Cryptanalysis of Short Exponent RSA with Primes Sharing Least Significant Bits

Hung-Min Sun[1], Mu-En Wu[1], Ron Steinfeld[3]
Jian Guo[2], and Huaxiong Wang[2,3]

[1] Department of Computer Science,
National Tsing Hua University, Taiwan
hmsun@cs.nthu.edu.tw, mn@is.cs.nthu.edu.tw
[2] School of Physical & Mathematical Sciences,
Nanyang Technological University, Singapore
{guojian,hxwang}@ntu.edu.sg
[3] Centre for Advanced Computing - Algorithms and Cryptography,
Department of Computing, Macquarie University, Australia
rons@ics.mq.edu.au

Abstract. LSBS-RSA denotes an RSA system with modulus primes, p and q, sharing a large number of least significant bits. In *ISC 2007*, Zhao and Qi analyzed the security of short exponent LSBS-RSA. They claimed that short exponent LSBS-RSA is much more vulnerable to the lattice attack than the standard RSA. In this paper, we further raise the security boundary of the Zhao-Qi attack by considering another polynomial. Our improvemet supports the result of analogue Fermat factoring on LSBS-RSA, which claims that p and q cannot share more than $\frac{n}{4}$ least significant bits, where n is the bit-length of pq. In conclusion, it is a trade-off between the number of sharing bits and the security level in LSBS-RSA. One should be more careful when using LSBS-RSA with short exponents.

Keywords: RSA, least significant bits (LSBs), LSBS-RSA, short exponent attack, lattice reduction technique, the Boneh-Durfee attack.

1 Introduction

Since 1978, RSA [20] is the most popular cryptosystem in the world. Its security is based on the hardness of factoring problem. Generally we apply 1024-bit RSA modulus to achieve the goal of factoring-infeasible, but such large modulus also causes the inefficiency in encryption and decryption of RSA. Consequently, many practical issues have been considered when implementing RSA such as how to reduce the encryption time (or signature-verification time), how to reduce the decryption time (or signature-generation time) [16], [17], etc.. One of the most common methods to reduce the decryption time is using a short private exponent d. However, in 1990 Wiener [25] showed that choosing too small private exponent is insecure when using RSA system. Indeed, instances of RSA with $d < N^{0.25}$

can be efficiently broken by the continued fraction attack, which is also called the Wiener attack. The boundary of the Wiener attack had been extended by Boneh and Durfee [3] in 1998. They took advantage of lattice reduction technique and showed that instance of RSA with $d < N^{0.292}$ should be considered insecure. Although their method is heuristic, the experiments demonstrate the effectiveness of the attack.

LSBS-RSA denotes an RSA system with modulus primes sharing a large number of least significant bits. This RSA variant was suggested to improve the computational efficiency of server-aided signature generation [6], [22]. Steinfeld and Zheng analyzed the security of LSBS-RSA under the partial key exposure attacks in [21], and [22]. Sun et. al. [19] further improved this result by using the property of LSBS-RSA. Their results show that LSBS-RSA with small public exponent is inherently resistant to the partial key exposure attacks. This gives an advantage of using small exponent LSBS-RSA in applications. However, it does not imply that LSBS-RSA is secure against all the small exponent attacks. Zhao and Qi [26] showed that LSBS-RSA is much more vulnerable than the standard RSA against the attack by using lattice reduction technique. Here we call the Zhao-Qi attack throughout this paper. Let α be the parameter such that $|p-q| = r \cdot 2^{(\frac{1}{2}-\alpha)n}$ for some odd integer r. The Zhao-Qi attack shows that LSBS-RSA is insecure under the condition

$$\beta < \tfrac{1}{6}\alpha + \tfrac{13}{12} - \tfrac{1}{3}\sqrt{\alpha^2 + (6\gamma+1)\alpha + \tfrac{12\gamma+1}{4}},$$

where β and γ satisfy $d = N^{\beta}$ and $e = N^{\gamma}$, respectively. For example, if p and q share $0.2n$ least significant bits and $e \approx N$ (*i.e.*, $\gamma = 1$, $\alpha = 0.3$), then LSBS-RSA will be insecure when $d < N^{0.335}$.

In this paper, we give a revised version of the Zhao-Qi attack to further raise the security boundary. Also, we provide a new method by considering another polynomial to attacking LSBS-RSA, which conducts to a better result compared with the Zhao-Qi attack. Our result shows that LSBS-RSA is insecure under the condition

$$\beta < \tfrac{2}{3}\alpha + \tfrac{5}{6} - \tfrac{4}{3}\sqrt{\alpha^2 + (\tfrac{3}{2}\gamma - \tfrac{1}{2})\alpha - \tfrac{6\gamma-1}{16}}.$$

Take the case $e \approx N$ for example, if the modulus primes share the $0.2n$ least significant bits (*i.e.*, $\gamma = 1$, $\alpha = 0.3$), LSBS-RSA will be insecure if $d < N^{0.662}$, which is much higher than Zhao and Qi's boundary. Moreover, compared with the Boneh-Durfee attack [3], [4] and de Weger's attack on RSA with small prime difference [24], our result yields an improvement when primes sharing a large number of least significant bits.

The remainder of this paper is organized as follows. In Section 2, we briefly review LSBS-RSA, lattice reduction technique, and the Zhao-Qi attack. In Section 3, we revise the Zhao-Qi attack to raise the security boundary. Section 4 shows the proposed method to analyze the security boundary of short exponent LSBS-RSA. Further discussions are shown in Section 5. Finally, we conclude this paper and give some open problems in Section 6.

2 Preliminaries

2.1 LSBS-RSA and the Notation: α, β, and γ

An RSA system with modulus primes sharing a large number of least significant bits is called LSBS-RSA. Denote an LSBS-RSA modulus $N = pq$ as the product of two large primes p and q, with p & q share the $(\frac{1}{2} - \alpha)n$ least significant bits, where $q < p < 2q$, and n is the bit-length of N. We may write $|p - q| = r \cdot 2^{(\frac{1}{2}-\alpha)n}$ for some integer r of αn bits and it is obvious that $\alpha \leq \frac{1}{2}$. In the following table we define the notation α, β, and γ used in the paper.

