On small secret key attack against RSA with high bits known prime factor

Yasufumi Hashimoto *

Abstract

It is well known that if the higher half bits of a prime factor are known or the secret key is small enough then the RSA cryptosystem is broken (e.g. [Coppersmith, J. Cryptology, 1997] and [Boneh-Durfee, Eurocrypt'99]). Recently, Sarkar-Maitra-Sarkar [Cryptology ePrint Archiv, 2008/315] proposed attacks against RSA under the conditions that the higher bits of a prime factor is known and the secret key is small. In the present paper, we improve their attacks to be effective for larger secret keys.

1 Introduction

The RSA cryptosystem [14] is famous as a public key cryptosystem based on the integer factorization problem. While there have been algorithms to factor integers such like the number sieve methods and the elliptic curve algorithm, their computational tasks are still far from polynomial time in general. However, it is known that the RSA can be broken in polynomial time under special conditions. For example, Coppersmith [5] and Boneh et al [3] found polynomial time algorithms to factor $n = pq$ when the higher or lower half bits of p are known (see also [7] and [8] for the recent works of factoring with known bits). On the other hand, Wiener [17], Boneh-Durfee [2] and Blömer-May [1] found that if the secret key d in the RSA is small enough ($d < n^{0.292\cdots}$) then n can be factored in polynomial time. Recently, Sarkar-Maitra-Sarkar ([12] and [15]) proposed attacks on the RSA under the conditions that the higher bits of p are known and the secret key is small. Their result is as follows.

Claim 1. *(Sarkar-Maitra-Sarkar, [15]) Let $n = pq$ be an integer with two primes p, q. Suppose that $p, q < cn^{1/2}$ with a small $c > 1$ and there exists a known integer p_1 such that*

*Institute of Systems, Information Technologies and Nanotechnologies, 7F 2-1-22, Momochihama, Fukuoka 814-0001, JAPAN, e-mail:hasimoto@isit.or.jp. Partially supported by JST Strategic Japanese-Indian Cooperative Programme on multidisciplinary Research Field, which combines Information and Communications Technology with Other Fields, and JSPS Grant-in-Aid for Young Scientists (B) no. 20740027.

Keywords. RSA, high bits known, small secret key attack, LLL reduction

$|p - p_1| < n^\alpha$ with $1/4 \le \alpha \le 1/2$. Denote by d, e respectively the secret and the public keys of the RSA cryptosystem modulo n, namely it holds that $ed \equiv 1 \bmod (p-1)(q-1)$. Suppose that $e < n$ and $d < n^\delta$ with $0 \le \delta \le 1$. If

$$\delta < 1 - \sqrt{\alpha},$$

then n can be factored in polynomial time of $\log n$.

The bound $\delta < 1 - 1/\sqrt{2} = 0.292\cdots$ for $\alpha = 1/2$ is just same to Boneh-Durfee's one in [2], and it is larger for smaller α. The aim in the present paper is to improve its bound as follows.

Claim 2. *Let $n, p, q, p_1, e, d, \alpha, \delta$ be as given in Claim 1. Put $q_1 := \lfloor n/p_1 \rfloor$ and fix integers $a, b < n^\gamma$ such that $0 \le \gamma \le 1/2 - \alpha$ and $|q_1/p_1 - b/a| < n^{\alpha - 1/2}$. If*

$$\delta < \begin{cases} \alpha + \frac{3}{2}\gamma + \frac{3}{4} - \sqrt{\left(2\alpha - \frac{1}{2} + \gamma\right)\left(2\alpha + \frac{7}{3}\gamma + \frac{5}{6}\right)}, & (36\alpha + 10\gamma \le 17), \\ 1 + \gamma - \sqrt{(1+\gamma)\left(2\alpha - \frac{1}{2} + \gamma\right)}, & (36\alpha + 10\gamma \ge 17). \end{cases}$$

then n can be factored in polynomial time of $\log n$.

When we take $a := \lfloor p_1/n^\alpha \rfloor$ and $b := \lfloor q_1/n^\alpha \rfloor$ ($\gamma = 1/2 - \alpha$), the bound is

$$\delta < \begin{cases} \frac{3}{2} - \frac{1}{2}\alpha - \sqrt{\alpha\left(2 - \frac{1}{3}\alpha\right)}, & (\alpha \le 6/13), \\ \frac{3}{2} - \alpha - \sqrt{\alpha\left(\frac{3}{2} - \alpha\right)}, & (\alpha \ge 6/13). \end{cases} \tag{1.1}$$

If a, b can be taken smaller, the bound of δ is larger. It is known that, if b/a is an approximation of q_1/p_1 by the continued fraction, then it holds that

$$\left|\frac{q_1}{p_1} - \frac{b}{a}\right| < \frac{1}{a^2} \qquad \text{(see Theorem 164 in [6])}.$$

