Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2010, Article ID 421348, 11 pages
doi:10.1155/2010/421348

Research Article

A New Method of Constructing a Lattice Basis and Its Applications to Cryptanalyse Short Exponent RSA

Mingqiang Wang and Haifeng Zhang

School of Mathemtics, Shandong University, 250100 Jinan, China

Correspondence should be addressed to Mingqiang Wang, mqwang71@hotmail.com

Received 10 December 2009; Accepted 22 February 2010

Academic Editor: J. Jiang

We provide a new method of constructing an optimal lattice. Applying our method to the cryptanalysis of the short exponent RSA, we obtain our results which extend Boneh and Durfee's work. Our attack methods are based on a generalization to multivariate modular polynomial equation. The results illustrate the fact that one should be careful when using RSA key generation process with special parameters.

1. Introduction

The RSA [1] cryptosystem is the most widely used public-key cryptosystem. The modulo N of RSA cryptosystem is the product of two large prime numbers p and q, without loss of generality, we assume that $p < q$. The public exponent e and the secret exponent d satisfy the equation

$$ed \equiv 1 \left(\mathrm{mod}\, \phi(N)\right), \tag{1.1}$$

where $\phi(N) = (p-1)(q-1)$ is Euler's totient function. In a typical RSA cryptosystem, p and q have approximately the same number of bits and $e < N$. The most basic security requirement for public key cryptosystem is that it should be hard to recover the secret key from the public key.

In order to speed up the decryption or signing process, one might be tempted to use small secret exponent. Unfortunately, Wiener [2] showed that if $d < N^{1/4}$, then the factorization of N can be found in polynomial time using only the public information (N, e).

In 1996, Coppersmith [3] introduced two methods for finding small roots of polynomial equations using lattice reduction, where one is for the univariate modular case and the other is for the bivariate case over the integers. Coppersmith's technique has been found many applications for breaking variants of RSA; for example, Boneh and Durfee [4] improved the bound of secret exponent to $d < N^{0.292}$, Coron and May [5] applied Coppersmith's technique to show the deterministic equivalence between recovering the secret exponent d and factoring N, and May [6] presented two polynomial time attacks for the case of imbalanced prime factors p and q.

For a given RSA modulo N, it is not difficult to get a polynomial time algorithm for finding $[\sqrt{N}]$, where $[\sqrt{N}]$ is the integral part of N. Then p and q can be rewritten as $p = [\sqrt{N}] - x_0$ and $q = [\sqrt{N}] + y_0$, where x_0, y_0 are unknown positive integers. Our observation is that the bound of secret exponent d of balanced RSA is related to the bound of $|x_0 - y_0|$. For instance, when p and q are twin prime numbers, that is, $q - p = 2$, then p is a root of the following polynomial:

$$N = x(x + 2). \tag{1.2}$$

Therefore, for any security exponent d, there often exists an algorithm that factors N with polynomial time. In general case, relations between the bound $|x_0 - y_0|$ and the bound of secret exponent d are obtained. Boneh and Durfee's results in [4] are special cases of our results in this paper.

We reduce our method into two cases according to the size of the public exponent e and obtain the results by applying a new method of constructing a lattice basis. When e is large, set $f_e(x, y) := x(y - A) + 1$, then the polynomial $f_e(x, y)$ has (k, U) as a root modulo e, where $U = y_0 - x_0$ and k satisfies

$$ed + k(N + 1 - p - q) = 1. \tag{1.3}$$

Let

$$g_{i_1 i_2}(x, y) = \frac{x^{i_1} y^{i_2}}{l^k} f_e(x, y)^k e^{m-k}, \tag{1.4}$$

for $k = 0, \ldots, m$, where l is a leading monomial of f_e (for a detailed definition, see Section 3). All the polynomials $g_{i_1 i_2}$ have the root (k, U) modulo e^m. A lattice L is defined by taking the coefficient vectors of $g_{i_1 i_2}(xX, yY)$ as a basis. In general, one can force the matrix of the lattice to be lower triangular. According to the *LLL*-algorithm, one hopes that the dimension of the lattice is as large as possible and entries of the diagonal are as small as possible. The following definitions are useful for describing our method clearly.

Definition 1.1. Suppose a lattice L is spanned by vectors $\{b_1, b_2, \ldots, b_\omega\}$ and the matrix describing L is a lower triangular. A vector of which the last entry of the row exceeds the modulo of the lattice is called a bad vector. A vector of which the last entry of the row is less than the modulo of the lattice is called a good vector. A lattice spanned by a basis of which all its vectors are good is called an optimal lattice.

