한국수학사학회지 제20권 제1호(2007년 2월), 103-112

RSA 안전성과 Coppersmith 정리*

강남대학교 응용수학전공 **이희정**
hjlee@kangnam.ac.kr

1997년 Coppersmith는 소인수분해를 모르는 법 N에 대한 합동방정식(modular equation)의 '작은 해'를 찾는 방법을 제안한다. 동시에 두 변수 다항식의 제한된 크기의 해를 찾는 방법도 격자이론을 이용하여 제안한다. 이러한 Coppersmith의 정리는 이후 암호학에서 매우 유용하게 사용되는데 특별히 RSA 암호체계에서 비밀 키를 찾아내거나 일부 비밀 키가 노출되었을 때 전체키를 복원하는 데에 중요한 역할을 한다. 본 논문에서는 Coppersmith의 정리를 살펴보고 이것이 RSA의 안전성에 어떠한 영향을 주었는지를 살펴본다.

주제어 : Coppersmith 정리, 격자이론, 다변수 합동방정식, 일부 키 노출 공격,

1. 서론

RSA는 가장 널리 사용되는 공개키 암호체계로서 소인수분해의 어려움에 기반을 둔 공개키 암호체계이다. 1976년 최초로 Rivest, Shamir, Adelman이 제안한 이후 끊임없는 공격을 받아왔으나 구현상의 오류를 제외하고는 어떠한 공격에도 안전하다고 간주되고 있다. 구현상의 오류란 여러 가지가 있을 수 있으나 특히 키 생성 과정에서 일어날 수 있는 오류에 대해서 살펴보려고 한다. 모두 다 알고 있다시피 RSA는 공개키 N, e와 비밀 키 p, q, d로 이루어진다. e와 d는 $\phi(N)$에 대해서 서로 역원 관계이다. 소수 p, q의 크기도 RSA의 안전성에 큰 영향을 주지만 공개키 e와 비밀 키 d의 크기도 안전성에 영향을 준다. 비밀 키 d의 크기가 너무 작으면 안전하지 않다는 것을 1990년 Wiener[1]가 최초로 밝혀낸 이후 어느 정도의 크기가 안전한 가에 대한 연구가 진행되었다. 또한, 비밀 키의 크기를 너무 크게 하면 효율성이 떨어지는 문제를 해결하기 위해서 중국인의 나머지 정리를 사용하는데 이때에도 어느 정도 크기의 비밀 키를 선택하는 것이 안전한 가에 대한 연구가 진행되었다. 이러한 연구가 가능하게 된 것은 1997년 Coppersmith[2]가 발표한 논문 때문이었다. 뿐만 아니라, RSA

* 이 논문은 2006년도 정부(교육인적자원부)의 재원으로 한국대학교육협의회 대학교수 국내교류 연구비 지원에 의한 것임.

는 키의 일부가 노출이 되면 전체키가 복원되는 취약점을 갖고 있는데 어느 정도의 노출이 공격에 취약한 가에 관한 연구도 활발히 진행되고 있다. 최근의 부채널 공격(side channel attacks)에 관한 연구가 활발히 진행되면서 더욱 관심을 받게 되었다. 이러한 모든 공격이 Coppersmith의 연구 결과로부터 가능하였다. 따라서 본 논문에서는 Coppersmith의 연구 결과를 살펴보고 이를 이용하여 최근까지 진행되어온 비밀키 관련 RSA 안전성 연구 결과를 살펴보려고 한다. 2장에서는 Coppersmith 정리를 살펴보고 이를 이용한 다변수 합동 방정식의 해를 구하는 방법을 살펴보고 3장에서는 비밀 키 크기와 관련된 RSA 공격의 연구 결과들을 살펴본다. 4장에서는 일부 키 노출에 따른 전체키 복원에 관한 연구 결과들을 살펴본 후 5장에서 이러한 연구 결과들로부터 향후 연구 방향에 대해서 알아본다.

