KJHM Vol. 16, No. 3, 2003, 101-108

RSA에 사용된 파라메터들에 관한 고찰*

강남대학교 응용수학 전공 **이희정**

Abstract

The RSA cryptosystem is most commonly used for providing privacy and ensuring authenticity of digital data. This system is based on the difficulty of integer factoring. Many attacks had been done, but none of them devastating. They mostly illustrate the dangers of improper use of RSA. Improper use implies many aspects, but here we imply the misuse of the parameters of RSA. Specially, sizes of parameters give strong effects on the efficiency and the security of the system. Parameters are also related each other. We analyze the relation of them. Recently many researchers are interested in side-channel attacks. We also investigate partial key exposure attacks, which was motivated by side-channel attacks. If a fraction of the secret key bits is revealed, the private key will be reconstructed. We also study mathematical background of these attacks, solving modular multivariate polynomial equations.

0. 서론

1977년 Ron Rivest, Adi Sharmir, Len Adelman에 의해서 처음으로 제안된 RSA 공개키 암호시스템은 전자 데이터의 비밀성과 인증을 위하여 오늘날 가장 널리 사용되고 있는 암호 시스템이다. 1977년 이후 계속적으로 이 시스템을 공격하였으나 오늘날까지는 성공하지 못하였다. 단지 구현상 키(파라메터)들을 사용함에 주의를 기울이지 않으면 위험하다는 것이 지적되었다[1]. 특히 시스템에 사용되는 키들의 크기에 관하여 연구가 많이 되고 있는데 RSA시스템에 사용되는 키에는 두 개의 소수 p와 q 그리고 그들의 곱 N, N과 서로 소인 e 및 법 $\phi(N)$(오일러 함수 값)에 대한 e의 역원 d가 있다. 이때, N과 e는 공개되고 d 와 p, q는 비밀키로 간직된다. 키들의 크기는 시스템의 안전성과 효율성에 영향을 주는데, 이들은 서로 밀접한 관계를 갖고 있다. 시스템에 사용된 두 소수의 곱의 크기는 1024비트 정도이면 소인수분해에 안전하다고 생각되었으나 최근에는 이것도 안전하지 못하다는 것이 증명되었

* 본 연구는 2003년 강남대학교 교내 연구비에 의해서 수행되었습니다.

다. 본 논문에서는 N을 직접 소인수분해를 하여 공격을 하는 것에 관해서는 언급하지 않고 주어진 N과 e로부터 비밀 키 d 또는 소수를 찾아내려는 공격에 초점을 맞추려고 한다. 이때, N의 크기는 대략 1024비트 정도를 사용한다고 가정한다. 그리고 효율성을 높이기 위해서 복호화 하는 과정에서 보통 중국인의 나머지 정리를 사용하는 데 이러한 경우에도 두 소수의 크기가 어느 정도여야 안전한지를 알아본다. side channel attack 등 어떠한 이유에서든 비밀키가 일부 노출 됐을 때 비밀 키 전부가 복원되는 경우를 살펴보려고 한다. 이러한 공격은 이산 대수 문제에 근거한 암호체계에서는 가능하지 않으나 RSA 암호체계에서는 가능하다. 이 경우 또한 공개키의 크기와 관계가 있다. 그리고 파라메터들의 크기에 따른 공격법이나 일부 비밀 키 노출에 따른 공격 모두, multivariate modular equation(다변수 합동방정식)의 해를 구하는 문제로 귀결된다. 따라서 공개키 N과 e가 주어졌을 때 비밀 키 d나 소수를 찾는 경우 또는 비밀키의 일부가 노출되었을 때 비밀 키 전부를 복원하는 경우에 사용되어진 multivariate modular equation의 해를 구하는 방법을 소개하려고 한다.