The key ingredient of the lattice reduction technique is to construct an optimal lattice of which the dimension is as large as possible. Jochemsz and May's strategy of constructing

a lattice basis [7] is to chose a continued subset of the polynomials $g_{i_1 i_2}$ as a lattice basis in which there may be some bad vectors. Our most significant contribution is that we can discard all the unnecessary bad vectors in a lattice basis with a simple new way and construct a lattice whose dimension of the lattice is large enough. We construct an optimal lattice basis by choosing a discontinued subset of the polynomials $g_{i_1 i_2}$. When e is small, a difference polynomial is chosen; similar methods but more complicated are applied to construct a lattice basis. In order to show that our method is practical, the properties of resultant are considered also in this paper.

The paper is organized as follows: some lattice preliminaries are given in Section 2. Section 3 shows the proposed method of attacking the RSA with large e. Section 4 shows the method of attacking the RSA with small e. The last section is the conclusion.

2. Lattice Theory

Let $b_1, b_2, \ldots, b_\omega \in \mathbb{Z}^n$ be linearly independent vectors with $\omega \leq n$. A lattice L spanned by $\{b_1, b_2, \ldots, b_\omega\}$ is the set of all integer linear combinations of $b_1, b_2, \ldots, b_\omega$. Such a set of vectors b_i's is called a lattice basis. We say that the lattice is full rank if $\omega = n$.

Let $f(x, y) = \sum_{i,j} a_{ij} x^i y^j \in \mathbb{Z}[x, y]$ be a bivariate polynomial with coefficients a_{ij} in the ring of integers. The Euclidean norm of f is defined as the norm of the coefficient vector $\|f\|^2 = \sum_{ij} a_{ij}^2$.

Lemma 2.1. *Let $B = \{b_1, b_2, \ldots, b_n\}$ be a basis. On input B, the L^3-algorithm outputs another basis $\{v_1, v_2, \ldots, v_n\}$ with*

$$\|v_1\| \leq \|v_2\| \leq 2^{n/4} \det(L)^{1/(n-1)}, \tag{2.1}$$

in time polynomial in n and in the bit-size of the entries in B.

Based on the *LLL*-algorithm, Coppersmith [3] presented a method of finding small solutions to the modular polynomial which has the desired small root over the integers. Howgrave-Graham [8] formulated a useful condition on how to find such a polynomial in terms of normal of a polynomial.

Lemma 2.2 (Howgrave-Graham [8]). *Let $h(x, y) \in \mathbb{Z}[x, y]$ which is the sum of at most ω monomials. Suppose that $h(x_0, y_0) \equiv 0 \bmod \varphi^m$, where $|x_0| < X$, $|y_0| < Y$ and $\|h(xX, yY)\| < \varphi^m / \sqrt{\omega}$. Then $h(x_0, y_0) = 0$ holds over the integers.*

3. The Case for Large e

Let e, d be integers such that $ed \equiv 1 (\mathrm{mod} \phi(N))$. It follows that there exists an integer k satisfying

$$ed + k(N + 1 - p - q) = 1. \tag{3.1}$$

Suppose that the public key and the security key satisfy $e < N^{\alpha}$, $d < N^{\beta}$ for some α, β. In this section, we consider the case that e is of the same order of magnitude as N and therefore α is very close to 1.

By (3.1), we have

$$k < \frac{2ed}{N} \leq N^{\alpha+\beta-1}. \tag{3.2}$$

Rewriting $p = [\sqrt{N}] - x_0$, $q = [\sqrt{N}] + y_0$, $A = N + 1 - 2[\sqrt{N}]$, and $U = y_0 - x_0$, we obtain

$$k(A - U) \equiv 1 (\mathrm{mod} e). \tag{3.3}$$

Suppose $f_e(x, y) := x(y - A) + 1$, then the polynomial $f_e(x, y)$ has (k, U) as a root modulo e.