α: α is the parameter such that $\lvert p - q\rvert = r \cdot 2^{(\frac{1}{2}-\alpha)n}$ for some odd integer r
β: β is the parameter such that $d = N^{\beta}$.
γ: γ is the parameter such that $e = N^{\gamma}$.

In addition, we define the function "LSB$(\cdot)$". Given an integer x of m bits, whose binary representation is

$$(x)_2 = (x_m, x_{m-1}, ...x_j, ..., x_i, ..., x_2, x_1)_2,$$

where $x_i = 0$ or 1 for $i = 1, ..., m$. Then, x_m should be 1, which is called the most significant bit of x. x_1 could be 0 or 1, which is called the least significant bit of x. Denote "LSB$_{i\tilde{}j}(x)$" as the i-th to j-th least significant bits of $(x)_2$, where $i < j$. That is,

$$\text{LSB}_{i\tilde{}j}(x) = (x_j, ..., x_i)_2.$$

And denote "LSB$_i(x)$" as the i-th least significant bit of $(x)_2$. That is,

$$\text{LSB}_i(x) = x_i.$$

The following lemma shows the exposed portion of the modulus primes if p and q share a number of least significant bits.

Lemma 1. *Let $N = pq$ denote an n-bit modulus in LSBS-RSA, where $LSB_{1\tilde{}m}(p) = LSB_{1\tilde{}m}(q)$. There exists an algorithm to compute the $LSB_{1\tilde{}2m}(p+q)$, $LSB_{1\tilde{}m}(p)$, and $LSB_{1\tilde{}m}(q)$ in time polynomial in n.*

Proof. Let $p = p_H \cdot 2^m + l$ and $q = q_H \cdot 2^m + l$. Thus, l is a solution to the modular quadratic congruence $x^2 \equiv N \pmod{2^m}$, and it can be computed at most for 4 candidates in time polynomial in n (see Lemma 1 in [22] for more detail). Consider the identity

$$(\tfrac{p+q}{2})^2 = (\tfrac{p-q}{2})^2 + N.$$

Replacing p and q by $p_H \cdot 2^m + l$ and $q_H \cdot 2^m + l$, respectively, conducts to

$$\text{LSB}_{1\tilde{}2m-2}\left(l \cdot (p_H + q_H) \cdot 2^m + l^2\right) = \text{LSB}_{1\tilde{}2m-2}(N).$$

Note that l is an odd integer. Thus, $l^{-1} \pmod{2^{2m-2}}$ exists and we denote it as l^{-1} for short. We have

$$\mathrm{LSB}_{1\text{-}2m-2}((p_H + q_H) \cdot 2^m) = \mathrm{LSB}_{1\text{-}2m-2}\left(l^{-1} \cdot (N - l^2)\right), \tag{1}$$

which implies

$$\begin{aligned} &\mathrm{LSB}_{1\text{-}2m-1}\left(\tfrac{p+q}{2}\right) = \mathrm{LSB}_{1\text{-}2m-1}((p_H + q_H)\, 2^{m-1} + l) \\ &= \mathrm{LSB}_{1\text{-}m}\,(p_H + q_H) \;||\; \mathrm{LSB}_m\left((p_H + q_H)\, 2^{m-1} + l\right) \;||\; \mathrm{LSB}_{1\text{-}m-1}\,(l), \end{aligned} \tag{2}$$

where "||" denotes the symbol for concatenation. Combining (1) and (2) we can compute $\mathrm{LSB}_{1\text{-}2m-1}\left(\frac{p+q}{2}\right)$. Thus, we have

$$\mathrm{LSB}_{1\text{-}2m}\,(p+q) = \mathrm{LSB}_{1\text{-}2m-1}\left(\tfrac{p+q}{2}\right) \;||\; 0,$$

which completes the proof.

The following corollary is the key point we used in the paper to improve the Zhao-Qi attack.

Corollary 1. *Let $N = pq$ denote an n-bit modulus of LSBS-RSA, where p and q share the $(\frac{1}{2} - \alpha)n$ least significant bits, i.e., $LSB_{1\text{-}(\frac{1}{2}-\alpha)n}\,(p) = LSB_{1\text{-}(\frac{1}{2}-\alpha)n}\,(q)$. Then, $LSB_{1\text{-}(\frac{1}{2}-\alpha)n}\,(p+q)$, $LSB_{1\text{-}(\frac{1}{2}-\alpha)n}\,(p)$, and $LSB_{1\text{-}(\frac{1}{2}-\alpha)n}\,(q)$, are known to the attacker.*

Proof. The proof is quite easy. We just replace m in Lemma 1 by $(\frac{1}{2} - \alpha)n$.

Note that we should set $\alpha > \frac{1}{4}$. In case of $\alpha \leq \frac{1}{4}$, which means that p and q share the $\frac{n}{4}$ least significant bits at least, the modulus N can be factored in time polynomial in n (see Corollary 1 in [22]). This result is analogue to the result of Fermat's factoring method, which factors N immediately if p and q share the $\frac{n}{4}$ most significant bits at least. We call the factoring attack when $\alpha \leq \frac{1}{4}$ as "Analogue Fermat factoring" in the paper.

2.2 Lattice Attack

A vector space L is called a lattice if L is spanned by ω linearly independent vectors, denoted as $\mathbf{u}_1$, $\mathbf{u}_2$, ..., $\mathbf{u}_\omega \in \mathbb{Z}^n$, over $\mathbb{Z}$. That is,

$$L = \left\{ \sum_{i=1}^{\omega} a_i \mathbf{u}_i \mid \text{where } a_i \in \mathbb{Z} \text{ and } \mathbf{u}_i \in \mathbb{Z}^n \text{ for } i = 1, ..., \omega \right\}.$$

$\mathbf{u}_1$, $\mathbf{u}_2$, ..., $\mathbf{u}_\omega$ are also called the basis of lattice L. We say that L is full rank if $\omega = n$. The determinant of a full rank lattice L, denoted as $\det(L)$, is equal to the determinant of the n by n matrix whose rows are $\mathbf{u}_1$, $\mathbf{u}_2$, ..., $\mathbf{u}_\omega$. Next we show the result of the output of the LLL algorithm, which produces a new basis of lattice L with the following properties.