1. RSA에 사용된 파라메터들의 크기에 관한 분석

주어진 소수의 크기에 따라 공개 키 e의 크기와 비밀 키 d의 크기가 효율성과 안전성에 영향을 주는데 공개키 e의 크기가 크면 사용자 입장에서 효율성이 떨어지게 되므로 작은 e를 사용하려고 한다. 예전에는 $e=3$을 썼으나 이는 공격에 취약하여 요즘은 보통 $2^{16}+1$을 사용한다. 비밀 키 d의 크기는 복호화 하거나 전자서명을 하는데 사용되므로 이것도 크기가 작을수록 효율적이다. 그러나 이것이 너무 작으면 또한 공격에 취약하다. 최초로 1990년 Wiener[2]는 두 소수의 크기가 같다고(비트 수의 크기) 가정했을 때 비밀 키 d가 $N^{0.25}$보다 작으면 N이 소인수 분해됨을 보였다. 그러나 만약 공개키 e가 $N^{1.5}$보다 크면 이러한 공격이 가능하지 않다. 이후 비밀 키 d와 공개키 e의 크기에 관하여 더욱 관심을 갖게 되었는데, Verhol과 Tilbog[3]는 d의 크기가 $N^{0.5}$보다 작으면 N이 소인수 분해됨을 보였다. 그러나 그들의 알고리즘은 exponential time이 걸리기 때문에 실질적이지 못했다. 1998년 Boneh와 Durfee[4]는 다항식 시간내의 알고리즘을 내놓았는데 그들에 의하면 두 소수의 크기가 같고 공개키 e의 크기가 N과 같을 때 비밀 키 d가 $N^{0.292}$보다 작으면 공격이 가능하다고 한다. 이때 e의 크기가 $N^{15/8}$보다 크면 이러한 공격이 가능하지 않다는 것도 보였다. 또한 이들은 e의 N에 대한 크기의 변화에 따라 공격 가능한 d의 크기를 분석해 놓았다.

$[d=N^{\delta},\ \delta<\frac{7}{6}-\frac{1}{3}(1+6\alpha)^{1/2}]$.

1999년 Sun, Yang, Laih[5]는 두 소수의 크기가 다르다면 비밀키의 크기가 Wiener와 Boneh의 bound보다 작더라도 그들의 공격방법에 안전한 구현 법을 3가지 형태로 제안하였다. 2000년 Nguyen[6]은 두 소수의 크기가 같거나(balanced) 혹은 다르더라도(unbalanced) N에 대한 e의 크기에 따라 비밀 키 d의 크기가 어느 정도까지 여야 안전한지를 분석해 놓

았다. 그는 Sun, Yang, Laih가 제안한 3가지 형태의 알고리즘 중에서 2가지는 안전하지 못함을 증명하였으나 나머지 한 방법은 공격에 성공하지 못하였다. 이후 Hong, Lee, Lee, Lee[7]가 Nguyen보다는 조금 향상 시켰으나 역시 공격에 성공하지는 못하였다.

지금까지의 분석은 비밀 키 d의 크기가 e의 크기에 따라 어느 정도여야 안전한가를 설명하였는데 d의 크기를 작게 하고도 즉 효율성을 유지하면서도 안전한 방법을 소개하려고 한다. Wiener[2]가 처음으로 중국인의 나머지 정리를 이용하여 위의 공격을 막는 방법을 제안했다. 즉, 법 $\phi(N)$에 대한 e의 역원 d를 구하는 대신에 법 $p-1$에 대한 e의 역원 $d_p \equiv d$를 구하고 동시에 법 $q-1$에 대한 e의 역원 $d_q \equiv d$를 구한 후 중국인의 나머지 정리에 의해서 법 $\phi(N)=(p-1)(q-1)$에 대한 e의 역원 d를 찾는다. 이때 d_p나 d_q는 작지만 중국인의 나머지 정리에 의해서 구해진 d의 크기는 더 이상 작지 않다. 따라서 효율성은 유지되면서 공격에 안전하다. 2002년 May[8]는 설사 이러한 중국인의 나머지 정리를 이용하여 비밀키 d를 선택한다고 하더라도 만약 두 소수의 크기에 대한 차이가 크면(unbalanced), 즉 작은 소수의 크기가 $N^{0.382}$보다 크지 않으면 공격에 취약함을 보였다.

2. 비밀 키 일부가 노출되었을 때

위와 같은 분석에 의해서 비밀키를 선택하였다 하여도 이것들을 보관하는 데에는 상당한 주의가 요망된다. 이때 어떠한 이유에서든 비밀키의 일부 정보가 유출된다면 이것도 공격에 노출될 수가 있다. Boneh[9] 등이 side channel attack을 연구하면서 어느 정도의 비밀키 d 정보가 어느 부분에서 노출되었을 때 d를 복원시킬 수 있는지를 연구하였다. 공개키 e의 크기가 작을 때 d 크기의 $\frac{1}{4}$정도만 노출이 되면 d를 복원할 수 있다고 하였다. e의 크기가 큰 경우도 연구해 놓았다. 여기서 e의 크기가 크다는 것은 e가 $N^{1/2}$보다는 작은 경우를 말한다. 자세한 내용은 아래에서 설명하도록 한다.

