비밀키를 NAF로 사용하는 암호시스템의 차분 전력분석 공격☆

Differential Power Analysis Attack on Cryptosystem adopted NAF Algorithm as a Secret Key Recoding Method

안 만 기* 하 재 철** 이 훈 재*** 문 상 재****
Mahn-Ki Ahn Jae-Cheol Ha Hoon-Jae Lee Sang-Jae Moon

요 약

전력 분석 공격은 스마트 카드를 사용하는 암호 시스템에 대한 물리적 공격이다. 본 논문에서는 타원곡선 암호 알고리듬을 사용하는 스마트 카드가 비밀키를 NAF(non-adjacent form)로 부호화하여 사용하여도 차분 전력분석 공격에 대응할 수 없음을 실험을 통하여 제시하였다. 공격 대상인 비밀키를 모르는 스마트 카드에서 암호 알고리듬 동작 시점부터 측정된 평균 전력 신호와 비밀키 변경이 가능한 스마트 카드에서 측정된 평균 전력 신호를 차분함으로써 비밀키를 한 비트씩 순차적으로 알아낼 수 있다.

Abstract

The power analysis attack is a physical attack which can be applied to the cryptosystems such as smartcard. We try to experimental attack to a smart card which implemented Elliptic Curve Cryptosystem adopting NAF algorithm as a secret key recording method. Our differential power analysis attack is a potential threat to that implementation. The attacker measures the power traces during the multiplication with secret key bits in a target smart card and the multiplication with the guessed bits in other experimental one. The comparison of these two traces gives a secret bit, which means that attacker can find all secret key bits successively.

Key words : smartcard, differential power analysis, NAF algorithm, Elliptic Curve Cryptosystem

1. 서 론

스마트 카드(smartcard)란 마이크로프로세서와 메모리를 내장하고 카드 내에서 데이터 연산 처리와 저장이 가능한 플라스틱 카드를 말한다[1]. 그런데 지금까지 알고리듬적으로 안전하다고 알려졌던 스마트 카드는 설계 시 고려되지 못한 부가적인 정보의 누출에 의해 비밀 정보를 알아내는 부-채널공격(side-channel attack)의 대상이 될 수 있다. 즉, 스마트 카드가 동작할 때 비밀키에 대한 연산이 자주 일어나므로 이러한 정보의 누출에 의해 시스템의 안전성에 큰 영향을 미칠 수 있다. 부-채널공격은 크게 시간 공격(timing attack)[2], 오류주입 공격(fault insertion attack)[3], 전력분석 공격(power analysis attack)[4,5] 그리고 전자기 누출 공격(electromagnetic emission attack)[6] 등으로 나눌 수 있다.

이러한 물리적 공격 중에서 전력분석 공격은 스마트 카드에 직접적인 물리적 변환을 가하지 않고 직접 소모전력 파형의 특성을 파악하여 비

* 준회원 : 국방품질관리소 연구원
mkahn@dqaa.go.kr(제1저자)
** 정회원 : 나사렛대학교 정보통신학과 조교수
jcha@kornu.ac.kr(공동저자)
*** 정회원 : 동서대학교 인터넷공학부 조교수
hjlee@dongseo.ac.kr(공동저자)
**** 정회원 : 경북대학교 공과대학 전자전기컴퓨터학부 교수
sjmoon@knu.ac.kr(공동저자)
☆ 본 연구는 정보통신부 대학정보통신연구센터(ITRC) 육성 지원사업의 지원으로 수행하였습니다.

밀키에 대한 정보를 알아내는 단순 전력분석 공격(SPA, simple power analysis)와 SPA에 통계적인 분석 방법과 에러 정정 기술을 도입한 차분 전력분석 공격(DPA, differential power analysis)로 분류된다. Paul Kocher는 CRYPTO'99에서 DES에 전력분석 공격을 적용했고 T. S. Messerges는 CHES'99에서 스마트 카드에 차분 전력분석 공격 실험(SEMD, MESD, ZEMD)을 적용한 바 있다[5,7,8].