Thus a, b can be taken much smaller than $n^{1/2-\alpha}$, especially close to or less than $n^{1/4-\alpha/2}$ for many cases. The bound of δ for $\gamma = 1/4 - \alpha/2$ is

$$\delta < \begin{cases} \frac{1}{4}\left(\alpha + \frac{9}{2} - \sqrt{\left(2\alpha - \frac{1}{3}\right)(10\alpha + 17)}\right), & (\alpha \le 29/62), \\ \frac{1}{4}\left(5 - 2\alpha - \sqrt{(5-2\alpha)(6\alpha - 1)}\right), & (\alpha \ge 29/62). \end{cases} \tag{1.2}$$

In 2002, Weger [16] proposed an attack when $|p - q| < n^\alpha$ and

$$\delta < \frac{1}{6}\left(4\alpha + 5 - 2\sqrt{(4\alpha - 1)(4\alpha + 5)}\right),$$

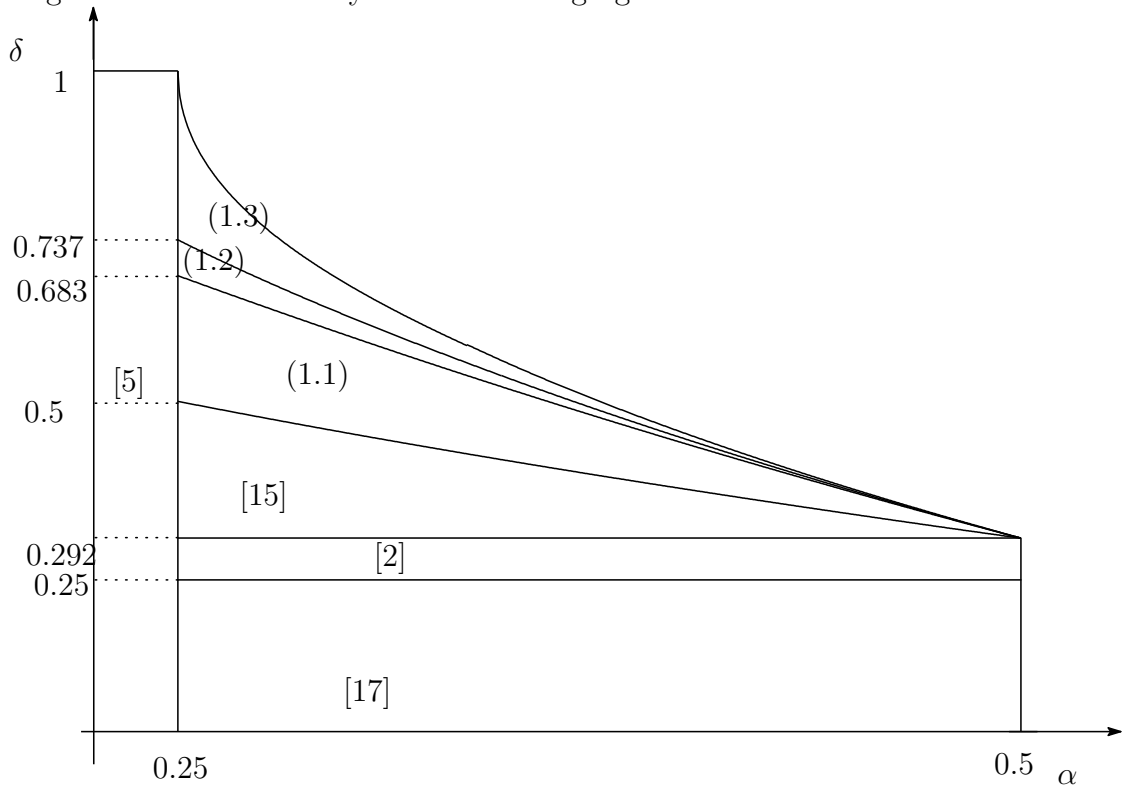
$$2 - 4\alpha < \delta < 1 - \sqrt{2\alpha - \frac{1}{2}}.$$

This situation is same that $p_1 = \lfloor \sqrt{n} \rfloor$ and $a = b = 1$, namely $\gamma = 0$. The bound of δ in Claim 2 for $\gamma = 0$ is as follows.

$$\delta < \begin{cases} \alpha + \frac{3}{4} - \sqrt{\left(2\alpha - \frac{1}{2}\right)\left(2\alpha + \frac{5}{6}\right)}, & (\alpha \leq 17/36), \\ 1 - \sqrt{2\alpha - \frac{1}{2}}, & (\alpha \geq 17/36). \end{cases} \tag{1.3}$$

While (1.3) does not completely cover Weger's bound, the difference is slight and (1.3) is effective also for the cases of $(a, b) = (2, 1), (3, 2), (5, 3)$, etc.

In the following figure, we summarize the bounds (1.1), (1.2), (1.3) and those in [5], [17], [2], [16] and [15]. Note that the difference between the bounds of [16] and (1.3) is too slight to be drawn clearly in the following figure.



