Journal of The Korea Institute of Information Security & Cryptology(JKIISC) ISSN 1598-3986(Print)
VOL.23, NO.4, August 2013 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2013.23.4.585

BNP 멱승 알고리듬에 대한 물리적인 조합 공격 및 대응책

김 형 동,† 하 재 철‡
호서대학교

A Physical Combined Attack and its Countermeasure on BNP Exponentiation Algorithm

Hyung-Dong Kim,† Jae-Cheol Ha‡
Hoseo University

요 약

최근 정보보호 장치를 이용하여 암호 알고리듬을 수행할 경우 부채널 공격과 오류 주입 공격을 결합한 물리적 조합 공격에 의해 비밀 키가 노출될 수 있음이 밝혀졌다. 특히, RSA 암호 시스템에서 수행하는 멱승 연산에 대해 한 번의 오류 주입과 전력 분석을 통해 조합 공격이 가능하다. 본 논문에서는 SPA(Simple Power Analysis)와 FA(Fault Attack)을 방어하기 위해 제안되었던 BNP(Boscher, Naciri, and Prouff) 멱승 알고리듬이 조합 공격에 취약함을 보이고자 한다. 또한, 오류 확산 기법에 기반하여 개인 키를 랜덤화시키는 대응 방안을 제안한다.

ABSTRACT

Recently, the combined attack which is a combination of side channel analysis and fault attack has been developed to extract the secret key during the cryptographic processes using a security device. Unfortunately, an attacker can find the private key of RSA cryptosystem through one time fault injection and power signal analysis. In this paper, we diagnosed SPA/FA resistant BNP(Boscher, Naciri, and Prouff) exponentiation algorithm as having threats to a similar combined attack. And we proposed a simple countermeasure to resist against this combined attack by randomizing the private key using error infective method.

Keywords: Side Channel Analysis, Fault Attack, Exponentiation, Combined Attack

I. 서 론

정보보호용 장치를 이용하여 암호화 연산을 수행할 경우, 칩 내부에 저장된 비밀 키를 이용하게 된다. 이 경우 장치가 동작할 때 발생하는 전자기적인 부가 정보를 이용하여 비밀 키를 찾아내는 부채널 분석(Side Channel Analysis, SCA) 공격이 1996년 Kocher에 의해 처음 제안되었다[1]. 부채널 공격은 주로 암호 장치의 소비 전력 신호를 측정하여 비밀 키와의 상관도를 조사하는 공격으로서 크게 단순 전력 분석(Simple Power Analysis, SPA) 공격과 차분 전력 분석(Differential Power Analysis, DPA) 공격으로 나눌 수 있다[2].

한편, 오류 주입 공격(Fault Attack, FA)은 1997년 Boneh 등에 의해 처음으로 제안된 물리적 공격으로서 암호 알고리듬을 수행하는 동안 공격자는

접수일(2013년 4월 22일), 수정일(2013년 5월 27일), 게재 확정일(2013년 7월 9일)
† 주저자, karuceace@nate.com
‡ 교신저자, jcha@hoseo.edu (Corresponding author)

암호용 칩에 고의적으로 오류를 주입하고 그 출력을 분석하여 비밀 키를 찾아내는 공격 기법이다[3]. 특히, 부채널 공격과 오류 공격은 국제 표준 블록 암호 알고리듬인 AES[4]나 RSA(Rivest, Shamir, and Adelman)[5] 등을 대상으로 많이 시도되었지만 두 공격 방법은 각각 독립적으로 연구되어 왔다.

그러나 최근 수동적 공격 방법인 부채널 공격과 능동적 공격 방법인 오류 공격을 결합한 조합 공격(Passive and Active Combined Attack, PACA)이 제안되었다[6]. 공개 키 암호 알고리듬인 RSA 멱승 알고리듬에 대한 조합 공격은 오류를 주입한 후 누출되는 전력 파형을 관찰함으로써 개인 키를 추출하는 방식을 사용하였다. 이 조합 공격은 SPA를 방어하기 위한 Left-to-Right형 Square and Multiply 멱승(exponentiation) 알고리듬에 대해 처음 시도되었고 실험을 통해 증명하였다. 그 후 블록 암호 알고리듬인 AES에 대해서도 조합 공격이 시도된 바 있다[7, 8].