Lemma 2. *[15] Suppose that L is a lattice with basis $\{\mathbf{u}_1, \mathbf{u}_2, ..., \mathbf{u}_\omega\}$. Given the input $\{\mathbf{u}_1, \mathbf{u}_2, ..., \mathbf{u}_\omega\}$, LLL algorithm can produce a new basis $\{\mathbf{b}_1, \mathbf{b}_2, ..., \mathbf{b}_\omega\}$ satisfying:*

1. $\|\mathbf{b}_i^*\|^2 \leq 2\left\|\mathbf{b}_{i+1}^*\right\|^2$ for $i = 1, ..., \omega - 1$.
2. If $\mathbf{b}_i = \mathbf{b}_i^* + \sum_{j=1}^{i-1} \mu_{i,j}\mathbf{b}_j^*$, then $|\mu_j| \leq \frac{1}{2}$ for all j and $i = 1, ..., \omega$.

We call $\{\mathbf{b}_1, \mathbf{b}_2, ..., \mathbf{b}_\omega\}$ an LLL-reduced basis of L. Here, we just mention one of the properties of LLL-reduced basis that will be used in the paper.

Theorem 1. *Let $\{\mathbf{b}_1, \mathbf{b}_2, ..., \mathbf{b}_\omega\}$ be an LLL-reduced basis of L. Then,*

$$\|\mathbf{b}_1\| \leq 2^{\frac{\omega}{2}} \det(L)^{\frac{1}{\omega}} \text{ , and } \|\mathbf{b}_2\| \leq 2^{\frac{\omega}{2}} \det(L)^{\frac{1}{\omega-1}} .$$

Coppersmith [7] took the advantage of LLL algorithm to find the small roots of a modular equation. Suppose that the norm of a polynomial $h(x, y) = \sum_{i,j} a_{i,j}x^i y^j$ is defined as $\|h(x, y)\|^2 = \sum_{i,j} a_{i,j}^{\mathbf{2}}$. Howgrave-Graham [13] followed Coppersmith's method to show the following lemma, which is a powerful tool in the cryptanalysis of RSA systems.

Lemma 3. *(Howgrave-Graham) Let $h(x, y) \in \mathbb{Z}[x, y]$ be a bivariate polynomial which is a sum of at most ω monomials. Suppose that*

1. *$h(x_0, y_0) = 0 \pmod{e^m}$, where $m \in \mathbb{N}$*
2. *$\|h(xX, yY)\| < \frac{e^m}{\sqrt{\omega}}$, where $|x_0| < X$, $|y_0| < Y$.*

Then $h(x_0, y_0) = 0$ holds over the integers.

The proof of Lemma 3 can be found in earlier citations, such as [7], [3], [4], [8], [9].

In the heuristic variant of the lattice attacks (with bivariate\trivariate modular polynomials) that we consider in this paper, we hope that we get two algebraically independent polynomials from the lattice. Given a modular polynomial $f(x, y) = 0 \pmod{e}$ with ω monomials. We may construct a set of polynomials with the same root as $f(x, y) = 0 \pmod{e}$, and regard these polynomials as a basis of the lattice L by representing their coefficients as the vectors with ω components. Then, applying the LLL algorithm to produce the first two shortest vectors in LLL basis, denoted as $f_1(x, y)$ and $f_2(x, y)$, whose norms are smaller than $2^{\frac{\omega}{2}} \det(L)^{\frac{1}{\omega}}$ and $2^{\frac{\omega}{2}} \det(L)^{\frac{1}{\omega-1}}$, respectively. Thus, according to Lemma 3, if we set $2^{\frac{\omega}{2}} \det(L)^{\frac{1}{\omega}} < \frac{e^m}{\sqrt{\omega}}$, then the root of $f_1(x, y) \pmod{e}$ and $f_2(x, y) \pmod{e}$ also hold over $\mathbb{Z}$. We then take their resultant with respect to one of the variables to eliminate it and get a univariate equation and solve for the root in the other variable. It is a well-known technique called the lattice attack. Zhao and Qi [26] used this technique to attack short exponent LSBS-RSA. Next, we briefly describe their attack.

2.3 The Zhao-Qi Attack

Assume that an LSBS-RSA modulus $N = pq$ satisfies $p - q = r \cdot 2^{(\frac{1}{2}-\alpha)n}$, where r is an odd integer. Then,

$$p + q = (p - q) + 2q = r \cdot 2^{(\frac{1}{2}-\alpha)n} + 2q. \tag{3}$$

Applying (3) to RSA equation yields

$$ed = k\left[(N + 1) - 2q - r \cdot 2^{(\frac{1}{2}-\alpha)n}\right] + 1.$$

Consider the polynomial

$$f(x, y, z) = x(A - 2y - az) + 1, \tag{4}$$

where $A = N + 1$, and $a = 2^{(\frac{1}{2}-\alpha)n}$. Then $(x_0, y_0, z_0) = (k, q, r)$ is a root of $f(x, y, z) \pmod e$. Define $X = N^{\gamma+\beta-1}$, $Y = N^{\frac{1}{2}}$, and $Z = N^{\alpha}$, then we have $|x_0| < X$, $|y_0| < Y$, and $|z_0| < Z$, respectively.

