情報保護學會論文誌
第14券 第5號, 2004. 10

작은 CRT 지수를 사용한 RSA에서의 일부 키 노출 공격

이 희 정†
강남대학교

Partial Key Exposure Attack on Unbalanced RSA with small CRT exponent

Hee Jung Lee
Kangnam University

요 약

RSA 공개키 시스템은 비밀키의 크기를 작게 하여 효율성을 높이고 있는 데 이는 안전성 측면에서 취약하다. 이를 보완하기 위하여 중국인의 나머지 정리를 이용한 비밀키 생성 기법이 많이 이용되고 있다. 그러나 이러한 기법은 side channel attack 에 매우 취약하다. 따라서 일부 키 노출에 따른 전체 키 복원에 관한 연구가 활발히 진행되고 있다. May는 2003년 Crypto에서 두 소수의 크기는 같고 중국인의 나머지 정리를 이용하여 비밀키를 생성한 경우에 비밀키의 일부 $N^{1/4}$ 비트가 노출되면 전체가 복원되는 것을 보였다. 또한, May는 2002년 Crypto에서 변형된 RSA형태 중의 하나인 두 소수의 크기가 다르고 작은 CRT(중국인의 나머지 정리) 지수를 이용한 RSA를 분석하였는데 이때 작은 소수의 크기가 $N^{0.382}$보다 작으면 CRT 지수의 크기에 따라 N이 소인수분해 될 수 있다고 경고하였다. 본 논문에서는 May의 두 소수의 크기가 다른 변형된 RSA(작은 소수의 크기가 $N^{0.382}$보다 큰 경우)에서 작은 CRT 지수를 이용하여 비밀키를 생성한 경우에 어느 정도의 노출이 전체를 복원하게 하는지를 살펴본다. 공개키 e가 너무 크지 않을 때 작은 소수 p의 크기와 관계없이 비밀키 d_p의 약 $N^{0.25}$정도의 비트가 노출되면 N이 소인수분해가 된다. p, q의 크기가 비슷할 때 p의 약 $N^{1/4}$비트만 노출이 되면 N을 소인수분해 할 수 있다는 것을 Coppersmith가 보였는데 본 논문에서는 두 소수의 크기가 다를 때도 약 $N^{1/4}$비트가 노출되면 소인수분해가 가능한 것을 보이고 이를 이용하여 위의 내용을 증명한다.

ABSTRACT

In Crypto 2002 May analyzed the relation between the size of two primes and private key in unbalanced RSA with small CRT exponent. Also in Crypto 2003 he showed that if $N^{1/4}$ amount of most significant bits(least significant bits) of d_p is exposed in balanced RSA with CRT, N can be factored. To prove this he used Howgrave-Graham's Theorem. In this paper we show that if $N^{1/4}$ amount of d_p, p is smaller than q, and bigger than $N^{0.382}$ to avoid May's attack, is exposed in

접수일 : 2004년 6월 15일 ; 채택일 : 2004년 6월 15일
* 본 연구는 2004년도 강남대학교 교내 연구비 지원에 의한 것임.
† hjlee@kangnam.ac.kr

unbalanced RSA with small CRT exponent, it is enough to expose d_p. We use Coppersmith's theorem with unbalanced primes.

Keywords : *CRT, unbalanced RSA, partial key exposure attack, Coppersmith theorem*

Ⅰ. 서 론

파라메터들의 크기 관계는 RSA 공개키 시스템의 안전성에 큰 영향을 준다.

1990년 Wiener[1]는 두 소수 p, q의 크기가 같을 때 비밀키 d가 $N^{0.25}$보다 작으면 비밀키를 찾아낼 수 있음을 continued fraction을 이용하여 보였다. 그 후 1998년 Boneh와 Durfee[2]는 두 소수 p, q의 크기가 서로 같을 때 비밀키가 $N^{0.292}$보다 작으면 N을 소인수분해 할 수 있고 따라서 비밀키를 찾아낼 수 있음을 보였다. Boneh 등의 공격을 피하기 위하여 1999년 Sun, Yang Laih[3]이 두 소수의 크기가 다른 경우의 3가지 형태의 알고리즘을 제안하였는데 그들에 따르면 비밀키를 작게 선택하여도 두 소수의 크기가 다르면 안전하다고 하였다. 그러나, 2000년 Nguyen[4]는 이들이 제안한 알고리즘도 공격에 취약함을 보였는데 두 소수의 크기가 서로 다르면 비밀키가 작을 때 위험할 뿐만이 아니라 오히려 두 소수의 크기가 다를수록 비밀키의 크기는 커야만 안전하다는 것을 보였다. 서로 다른 크기의 두 소수에 대한 비밀키의 크기는 공개키 e의 크기와도 밀접한 관계가 있는데 Nguyen은 이를 모두도 분석해 놓았다.

