情報保護學會論文誌
第19卷 第5號, 2009. 10

비정상 전원 전압을 이용한 RSA 암호 시스템의 실험적 오류 주입 공격

박 제 훈,[1†] 문 상 재,[1‡] 하 재 철[2]
[1]경북대학교, [2]호서대학교

An Experimental Fault Injection Attack on RSA Cryptosystem using Abnormal Source Voltage

JeaHoon Park,[1†] SangJae Moon,[1‡] JaeCheol Ha[2]
[1]Kyungpook National University, [2]Hoseo University

요 약

CRT-RSA 알고리즘이 스마트카드나 마이크로컨트롤러 등의 암호 장치에 구현된 경우, 레이저 주입, 전자파 방사, 이온 빔 주사, 전압 글리치 주입 등의 오류 주입 기술 등에 의해 CRT-RSA 알고리즘의 비밀 소인수 p, q가 쉽게 노출될 수 있다. 그 중 전압 글리치 오류는 대상 암호 장치에 어떠한 조작이나 변형 없이 적용 가능하여 보다 실제적이다. 본 논문에서는 비정상 전원 전압을 이용한 오류 주입 공격을 실험하였다. 실험 결과 기존에 알려진 고전압 글리치를 주입하는 방법 외에도 전원 전압을 일정 시간동안 단절함으로써 CRT-RSA의 비밀 소인수 p,q를 알아낼 수 있었다.

ABSTRACT

CRT-based RSA algorithm, which was implemented on smartcard, microcontroller and so on, leakages secret primes p and q by fault attacks using laser injection, EM radiation, ion beam injection, voltage glitch injection and so on. Among the many fault injection methods, voltage glitch can be injected to target device without any modification, so more practical. In this paper, we made an experiment on the fault injection attack using abnormal source voltage. As a result, CRT-RSA's secret prime p and q are disclosed by fault attack with voltage glitch injection which was introduced by several previous papers, and also succeed the fault attack with source voltage blocking for proper period.

Keywords: Fault injection attack, CRT-RSA, Source voltage blocking, Voltage glitch, Microcontroller

I. 서 론

CRT-RSA 암호 시스템은 일반 RSA 암호 시스템에 비해 효율적이며, 소인수 분해 문제에 기반 하여 이론적으로 높은 안전성을 제공하지만 최근에 등장한 오류 주입 공격에 매우 취약한 특성을 보인다[1-4]. 오류 주입 공격자는 암호 칩 내부에서는 수행되는 암호 알고리즘 연산 도중 오류를 주입하여 잘못된 결과 값을 출력하거나 칩이 오동작 하도록 만들어 CRT-RSA 암호 시스템의 비밀 소인수 p, q를 추출해 낼 수 있다. 암호 칩에 오류를 주입하는 방법으로는 하드웨어 칩의 특정 부분에 전압 글리치(glitch)를 넣거나 전자파 방사 그리고 레이저 주사와 같은 방법을 이용한다.

물론, CRT-RSA 암호 알고리즘에 적용 가능한 오류 주입 공격 방법뿐만 아니라 이에 대한 방어 대책들도 많이 연구되고 있다[5-10]. 하지만, 대부분의 연구 결과들은 공격 대상 칩 대한 실제적인 실험 결과가 아닌 이론적 결과여서, 오류 주입 공격을 실험적 방법

접수일(2009년 7월 2일), 수정일(2009년 8월 8일),
게재확정일(2009년 9월 2일)
† 주저자, jenoon65@ee.knu.ac.kr
‡ 교신저자, sjmoon@ee.knu.ac.kr

으로 증명한 연구는 국내·외적으로 많지 않다. 실제 CRT-RSA에 오류 주입 공격을 실험한 연구 결과들로는 영국의 Cambridge 대학[11], 벨기에의 Louvain 대학[12], 오스트리아의 Graz 대학[13] 연구 그룹 정도이며 국내에서는 디캡된 칩의 내부 회로에 레이저 오류를 주입한 실험 결과[14]가 발표되었다.

