Discrete Applied Mathematics 203 (2016) 127–133

Contents lists available at ScienceDirect

Discrete Applied Mathematics

journal homepage: www.elsevier.com/locate/dam

Revisiting Prime Power RSA

Santanu Sarkar

Department of Mathematics, Indian Institute of Technology Madras, Sardar Patel Road, Chennai 600 036, India

ARTICLE INFO

Article history:
Received 2 April 2014
Received in revised form 27 August 2015
Accepted 1 October 2015
Available online 27 October 2015

Keywords:
Partial key exposure
Lattice
Prime Power RSA
Small decryption exponent

ABSTRACT

Recently Sarkar (DCC 2014) has proposed a new attack on small decryption exponent when RSA Modulus is of the form $N = p^r q$ for $r \geq 2$. This variant is known as Prime Power RSA. The work of Sarkar improves the result of May (PKC 2004) when $r \leq 5$. In this paper, we improve the work of Sarkar when $2 < r \leq 8$.

We also study partial key exposure attack on Prime Power RSA. Our result improves the works of May (PKC 2004) when $r \leq 8$ and the decryption exponent $d < N^{\frac{1}{r+1}+\frac{3r-2\sqrt{3r+3}+3}{3(r+1)}}$.

1. Introduction

In the domain of public key cryptography, RSA has been the most popular cipher since its inception in 1978 by Rivest, Shamir and Adleman. Wiener [22] presented an important result on RSA by showing that one can factor N in polynomial time if the decryption exponent $d < \frac{1}{3}N^{\frac{1}{4}}$. Later using the idea of Coppersmith [6], Boneh and Durfee [3] improved this bound up to $d < N^{0.292}$.

There are several RSA variants proposed in the literature for efficiency and security point of view. In this paper, we consider Prime Power RSA, where RSA modulus N is of the form $N = p^r q$ where $r \geq 2$. The modulus $N = p^2 q$ was first used by Fujioka et al. in Eurocrypt 1991 [9]. In Eurocrypt 1998, Okamoto et al. [19] also used $N = p^2 q$ to design a public key crypto system.

There are two variants of Prime Power RSA. In the first variant $ed \equiv 1 \bmod p^{r-1}(p-1)(q-1)$, where as in the second variant $ed \equiv 1 \bmod (p-1)(q-1)$. In [11], authors proved that polynomial time factorization is possible for the second variant if $d < N^{\frac{2-\sqrt{2}}{r+1}}$.

For the first variant, Takagi in Crypto 1998 [21] proved that when $d \leq N^{\frac{1}{2(r+1)}}$, one can factor N in polynomial time. Later in PKC 2004, May [18] improved this bound up to $d < N^{\max\left\{\frac{r}{(r+1)^2}, (\frac{r-1}{r+1})^2\right\}}$. Recently, Lu et al. [16,17] have shown that one can factor N when $d < N^{\frac{r(r-1)}{(r+1)^2}}$, which improves the work of [18].

Sarkar [20] has considered the polynomial $f_e(x, y, z) = 1 + x(N - y^r - y^{r-1}z + y^{r-1})$ over $\mathbb{Z}_e$ whose root is $(x_0, y_0, z_0) = (b, p, q)$, where $ed = 1 + b\phi(N)$ to analyze the RSA modulus $N = p^r q$. In this paper we consider the same polynomial. But our lattice construction to solve this polynomial is different from [20]. As a result, we improve the existing works of [18,20,16] when $r = 3, 4$.

Partial exposure on d. In Crypto 1996, Kocher [12] first proposed a novel attack which is known as partial key exposure attack. He showed that an attacker can get a few bits of d by timing characteristic of an RSA implementing device. Fault

E-mail address: sarkar.santanu.bir@gmail.com.

http://dx.doi.org/10.1016/j.dam.2015.10.003
0166-218X/

attacks [2] and power analysis [13] are other important side channel attacks in this direction. Boneh, Durfee and Frankel [4] first proposed polynomial time algorithms when the attacker knows a few bits of the decryption exponent. The approach of [4] works only when the upper bound on e is $\sqrt{N}$. Later this constraint was removed by Blömer et al. in Crypto 2003 [1] and Ernst et al. in Eurocrypt 2005 [8].

