情報保護學會論文誌
第20卷 第2號, 2010. 4

이중 멱승과 오류 확산 기법을 이용한 RSA-CRT에서의 물리적 공격 대응 방법*

길 광 은,† 오 두 환, 백 이 루, 하 재 철‡
호서대학교 정보보호학과

Countermeasure for Physical Attack in RSA-CRT using Double Exponentiation Algorithm and Fault Infective Method*

KwangEun Gil,† DooHwan Oh, YiRoo Baek, JaeCheol Ha‡
Dept. of Information Security, Hoseo University

요 약

중국인의 나머지 정리에 기반한 RSA-CRT 알고리즘은 오류 주입 공격에 취약하다는 점이 실험적으로 검증되었다. 본 논문에서는 RSA-CRT 알고리즘에 대한 현재까지의 오류 주입 공격 방어 대책을 분석하고 최근 제시된 Abid와 Wang이 제안한 대응 방법의 취약점을 분석한다. 이를 바탕으로 이중 멱승과 오류 확산 기법을 사용한 오류 주입 공격 대응책을 제시한다. 논문에서 제안한 방식은 오류 확산용 검증 정보를 이중 멱승 기법을 이용하여 효율적으로 계산하도록 하였으며 수동적 부채널 공격인 단순 전력 분석 공격과 (N-1) 공격에 강한 멱승 알고리즘을 개발하였다.

ABSTRACT

Many experimental results shows that RSA-CRT algorithm can be broken by fault analysis attacks. We analyzed the previous fault attacks and their countermeasures on RSA-CRT algorithm and found an weakness of the countermeasure proposed by Abid and Wang. Based on these analyses, we propose a new countermeasure which uses both double exponentiation and fault infective computation method. The proposed method efficiently computes a fault verification information using double exponentiation. And, it is designed to resist simple power analysis attack and (N-1) attack.

Keywords: RSA, Chinese Remainder Theorem, Fault Analysis Attack, Side Channel Attack, (N-1) Attack

I. 서 론

현재 RSA는 가장 널리 쓰이는 공개키 암호 시스템 중 하나이다[1]. 하지만 비밀키를 사용한 멱승(exponentiation) 연산은 스마트카드와 같이 연산 능력이나 메모리 자원이 제한된 임베디드 시스템에서 사용하기에 많은 부담을 주고 있다. 이러한 단점을 극복하고자 중국인의 나머지 정리(Chinese Remainder Theorem)를 이용한 RSA-CRT 멱승 기법이 널리 사용되고 있다. RSA-CRT는 일반 RSA보다 이론적으로 계산 속도가 약 4배 정도 빠르며 실제 구현 시에도 3배 이상 빠른 특성을 가지고 있기 때문에 계산량과 자원이 제한된 시스템에서 효율적으로 사용된다[2].

하지만 RSA-CRT 멱승 알고리즘은 오류 분석 공격(fault analysis attack) 혹은 오류 주입 공격(fault injection attack)이라 불리는 능동적인 물리 공격에 매우 취약한 것으로 밝혀졌다[3]. 오류 주입 공격은 1996년 Bellcore사에서 RSA 암호 시스

접수일(2009년 12월 17일), 게재확정일(2010년 2월 18일)
* 이 논문은 2009년도 호서대학교의 재원으로 학술연구비 지원을 받아 수행된 연구임. (2009-0183)
† 주저자, kke0805@nate.com
‡ 교신저자, jcha@hoseo.edu

템에 대한 공격 방법으로 처음 소개되었는데 공격자가 암호화 연산 중 의도적인 오류를 주입한 후 오류가 주입된 출력을 이용하여 비밀키를 찾아내는 공격 기법이다. 이와 같은 오류 공격을 RSA-CRT 알고리즘에 적용하면 단 한 번의 오류 주입만으로도 비밀키를 얻어낼 수 있다는 것이 발표되었다[4, 5]. 최근에는 이와 같은 오류 공격 기법이 다양화되어 하드웨어 칩의 특정 부분에 글리치(glitch)를 발생하거나 레이저 방사에 의해 오류를 주입하여 비밀키를 얻어내는 실험적 공격도 발표되고 있다[6, 7].

한편, 이러한 오류 주입 공격에 대응하기 위해 많은 대응책들이 발표되었는데 현재까지 나온 RSA-CRT에 대한 오류 공격 대응 알고리즘은 크게 오류 검사 방법과 오류 확산 방법으로 나눌 수 있다[8, 9]. 그러나 기존에 제시된 대응 방법들 중에는 아직 안전성이 완전히 검증되지 않았거나 차후에 등장한 발전된 공격 모델에 대해서는 위험 요소가 존재하는 경우도 있다. 또한, 최근에는 오류 공격뿐만 아니라 부채널 공격의 발전으로 인하여 전력 분석 공격과 같은 수동적 물리 공격에 대한 대응책도 병행해서 제안되고 있다[10].

본 논문에서는 RSA-CRT에 대한 기존 방어 대책 중 최근 Abid와 Wang이 제시한 대응 알고리즘[11]의 취약점을 분석한다. 이러한 분석을 바탕으로 오류 공격뿐만 아니라 지금까지 발표된 알려진 부채널 공격에 대응할 수 있는 새로운 RSA-CRT 알고리즘을 제안한다. 제안하는 알고리즘은 비밀키의 멱승 결과를 검증하기 위해 다른 멱승 과정을 추가한 이중 멱승 알고리즘을 사용하였으며 오류가 발생하면 결합 과정에서 오류가 확산되도록 하여 비밀키 추출이 불가능하도록 설계하였다. 또한, 멱승과정에서 atomic방법[12]을 적용하여 단순 전력 분석(simple power analysis) 공격과 (N-1) 공격[13]에도 대응할 수 있도록 하였다.