본 논문에서는 타원곡선 암호시스템(Elliptic Curve Cryptosystem, ECC)[9]을 사용하는 스마트 카드에서의 부-채널 공격 중 차분 전력분석 공격을 실험하였다. 소프트웨어적으로 구현된 타원곡선 암호시스템에서는 계산 속도를 높이기 위해 비밀키를 NAF형으로 부호화하여 사용하는데 이 경우에도 MESD (Multiple Exponent Single Data) 공격 방법을 사용하는 전력분석에 의해 비밀키 추측이 가능함을 보였다. 또한 암호 알고리듬의 연산 시 비밀키에 따른 연산 시간의 차이로 시차 공격이 이루어짐을 검증하였다. 논문의 2장에서는 타원곡선 암호 알고리듬의 연산 과정을 알아본다. 3장에서는 소프트웨어로 구현된 ECC에 대해 비밀키를 NAF형으로 사용할 때 차분 전력분석 공격을 실험하여 공격이 성공할 수 있음을 보인다. 4장에서 결론을 맺는다.

2. 타원곡선 암호시스템

2.1 타원곡선의 정의

타원곡선 암호시스템은 1985년 Miller[9]와 Koblitz[10]에 의해 독립적으로 제안된 방식으로 유한체 상에서 정의된 타원곡선 식을 만족하는 점들의 집합에서 적당한 연산을 적용하여 그룹을 정의하고 이 그룹에서 암호시스템을 구성한다. 예를 들어 유한체 $GF(p)$에서 3차 동차식인 Weierstrass 방정식을 만족하는 점의 집합을 정의하는 타원곡선 $E(GF(p))$ 시스템을 가정하자. 이 타원곡선 위의 점 $P \in E(GF(p))$와 $Q \in E(GF(p))$가 주어질 때, $Q = dP$를 만족하는 비밀키 d $(0 \le d \le n-1)$를 찾는 문제를 타원곡선 이산대수 문제(Elliptic Curve Discrete Logarithm Problem, ECDLP)로 정의하며 이를 해결하는 어려움에 타원곡선 암호 알고리듬의 안전도를 두고 있다.

타원곡선을 정의하는 Weierstrass 방정식은 다음과 같이 간단하게 쓸 수 있다.

$$y^2 = x^3 + ax + b \qquad (1)$$
$$a, b \in GF(p),\ 4a^3 + 27b^2 \neq 0 \bmod p$$

타원곡선 $E(GF(p))$는 위의 등식을 만족하는 점(x, y)과 점에 대한 연산 시 덧셈 '+'에 대한 항등원으로 작용하는 무한원점 O로 구성된다.

2.2 덧셈-뺄셈 방법(Addition-Subtraction Method)의 연산 과정

타원곡선 위의 점 P를 d번 더하는 연산을 한 점에 대한 스칼라 곱셈(scalar multiplication)연산이라 하고 dP로 표기한다. 기존의 유한체 상에서의 연산과 비슷하게 메시지의 암·복호 과정과 디지털 서명의 서명검증과정의 속도는 스칼라 곱셈 연산의 속도와 비례하므로 효율적인 고속 연산 알고리듬이 필요하다. 스칼라 곱셈 방법 중 덧셈-뺄셈 방법은 dP에서 비밀키 d를 부호화된 이진수(signed binary)로 표현하여 연산을 수행한다. 덧셈-뺄셈 방법 방법에서는 비밀키 d를 식 (2)과 같이 NAF(non-adjacent form) 표현으로 쓸 수 있다[11].

$$d = \sum_{i=0}^{l} c_i \cdot 2^i,\ c_i \in \{-1, 0, 1\} \qquad (2)$$

예를 들면, 하나의 정수 d에 대하여 부호화된 이진수는 많이 있지만 NAF 부호화는 다음과 같다. 여기서 $\bar{1}$은 -1을 의미한다.

NAF는 이진 표현에서 부호화된 이진수로 바꾼

INPUT : The point P and the integer d
OUTPUT : $Q = dP$

$Q \leftarrow P$
for i from l-2 to 0 do
  Set Q← 2Q
  if c_i = 1 then $Q \leftarrow Q + P$
  if c_i = -1 then $Q \leftarrow Q - P$
output Q

(그림 1) 덧셈-뺄셈 스칼라 곱셈 알고리듬

$d = 111011110$
$= 2^8+2^7+2^6++2^4+2^3+2^2+2^1 = 478$ (정수)
$d = 1000\bar{1}00\bar{1}10 = 2^9-2^5-2^2+2^1 = 478$
(부호화된 이진수)
$d = 100\bar{1}1000\bar{1}0 = 2^9-2^6+2^5-2^1 = 478$
(부호화된 이진수)
$d = 1000\bar{1}000\bar{1}0 = 2^9-2^5-2^1 = 478$
(NAF 부호화)

수열 중 인접한 두 비트에서 적어도 한 비트가 '0'이 되도록 만든 형태인데 하나의 정수에 대한 NAF 표현은 유일하다는 특성을 갖는다. 그림 1은 비밀키 d를 부호화된 이진수 표현 방법 중 NAF 형태로 표현한 후 이를 이용하여 타원곡선 상에서 스칼라 곱셈을 하는 덧셈-뺄셈 알고리듬을 기술한 것이다.