본 논문에서는 CRT-RSA 암호시스템을 실제 상용화된 마이크로프로세서에 구현했을 경우 보다 적용이 용이한 오류 주입 기술을 실험하기 위해 공격 대상 칩에 어떠한 조작도 가하지 않고 외부에서 입력되는 전원 전압을 순간적으로 차단하거나 고전압 글리치를 주입하는 방법으로 칩의 잘못된 연산을 유도하는 실험을 수행하였다. 그 결과 비정상 전원 전압을 이용한 오류 주입에 의해 출력된 오류 결과 값을 이용하여 CRT-RSA 암호 시스템의 비밀 소인수 p, q를 알아 낼 수 있었다.

II. RSA 암호 시스템에 대한 오류 주입 공격

2.1 CRT-RSA 알고리즘

CRT-RSA 알고리즘은 일반 RSA 알고리즘이 모듈러스 N에서 연산하는 것과 달리 비밀 소인수인 p, q 상에서 각각 계산한 후, 두 결과를 재결합(recombination)하여 최종 서명을 출력한다. [그림 1]은 가우스(Gauss) 재결합 방법을 사용하는 CRT-RSA 알고리즘을 보여주고 있다.

여기서, d는 비밀키이고, m은 입력 메시지이다.

CRT-RSA 알고리즘은 일반 RSA에 비해 절반정도의 유한체 $GF(p)$와 $GF(q)$에서 연산이 수행되므로 약 4배 정도 빠른 연산 속도를 가지는 것으로 알려져 있다. 또한 유한체 연산에 필요한 p와 q가 노출되지 않기 때문에 S_p와 S_q 연산 중간값을 예측할 수 없어 일반 RSA 알고리즘과 달리 전력 분석 공격 적용이 어렵다[15].

입력 : p, q, d, p_I, q_I, N, m
여기서, $p_I = p^{-1} \bmod q$, $q_I = q^{-1} \bmod p$.
출력 : $S = m^d \bmod N$

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

[그림 1] CRT-RSA 서명 알고리즘

[그림 1]에서 사용한 Gauss 재결합 방법 외에도 식 (1)과 같은 Garner의 재결합 방법을 사용하기도 한다.

$$S = S_q + [(S_p - S_q) \cdot q_I \bmod p] \bmod N \tag{1}$$

일반적으로 Garner 재결합 방식이 Gauss 재결합 방식보다 역수 계산이 한번 적은 장점이 있어 흔히 이용된다. 그러나 본 논문의 오류 주입 공격은 재결합 과정이 다르더라도 두 방식에 모두 적용된다.

2.2 오류 주입 공격에 대한 이론적 배경

CRT-RSA 알고리즘에 대한 오류 주입 공격 방법은 1996년 Bellcore사에서 처음 제안한 것으로서 $GF(p)$체 상의 멱승이나 $GF(q)$체 상의 멱승 과정에 오류를 주입하여 효과적으로 CRT-RSA 알고리즘의 비밀 소인수인 p와 q를 알아낼 수 있는 공격 방법이다[2,3]. 공격이 적용되는 원리는 식 (2)와 같다. 식 (2)에서는 $S_p = m^{d_p} \bmod p$를 계산하는 과정에 오류가 주입되었다고 가정한다.

$$\begin{aligned} & GCD(S - S', N) \\ &= GCD((S_p \cdot q \cdot q_I + S_q \cdot p \cdot p_I) \\ &\quad - (S_p' \cdot q \cdot q_I - S_q \cdot p \cdot p_I), N) \\ &= GCD((S_p \cdot q \cdot q_I - S_p' \cdot q \cdot q_I), N) \\ &= GCD((S_p - S_p') \cdot q_I, \ p \cdot q) \\ &= q \end{aligned} \tag{2}$$

여기서, S'은 오류 서명값이고, $GCD()$는 최대공약수를 구하는 함수이다.