II. RSA-CRT 알고리즘과 오류주입 공격

RSA 공개키 암호 시스템을 구성하는 파라미터 생성 과정을 정리하면 다음과 같다.

① 큰 소수 p와 q를 선정하고 $N=p\cdot q$를 계산한다.

② $GCD(\phi(N),e)=1$을 만족하는 e를 선택하여 공개키로 한다. 여기서 ϕ는 오일러 totient 함수이다.

③ $e\cdot d\equiv 1 \bmod \phi(N)$이 되는 d를 계산하여 비밀키로 한다.

Input : p, q, d, p_I, q_I, N, m
Output : $S=m^d \bmod N$

1. $S_p=m^{d_p} \bmod p$, $S_q=m^{d_q} \bmod q$,
   where, $d_p=d \bmod (p-1)$, $d_q=d \bmod (q-1)$
2. $S=(S_p\cdot(q\cdot q_I))+(S_q\cdot(p\cdot p_I)) \bmod N$
3. Return S

[그림 1] Gauss 기법을 사용한 RSA-CRT

여기서 공개 정보는 N, e이며 비밀 정보는 p, q, d이다. 메시지 m에 대한 서명(혹은 복호)은 $S=m^d \bmod N$으로 계산하며 서명 검증(혹은 암호) 과정은 $S^e \bmod N$를 계산하여 m과 동일한지를 검사하는 과정으로 진행된다. [그림 1]은 RSA-CRT 알고리즘을 이용한 서명 $m^d \bmod N$의 계산 과정을 나타낸 것인데 여기서 p_I, q_I는 각각 $p_I=p^{-1} \bmod q$, $q_I=q^{-1} \bmod p$이다.

[그림 1]의 단계 2는 Gauss방식을 이용한 CRT 재결합(recombination) 방법인데 논문에서는 간단히 $S=CRT(S_p,S_q)$로 표기한다. CRT 기법에서는 기존의 RSA에서 사용하는 모듈러 N에 대한 멱승 대신 절반 크기인 모듈러 p와 q에 대한 멱승을 수행함으로써 기존의 RSA기법에 비해 약 4배 빠른 연산 효율성을 가질 수 있다.

그러나 Boneh 등은 RSA-CRT 서명 과정에서 S_p나 S_q의 연산 과정에서 어느 한 값에 오류가 주입되어 정확하지 않은 서명 S'을 구할 수 있을 경우 비밀키를 찾을 수 있다고 제안하였다[4]. 예를 들어 공격자가 [그림 1]에 S_p연산 중 어떠한 오류를 주입하여 S_p'로 계산되고 최종 오류 서명 S'를 얻었다고 가정하자. 이것은 $S=S' \bmod q$이고 $S\neq S' \bmod p$의 성질을 만족하게 되므로 정상 서명문 S와 오류 서명 S'을 이용하여 $q=GCD(S-S',N)$를 계산하면 쉽게 비밀 값 q를 얻을 수 있다. 또한 오류 서명 S'만 알고 있을 경우에는 공개 정보를 이용하여 $q=GCD(S'^e-m, N)$에 의해 소수 q를 구할 수 있다[5].

III. 오류주입 공격에 대한 기존 대응방법 분석

오류 주입 공격에 대응하는 방법은 크게 오류가 주입되었는지 여부를 검사하는 검사 방법과 오류가 주입되면 그 오류를 서명문에 확산시켜 공격자가 원하는 결과값을 얻을 수 없도록 하는 오류 확산 방법이 있다.

3.1 오류 검사 방법

오류 검사를 이용한 대표적인 대응책으로는 Shamir의 방법이 있는데 여기에서는 32비트 정도의 랜덤 수 r을 발생시킨 후 각각 소수 p나 q와 곱하여 확장된 가환 환(commutative ring)에서 모듈러 연산을 수행하였다[8]. 즉, 생성한 임의의 랜덤 수 r을 이용하여 각각 $S_p^* = m^d \bmod p \cdot r$, $S_q^* = m^d \bmod q \cdot r$으로 계산한다. 이후 오류가 주입되었는지 여부를 $S_p^* \equiv S_q^* \bmod r$과 같은 검사 연산을 통해 확인하는 방법이다. 이 후 Joye 등은 Shamir의 방법을 일반화하여 랜덤 수 r_1과 r_2를 생성한 후, 각각 S_p^*와 S_q^*연산 시 p나 q와 곱하여 확장된 두 개의 가환 환에서 모듈러 연산을 수행하는 방법을 제안하기도 하였다[14].

이 외에도 Giraud는 오류 검사 기법을 이용하는 방법으로 Montgomery Ladder 멱승 알고리즘을 이용하는 오류 공격 대응책을 제안하였다[15]. 이 방법에서는 멱승의 결과로 나온 $(S_p^*, S_p) = (m^{d_p}, m^{d_p+1})$와 $(S_q^*, S_q) = (m^{d_q}, m^{d_q+1})$쌍을 이용하여 두 종류의 출력 값$(S, S^*) = (CRT(S_p, S_q), CRT(S_p^*, S_q^*))$을 생성하고 $S = m \cdot S^* \bmod N$를 만족하는지 조사하여 오류 주입 여부를 검사하였다. 그러나 2007년 Kim과 Quisquater는 WISTP에서 발표한 논문[7]에서 비교 연산을 이용한 대응 방법을 사용하면 S_p나 S_q 연산 시 첫번째 오류를 넣고 비교 연산에서 두 번째 오류를 주입하여 이 과정을 건너뛰게 함으로써 2차 오류 주입 공격이 성공할 수 있음이 실험적으로 증명되었다.