The approach of our attack is similar to Boneh-Durfee's [2] and Sarkar-Maitra-Sarkar's [15] ones using the LLL algorithm. The difference is the choice of unknown parameters and the polynomials to be solved; Sarkar-Maitra-Sarkar used equations of two variables, but we use equations of three variables with a condition.

2 Preparations

The main tool in this paper is the LLL algorithm proposed in [11]. In this section, we give some preparations for our approaches.

2.1 Howgrave-Graham's lemma

Let $h(x,y,z)$ be a polynomial of (x,y,z) with integer coefficients and at most w monomials. Denote by $||h(x,y,z)||$ the square root of the sum of squares of the coefficients in $h(x,y,z)$. Suppose that there exist integers x_0, y_0, z_0 and positive integers X, Y, Z, M such that

$$\begin{aligned} &h(x_0,y_0,z_0) \equiv 0 \bmod M, \quad \text{with } |x_0|<X, |y_0|<Y, |z_0|<Z, \\ &||h(xX,yY,zZ)|| < M/\sqrt{w}. \end{aligned}$$

Howgrave-Graham's lemma [9] claims that $h(x_0,y_0,z_0)=0$ holds over integers.

2.2 LLL reduction

Let $n_1, n_2 \geq 1$ be integers with $n_1 \geq n_2$ and $\{u_1, \cdots, u_{n_2}\}$ a set of linearly independent vectors in $\mathbb{R}^{n_1}$. Denote by L the lattice generated by $\{u_1, \cdots, u_{n_2}\}$ and

$$\det(L) := \prod_{i=1}^{n_2} ||u_i^*||,$$

where $\{u_i^*\}$ is the set of vectors given by the Gram-Schmit orthogonalization and $||*||$ is the Euclidean norm. Note that, if $n_1 = n_2$, $\det L$ coincides the determinant of the square matrix $(u_1, \cdots, u_{n_2})$. The LLL algorithm [11] finds vectors b_1, b_2 such that

$$||b_1|| \leq 2^{\frac{n_2-1}{4}} (\det L)^{\frac{1}{n_2}}, \quad ||b_2|| \leq 2^{\frac{n_2}{4}} (\det L)^{\frac{1}{n_2-1}}$$

in polynomial time of n_1, n_2 and the logarithms of the entries in $(u_1, \cdots, u_{n_2})$.

3 Small secret key attack

3.1 Setting the base polynomial

First recall the notations.

Let $n = pq$ be an integer with two primes p, q, and e, d integers with $ed \equiv 1 \bmod (p-1)(q-1)$. Suppose that $p, q < cn^{1/2}$ with a small $c > 1$. By the definitions of e, d, we see that there exists an integer k such that

$$k(n+1-p-q) - 1 \equiv 0 \bmod e. \tag{3.1}$$

Note that Boneh-Durfee [2] used the equation

$$x(-y+n+1) - 1 \equiv 0 \bmod e$$

with a solution $(x,y) = (k, p+q)$ in their original attack.

Let p_1 be an integer with $|p-p_1| < n^\alpha$ $(1/4 \leq \alpha \leq 1/2)$. Put $q_1 := \lfloor n/p_1 \rfloor$, $p_2 := p-p_1$ and $q_2 := q - q_1$. We see that $|p_2|, |q_2| < n^\alpha$. Note that Sarkar-Maitra-Sarkar [15] used the equation

$$x(-y + n + 1 - p_1 - q_1) - 1 \equiv 0 \bmod e$$

with a solution $(x, y) = (k, p_2 + q_2)$ in their small secret key attack.

Let a, b be integers with $|q_1/p_1 - b/a| < n^{\alpha - 1/2}$ and $a, b < n^\gamma$ $(0 \leq \gamma \leq 1/2 - \alpha)$. Put $\Delta_0 := aq_2 + bp_2$. Since $n = pq = (p_1 + p_2)(q_1 + q_2)$, we have

$$\begin{aligned} a(n - p_1q_1) =& aq_2(p_1 + p_2) + aq_1p_2 \\ =& (p_1 + p_2)\Delta_0 + ap_1p_2(q_1/p_1 - b/a) - bp_2^2 \\ =& p_1\Delta_0 + O(n^{2\alpha+\gamma}). \end{aligned}$$

This means that

$$\left| \Delta_0 - \left\lfloor \frac{a(n - p_1q_1)}{p_1} \right\rfloor \right| = O\left(n^{2\alpha - 1/2 + \gamma}\right).$$

Put $\Delta := \Delta_0 - \lfloor a(n - p_1q_1)/p_1 \rfloor = aq_2 + bp_2 - \lfloor an/p_1 \rfloor + aq_1$. Then the relation $n = pq$ with unknown $p, q < cn^{1/2}$ is written by

$$bp_2^2 = p_2\Delta + p_1\Delta + (\lfloor an/p_1 \rfloor - bp_1)p_2 + (p_1\lfloor an/p_1 \rfloor - an) \tag{3.2}$$

with unknown $p_2 = O(n^\alpha)$, $\Delta = O(n^{2\alpha - 1/2 + \gamma})$.