May in PKC 2004 [18] studied partial key exposure attack on Prime Power RSA. He showed that one can factor N in polynomial time from the knowledge of d_0 where $|d - d_0| < N^{\max\left\{\frac{r}{(r+1)^2}, (\frac{r-1}{r+1})^2\right\}}$ when RSA modulus $N = p^r q$. Lu et al. [16] improve the work of [18] and show that factorization of N can be possible when $|d - d_0| < N^{\frac{r(r-1)}{(r+1)^2}}$. So in particular, when $r = 2$, approach of [16] works when $|d - d_0| < N^{0.22}$. We have improved this bound up to $N^{0.33}$. Unfortunately, our method works only when $d < N^{0.67}$.

2. Useful lemmas and preliminaries

Consider w many linearly independent vectors $b_1, \ldots, b_w \in \mathbb{R}^n$. The set

$$L = \left\{ \boldsymbol{b} : \boldsymbol{b} = \sum_{i=1}^{w} c_i b_i, \;\; c_1, \ldots, c_w \in \mathbb{Z} \right\}$$

is called an w dimensional lattice with basis $B = \{b_1, \ldots, b_w\}$. A lattice is of full rank when $w = n$ and in this paper we only use such lattices. The determinant of L is defined as $\det(L) = \det(M)$, where the rows of M are the vectors from B. When $b_1, \ldots, b_w \in \mathbb{Z}^n$, the lattice L is called an integer lattice.

In 1982, Lenstra, Lenstra and Lovász [15] proposed a polynomial time algorithm (known as LLL algorithm) to obtain another basis with some useful properties: given a basis $b_1, \ldots, b_w$ of a lattice L, LLL algorithm gives a (reduced) basis $u_1, \ldots, u_w$ with

$$\|u_1\| \leq \|u_2\| \leq \|u_3\| \leq 2^{\frac{w(w-1)}{4(w-2)}} \det(L)^{\frac{1}{w-2}}. \tag{1}$$

In [6], Coppersmith formulated seminal ideas to find small roots of modular polynomials in single variable and also of polynomials in two variables over the integers. These deterministic techniques have many important consequences in cryptography. The idea of [6] can also be extended to more than two variables, but the method becomes a heuristic in that case. The following result due to Howgrave-Graham [10] gives a sufficient condition under which modular roots become the roots over integers for polynomials in three variables.

Theorem 1. *Let $g(x, y, z)$ be a polynomial with integer coefficients which is a sum of w many monomials. Suppose that*
1. *$g(x_0, y_0, z_0) \equiv 0 \bmod e^m$ for positive integers e, m and $|x_0| < X$, $|y_0| < Y$, $|z_0| < Z$.*
2. *$\|g(xX, yY, zZ)\| < \frac{e^m}{\sqrt{w}}$,*

Then $g(x_0, y_0, z_0) = 0$ holds over integers.

Suppose we have w polynomials $b_1, \ldots, b_w$ in the variables x, y, z such that $b_1(x_0, y_0, z_0) = \cdots = b_w(x_0, y_0, z_0) = 0 \bmod e^m$ with $|x_0| < X$, $|y_0| < Y$ and $|z_0| < Z$. Now we construct a lattice L with the coefficient vectors of $b_1(xX, yY, zZ), \ldots, b_w(xX, yY, zZ)$. Since lattice reduction is a series of elementary row operations, after reduction, we get three polynomials $u_1(x, y, z)$, $u_2(x, y, z)$ and $u_3(x, y, z)$ such that

$$u_1(x_0, y_0, z_0) = u_2(x_0, y_0, z_0) = u_3(x_0, y_0, z_0) = 0 \bmod e^m$$

which correspond to first three vectors of the reduced basis. Also by the property of LLL algorithm, we have

$$\|u_1(xX, yY, zZ)\| \leq \|u_2(xX, yY, zZ)\| \leq \|u_3(xX, yY, zZ)\| \leq 2^{\frac{w(w-1)}{4(w-2)}} \det(L)^{\frac{1}{w-2}}.$$

Hence by Theorem 1, if

$$2^{\frac{w(w-1)}{4(w-2)}} \det(L)^{\frac{1}{w-2}} < \frac{e^m}{\sqrt{w}},$$

then we have $u_1(x_0, y_0, z_0) = u_2(x_0, y_0, z_0) = u_3(x_0, y_0, z_0) = 0$. The required condition can be taken as $\det(L)^{\frac{1}{w-2}} < e^m$ by neglecting the terms $2^{\frac{w(w-1)}{4(w-2)}}$ and $\frac{1}{\sqrt{w}}$. Again if $w \gg 2$, we can simplify the condition as $(\det(L))^{\frac{1}{w}} < e^m$.