3.2 오류 확산 방법

오류 주입 여부를 검사하는 방법 이외에도 오류가 주입될 경우 오류로 인한 랜덤한 값을 최종 서명값에 확산시켜 공격자에게 유용하지 않은 값을 출력시키는 기법이 있다. 오류 확산 기법은 처음 Yen 등의 논문[9]에서 제시되었으며 Blomer 등이 제안한 BOS 기법[16]이 대표적인 방법이라 할 수 있다. 즉, BOS의 대응 기법에서는 S_p나 S_q를 계산하는 단계에서 오류가 발생하면 오류 확산 값 c_1나 c_2값이 랜덤한 값이 되고 (정상적인 경우에는 모두 최종 서명 $S^{c_1 \cdot c_2} \bmod N$을 계산하도록 하여 오류가 서명에 확산되도록 하였다. 그러나 BOS 기법은 Wagner가 제안한 공격[17]에 취약함이 밝혀졌다. 이후 Kim과 Quisquater는 전력 공격에 대응할 수 있는 모듈러 멱승 알고리즘과 BOS 오류 주입공격 대응기법을 결합한 방법[18]을 제시한 바 있다. 그러나 Kim과 Quisquater 대응 기법에서 사용하는 멱승 알고리즘은 특정한 입력을 통한 전력 분석 공격인 (N-1) 공격[13]에 취약한 것으로 알려져 있다[19].

3.3 Abid-Wang 대응 방법의 취약성

3.3.1 Abid-Wang 대응 방법

2008년 Abid와 Wang은 RSA-CRT에 대한 오류 주입 공격을 방어하기 위해 오류 확산 방법을 이용한 대응책을 제안한 바 있다[11]. 제안한 방법을 요약하면 다음과 같다. 서명자는 비밀키 d보다 작은 t를 선택하고 새로운 키 쌍 $d_t = d + t$, $e_t = d_t^{-1} \bmod \phi(N)$, $d_s = d - t$를 사전 계산한다. 이 후 서명은 다음과 같이 진행한다.

① 먼저 $m_p = m \bmod p$, $m_q = m \bmod q$를 계산한다.

② $S_{pt} = m_p^{d_s \bmod (p-1)} \bmod p$,
$S_{qt} = m_q^{d_s \bmod (q-1)} \bmod q$. $X_p = m_p{}^t \bmod p$,
$X_q = m_q{}^t \bmod q$를 계산한다.

③ $S_p = S_{pt} X_p \bmod p$, $S_q = S_{qt} X_q \bmod q$,
$S = (CRT(S_p, S_q) + \tilde{m}) \bmod N$를 계산한다.

단, 여기서 $\hat{m} = (((S_p X_p)^{e_t} \bmod p - m_p) ++ ((S_q X_q)^{e_t} \bmod q - m_q))$이며 $\tilde{m} = \hat{m} \cdot (N / \min(p,q) + 1)$이다.

오류가 없을 경우에는 $\hat{m}$는 0이 되어 $\tilde{m}$도 0이 되므로 정상적인 서명이 된다.

3.3.2 취약성 분석

여기에서는 Abid-Wang이 제안한 대응 방법에서 특정 연산에 오류가 주입될 경우 비밀키를 찾을 수 있음을 보이고자 한다. 공격자는 단계 1에 있는 $m_p' = m \bmod p$의 계산 과정에 오류를 주입했다고 가정하자. 그러면 각 단계의 오류는 다음과 같이 확산될 것이다.

① $m_p' = m \bmod p$, $m_q = m \bmod q$를 계산한다.

② $S_{pt}' = m_p'{}^{d_s \bmod (p-1)} \bmod p$,
$S_{qt} = m_q^{d_s \bmod (q-1)} \bmod q$, $X_p' = m_p'{}^t \bmod p$,
$X_q = m_q{}^t \bmod q$를 계산한다.

③ $S_p' = S_{pt}' X_p' \bmod p$, $S_q = S_{qt} X_q \bmod q$
$S' = (CRT(S_p', S_q) + \tilde{m}') \bmod N$을 계산한다.

여기서 $\hat{m}' = (((S_p' X_p')^{e_t} \bmod p - m_p') + ((S_q X_q)^{e_t} \bmod q - m_q))$이며 $\tilde{m}' = \hat{m}'(N/\min(p,q)+1)$이다. 이와 같은 오류를 주입했을 경우 $\tilde{m}'$이 어떤 값을 가지는지 주목할 필요가 있다. 정상 서명인 경우에는 확인 수식 $\hat{m}$에서 $((S_q X_q)^{e_t} \bmod q - m_q)$은 0이 된다. 그런데 오류가 주입된 경우에도 $((S_p' X_p')^{e_t} \bmod p - m_p')$는 다음과 같이 0이 된다.

$$((S_p' X_p')^{e_t} \bmod p - m_p')$$
$$= (m_p'^{\,d}\ m_p'^{\,t})^{e_t} \bmod p - m_p'$$
$$= (m_p'^{\,ed_t}) - m_p' = 0$$

따라서 $\tilde{m}'$은 결국 0이 되고 잘못된 서명 S'에는 S_p'의 오류만 주입된다. 즉, $S' = CRT(S_p', S_q)$와 같이 오류가 발생한다. 따라서 $GCD(S-S', N)$ 혹은 $GCD(S'^{\,e} - m, N)$을 이용하여 비밀키 q를 찾을 수 있다. 이 공격은 $m_q' = m \bmod q$의 계산과정에서 오류를 주입해도 같은 원리로 비밀키 p를 찾을 수 있다.