Now, multiplying $-a$ to the both hand sides of (3.1) and substituting $aq_2 = \Delta - bp_2 + \lfloor a(n - p_1q_1)/p_1 \rfloor$, we have

$$k\left(\Delta + (a - b)p_2 - an + ap_1 + \lfloor an/p_1 \rfloor - a\right) + a \equiv 0 \bmod ae.$$

Thus, when we put

$$f(x, y, z) := bx\left(y + (a - b)z + N_1\right) + ab, \tag{3.3}$$

where $N_1 := -an + ap_1 + \lfloor an/p_1 \rfloor - a$, it holds that $f(k, \Delta, p_2) \equiv 0 \bmod abe$.

In our attack, we will use the equations $f(x, y, z) \equiv 0 \bmod abe$ and

$$bz^2 = yz + p_1y + M_1z + M_2, \tag{3.4}$$

where $M_1 := \lfloor an/p_1 \rfloor - bp_1$ and $M_2 := p_1\lfloor an/p_1 \rfloor - an$.

3.2 Process of the attack

Step 1. Fix an integer $m \geq 1$ and construct a set of polynomials $\{F_I(x, y, z)\}_I$ by using $f(x, y, z)$ such that $F_I(k, \Delta, p_2) \equiv 0 \bmod (abe)^m$ holds for any I.

Step 2. Generate a lattice L by the vectors whose entries are the coefficients of $\{F_I(xX, yY, zZ)\}_I$ where $X = O(n^{\delta})$, $Y = O(n^{2\alpha-1/2+\gamma})$ and $Z = O(n^{\alpha})$.
Step 3. Apply the LLL algorithm to the lattice L to get small vectors b_1, b_2. Denote by $h_1(x, y, z)$ and $h_2(x, y, z)$ the polynomials corresponding to b_1 and b_2 respectively.
Step 4. Find a solution (x_0, y_0, z_0) of $h_1(x, y, z) = 0$, $h_2(x, y, z) = 0$ and $bz^2 = yz + p_1y + M_1z + M_2$ such that $|x_0| < X$, $|y_0| < Y$ and $|z_0| < Z$.

In Step 4, one sometimes takes resultants among polynomials to reduce the number of variables. Then, in our attack, we must assume that such resultants do not vanish.

Due to the LLL algorithm and Howgrave-Graham's lemma, we see that this attack will work effectively when

$$2^{n_2/4} (\det L)^{\frac{1}{n_2-1}} < (abe)^m/\sqrt{w}. \tag{3.5}$$

From the following subsection, we construct $\{F_I(x, y, z)\}_I$ and discuss when the inequality (3.5) holds.

3.3 Generating the polynomials and the lattice

For simplicity, we write

$$g(x, y, z) = \mathrm{lc}\{g_i(x, y, z) \mid i \in I\}$$

when $g(x, y, z)$ is a linear combination of $\{g_i(x, y, z) \mid i \in I\}$.

Let $m \geq 1$ be an integer and

$$F^{(s)}_{l,i,j}(x, y, z) := (abe)^{m-l} x^i y^j z^s f^l(x, y, z),$$

where the parameters $\{l, i, j, s\}$ are taken by

$$\begin{cases} 0 \leq l \leq m, 0 \leq i \leq m - l, j = 0, s = 0, 1, \\ 0 \leq l \leq m, i = 0, s = 0, 1, 1 \leq j \leq t_{l,s}, \end{cases}$$

where $t_{l,0}, t_{l,s}$ are integers depending on l and m. Since $f(k, \Delta, p_2) \equiv 0 \bmod abe$, $(x_0, y_0, z_0) = (k, \Delta, p_2)$ is a common solution of $F^{(s)}_{l,i,j}(x, y, z) \equiv 0 \bmod (abe)^m$. Such polynomials are of three variables x, y, z. Now, remember (3.4) that

$$bz^2 = yz + \mathrm{lc}\{y, z, 1\}.$$

Then we have

$$b^2z^3 = (bz)(bz^2) = y(bz^2) + \mathrm{lc}\{yz, bz^2, z\} = y^2z + \mathrm{lc}\{y^2, yz, y, z, 1\}.$$

Recursively, we can obtain

$$b^{l-1}z^l = y^{l-1}z + \mathrm{lc}\{y^{l-1}, y^iz, y^i \mid 0 \leq i \leq l - 2\} \tag{3.6}$$

for any $l \geq 2$. This means that, using such relations between y and z, we can express

$$F^{(s)}_{l,i,j}(x, y, z) = \mathrm{lc}\left\{x^{l_1}y^{l_2}z, x^{l_1}y^{l_2} \mid 0 \leq l_1 \leq l + i, 0 \leq l_2 \leq l + j\right\}.$$

Thus we take the lattice L by the coefficients in such expressions of $F^{(s)}_{l,i,j}(x, y, z)$.