2. Coppersmith 정리

1997년 Coppersmith는 "Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities"[2]라는 논문에서 한 변수 합동방정식의 '작은' 해를 구하는 방법(정리 1)과 정수상의 두 변수 다항식의 일부 해를 구하는 방법(정리 2)을 제안한다. 또한, 정리 2를 이용하여 RSA에서 한 소수의 일부 비트들(약 반 정도)을 알면 N을 소인수분해 할 수 있음을 보였다.(따름정리)

Coppersmith 정리 1

$p(x)$는 차수가 δ이고 소인수분해를 알지 못하는 N에 대하여 합동다항식일 때 X를 희망하는 해 $|x_0$의 제한된 크기라고 하자. 만약 $X \le N^{1/\delta}$이면 $p(x_0) \equiv 0 \bmod N$을 만족하는 정수 해 x_0를 $(\log N, 2^{\delta})$에 대한 다항식 시간 안에 찾을 수 있다. 단, $x_0 | \le X$

Coppersmith 정리 2

$p(x,y)$를 정수상의 두 변수 기약다항식이라고 하자. 각각의 변수에 대해서 최고 차수가 각각 δ라 하고 X, Y는 원하는 해 x_0, y_0의 제한된 크기라고 할 때 $\tilde{p}(x,y) = p(Xx, yY)$라 하자. 이때 $\tilde{p}$의 계수들 중에서 절대값이 가장 큰 것을 W라 하고 만약 $XY \le W^{2/(3\delta)}$이면 $(\log W, 2^{\delta})$에 대한 다항식 시간 안에 $p(x_0, y_0) = 0$을 만족하는 모든 정수해 x_0, y_0를 찾을 수 있다. 단, $|x_0| < X$, $|y_0| < Y$.

따름 정리

$N=pq$를 n비트의 수라 하고 $r \geq 2^{n/4}$일 때 $p_0 \equiv p \bmod r$인 p_0가 알려지면 n에 대한 다항식 시간 안에 N을 소인수분해 할 수 있다.

※ 이들에 대한 증명은 [2]를 참조

Coppersmith의 정리 1은 한 변수 합동다항식의 '작은' 해를 구하는 것이다. 거의 비슷한 시기에 How-Grave Graham[3]은 Coppersmith와는 별도로 같은 내용을 발표하였다. Coppersmith가 사용한 행렬은 다소 복잡한데 How-Grave Graham이 사용한 행렬은 훨씬 간단하며 이들은 서로 dual관계이다. 1998년 Boneh, Durfee는 Coppersmith[4]의 이론에 근거하여 두 변수 합동다항식의 일부 해를 구하는 방법을 소개하였는데 How-Grave Graham의 행렬을 사용하였다.

두 변수 합동다항식의 일부 해 구하기

$f(x,y) \equiv 0 \bmod N$의 해 (x_0, y_0)는 Coppersmith의 한 변수 합동다항식과 마찬가지로 $\| f(x_0, y_0) \| < \frac{N}{\sqrt{w}}$이면 정수 상의 해임을 알 수 있다. 이때 w는 다항식에 있는 항의 개수이다.(How-Grave Graham) 또한, $f(x,y) \equiv 0 \bmod N$의 해 (x_0, y_0)는 $f^m(x,y) \equiv 0 \bmod N^m$을 만족한다. 그러므로, 충분히 큰 m을 정하여 노름이 $\frac{N^m}{\sqrt{w}}$보다 작은 다항식을 찾아서 정수상의 해를 찾으면 그들 중에 해 (x_0, y_0)가 있음을 알 수 있다. 정수상의 해를 구하는 문제는 다항식 시간 안에 가능하다. 노름이 작은 크기의 다항식을 구하기 위하여 격자이론을 이용한다. 즉, $x_0 < X$, $|y_0| < Y$라 하자.

$$g_{i,k}(x,y) = N^{m-k} x^i f^k(x,y), \quad i = 0, 1, \cdots, \deg f - 1, \quad k = 0, \cdots, m$$

$$h_{j,k}(x,y) = N^{m-k} y^j f^k(x,y), \quad j = 0, 1, \cdots, t, \quad k = 0, \cdots, m$$

(x_0, y_0)는 위의 다항식들에 대해서 법 N^m에 대해서 해임을 알 수 있다.