같은 원리로 $S_q = m^{d_q} \bmod q$에 오류를 넣으면 소수 p를 찾아낼 수도 있다. 즉, S_p 계산중에 오류가 주입되면 q값을 알아낼 수 있으며, S_q 계산중에 오류가 주입되면 p값을 알아낼 수 있다. 또한, Joye 등은 정상적인 서명값이 없더라도 한 개의 오류 서명만을 이용하여 CRT- RSA 암호 시스템의 비밀 키를 알아낼 수 있는 방법을 제안하였다[4].

$$GCD(((S')^e - m), N) = q \tag{3}$$

이러한 오류 주입 공격이 제시된 이후 오류 주입 공격에 대응할 수 있는 다양한 대응 알고리즘들이 제시되었을 뿐만 아니라 보다 정교한 오류 주입 공격 방법

들이 제안되었지만 대부분이 이론적인 접근 방법만을 사용하고 있다[7-10].

III. 전원 전압에 대한 오류 주입 공격

최근 국내에서 공격 대상 칩을 디캡하여 내부 회로를 노출 시킨 후 레이저를 이용해 오류 연산을 유도한 실험 결과가 발표되었다[14]. 본 논문에서는 [14]와는 다르게 공격 대상 칩에 어떠한 변형도 가하지 않고 오류 연산을 유도할 수 있도록 칩의 전원부에 적용 가능한 오류 주입 공격 방법을 실험하였다. 실험 결과 외국 사례들에서 소개된 전압 글리치 오류 주입 실험[12]을 이용하여 비밀 소인수를 알아낼 수 있었고 전원 전압을 순간적으로 단절하는 방법으로도 오류 연산을 유도할 수 있었다.

3.1 주요 실험 장비

3.1.1 공격 대상 칩

상용 마이크로프로세서인 ATmega128 칩에 오류 주입 공격을 시도하였으며, [표 1]은 ATmega128의 주요 제원을 나타낸 것이다[16].

[표 1] ATmega128 사양 및 특성

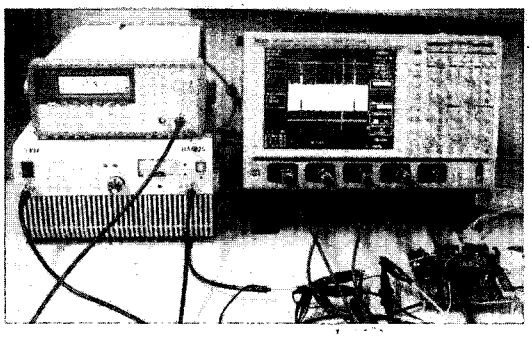
Program Memory	Bytes	128K
	# Optional External memory	~ 64K
Data SRAM (Bytes)		4K
EEPROM (Bytes)		4K
주 클럭		16MHz
구동 전압		4.5V ~ 5.5V

3.1.2 전력 증폭기

전원 전압을 단절하거나 순간적으로 증폭시키기 위하여 NF 사의 High Speed Bi-polar Amplifier BA4825 장비를 사용하였다[17].

[표 2] 전력 증폭기의 주요 재원

주파수대역	DC ~ 2MHz
이득 설정 가능	고정 : ×1 ×10, ×20, ×50 가변 : ×1(CAL) ~ ×3 연속
고출력 전압/전류	100Vrms (300Vpp), 0.5Arms



[그림 2] 오류 주입 공격 실험 환경

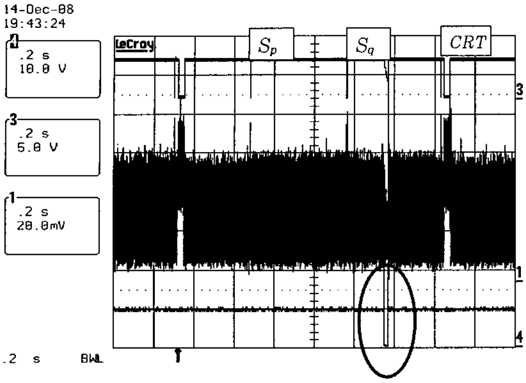
[그림 2]는 전원 전압 단절과 전압 글리치 인가 실험을 하기 위한 실험 환경을 나타낸 것이다. [그림 2]에서 함수 발생기의 출력을 전력 증폭기의 입력으로 사용하였고, 전력 증폭기의 출력을 ATmega128 칩의 전원으로 사용하였다. 그리고 암호 칩을 제어하는 PC와는 시리얼 통신을 통해 시스템 파라미터를 입력하고 연산된 결과를 출력하도록 하였다.