3. NAF를 사용하는 ECC의 차분 전력분석 공격

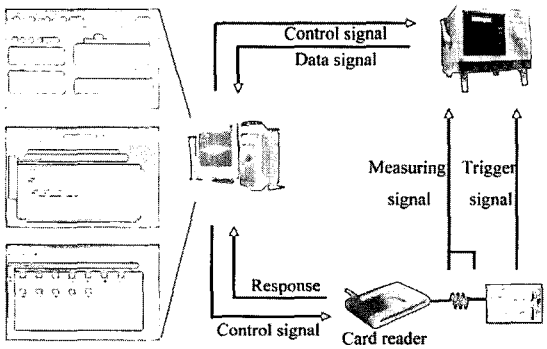
본 장에서는 NAF를 부호 방법을 이용하여 덧셈-뺄셈 알고리듬으로 스칼라 곱셈을 실행할 경우 차분 전력 분석 공격을 시도한다. 실험에 사용된 장비 제원 및 실험과정을 제시하고 측정한 전력 분석을 통해 비밀키 공격이 가능함을 증명하고자 한다.

3.1 차분 전력분석 공격의 실험 장비 및 제원

전력분석 공격 실험을 위해서는 카드 리더기, 카드, 오실로스코프, PC, 에뮬레이터 등을 설치해야 한다. 먼저 소모전력 파형를 측정하기 위한 디지털 오실로스코프 및 접촉식 스마트 카드와 관련 응용 프로그램이 PC에 설치된다. PC에서는 C 언어를 기반으로 스칼라 곱셈 프로그램을 작성하여 에뮬레이터를 사용해 기계어 코드를 생성한다. 생성된 기계어 코드를 스마트 카드의 EEPROM 영역에 입력하고 카드를 동작시킨다. 마지막으로 카드의 그라운드(GND)단자를 20 Ω 정도의 저항을 연결하여 전압 파형을 측정한다[12]. 표 1은 실험 장비에 대한 사양을 나타내며 그림 2는 실험 장비의 구성도이다.

(표 1) 실험 장비 사양

	스마트 카드	에뮬레이터	오실로스코프	컴퓨터
주파수	3.58MHz	25MHz	500MHz	400MHz
CPU	8bit	8bit	-	Pentium II
RAM	512 bytes	-	-	128Mbytes
EEPROM	8 Kbytes	-	-	-
시스템 전압	2.5V~5.5V	3V~5V	-	-
다운 속도		115200bps	-	-
표본화율	-	-	4Gsamples /sec	-



(그림 2) 실험장비 구성도

3.2 차분 전력분석 공격의 실험 과정

공격자는 암호 알고리듬의 종류와 동작 시점, 그리고 비밀키의 비트 수 l을 알고 있다고 가정

한다. MESD 공격은 두 개의 스마트 카드(비밀키가 담긴 공격대상 카드와 키 값을 변경할 수 있는 비교용 카드)를 이용하여 공격하는 기술이다. 즉, 동일한 메시지에 대하여 스칼라 곱셈을 실행하는데 비밀키를 모르는 공격대상카드의 평균전력 파형과 비밀키 변경이 가능한 비교용 카드의 평균전력 파형을 차분함으로써 키 비트를 순차적으로 알아내는 공격 방법이다. 단계적으로 보면 다음과 같이 데이터 수집 단계와 분석 단계로 나누어 한 비트씩 공격하는데 비밀키 변경이 가능한 스마트 카드의 비밀키를 공격 대상 카드의 비밀 키 비트와 동일한 형태로 변경하면서 순차적으로 모든 비트를 찾게 된다.