위의 다항식들의 x, y대신에 Xx, Yy를 대입하여 그들의 계수들로 이루어진 행벡터들을 만든다. 이러한 행벡터들로 이루어진 격자(Lattice), L에서 가장 짧은 벡터를 찾는다. Minkowski에 의하면 노름의 크기가 $\sqrt{n}(detL)^{1/n}$보다 작은 벡터가 존재한다고 한다. n은 격자 L의 차원이다. 그러한 벡터를 찾기 위해서 LLL 알고리즘을 이용하는데 Minkowski 보다는 다소 크지만 $2^{n/2}(detL)^{1/n}$보다 작거나 같은 벡터를 다항식 시간 안에 찾을 수 있다. 두 변수 다항식의 해를 구하기 위해서는 또 다른 다항식이 필요한데 이때 두 번째로 짧은 벡터를 찾는다. 크기가 $2^{n/2}(detL)^{1/(n-1)}$보다 작거나 같은 두 번째로 짧은 벡터를 찾을 수 있다. $2^{n/2}(detL)^{1/n}$과 $2^{n/2}(detL)^{1/(n-1)}$이 모두

$\frac{N^m}{\sqrt{w}}$ 보다 작다면 X, Y를 제거한 이들의 정수 상의 해들 중에는 (x_0, y_0)이 있다는 것을 알 수 있다. 이들로부터 X, Y를 제거한 두 다항식은 (x_0, y_0)을 공통으로 해를 갖고 있기 때문에 resultant를 구하면 그 값이 0이 된다. 이때 resultant는 한 변수 다항식 형태가 되므로 일차 방정식의 해를 구하는 문제가 된다. 여기서 x_0(또는 y_0)를 얻은 후 두 변수 다항식에 대입하여 다시 한 변수 방정식을 얻어서 해를 구하면 된다. 문제는 resultant가 한 변수 다항식이 아니라 0이 나오면 더 이상 진행을 할 수 없다. 즉, 두개의 짧은 벡터들이 $x-y$항을 공통으로 갖는다면 (algebraically independent 하지 못할 경우) resultant는 0이 된다. 그럼에도 불구하고 현재까지 어느 경우에도 0이 나온 적이 없었다. 따라서 이 방법은 heuristic함에도 불구하고 매우 효율적인 방법임을 알 수 있다.

3. 비밀키 크기와 Coppersmith 정리

RSA는 서로 다른 두 소수의 곱을 $N=pq$라 할 때 N에 대한 오일러 함수 값 $\phi(N)$과 서로 소인 임의의 정수 e를 선택하고 $\phi(N)$에 대한 e의 역원, d를 계산한 후 N과 e를 공개키로 하고 d와 p,q를 비밀 키로 하는 공개키 암호체계이다. 그동안 수많은 공격이 있었지만 사용상의 부주의를 제외하고는 아직 안전하다고 간주되고 있다. 여기서 사용상의 부주의란 구현상의 오류를 뜻하는 데 특히 키 생성과정에서 비밀 키의 크기가 작으면 위험에 노출된다고 알려지고 있다. 어느 정도 크기의 비밀 키를 선택하는 것이 안전한 가, 다시 말하면 어느 정도의 비밀 키를 사용하면 공격이 가능한 가에 대한 문제를 해결하는 데에 사용되는 핵심적인 이론이 바로 Coppersmith 정리이다. 물론 1990년에 Wiener[1]가 처음으로 비밀 키의 크기가 너무 작으면 안전하지 않다는 것을 경고하였는데 이때 그는 연분수 이론을 가지고 비밀 키의 크기가 $N^{1/4}$보다 작으면 비밀 키를 찾아 낼 수 있다는 것을 보였다. 그 후 1997년 Coppersmith의 정리가 발표되자 1998년 Boneh, Durfee[4]등이 Coppersmith의 정리를 응용하여 두 변수 합동다항식의 해를 구하는 문제를 이용하여 비밀 키의 크기를 $N^{0.292}$까지 확장하였다. 이러한 결과는 두 소수의 크기가 같고 공개키 e의 크기가 N과 같다는 가정 하에서 얻은 것이다. 따라서 두 소수의 크기가 다르거나 e의 크기가 N과 다르다면 비밀 키의 크기가 다소 작아도 된다고 1999년 Sun, Yang, Laih[5]가 주장하였는데 2000년 Nguyen[6]은 세 변수 합동다항식의 작은 해를 구하는 방법을 이용하여 오히려 두 소수의 크기가 다르면 비밀 키의 크기는 더 커야만 안전하다는 것을 보였다.