3.2 전원 전압 단절 실험

실험에 사용된 오류 주입 공격 방법은 CRT-RSA의 비트 크기나 이론적인 취약성과는 상관없이 적용된다. 본 논문에서는 공격 대상 칩의 용량 문제로 256비트의 CRT-RSA 알고리즘을 8비트 마이크로프로세서인 ATmega128 칩에 구현하여 사용할 경우 오류

[표 3] CRT-RSA 알고리즘의 주요 파라미터

비밀 키 d	5CC2E64A689B0048A57F5D3E4520A1B7B849935A622F192DB3C3620B142C148B
비밀 키 d_p	DCEEBBA88BC8C89A61DEBA8E2D8A9A5D
비밀 키 d_q	21F15D8BC0A375150330D5B87AA0CACF
공개 키 e	6B633E3C408F104C182AC3DFB2E4BC5DD6D39E3B1A117A2DAF9EFF6027B74A57
비밀 값 p	F4EF38D2CAFF310D2A024BE1FE192D73
비밀 값 q	DC09277087E630B53DDBB6BE707BBC2F
합성수 N	D28656FA4233CEC43317C9B91CBED8664527A8DB6EBFEA9F80467C6D4A40CC1D



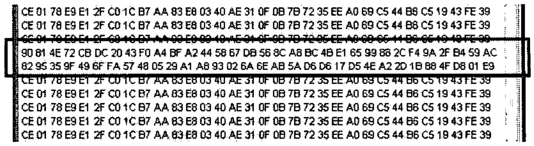
〔그림 3〕 전원 전압 단절 시의 오실로스코프 파형

주입 공격 가능 여부를 검증하고자 한다. 〔표 3〕은 256비트용 CRT-RSA 암호 시스템에 사용된 시스템 파라미터를 16진수로 정리한 것이다. 〔표 3〕에서 e와 N은 공개되는 값이고, d, p, q, d_p, d_q는 비밀 정보이다.

〔그림 3〕은 CRT-RSA 알고리즘이 동작하는 중 ATmega128칩의 전원 전압이 5V에서 순간적으로 0V로 변했을 때의 오실로스코프 파형 변화를 보여주고 있다. 〔그림 3〕에서 제일 상단의 신호는 CRT-RSA 알고리즘의 세부 연산을 구분하기 위한 I/O 신호이고, 두 번째 중간에 위치한 신호는 소비 전력 파형인데 S_p, S_q, CRT 재결합 연산 구간으로 구별된다. 세 번째 신호는 ATmega128 칩에 인가되는 실제 전원 전압을 나타내고 있다.

〔그림 3〕에서 보면 $S_q = S^{d_q} \bmod q$가 계산되는 중에 전원 전압 5V에서 0V로 변하여 일정 시간동안 전원 전압이 단절되고 있다는 것을 알 수 있다. 전압 단절 시점에 따라 약간의 차이는 있었지만 약 27ms 미만의 시간동안 전압을 단절하면 정상동작하면서 정상 결과값을 출력하지만, 약27ms~30ms의 시간 동안 전원 전압을 단절하면 ATmega128 칩의 오류 동작이 유도되어 오류 결과를 출력하는 것을 확인할 수 있었다. 그리고, 30ms 이상의 시간동안 전원 전압을 단절하면 칩의 동작이 멈추는 것을 확인하였다. 〔그림 4〕는 전원 전압 단절로 인한 오류 출력 결과들을 보여주고 있다.