3.4 Estimating δ by the full rank lattice

First, we study the case when $t_{l,0} = t_{l,1} = t$ and t does not depend on l. Such a choice of $t_{l,0}, t_{l,1}$ does not give the bound of δ in Claim 2 but gives a bound corresponding to Boneh-Durfee's first bound $\delta < 0.284\cdots$ (see [2]).

By the definition of f and the condition (3.6), we have

$$\begin{aligned} f^l(x,y,z) =& b^l x^l y^l + \mathrm{lc}\{b^l x^{l_1} y^{l_2} z^{l_3} \mid 0 \le l_2 + l_3 \le l_1 \le l, (l_1,l_2) \neq (l,l)\} \\ =& b^l x^l y^l + \mathrm{lc}\{x^{l_1} y^{l_2} z, x^{l_1} y^{l_2} \mid 0 \le l_2 \le l_1 \le l, (l_1,l_2) \neq (l,l)\}. \end{aligned} \tag{3.7}$$

Similarly, we obtain

$$\begin{aligned} zf^l(x,y,z) =& zb^l x^l (y+(a-b)z)^l + \mathrm{lc}\{b^l x^{l_1} y^{l_2} z^{l_3+1} \mid 0 \le l_2 + l_3 \le l_1 < l\} \\ =& x^l \sum_{i=0}^{l} \binom{l}{i} y^{l-i} (a-b)^i b^l z^{i+1} + \mathrm{lc}\{b^l x^{l_1} y^{l_2} z^{l_3+1} \mid 0 \le l_2 + l_3 \le l_1 < l\} \\ =& x^l \sum_{i=0}^{l} \binom{l}{i} y^{l-i} (a-b)^i b^{l-i} y^i z \\ & + \mathrm{lc}\left\{x^l y^l, x^{l_1} y^{l_2} z, x^{l_1} y^{l_2} \mid 0 \le l_2 \le l_1 \le l, (l_1,l_2) \neq (l,l)\right\} \\ =& a^l x^l y^l z + \mathrm{lc}\left\{x^l y^l, x^{l_1} y^{l_2} z, x^{l_1} y^{l_2} \mid 0 \le l_2 \le l_1 \le l, (l_1,l_2) \neq (l,l)\right\}. \end{aligned} \tag{3.8}$$

Due to (3.7) and (3.8), we see that L is expressed by a triangle matrix with diagonal entries $\{(ae)^{m-l} b^m X^{l+i} Y^{l+j}, (be)^{m-l} a^m X^{l+i} Y^{l+j} Z\}_{l,i,j}$.

	$a^m x^m y^{m+t} z$	$b^m x^m y^{m+t}$	$\cdots$	$a^m x^m y^m z$	$b^m x^m y^m$	$a^m b e x^m y^{m-1} z$	$a b^m e x^m y^{m-1}$	$\cdots$
$F^{(1)}_{m,0,t}$	1	$*$	$\cdots$					
$F^{(0)}_{m,0,t}$	0	1				$*$		
$\vdots$	$\vdots$	$\vdots$	$\ddots$					
$F^{(1)}_{m,0,0}$				1	$*$	$*$	$*$	$\cdots$
$F^{(0)}_{m,0,0}$					1	$*$	$*$	$\cdots$
$F^{(1)}_{m-1,1,0}$		0				1	$*$	$\cdots$
$F^{(0)}_{m-1,1,0}$				0			1	
$\vdots$								$\ddots$

Thus the determinant of L is calculated by

$$\begin{aligned} \det L = \prod_{l=0}^{m} \Bigg[& \prod_{i=0}^{m-l} \left(b^m (ae)^{m-l} X^{l+i} Y^l\right) \left(a^m (be)^{m-l} X^{l+i} Y^l Z\right) \\ & \times \prod_{j=1}^{t} \left(b^m (ae)^{m-l} X^l Y^{l+j}\right) \left(a^m (be)^{m-l} X^l Y^{l+j} Z\right) \Bigg]. \end{aligned}$$

Recall that $a, b < n^\gamma, e < n, |X| < n^\delta, |Y| < n^{2\alpha-1/2+\gamma}$ and $|Z| < n^\alpha$. Then we have

$$\frac{1}{m^3}\log_n(|\det L|) < \left(\frac{2}{3}+T\right)(1+\gamma)+(1+2T)\gamma+\left(\frac{2}{3}+T\right)\delta \\ +\left(\frac{1}{3}+T+T^2\right)\left(2\alpha-\frac{1}{2}+\gamma\right)+O(m^{-1}),$$

where $T := t/m$. Since $n_1 = n_2 = (1+2T)m^2 + O(m)$, the inequality (3.5) holds when

$$\left(2\alpha-\frac{1}{2}+\gamma\right)T^2-\left(\frac{3}{2}-2\alpha-\delta\right)T+\frac{1}{3}\left(2\alpha-\frac{3}{2}+2\delta\right) < O(m^{-1}).$$