구체적인 결과는 아래 표와 같다.

$\log_N(p)$ \ $\log_N(e)$	1.0	0.9	0.86	0.8	0.7	0.6	0.55
0.5	0.284	0.323	0.339	0.363	0.406	0.451	0.475
0.4	0.296	0.334	0.350	0.374	0.415	0.460	0.483_{II}
0.3	0.334	0.369	0.384	0.406	0.446	0.487	0.510
0.25	0.364_{I}	0.398	0.412_{III}	0.433	0.471	0.511	0.532
0.2	0.406	0.437	0.450	0.470	0.505	0.542	0.562
0.1	0.539	0.563	0.573	0.588	0.615	0.644	0.659

이와 같이 비밀 키의 크기가 너무 작으면 위험에 노출된다는 것을 알았지만 비밀 키의 크기가 너무 크면 복호화 과정이나 전자 서명 등에서 효율성이 떨어진다. 따라서 이러한 문제를 해결하기 위해서 Wiener는 중국인의 나머지 정리를 사용한 해결책을 제안한다. 즉, 각각의 소수에 대하여 작은 비밀 키를 선택한 후에 이들을 중국인의 나머지 정리를 이용하여 법 N에 대한 비밀 키 d를 구한다면 더 이상 비밀 키 d는 작은 값이 아니다. 또한, 중국인의 나머지 정리를 계산하는 것은 매우 빠르기 때문에 효율성과 안전성을 동시에 만족할 수가 있다. 그렇다면 각각의 소수에 대한 비밀 키는 얼마나 작게 하여도 안전한 가에 대해서 사람들은 관심을 갖게 되었다. 두 소수의 크기가 같고 공개키 e의 크기가 N과 같다는 가정 하에서 2002년까지 비밀 키를 찾아내는 가장 잘 알려져 있는 알고리즘은 $\mathcal{O}(\min\sqrt{d_p},\sqrt{d_q})$의 시간이 걸렸다. 2002년 May[7]가 처음으로 다항식 시간 안에 비밀 키를 찾아내는 방법을 제안하였는데 이는 두 소수의 크기가 다른 경우에만 가능하였다. 작은 소수의 크기를 $q < N^{\beta}$라 하면 비밀 키 d_q는 $Z^*_{(q-1)/2}$상의 임의의 수를 선택하고 비밀 키 d_p는 Z^*_{p-1}상의 작은 수를 선택한 후 중국인의 나머지 정리를 이용하여 비밀 키 d를 구한다. May는 두 가지 방법을 이용하는 데 두 변수 합동방정식의 해를 구함에 있어서 $ed_p \equiv 1 \bmod p-1$의 관계를 법 p에 관해서 또 법 e에 관한 두 개의 방정식을 설정한다. 법 p에 관한 방정식 $f(x,y) \equiv ex - y$의 해를 구하는 방법은 Coppersmith와 마찬가지로 격자이론을 이용하여 가장 짧은 벡터를 찾아낸다. 가장 짧은 벡터로부터 여러 관계를 이용하여 직접 해를 찾아낸다. 즉 확정적인 (deterministic) 해를 얻는다. 반면에 법 e에 관한 방정식 $f(x,y) \equiv x(N-y) - N$은 가장 짧은 벡터와 두 번째로 짧은 벡터를 찾아내어 resultant를 구한다. 이러한 resultant의 값은 한 변수 방정식이 되므로 해를 쉽게 구할 수 있다. 이로부터 나머지 변수에 대한 해를 구하게 된다. 그러나 짧은 두 벡터가 공통의 해를 갖게 되면 resultant의 값이 0이 되므로 해를 구할 수 없게 된다. 그럼에도 불구하고 현재까지 이러한 방법을 이용한 어떠한 경우도 0이 나오지 않았다. 따라서 매우 유용하게 사용되고 있으나 아직까지는 heuristic하다. 법 p에 관해서 β는 최대 0.382까지 가능하였고 법 e에 관해서는 3/8까지 가능하였다. 비록 법 p에 관해서 구한 값이 법 e에 관한 것보다 다소 큰 값을 얻었지만 같은 크기의 소수 q에 대해서