위와 같은 오류 공격에 대한 간단한 대응 방법은 단계 3에서 단계 1에 계산해 두었던 m_p나 m_q를 그대로 사용하지 않고 메시지 m을 불러와 $m \bmod p$, $m \bmod q$를 다시 계산하여 사용하여야 한다. 이렇게 하면 1단계에서 오류를 주입하더라도 3단계에서 $((S_p' X_p')^{e_t} \bmod p - (m \bmod p))$가 0이 되지 않아 오류 주입 공격을 방어할 수 있다. 그러나 Abid-Wang 대응 방법은 이러한 취약점 개선을 한다고 하더라도 약 6번의 멱승을 수행해야 하므로 계산량 측면에서 상당히 비효율적인 대응 기법이다.

IV. 제안하는 오류 주입 공격 및 부채널 공격 대응 방법

본 논문에서는 상기한 분석을 바탕으로 안전하고 효율적인 RSA-CRT 기법을 제안하고자 한다. 제안하는 알고리즘은 다양한 오류 공격에 방어할 수 있고 전력 분석 공격이나 (N-1) 공격과 같은 다른 부채널 공격에 대해서도 안전하며 계산 효율성을 향상시켜 스마트카드와 같은 임베디드 시스템에서도 사용할 수 있도록 설계하였다.

4.1 오류 주입 공격 대응방법

오류 주입 공격에 대응할 수 있는 새로운 기법은 다음과 같다. 먼저, 서명자는 $\phi(N)$과 서로 소인 k비트 (약 16비트)의 e_t를 선택하고 $d_t = e_t^{-1} \bmod \phi(N)$를 만족하는 키 쌍 (e_t, d_t)를 계산한다. 이 경우 d_t는 d보다는 크고 $\phi(N)$보다는 작은 값이 되는 조건을 만족해야 한다. 이후 $d_t = d + t \bmod \phi(N)$을 만족하는 t를 구한다. 기존의 Abid와 Wang의 방법에서는 t를 먼저 선택하고 새로운 키 쌍, $d_t = d + t$, $e_t = d_t^{-1} \bmod \phi(N)$ 순서로 사전 계산했던 것과 달리 본 논문에서는 작은 e_t를 먼저 선택하고 최종적으로 t를 구할 수 있도록 하였다. 그 이유는 이후에 설명이 되겠지만 검증 계산의 효율성을 고려한 것이다. 즉, 오류 주입 여부를 판단하는 멱승을 지수 e_t로 하는 경우 e_t를 작게 하는 것이 최대한 유리하기 때문에 본 논문에서는 먼저 e_t를 결정하도록 설계하였다. 시스템 파라미터를 설정한 후 서명 과정은 [그림 2]와 같이 나타낼 수 있다.

여기서 계산 과정이 정상적으로 진행된다면 $V=0$, $c=1$이 되고 $S^* = CRT(S_p, S_q)$, $S = m^d \bmod N$이 되어야 한다. [그림 2]와 같이 단계 1에서 생성된 계산 값 S_p, S_q와 X_p, X_q를 이용하여 오류 확산 값 V를 계산한다. V값은 랜덤한 값으로 초기화되어 있으며, 오류 주입이 없는 정상적인 서명의 경우 V값은 다음과 같은 등식이 성립한다.

$$((S_p X_p)^{e_t} - m) \bmod p = ((m^{d_p} m^{t_p})^{e_t} - m) \bmod p$$
$$= ((m^{d_t})^{e_t} - m) \bmod p$$
$$= 0$$

같은 방법으로 $((S_q X_q)^{e_t} - m) \bmod q = 0$로 계산되며, 오류가 없을 경우 최종적으로 $V=0$을 만족하게 된다. 이 후 두 값을 XOR한 후 결합 과정을 거쳐 임시 서명 S^*를 얻을 수 있다. 그리고 CRT 결합 과정에서 생길 수 있는 오류를 고려하여 단계 4의 검증 과정을 거친 후 S^*에 오류 확산용 임시 값 c를 멱승하게 된다. 이 때 c와 S도 V와 마찬가지로 랜덤한 값으로 초기화되

Input : $p, q, d_p, d_q, t_p, t_q, p_I, q_I, N, m$
Output : $S = m^d \bmod N$

1. $S_p = m^{d_p} \bmod p$, $S_q = m^{d_q} \bmod q$
   $X_p = m^{t_p} \bmod p$, $X_q = m^{t_q} \bmod q$
   .where, $d_p = d \bmod (p-1)$, $d_q = d \bmod (q-1)$
   $t_p = t \bmod (p-1)$, $t_q = t \bmod (q-1)$
2. $V = (((S_p X_p)^{e_t} - m) \bmod p) \oplus (((S_q X_q)^{e_t} - m) \bmod q)$
3. $S^* = (S_p'(q \oplus V) q_I) + (S_q'(p \oplus V) p_I)) \bmod N$
4. $c = ((S^* - S_p) \bmod p \oplus (S^* - S_q) \bmod q) + 1$
5. $S = (S^*)^c$
6. Return S

[그림 2] 오류 공격에 대응하는 RSA-CRT 알고리즘

어 있다고 가정한다. 만약 오류가 없는 정상 서명인 경우, c는 1이 되며, $(S^*)^c$를 계산하여 서명 S를 출력하게 된다.

4.2 부채널 공격에 대응하는 이중 멱승 알고리즘

오류 주입 공격에 대응하는 [그림 2]의 알고리즘에서 S_p와 X_p는 같은 메시지 m에 대한 모듈러 p상의 멱승 연산이고 S_q와 X_q는 같은 메시지 m에 대한 모듈러 q에 대한 멱승 연산이다. 따라서 S_p와 X_p의 멱승 연산을 효율적으로 처리하기 위해 이중 멱승(double exponentiation) 방법을 제안하고자 한다.