Wiener는 비밀키의 크기를 작게 하면서도 안전하게 하기 위해서 두 가지 방법을 제안했는데 하나는 큰 공개키 e를 사용하는 것이고 다른 하나는 중국인의 나머지 정리(The Chinese Remainder Theorem)를 활용하는 것이다. 그러나 2002년 May[5]가 Crypto에서 두 소수의 크기가 다르면 중국인의 나머지 정리를 이용하여 비밀키를 생성한다고 하여도 공격이 가능함을 보였다. 이때 효율성을 높이기 위해서 작은 소수에 대한 비밀키는 임의로 선택하더라도 큰 소수의 비밀키는 작게 선택하는데 이를 '작은 CRT 지수'라고 한다. 이와 같이 각각의 소수에 대해서 선택한 비밀 키들을 중국인의 나머지 정리를 이용하여 비밀키를 생성한다고 하더라도 작은 소수가 $N^{0.382}$보다 작으면 위험하다는 것을 보였는데 구체적으로 작은 소수 p의 크기를 N^{β}라하고, 작은 CRT 지수, d_q의 크기를 $N^{\delta'}$라 할 때 이들의 관계는 $\delta' = 1/2 - 3/2\beta + 1/2\beta^2$ (또는 $\delta' = 1 - 5/3\beta - 2/3\sqrt{3\beta - 5\beta^2}$)가 됨을 보였다. 즉, 작은 소수 p의 크기가 작으면 작을 수록 '큰' 작은 CRT 지수를 찾아낼 수 있다는 것이다. 다시 말해서 두 소수의 크기가 차이가 많이 나지 않을수록 작은 CRT 지수를 선택하여도 안전하다는 것이다.

위와 같이 안전한 비밀키를 선택한다고 하더라도 side channel attack을 통하여 비밀키의 일부 노출을 막을 수는 없다. 따라서 위와 같은 상황에서 일부 비밀키의 노출로 인하여 비밀키 전체를 복원할 수 있는지에 대해서 알아봐야 한다. Boneh와 Durfee[6]은 비밀키의 일부가 노출되면 전체를 복원될 수 있음을 보였다. 이때 조건은 두 소수의 크기가 같다는 것과 공개키가 작거나 최대 $\sqrt{N}$보다 작다는 것이다. 그리고 비밀키 d에 대해서 N의 비트수를 n이라 할 때 $n/4$정도의 least significant bits를 알아야 한다는 것이다. Boneh 등은 $n/4$정도의 p의 least significant bits나 most significant bits를 알면 N을 소인수분해 할 수 있다는 Coppersmith의 정리[7]을 이용하였다. 2003년 May[8]은 공개키가 $N^{0.5} < e < N^{0.725}$ 범위에서 비밀키가 $n/4$정도 노출되면 N을 소인수분해 할 수 있다는 것을 보였다. 그리고 중국인의 나머지 정리를 이용하여 비밀키를 선택할 때도 d_p의 least significant bits나 most significant bits들을 약 $n/4$정도 알게 되면 비밀키를 복원할 수 있음을 보였다. May는 N을 소인수분해하기 위해서는 $kp + \varepsilon$만을 알면 가능하다는 Howgrave-Graham의 정리[9]를 사용하였다.(k는 알려지지 않고 ε는 에러 항으로 크기가 $N^{1/4}$보다 작다.)

정리 1 (Coppersmith)

$N = pq$라 하자. N의 비트수를 n이라 할 때 약 $n/4$ 정도의 least significant 비트나 약 $n/4$ 정도의 most significant 비트를 알면 N을 효율적으로 인수분해 할 수 있다.

정리 2 (Howgrave-Graham)

$N=pq$이라 하고 k는 알려지지는 않았지만 q의 배수는 아니라 하자.