본 논문에서는 SPA와 FA를 동시에 방어하기 위해 제안된 BNP(Boscher, Naciri, and Prouff) 멱승 알고리듬[9]에서도 조합 공격이 가능함을 밝히고자 한다. 또한 조합 공격에 대응하는 방어 대책으로서 오류 확산 기법에 기반한 개인 키 랜덤화 기법을 제안한다. 제안하는 대응 알고리듬은 기존의 조합 공격에 안전하며 추가적인 연산이 적어 매우 효율적으로 구현될 수 있다.

II. RSA에 대한 물리적 조합 공격

2.1 RSA 멱승 알고리듬

공개 키 암호 시스템 RSA에서는 비밀 소수 p와 q의 곱인 모듈러스 n을 계산하여 공개한다. 그리고 $(p-1)\cdot(q-1)$과 서로 소(co-prime)인 공개 키 e를 생성하며 개인 키 d를 다음과 같이 계산하여 비밀로 보관하여 사용한다.

$d = e^{-1} \bmod (p-1)\cdot(q-1)$

주어진 메시지 M에 대한 서명은 개인 키를 사용하여 다음과 같이 생성한다.

$S = M^d \bmod n$

RSA 서명 생성시 계산 효율을 높이기 위해서 중국인의 나머지 정리를 사용한 RSA-CRT(RSA with Chinese Remainder Theorem)[10] 기법을 사용하기도 한다. 이때 일반 RSA 서명이나 RSA-CRT 서명을 수행할 때 멱승 연산이 필수적이며 가장 간단한 멱승 알고리듬으로서 이진(binary) 방법이 있다.

그러나 이진 멱승 알고리듬은 SPA 부채널 공격에 취약한 특성이 있어 Square and Multiply Always 멱승 알고리듬이 제안되기도 하였으나 이 알고리듬은 C-Safe 오류 공격[11]에 취약하다고 알려져 있다. 따라서 SPA/C-Safe 공격을 방어하기 위해 더미(dummy) 곱셈 연산이 없는 Montgomery Ladder 멱승 알고리듬[12]이나 Atomicity에 기반한 멱승 알고리듬[13] 그리고 BNP 멱승 알고리듬[9] 등이 제안되었다.

한편, 2007년 Amiel과 Villegas에 의한 물리적 조합 공격은 SPA/FA 공격을 방어할 수 있는 Atomicity에 기반한 멱승 알고리듬에 직접 적용되었다[6]. 이 멱승 알고리듬을 나타낸 것이 [그림 1]인데 논문에서는 DPA를 방어하기 위해 작은 랜덤 수 r_1과 r_2를 이용하여 메시지를 랜덤화하는 방법을 사용하였다. 여기서 $\neg k$는 비트 k에 대한 부정(negative) 논리를 의미한다.

입력 : 메시지 M, l 비트의 개인 키 d
$d = (d_{l-1}d_{l-2}\cdots\cdots d_1d_0)_2$
출력 : $M^d \bmod n$

1. 작은 크기의 랜덤 수 r_1, r_2 생성
2. $R_0 = 1 + r_1 \cdot n$
3. $R_1 = M + r_1 \cdot n \bmod (r_2 \cdot n)$
4. $k = 0$
5. For i from $l-1$ to 0 do
   5.1 $R_0 = R_0 \cdot R_k \bmod (r_2 \cdot n)$
   5.2 $k = k \oplus d_i$
   5.3 $i = i - \neg k$
6. $S = R_0 \bmod n$
7. Return(S)

[그림 1] SPA/DPA/C-safe 공격 방어 알고리듬

이 멱승 알고리듬을 사용할 때 주의할 것은 서명을 출력하기 전에 오류 주입 여부를 최종적으로 확인하는 과정을 추가하거나, 서명문 S를 공개 키로 멱승 연산을 수행하여 메시지 M이 되는지 확인해야 한다는 점이다. 그러나 이러한 확인 과정은 [그림 1]의 단계 6의 모든 연산이 끝나는 시점에 수행된다. 따라서 다음에 설명할 조합 공격이 시도되어도 전력 신호는 이미 노출된 상태이므로 최종 오류 주입 여부를 확인하는 과정은 너무 늦은 검사가 된다.