한편, 오류 주입 공격 이외의 다른 물리적 공격으로는 전력 분석 공격이 있는데 여기에는 단순 전력 분석(simple power analysis) 공격과 차분 전력 분석(differential power analysis) 공격이 있다. 멱승 알고리즘이 단순 전력 분석 공격에 대응하기 위해서는 비밀키와 연산 파형과의 연관성을 배제하는 것이 중요하며 대응 방법으로 multiply-and-square always 방법이나 atomic 기법[12]이 사용될 수 있다. 단순 전력 분석 공격에 대응하기 위한 atomic 기법이란 멱승 연산시 곱셈과 제곱 연산을 구별할 수 없도록 제곱도 곱셈 모듈을 사용하도록 하여 비밀키 비트의 구별을 없애고자 한 기법을 말한다.

본 논문에서는 오류 주입 공격에 대응하기 위한 이중 멱승 알고리즘을 구현하면서 단순 전력 분석 공격과 (N-1) 공격도 동시에 방어하는 알고리즘을 제시하고자 한다. 단순 전력 분석 공격을 방어를 위해서는 이중 멱승에 대한 atomic 방법을 적용하며 (N-1) 공격을 방어하기 위해서는 (N-1)의 입력 효과를 없애기 위해 알고리즘 자체를 변형한다. 여기서 주의할 점은 RSA-CRT 알고리즘의 경우, 차분 전력 분석 공격에 필요한 연산체 p나 q를 공개하지 않으므로 차분 전력 분석 공격은 고려하지 않아도 된다는 것이다. [그림 2]의 단계 1에서 $S_p = m_p^{d_p} \bmod p$ 와 $X_p = m_p^{t_p} \bmod p$를 동시에 계산하는 이중 멱승 알고리즘을 나타낸 것이 [그림 3]이다.

제안하는 이중 멱승 알고리즘에서 초기 레지스터는 메시지에 대한 m_p^2과 1로 각각 초기화 한다. 이후 Right-to-Left 이진 멱승 방식으로 atomic방법을 적용하여 계산하되 d_p와 t_p의 최하위 비트에 대한 연산은 단계 4와 5에서 별도로 처리한다. 즉, 단계 2에서 시작하는 비트의 인덱스 i를 1로 두어 d_{p_1}과 t_{p_1}에 관한 비트 연산부터 처리하게 하였다. 비밀키 비트 d_{p_i}와 t_{p_i} 값에 상관없이 m_p에 대해 연속적인 제곱을 하는 부분을 레지스터 R_0에 저장하였다. 또한, d_{p_i}와 t_{p_i}의 비트 값이 동시에 1일 경우에는 해당 결과를 R_3에 저장하였다.

또한, d_{p_i}만 1인 경우에는 레지스터 R_1에, t_{p_i}만 1인 경우에는 R_2에 저장하도록 하였다. 따라서 최종적인 S_p를 구할 때는 단계 4에서와 같이 R_1과 R_3를 서로 곱하고 X_p를 구할 때는 단계 5에서와 같이 R_2와 R_3를 서로 곱하여 최종 결과를 출력하였다. 물론 최하위 비트에 따라서 단계 4와 5에서 m_p을 한번 더 곱해 주는지 여부를 결정하게 된다.

이와 같이 구성함으로써 단순 전력 분석 공격을 방어할 수 있으며 (N-1) 공격을 방어할 수 있다. 여기서 분석을 위해 공격자가 (N-1) 값을 [그림 2]의 RSA-CRT 연산의 입력으로 주입하였다고 가정하자. 그러면 [그림 3]에서는 입력 값이 $m_p = m \bmod p = (N-1) \bmod p = (p \cdot q - 1) \bmod p = p - 1$ 이 된다. 그러나 단계 1에서 m_p^2값이 1이 되므로 단계 3.2에서는 d_{p_i}와 t_{p_i}가 하나라도 1이면 매번 동일한 $R_k = R_k \cdot R_0 = 1 \cdot 1$ 연산만 수행하게 되고 k값이 0인 경우도 $R_0 = R_0 \cdot R_0 = 1 \cdot 1$이 수행되어 전력 파형 분석을 통해 d_{p_i}나 t_{p_i} 정보를 얻을 수 없게 된다. 즉, (N-1) 공격을 방어하기 위해 R_0 레지스터의 값을 (N-1)로 시작하는 것이 아니라 1로 시작함으로써 비밀 비트에 따른 연산이 차별화되지 않도록 설계하였다. 이러한 이중 멱승 방법은 (S_p, X_p)와 (S_q, X_q)쌍을

Input :
m_p, p, $d_p = (d_{p_{n-1}}, .., d_{p_0})_2$, $t_p = (t_{p_{n-1}}, .., t_{p_0})_2$
Output :
$S_p = R_1 = m_p^{d_p} \bmod p$, $X_p = R_2 = m_p^{t_p} \bmod p$

1. $R_0 = m_p^2$, $R_1 = R_2 = R_3 = 1$
2. $i = 1$, $k = 0$
3. while$(i \le n-1)$ do
   3.1 $k = (2t_{p_i} + d_{p_i}) \oplus k$
   3.2 $R_k = R_k \cdot R_0$
   3.3 $i = i + (\neg k)$
4. if$(d_{p_0} = 1)$ $R_1 = R_1 \cdot R_3 \cdot m_p$
   else $R_1 = R_1 \cdot R_3$
5. if$(t_{p_0} = 1)$ $R_2 = R_2 \cdot R_3 \cdot m_p$
   else $R_2 = R_2 \cdot R_3$
6. Return (R_1, R_2)

[그림 3] 단순 전력 분석 공격과 (N-1) 공격에 대응하는 이중 멱승 알고리즘

생성할 때 각각 적용할 수 있으며 두 개의 지수에 대한 멱승을 병렬적으로 처리하면서 공통적인 연산 부분을 한 번에 처리할 수 있도록 구현한 것이다.