는 법 e에 관한 방법이 더 큰 비밀 키 d_q를 찾아 낼 수 있었다. 비밀 키 d_q의 크기를 $d_p < N^{\delta}$라 할 때 구체적으로 β와 δ의 관계는 다음과 같다. 법 p에 관해서는 $3\beta - \beta^2 + 2\delta \leq 1 - \varepsilon$(여기서 ε는 임의의 작은 수), 법 e에 관해서는 $\frac{2}{3}(\beta + \sqrt{3\beta + \beta^2}) + \delta \leq 1 - \varepsilon$를 얻는다. 이후 2006년 May[8]가 다시 이를 확장하는데 β를 최대 0.468까지 가능함을 보였다. 이는 머지않은 장래에 두 소수의 크기가 같을 때에도 다항식 시간 안에 비밀 키를 찾아낼 수 있다는 희망을 갖게 한다. May는 예전과 마찬가지로 법 e에 관한 방정식을 이용하여 해를 구하는데 다른 점은 세 변수 합동다항식을 이용하여 범위를 확장하였다. 구체적인 관계는 다음과 같다.

$$\delta \leq \frac{1}{3}(3 - 2\beta - \beta^2 - \sqrt{12\alpha\beta - 12\alpha\beta^2 + 4\beta^2 - 5\beta^3 + \beta^4}) - \varepsilon$$

(여기서 α란 $e = N^{\alpha}$.)

위에서 언급한 May의 3가지 서로 다른 방법들의 결과를 그래프로 표현하면 아래와 같다.

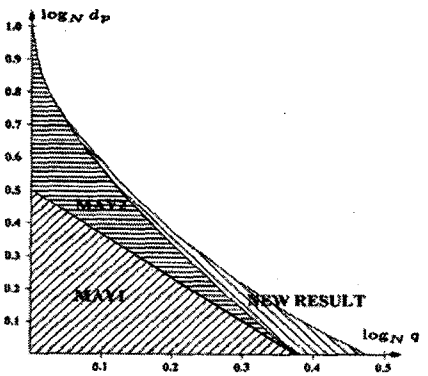

Fig. 1. The attacks of [10] in comparison with the new approach

May는 동시에 두 소수의 크기가 같을 때 일부 다항식 시간 안에 해를 찾았다. e가 N에 비해서 상당히 작고 $d_p, d_q \leq \min\left\{\left(\frac{N}{e}\right)^{\frac{2}{5}}, N^{\frac{1}{4}}\right\}$을 만족하면 다항식 시간 안에 해를 찾을 수 있음을 보였다. 그러나 이 방법은 Coppersmith의 정리를 이용한 기존의 방법이 아니다.

4. 일부 키 노출과 Coppersmith 정리

RSA는 Diffie-Hellman 키 교환이나 ElGamal 암호체계와 같은 이산대수문제에 기

반을 둔 암호체계와 달리 일부 키가 노출이 되면 키가 복원될 수 있는 취약점을 갖고 있다. 따라서 어느 정도의 노출이 위험한 가에 대한 연구가 활발히 진행되고 있는데 이러한 연구의 핵심이 되는 이론도 Coppersmith 정리이다. 1998년 Boneh, Durfee, Frankel[9]이 비밀 키의 일부 노출로 N을 소인수분해 하는 방법을 발표하였다. 물론 모든 경우는 아니고 각각의 제한이 있다. 여기서 일부 노출이란 아무 곳이나 일부를 듬성듬성 알아서 되는 것은 아니고 연속적으로 the most significants(MSB)나 the least significants(LSB)를 일부 알았을 때만이 가능하다. 그들의 결과를 요약해 보면 다음과 같다.

① $N\equiv 3 \bmod 4$이고 $e<2^{(n/4)-3}$일 때 비밀키 d의 $n/4$ LSBs 가 주어지면 n과 e에 대한 다항식 시간 안에 전체 d를 찾아낼 수 있다.(N의 비트수를 n라 하자.)

② e가 소수이고 $\{2^t,\cdots,2^{t+1}\}$안의 임의의 크기를 가질 때($n/4\le t\le n/2$), d의 t MSBs이 주어지면 n에 대한 다항식 시간 안에 d를 찾을 수 있다.