또한 특별히 스마트카드와 같은 용량이 작은 장치에 전자서명과 같은 역할을 수행하려고 하면 비밀 키 d를 적재하여야 하는데 수행 능력을 빠르게 하기 위해서 보통 중국인의 나머지 정리를 이용하여 전자서명 또는 복호화 한다. 이런 때에도 비밀 키 d_p의 부분 정보가 유출되면 위험하다는 것을 May[10]가 지적하였다. 또한 그는 Boneh[9]의 연구 결과를 확장했는데 공개키 e의 크기가 Boneh의 bound보다 더 커도 공격이 가능함을 보였고 비밀키의 노출 양이 더 작더라도 공격이 가능함을 보였다. 이에 대한 구체적인 내용은 다음과 같다.

2.1. 공개키 e의 크기가 작을 때

공격자가 비밀키의 일부를 알게 되면 공개키 e의 크기가 작을 때 비밀 키 전부를 복원할 수 있다. 비밀키의 비트 수를 n이라 하면 $n/4$정도의 비트만 알면,(여기서 $n/4$ 정도의 크

기란 least significant bit들의 크기를 말한다) 전부를 복원할 수 있다. 그 뿐만이 아니라 알려진 비트들의 위치가 $n/4$에서 $n/2$일 때도 비밀키를 전부 복원할 수 있다. 그러나 임의의 위치에 있는 $n/4$ 크기의 비트들을 알 때에는 아직 복원할 수 없다. 이것은 앞으로 연구되어져야 할 과제이다. 대략적인 공격방법은 다음과 같다.

Coppersmith[11, 12]는 LLL lattice reduction 알고리즘을 이용하여 두 변수 합동 방정식의 해를 적당한 한계 범위 안에서 구하였다. Coppersmith의 방법을 이용하여 RSA에 사용된 두 소수 중에서 하나가 반 정도의 비트들에 노출되었다면 합성수 N을 인수분해 할 수 있음이 증명되었는데 비밀키의 일부 노출에 따른 비밀 키 복원도 위의 결과들을 이용한다. 즉, $n/4$ 정도의 least significant bit들을 알았을 때 $ed_0 \equiv 1+k(N-x-N/x+1) \bmod 2^{n/4}$의 관계식을 얻게 된다($d \equiv d_0 \bmod 2^{n/4}$). 이때, k는 e보다 작으므로 k를 추측해서 대입하고 방정식을 간단히 하면 $N \equiv 3$ 법 4, 그리고 e의 크기가 $2^{(n/4)\ 3}$보다 크지 않을 때 N을 소인수분해 할 수 있다. $N \equiv 1$ 법 4일 때는 다소 복잡하다. R. Steinfeld와 Y. Zheng가 위의 경우를 다소 변경하여 공격하는 것을 보여줬다. 동시에 이러한 공격에 대응하기 위해서는 큰 u에 대해서 $p \equiv q$ 법 2^u을 만족하는 두 소수를 선택할 것을 권유했다.

여기서 비밀 키 d의 most significant bits을 어느 정도 알면 공격이 가능할까 하는 생각을 할 수 있는데 그것은 불가능하다. 왜냐하면 공개키의 크기가 작을 때에는 공격자는 주어진 N과 e로부터 반 정도의 most significant bits을 알 수 있다. 따라서 이러한 사실이 공격자가 d의 나머지 반을 알아내는 데에 아무런 도움을 주지 않는다. 다시 말해서 비밀 키 d의 반 정도의 most significant bits을 알았을 때 전체 d를 찾을 수 있는 알고리즘이 있다면 이것은 RSA를 깰 수 있는 알고리즘이 존재하는 것과 같다.