2.2 RSA 알고리듬에 대한 조합 공격 및 대응책

Amiel과 Villegas는 상기한 Atomicity에 기반한 SPA/DPA/C-Safe 공격을 방어하는 멱승 알고리듬에 대해 오류 공격과 SPA 공격을 조합하여 비밀 키를 찾아낼 수 있음을 보였다[6]. 이 공격의 핵심은 알고리듬 수행 중 오류를 주입하여 [그림 1]의 단계 2를 수행하지 않고 건너뛰게 하는 것이다. 그리고 이 상태에서 소비되는 전력 파형을 관측하여 SPA 방법으로 개인 키 d를 찾아내는 기법이다. 즉, R_0는 일반적으로 0으로 초기화 될 것이고 단계 2를 수행하지 않으면 이 멱승에서는 자승 연산인 $R_0 = R_0 \cdot R_0 = 0 \cdot 0 \bmod n$와 곱셈 연산인 $R_0 = R_0 \cdot M \bmod n$을 수행하게 된다. 그런데 이 두 연산은 소비되는 전력이 달라 서로 구별이 가능하다. 따라서 개인 키 d의 각 비트인 d_i가 0일 경우에는 자승만 수행하고 1일 경우에는 자승과 곱셈을 수행한다는 점을 이용하면 단순 전력 파형 관측만으로도 개인 키를 구할 수 있다.

이러한 조합 공격을 방어하기 위한 방안으로 Schmidt 등은 공격이 이루어지는 [그림 1]의 for 문 내의 매 루프마다 R_0나 R_1이 0이 되는지 검사하여 개인 키를 복구하지 못하도록 멱승 알고리듬을 개선하였다[14]. 여기서 Schmidt 등이 가정했던 공격자의 오류 공격 모델은 3가지이다. 공격자는 특정 레지스터에 랜덤한 값을 주입하거나 알려진 값(모두 0 혹은 1인 경우도 포함)을 주입할 수 있는 능력이 있다고 가정하였다. 그리고 공격자는 명령어를 건너뛰거나 순환 루프를 빠져나올 수 있다는 가정을 하였다. 또한, 한 번의 멱승 알고리듬 수행시 한번의 오류만 주입할 수 있다는 1차 오류 주입 공격만을 전제도 대응책을 설계하였다.

그러나 Schmidt 등의 대응 방법은 Feix와 Venelli에 의해 다시 조합 공격이 가능하다는 취약점이 발견되었다[15]. Schmidt 등의 대응 방법이 취약한 이유는 오류 공격이 발생하면 개인 키가 이미 알려진 값으로 변경된다는 점 때문이다. 따라서 Feix와 Venelli는 오류 공격이 감지한 이후에라도 개인 키를 랜덤하게 바꾸어 주어야 추가적인 공격을 막을 수 있다고 주장하였다. 한편, Feix와 Venelli는 자승과 곱셈을 구별할 수 있다는 가정하에서 공격자가 오류 주입을 통해 지수(exponent)에 대한 블라인딩을 생략시켜도 개인 키를 보호할 수 있는 방안을 제안였는데 이 경우 Schmidt 등의 대응 알고리듬에 비해 각 루프마다 랜덤 수 발생 및 모듈라 감소 연산이 추가된다.

III. BNP 알고리듬에 대한 조합 공격과 대응책

3.1 BNP 멱승 알고리듬에 대한 조합 공격

한편, SPA와 C-safe 오류 공격을 방어하기 위한 알고리듬으로 BNP 멱승 알고리듬[9]이 있다. BNP 알고리듬은 Right-to-Left 형태의 이진 알고리듬으로서 [그림 2]에 나타낸 바와 같다. BNP 알고리듬에서도 DPA 공격을 방어하기 위해 [그림 1]과 같이 작은 랜덤 수 r_1과 r_2 를 이용하여 메시지를 랜덤화하는 방법 등을 사용할 수 있으나 설명의 편의를 위해 원 논문에서 제시한 SPA/C-safe 오류 공격만 방어하는 알고리듬으로 설명하고자 한다.