A monomial l of f_e, with coefficient a_l, is called a leading monomial if there are no monomials in f_e besides l that is divisible by l. Here the leading monomial of f_e is xy and its coefficient is 1. Let $\varepsilon > 0$ be an arbitrarily small constant. Depending on $1/\varepsilon$, we fix an integer m. For $k \in \{0, \ldots, m + 1\}$, we define the sets M_k of monomials as

$$\begin{aligned} M_0 &:= \left\{ x^{i_1} y^{i_2} \mid x^{i_1} y^{i_2} \text{ is a monomial of } f_e^m \right\} \bigcup_{1 \leq j \leq t} \left\{ x^{i_1} y^{i_1 + j} \mid 1 \leq i_1 \leq m \right\}, \\ M_k &:= \left\{ x^{i_1} y^{i_2} \mid x^{i_1} y^{i_2} \text{ is a monomial of } f_e^m \text{ and } \frac{x^{i_1} y^{i_2}}{l^k} \text{ is a monomial of } f_e^{m-k} \right\} \\ &\quad \bigcup_{1 \leq j \leq t} \left\{ x^{i_1} y^{i_1 + j} \mid k \leq i_1 \leq m \right\}, \end{aligned} \tag{3.4}$$

where t is a parameter to be chosen later. We note that each set M_k in [7] is the whole monomials of f_e^{m-k}, while, in our method, we discard all bad rows of the lattice and consider part monomials of f_e^{m-k}.

We define the following shift polynomials

$$g_{i_1 i_2}(x, y) = \frac{x^{i_1} y^{i_2}}{l^k} f_e(x, y)^k e^{m-k}, \tag{3.5}$$

for $k = 0, \ldots, m$, and $x^{i_1} y^{i_2} \in M_k \setminus M_{k+1}$.

All the polynomials $g_{i_1 i_2}$ have the root (k, U) modulo e^m. We define a lattice L by taking the coefficient vectors of $g_{i_1 i_2}(xX, yY)$ as a basis. We can force the matrix describing L to be lower triangular. It is not difficult to see that the sets M_k can be rewritten as

$$\begin{aligned} M_0 &:= \left\{ x^{i_1} y^{i_2} \mid 0 \leq i_2 \leq i_1 \leq m \right\} \bigcup_{1 \leq j \leq t} \left\{ x^{i_1} y^{i_1 + j} \mid 1 \leq i_1 \leq m \right\}, \\ M_k &:= \left\{ x^{i_1} y^{i_2} \mid k \leq i_2 \leq i_1 \right\} \bigcup_{1 \leq j \leq t} \left\{ x^{i_1} y^{i_1 + j} \mid k \leq i_1 \leq m \right\}. \end{aligned} \tag{3.6}$$

Table 1

	1	x	xy	x^2	x^2y	xy^2	x^2y^2	x^2y^3
e^2	e^2							
xe^2	$*$	Xe^2						
fe	$*$	$*$	XYe					
x^2e^2	$*$	$*$	$*$	X^2e^2				
xfe	$*$	$*$	$*$	$*$	X^2Ye			
yfe	$*$	$*$	$*$	$*$	$*$	XY^2e		
f^2	$*$	$*$	$*$	$*$	$*$	$*$	X^2Y^2	
yf^2	$*$	$*$	$*$	$*$	$*$	$*$	$*$	XY^3

As an example, we consider the case $m = 2$, and $t = 1$. From the definition of M_k, we have

$$\begin{aligned} M_0 &= \left\{x^2y^3, x^2y^2, xy^2, x^2y, x^2, xy, x, 1\right\}, \\ M_1 &= \left\{x^2y^3, x^2y^2, xy^2, x^2y\right\}, \qquad M_2 = \left\{x^2y^3, x^2y^2\right\}. \end{aligned} \tag{3.7}$$

The matrix of the lattice for $m = 2$ is shown in Table 1.

In general, we find that the condition $\det(L) < e^{m(\omega+1-n)}$, derived from Lemmas 2.1 and 2.2, can be reduced to

$$X^{s_1}Y^{s_2} < e^{s_N}, \quad \text{for} \begin{cases} s_t = \displaystyle\sum_{x^{i_1}y^{i_2}\in M_0} i_t, \qquad t = 1,2 \\ s_N = \displaystyle\sum_{k=1}^{m} |M_k|. \end{cases} \tag{3.8}$$

Assuming that $|U| \le N^{\gamma}$, inequality (3.8) is equivalent to

$$(\alpha + \beta - 1)s_1 + \gamma s_2 - \alpha s_N < 0. \tag{3.9}$$

By calculation, we obtain that

$$\begin{aligned} s_1 &= \frac{m(m+1)(2m+4+3t)}{6}, \\ s_2 &= \frac{m(m+1)(m+2)}{6} + \frac{mt(m+t+2)}{2}, \\ s_N &= \frac{m(m-1)(m+1+3t)}{6}. \end{aligned} \tag{3.10}$$