Ignoring the right hand side and taking $T = (3/2-2\alpha-\delta)/2(2\alpha-1/2+\gamma)$ to minimize the left hand side, we can obtain the bound

$$\delta < \frac{1}{6}\left(5+4\alpha+8\gamma-2\sqrt{(4\alpha-1+2\gamma)(5+4\alpha+8\gamma)}\right). \tag{3.9}$$

Note that the bound above coincides $\delta < 0.284\cdots$ when $\alpha = 1/2$ and $\gamma = 0$.

3.5 Improved bound

In this subsection, we will improve (3.9) and get the bound in Claim 2 corresponding to Boneh-Durfee's $\delta < 0.292\cdots$ ([2]). To get its bound, they used a lattice not given by a square matrix. While it is not easy to estimate the determinant of such a lattice in general, they estimate it by using the "geometrically progressive matrix". It has been used also in [4], [10], [16], [15] etc. However, it cannot be used directly in our work, since the structures of polynomials and the lattice are different. Then we will estimate the determinant by the elimination, not by the "geometrically progressive matrix".

First, due to (3.7) and (3.8), we see that $\{F^{(0)}_{l,i,0}, F^{(1)}_{l,i,0} \mid 0 \le l \le m, 0 \le i \le m-l\}$ is reduced to $\{b^m(ae)^{m-l}x^{l+i}y^l, a^m(be)^{m-l}x^{l+i}y^lz\}_{l,i}$ by the elimination.

Next, study $F^{(s)}_{l,0,j}$. By the definition of f and the relation (3.4), we have

$$\begin{aligned} f(x,y,z) =& b(xy+a)+\mathrm{lc}\{xz,x\},\\ zf(x,y,z) =& az(xy+b)+\mathrm{lc}\{f,xz,x,z,1\}. \end{aligned}$$

This gives that

$$y^jf^l = f\left(y^jf^{l-1}\right) = by^j(xy+a)f^{l-1}+\mathrm{lc}\{xy^jzf^{l-1}, xy^jf^{l-1}\}, \tag{3.10}$$

$$\begin{aligned} y^jzf^l =& zf\left(y^jf^{l-1}\right)\\ =& ay^jz(xy+b)f^{l-1}+\mathrm{lc}\{y^jf^l, xy^jzf^{l-1}, xy^jf^{l-1}, xy^jf^{l-1}\}. \end{aligned} \tag{3.11}$$

Recall that

$$xy = \mathrm{lc}\{f,xz,x,1\}, \qquad xyz = \mathrm{lc}\{zf,f,xz,x,z,1\}.$$

Then we have

$$\begin{aligned} xy^2 = y(xy) =& \mathrm{lc}\{yf, xyz, xy, y\} = \mathrm{lc}\{yf, zf, f, y, xz, x, z, 1\}, \\ xy^2z = y(xyz) =& \mathrm{lc}\{yzf, yf, xyz, xy, yz, y\} = \mathrm{lc}\{yzf, yf, zf, f, yz, y, xz, x, z, 1\}. \end{aligned}$$

Recursively we can obtain

$$xy^j = \mathrm{lc}\{y^{j-1}f, y^{j-1}, y^{j_1}zf, y^{j_1}f, y^{j_1}z, y^{j_1}, xz, x \mid 0 \le j_1 \le j-2\}, \tag{3.12}$$

$$xy^jz = \mathrm{lc}\{y^{j_1}zf, y^{j_1}f, y^{j_1}z, y^{j_1}, xz, x \mid 0 \le j_1 \le j-1\} \tag{3.13}$$

Substituting the aboves into (3.10) and (3.11), we get

$$\begin{aligned} y^jf^l =& by^j(xy+a)f^{l-1} + \mathrm{lc}\{y^{j_1}zf^l, y^{j_1}f^l, y^{j_1}zf^{l-1}, y^{j_1}f^{l-1}, \\ & x^{l_1}y^{l_2}z, x^{l_1}y^{l_2} \mid 1 \le j_1 \le j-1, 0 \le l_2 \le l_1 \le l\}, \\ y^jzf^l =& ay^jz(xy+b)f^{l-1} + \mathrm{lc}\{y^jf^l, y^jf^{l-1}, y^{j_1}zf^l, y^{j_1}f^l, y^{j_1}zf^{l-1}, y^{j_1}f^{l-1}, \\ & x^{l_1}y^{l_2}z, x^{l_1}y^{l_2} \mid 1 \le j_1 \le j-1, 0 \le l_2 \le l_1 \le l\}. \end{aligned}$$

	y^jzf^l	y^jf^l	y^jf^{l-1}	$y^{j-1}zf^l \quad \cdots \quad y^{j-1}f^{l-2}$	$\cdots$	$x^{l_1}y^{l_2}z^s(l_2 \le l_1)$
$ay^jz(xy+b)f^{l-1}$	1	*	*			
$by^j(xy+a)f^{l-1}$	0	1	0	$*$	$\cdots$	$*$
$by^j(xy+a)f^{l-2}$	0	0	1			
$ay^{j-1}z(xy+b)f^{l-1}$				1 $\quad\quad$ *		
$\vdots$		0		$\ddots$		$*$
$by^{j-1}(xy+a)f^{l-3}$				$0 \quad\quad$ 1		
$\vdots$		$\vdots$		$\vdots$	$\ddots$	