V. 제안 기법 분석

5.1 안전성 분석

제안한 오류 공격 대응 알고리즘은 Abid-Wang이 제안한 오류 주입 대응 방식을 기반으로 오류가 발생하면 재결합에 사용되는 두 비밀키 p, q와 직접 XOR하여 오류를 확산시키는 것이 특징이다. 또한 재결합 과정에서 발생할 수 있는 다른 오류를 확인하기 위해 [그림 2]의 단계 4와 5의 과정을 두었다. 그 이유는 단계 4나 단계 5가 없을 경우에는 단계 3에서의 오류 주입만으로 비밀키를 추출할 수 있기 때문이다. 즉, 단계 3에서 S_p나 S_q를 곱하는 연산에서 오류 값 S_p' 혹은 S_q'으로 CRT 재결합이 이루어지면 2장에서 설명한 공격이 그대로 적용된다. 따라서 이러한 오류 확산 방법은 비교 연산을 건너뛰는 2차 오류 주입 공격[7]에 대해서도 안전하다고 할 수 있다.

본 논문에서 제안한 [그림 2]의 오류 공격 대응 알고리즘의 안전성을 분석하기 위해서 각 파라미터별로 오류가 주입된 경우를 단계별로 분석하였다. 여기서 적용되는 오류 공격 모델은 특정한 시점에 일시적인 오류를 주입하며 공격자는 오류가 주입된 값을 알지는 못한다고 가정한 것이다.

- 분석 1) 단계 1의 S_p 또는 S_q연산 과정 또는 파라미터에 오류가 주입된 경우 :

S_p에 오류가 주입되었다고 가정하면 이 오류는 $(((S_p{}' X_p)^{e_t} - m) \bmod p) \neq 0$과 같이 되어 랜덤한 값으로 오류가 확산되어 V가 랜덤한 값이 된다. 따라서 CRT 결합과정에 비밀 값 p와 q에 랜덤한 값이 XOR되어 확산되므로 공격자에게 유용하지 않은 오류 서명이 출력된다.

- 분석 2) 단계 1의 X_p또는 X_q연산 과정 또는 파라미터에 오류가 주입된 경우 :

이 경우도 위의 S_p나 S_q에 오류가 주입된 경우와 마찬가지로 V값이 랜덤화 된다. 따라서 공격자에게 의미없는 오류 서명 값이 출력된다.

- 분석 3) 단계 2의 V의 연산 과정 또는 파라미터에 오류가 주입된 경우 :

V를 생성하는 단계에 사용하는 어느 파라미터에서든지 오류가 발생할 경우 랜덤한 서명 값으로 출력되며, 만약 V를 계산하는 부분만 건너뛰는 오류를 주입하게 된다 하더라도 초기에 랜덤한 값으로 설정되어 있는 V값으로 인하여 공격자가 원하는 값을 출력할 수 없게 된다.

- 분석 4) 단계 3의 CRT 재결합 과정에 오류가 주입된 경우 :

CRT 재결합 과정에서 사용하는 S_p나 S_q에 오류가 주입될 경우는 S^*값에 오류가 확산되어 단계 4에서 오류 확산 값 c가 랜덤한 값으로 계산된다. 또한 단계 4를 건너뛰는 오류를 주입하더라도 초기에 c가 랜덤한 값으로 설정되기 때문에 공격자가 원하는 오류 서명 값을 출력할 수 없다.

- 분석 5) 2차 오류가 주입된 경우 :

단계 1의 멱승 과정이나 단계 3의 결합과정에서 첫 번째 오류가 주입되고 단계 2의 V값 계산 또는 단계 4의 c값 계산 그리고 단계 5의 최종 서명 계산 과정에서 두 번째 오류로 연산을 건너뛴다 하더라도 사용되는 파라미터는 초기 값이 모두 랜덤 값으로 설정되어 있기 때문에 공격자가 원하는 오류 서명 값을 얻을 수 없다.

오류 공격 이외에도 단순 전력 분석 공격과 (N-1) 공격에 대응하기 위해 이중 멱승 알고리즘을 개발하였다. 제안한 멱승 알고리즘은 [그림 3]에서 나타나듯이 atomic방법을 사용하여 비밀키 비트에 상관없이 항상 곱셈을 하는 구조이므로 단순 전력 분석공격에 대응할 수 있다. 또한 (N-1) 공격에 대해서는 R_0에 입력 값 $p-1$ 값이 들어간다 하더라도 비밀키에 따른 모든 곱셈 연산이 동일하므로 비밀 비트에 따른 전력 파형을 구분할 수 없어 공격자는 비밀키를 찾을 수 없다.

