RSA-CRT에서의 오류주입 공격 대응책 비교 분석

백이루*, 길광은*, 김환구*, 하재철*†
*호서대학교 정보보호학과
e-mail:blr83@nate.com, kke0805@nate.com, hkkim@hoseo.edu, jcha@hoseo.edu

Analysis and Comparison of Countermeasures for Fault Induce Attack on RSA-CRT

YiRoo Baek*, KwangEun Gil*, HwanKoo Kim*, JaeCheol Ha*
*Dept of Information Security, Hoseo University

요 약

최근 오류주입 공격 기술이 발달함으로써 RSA-CRT 암호 알고리듬을 수행하는 동안 비밀 키를 찾아내는 것이 가능해졌다. RSA-CRT에서는 단 한 번의 오류주입을 통해 비밀 키 전체를 찾아낼 수 있어 공격에 매우 취약한 특성을 보인다. 이에 대한 대응책이 여러 가지 발표되었지만 일부는 다른 물리적 공격 취약점이 발견되기도 하였고, 구현의 효율성을 저하시키는 요인이 되기도 하였다. 본 논문에서는 최근까지 제시된 RSA-CRT 오류주입 공격 대응책을 물리적 공격에 대한 안전성과 효율성면에서 비교 분석하고 효율적인 대응책 개발을 위한 고려사항들을 살펴본다.

1. 서론

소인수 분해 문제를 기반으로 하는 RSA 암호 알고리듬은 현재 보안과 관련된 많은 분야에서 널리 사용되고 있는 공개키 암호 알고리듬이다[1]. 그러나 이러한 RSA 알고리듬은 멱승(exponentiation) 연산으로 인해 대칭키 암호 알고리듬에 비해서 연산 시간이 오래 걸리는 단점이 있다. 이러한 단점을 극복하기 위해 중국인의 나머지 정리(Chinese Remainder Theorem)를 이용한 계산법을 사용하는 RSA-CRT 알고리듬이 제안되었다[2]. RSA-CRT는 이론적으로 일반 RSA보다 계산속도가 약 4배정도 빠르기 때문에 스마트카드와 같은 임베디드 시스템뿐만 아니라 일반 시스템에서도 많이 사용된다.

최근 부채널 공격(side-channel attack)과 오류주입 공격(fault insertion attack)과 같은 물리적 공격들은 시스템에 큰 위협이 되고 있으며, 특히 스마트카드와 같은 임베디드 시스템들이 주요 공격 대상이 되고 있다. 이러한 공격들 중 오류주입 공격은 하드웨어의 결함 또는 소프트웨어의 버그 등을 이용하거나 전압 글리치(glitch) 또는 전자파 방사 등과 같은 방법을 통해 오류를 주입하고, 이를 통해 얻은 데이터를 이용하여 비밀 정보를 추출하는 공격이다[3]. 이러한 오류주입 공격은 1996년 Bellcore사에서 RSA 암호시스템에 대한 공격 방법으로 처음 소개되었다[4].

RSA-CRT는 단 한 번의 오류주입만으로도 비밀키를 추출할 수가 있기 때문에 오류주입 공격에 특히 취약하다[5]. 따라서 이에 대한 많은 대응 방안들이 연구되었고, 많은 대응책들이 제시되었다[6-11].

본 논문에서는 최근까지 제안된 RSA-CRT 오류주입 공격 대응 방안들 중에서 대표적인 몇 가지 알고리듬들을 소개하고, 이 알고리듬들을 안전성과 효율성면에서 비교 분석하였다. 또한 효율적인 대응책 개발을 위한 고려사항들에 대해서도 논의한다.

2. RSA-CRT에 대한 오류주입 공격

RSA-CRT에서 서명 $S \equiv m^d \bmod N$은 다음과 같이 계산된다.

먼저 두 개의 큰 소수 p와 q를 선택하여 $N = p \cdot q$를 구하고, $\gcd(\phi(N), e) = 1$이 되는 공개키 e를 선택한다. 그 다음 $e \cdot d \equiv 1 \bmod \phi(N)$을 만족하는 비밀키 d를 구하고, d를 이용하여 $d_p = d \bmod (p-1)$과 $d_q = d \bmod (q-1)$를 계산한다. 서명의 생성은 다음과 같다.