입력 : 메시지 M, l 비트의 개인 키 d
$d = (d_{l-1} d_{l-2} \ldots\ldots d_1 d_0)_2$
출력 : $M^d \bmod n$ or "error"

1. $R[0] = 1$
2. $R[1] = 1$
3. $A = M$
4. For i from 0 to $l-1$ do
   4.1 $R[\overline{d_i}] = R[\overline{d_i}] \cdot A \bmod n$
   4.2 $A = A^2 \bmod n$
5. if$((M \neq R[0] \cdot R[1] = A \bmod n) \& (A \neq 0))$
   then Return$(R[0])$
   else Return("error")

[그림 2] SPA/C-safe 공격 방어 BNP 알고리듬

BNP 알고리듬에서는 두 개의 레지스터를 이용하는데 개인 키의 각 비트가 0인지 1인지에 따라 해당되는 값을 저장하고 이를 통해 단계 5에서 오류 주입여부를 판단한 후, 이상이 없으면 서명을 출력한다. 물론 이 알고리듬은 RSA-CRT 연산에서도 추가적인 오류 주입 공격을 방어하기 위해 유용하게 적용할 수 있다.

본 논문에서는 이러한 BNP 멱승 알고리듬에서도 조합 공격으로 개인 키를 공격할 수 있음을 보이고자 한다. 조합 공격의 형태는 Amiel과 Villegas가 제안했던 방법[6]과 비슷한 방법으로 처음 초기화 과정에서 오류 주입을 통해 해당 명령어를 건너뛸 수 있고 이후에는 단순 전력 분석이 가능함을 전제로 한다.

먼저 제안 공격에서는 [그림 2]의 단계 1을 건너뛰어 $R[0]$의 초기 값 0이 그대로 저장된 후 멱승 연산이 진행됨을 가정하자. 이때 단계 4의 연산을 보면 다음과 같이 두 종류의 연산만 수행된다.

$d_i=0$일 때, $R[1]=R[1]\cdot A \bmod n$

$d_i=1$일 때, $R[0]=R[0]\cdot A=0\cdot A \bmod n=0$

따라서 랜덤한 두 값을 모듈러 곱셈하는 것과 0과 곱하여 연산하는 것을 해밍웨이트 차이에 의해 단순 전력파형으로 구별할 수 있다면 쉽게 개인 키를 얻을 수 있다. 물론 단계 5의 검사 과정에서 오류 주입 사실을 검출할 수 있겠지만 이미 그때는 전력 파형이 누출된 상태이므로 조합 공격을 막을 수 없다.

또한, 단계 2에서 $R[1]$의 값이 0이 되도록 건너뛰는 공격도 동일한 개념으로 적용될 수 있다. 이 경우에는 다음과 같이 두 종류의 연산만 수행되므로 SPA에 의해 개인 키가 노출될 수 있다.

$d_i=0$일 때, $R[1]=R[1]\cdot A=0\cdot A \bmod n=0$

$d_i=1$일 때, $R[0]=R[0]\cdot A \bmod n$

결론적으로 모듈러 곱셈시 일반 랜덤 수를 모듈러 곱셈하는 것과 0을 곱하여 모듈러 곱셈을 하는 것을 단순 전력 분석을 통해 구별할 수 있다면 BNP 멱승 알고리듬은 공격 시점이 1단계 혹은 2단계로 늘어나게 되어 Atomicity에 기반한 멱승 알고리듬보다 더 용이하게 공격된다고 볼 수 있다.

3.2 조합 공격에 대한 대응 방법

따라서 BNP 멱승 알고리듬에 대해 조합 공격을 방어할 수 있는 대응책이 필요하다. 제안하는 대응방법에서는 개인 키를 먼저 랜덤 수와 XOR하여 블라인딩한 상태에서 레지스터 $R[0]$나 $R[1]$이 오류 공격에 의해 0으로 되었을 때에는 개인 키 d를 제대로 복구할 수 없도록 하여 개인 키를 보호하고자 한다. 즉, 오류 주입시 오류가 주입된 사실을 검출 기법을 통해 인지하여 그 오류를 개인 키로 확산시키는 방법이다. 〔그림 3〕은 기본 BNP 멱승 알고리듬에 명령어를 건너뛰고 전력을 분석하는 조합 공격을 방어하기 위한 알고리듬을 제시한 것이다.