2.2. 공개키 e의 크기가 적당히 클 때($e < \sqrt{N}$)

e의 범위가 2^t에서 2^{t+1}일 때(t는 {0, ···, $n/2$}) 비밀키를 찾기 위해서는 위의 경우와 달리 most significant bits을 알아야 한다. e가 커져서 위와 마찬가지로 k를 brute force로 찾기는 불가능하다. 그러나 e가 $\sqrt{N}$보다 작을 때 $\log_2 e$ 정도의 d에 대한 most significant bits를 알면 k를 찾을 수 있다는 것을 보인다. 그러면 e가 소수일 때 또는 e의 소인수분해를 알 때에는 d의 t most significant bits만을 알면 N을 소인수분해 할 수 있다. e의 소인수분해를 알 수 없을 때에는 k가 $\varepsilon \cdot e$보다 크다고 가정하면($\varepsilon > 0$)) n-t most significant bits의 d를 알면 모든 d를 복원하는 알고리즘이 있다.

2.3. e의 크기가 $\sqrt{N}$보다 클 때(May의 확장)

May[10]는 Boneh 등이 해결하지 못했던 e가 큰 경우 비밀키를 복원하는 데 성공했는데, 공개 키 e의 크기가 $\sqrt{N}$보다 클 때 비밀키의 most significant bits 또는 least significant bits를 알면 공격이 가능함을 보였다. most significant bits를 알 때는 e의 크기가 [$N^{0.5}$,

$N^{0.725}$] 범위에서 공격하는 알고리즘을 제안하였고 least significant bits 을 알았을 때는 e의 크기가 좀 더 나은 $N^{7/8}$까지 공격이 가능하다는 것을 보였다. 또한 May는 빠른 RSA 암호 체계인 중국인의 나머지 정리를 이용한 비밀 키 설정(복호화 과정에서)을 하여도 작은 공개 키를 사용하면 법 $p-1$에 대한 반정도의 비밀키의 유출로 N이 소인수분해 될 수 있음을 보였다.

3. Modular Equation(합동 방정식)의 해를 구하는 방법

Coppersmith[11, 12]는 univariate modular equation이 주어졌을 때 '작은' 해를 구하는 방법을 보여주었다. 이때 '작은' 해란 다항식의 차수를 d라 하고 합동식의 법을 N이라 할 때 $N^{1/d}$보다 작은 경우를 말한다. 그러나 bivariate(multivariate) modular equation일 경우는 heuristic하게 밖에는 해를 구할 수 없다. 자세한 내용은 다음과 같다.

다항식 $f(x)$의 노름(norm)을 계수들의 제곱의 합들의 제곱근이라고 하자.

($f(x)=\sum_{i=0}^{n} a_i x^i$일 때 $\| f(x) \| = \sqrt{\sum a_i^2}$.)

Howgrave-Graham[13]은 임의의 크기 X보다 작은 x_0이 합동다항식 $f(x)\equiv 0 \bmod N$의 해가 될 때 $\| f(xX) \| < N/\sqrt{d}$를 만족하면, 다항식 $f(x)$는 정수상의 해, x_0을 갖는다는 것을 증명하였다. 따라서 합동 방정식의 해는 다항식의 노름이 작을 때 이를 정수상의 방정식으로 간주하여 해들을 구한 후 그들 중에서 작은 해를 찾을 수 있다. 문제는 모든 다항식이 원하는 크기의 값을 대입했을 때 노름이 주어진 조건만큼 작지 않다는 것이다. 이것을 해결하기 위해서 주어진 다항식과 해, x_0은 공통으로 하면서 노름이 작은 다항식을 찾는다. 즉, $f(x)$, $xf(x)$, $x^2f(x)$, $\cdots$, $x^nf(x)$의 일차결합 형태, $h(x)$로 만들어 노름이 원하는 만큼 작도록 한다. 그러나 이 다항식도 항상 조건을 만족하는 것이 아니다. Coppersmith는 이러한 문제를 해결하기 위해서 $f(x)\equiv 0 \bmod N$을 만족하는 해는 $f^k(x)\equiv 0 \bmod N^k$을 만족한다는 생각을 한다. 여기서 k를 충분히 크게 하면 $\|f^k(xX)\| < N^k/\sqrt{w}$ (w는 다항식 $f^k(x)$의 항의 개수)를 만족시킬 수 있다. 이를 위해서 $f(xX)$의 계수들을 벡터로 하는 lattice를 만든다. Minkovski는 lattice의 가장 짧은 벡터는 $\lambda \det(L)^{1/n}$보다 작다고 하였다. 여기서 n은 lattice의 dimension이고 λ는 상수이다. 그러나 가장 짧은 벡터를 찾는다는 것은 쉽지가 않다. 따라서, LLL 알고리즘을 이용하는데 LLL 알고리즘은 $2^{1/n}\det(L)^{1/n}$보다 작은 벡터를 찾을 수 있다. 이때, $2^{1/n}\det(L)^{1/n}$이 $N^k/\sqrt{w}$보다 작으면 정수상의 다항식으로 생각하여 해를 구한 후 주어진 범위 안의 해를 찾을 수 있다. 따라서 univariate인 경우는 확정적(deterministic)으로 작은 해를 구할 수 있다. bivariate 경우는 마찬가지로 두 변수 x와 y에 대한 X와 Y의 범위를 정한 후 $f(xX, yY)$의 노름이 $N/\sqrt{w}$보다 작으면 $f(x, y)$의 정수상의 해 중에서 X, Y보다 작은 것들을 두 변수 합동 방정식의 해로 구하면 된다. univariate 경우와 마찬가지로