256 비트 CRT-RSA 알고리즘의 정상 서명값은 'CE0178E9E12FC01CB7AA83E80340AE310F0B7B7235EEA069C544B6C51943FE39' 이지만, 〔그림 4〕의 출력들을 살펴보면 정상 서명값과 다른 오류 서명값들을 출력됨을 알 수 있다. 오류 출력들 중



〔그림 4〕 전압 단절에 의한 오류 서명 출력

하나를 이용하여 Bellcore 공격을 적용하면 다음과 같다.

• 정상 서명값 :
CE0178E9E12FC01CB7AA83E80340AE310F0B7B7235EEA069C544B6C51943FE39

• 오류 서명값 :
90814E72CBDC2043F0A4BFA2445867DB568CA8BC4BE16599882CF49A2FB459AC

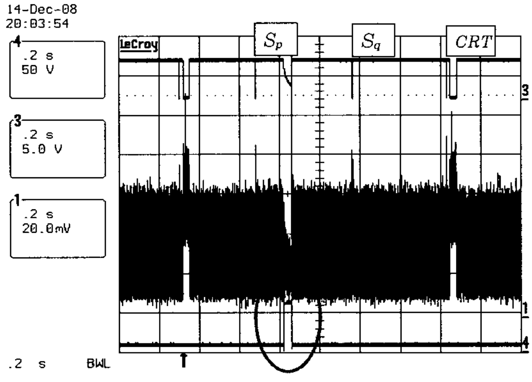
• 정상 서명값 - 오류 서명값 :
3D802A7715539FD8C705C445BEE84655B87ED2B5EA0D3AD03D17C22AE98FA48D

• GCD(정상 서명값 - 오류 서명값, N)
= F4EF38D2CAFF310D2A024BE1FE192D73 = p

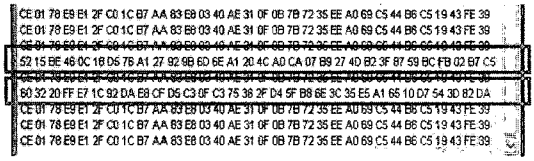
같은 방법으로 $S_p = m^{d_p} \bmod p$ 계산 중에 전압 글리치 오류를 주입하여 잘못된 서명 값을 이용하면 비밀 값 q를 알아낼 수 있다.

3.3 전압 글리치 주입 실험

벨기에의 Louvain 대학의 연구 사례를 참고하여 CRT-RSA 알고리즘이 동작하는 중 ATmega128 칩의 전원 전압을 5V에서 순간적으로 50V로 변화시켜 전압 글리치를 회로에 인가하는 실험을 수행 하였다. 〔그림 5〕는 전압 글리치 인가에 따른 소비 전력



〔그림 5〕 전원 글리치 인가 시의 오실로스코프 파형



〔그림 6〕 전압 글리치 인가에 의한 오류 서명 출력

변화를 보여주고 있다.

〔그림 5〕에서와 같이 $S_p = m^{d_p} \bmod p$를 계산하는 과정 중에 전압 글리치가 주입되었다. 실험에서는 38ms 이하의 시간동안 50V의 전압을 주입해도 칩은 정상동작하면서 올바른 서명 값을 출력한다. 하지만, 약 38ms ~ 40ms 시간동안 50V 전압을 주입하면 칩은 오류 서명 값을 출력하였다. 그리고 40ms 이상의 시간동안 주입할 경우에는 칩이 동작을 멈추는 것을 확인할 수 있었다. 다음의 〔그림 6〕은 전압 글리치 오류를 주입할 때의 CRT-RSA 알고리즘 출력을 나타내고 있다.

앞선 전압 단절 실험과 마찬가지로 오류 출력값을 이용하여 Bellcore 공격을 적용하면 $S_p = m^{d_p} \bmod p$ 계산 과정 중에 오류가 주입되었기 때문에 비밀 소인수 q를 알아낼 수 있다.