Note that $f(x, y, z)$ can be further reduced by multiplying $(-a)^{-1} \pmod e$ to eliminate the coefficient of xz. Thus, we transform the equation (4) to

$$F(x, y, z) = A'x + B'xy + xz + C' \pmod e.$$

In order to construct the lattice, Zhao and Qi considered the polynomials

$$\begin{array}{l} g_{l,i,b}(x, y, z) := e^{m-l}x^i y^b F^l(x, y, z), \text{ for } l = 0, ..., m - 1;\ i = 1, ..., m - l;\ b = 0, 1; \\ h'_{j,l}(x, y, z) := e^{m-l}(az)^j F^l(x, y, z), \text{ for } l = 0, ..., m \text{ and } j = 0, ..., t; \\ h''_{j,l}(x, y, z) := e^{m-l}y^j F^l(x, y, z), \text{ for } l = 0, ..., m \text{ and } j = 1, ..., t; \end{array} \tag{5}$$

where m and t are two parameters in $\mathbb{N}$. It can be observed that $(x_0, y_0, z_0) = (k, q, r)$ is a root of $g_{l,i,b}(x, y, z)$, $h'_{j,l}(x, y, z)$, and $h''_{j,l}(x, y, z)$ modulo e^m.

Zhao and Qi solved the modular equation (4) by using the lattice reduction technique shown above. According to their calculation, the sufficient condition to find (x_0, y_0, z_0) is

$$\beta < \tfrac{1}{6}\alpha + \tfrac{13}{12} - \tfrac{1}{3}\sqrt{\alpha^2 + (6\gamma + 1)\alpha + \tfrac{12\gamma+1}{4}}. \tag{6}$$

This gives the security boundary of the Zhao-Qi attack. In the next section we revise the Zhao-Qi attack to further raise the above security boundary.

3 The Zhao-Qi Attack Revised

In this section we point out that the boundary of the Zhao-Qi attack can be further raised by using Corollary 1. Note that , in LSBS-RSA, according to Corollary 1, $\mathrm{LSB}_{1^{-}(\frac{1}{2}-\alpha)n}(p)$ can be computed efficiently in polynomial time in

n. We may denote $q = \widetilde{q} \cdot 2^{(\frac{1}{2}-\alpha)n} + q_0$ and replace y by $y \cdot 2^{(\frac{1}{2}-\alpha)n} + q_0$ in (4). Then, (4) is transformed to

$$f'(x, y, z) = x\left[(A - 2q_0) - 2ay - az\right] + 1,$$

where $A = N + 1$, and $a = 2^{(\frac{1}{2}-\alpha)n}$. Then $(x_0, y_0, z_0) = (k, \widetilde{q}, r)$ is a root of $f'(x, y, z) \pmod e$. Note that the size of the root y_0 is reduced when compared with that of $f(x, y, z)$. In fact, since the sizes of $\widetilde{q}$ and r are about αn bits, we may further simplify $f'(x, y, z)$ to

$$f''(x, y) = x\left[(A - 2q_0) - ay\right] + 1 \pmod e, \tag{7}$$

with the root $(k, 2\widetilde{q}+r) \pmod e$. The problem of solving (7) is similar to the *Small Inverse Problem* introduced in 1999 by Boneh and Durfee [3], [4]. However, we do not deal with this polynomial here, instead of considering another polynomial which will yield a better boundary. We show the detail in the next section.

4 Proposed Attack

According to Corollary 1, $\mathrm{LSB}_{1^{\sim}(1-2\alpha)n}(p+q)$ is known to attackers in an LSBS-RSA system. In this section we take this advantage to further extend the boundary of the revised Zhao-Qi attack. Denote

$$p + q = \overline{\phi} \cdot 2^{(1-2\alpha)n} + \phi_0,$$

where $\phi_0 = \mathrm{LSB}_{1^{\sim}(1-2\alpha)n}(p+q)$, and $\overline{\phi}$ is an unknown number of $(2\alpha - \frac{1}{2})n$ bits. Thus, the RSA equation can be derived to

$$ed = k\left[(N + 1 - \phi_0) - \left(\overline{\phi} \cdot 2^{(1-2\alpha)n}\right)\right] + 1.$$

Consider the modular equation

$$f^*(x, y) = x\,(B - by) + 1 \pmod e, \tag{8}$$

where $B = N + 1 - \phi_0$, $b = a^2 = 2^{(1-2\alpha)n}$, then $(x_0, y_0) = (k, \overline{\phi})$ is a root of $f(x, y) \pmod e$. Define $X = N^{\gamma+\beta-1}$, $Y = N^{2\alpha-\frac{1}{2}}$, we have $|x_0| < X$, and $|y_0| < Y$. Note that the form of the modular equation (8) is the same as the form in (7). In particular, the upper bound Y in (8) is much smaller than that in (7). This is the reason why we use the polynomial (8) instead of using (7) to attack short exponent LSBS-RSA, because the boundary derived from (8) will be better than the boundary derived from (7). However, this is not enough. We further simplify the equation (8) by multiplying $(-b)^{-1} \pmod e$ (note that this inverse exists since b is a power of 2 while e is odd). The advantage is that the coefficient of the leading monomial xy is 1 and hence we remove the powers of b from the determinant of the lattice and allow larger β while satisfying the determinant inequality.

Consequently, we get the alternative polynomial having $(x_0, y_0) = (k, \overline{\phi})$ as a zero root modulo e, that is

$$f(x, y) = xy + B'x + C' \pmod{e}, \tag{9}$$

where $B' = B(-b)^{-1} \pmod{e}$ and $C' = (-b)^{-1} \pmod{e}$. We construct the lattice by considering the polynomials

$$g_{i,l}(x, y) := x^i f^l(x, y) e^{m-l} \pmod{e^m}, \text{ for } l = 0, ..., m;\ i = 0, ..., m - l;$$
$$h_{j,l}(x, y) := y^j f^l(x, y) e^{m-l} \pmod{e^m}, \text{ for } l = 0, ..., m \text{ and } j = 1, ..., t.$$