5.2 계산 효율성 분석

[그림 2]의 제안 알고리즘의 가장 큰 특징 중 하나는 k비트 정도의 작은 e_t를 먼저 선택한 후 $d_t = e_t^{-1} \bmod \phi(N)$를 구하고 $d_t = d + t \bmod \phi(N)$가 되는 t를 사전에 구한다는 점이다. 이렇게 함으로써 단계 1의 계산량은 이중 멱승 알고리즘을 이용하여 감소시키며 단계 2의 계산은 작은 크기의 e_t를 사용함으로써 계산량을 줄일 수 있도록 설계하였다. 따라서 오류 공격 대응 알고리즘의 단계 2에서의 멱승 계산이 두 배로 증가하는 것처럼 보이지만 S_p와 X_p를 계산할 때 동일한 메시지 m_p를 사용하므로 멱승 연산에 항상 공통

으로 계산되는 제곱 연산을 한번으로 처리하도록 개발하였다. 이러한 연산 기법은 두 멱승을 병렬 처리하는 효과를 가짐으로써 계산 효율을 높일 수 있다. 여기서 주의할 점은 e_t나 d_t, t 값들은 외부로 노출되는 값이 아니고 서명자 자신의 시스템 내부에서만 사용되는 파라미터이고 자체 오류 검증용으로만 사용되는 값이므로 e_t값은 작은 크기의 수라도 비밀키 d를 유지하는 안전성에 전혀 영향을 받지 않는다.

다음 [표 1]은 오류 주입 대응책으로 제시된 각 대응 방식의 안전성과 계산 효율성을 비교한 것이다. 계산량 비교를 위해서는 사용되는 파라미터의 비트 길이가 중요한데 여기서 l은 모듈러 p 또는 q와 같은 소수의 길이를 나타내며, n은 l비트에서 $(l+n)$비트로 가환 환을 크게 하는 확장 파라미터의 길이를 나타낸다. [표 1]에서 사용된 표기 중 a^b는 a비트 크기 정수에 b비트의 지수(exponent)로 모듈러 멱승 연산을 한다는 의미이다. 예를 들어 512비트의 p와 q를 사용하는 서명 시스템이라면 RSA-CRT 기법의 경우 512비트의 모듈러 길이 l과 비밀 지수 값 길이 l의 멱승 연산을 2번 하게 되므로 $2(l)^l$로 나타낸 것이다. 단, 여기서 정수의 길이 a가 2배 늘어나면 멱승 전체 계산량은 4배가 늘어나고 지수 길이 b가 2배 늘어나면 멱승 전체 계산량은 비례하여 2배 늘어나게 된다.

[표 1]에서 보면 Giraud기법이나 Kim-Quisquater기법의 경우에는 오류 공격에는 안전한 방법으로 알려져 있지만 일반적인 RSA-CRT기법에 비해 연산량이 1.33배 혹은 1.55배까지 증가하는 것을 볼 수 있다. Abid-Wang의 대응 방법은 안전성면에서도 취약할 뿐 아니라 계산량 측면에서도 RSA-CRT 방법에 비해 약 3배 정도 증가하게 된다.

제안한 방법은 위에서 분석한 바와 같이 현재까지 알려진 부채널 공격에 대해 안전하며, 이중 멱승의 사용함으로써 한 번의 멱승보다 약 1.16배의 곱셈의 수가 증가하게 된다. 즉, 일반 RSA-CRT는 l비트의 멱승은 평균 $1.5l$번의 모듈라 곱셈(평균 l번의 제곱+$0.5l$번의 곱셈)이 필요한데 제안 방식은 $1.75l$번(평균 l번의 제곱+$0.75l$번의 곱셈)의 모듈라 곱셈이 필요하다. 따라서 약 $1.75/1.5=1.16$배의 모듈라 곱셈 수 증가가 예상된다. 또한 [그림 2]의 단계 2에서 지수 e_t값에 대한 멱승이 필요하므로 l^k길이의 멱승 연산이 필요하다. 따라서 기존 RSA-CRT 보다 약 1.2배의 연산량 증가가 필요하지만 타 방식에 비해 고속으로 안전한 RSA 서명 시스템을 구현할 수 있다.

[표 1] RSA-CRT알고리즘의 안전성 및 연산량 비교 ($l=512$, $n=80$, $k=16$일 때)

구 분	안전성	멱승 연산 길이	연산량 비율(%)
RSA[1]	-	$(2l)^{2l}$	400.00
RSA-CRT[4, 5]	X	$2(l^l)$	100.00
Giraud[15]	O	$2(l+n)^l$	133.69
Kim-Quisquater [18]	O	$2((l+n)^l+2n^n)$	155.34
Abid-Wang[11]	X	$6(l^l)$	300.00
Proposed	O	$2((1.16(l)^l)+l^l)$	119.79

VI. 결 론

본 논문에서는 RSA-CRT 기법에 대한 다양한 오류 주입 공격에 대한 대응 방법을 살펴보고, 최근 Abid-Wang이 제안한 오류 공격 대응 알고리즘의 취약점을 분석하였다. 분석한 내용을 바탕으로 오류 주입 공격에 대응할 수 있는 새로운 기법을 제안하였다. 제안 기법은 이중 멱승 기법과 짧은 길이의 연산 검증 파라미터를 활용하여 서명 계산 과정의 계산량을 줄이도록 하였다. 또한 오류 확산 개념을 적용하여 2차 오류 주입 공격에도 강인한 알고리즘으로 설계하였다. 이와 더불어 단순 전력 분석 공격이나 (N-1) 공격에 효과적으로 대응할 수 있도록 이중 멱승 알고리즘을 개발하였다. 이 대응 기법은 연산 능력이 제한적이고 물리적 보안성이 취약한 임베디드 시스템에 RSA-CRT 서명이나 복호 시스템을 구현하는데 효과적으로 사용할 수 있다.

참 고 문 헌

[1] R. Rivest, A. Shamir, and L. Adelman, "A method for obtaining digital signature and public key cryptosystems," Comm. of ACM, vol. 21, no. 2, pp. 120-126, Feb. 1978.