k를 충분히 크게 하여 노름이 조건을 만족하도록 하기 위해서 lattice를 만든다. 이때, 생성자로 소위 'x shifted $f(x, y)$' 또는 'y shifted $f(x, y)$' 형태를 이용한다.

($g_{i,j}(x, y)=N^{m-j}x^i f^j(x, y)$, $h_{i,j}(x, y)=N^{m-j}y^i f^j(x, y)$)

생성된 lattice에서 가장 짧은 벡터를 찾기 위해서 LLL 알고리즘을 이용한다. 그런데 여기서 univariate과 다른 점은 변수가 두 개 이상이기 때문에 가장 짧은 벡터 하나 가지고는 해를 찾을 수 없다 (물론 May는 다항식이 가지고 있는 특성을 살펴서 해를 찾아냈는데 이때는 가장 짧은 벡터 하나만으로도 가능했다. 그러나 이러한 방법은 아주 특별한 경우에만 가능하다.) lattice의 successive minima에 의해서 두 번째로 짧은 벡터를 찾을 수 있는데 마찬가지로 LLL 알고리즘에 의해서 가장 짧은 그리고 두 번째로 짧은 벡터를 찾을 수 있다. (λ_1, $\lambda_2 < 2^{1/(n-1)}\det(L)^{1/(n-1)}$) 따라서 $2^{1/(n-1)}\det(L)^{1/(n-1)}$이 $N^k/\sqrt{w}$ 보다 작으면 그 조건하에서는 정수 상의 다항식의 작은 해가 합동다항식의 해가 된다. 해의 범위인 X, Y 등의 크기나 생성자의 형태, lattice의 크기(dimension), n, 그리고 법(mod) N^k에서 k의 크기 등의 관계에 대해서는 구체적으로 살펴봄으로써 공격 가능한 범위를 알 수 있다. 여기서는 생략한다.

이렇게 찾은 두 개의 벡터들로부터 연립방정식을 얻는다. x 혹은 y의 한 변수에 대한 이들의 resultant를 구하면 두 방정식은 같은 해를 가지므로 그 resultant의 값은 0이 된다. 따라서 한 변수에 대한 방정식의 해를 구한 후 두 변수 방정식에 대입하여 나머지 변수에 대한 해를 구할 수 있다. 여기서 문제는 두 개의 벡터로부터 얻은 다항식들이 과연 공통의 일차인수를 갖지 않는가 하는 문제다. 다시 말해서 이들이 algebraically independent하는가 인데 현재까지는 이를 증명을 하지 못했다. 단지 heuristically 모든 것이 잘 해결된다는 것이다. 즉, 현재까지 한번도 0이 나온 경우가 없었다.

4. 결론

지금까지의 연구 결과를 살펴보면 e에 의한 d를 임의로 선택할 때는 물론이고 중국인의 나머지 정리를 사용하여 비밀키를 선택하더라도 두 소수의 크기 차이가 크면 클수록 공격에 안전하지 못함을 알 수 있었다. 중국인의 나머지 정리를 사용하지 않고 복호화 할 경우는 공개키 e를 대략 N과 크기가 같을 때 비밀키가 $N^{0.292}$보다 크면 안전하다. 또 중국인의 나머지 정리를 사용할 경우에는 작은 소수의 크기가 $N^{0.382}$보다 작으면 위험하다. 따라서 두 소수의 크기가 거의 같고 중국인의 나머지 정리를 이용하여 비밀키를 찾는다면 현재까지는 가장 안전하고 효율적인 RSA 암호시스템이 될 것이다.

side channel 공격에 의해서 혹은 어떤 이유에서건 비밀 키 d가 일부 노출되었을 때 공개키 e가 $N^{7/8}$보다 작으면 위험하다는 것을 알 수 있다. 물론 노출된 비밀키의 비트들은

연속적 이여야 만 가능하지 부분부분 알려져서는 복원이 가능하지 않다. 결론적으로 비밀키가 N의 $\frac{1}{4}$ 양만큼의 비트들이 연속적으로 알려지면 e가 아주 크지 않는 한 공격에 취약하다.