This means that, if

$$t_{l-1,0} \le t_{l,0} \le t_{l-1,1} + 1, \quad t_{l-1,1} \le t_{l,1} \le t_{l-1,0}, \tag{3.14}$$

then

$$\left\{F^{(0)}_{l,0,j}, F^{(1)}_{l,0,j}, b^m(ae)^{m-l}x^{l+i}y^l, a^m(be)^{m-l}x^{l+i}y^lz\right\}_{l,i,j}$$

is reduced to

$$\left\{F^{(0)}_{0,0,j}, F^{(1)}_{0,0,j}, (ae)^{-1}(xy+a)F^{(0)}_{l-1,0,j}, (be)^{-1}(xy+b)F^{(1)}_{l-1,0,j}, b^m(ae)^{m-l}x^{l+i}y^l, a^m(be)^{m-l}x^{l+i}y^lz\right\}_{l,i,j}$$

by the elimination. Of course, the determinants of two lattices corresponding to the sets of polynomials above are same. Repeating such operations, we can reduce it to

$$\left\{(ae)^{m-l}b^my^j(xy+a)^l, (be)^{m-l}a^my^j(xy+b)^lz, b^m(ae)^{m-l}x^{l+i}y^l, a^m(be)^{m-l}x^{l+i}y^lz\right\}_{l,i,j}$$

with the same determinants. Thus the determinant of the corresponding lattice L is estimated by

$$|\det L| \le \prod_{l=0}^{m} \left[\prod_{i=0}^{m-l} |ae|^{m-l}|b|^m|X|^{l+i}|Y|^l \prod_{j=1}^{t_{l,0}} |ae|^{m-l}|b|^m(|XY|+|a|)^l|Y|^j \right.$$
$$\left. \times \prod_{i=0}^{m-l} |be|^{m-l}|a|^m|X|^{l+i}|Y|^l|Z| \prod_{j=1}^{t_{l,1}} |be|^{m-l}|a|^m(|XY|+|b|)^l|Y|^j|Z| \right]$$

under the condition (3.14). Letting $T_1, T_2 \ge 0$ such that $t_{l,0}, t_{l,1} = T_1 l + T_2 m + O(1)$, we have

$$\frac{1}{m^3}\log_n|\det L| < \left(2\alpha - \frac{1}{2} + \gamma\right)\left(\frac{1}{3}T_1^2 + T_1T_2 + T_2^2\right) + \left(\frac{2}{3}\delta + \frac{4}{3}\alpha + 2\gamma\right)T_1$$
$$+ \left(\delta + 2\alpha + 4\gamma + \frac{1}{2}\right)T_2 + \left(\frac{2}{3}\delta - \frac{2}{3}\alpha + 2\gamma + \frac{1}{2}\right) + O(m^{-1}).$$

Since $n_2 = (T_1 + 2T_2 + 1)m^2 + O(m)$, the condition (3.5) holds when

$$(2\alpha - 1/2 + \gamma)(T_1^2 + 3T_1T_2 + 3T_2^2) + (2\delta + 4\alpha - 3)T_1$$
$$+ 3(\delta + 2\alpha - 3/2)T_2 + 2\delta + 2\alpha - 3/2 < O(m^{-1}). \tag{3.15}$$

The condition (3.14) means that it must be $T_1 \le 1/2$. Then, in order to minimize the left hand side of (3.15), take T_1, T_2 as follows.

$$T_1 = \begin{cases} \dfrac{3 - 2\delta - 4\alpha}{4\alpha - 1 + 2\gamma}, \\ \dfrac{1}{2} \end{cases} \qquad T_2 = \begin{cases} 0, & (\delta \ge 7/4 - 3\alpha - \gamma/2)\,, \\ \dfrac{7/4 - 3\alpha - \gamma/2 - \delta}{4\alpha - 1 + 2\gamma}, & (\delta \le 7/4 - 3\alpha - \gamma/2)\,. \end{cases}$$