③ e가 $\{2^t,\cdots,2^{t+1}\}$안의 수이고 최대 r개의 서로 다른 소수들의 곱으로 표시된다면 e의 소인수분해와 d의 t MSBs이 알려졌을 때 n과 2^r에 대한 다항식 시간 안에 d를 찾을 수 있다.($n/4\le t\le n/2$)

④ e의 소인수분해를 알지 못할 때 그리고 e가 $\{2^t,\cdots,2^{t+1}\}$안에 있을 때 ($t\in 0,\cdots,n/2$) 그리고 $d>\varepsilon N$ 이면($\varepsilon>0$) 주어진 d의 $n-t$ MSBs 으로부터 n과 $1/\varepsilon$에 대한 다항식 시간 안에 d를 찾을 수 있다.

위의 결과들은 Coppersmith의 따름 정리를 이용하여 얻을 수 있다. e의 크기가 작을 때 공개된 N과 e 그리고 d_0의 관계식으로부터 k에 대한 임의의 값 k을 대입하여 p에 대한 $2^{n/4}$ LSBs을 찾아낸다. 그 후 따름 정리에 의하여 N을 소인수분해 한다. 그러면 자동적으로 d를 찾을 수 있다. e가 중간 정도의 크기를 가질 때에는 MSBs의 노출에 대해서 공격이 가능한 데 e의 형태에 따라서 공격방법이 다르다. e가 소수거나 소인수분해를 알 경우는 법 e에 대한 이차 방정식의 해가 소수 p이므로 e의 크기가 $2^{n/4}$보다 크거나 같기만 하면 Coppersmith의 따름 정리를 활용할 수 있다.

2003년 Blömer와 May[10]는 "New Partial Key Exposure Attacks on RSA"란 논문에서 Boneh, Durfee, Frankel의 결과를 확장한다. BDF는 e의 크기가 $N^{1/2}$가지 가능하였으나 이들은 MSBs 경우 e가 $[N^{1/2},N^{0.725}]$까지, LSBs의 경우 $e<N^{7/8}$까지 공격이 가능한 다항식 시간의 알고리즘을 제안한다. MSBs 경우 e의 크기가 커질수록 d의 비트수도 더 많이 알아야지만 공격이 가능하다. Blömer와 May는 BDF가 Coppersmith의 따름 정리를 이용한 것과는 달리 Coppersmith의 정리 1을 세 변수 합동다항식의 경우로 바꾸어서 증명한다. 물론 결과는 heuristic하다. LSBs의 경우는 아

주 작은 경우를 제외한 $e<N^{1/2}$까지는 증명이 가능한 방법으로 N을 소인수분해 하고 모든 $e<N^{7/8}$에 대해서는 Coppersmith의 다변수 합동다항식을 이용하여 다항식 시간 안에 N을 소인수분해 한다. 이 경우 heuristic하지만 더 좋은 결과를 얻었다. 이 외에도 중국인의 나머지 정리를 이용하여 비밀 키를 생성한 경우 d_p의 비트수가 어느 정도 노출이 되면 공격이 가능한 지를 보였다. 이때 두 소수의 크기는 같다고 간주하였다. 2006년 Lee, Park, Kwon[11]은 두 소수의 크기가 다른 법 N에 대해서 중국인의 나머지 정리를 사용한다면 어느 정도의 비트수가 노출되면 공격에 가능한 지를 살펴보았다. 상세한 결과는 아래의 표에 나타나 있다.([9],[10].[11] 참조)