[2] C. Couvreur and J.J. Quisquater, "Fast decipherment algorithm for RSA public-key cryptosystem," Electronics Letters, vol. 18, no. 21, pp. 905-907, Oct. 1982.

[3] J.S. Coron, "Resistance Against Differ-

ential Power Analysis for Elliptic Curve Cryptosystems," CHES'99, LNCS 1717, pp. 292-302, 1999.

[4] D. Boneh, R.A. DeMillo, and R.J. Lipton, "On the importance of checking cryptographic protocols for faults," EUROCRYPT'97, LNCS 1233, pp. 37-51, 1997.

[5] M. Joye, A.K. Lenstra, and J.J. Quisquater, "Chinese remaindering based cryptosystems in the presence of faults," Journal of Cryptology, vol. 12, no. 4, pp. 241-245, Dec. 1999.

[6] C. Aumuller, P. Bier, W. Fischer, P. Hofreiter, and J.P. Seifert, "Fault attack on RSA with CRT: Concrete results and practical countermeasures," CHES'02, LNCS 2553, pp. 260-275, 2002.

[7] C. Kim and J.J. Quisquater, "Fault Attacks for CRT Based RSA: New Attacks, New Results, and New Countermeasures," WISTP'07, LNCS 4462, pp. 215-228, 2007.

[8] A. Shamir, "Mehtod and apparatus for protecting public key schemes from timing and fault attacks," United States Patent p-5991415, Nov. 1999.

[9] S. Yen, S. Kim, S. Lim, and S. Moon, "RSA speedup with residue number system immune against hardware fault cryptanalysis," ICISC'01, LNCS 2288, pp. 397-413, 2001.

[10] F. Funaroli and D. Vigilant, "Blinded fault resistant exponentiation," FDTC '06, LNCS 4236, pp. 62-70, 2006.

[11] Z. Abid and W. Wang, "Countermeasures for Hardware Fault Attack in Multi-Prime RSA Cryptosystems," International Journal of Network Security, vol. 6, no. 2, pp. 190-200, Mar. 2008.

[12] B. Chevallier-Mames, M. Ciet, and M. Joye, "Low-cost solutions for preventing simple side-channel analysis: side-channel atomicity," IEEE Transactions on Computers, vol. 53, no. 6, pp. 760-768, June 2004.

[13] S. Yen, W. Lien, S. Moon, and J. Ha, "Power Analysis by Exploiting Chosen Message and Internal Collisions-Vulnerability of Checking Mechanism for RSA Decryption," Mycrypt'05, LNCS 3715, pp. 183-195, 2005.

[14] M. Joye, P. Pailler, and S.M. Yen, "Secure evaluation of modular functions," International Workshop on Cryptology and Network Security-2001, pp. 227-229, Sep. 2001.

[15] C. Giraud, "An RSA Implementation Resistant to Fault Attacks and Simple Power Analysis," IEEE Trans on Computers, vol. 55, no. 9, pp. 1116-1120, Sep. 2006.

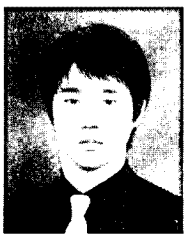
[16] J. Blomer, M. Otto, and J.P. Seifert, "A new CRT-RSA algorithm secure against Bellcore attacks," 10th ACM Conference on Computer and Communications Security, pp. 311-320, Oct. 2003.

[17] D. Wagner, "Cryptanalysis of a provably secure CRT-RSA algorithm," 11th ACM Conference on Computers and Communications Security, pp. 92-97, Oct. 2004.

[18] C. Kim and J.J. Quisquater, "How can we overcome both side channel analysis and fault attacks on RSA-CRT?," FDTC'07, pp. 21-29, Aug. 2007.

[19] J. Ha, C. Jun, J. Park, and S. Moon, "A New CRT-RSA Scheme Resistant to Power Analysis and Fault Attacks," International Conference on Convergence and Hybrid Information Technology - ICCIT'08, pp. 351-356, Nov. 2008.

〈著者紹介〉



길 광 은 (Kwang Eun Gil) 학생회원
2008년 2월: 호서대학교 정보보호학과 학사
2010년 2월: 호서대학교 정보보호학과 석사
2010년 2월~현재: (주)제너시스템즈 연구원
〈관심분야〉 네트워크 보안, 인증 및 평가, 암호 알고리즘

오 두 환 (Doo Hwan Oh) 학생회원
2010년 2월: 호서대학교 정보보호학과 학사
2010년 3월~현재: 호서대학교 정보보호학과 석사과정
〈관심분야〉 암호 알고리즘, 하드웨어 보안

백 이 루 (Yi Roo Baek) 학생회원
2008년 8월: 호서대학교 정보보호학과 학사
2008년 9월~현재: 호서대학교 정보보호학과 석사과정
〈관심분야〉 네트워크 보안, 프로토콜, 스마트 카드 보안

하 재 철 (Jae Cheol Ha) 종신회원
1989년 2월: 경북대학교 전자공학과 학사
1993년 8월: 경북대학교 전자공학과 석사
1998년 2월: 경북대학교 전자공학과 박사
1998년 3월~2006년 1월: 나사렛대학교 전자계산소장, 학술정보관장, 입시학생처장
1998년 3월~2007년 2월: 나사렛대학교 정보통신학과 부교수
2006년 7월~2006년 12월: QUT in Australia 연구 교수
2007년 3월~현재: 호서대학교 정보보호학과 부교수
2002년 3월~현재: 한국정보보호학회 이사
2009년 1월~현재: 한국산학기술학회 이사
〈관심분야〉 정보보호, 네트워크 보안, 스마트카드 보안