기 위해 4-NAF 스칼라곱셈 알고리즘을 사용하는 것으로 확인되었다.

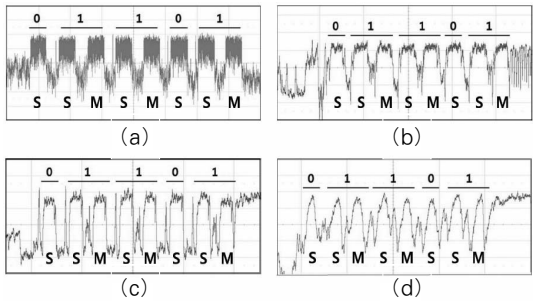

Fig.5. EM traces of RSA Algorithm from Four Types of Smartphones

실험 장비를 4-NAF 스칼라곱셈 분석에 적합하도록 설정하기 위해 OpenSSL 라이브러리를 이용하여 4-NAF 스칼라곱셈 알고리즘을 반복 수행시키는 프로그램을 구현하였다. 구현된 프로그램을 (c) 스마트폰에 설치하여 동작시킨 후, 스팩트럼분석기의 중심주파수, RBW, VBW를 변화시켜가면서 적절한 설정값을 검색하였다. Table 2.는 실험을 위해 스마트폰에 구현한 4-NAF 스칼라곱셈 알고리즘의 변수값을 보여주고 있다.

Fig.6.은 4-NAF 스카라곱셈의 전자기파 신호를 보여주고 있다.

Table 2. Parameters of 4-NAF Scalar Multiplication Algorithm

변수	변수값
p	FFFFFFFF00000001000000000000000000000000FFFFFFFFFFFFFFFFFFFFFFFF
Secret key (binary form)	7EF44D1F6D09807B102CD054B073A2638972A95DD28AA8FAED4E6E699F36DA51
Secret key (4-NAF form)	70000(-1)0000005000005000700000(-1)0007000(-3)0001000(-7)000(-7)00010007000(-5)000010000000100007000300000500000(-3)0003000007000300005000100(-5)0000100003000(-1)000500000(-3)000(-3)000(-5)000(-1)000700010000050005000100(-1)0000(-5)000(-1)000070000(-7)00000700007000(-5)000(-3)000(-3)00000000(-7)00005000(-5)000003001

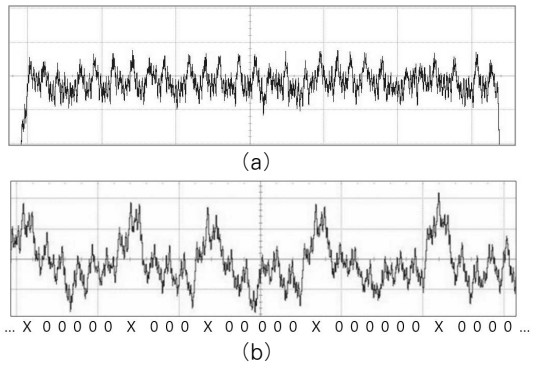

Fig.6. EM Trace of 4-NAF Scalar Multiplication Algorithm (Center freg.:1.19GHz, RBW:8MHz, VBW:10kHz)

Fig.6. (a)는 4-NAF 스칼라곱셈 알고리즘 전체의 전자기파 신호이고, Fig.6. (b)는 일부 구간을 확대하여 보여주고 있다. 스팩트럼분석기의 설정값이 올바르게 셋팅이 되면 4-NAF 스칼라곱셈 연산 구간을 구분할 수 있으며, Fig.6. (b)에서와 같이 측정된 전자기파 신호에서 'X'에 해당하는 전자기파 신호와 '0'에 해당하는 전자기파 신호를 구분할 수 있다. 여기서 X는 4-NAF 값에서 ±1, ±3, ±5, ±7을 통칭하고 있다. w-NAF 값에서 '0'과 'X'가 구분되면 비밀키의 비트 길이에 기인하는 안전도를 온전히 제공하지 못한다. 즉, 다음 수식과 같은 안전도만를 제공할 수 있게 된다.

$$((w-1)\times X\text{의 개수})-bit \quad (1)$$

실험에 사용한 256-bit 비밀키의 경우 안전도가 (3*54)-bit 안전도로 감소하는 것을 확인할 수 있었다.