Thus if $\det(L) < e^{mw}$, after lattice reduction we will get three polynomials $u_1(x_0, y_0, z_0) = u_2(x_0, y_0, z_0) = u_3(x_0, y_0, z_0) = 0$. We want to find x_0, y_0, z_0 from u_1, u_2, u_3. Although our technique works in practice as noted from the experiments we perform, we need the following heuristic assumption for theoretical results.

Assumption 1. Our lattice-based construction yields algebraically independent polynomials. The common roots of these polynomials can be efficiently computed by using techniques like calculation of the resultants or finding a Gröbner basis.

It is important to fix the degrees of the polynomials, since time complexity of the Gröbner basis computation is in general double-exponential in the degrees of the polynomials [7]. For this reason, the dimension of the lattice that we construct should not be large.

3. Small decryption exponent attack on Prime Power RSA

In this section we will consider the case when RSA modulus is of the form $N = p^r q$ where $r \geq 2$.

Theorem 2. *Let $N = p^r q$ be an RSA modulus with $p \approx q \approx N^{\frac{1}{r+1}}$. Let the public exponent $e(\approx N)$ and private exponent d satisfies $ed \equiv 1 \mod \phi(N)$. Then under Assumption 1, N can be factored in polynomial time if $d \leq N^{\tau(r)}$, where $\tau(r)$ is a function of r.*

Proof. We have $ed \equiv 1 \mod \phi(N)$ where $N = p^r q$. So we can write $ed = 1 + b(N - p^r - p^{r-1}q + p^{r-1})$. Now we want to find the root $(x_0, y_0, z_0) = (b, p, q)$ modulo e of the polynomial

$$f_e(x, y, z) = 1 + x(N - y^r - y^{r-1}z + y^{r-1}).$$

Let $d \approx N^{\delta}$. Since e is of order N, we have $b \approx N^{\delta}$. Let $X = N^{\delta}$, $Y = Z = N^{\frac{1}{r+1}}$. Clearly, (X, Y, Z) provides the upper bounds of the elements in the root (x_0, y_0, z_0), neglecting any small constant. Note that $y_0^r z_0 = N$. Now we define a set of polynomials which will be used to construct a lattice.

For integers $m, a, t \geq 0$, we consider the following polynomials

$$g_{i,j,k}(x, y, z) = x^i y^{(r-1)i+k} z^{i+a} f_e^j(x, y, z) \quad \text{where } i = 0, \ldots, m,\ j = 0, \ldots, m - i,\ k = 0, \ldots, r \quad \text{and}$$
$$g'_{i,j,0}(x, y, z) = y^{(r+j)} z^a f_e^i(x, y, z) \quad \text{where } i = 0, \ldots, m,\ j = 1, \ldots, t - r.$$

We replace each occurrence of the monomial $y^r z$ in $g_{i,j,k}$ by N. Let the new polynomial be $h''_{i,j,k}$. Now we want to make the coefficient of the monomial $x^{i+j}\, y^{k+(r-1)i+rj-rl} z^{i+a-l}$ in $h''_{i,j,k}$ to be 1, where $l = \min\left\{\left\lfloor \frac{k+(r-1)i+rj}{r} \right\rfloor, i + a\right\}$. Let A be its coefficient in $h''_{i,j,k}$. Assume $\gcd(A, e) = 1$. Let $AB \equiv 1 \mod e^m$.

Now consider the set of polynomials

$$h_{i,j,k}(x, y, z) = B h''_{i,j,k}(x, y, z) e^{m-j}.$$

Similarly construct $h'_{i,j,0}(x, y, z)$ from $g'_{i,j,0}(x, y, z)$. Note that both

$$h_{i,j,k}(x_0, y_0, z_0) = h'_{i,j,k}(x_0, y_0, z_0) = 0 \mod e^m.$$

Next, we form a lattice L by taking the coefficient vectors of the shift polynomials $h_{i,j,k}(xX, yY, zZ)$ and $h'_{i,j,k}(xX, yY, zZ)$ as basis. Here we choose polynomials in a clever way to reduce the size of the determinant of the corresponding lattice.