(1) 데이터 수집 단계
- 공격 대상의 스마트 카드에서 소모되는 전력을 표본화하여 소모전력 데이터 $T_i[j]$를 수집한다. i는 반복적인 측정 횟수 $(1 \le i \le K)$ 이며 j는 샘플의 개수로 표본화율에 비례한다.
- 비밀키 변경이 가능한 카드의 추측한 키 $d=(d_{l-1}, d_{l-2}, \ldots, d_0)$라 할 때 1-2번째의 비트의 연산되는 시점부터 소모전력 파형 $S_i[j]$을 수집한다. d_{l-1}는 최상위 비트로 항상 '1'이다.

(2) 데이터 분석 단계
- 잡음신호 감소와 차분 데이터의 정확성을 위해 통계적인 방법을 사용한다. 두 소모전력 데이터를 평균한 다음 차분한다.

$$D[j]=\frac{1}{K}\sum_{i=0}^{K} T_i[j]-\frac{1}{K}\sum_{i=0}^{K} S_i[j] = \overline{T}[j]-\overline{S}[j] \quad (3)$$

- 차분 전력 데이터 D[j]가 추측한 비트나 다음 비트 위치에서 피크를 보여주면 공격대상 카드의 비밀키와 추측한 비트가 비밀키와 다름을 알 수 있다.
- 비밀키를 NAF로 변형됨으로 올바른 비트가 '0'으로 확인되면 다음 비트는 '0'과 '1' 그리고 '-1'로 분류된다. 올바른 비트가 '1'이나 '-1'로 확인되면 다음 비트는 반드시 '0'이므로 그 다음 비트를 공격 대상으로 한다.

3.3 차분 전력분석 공격의 실험 결과

논문에서는 덧셈-뺄셈 스칼라 곱셈연산 시 비밀키에 대하여 NAF 형태로 표현된 키를 적용하기로 하였다. 이와 같은 스마트 카드에 대한 공격을 할 경우에는 다음과 같은 NAF의 성질이 분석에 이용된다. 먼저 NAF은 인접한 비트가 '1'이면 다음 비트는 '1'이 나올 수 없다. 식 (2)에서 c_i는 세 가지의 경우가 나오므로 차분 전력분석 공격 과정에서 정확한 비밀키를 얻기 위해 최소한 두 번 이상의 추측이 필요하다. NAF를 사용하는 알고리듬은 두 번째 비트가 반드시 '0'이다. 하지만 세 번째 비트는 '0'과 '1' 그리고 '-1'의 경우를 모두 고려 해야 한다. 반면 비밀키 비트가 '1'이나 '-1'임을 알면 반드시 다음 비트는 '0'임을 알 수 있다.

공격의 실제적인 예로서 스마트 카드에 사용된 ECC가 $GF(p)$상에서 p=1013, a=3 그리고 b=12이고 비밀키가 589, 즉, 이진수로 1001001101이라 할 때 NAF를 적용하면 $1001010\overline{1}01$로 변경된다. 세 번째 비트를 추측할 때 연산될 값들을 보면 표 2와 같다. 공격자는 두 번째 비트가 '0'임을 알고 있으므로 세 번째 비트부터 추측하게 되는데 세 번째 비트가 가질 수 있는 비트는 0, 1 혹은 $\overline{1}$이다. 비밀키 중 5개의 비트만을 연산해 보면 공격대상 비밀키가 "10010"를 연산할 때 추측한 키 d1을 가정하면 "101XX"로 추측되고 네 번째 비트에서 연산되는 값은 10P이거나 11P가 연산될 수 있다. 또 추측한 키 d_2를 가정하면 "$10\overline{1}$XX"로 추측할 때는 다음 연산되는 값은 6P이거나 7P이다. 따라서 세 번째 비트가 원래 공격용 비밀키와 같지 않으면 차분 전력 신호는 피크를 나타낼 것이다. 또한 해당 비트가 0인지, 1인지 혹은 $\overline{1}$인

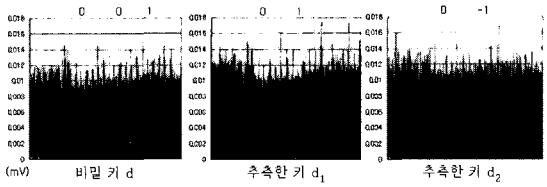
(표 2) 세 번째 비트의 연산될 데이터
(X는 예상할 수 없는 키)