For any m, the left hand side of (3.9) is minimized at $t = m(1-\beta-\gamma)/2\gamma$. Plugging this value into (3.9) and omitting a neglect number, we have

$$4\alpha\gamma + 2\beta\gamma + \gamma^2 - 3\beta^2 - 2\gamma + 6\beta - 3 < 0. \tag{3.11}$$

Notice that there are some bad rows in the above lattice. Next, we refine the construction method and improve the above result. In fact, the following lattice is an optimal lattice.

For $k \in \{1, \ldots, m+1\}$, let

$$\begin{aligned} t_k &= \frac{2-\alpha-\beta-\gamma}{\gamma}k, \qquad t_0 = \max\{t_1, \ldots, t_m\}, \\ M_0 &:= \left\{x^{i_1}y^{i_2} \mid x^{i_1}y^{i_2} \text{ is a monomial of } f_e^m\right\} \bigcup_{0\le k\le m} \bigcup_{1\le j\le t_k} \left\{x^{i_1}y^{i_1+j} \mid i_1 = k\right\}, \\ M_k &:= \left\{x^{i_1}y^{i_2} \mid x^{i_1}y^{i_2} \text{ is a monomial of } f_e^m \text{ and } \frac{x^{i_1}y^{i_2}}{l^k} \text{ is a monomial of } f_e^{m-k}\right\} \\ &\quad \bigcup_{k\le l\le m} \bigcup_{1\le j\le t_l} \left\{x^{i_1}y^{i_1+j} \mid i_1 = l\right\}. \end{aligned} \tag{3.12}$$

The definition of shift polynomials $g_{i_1 i_2}(x, y)$ is the same as above. From the definition of M_k, we have

$$\begin{aligned} M_0 &:= \left\{x^{i_1}y^{i_2} \mid 0 \le i_2 \le i_1 \le m\right\} \bigcup_{0\le k\le m} \bigcup_{1\le j\le t_k} \left\{x^{i_1}y^{i_1+j} \mid i_1 = k\right\}, \\ M_k &:= \left\{x^{i_1}y^{i_2} \mid k \le i_2 \le i_1\right\} \bigcup_{k\le l\le m} \bigcup_{1\le j\le t_l} \left\{x^{i_1}y^{i_1+j} \mid i_1 = l\right\}. \end{aligned} \tag{3.13}$$

By some rather complex calculations, we obtain that

$$\begin{aligned} s_1 &= \frac{m(m+1)(m+2)}{3} + a\frac{m(m+1)(2m+1)}{6}, \\ s_2 &= \frac{m(m+1)(m+2)}{6} + a^2\frac{m(m+1)(2m+1)}{12} \\ &\quad + a\frac{m(m+1)}{4} + a\frac{m(m+1)(2m+1)}{6}, \\ s_N &= \frac{m(m-1)(m+1)}{6} + a\frac{m(m+1)(2m+1)}{6}, \end{aligned} \tag{3.14}$$

where $a = (2-\alpha-\beta-\gamma)/\gamma$. The inequality (3.9) leads to

$$-2\alpha + 2\beta + \alpha^2 - \beta^2 + \alpha\gamma < 0. \tag{3.15}$$

From Lemma 2.1 and the estimations of (3.8), it is easy to see that if

$$-2\alpha + 2\beta + \alpha^2 - \beta^2 + \alpha\gamma < 0, \tag{3.16}$$

we are guaranteed to find two vectors in L that are shorter than the bound $e^m/\sqrt{\dim(L)}$. The vectors are the coefficient vectors of two bivariate polynomials $h_1(xX, yY)$ and $h_2(xX, yY)$. By Howgrave-Graham's theorem, $h_1(x, y)$ and $h_2(x, y)$ have the same root (k, U) over the integers. By taking resultant of $h_1(x, y)$ and $h_2(x, y)$ with respect to y, we get $g(x)$ with root k. We can easily extract k from $g(x)$ with standard root finding algorithms. Therefore, we can find U from $h_1(x, y)$ or $h_2(x, y)$. This completes the description of the attack. The heuristic fact that we have in our approach is as follows.

Fact 1. The probability that the construction described above yields zero polynomial that is, $g(x)$ is a zero polynomial is neglectable.