약 $N^{1/4}$정도의 오차 범위 안에서 kp의 값을 갖게 되면 다항식시간 안에 N을 소인수분해 할 수 있다.

본 논문에서는 두 소수의 크기가 다르면서 중국인의 나머지 정리를 사용하여 비밀키를 생성할 때 과연 어느 정도의 비밀키가 노출되면 비밀키 전체가 복원될 수 있는지 알아보려고 한다. 이때 작은 소수를 $N^{0.382}$보다 크게 선택하면 작은 CRT지수의 크기와 상관없이 May의 공격에 안전하다. 따라서 작은 소수는 $N^{0.382}$보다 크고 CRT지수는 임의의 크기로 선택한다고 하자. 물론 효율성을 높이기 위해서는 '작은' CRT 지수가 선택된다고 가정할 수 있다. e의 크기가 작을 때 두 소수의 크기와 관계없이 노출된 비밀키의 비트수가 $N^{1/4}$정도이면 전체가 복원됨을 알 수 있다. 이를 Coppersmith 정리의 변형을 이용하여 증명한다.

2장에서는 작은 CRT 지수를 이용한 크기가 다른 두 소수를 이용한 RSA를 소개하고 3장에서 크기가 다른 두 소수의 RSA에서 소수의 일부를 알면 소인수분해 되는 Coppersmith 정리의 변형을 증명하고 이를 이용하여 일부키 노출에 따른 N의 소인수분해(전체 키의 복원)을 살펴본다.

II. 작은 CRT 지수를 사용한 변형된 RSA

RSA의 효율성과 안전성을 높이기 위해서 중국인의 나머지 정리를 이용한 비밀키 생성 기법이 많이 사용되고 있다. 이때 같은 크기의 두 소수를 이용할 때가 크기가 다른 두 소수를 이용할 때보다 공격에 안전하나 효율성을 높이기 위해서 서로 다른 크기의 두 소수를 선택할 때가 있다. 이러한 경우의 안전성은 작은 CRT 지수의 크기와 밀접한 관계가 있다. May[5]가 소개한 키생성 과정을 살펴보고 소수의 크기와 작은 CRT 지수의 크기 관계가 안전성에 끼치는 영향을 살펴본다.

1. 작은 CRT 지수를 사용한 키 생성

공개키 N의 비트수를 n, 작은 소수 q의 크기는 N^{β}, 작은 CRT 지수, d_p의 크기를 N^{δ}라 하자. 이때 $\beta \le 1/2$ 이고 $\delta \le 1$ 이다.

- 임의의 소수 p, q를 각각 크기가 $(1-\beta)n, \beta n$ 이 되도록 선택한다. $p-1$과 $\frac{q-1}{2}$는 서로소이다. $N=pq$를 계산한다. 만약 $q < N^{\beta}$가 아니면 두 소수를 다시 선택한다.
- 비밀키 $d_p \in Z^*_{p-1}$ 를 크기가 N^{δ}보다 작게 선택한다. 비밀키 $d_q \in Z^*_{\frac{q-1}{2}}$는 임의의 크기로 선택한다.
- $d \equiv d_p \bmod p-1, d \equiv d_q \bmod \frac{q-1}{2}$를 만족하는 $d \bmod \frac{\phi(N)}{2}$를 중국인의 나머지 정리를 이용하여 구한다.
- 법 $\frac{\phi(N)}{2}$에 대한 d의 역원 e를 구한다.
- N과 e를 공개한다.

2. 작은 CRT 지수와 큰 소수의 크기 관계

큰 소수 p와 d_p, 그리고 e는 다음과 같은 관계를 갖는다.

$$d \equiv d_p \bmod p-1, ed_p - 1 = k(p-1),$$
$$ed_p - 1 + k = kp$$

$$|k+1| = \left|\frac{ed_p - 2}{p-1}\right| < \frac{ed_p}{p-1} < \frac{q-1}{2} d_p < N^{\beta+\delta}$$