† 교신저자 (jcha@hoseo.edu)

$$S_p = m^{d_p} \bmod p$$
$$S_q = m^{d_q} \bmod q$$
$$S = CRT(S_p, S_q)$$

여기서 결합과정인 $CRT(S_p, S_q)$를 계산하기 위한 방법으로 Gauss 방법과 Garner 방법이 많이 사용되는데, Garner 방법이 Gauss 방법보다 좀 더 효율적이다. 여기서 Garner 방법은 다음과 같다.

$$S = CRT(S_p, S_q) = S_q + q \cdot ((S_p - S_q) \cdot I_q \bmod p)$$
$$(I_q = q^{-1} \bmod p)$$

RSA-CRT에서 오류주입 공격은 1997년 Boneh 등이 처음 제안하였다[3]. 이 공격은 RSA-CRT 서명 생성과정에서 S_p나 S_q 둘 중에 어느 하나의 값에 오류가 주입되어 오류가 주입된 서명 S'을 구할 수 있을 경우, 동일한 하나의 메시지에 대해 정상 서명 S와 오류 서명 S'을 이용하여 N을 소인수 분해하는 공격이다. 다시 말하면 정상 서명 값이 S이고, S_p를 연산할 때 오류가 주입되어 생성된 값 S_p'로 인해 생성된 오류 서명 S'을 이용하여 $GCD(S - S', N)$을 계산하여 비밀 소수 q를 구할 수 있다.

3. RSA-CRT에서의 오류주입 공격에 대한 대응 방안들

이 장에서는 지금까지 알려진 RSA-CRT에서의 오류주입 공격에 대한 대응 방안들 가운데 대표적인 몇 가지 알고리듬을 알아본다.

3.1 BOS 기법[6]

BOS 기법은 Shamir의 대응책[7]을 확장한 대응책으로 오류가 주입되었는지 확인하는 단계를 제거하고 오류전파의 성질을 이용한다.

BOS 기법에서는 랜덤수 t_1과 t_2를 선택하고 $d_p \equiv d \bmod \phi(p \cdot t_1)$, $d_q \equiv d \bmod \phi(q \cdot t_2)$, $e_{t_1} \equiv d^{-1} \bmod t_1$, $e_{t_2} \equiv d^{-1} \bmod t_2$를 사전에 계산하여 다음의 단계들을 수행함으로써 서명을 계산한다.

(1) $S_p = m^{d_p} \bmod (p \cdot t_1)$
(2) $S_q = m^{d_q} \bmod (q \cdot t_2)$
(3) $S = CRT(S_p, S_q) \bmod (N \cdot t_1 \cdot t_2)$
(4) $c_1 = (m - S^{e_{t_1}} + 1) \bmod t_1$
(5) $c_2 = (m - S^{e_{t_2}} + 1) \bmod t_2$
(6) $Sig = S^{c_1 c_2} \bmod N$

위와 같이 각 단계들 중에서 오류가 발생하면 그 오류가 서명에 확산되도록 구성되었다.

3.2 Giraud 기법[8]

Giraud는 Montgomery Ladder 멱승 알고리듬을 이용하여 멱승 연산을 수행하고, 그 결과 값들을 이용하여 오류의 주입 여부를 확인하는 대응 기법을 제시하였다.

Giraud의 대응 기법은 m^{d_p}와 m^{d_q}를 계산하는 것을 Montgomery Ladder 멱승 알고리듬을 이용하여 계산한다. 따라서 그 결과 값은 (m^{d_p}, m^{d_p+1})과 (m^{d_q}, m^{d_q+1})가 나오게 되는데, 일반적으로 m^{d_p}와 m^{d_q} 값만을 사용하지만 Giraud는 오류주입을 확인하기 위해 두 값을 모두 사용하여 m^{d_p}와 m^{d_q}를 결합한 S와 m^{d_p+1}와 m^{d_q+1}을 결합한 S'을 통해 S'과 $m \cdot S \bmod N$이 같은지 비교하여 오류주입 여부를 판단한다.

3.3 BNP 기법[9]

2007년 Boscher 등이 제안한 기법으로 Right-to-Left 방식의 멱승 알고리듬과 오류주입을 확인하는 단계를 통해 안전한 멱승 연산을 하고, 이를 RSA-CRT에 적용하여 오류주입 공격에 안전한 RSA-CRT를 수행하는 방법을 제시하였다.

BNP 알고리듬은 Right-to-Left 멱승 알고리듬을 이용하여 d가 n비트일 때 $(m^d, m^{\bar{d}}, m^{2^n})$을 구하고, 아래의 식을 통해 오류주입 여부를 판단함으로써 오류주입 공격에 안전한 멱승 알고리듬을 제안하였다.

$$m \cdot m^d \cdot m^{\bar{d}} = ? m^{2^n} \quad (\bar{d} = 2^n - d - 1)$$

RSA-CRT에서는 아래와 같이 p와 q로 나누어 멱승을 수행하고, 세 번의 결합과정을 거쳐 생성된 값들로 서명을 생성하고 오류를 탐지한다.