In practice, we can assume that $g(x)$ is a nonzero polynomial. The following lemma shows that Fact 1 holds.

Lemma 3.1. *Let $h_1(x, y), h_2(x, y)$, and $g(x)$ be defined as above. Then $g(x)$ is a zero polynomial if and only if* $\gcd(h_1(x, y), h_2(x, y)) \neq 1$.

Proof. Lemma 3.1 follows from Lemma 8.2 in [9]. □

In fact, if the polynomials h_1, h_2 are random chosen, then the probability that $g(x)$ is a zero polynomial is neglectable. From the above discussion, we get the following result.

Theorem 3.2. *Let e, d be defined as above and $U < N^{\gamma}$. If*

$$-2\alpha + 2\beta + \alpha^2 - \beta^2 + \alpha\gamma < 0, \tag{3.17}$$

then we can factor N with polynomial time.

We note that when $\alpha = 1$, $\gamma = 1/2$, the inequality in Theorem 3.2 becomes

$$\beta^2 - 2\beta + \frac{1}{2} > 0, \tag{3.18}$$

which is the result in [4]

4. The Case for Small Exponent e

In this section, we suppose that α is smaller than 1. Rewriting

$$\begin{aligned} p &= \sqrt{[N]} - x_0, \qquad q = \sqrt{[N]} + y_0, \\ A &= 1 - 2\sqrt{[N]}, \qquad U = y_0 - x_0, \end{aligned} \tag{4.1}$$

by (3.1), we have

$$ed + k(A - U) \equiv 1 (\mathrm{mod}\, N). \tag{4.2}$$

Let

$$f_N(x,y,z) = yz - ex - Ay + 1. \tag{4.3}$$

It is easy to see that $f_N(x,y,z)$ has (d,k,U) as a root modulo N. The similar method in section 3 can be applied to three variants polynomial f_N. Here the leading monomial of f_N is yz and the coefficient is 1. Let $\varepsilon > 0$ be an arbitrarily small constant. According to the size of $1/\varepsilon$, we fix an integer m. For $k \in \{0,\ldots,m+1\}$, let

$$t_k = ak - bm, \qquad t_0 = \max\{t_1,\ldots,t_m\}, \tag{4.4}$$

and $c = b/a$, where $a = (2-\alpha-\gamma)/\gamma$, $b = \beta/\gamma$. Define the sets M_k of monomials as follows

$$\begin{aligned} M_0 &:= \left\{x^{i_1}y^{i_2}z^{i_3} \mid x^{i_1}y^{i_2}z^{i_3} \text{ is a monomial of } f^m\right\} \\ &\quad \bigcup_{1\le j\le t_0}\left\{x^{i_1}z^j \mid 0 \le i_1 \le m - cm\right\} \bigcup_{cm\le k\le m}\bigcup_{1\le j\le t_k}\left\{x^{i_1}y^k z^{k+j} \mid 1 \le i_1 \le m-k\right\}, \\ M_k &:= \left\{x^{i_1}y^{i_2}z^{i_3} \mid x^{i_1}y^{i_2}z^{i_3} \text{ is a monomial of } f^m \text{ and } \frac{x^{i_1}y^{i_2}z^{i_3}}{l^k} \text{ is a monomial of } f^{m-k}\right\} \\ &\quad \bigcup_{cm\le k\le m}\bigcup_{k\le l\le m}\bigcup_{1\le j\le t_l}\left\{x^{i_1}y^l z^{l+j} \mid 1 \le i_1 \le m-k\right\}. \end{aligned} \tag{4.5}$$

We define the following shift polynomials:

$$g_{i_1i_2i_3}(x,y,z) = \frac{x^{i_1}y^{i_2}z^{i_3}}{l^k} f(x,y,z)^k N^{m-k}, \tag{4.6}$$

for $k = 0,\ldots,m$, and $x^{i_1}y^{i_2}z^{i_3} \in M_k \setminus M_{k+1}$.