May 이전까지는 공개키 e와 비밀키 d의 크기를 분석할 때 modular multivariate polyno- mial equation(다 변수 합동방정식)의 해를 heuristic하게만 구할 수 있었다. 그러나 May는 일부 노출된 비밀키의 비트들을 가지고 전체를 복원하는데 deterministic한 방법으로 구한다. 따라서 주어진 조건에 따라서 다 변수 합동방정식의 해를 확정적으로 구할 수도 있음을 알아보았다. 또한, May가 사용한 합동다항식을 보면 다항식의 형태에 따라 helper polyno- mial을 얻지 못하는 경우가 있음을 보았다. 다변수 합동방정식의 해를 구하기 위해서는 lattice를 만드는데 이때 사용되는 생성자의 형태에 따라 결과가 다르게 나온다. 이러한 생성자의 해의 범위에 관한 연구, 가장 짧은 두 벡터가 algebraically independent한가에 대한 연구, 또한 이러한 것이 증명 불가능할 경우 연립 고차방정식의 해를 구하는 다른 방법 등에 관한 연구가 더 계속되어야 할 것이다.

참고 문헌

1. Boneh, D., "Twenty years of attacks on the RSA cryptosystem," *Notices of the AMS* 46(2), 203-213, 1999.
2. Wiener, M., "Cryptanalysis of short RSA secret exponents," *IEEE Transaction on Info. Th.* Vol. 36, No. 3, pp. 553-558, 1990.
3. Verhol, E., van Tilborg, H., "Cryptanalysis of less short RSA secret exponents," *Applicable Algebra in Engineering, Communication and Computing*, Springer-Verlag, Vol. 8, pp. 425-435, 1997.
4. Boneh, D., Durfee, G., "Cryptanalysis of RSA with private key d less than $N^{0.292}$," *Proc. of CRYPTO 2002, LNCS 2442*, pp. 242-256, Springer-Verlag, 2002.
5. Sun, H.-M., Yang, W-C., Laih, C.-S., "On the design of RSA with short secret exponent," in *Proc. of Asiacrypt'99, Vol. 1716 of LNCS*, pp. 150-164, IACR, Springer-Verlag, 1999.
6. Durfee, G., Nguyen, P.Q., "Cryptanalysis for the RSA schemes with short secret exponent from Asiacrypt'99," in *Proceedings of Asiacrypt 2000, LNCS, IACR*, Springer-Verlag, 2000.
7. Hong, H.-S., Lee, H.-K., Lee, H.-S., Lee, H.J., "The better bound of private key in RSA with unbalanced primes," *Applied Mathematics and Computation* Vol 139/2-3, pp. 351-362, 2003.

8. May, A., "Cryptanalysis of Unbalanced RSA with Small CRT-Exponent," in *Proc. of CRYPTO 2002, LNCS 2442*, pp. 242-256, Springer-Verlag, 2002.
9. Boneh, Durfee, Frankel, "Exposing an RSA given a small fraction of the private key bits, Asiacrypt98," *LNCS* vol. 1514, Springer-Verlag, pp. 25-34, 1998.
10. May, A., "New Partial Key Exposure Attacks on RSA," in *Proc. of CRYPTO 2003, LNCS*, pp. -, Springer-Verlag, 2003.
11. Coppersmith, D., "Small solutions to polynomial equations and low exponent RSA vulnerabilities," *Journal of Cryptology* vol. 10, pp. 233-260, 1997.
12. Coppersmith, D., "Finding small solutions to small degree polynomials," *IBM research report*, 2001.
13. Howgrave-Graham, N., "Finding small roots of univariate modular equations revisited," in *Proceedings Cryptography and Coding, LNCS*, vol. 1355, Springer-Verlag, pp. 131-142, 1997