$ed_p - 1 + k = kp$에서 e를 알고 있으므로 d_p와 $k-1$을 찾는 법 p에 관한 합동 방정식을 얻을 수 있다. 이를 $f_p(x, y)$라 하자. 다시 말해서 $f_p(x, y) = ex - y$를 얻게 되고 해 $(x_0, y_0) = (d_p, k+1)$이며 d_p는 N^{δ}보다 작고, $k+1$은 $N^{\delta+\beta}$보다 작다. Howgrave-Graham의 정리를 이용하여 정수상의 다항식으로 전환하면 2차원 Lattice에서는 $3\beta + 2\delta \le 1 - \log_N$ (4)의 관계를, 임의의 차수로 확장하면 $3\beta - \beta^2 + 2\delta \le 1$의 관계를 얻게 된다. 이는 β가 0.382까지 해를 구할 수 있고 따라서 소인수분해가 가능하다는 것이다. 그러나 이 경우 작은 CRT 지수는 거의 0에 가깝다. 법 e에 대해서 함수를 선택하면 법 p의 경우와 비교해서 $\beta = 0.23$까지는 더 큰 CRT 지수를 선택할 수 있으나 $\beta = 1/3$까지만 해를 구할 수 있다.

위의 결과에서 우리는 작은 소수의 크기를 $N^{0.382}$ 보다 크게 정하면 작은 CRT 지수를 선택하더라도 위의 공격에 안전하다. 동시에 작은 소수를 선택하더라도 CRT 지수를 크게 선택하면 공격을 피할 수 있다.

[참고]

1. 법 e에 관해서는 함수 $f_e(y,z)=y(N-z)$, $-N(y_0,z_0)=(k+1,q) \bmod e$, $Y=N^{\beta+\delta}$, $Z=N^{\beta}$를 얻는다.
2. 법 p에서 해를 구할 때에는 정수상의 다항식을 이용하여 N을 소인수분해 할 수 있는데[5] 이와 같은 방법은 실험적(heuristic)인 것이 아니고 결정적(deterministic)이다. 이에 반해서 법 e에 관해서는 실험적으로 밖에는 해를 구할 수 없다.

III. 작은 소수의 크기가 $N^{0.382}$보다 크고 임의의 CRT 지수를 사용한 RSA의 일부 키 노출

작은 소수의 크기가 $N^{0.382}$보다 크고 임의의 CRT 지수를 사용한 RSA에서 일부 키가 노출되었을 때 전체를 복원할 수 있는지에 대해서 알아보기 위해서 크기가 다른 두 소수 중에서 일부분을 알았을 때 소인수분해가 가능한지를 알아본다. 이는 위의 Coppersmith 정리의 변형이라고 할 수 있다. 증명은 Coppersmith의 bivariate polynomial의 해를 구하는 방법을 이용한다[7].

정리 3 (Coppersmith-unbalanced)

두 소수의 크기와 관계없이 소수의 $N^{1/4}$ 정도의 비트를 알면 소인수분해가 가능하다.

증명:

1) MSB 경우

$p \approx 2^{n_1}$, $q \approx 2^{n_2}$ $N=pq \approx 2^{n_1+n_2=n}$, p의 m MSB를 안다고 하자.

$p=2^{n_1-m}p_1+x_0$, $q=2^{n_2-m}q_1+y_0$라 하자. 이때 $|x_0|<2^{n_1-m}=X$, $|y_0|<2^{n_2-m}=Y$ 이다.

$f(x,y)=(p_1+x)(q_1+y)-N$의 해를 구하면 N을 소인수분해 할 수 있다.

Coppersmith의 정리[7]을 이용하여 $\gamma f(xX, yY)$ 계수들의 최고 값을 W라고 하면

$$W=\max\{p_1q_1-N,\ q_1X, p_1Y, XY\},$$

$XY \le W^{2/3\delta}$을 만족할 때 두 변수 방정식의 해를 구할 수 있다.(δl은 각 변수의 최고 차수). $\delta=1$, $W=2^{n-m}$이므로 $XY \approx 2^{n-2m} < (2^{n-m})^{2/3}$을 만족하는 m을 구하면 된다.

따라서, $m > n/4$이면 해 (x_0, y_0)를 구할 수 있고 소인수분해가 가능하다.

2) LSB 경우

$$p=2^m x_0+p_0,\ q=2^m y_0+q_0,$$

이때 $|x_0|<2^{n_1-m}$, $|y_0|<2^{n_2-m}$ 이다.