4.2 Play 스토어 어플리케이션에 대한 전자기파분석 실험

4-NAF 스칼라곱셈 연산을 구분할 수 있도록 설정된 스팩트럼분석기를 이용하여 실제 Play 스토어 동작 중 스칼라곱셈 연산을 구별하고 4-NAF 값에서 '0'과 'X'가 구분 가능한지를 확인하였다. 추가적으로 Play 스토어 접속 시 SSL 통신을 위한 SSL handshake protocol이 정상적으로 동작하고 ECDH 연산이 수행되는 지를 확인하기 위해 wire shark 프로그램을 이용하여 무선통신 데이터 패킷을

Fig.7. Captured Packets of SSL Handshake Protocol

관찰하였다. Fig.7.은 wire shark 프로그램으로 수집된 무선 데이터 패킷을 보여주고 있다.

'Client Key Exchange' 과정이 항상 수행되지 않기 때문에 실험에서는 wire shark를 이용하여 'Client Key Exchange' 과정의 수행이 확인되었을 때 측정된 전자기파 신호를 분석하였다. 즉, 키 설정을 위해 스마트폰 CPU에서 4-NAF 스칼라곱셈이 수행될 때 측정된 전자기파 신호를 분석한다.

Fig.8. (a)의 전자기파 신호는 사용자가 Play 스토어 어플리케이션을 터치하는 순간부터 수 초간 측정된 신호이다. Fig.8. (b)는 Fig.8. (a)에서 Fig.6.과 같은 전자기파 신호가 나타나는 구간을 검색하여 확대한 그림이다. Fig.6.과 마찬가지로 Fig.8. (b)의 전자가파 신호에서도 'X'에 해당하는 전자기파 신호와 '0'에 해당하는 전자기파 신호를 구분할 수 있다. 즉 Play 스토어의 SSL 통신 설정 과정 중 ECDH 키 교환 프로토콜에 사용되는 256-bit 비밀키의 안전도가 수식 (1)의 안전도로 감소한다.

이와 같은 결과는 공격 대상 알고리즘에 대한 사전 준비를 통해 적절한 설정값이 세팅된 실험 장비를 이용하면 프로토콜이나 전체 어플리케이션 수행 중 연산 시점에 상관없이 단 한 번의 알고리즘 수행으로도 전자기파분석 공격을 적용할 수 있다는 것을 의미한다.

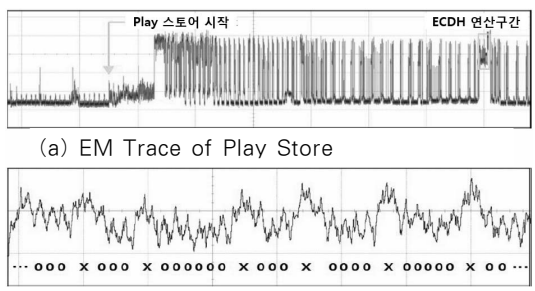

Fig.8. EMA Results of Play Store Application

실험의 예로 보인 256-bit 4-NAF 스칼라곱셈 알고리즘의 경우에는 전자기파분석 공격 적용만으로 비밀키 직접 추출하기는 어렵지만, 이에 대한 대응방안을 고려하지 않은 암호 알고리즘이 스마트폰 CPU에서 연산되는 경우에는 비밀키 노출의 위험이 존재한다. 따라서 스마트폰 CPU나 스마트폰 어플리케이션 개발 시 금융IC카드에 적용되는 물리적 공격에 대한 안전도 검증을 비롯한 여러 가지 대응 방안에 대한 고려가 필요할 것이다.