Take the case $m = 3$, $t = 1$, for example. The coefficient matrix for this case is $M =$

ijl		1	x	xy	x^2	x^2y	x^2y^2	x^3	x^3y	x^3y^2	x^3y^3	y	xy^2	x^2y^3	x^3y^4
000	e^3	e^3													
100	xe^3		e^3X												
001	fe^2	-	-	e^2XY											
200	x^2e^3				e^3X^2										
101	xfe^2		-		-	e^2X^2Y									
002	f^2e	-	-	-	-	-	eX^2Y^2								
300	x^3e^3							e^3X^3							
201	x^2fe^2				-			-	e^2X^3Y						
102	xf^2e		-		-	-		-	-	eX^3Y^2					
003	f^3	-	-	-	-	-	-	-	-	-	X^3Y^3				
010	ye^3											e^3Y			
011	yfe^2			-								-	e^2XY^2		
012	yf^2e			-		-	-					-	-	eX^2Y^3	
013	yf^3			-		-	-		-	-	-	-	-	-	X^3Y^4

Let M_x and M_y denote the matrices with the coefficient vectors of $g_{i,l}(x, y)$ and $h_{j,l}(x, y)$, respectively. We have

$$\begin{aligned} \det(M_x) &= e^{\frac{m(m+1)(m+2)}{3}} \cdot X^{\frac{m(m+1)(m+2)}{3}} \cdot Y^{\frac{m(m+1)(m+2)}{6}} \\ \det(M_y) &= e^{\frac{tm(m+1)}{2}} \cdot X^{\frac{tm(m+1)}{2}} \cdot Y^{\frac{t(m+1)(m+t+1)}{2}}. \end{aligned} \tag{10}$$

Applying $X = e^{\frac{\gamma+\beta-1}{\gamma}}$, and $Y = e^{\frac{2\alpha-1/2}{\gamma}}$ to (10) yields

$$\begin{aligned} \det(M_x) &= e^{\frac{m(m+1)(m+2)}{3} + \left(\frac{\gamma+\beta-1}{\gamma} \cdot \frac{m(m+1)(m+2)}{3}\right) + \left(\frac{2\alpha-1/2}{\gamma} \cdot \frac{m(m+1)(m+2)}{6}\right)} \\ &= e^{\frac{m(m+1)(m+2)}{3} \cdot \left(2 + \frac{\alpha+\beta-5/4}{\gamma}\right)} \\ \det(M_y) &= e^{\frac{tm(m+1)}{2} + \left(\frac{\gamma+\beta-1}{\gamma} \cdot \frac{tm(m+1)}{2}\right) + \left(\frac{2\alpha-1/2}{\gamma} \cdot \frac{t(m+1)(m+t+1)}{2}\right)} \\ &= e^{\frac{tm(m+1)}{2} \cdot \left(2 + \frac{\beta-1}{\gamma}\right) + \left(\frac{2\alpha-1/2}{\gamma} \cdot \frac{t(m+1)(m+t+1)}{2}\right)}. \end{aligned}$$

Note that if we only consider the x-shift, *i.e.*, $g_{i,l}(x, y)$, to satisfy the requirement in Lemma 3 we have to set $\det(M_x) < e^{m\omega_x}$, where $\omega_x = \frac{(m+1)(m+2)}{2}$ is the dimension of M_x. Thus, we have

$$\frac{m(m+1)(m+2)}{3} \cdot \left(2 + \frac{\alpha+\beta-5/4}{\gamma}\right) < m \cdot \frac{(m+1)(m+2)}{2}. \tag{11}$$

Simplifying (11) yields

$$\alpha + \beta < \tfrac{5}{4} - \tfrac{\gamma}{2}. \tag{12}$$

Note that for the usual case ($\alpha = \frac{1}{2}$, $\gamma = 1$), we may attack RSA when $\beta < \frac{1}{4}$, which achieves the same boundary as the Wiener attack [25].

Moreover, we further include the y-shift, *i.e.*, $h_{j,l}(x, y)$, to our attack. By setting $\det(M) = \det(M_x) \cdot \det(M_y) < e^{m\omega}$, where $\omega = \frac{(m+1)(m+2)}{2} + t(m+1)$ is the dimension of M, we have

$$\tfrac{m(m+1)(m+2)}{3} \cdot \left(2 + \tfrac{\alpha+\beta-5/4}{\gamma}\right) + \tfrac{tm(m+1)}{2} \cdot \left(2 + \tfrac{\beta-1}{\gamma}\right) + \left(\tfrac{2\alpha-1/2}{\gamma} \cdot \tfrac{t(m+1)(m+t+1)}{2}\right)$$

$$< \tfrac{m(m+1)(m+2)}{2} + tm(m+1),$$

which leads to

$$\tfrac{m(m+2)}{3} \cdot \left(\tfrac{1}{2} + \tfrac{\alpha+\beta-5/4}{\gamma}\right) + \tfrac{tm}{2} \cdot \tfrac{\beta-1}{\gamma} + \left(\tfrac{2\alpha-1/2}{\gamma} \cdot \tfrac{t(m+t+1)}{2}\right) < 0, \tag{13}$$

After simplifying the left hand side of (13) as a quadratic polynomial with variable t we get

$$\left[\tfrac{2\alpha-1/2}{\gamma}\right] \cdot t^2 + \left[m\tfrac{\beta-1}{\gamma} + (m+1)\tfrac{2\alpha-1/2}{\gamma}\right] \cdot t + \left[\tfrac{2m(m+2)}{3}(\tfrac{1}{2} + \tfrac{\alpha+\beta-5/4}{\gamma})\right] < 0. \tag{14}$$

Note that the left hand side of (14) would be minimized at

$$t = \frac{-\left[m\frac{\beta-1}{\gamma} + (m+1)\frac{2\alpha-1/2}{\gamma}\right]}{2\left[\frac{2\alpha-1/2}{\gamma}\right]} = \frac{-[m(\beta-1) + (m+1)(2\alpha-1/2)]}{4\alpha-1} = \frac{(\frac{3}{2}-2\alpha-\beta)m - 2\alpha + \frac{1}{2}}{4\alpha-1}. \tag{15}$$