입력 : 메시지 M, l 비트의 개인 키 d
$d=(d_{l-1}d_{l-2}\cdots\cdots d_1d_0)_2$
출력 : $M^d \bmod n$ or "error"

0. l비트의 랜덤 수 r을 생성
1. $R[0]=1$
2. $R[1]=1$
3. $A=M$
4. $c=r\oplus d$
5. For i from 0 to $l-1$ do
   5.1 $c_i=((\perp R[0])\wedge(\perp R[1])\wedge c_i)\oplus r_i$
   5.2 $R[\overline{c_i}]=R[\overline{c_i}]\cdot A \bmod n$
   5.3 $A=A^2 \bmod n$
6. if$((M\not\equiv R[0]\cdot R[1]=A \bmod n)\&(A\neq 0))$
   then Return($R[0]$)
   else Return("error")

〔그림 3〕 조합 공격을 방어하는 BNP 알고리듬

제안하는 알고리듬에서 $\perp R[i]$ 연산은 $R[i]$가 0이면 결과는 0이 되며 $R[i]$가 0이 아니면 결과가 1이 되는 연산자로서 오류 주입 여부를 감지하여 개인 키를 정상적으로 복원하는 작용을 한다. 즉, $R[i]$가 0이 되면 개인 키를 공격자가 알지 못하는 다른 값 c_i로 변하게 함으로써 조합 공격을 쉽게 방어할 수 있다. 물론 단계 5.1을 if 문과 같은 조건문을 이용하여 아래처럼 검사 기법으로 구현할 수도 있다.

```
if((R[0] ≠ 0) ∧ (R[1] ≠ 0)) {
    c_i = c_i ⊕ r_i
}
```

그러나 Feix와 Venelli에서 가정한 바와 같이 위의 if문에 플래그에 오류를 주입하여 쉽게 문장을 건너뛸 수 있다고 가정하면, 공격자는 $R[i]$를 0으로 초기화시킨 후 다시 if문에 대한 대한 2차 오류 주입 공격을 시도하여 개인 키 한 비트를 찾을 가능성도 있다.

따라서 〔그림 3〕의 5.1과 같이 if문과 같은 조건문을 사용하지 않고 개인 키를 복원하는 방법이 필요하다. 특히, $\perp R[i]$ 연산을 산술적으로 처리하는 방법이 필요하다. 아래 방법은 $b=\perp R[i]$ 연산을 처리할 수 있는 예를 나타낸 것이다. 이러한 기능은 명령어를 건너뛰는 공격에 견딜 수 있도록 for문 등으로도 구현할 수 있다.

```
k = b = 0
while(!b ∧ (k < l)) {
        b = (R[i] ≫ k)%2
        k++
}
```

제안 방식의 또 다른 특징은 $R[i]$ 값을 검사하는 시점을 모듈러 곱셈이 발생하기 이전에 수행하게 함으로써 모듈러 곱셈으로 인한 d_i 비트의 노출을 최소화 하였다. 반면 기존의 방법들은 모듈러 곱셈을 수행한 후 오류 주입 여부를 검사하도록 하여 단순 전력 분석에 의한 개인 키 비트의 노출 가능성을 그대로 내재하고 있다. 또한, 제안 방식은 오류 확산 기법을 이용하면서도 단계 5.1에서 보는 바와 같이 각 루프마다 한 비트씩 개인 키를 복원하도록 하여 추가되는 연산량을 최소화 하였다.