V. 결 론

본 논문에서는 G. Kenworthy의 실험 환경을 스펙트럼분석기와 오실로스코프를 이용하여 개선한 후 상용 어플리케이션의 전자기파분석 공격에 대한 취약점을 분석하였다. Play 스토어 어플리케이션에 대한 실험 결과 단 한 번의 Play 스토어 실행으로도 SSL 통신 설정 과정 중 연산되는 w-NAF 연산 구간을 구분할 수 있었으며, w-NAF 스칼라곱셈의 스칼라값이 '0'인지 '0'이 아닌지도 구분할 수 있었다. 이러한 결과는 상용 어플리케이션 구현 방식에 따라 매우 큰 위협이 될 수 있다. 또한 안드로이드 기반의 스마트폰뿐만 아니라 iOS 기반 스마트폰에도 유사한 방식으로 적용 가능할 것이다. 향 후 공격 대상 스마트폰과 어플리케이션에 적절한 설정값의 효과적인 검색 방법에 대한 연구와 측정된 전자기파 신호 분석의 오류 판정 보정 방법에 대한 연구는 전자기파분석 공격을 보다 실제적이고 위협적인 공격으로 만들 수 있을 것이다.

이와 같은 취약점을 보완하기 위해 스마트폰 CPU와 스마트폰 어플리케이션 개발 시 금융IC카드에 적용되는 물리적 공격에 대한 안전도 검증이 필요할 것이다. 또한 물리적 공격 대응방안, 어플리케이션 역분석 방지 방안 등에 대한 추가적인 고려가 반드시 필요하다.

References

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

[2] T. Messerges, E. Dabbish, and R. Sloan, "Power Analysis Attacks of Modular Exponentiation in Smartcards," CHES 1999, LNCS 1717, pp.144-157, Aug. 1999.

[3] P. Kocher, J. Jaffe, B. Jun, and P. Rohatgi, "Introduction to differential power analysis," Journal of Cryptographic Engineering, Vol. 1, Issue 1, pp.5-27, Mar. 2011.

[4] G. Kenworthy, "Secret Cryptographic Key Extraction form Mobile Devices using RF EM Emissions," DesignCon 2012, Session 12-WP6, Jan. 2012.

[5] J. Quisquater and D. Samyde, "Electromagnetic analysis (EMA): measures and counter-measures for smart cards," E-smart 2001, LNCS 2140, pp.200-210, Sept. 2001.

[6] D. Agrawal, B. Archambeault, J. Rao, and P. Rohatgi, "The EM side-channel(s)," CHES 2002, LNCS 2523, pp.29 - 45, Sug. 2002.

[7] C. Gebotys, H. Simon, C. Tiu, "EM Analysis of Rijndael and ECC on a Wireless Java-Based PDA," CHES 2005, LNCS 3659, pp.250 - 264, Sept. 2005.

[8] ICOM IC-R7000 datasheet, http://www.icom.co.jp/world/support/download/manual/pdf/IC-R7000.pdf

[9] Ettus USRP N200 datacheet, https://www.ettus.com/content/files/07495_Ettus_N200-210_DS_Flyer_HR.pdf

[10] GNU radio webpage, http://gnuradio.squarespace.com

[11] Internet Engineering Task Force, "The TLS Protocol," RFC 2246, 1999.

[12] Teledyne Lecroy 804Zi-A datasheet, http://cdn.teledynelecroy.com/files/pdf/wavemaster_8_zi-a_datasheet.pdf

[13] Agilent E4440A datasheet, http://cp.literature.agilent.com/litweb/pdf/5980-1284E.pdf

[14] OpenSSL webpage, http://www.openssl.org/

〈저자소개〉

사 진

박 제 훈 (JeaHoon Park) 정회원
2004년 2월: 경북대학교 전자·전기공학부 졸업
2006년 2월: 경북대학교 전자공학과 석사
2011년 2월: 경북대학교 전자공학과 박사
2011년 1월~2012년1월: 국방기술품질원 선임연구원
2012년 2월~현재: ETRI부설연구소 연구원
〈관심분야〉 부채널분석, 정보보호시스템 안전성 분석

사 진

김 수 현 (Soo Hyeon Kim) 정회원
1999년 2월: 전북대학교 정보통신공학과 졸업
2001년 2월: 전북대학교 컴퓨터공학과 석사
2001년 3월~현재: ETRI부설연구소 선임연구원
〈관심분야〉 정보보호시스템 설계 및 안전성 분석

사 진

한 대 완 (Daewan Han) 정회원
1997년 2월: 서울대학교 수학과 석사
2007년 8월: 서울대학교 수학과 박사
2001년 3월~현재: ETRI부설연구소 선임연구원
〈관심분야〉 암호 설계 및 분석, 정보보호시스템 안전성 분석