$f(x,y)=(2^m x+p_0)(2^m y+q_0)-N$은 계수들이 2^m를 공통으로 가지므로 irreducible polynomial이라는 조건을 만족시키지 못한다. 따라서,

$$f(x,y)=\frac{(2^m x+p_0)(2^m y+q_0)-N}{2^m}=2^m xy+q_0x+p_0y+\frac{p_0q_0-N}{2^m}$$

을 사용하여 해를 구한다.($p_0q_0 \equiv N \bmod 2^m$.)

MSB의 경우와 마찬가지로 $W=2^{n-m}$이고 $XY=2^{n-2m}$이므로 $m>1/4$이면 된다. 다시 말해서 LSB의 경우도 소수의 크기와 관계없이 $N^{1/4}$ 정도의 비트를 알면 소인수분해가 가능하다. ■

소수들의 크기가 다른 경우, 특히 작은 소수 q의 크기가 $N^{0.382}$보다 크고 $N^{0.5}$보다 작은 경우의 일부 비밀키 노출에 대해서 알아보려고 한다. 이때 정리 3을 이용한다.

1. d_p의 일부 least significant bits를 알 때

정리 4

RSA에서 서로 다른 크기의 두 소수와 중국인의 나머지 정리를 이용하여 비밀키를 생성하였을 때 작은 소수에 대한 비밀키 d_p의 노출된 부분이 $N^{1/4+s'}$이면 비밀키가 복원된다. 이때 $e-1=2^{s'}t'$.

증명 :

d_0는 d_p의 알고 있는 least significant bits라 하자.

$ed_p-1=k(p-1)$, $d_p \equiv d_0 \bmod 2^{n/4}$, n은 N의 비트수. 이때, $ed_0-1 \equiv k(p-1) \bmod 2^m$

e, d_0를 알고 있고 k는 e보다 작으므로 e만큼의 k를 대입해보면 $kx \equiv ed_0-1 \bmod 2^m$의 일차 합동 방정식을 얻게 된다. $x=p-1$을 법 2^m에 대해서 구할 수 있다. k가 홀수이면 유일 해를 갖지만 k가 짝수이면 즉, $k=2^s t$이고 $(2^m, 2^s)=2^l$, $2^s | ed_0-1$일 때 x는 법 2^{m-l}에 대해서 해가 존재하므로 2^l개만큼의 $p-1$후보를 얻게된다. 그러므로 $2^{m-l} \approx N^{1/4}$이면 d_p를 회복할 수 있다. $k<e$이므로 $e-1=2^{s'}t'$이라고 할 때 $l \le s \le s'$. 따라서 $m > 1/4+s'$이면 $m > 1/4+l$. 그러므로 최대 $N^{1/4+s'}$ LSB를 알면 N을 소인수 분해할 수 있다. ■

2. d_p의 일부 most significant bits를 알 때

정리 5 e의 크기를 N^{α}, $\alpha \in (0, 1/4)$라 하자. 비밀키 d_p의 $N^{1/4-\alpha}$ 의 MSB를 알면 N을 소인수분해 할 수 있다.

증명 :

$ed_p-1=k(p-1)$이다. $|d_p-d_1|<N^{\delta}$ 라 하자.

$\overline{p}=\frac{ed_1-1+k}{k}$ k는 e보다 작으므로 e만큼의 k를 대입해보면,

$$|p-\overline{p}| = \left|\frac{ed_p-1+k}{k} - \frac{ed_1-1+k}{k}\right| = \left|\frac{e(d_p-d_1)}{k}\right| < |e| \cdot |d_p-d_1| < N^{\alpha+\delta}$$

$|p-\overline{p}|<N^{1/4}$이면, $\alpha+\delta<1/4$, 즉, $\delta<1/4-\alpha$이면 Coppersmith 정리에 의하여 N을 소인수분해 할 수 있다. ■