Now dimension w of L is given by $w = \sum_{i=0}^{m} \sum_{j=0}^{m-i} \sum_{k=0}^{r} 1 + \sum_{i=0}^{m} \sum_{j=1}^{t-r} 1 = \frac{r+1}{2} m^2 + mt + o(m)$. Let the determinant of L be $\det(L) = X^{s_x} Y^{s_y} Z^{s_z} e^{s_e}$. Now $s_x = \sum_{i=0}^{m} \sum_{j=0}^{m-i} \sum_{k=0}^{r} (i + j) + \sum_{i=0}^{m} \sum_{j=1}^{t-r} i = \frac{m^3(r+1)}{3} + \frac{m^2 t}{2} + o(m^3)$. Similarly, $s_e = \frac{m^3(r+1)}{3} + \frac{m^2 t}{2} + o(m^3)$.

During the calculations of s_y, we assume either $m > a$ or $a - \frac{t}{r} < m < a$.

Now

$$\begin{aligned} s_y &= \sum_{i=0}^{m} \sum_{j=0}^{m-i} \sum_{k=0}^{r} \left((r-1)i + k + rj - r \min\left(\left\lfloor \frac{(r-1)i + k + rj}{r} \right\rfloor, i + a \right) \right) \\ &\quad + \sum_{i=0}^{m} \sum_{j=1}^{t-r} \left(ri + r + j - r \min\left(\left\lfloor \frac{ri + r + j}{r} \right\rfloor, a \right) \right) \\ &= \frac{(3a^2 m - 3am^2 + m^3) r^2}{6} - \frac{(2am - m^2) rt}{2} + \frac{mt^2}{2} - \frac{(a^3 r^3 - 3a^2 r^2 t + 3art^2 - t^3)}{6r} + o(m^3). \end{aligned}$$

Assuming $m \geq a - \frac{t}{r}$, we have

$$\begin{aligned} s_z &= \sum_{i=0}^{m} \sum_{j=0}^{m-i} \sum_{k=0}^{r} \left(i + a - \min\left(\left\lfloor \frac{(r-1)i + k + rj}{r} \right\rfloor, i + a \right) \right) + \sum_{i=0}^{m} \sum_{j=1}^{t-r} \left(a - \min\left(\left\lfloor \frac{ri + r + j}{r} \right\rfloor, a \right) \right) \\ &= \frac{\frac{ma^2 r^3}{2} - \frac{a^3 r^3}{6} + \frac{m^2 ar^2}{2} + \frac{a^2 tr^2}{2} + \frac{m^3 r}{6} - \frac{at^2 r}{2} + \frac{t^3}{6}}{r^2} + o(m^3). \end{aligned}$$

One gets the root (x_0, y_0, z_0) using lattice reduction over L, if $\det(L) < e^{mw}$.

Table 1
Numerical upper bound of δ for different values of r.

r	[18]	[20]	[16]	$\tau(r)$
2	0.222	0.395	0.222	0.395
3	0.250	0.410	0.375	0.461
4	0.360	0.437	0.480	0.508
5	0.444	0.464	0.555	0.545
6	0.510	0.489	0.612	0.574
7	0.562	0.512	0.656	0.598
8	0.605	0.532	0.691	0.619
9	0.640	0.549	0.720	0.637
10	0.669	0.565	0.744	0.653

Table 2
Numerical values of δ for different parameters.

r	m	a	t	δ	Lattice dimension
3	22	20	49	0.42	2162
4	14	15	48	0.44	1260
5	11	12	44	0.45	936
6	19	26	119	0.52	3730

Let $a = \tau_1 m$ and $t = \tau_2 m$, where τ_1, τ_2 are non-negative real numbers. Now putting the values of $\det(L)$ and w in the condition $\det(L) < e^{mw}$, we need

$$\eta(\tau_1, \tau_2) = -\frac{1}{6}\delta(2r + 3\tau_2 + 2) + \frac{1}{6}r + \frac{1}{2}\tau_2 - \frac{\left(3\tau_1^2 - 3\tau_1 + 1\right)r^2 - 3(2\tau_1 - 1)r\tau_2 + 3\tau_2^2}{6(r+1)} + \frac{(\tau_1 r - \tau_2)^3\left(\frac{1}{r} + \frac{1}{r^2}\right) - \frac{3\tau_1^2 r^3 + 3\tau_1 r^2 + r}{r^2}}{6(r+1)} + \frac{1}{6} > 0.$$

For a fixed δ, we will take the partial derivative of η with respect to τ_1, τ_2 and equate each of them to 0, we get $\tau_1 = -\frac{(\delta-1)r^2 + (\delta-1)r + 1}{2r}$ and

$$\tau_2 = -\frac{(\delta-1)r^3 + 2\delta r^2 + \delta r - 2\sqrt{-(\delta-1)r^2 - (2\delta-1)r - \delta + 1}\,r + 1}{2(r+1)}.$$

Now put these values of τ_1, τ_2 in η. Inequality $\eta > 0$ gives an upper bound of δ. Call this upper bound $\tau(r)$. So when $\delta \leq \tau(r)$, $\eta > 0$.