(1) $(S_p, S_p', T_p) \leftarrow (m^{d_p} \bmod p, m^{\bar{d_p}} \bmod p, m^{2^l} \bmod p)$
(2) $(S_q, S_q', T_q) \leftarrow (m^{d_q} \bmod q, m^{\bar{d_q}} \bmod q, m^{2^l} \bmod q)$
(3) $S \leftarrow ((S_q - S_p) \cdot A \bmod q) \cdot p + S_p$

(4) $S' \leftarrow ((S_q' - S_p') \cdot A \bmod q) \cdot p + S_p'$

(5) $T \leftarrow ((T_q - T_p) \cdot A \bmod q) \cdot p + T_p$

(6) $m \cdot S \cdot S' = ? \; T \bmod N$

3.4 Boscher 등의 기법[10]

2009년 Boscher 등은 Fumaroli와 Vigilant가 제안했던 대응책이[11] 오류주입 공격에 취약함을 지적하고, 이전에 제안했던 BNP 알고리듬을 기반으로 하여 전력분석 공격과 오류주입 공격에 안전한 새로운 멱승 알고리듬과 이를 RSA-CRT에 적용한 대응책을 제안하였다. 제안한 기법은 BNP 알고리듬과 거의 유사하고, 차분전력분석(differential power analysis)[12] 공격을 방어하기 위해 데이터를 블라인딩(blinding) 하는 과정이 추가되었다.

4. 대응 방안들의 안전성 및 효율성 분석

이 장에서는 3장에서 소개된 대응 방안들의 안전성과 효율성을 분석해본다.

4.1 안전성 분석

4.1.1 BOS 기법

BOS 기법은 Wagner에 의해 안전하지 않음이 밝혀졌다[13]. Wagner는 BOS 기법이 RSA-CRT 연산을 할 때 메시지 m이 로드되는 시점에서 일시적인 오류를 주입하는 오류주입 공격에 취약하다고 지적하였다. 나중에 저자들이 개선된 알고리듬을 제안하였으나 안전성에 대하여 논란이 되고 있다.

4.1.2 Giraud 기법

Giraud는 Montgomery Ladder 멱승 알고리듬을 이용하는 기법을 제안하였는데, Montgomery Ladder 멱승 알고리듬이 Relative 단순전력분석(simple power analysis)[14] 공격에 취약하다고 알려져 이를 개선한 알고리듬을 발표하였다.

개선된 알고리듬은 단순전력분석 공격과 오류주입 공격에 안전하다.

4.1.3 BNP 기법

BNP 기법은 RSA-CRT에서 멱승 연산을 하기 전에 비밀키 값인 d_p에 오류를 주입하게 되면 오류탐지 과정을 통과하게 되어 오류 서명을 출력하게 되는 취약점이 존재한다.

4.1.4 Boscher 기법

Boscher 기법은 멱승 알고리듬에서 $N-1$공격을 통해 단순전력분석 공격이 가능하다는 취약점이 있고, 멱승 연산을 수행하기 전, 메시지 M을 로드할 때에 오류를 주입하면 오류탐지 과정을 통과하게 되는 취약점이 존재한다.

4.2 효율성 분석

표 1은 본 논문에서 소개한 대응 방안들의 계산량을 비교한 것이다. 여기서 l은 비밀 소수 p와 q의 길이를 나타내고, n은 모듈러 연산체 확장을 위한 랜덤수의 길이를 나타낸다.

표 1은 RSA-CRT 연산을 100%로 두고 각각의 알고리듬들의 계산량을 이론적으로 비교한 것이다.

[표 1] 각 대응 방안들의 계산량 비교($l=512, n=80$일 때)

구분	멱승 연산 길이	연산량 비율(%)
RSA[1]	$(2l)^{2l}$	400.00
RSA-CRT[2]	$2(l^l)$	100.00
BOS[6]	$2((l+n)^{(l+n)}+n^n)$	154.96
Giraud[8]	$2(l+n)^l$	133.69
BNP[9]	$2(l^l)$	100.00
Boscher et al.[10]	$2(l^l)$	100.00

표 1의 연산량을 산출하는 예를 들어보면 $(l+n)^{(l+n)}$의 연산량은 l^l의 연산량에 비해 $((l+n)/l)^3$의 연산량을 가진다. 따라서 $l=512$이고, $n=80$일 경우 약 1.5458배의 연산량을 가지게 된다.

표 1을 기반으로 하여 효율성을 분석해보면 BOS 기법은 오류를 탐지하는 단계가 없는 대신 오류 전파 기법을 사용하고 있는데, 연산체와 지수를 확장하여 n비트 모듈러스에서 멱승을 두 번 수행하므로 연산량이 많이 증가하여 다른 대응 방안들에 비해 비효율적임을 알 수 있고, Giraud 기법은 전력분석 공격 방지를 위한 연산체 확장으로 기존 RSA-CRT보다 연산량이 약간 증가하였다. BNP 기법과 Boscher 등의 기법은 연산체나 지수의 확장 없이 오류탐지 단계를 사용하므로 효율적이라 할 수 있다.