All the polynomials $g_{i_1i_2i_3}$ have the root (d,k,U) modulo N^m. We define a lattice L by taking the coefficient vectors of $g_{i_1i_2i_3}(xX,yY,zZ)$ as a basis. We can force the matrix describing L to be lower triangular. The sets M_k can be rewritten as follows:

$$\begin{aligned} M_0 &= \left\{x^{i_1}y^{i_2}z^{i_3} \mid 0 \le i_1 + i_2 \le m, \text{and } 0 \le i_3 \le i_2\right\} \\ &\quad \bigcup_{1\le j\le t_0}\left\{x^{i_1}z^j \mid 0 \le i_1 \le m - cm\right\} \bigcup_{cm\le k\le m}\bigcup_{1\le j\le t_k}\left\{x^{i_1}y^k z^{k+j} \mid 1 \le i_1 \le m-k\right\}, \\ M_k &= \left\{x^{i_1}y^{i_2}z^{i_3} \mid k \le i_1 + i_2 \le m, \text{and } k \le i_3 \le i_2\right\} \\ &\quad \bigcup_{cm\le k\le m}\bigcup_{k\le l\le m}\bigcup_{1\le j\le t_l}\left\{x^{i_1}y^l z^{l+j} \mid 1 \le i_1 \le m-k\right\}. \end{aligned} \tag{4.7}$$

Table 2

	1	x	y	x^2	y^2	xy	yz	xyz	y^2z	y^2z^2
N^2	N^2									
xN^2	$*$	XN^2								
yN^2	$*$	$*$	YN^2							
x^2N^2	$*$	$*$	$*$	X^2N^2						
y^2N^2	$*$	$*$	$*$	$*$	Y^2N^2					
xyN^2	$*$	$*$	$*$	$*$	$*$	XYN^2				
fN	$*$	$*$	$*$	$*$	$*$	$*$	YZN^2			
xfN	$*$	$*$	$*$	$*$	$*$	$*$	$*$	$XYZN^2$		
yfN	$*$	$*$	$*$	$*$	$*$	$*$	$*$	$*$	Y^2ZN^2	
f^2	$*$	$*$	$*$	$*$	$*$	$*$	$*$	$*$	$*$	$Y^2Z^2N^2$

For example, we consider the case $m = 2$. From the definition of M_k, we have

$$\begin{aligned} M_0 &= \left\{y^2z^2, y^2z, xyz, yz, y^2, xy, x^2, x, y, 1\right\}, \\ M_1 &= \left\{y^2z^2, y^2z, xyz, yz\right\}, \qquad M_2 = \left\{y^2z^2\right\}. \end{aligned} \tag{4.8}$$

The matrix of the lattice for $m = 2$ is shown in Table 2.

In general, we find that $\det(L) < N^{m(\omega+1-n)}$, derived from Lemmas 2.1 and 2.2, can be reduced to

$$X^{s_1}Y^{s_2}Z^{s_3} < N^{s_N}, \quad \text{for} \begin{cases} s_t = \displaystyle\sum_{x^{i_1}y^{i_2}z^{i_3}\in M_0} i_t, \qquad t = 1,2,3, \\ s_N = \displaystyle\sum_{k=1}^{m} |M_k|. \end{cases} \tag{4.9}$$

Let $|U| \le N^{\gamma}$. Hence, the inequality (4.9) is equivalent to

$$\beta s_1 + (\alpha + \beta - 1)s_2 + \gamma s_3 \le s_N. \tag{4.10}$$

By calculation, we obtain that

$$\begin{aligned} s_1 &= \frac{m^4}{24} + \frac{(a-b)^4}{24a^3}m^4 + O\left(m^3\right), \\ s_2 &= \frac{m^4}{12} + \frac{a^4 - 2a^3b + 2ab^3 - b^4}{12a^3}m^4 + O\left(m^3\right), \\ s_N &= \frac{m^4}{24} + \frac{(a-b)^4}{24a^2}m^4 + \frac{a^4 - 2a^3b + 2ab^3 - b^4}{12a^3}m^4 + O\left(m^3\right). \end{aligned} \tag{4.11}$$

Plugging these value into (4.10) and omitting the neglect terms, we get that

$$\begin{aligned}&\beta\left(3a^3+(a-b)^3(3a+b)\right)+\alpha\left(2a^3+2(a+b)(a-b)^3\right)\\&\quad+\gamma\left(a^3+(a-b)^3\left(a^2-ab+2a+2b\right)\right)-\left(3a^3+(a-b)^3(7a-3b)\right)<0,\end{aligned}\tag{4.12}$$