IV. 결 론

본 논문에서는 상용 ATmega128 칩에 CRT-RSA 암호시스템을 구현한 후, 공격 대상 칩에 어떠한 변형도 가하지 않은 채로 적용 가능한 전압 단절 오류와 전압 글리치 오류 주입 실험을 수행하였다. 그 결과 약 27ms ~ 30ms의 시간동안 전원 전압을 단절하게 되면 ATmega128 칩의 오류 동작을 하였으며 약 50V의 전압 글리치를 전원단에 38ms ~ 40ms 시간동안 주입하게 되면 오류 결과값을 출력한다는 것을 확인하였다. 또한 오류 출력 결과를 이용하여 Bellcore 공격을 적용한 결과 CRT-RSA 알고리즘의 비밀 값인 p, q를 알아낼 수 있었다.

참 고 문 헌

〔1〕 C. Couvreur and J.J. Quisquater, "Fast decipherment algorithm for RSA public-key cryptosystem," Electronics Letters, vol. 18, issue. 21, pp. 905 - 907, Oct. 1982.

〔2〕 D. Boneh, R. DeMillo, and R. Lipton, "New Threat Model Breaks Crypto Codes," Bellcore Press Release, Sep. 1996.

〔3〕 A. Lenstra, "Memo on RSA Signature Generation in the Presence of Faults," private communication (available from the author), Sep. 1996.

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

〔5〕 D. Boneh, R. DeMillo, and R. Lipton, "One the importance of checking cryptographic protocols for faults," Eurocrypt Conference-EUROCRYPT'97, LNCS 1233, pp. 37-51, 1997.

〔6〕 C. Giraud, "Fault resistant RSA implementation," Workshop on Fault Diagnosis and Tolerance-FDTC'05, LNCS 2779, pp. 142-151, 2005.

〔7〕 S. Yen, S. Kim, S. Lim, and S. Moon, "RSA speedup with residue number system immune against hardware fault cryptanalysis," International Conference on Information Security and Cryptology-ICISC'01, LNCS 2288, pp. 397-413, 2001.

〔8〕 S. Yen, D. Kim, and S. Moon, "Cryptanalysis of two protocols for RSA with CRT based on fault infection," Workshop on Fault Diagnosis and Tolerance-FDTC'06, LNCS 4236, pp. 53-61, 2006.

〔9〕 J. Blömer, M. Otto, and J. Seifert, "A new CRT RSA algorithm secure against Bellcore attacks," Proceedings of the 10th ACM conference on Computer and communications security, pp. 311-320, Oct. 2003.

〔10〕 D. Wagner, "Cryptanalysis of a provably secure CRT-RSA algorithm," Proceedings of the 11th ACM conference on Computer and communications security, pp. 92-97, Oct. 2004.

〔11〕 S. Skorobogatov and R. Anderson,

"Optical Fault Injection Attack," Workshop on Cryptographic Hardware and Embedded Systems-CHES '02, LNCS 2523, pp. 2-12, 2002.

[12] C. Kim and J. Quisquater, "Fault Attacks for CRT Based RSA: New Attacks, New Results, and New Countermeasures," Workshop in Information Security Theory and Practice-WISTP'07, LNCS 4462, pp. 215-228, 2007.

[13] M. Schmidt and M. Hutter, "Optical and EM Fault-Attacks on CRT-based RSA: Concrete Results," Proceedings of the 15th Austrian Workshop on Microelectronics, pp. 61-67, Oct. 2007.

[14] 박제훈, 문상재, 하재철, "CRT-RSA 암호시스템에 대한 광학적 오류 주입 공격의 실험적 연구," 정보보호학회논문지, 19(3), pp. 51-57, 2009년 6월.

[15] T. Messerges, E. Dabbish, and R. Sloan, "Power Analysis Attacks of Modular Exponentiation in Smartcards," Workshop on Cryptographic Hardware and Embedded Systems-CHES'99, LNCS 1717, pp. 144-157, 1999.

[16] Atmel, http://www.atmel.com/dyn/product/product_card.asp?part_id=2018

[17] NF, http://www.nfcorp.co.jp/english/ pro/pp/p_amp/h_spe/ba/index.html