비밀키 d	Bit	1	0	0	1	0	…
	Doubling		2P	4P	8P	18P	…
	Addition				9P		…
추측한 키 d_1	Bit	1	0	1	X	X	…
	Doubling		2P	4P	10P	·	…
	Addition			5P	11P	·	…
추측한 키 d_2	Bit	1	0	-1	X	X	…
	Doubling		2P	4P	6P	·	…
	Addition			3P	7P	·	…

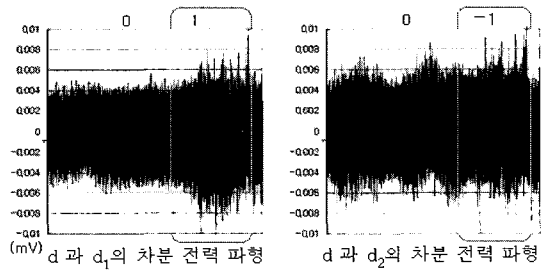
지는 다음 비트의 전력 파형을 분석한 후, 차분 값을 비교하면 서로 다른 비트의 경우에 피크가 형성됨을 알 수 있다. 이는 추측한 비트에 따라 연산 과정이 다르므로 차분하는 과정에서 다음 비트의 덧셈 연산을 수행한 전력 파형과 두배 연산을 수행한 전력 파형이 차분된다.

스마트 카드에서 그림 1의 스칼라 곱셈 알고리듬을 수행할 경우 알고리듬 자체에는 조건문이 있으며 이 조건문에 따라 두배 연산만 할 것인지, 덧셈 연산을 할 것인지가 결정된다. 그런데 두배 연산과 덧셈 연산의 수행시간과 전력 소비량이 같지 않다는 점에 유의할 필요가 있다. 따라서 세 번째 비트 '0'이 두배 연산을 실행한 이후를 관찰해 보면, 추측한 비트가 '1'이나 '-1' 인 경우에는 두배와 덧셈 연산의 전력소비량 차이에 의해 두 스마트 카드의 차분 전력 파형은 피크가 형성됨을 볼 수 있다. 따라서 공격 대상용 스마트 카드의 정확한 비밀 비트가 '0'임을 알 수 있다. 그림 3은 비밀키와 추측한 키의 평균 전력 파형으로 측정 횟수를 200회로 설정하고 반복적인 실험을 수행하여 얻은 전력 파형이다.

비밀키와 추측한 키가 동일하게 연산되는 영역과 그렇지 않은 영역을 전력 파형으로 구별하기 위해 문턱전압 V_{th}=2mV로 설정하였다. 그림 4는 평균한 비밀키 d와 추측한 키 d_1, d_2를 차분하여 얻은 전력 파형으로서 추측이 틀린 세 번째 비트



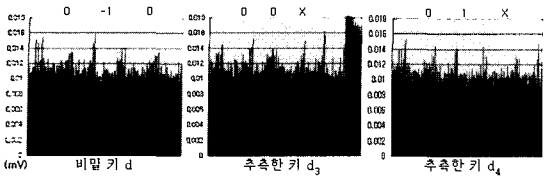
(그림 3) 비밀키와 추측한 키의 평균 전력 파형



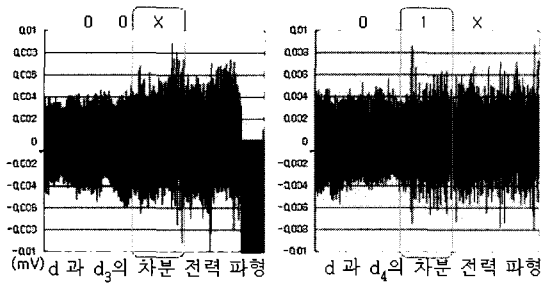
(그림 4) 비밀키에 대한 각각의 차분 전력 파형

에서 피크가 형성됨을 확인할 수 있다. 그림에서 보는 바와 같이 피크가 나타나는 비트 위치에서는 추측이 틀렸음을 알 수 있으며 실험용 스마트 카드의 비밀 키 '0'으로 수정한 후 다음 비트를 공격한다.