Plugging (15) in (14) yields

$$\left[\tfrac{2\alpha-1/2}{2\gamma}\right] \cdot \left(\tfrac{(\frac{3}{2}-2\alpha-\beta)m-2\alpha+\frac{1}{2}}{4\alpha-1}\right)^2 + \left[m\tfrac{\beta-1}{2\gamma} + (m+1)\tfrac{2\alpha-1/2}{2\gamma}\right] \cdot \tfrac{(\frac{3}{2}-2\alpha-\beta)m-2\alpha+\frac{1}{2}}{4\alpha-1}$$

$$+ \left[\tfrac{2m(m+2)}{3}(\tfrac{1}{2} + \tfrac{\alpha+\beta-5/4}{\gamma})\right] < 0. \tag{16}$$

Multiplying (16) by 2γ yields

$$\left(2\alpha - \tfrac{1}{2}\right) \cdot \left(\tfrac{(\frac{3}{2}-2\alpha-\beta)m-2\alpha+\frac{1}{2}}{4\alpha-1}\right)^2 + \left[m(\beta-1) + (m+1)\left(2\alpha - \tfrac{1}{2}\right)\right] \cdot \tfrac{(\frac{3}{2}-2\alpha-\beta)m-2\alpha+\frac{1}{2}}{4\alpha-1}$$

$$+ \tfrac{2m(m+2)}{3}(\tfrac{\gamma}{2} + \alpha + \beta - \tfrac{5}{4}) < 0.$$

After simplifying the first term and the second term we have

$$\tfrac{1}{2(4\alpha-1)} \cdot \left((\tfrac{3}{2} - 2\alpha - \beta)m - 2\alpha + \tfrac{1}{2}\right)^2 - \tfrac{1}{4\alpha-1} \cdot \left((\tfrac{3}{2} - 2\alpha - \beta)m - 2\alpha + \tfrac{1}{2}\right)^2$$

$$+ \left[\tfrac{2m(m+2)}{3}(\tfrac{\gamma}{2} + \alpha + \beta - \tfrac{5}{4})\right] < 0.$$

Combining the first term and the second term we get

$$\frac{-1}{2(4\alpha-1)} \cdot \left((\frac{3}{2}-2\alpha-\beta)m-2\alpha+\frac{1}{2}\right)^2 + \left[\frac{2m(m+2)}{3}(\frac{\gamma}{2}+\alpha+\beta-\frac{5}{4})\right] < 0$$

which is simplified to

$$\frac{2m(m+2)}{3}(\frac{\gamma}{2}+\alpha+\beta-\frac{5}{4}) \cdot 2\,(4\alpha-1)) < \left((\frac{3}{2}-2\alpha-\beta)m-2\alpha+\frac{1}{2}\right)^2.$$

Thus, we get the inequality

$$(2\gamma+4\alpha+4\beta-5)\,(4\alpha-1) < \frac{3\left((\frac{3}{2}-2\alpha-\beta)m-2\alpha+\frac{1}{2}\right)^2}{m(m+2)} = \frac{3\left((\frac{3}{2}-2\alpha-\beta)-\frac{2\alpha}{m}+\frac{1}{2m}\right)^2}{1+\frac{2}{m}}. \tag{17}$$

As m goes to infinity, (17) becomes

$$(2\gamma+4\alpha+4\beta-5)\,(4\alpha-1) < 3\left(\frac{3}{2}-2\alpha-\beta\right)^2. \tag{18}$$

We give more discussions in the next section.

5 Further Discussions

5.1 The Summary of Our Attack

In conclusion, the boundary that our attack can succeed is

$$\beta < \frac{2}{3}\alpha + \frac{5}{6} - \frac{4}{3}\sqrt{\alpha^2 + (\frac{3}{2}\gamma - \frac{1}{2})\alpha - \frac{6\gamma-1}{16}},$$

where $\frac{1}{4} \le \alpha \le \frac{1}{2}$. For the case $\gamma = 1$, we have the boundary

$$\beta < \frac{2}{3}\alpha + \frac{5}{6} - \frac{4}{3}\sqrt{\alpha^2 + \alpha - \frac{5}{16}}. \tag{19}$$

The curve of (19) is shown in Fig 1. We also show the other attacks, which includes the Wiener attack, Boneh-Durfee attack, and the Analogue Fermat factoring. As can be seen in Fig 1, if p and q share the $\frac{n}{4}$ least significant bits at least, *i.e.*, $\alpha \le 0.25$, the Analogue Fermat factoring can factor N efficiently. The Wiener attack and the Boneh-Durfee attack (short for B-D attack) work in the case $\beta < \frac{1}{4}$ and $\beta < 0.284$, respectively. We should point out in B-D attack [3], [4], Boneh and Durfee use the geometrically progressive matrices to eliminate the larger terms in the coefficient matrix, and thus the upper bound is further extended from $d < N^{0.284}$ to $d < N^{0.292}$. This technique can also be applied to our method but we do not discuss it here.

5.2 Experiments

We have performed the experiments on a server containing Intel processors of 2.4 GHz Core 2 Quad, with 2 GB Memory. The lattice basis reductions are done

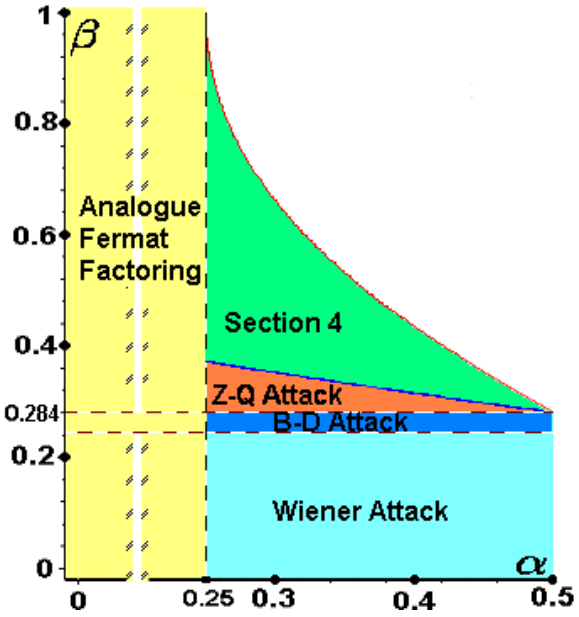

Fig. 1. Insecure Region of α and β for which LSBS-RSA with $\gamma = 1$

using Shoup's NTL [14]. We have to mention that, like the Boneh-Durfee attack, our attack is also heuristic since the resultant computations may fail even with low probability. Also, we just experimented for the samples on LSBS-RSA with short private exponent, and $e \approx N$ (*i.e.*, $\gamma \approx 1$). Note that the size of 1024 bits, or 2048 bits for the modulus are often used in the current computational environment. However, we just experimented for the size of 128 bits for the reason of simplicity. The experimental results are shown in the following.