The former (T_1, T_2) gives

$$7/4 - 3\alpha - \gamma/2 \le \delta < 1 + \gamma - \sqrt{(1+\gamma)(2\alpha - 1/2 + \gamma)}, \tag{3.16}$$

and the later does

$$\delta < \alpha + \frac{3}{2}\gamma + \frac{3}{4} - \sqrt{\left(2\alpha - \frac{1}{2} + \gamma\right)\left(2\alpha + \frac{7}{3}\gamma + \frac{5}{6}\right)}. \tag{3.17}$$

Combining (3.16) and (3.17), we get the bound in Claim 2. □

4 Experiments

We tried our approach for $(\log_2 n, \alpha, \delta) \sim (1000, 0.4, 0.37)$ and $(1000, 0.3, 0.5)$. The machine was with Windows 7 and Core-i7 2.67 GHz, and the LLL algorithm was by Pari/gp

ver. 2.3.5 [13]. Computing the continued fractions of q_1/p_1, we found a, b with $\gamma \sim 0.05$ and $\gamma \sim 0.1$ respectively. We take $m = 7$, $\{t_{l,0}\}_{0 \le l \le 7} = \{0, 1, 1, 2, 2, 3, 3, 3\}$ and $\{t_{l,1}\} = \{0, 0, 1, 1, 2, 2, 3, 3\}$ ($w = 99$) for the former case and $m = 5$, $\{t_{l,0}\}_{0 \le l \le 5} = \{0, 1, 1, 2, 2, 2\}$ and $\{t_{l,1}\} = \{0, 0, 1, 1, 2, 2\}$ ($w = 56$) for the later case. Then the desired solutions were found respectively with about 1 hour and 6 minutes computations for the LLL reductions. Since the theoretical bounds in [15] are $\delta < 0.367\cdots$ for $\alpha = 0.4$ and $\delta < 0.452\cdots$ for $\alpha = 0.3$, we see that our approach really gives an improvement of [15].

5 Conclusion

Wiener [17] and Boneh-Durfee [2] proposed attacks when the secret key is small enough, and Sarkar-Maitra-Sarkar [15] proposed attacks for larger secret keys when higher bits of a prime factor are known. We further improve their upper bound for the secret key as described in Claim 2. Recall that our bound is larger as γ is smaller. This means that, if the ratio q/p is approximated by a ratio between smaller integers, then larger secret keys are required. Thus, in the process to choose prime factors p, q on RSA, one should check approximations of q/p in some way, for example by the continued fractions.

References

[1] J. Blömer and A. May, *Low secret exponent RSA revisited*, LNCS **2146** (2001), pp. 4-19.

[2] D. Boneh and G. Durfee, *Cryptanalysis of RSA with private key d less than* $N^{0.292}$, Eurocrypt'99, LNCS **1592** (1999), pp. 1–11.

[3] D. Boneh, G. Durfee and Y. Frankel, *Exposing an RSA private key given a small fraction of its bits*, Asiacrypt'98, LNCS **1514** (1999), pp. 25–34.

[4] M. Ciet, F. Koeune, F. Laguillaumie and J.J. Quisquater, *Short private exponent attacks on fast variants of RSA*, UCL Crypto Group Tech. Rep. CG-2002/4, 2002.

[5] D. Coppersmith, *Small Solutions to polynomial equations, and low exponent RSA vulnerability*, J. Cryptology, **10** (1997), pp. 233–260.

[6] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers*, Fifth edition, Oxford University Press, 1979.

[7] N. Heninger and H. Shacham, *Reconstructing RSA private keys from random key bits*, Crypto'09, LNCS **5677**, pp. 1-17.

[8] M. Herrmann and A. May, *Solving linear equations modulo divisors: On factoring given any bits*, Asiacrypt'08, LNCS **5350**, pp. 406–424.

[9] N. Howgrave-Graham, *Finding small roots of univariate modular equations revisited*, LNCS **1355** (1997), pp. 131–142.

[10] K. Itoh, N. Kunihiro and K. Kurosawa, *Small secret key attack on a variant of RSA (Due to Takagi)*, CT-RSA'08, LNCS **4964** (2008), pp. 387–406.

[11] A. Lenstra, H. Lenstra and L. Lovasz, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), pp. 515–534.

[12] S. Maitra and S. Sarkar, *Revisiting Wiener's attack – new weak keys in RSA*, ISC 2008, LNCS **5222**, pp. 228–243.

[13] *PARI/GP developmemt*, http://pari.math.u-bordeaux.fr/.

[14] R.L. Rivest, A. Shamir and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Comm. ACM **21** (1978), pp. 120–126.

[15] S. Sarkar, S. Maitra and S. Sarkar, *RSA cryptanalysis with increased bounds on the secret exponent using less lattice dimension*, Cryptology ePrint Archiv 2008/315.

[16] B. de Weger, *Cryptanalysis of RSA with small prime difference*, Appl. Algebra Eng. Commun. Comput., **13** (2002), pp. 17–28.

[17] M. J. Wiener, *Cryptanalysis of short RSA secret exponents*, IEEE Trans. Information Theory, **36** (1990), pp. 553–558.