다음으로 공격 대상 비밀키의 비트가 '1'이거나 '-1'인 경우를 고려해 보자. 보다 상세한 설명을 위해 NAF로 표현된 공격 대상 비밀키가 $1001010\bar{1}01$라 가정하고 비트 '$\bar{1}$'에 대한 실험을 통해 분석 결과를 제시한다. 여덟 번째의 비트가 '0'이 아닌 '$\bar{1}$'비트이므로 수행시간이 '0'일 때보다 길고 '1'이라고 추측할 때와 거의 동일한 연산 시간을 가진다. 그러나 '1'이라고 추측하여 동일한 연산 시간을 가지더라도 추측한 키의 덧셈 연산에서 연산되는 데이터 값이 달라서 공격 대상의 비트부터 피크를 볼 수 있다. 그러나 추측한 키가 '0'일 때를 고려해 보자. 두배 연산 수행시간은 비밀키의 덧셈 연산 수행 시간에 비해 빨라서 차분 전력은 추측용 카드의 아홉 번째 비트의 두배 연산 과정과 공격 대상 비밀키의 여덟 번째 비트에 대한 덧셈 연산 과정의 소모전력 파형이 차분된 것이다. 따라서 추측한 비트의 다음 비트, 즉 아홉 번째 비트에서 피크를 확인할 수 있다.



(그림 5) 비밀키와 추측한 키의 평균 전력 파형



(그림 6) 비밀키에 대한 차분 전력 파형

결론적으로 추측한 비트를 '0'으로 예측하였는데 공격대상 비밀키와 다른 경우에는 피크가 추측한 비트의 다음 비트 위치에서 생성되는 것을 미리 주지하여야 한다. 이것은 덧셈과 뺄셈 연산시에 수행하는 연산에 따른 수행 시간이 다르기 때문이다. 그림 5는 비밀키와 추측한 키에 대하여 200회의 측정 회수로 소모 전력을 수집한 후 이를 평균한 파형이다.

그림 6은 전력 피크를 확인하기 위한 문턱전압 V_{th}=2mV로 설정할 때 차분 전력분석 파형을 나타낸 것으로 잘못 추측한 비트가 '1'일 때는 추측한 비트 해당 위치에서 피크가 발생됨을 볼 수 있다. 그러나 '0'으로 잘못 추측했을 경우에는 추측한 비트 위치에서는 피크를 볼 수 없고 다음 비트 위치에서 피크가 형성됨을 확인할 수 있다.

스칼라 곱셈 속도를 높이기 위해 비밀키를 NAF 형태로 표현한 후 덧셈-뺄셈 알고리듬을 수행해도 공격 대상 카드와 키를 변경할 수 있는 카드만 있으면 MESD 공격이 가능함을 확인할 수 있다. 이러한 사실은 차분 전력 분석 공격에 대응하기 위해서는 최소한 비밀키에 대한 스칼라 곱셈 시에는 비밀키가 랜덤한 특성을 유지하도록 재부호화 할 필요가 있다. 매 스칼라 곱셈 시마다 비밀키의 부호화 방법이 달라지면 공격 시마다 랜덤한 전력 파형을 생성하게 될 것이고 이는 전력 차분의 상관성을 없애 유용한 공격 대응 방법이 될 수 있다.

4. 결 론

본 논문에서는 부-채널 공격 중에서 강력한 공격 방법인 차분 전력 분석 공격을 타원곡선 암호 시스템에 적용하였다. 스마트 카드 설계 시 수학적으로 안전하다는 타원곡선 암호 알고리듬을 사용하고 고속화를 위해 NAF 부호를 통한 덧셈-뺄셈 스칼라 곱셈 방법을 사용했다고 하더라도 차분 전력분석 공격에는 대응할 수 없음을 실험을 통하여 검증하였다. 따라서 스마트 카드에 암호 알고리듬을 구현할 경우에는, 물리적 측면의 안전성을 고려하여 단순 전력분석 공격, 차분 전력분석공격 그리고 기타 다른 부-채널 공격에도 대응할 수 있는 안전한 알고리듬을 사용하는 것이 매우 중요하다.

참 고 문 헌

[1] W. Rankl and W. Effing, Smart Card Handbook, Second Edition, JOHN WILY & SONS, LTD. 1999.

[2] P. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems," in Proceedings of Advances in Cryptology-CRYPTO'96, pp. 104~113, Springer-Verlag, 1996.

[3] E. Biham and A. Shamir, "Differential Fault Analysis of Secret Key Cryptosystems", in Proceedings of Advances in Cryptology-CRYPTO'97, pp. 513~525, Springer-Verlag, 1997.