n	α	d	β	m	t	Rank of Lattice	Running Time	Advantage over Z-Q Attack
128 bits	0.275	90 bits	0.704	5	12	93	36 sec	43 bits
128 bits	0.300	77 bits	0.607	5	7	63	9.5 sec	31 bits
128 bits	0.350	61 bits	0.478	5	3	39	3.0 sec	17 bits
128 bits	0.425	45 bits	0.350	5	2	33	0.7 sec	5 bits

The entries for β in the table are the tested values for which the attacks succeeded. As can be seen in the last column of the table, our attacks achieved the higher boundary than the one of the Zhao-Qi attack. In addition, we have to point out that considering LSBS-RSA with $\gamma < 1$ (*i.e.*, $e << N$) and $\beta < 1$ (*i.e.*, $d << N$) is not practical. Up to now there is no research about designing LSBS-RSA with short private and public exponents simultaneously. The most related work for designing short private and public exponents RSA was proposed by Sun *et. al.*[16], [17], but the modulus primes in their key-generation schemes cannot be determined as desired. Hence, it seems meaningless to cryptanalyze

$\gamma = \log_N(e)$	$\gamma = 1.0$	$\gamma = 0.9$	$\gamma = 0.86$	$\gamma = 0.8$	$\gamma = 0.7$	$\gamma = 0.6$	$\gamma = 0.55$
$\alpha = 0.5$	0.284	0.323	0.339	0.364	0.407	0.452	0.476
$\alpha = 0.4$	0.437	0.468	0.480	0.500	0.534	0.571	0.590
$\alpha = 0.3$	0.662	0.681	0.688	0.700	0.721	0.743	0.754
$\alpha = 0.25$	1	1	1	1	1	1	1

Table 1. The upper bound or lower bound of β for which our attack can succeed in LSBS-RSA.

the security of short exponent LSBS-RSA with $\gamma < 1$. Even so, in Table 1 we still summarize the largest β for which the proposed attack can succeed.

5.3 Further Improvement

To further extend the boundary of our attack, we may focus on the approximation to $p + q$. Generally, $p + q$ is estimated as $2\lceil\sqrt{N}\rceil$. Sun, Wu, & Chen [18] proposed a method, called *EPF*, to estimate the most significant bits of $p + q$. With this technique, we may reduce the quantity of Y in (8) and this may conduct to a better boundary of LSBS-RSA for security. More precisely, suppose that $p+q$ is estimated as ϕ_E, with the error $|(p + q) - \phi_E| < 2^m$, where $m < \frac{n}{2}$, then the RSA equation can be represented as

$$ed = x\left[(N + 1) - (\phi_E + y)\right] + 1,$$

where $x_0 = k$, and $y_0 < 2^m$ are two unknown numbers. The above equation gives us a motivation to combine de Weger's result [24] with our attack. Next, we briefly describe it.

5.4 LSBS-RSA with Small Prime Difference

Recall that $p-q = r \cdot 2^{(\frac{1}{2}-\alpha)n}$, for some integer r. In general, the quantity of r is about $2^{\alpha n}$. Here we consider the case that bit-length of r is much smaller than αn. This means p and q share a number of the most significant bits. The cryptanalysis of this RSA modulus had been analyzed by de Weger [24]. We suppose that p and q share the α_M most significant bits, which implies $p - q < 2^{\frac{n}{2}-\alpha_M}$, and share the α_L least significant bits, which implies $p-q = r_L \cdot 2^{\alpha_L}$ for some integer r_L. Thus, $p - q$ can be represented as

$$p - q = r_L \cdot 2^{\alpha_L}, \text{ where } r_L < 2^{\frac{n}{2}-(\alpha_M+\alpha_L)}.$$

And then, $p + q$ can be computed from the identity:

$$(p + q)^2 = (p - q)^2 + 4N = r_L^2 \cdot 2^{2\alpha_L} + 4N.$$

Using the representation of $p + q$ above may yield a better boundary for the lattice attack on this kind of RSA variant. However, we do not show the detail here but leave it in the full version.

6 Conclusion and Future Work

In this paper, we give a revised version of the Zhao-Qi attack to further raise the security boundary of LSBS-RSA. In addition, we also propose a method by considering another polynomial to attacking LSBS-RSA, which conducts to a better result compared with the Zhao-Qi attack. Our result shows that LSBS-RSA is getting more vulnerable as smaller exponents or more number of primes sharing bits.

An interesting question is how to design an LSBS-RSA with short public and private exponents simultaneously. Note that in Sun *et. al.*'s schemes [16], [17], we cannot choose modulus primes randomly in order to produce desired public and private exponents. Up to now it is still an open problem to design such scheme to achieve balanced short exponents RSA with prime sharing a large number of least (or most) significant bits. Conversely, the cryptanalysis of such RSA variant, if it exists, is worth to research as well.

Although LSBS-RSA is beneficial to the computational efficiency in several applications, such as server-aided signature generation [6], we have to indicate using LSBS-RSA also raises the risk in the security [21], [22], [24], [26]. We believe it is a trade-off between the efficiency and the security level, and thus one should be more careful in using such RSA variants.