〔표 1〕 멱승 알고리듬에 대한 조합 공격 대응책 비교

구분	Schmidt 등 방법〔14〕	Feix-Venelli 방법〔15〕	제안 방법
대상 멱승 알고리듬	Left-to-Right Atomicity	Left-to-Right Atomicity	Right-to-Left BNP
방어책의 핵심	레지스터가 0인 경우 개인 키 d를 고정된 값으로 변경	레지스터가 0인 경우 개인 키 d를 랜덤한 값으로 변경	레지스터가 0인 경우 개인 키 d를 제대로 복원하지 못함
안전성	Feix-Venelli 에 의해 취약점 발견	조합 공격에 안전함 검사시 if문 사용	조합 공격에 안전함 if문을 제거함
SPA 특성	d의 블라인딩 과정을 생략하면 자승과 곱셈을 구별하는 SPA에 취약	d의 블라인딩 과정을 생략하면 자승과 곱셈을 구별하는 SPA에 강함	자승과 곱셈을 구별하는 SPA에 강함
모듈러 연산	평균 $1.5l$번 모듈러 곱셈	평균 $1.5l$번 모듈러 곱셈 + 평균 $1.5l$번의 모듈러 감소	$2l$번 모듈러 곱셈

한편, 제안 방식에서 랜덤 수 r과 그림 3의 단계 1이나 2에서 동시에 오류가 주입되는 2차 오류를 가정해 볼 필요가 있다. 제안 방법은 랜덤 수 발생기에 대한 오류 주입 공격으로 인해 랜덤 수 r이 알려진 값(모두 0이나 1인 경우도 포함)으로 저장되고, 연속적인 2차 공격에 의해 $R[i]$를 0으로 초기화할 수 있다고 하더라도 기존의 조합 공격이 적용되지 않도록 설계되었다. 즉, 2차 오류 주입 공격에서 $R[i]$중 하나가 0이면 단계 5.1에서 새로운 c_i 는 r_i가 되는데 이 역시 d_i와는 관련이 없으므로 비밀 키 정보를 누출시키지 않게 된다. 결국, $R[i]$만 0이 되는 1차 오류 주입 공격에서는 c_i값을 공격자가 알 수 없는 랜덤 수 r_i로 바꾸어 주며, $R[i]$와 r이 동시에 0이 되는 2차 공격에서는 c_i를 강제로 0으로 초기화함으로써 비밀 키에 대한 노출이 없도록 하였다.

지금까지 제안된 멱승 알고리듬에 대한 조합공격의 대응책을 비교한 것이 〔표 1〕이다. 기존의 대응 방법과 제안 방법은 공격 대상 멱승 알고리듬이 다르고 SPA나 DPA 등을 방어하는 방법이 서로 다르므로 절대적인 비교는 어렵다. 다만 Feix-Venelli 방법은 Schmidt 등의 방법에서 오류 주입시 개인 키 d를 랜덤하게 바꾸도록 하였으며 Atomicity 멱승 연산 방법의 단점인 곱셈과 자승 연산이 구별 가능한 환경에서 SPA 공격〔16〕이 되는 것을 방지하도록 구현하였다.

논문에서의 조합공격 대응 방식은 BNP 알고리듬에 기반하고 있으며 동일한 공격 모델하에서 비교적 간단한 방법으로 조합공격을 방어하도록 설계하였다. 특히, 논문 〔9〕에서는 BNP 알고리듬이 RSA-CRT〔10〕에서 유용하게 사용할 수 있다고 주장하였는데, 본 논문에서 제안하는 멱승 방식도 RSA-CRT 연산에 사용된 특성을 그대로 유지하게 되어 효과적인 적용이 가능하다. 결국, 제안 방법은 Schmidt 등의 대응 방법이나〔14〕 Feix와 Venelli의 대응 방법〔15〕에 비해 계산량이나 안전성면에서 효율적이므로 Atomicity에 기반한 멱승 알고리듬에 대한 조합 공격〔6〕의 대응책으로도 유용하게 사용할 수 있다.

IV. 결 론

본 논문에서는 BNP 멱승 알고리듬이 오류 주입 공격과 SPA 부채널 공격이 결합된 조합 공격에 취약함을 증명하였다. 또한, 오류 주입이 감지되면 개인 키 값에 랜덤한 값이 확산되는 조합 공격 대응 기법을 제안하였다. 제안하는 대응 방법은 오류 확산 기법에 기반하여 비교적 적은 추가 연산으로 물리적 조합 공격을 효과적으로 방어할 수 있다.