	$\alpha=\log_N(e)$	필요로 하는 비트수	비고
BDF	$[\frac{1}{4},\frac{1}{2}]$	α	e소수 또는 소인수분해가 알려짐
BDF	$[0,\frac{1}{2}]$	$1-\alpha$	$\frac{d}{\phi(N)}=\Omega(1)$
May,Blömer	$[\frac{1}{2},\frac{\sqrt{6}-1}{2}]$	$\frac{1}{8}(3+2\alpha+\sqrt{36\alpha^2+12\alpha-15})$	heuristic
BDF	$[0,\frac{1}{2}]$	$\frac{3}{4}$	$\frac{d}{\phi(N)},\frac{p-q}{\sqrt{N}}=\Omega(1)$
May,Blömer	$[0,\frac{1}{4}]$	$\frac{1}{4}+\alpha$	d_p의 비트수
LPK	$[0,\frac{1}{4}]$	$\frac{1}{4}+\alpha$	$q\ll p$
BDF	$\delta(\log_N\log N)$	$\frac{1}{4}$	$N\equiv 3 \bmod 4$
May,Blömer	$[0,\frac{1}{2}]$	$\frac{1}{2}+\alpha$	$\delta(N^{\alpha-\varepsilon})$를 제외한 모든 e
May,Blömer	$[0,\frac{7}{8}]$	$\frac{1}{6}+\frac{1}{3}\sqrt{1+6\alpha}$	heuristic
May,Blömer	$\delta(\log_N\log N)$	$\frac{1}{4}$	d_p의 비트수
LPK	$\delta(\log_N\log N)$	$\frac{n}{4}+s'$	$q\ll p,\ e-1=2^{s'}t$

5. 결론

1990년 Wiener가 RSA에서의 작은 비밀 키의 위험을 지적한 이래 현재까지 비밀 키와 관련된 RSA 안전성 분석에 관하여 살펴보았다. 이러한 안전성 분석은 결국 Coppersmith의 연구 결과에 의해서 가능한 것이었다. Wiener의 연분수를 이용한 결

과도 Coppersmith의 두 변수 합동방정식의 해를 구할 때 소위 "x-shift"만을 사용하여서 나온 결과와 일치 하였다. Boneh, Durfee및 Nguyen의 결과들도 두 변수 혹은 세 변수의 합동방정식의 해를 구함으로써 얻은 것들이다. May가 제안한 중국인의 나머지 정리를 이용한 RSA의 비밀 키를 찾는 공격에서도 세 변수 합동방정식의 해를 구하는 것이 두 변수 합동방정식의 해를 구하는 것, 또는 결정적인(deterministic) 방법으로 해를 구하는 것보다 더 나은 결과를 얻을 수 있었다. 다른 주의 깊게 살펴볼 점은, 일부 키 노출에 따른 전체 키 복원에 관한 공격들도 두 변수 다항식의 해를 구하는 것보다 세 변수 합동다항식의 해를 구하는 것이 더 나은 결과를 가져옴을 알 수 있었다. 현재까지의 연구 결과를 보아서는 한 변수 보다는 두 변수, 두 변수보다는 세 변수 합동방정식의 해를 구하는 것이 더 나은 결과를 얻을 수 있음을 알 수 있었고 두 변수 다항식의 해를 구하는 것보다는 다변수 합동방정식을 이용하는 것이 더 나은 결과를 얻을 수 있다는 것을 알 수 있었다. 따라서 향후 암호학적 응용에 있어서 Coppersmith 정리에 기반을 둔 다변수 합동방정식의 해를 찾는 문제로 변환할 수 있다면 좋은 결과를 얻을 수 있으리라 기대된다. 최근에도(2006년) May는 기존에 존재하고 있는 다양한 형태의 RSA에서 이러한 다변수 합동방정식의 활용을 시도하고 있다.

참고 문헌

1. M. Wiener, "Cryptanalysis of short RSA secret exponents", IEEE Transactions on Infor. Th, Vol.36, No.3, 553-558(1990).
2. Don Coppersmith, "Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities", J. of Cryptology, Vol. 10, 233-260(1997).
3. N.Howgrave-Graham, "Finding small roots of univariate modular equations revisited", Proc. of Cryptography and Coding, LNCS 1355, Springer- Verlag, 131-142(1997).
4. D. Boneh, G. Durfee, "Cryptanalysis of RSA with private key d less than $N^{0.292}$", IEEE Transactions on Information Theory Vol.46(4), 1339-1349(2000).
5. Sun, Yang Laih, "ON the design of RSA with short secret exponent", In proc. of Asiacrypt'99, LNCS vol. 1716, IACR, Springer-Verlag, 150-164(1999).
6. G. Durfee, P. Nguyen, "Cryptanalysis of the RSA schemes with short Secret Exponent from Asiacrypt'99", Proc. of Asiacrypt 2000, LNCS vol.1976, Springer, 14-29(2000).
7. Alexander May, "Cryptanalysis of Unbalanced RSA with small CRT-exponent", Crypto 2002, LNCS 2442, 242-256(2002).