Acknowledgment

The work was supported in part by the National Science Council, Taiwan, under Contract No. NSC 96-2628-E-007-025-MY3, the Singapore National Research Foundation under Research Grant NRF-CRP2-2007-03, the Singapore Ministry of Education under Research Grant T206B2204 and the Australian Research Council under ARC Discovery Project DP0665035. Ron Steinfeld's work was supported by a Macquarie University Research Fellowship.

References

1. D. Boneh, G. Durfee and Y. Frankel, "An Attacks on RSA Given a Small Fraction of the Private Key Bits," Advanced in Cryptology – ASIACRYPT '98, LNCS 1514, Springer-Verlag, pp.25-34, 1998.
2. D. Boneh, G. Durfee and 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.
3. D. Boneh and G. Durfee, "Cryptanalysis of RSA with private key d less than $N^{0.292}$. In proceedings Eurocrypt' 99, LNCS, vol. 1952, Springer-Verlag, pp. 1-11, 1999.
4. D. Boneh and G. Durfee. Cryptanalysis of RSA with private key d less than $N^{0.292}$,". *IEEE Transactions on Information Theory*, 46(4):1339–1349, July 2000.
5. J. Blömer and A. May, "New Partial Key Exposure Attacks on RSA," Advanced in Cryptology – CRYPTO'03, LNCS 2729, Springer-Verlag, pp.27-43, 2003.

6. M. Bellare and P. Rogaway, "The exact security of digital signatures: How to sign with RSA and Rabin", Advanced in Cryptology – EUROCRYPTO'96, LNCS 1070, Springer-Verlag, pp.399-416, 1996.
7. D. Coppersmith, "Finding a Small Root of a Bivariate Integer Equation; Factoring with High Bits Known", Proceedings of Eurocrypt'96, LNCS 1070, pp. 178–189, 1996.
8. J-S. Coron, "Finding Small Roots of Bivariate Integer Polynomial Equations Revisited", Advanced in Cryptology – EUROCRYPTO'04, LNCS 3027, Springer-Verlag, pp.492-505, 2004.
9. J-S. Coron, "Finding Small Roots of Bivariate Integer Polynomial Equations: A Direct Approach," Advanced in Cryptology – CRYPTO'07, LNCS 4622, Springer-Verlag, pp.379-394, 2007.
10. G. Durfee, P. Q. Nguyen, "Cryptanalysis of the RSA Schemes with Short Secret Exponent form Asiacrypt '99," Advances in Cryptology-Asiacrypt'00, LNCS 1976, Springer-Verlag, pp.1-11, 2000.
11. M. Ernst, E. Jochemsz, A. May, B. de Weger, "Partial Key Exposure Attacks on RSA up to Full Size Exponents," Advanced in Cryptology – EUROCRYPT'05, Springer-Verlag, pp.371-386, 2005.
12. J. Hastad, "Solving simultaneous modular equations of low degree", SIAM J. of Computing, Vol. 17, pp.336-341, 1988.
13. N. Howgrave-Graham, "Finding small roots of univariate modular equations revisited," in Proceedings of Cryptography and Coding, LNCS, vol. 1355, Springer-Verlag, pp.131-142, 1997.
14. Victor Shoup. NTL: A Library for doing Number Theory, online available at http://shoup.net/ntl
15. A. Lenstra, H. Lenstra, L. Lovasz, "Factoring Polynomials with Rational Coefficients," Mathematiche Annalen 261, pp.515-534.
16. H.-M. Sun, W.-C. Yang and C.-S. Laih, "On the design of RSA with short secret exponent", Proceedings of Asiacrypt'99, LNCS 1716, pp. 150–164, 1999.
17. H.-M. Sun and C.-T. Yang. RSA with balanced short exponents and its application to entity authentication. *Public Key Cryptography - PKC 2005*, volume 3386 of *Lecture Notes in Computer Science*, pp. 199–215. Springer, 2005.
18. H.-M. Sun, M.-E. Wu, and Y.-H. Chen, "Estimating the Prime Factors of an RSA Modulus and an Extension of the Wiener Attack," in *Proc. Applied Cryptography and Network Security 2007 — ACNS'07*, ser. Lecture Notes in Computer Science, J. Katz et al., Eds. Heidelberg: Springer, 2007, vol. 4521, pp. 116-128.
19. Hung-Min Sun, Mu-En Wu, Huaxiong Wang, and Jian Guo: On the Improvement of the BDF Attack on LSBS-RSA. ACISP 2008: 84-97
20. R. Rivest, A. Shamir and L. Aldeman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", *Communications of the ACM* , Vol. 21, No.2, pp.120-126, 1978.
21. R. Steinfeld, and Y. Zheng, "An Advantage of Low-Exponent RSA with Modulus Primes Sharing Least Significant Bits," in *Topic in Cryptology - CT-RSA 2001*, ser. Lecture Notes in Computer Science, D. Naccache, Ed. Heidelberg: Springer, 2001, vol. 2020, pp. 52-62.
22. R. Steinfeld, and Y. Zheng, "On the Security of RSA with Primes Sharing Least-Significant Bits," *Appl. Algebra Eng. Commun. Comput.*, Heidelberg: Springer, 2004, vol. 15, no. 3(4), pp. 179-200.
23. E. R. Verheul and H. C. A. van Tilborg. Cryptanalysis of '*less short*' RSA secret exponents. *Appl. Algebra Eng. Commun.*

24. B. de Weger, "Cryptanalysis of RSA with small prime difference", *Applicable Algebra in Engineering, Communication and Computing*, Vol. 13, pp. 17-28, 2002.
25. M. J. Wiener. Cryptanalysis of short RSA secret exponents. *IEEE Trans. Information Theory*, 36(3):553–559, May 1990.
26. Y.-D. Zhao, and W.-F. Qi, "Small Private-Exponent Attack on RSA with Primes Sharing Bits," in *Proc. Information Security Conference 2007 — ISC 2007*, ser. Lecture Notes in Computer Science, J. Garay et al., Eds. Heidelberg: Springer, 2007, vol. 4779, pp. 221-229.