[4] P. Kocher, J. Jaffe, and B. Jun, "Introduction to Differential Power Analysis and Related Attacks," Available at http://www.cryptography.com/dpa/technical/index.html, 1998.

[5] P. Kocher, J. Jaffe, and B. Jun, "Differential

Power Analysis," in Proceedings of Advances in Cryptology-CRYPTO'99, pp. 388~397, Springer-Verlag, 1999.

[6] Josyula R. Rao and Pankaj Rohatgi, "Thev-EMpowering Side-Channel(s)," in Pre-Proceedings of Workshop on Cryptographic Hardware and Embedded Systems-CHES'02, pp. 29~45, Springer-Verlag, 2002.

[7] T. S. Messerges, E. A. Dabbish and R. H. Sloan, "Investigations of Power Analysis Attacks on Smartcards," in Proceedings of USENIX workshop on Smartcard Technology, May, 1999.

[8] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Power Analysis Attacks on Moular Exponentiation in Smart cards," in Proceedings of Workshop on Cryptographic Hardware and Embedded Systems-CHES'99, pp. 144~157, Springer-Verlag, 1999.

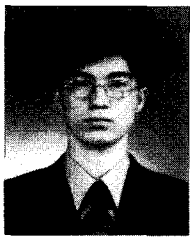
[9] N. Koblitz, "Elliptic curve cryptosystems," Mathematics of Computation, vol. 48, pp. 203~209, 1987.

[10] V. Miller, "Uses of elliptic curves in crypto in cryptography," in Proceedings of Advances in Cryptology-CRYPTO'85, pp. 417~426, Springer-Verlag, 1985.

[11] F. Morain, J. Olivos. "Speeding up the computation of an elliptic curve using addition-subtraction chains", Inform. Theory Appl. 24, pp. 531~543, 1990.

[12] 안만기, 곽동진, 이훈재, 하재철, 문상재, "멱승 알고리듬의 데이터 변화를 이용한 스마트 카드의 차분 전력분석 공격," 통신정보합동학술대회, Vol. 12, No. 1, pp. IV-A.1.1~4, April, 2002.

◐ 저 자 소 개 ◑



안 만 기
2000년 경북대학교 전자전기공학부 졸업(학사)
2001년 삼성전자 프린터 사업부 C-LBP 연구원
2003년 경북대학교 대학원 전자공학과 졸업(석사)
2003년 4월~현재 : 국방품질관리소 연구원
관심분야 : 정보보호, 스마트카드 보안, 정보통신 etc.
E-mail : mkahn@dqaa.go.kr

하 재 철
1989년 경북대학교 전자공학과 졸업(학사)
1993년 경북대학교 대학원 전자공학과 졸업(석사)
1998년 경북대학교 대학원 전자공학과 졸업(박사)
2000년 나사렛대학교 전자계산소장
2002년 나사렛대학교 학술정보관장
1998년~현재 : 나사렛대학교 정보통신학과 조교수
관심분야 : 정보보호, 네트워크 보안, 스마트카드 보안, etc.
E-mail : jcha@kornu.ac.kr

이 훈 재
1985년 경북대학교 전자공학과 졸업(학사)
1987년 경북대학교 대학원 전자공학과 졸업(석사)
1998년 경북대학교 대학원 전자공학과 졸업(박사)
1998년 국방과학연구소 선임연구원
2002년 경운대학교 컴퓨터전자정보공학부 조교수
2002년~현재 : 동서대학교 인터넷공학부 조교수
관심분야 : 암호이론, 네트워크보안, 디지털 통신, etc.
E-mail : hjlee@dongseo.ac.kr

문 상 재
1972년 서울대학교 공업교육(전자)학과 졸업(학사)
1974년 서울대학교 대학원 전자공학과 졸업(석사)
1984년 미국 UCLA 전자공학과 졸업(박사)
1985년 UCLA Postdoctoral 근무, 미국 OMNET 컨설턴트
1974년~현재 : 경북대학교 공과대학 전자전기컴퓨터학부 교수
2000년~현재 : 경북대학교 이동네트워크 정보보호기술 연구센터 소장
2002년~현재 : 한국정보보호학회 명예회장
관심분야 : 정보보호, 디지털 통신, 이동 네트워크, etc.
E-mail : sjmoon@knu.ac.kr