which guarantees that we can find three vectors in L that are shorter than the bound $N^m/\sqrt{\dim(L)}$. These vectors are the coefficient vectors of three trivariate polynomials $f_1(xX,yY,zZ)$, $f_2(xX,yY,zZ)$, and $f_3(xX,yY,zZ)$. By Howgrave-Graham's theorem, $f_1(x,y,z)$, $f_2(x,y,z)$, and $f_3(x,y,z)$ have the root (d,k,U) over the integers. Afterward, we take the resultant of these integral polynomials with respect to the variable z and obtain two bivariate polynomials $g_1(x,y)$ and $g_2(x,y)$ with root (d,k). By taking resultant of $g_1(x,y)$ and $g_2(x,y)$ with respect to y, we get $g(x)$ with root d. d can be easily extracted from $g(x)$ with standard root finding algorithms. Therefore, we can find k from $g_1(x,y)$ or $g_2(x,y)$. Similarly, we can get U. By $U=x_0-y_0$ and $N=(\sqrt{[N]})^2+\sqrt{[N]}(y_0-x_0)-x_0y_0$, then N can be factored with polynomial time. This completes the description of the attack. The heuristic fact that we have in our approach is as follows.

Fact 2. The probability that the construction described above yields zero polynomial that is, $g(x)$ is a zero polynomial is neglectable.

A similar discussion as Fact 1, we have that for random choice $f_1(x,y,z)$, $f_2(x,y,z)$, and $f_3(x,y,z)$, the probability that $g(x)$ is a zero polynomial is neglectable. Therefore, in practice, we can assume that $g(x)$ is a nonzero polynomial.

Theorem 4.1. *Let e,d be defined as above and $U<N^\gamma$. If*

$$\begin{aligned}&\beta\left(3a^3+(a-b)^3(3a+b)\right)+\alpha\left(2a^3+2(a+b)(a-b)^3\right)\\&\quad+\gamma\left(a^3+(a-b)^3\left(a^2-ab+2a+2b\right)\right)-\left(3a^3+(a-b)^3(7a-3b)\right)<0,\end{aligned}\tag{4.13}$$

then we can factor N with polynomial time, where $a=(2-\alpha-\gamma)/\gamma$, $b=\beta/\gamma$.

As a special case of Theorem 4.1, one can see that when $2\alpha+\gamma\le 1.5$ and $d\le N^{1/2}$, there exists an algorithm that factors N with polynomial time.

5. Conclusion

In this paper, we obtained our results by taking advantage of lattice reduction technique. By improving the Jochemsz and May [7] strategy of constructing a lattice basis, we throw the bad rows in the lattice and obtain an optimal lattice. Applying the method of constructing an optimal lattice to cryptanalyse short exponent RSA, we get the main results which extend those of Boneh and Durfee in [4].

Acknowledgments

This work is supported by National 973 (Grant no. 2007CB807902), NSFC project under (Grant no. 60873041), nature science of Shandong province (Grant no. Y2008G23), and Doctoral Fund of Ministry of Education of China (Grant no. 20090131120012).

References

[1] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[2] M. J. Wiener, "Cryptanalysis of short RSA secret exponents," *IEEE Transactions on Information Theory*, vol. 36, no. 3, pp. 553–558, 1990.

[3] D. Coppersmith, "Small solutions to polynomial equations, and low exponent RSA vulnerabilities," *Journal of Cryptology*, vol. 10, no. 4, pp. 233–260, 1997.

[4] D. Boneh and G. Durfee, "Cryptanalysis of RSA with private key d less than $N^{0.292}$," *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1339–1349, 2000.

[5] J.-S. Coron and A. May, "Deterministic polynomial-time equivalence of computing the RSA secret key and factoring," *Journal of Cryptology*, vol. 20, no. 1, pp. 39–50, 2007.

[6] A. May, "Cryptanalysis of unbalanced RSA with small CRT-exponent," in *Proceedings of the 22nd Annual International Cryptology Conference (Crypto '02)*, vol. 2442 of *Lecture Notes in Computer Science*, pp. 242–256, Springer, 2002.

[7] E. Jochemsz and A. May, "A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants," in *Proceedings of the 12th International Conference on the Theory and Application of Cryptology and Information Security*, pp. 267–282, 2006.

[8] N. Howgrave-Graham, "Finding small roots of univariate modular equations revisited," in *Proceedings of the 6th IMA International Conference on Cryptography and Coding*, vol. 1355 of *Lecture Notes in Computer Science*, pp. 131–142, Springer, 1997.

[9] S. Lang, *Algebra*, vol. 211 of *Graduate Texts in Mathematics*, Springer, New York, NY, USA, 3rd edition, 2002.