5. 효율적인 대응책 개발을 위한 고려사항

이 장에서는 효율적인 대응책 개발을 위하여 어떤 사항들을 고려해야 하는지에 대해서 논의해보도록

한다.

효율적인 대응책 개발을 위해서는 많은 사항들이 고려되어야 한다. 여러 가지 공격들에 대해서 안전해야 하며, 아무리 안전하더라도 효율성이 고려되지 않으면 좋은 알고리듬이라 할 수 없으므로 알고리듬을 효율적으로 수행하기 위한 방법들이 고려되어야 한다. 또한 오류주입 공격뿐만 아니라 다른 부채널 공격에 대해서도 대응할 수 있도록 고려되어야 한다. 따라서 이와 같은 점들을 고려했을 때, 효율적인 대응책 개발을 위한 고려사항을 아래와 같이 나타낼 수 있다.

① 안전성 : 현재까지 알려져 있는 영구적 오류나 일시적 오류주입 공격들에 대하여 안전해야 한다.

② 효율성 : 가능한 적은 계산량으로 서명을 생성할 수 있어야 한다.

③ 구현의 용이성 : 레지스터나 메모리의 사용을 가능한 줄여 스마트카드와 같은 제한된 자원을 가진 시스템에서도 구현이 용이하도록 설계되어야 한다.

④ 확장성 : 오류주입 공격뿐만 아니라 전력분석 공격과 같은 다른 부채널 공격에도 안전해야 한다.

6. 결론

본 논문에서는 최근까지 RSA-CRT에서 오류주입 공격에 대한 대응 방안들을 소개하고, 그들에 대한 안전성 및 효율성 분석을 해보았다. 또한 효율적인 대응책 개발을 위한 고려사항들에 대해서도 논의하였다.

현재도 오류주입 공격과 그에 대한 대응책들이 많이 연구되고 있지만 그에 대한 안전성과 효율성에 대한 취약점들이 나타나고 있다. 따라서 본 논문에서 논의한 효율적인 대응책을 위한 고려사항들을 충분히 고려하여 안전하고 효율적인 대응 방안을 설계하도록 해야 할 것이다.

참고문헌

[1] R. Rivest, A. Shamir, L. Adleman, "A Method for Obtaining Digital Signatures and Public-key Cryptosystems," *ACM*, Vol. 21, pp. 120-126. 1978.

[2] C. Couvreur, J. Quisquater, "Fast Decipherment Algorithm for RSA Public-Key Cryptosystem," *Electronics Letters*, Vol. 18, pp. 905-907, 1982.

[3] C. AumÄuller, P. Bier, W. Fischer, P. Hofreiter, and J. Seifert, "Fault Attacks on RSA with CRT: Concrete Results and Practical Countermeasures," *CHES'02*, Vol. 2523, *LNCS*, pp. 260 - 275. 2002.

[4] D. Boneh, R. DeMillo, R. Lipton, "On the Importance of Checking Cryptographic Protocols for Fault," *EUROCRYPT'97*, Vol. 1233, *LNCS*, pp. 37-51, 1997.

[5] M. Joye, A. Lenstra, and J. Quisquater, "Chinese Remaindering Based Cryptosystems in the Presence of Fault", *Journal of Cryptology*, Vol. 12, pp. 241-245, 1999.

[6] J. Blömer, M. Otto, J. Seifert, "A New CRT-RSA Algorithm Aecure Against Bellcore Attacks," *ACM*, pp. 311-320, 2003.

[7] A. Shamir, "Method and Apparatus for Protecting Public Key Schemes from Timing and Fault Attacks", *US Patent*, No. 5,991,415, 1999.

[8] C. Giraud, "Fault Resistant RSA Implementation," *FDTC'05*, Vol. 2779, *LNCS*, pp. 142 - 151, 2005.

[9] A. Boscher, R. Naciri, and E. Prouff, "CRT RSA Algorithm Protected Against Fault Attacks," *WISTP 2007*, Vol. 4462, *LNCS*, pp. 237 - 252, 2007.

[10] A. Boscher, H. Handschuh, E. Trichina, "Blinded Fault Resistant Exponentation Revisited," *FDTC'09*, *IEEE*, pp. 3-9, 2009.

[11] G. Fumaroli and D. Vigilant, "Blinded Fault Resistant Exponentiation," *FDTC'06*, Vol. 4236, *LNCS*, pp. 62 - 70, 2006.

[12] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," *CRYPTO'99*, Vol. 1666, *LNCS*, pp. 388-397, 1999.

[13] D. Wagner, "Cryptanalysis of a Provably Secure CRT-RSA Algorithm," *ACM*, pp. 92 - 97, 2004.

[14] S. Yen, L. Ko, S. Moon, and J. Ha, "Relative Doubling Attack Against Montgomery Ladder," *ICISC'05*, *LNCS*, Vol. 3935, pp. 117-128, 2006.