참고문헌

〔1〕 P. Kocher, "Timing Attacks on Implementation of Diffie-Hellman, RSA, DSS, and Other Systems," CRYPTO'96, LNCS 1109, pp. 104-113, 1996.

〔2〕 P. Kocher, J. Jae, and B. Jun, "Differential power analysis," CRYPTO'99, LNCS 1666, pp. 388-397, 1999.

〔3〕 D. Boneh, R. DeMillo, and R. Lipton, "On the Importance of Checking Crypto-

graphic Protocols for Faults," EUROCRYPTO'97, LNCS 1233, pp. 37-51, 1997.
[4] National Institute of Standards and Technology, "Advanced Encryption Standards," NIST FIPS PUB 197, 2001.
[5] R. Rivest, A Shamir, and L, Adelman, "A method for obtaining digital signature and public-key cryptosystems," Comm. of the ACM vol. 21, no 2, pp. 120-126, 1978.
[6] F. Amiel, K. Villegas, B. Feix, and L. Mercel, "Passive and Active Combined Attacks: Combining fault attacks and side channel analysis," FDTC'07, IEEE-CS, pp. 92-102, 2007.
[7] C. Clavier, B. Feix, G. Gagnerot, and M. Roussellet, "Passive and Active Combined Attacks on AES: Combining Fault Attacks and Side Channel Analysis." FDTC'10, IEEE CS, pp. 10-19, 2010.
[8] T. Roche, V. Lomn, and K. Khalfallah, "Combined Fault and Side-Channel Attack on Protected Implementations of AES," In Proceedings of Smart Card Research and Advanced Applications, LNCS 7079, pp. 65-83, 2011.
[9] A. Boscher, R. Naciri, and E. Prouff, "CRT-RSA Algorithm Protected Against Fault Attacks," WISTP'07, LNCS 4462, pp. 237-252, 2007.
[10] C. Couvreur and J. J. Quisquater, "Fast decipherment algorithm for RSA public-key cryptosystem," Electronics Letters vol. 18, pp. 905-907, 1982.
[11] S. M. Yen and M Joye, "Checking before output may not be enough against fault-based cryptanalysis," IEEE Trans. on Computers, vol. 49, pp. 967-970, 2000.
[12] M. Joye and S. M. Yen, "The Montgomery Powering Ladder," CHES'02, LNCS 2523, pp. 291-302, 2002.
[13] B. Chevallier-Mames, M. Ciet, and M. Joye, "Low-Cost Solutions for Preventing Simple Side-Channel Analysis: Side-Channel Atomicity," IEEE Trans. on Computers vol. 53, pp. 760-768, 2004.
[14] J. M. Schmidt, M. Tunstall, R. Avanzi, I. Kizhvatov, and D. Oswald, "Combined Implementation attack resistant exponentiation," LATIN- CRYPT'10, LNCS 6212, pp. 305-322, 2010.
[15] B. Feix and A. Venelli, "Defeating with Fault Injection a Combined Attack Resistant Exponentiation," COSADE'13, LNCS 7864, pp. 32-45, 2013.
[16] F. Amiel, B. Feix, M. Tunstall, C. Whelen, and W. Marnane, "Distinguishing Multiplications from Squaring Operations," SAC'08, LNCS 5381, pp. 346-360, 2009.

〈저자소개〉

김 형 동 (Hyung-Dong Kim) 학생회원
2012년 2월: 호서대학교 정보보호학과 졸업
2012년 3월 ~ 현재: 호서대학교 대학원 정보보호학과 석사 과정
〈관심분야〉 부채널 공격, 무선 네트워크 보안, 스마트폰 보안,

하 재 철 (Jae-Cheol Ha) 종신회원
1989년 2월: 경북대학교 전자공학과 졸업
1993년 2월: 경북대학교 전자공학과 석사
1998년 2월: 경북대학교 전자공학과 박사
1998년 3월~2007년 2월: 나사렛대학교 정보통신학과 부교수
2007년 3월~현재: 호서대학교 정보보호학과 교수
〈관심분야〉 정보보호, 네트워크 보안, 부채널 공격