IV. 결 론

본 논문에서는 p의 크기가 $N^{0.382}$보다 크고 CRT 지수의 크기와 관계없이 비밀키가 생성되었을 경우 어느 정도의 비밀키가 노출되면 위험한지를 알아보았다. May는 Howgrave-Graham의 정리를 이용하여 두 소수의 크기가 같을 때 중국인의 나머지 정리를 이용한 경우에도 비밀키 d_p가 $n^{1/4}$정도만 노출되면 전체가 복원됨을 보였는 데 본 논문에서는 두 소수의 크기가 다르고 중국인의 나머지 정리를 이용할 경우에도 비밀키의 $n^{1/4}$정도만 알면(LSB의 경우) 전체를 복원할 수 있음을 보였다. May는 Howgrave-Graham의 정리를 이용하여 증명하였고 본 논문에서는 Coppersmith의 변형을 증명하여 이를 이용하여 소수의 크기가 다른 경우를 살펴보았다. 두 소수의 크기가 같거나 다르거나 Coppersmith 정리를 사용하나 Howgrave-Graham의 정리를 이용하나 전체를 복원하기 위해서는 같은 양의 비밀키 노출이 필요하다는 것을 발견하였다. 또한 작은 CRT 지수를 사용한 RSA가 그렇지 않은 RSA보다 효율성은 높고 partial key exposure attack에는 같은 양의 노출이 필요하므로 더 유용하다고 할 수 있다.

앞으로 연구되어져야 할 과제로는 두 소수의 크기가 다르고 중국인의 나머지 정리를 사용하지 않을 경우는 어느 정도의 비밀키 노출에 위험한가를 알아보아야 할 것이다. 이것은 Boneh가 두 소수의 크기가 같은 경우 e가 $\sqrt{N}$보다 작고 May의 경우는 $N^{0.5}<e<N^{0.725}$으로 나누어 살펴보았듯이 두 소수의 크기가 다를 때에도 각각의 경우로 나누어 분석해 볼 수 있을 것이다. 또 다른 과제로는 두 소수의 크기가 다를 때 Howgrave-Graham 정리는 어떻게 변형될 수 있는지 살펴본다면 여러 경우에 응용될 수 있으리라 생각된다.

참 고 문 헌

[1] M. Wiener, "Cryptanalysis of short RSA secret exponents", IEEE Transactions on Infor. Th, vol.36,No.3, pp. 553-558, 1990

[2] D.Boneh, G.Durfee, "Cryptanalysis of RSA with private key d less than $N^{0.292}$", IEEE Transactions on Information Theory vol.46(4), 2000

[3] Sun, Yang Laih, "ON the design of

RSA with short secret exponent", In proc. of Asiacrypt'99, LNCS vol. 1716, pp.150-164, IACR, Springer-Verlag, 1999

[4] G.Durfee, P.Nguyen, "Cryptanalysis of the RSA schemes with short Secret Exponent from Asiacrypt'99", Proc. of Asiacrypt 2000, LNCS vol.1976, Springer, pp.14-29, 2000

[5] Alexander May, "Cryptanalysis of Unbalanced RSA with small CRT-exponent", Crypto 2002, LNCS 2442, pp. 242-256, 2002

[6] D.Boneh, G.Durfee, Y.Frankel, "Exposing an RSA Private Key Given a Small Fraction of its Bits", Full version of the work from Asiacrypt'98, available at http://crypto.stanford.edu/~dabo/abstracts/bits_of_d.html 1998

[7] D. Coppersmith, "Small Solutions to Polynomial Equations, and Low Exponent RSA vulnerabilities", J. of Cryp--tology 10(4), 1997

[8] Johannes Blömer, Alexander May, "New Partial Key Exposure Attacks on RSA", Crypto 2003, LNCS 2729, pp.27-43, 2003

[9] N. Howgrave-Graham, "Approximate Integer Common Divisors", CaLC 2001, Lecture Notes in Computer Science vol.2146, pp.51-66, 2001

[10] D. Boneh., "Twenty years of Attacks on the RSA Cryptosystem", Notices of the AMS, 1999

[11] N.Howgrave-Graham, "Finding small roots of univariate modular equations revisited", Proc. of Cryptography and Coding, LNCS 1355, Springer-Verlag, 1997

[12] 조동욱, 김영수, 정권성, 원동호, RSA 암호방식의 안전성에 관한 연구, 정보보호학회지 제8권4호, pp.15-46, 1998

〈著者紹介〉

이 희 정 (Hee Jung Lee) 정회원

1980년 2월 : 이화여자대학교 문리대학 수학과 졸업
1989년 8월 : 펜실베니아 주립대학교(Penn. State Univ.) 이학박사
1994년 3월~현재 : 강남대학교 응용수학 전공 부교수
〈관심분야〉 정수론, 암호학