Now when $\eta > 0$, we get three polynomials f_0, f_1, f_2 after lattice reduction such that $f_0(x_0, y_0, z_0) = f_1(x_0, y_0, z_0) = f_2(x_0, y_0, z_0) = 0$. Under Assumption 1, we can extract x_0, y_0, z_0. □

Exact expression of $\tau(r)$ in Theorem 2 is very complicated. Hence in Table 1, we present a few values of $\tau(r)$ for different values of r. One can note that from Table 1, our method will be better than the existing works for $r = 3, 4$. Also in Table 2, we present a few numerical values of δ for different values of r, m, a, t. Our result is better than the work of [20] and [18] if $2 < r \leq 8$. When $r > 4$, the work of [16] is better than our approach. However, Boneh et al. in Crypto 1999 [5] proved that a fraction of $\frac{1}{r+1}$ fraction of bits of MSBs of p are sufficient for polynomial time factorization. Also for large r, Elliptic Method Factorization [14] will be efficient because size of primes would be reduced for larger values of r. Hence for all practical purpose value of r cannot be large.

Experimental results. We have implemented the code in SAGE 5.12 on a Linux Mint 12. The hardware platform is HP Compaq 6200 Pro MT PC with a 3.4 GHz Inter(R) Core i7-2600 CPU. Gröbner basis always contains a polynomial of the form $y - p$. Hence we can always extract the root successfully. We present the experimental results for the following cases: $r = 3$ and δ is in the range 0.270–0.341; $r = 4$ and $\delta = 0.362$ (see Table 3).

Remark 1. Experimental results presented in [20] are up to $\delta = 0.27$. In particular, when $\delta = 0.27$, the lattice constructed in [20] is of dimension 220 when $r = 3$. From the above table we can see that the dimension of the lattice in this construction is 102 when $r = 3$ and $\delta = 0.27$.

4. Partial key exposure attack on Prime Power RSA

We will start with the following lemma. Our proof is similar to [1].

Table 3
Experimental results for 1024-bit $N = p^r q$.

r	m	a	t	δ	LD	Time in seconds	
						LLL Algorithm	Gröbner basis
	5	3	6	0.270	102	1700.05	120.76
	5	4	9	0.288	120	7761.85	1364.29
	5	4	10	0.291	126	10347.65	1576.04
3	6	4	8	0.301	147	15875.70	2433.46
	6	5	11	0.313	168	47205.86	10018.92
	7	5	10	0.325	200	94117.08	13793.54
	7	5	12	0.331	216	114720.15	17936.09
	8	6	12	0.341	261	345864.51	52022.77
4	7	6	16	0.362	276	340649.58	107403.42

Lemma 1. *Let $N = p^r q$ be an RSA modulus with $p \approx q \approx N^{\frac{1}{r+1}}$. Let the public exponent $e(\approx N)$ and private exponent $d(\approx N^{\delta})$ satisfies $ed = 1 + b\phi(N)$. Given an approximation d_0 of d with $|d - d_0| < N^{\beta}$, one can find out an approximation b_0 of b such that $|b - b_0| < N^{\lambda}$ where $\lambda = \max\left\{\beta, \delta - \frac{1}{r+1}\right\}$.*

Proof. Let $b_0 = \lfloor \frac{ed_0}{N} \rfloor$. Note that $b = \frac{ed-1}{N-p^r-p^{r-1}q+p^{r-1}}$.

So

$$\begin{aligned}
\left|b - b_0\right| &\approx \left|\frac{ed_0}{N} - \frac{ed}{N - p^r - p^{r-1}q + p^{r-1}}\right| \\
&\leq \frac{eN|d - d_0|}{N\left(N - p^r - p^{r-1}q + p^{r-1}\right)} + \frac{ed_0\left(p^r + p^{r-1}q - p^{r-1}\right)}{N\left(N - p^r - p^{r-1}q + p^{r-1}\right)} \\
&< N^{\beta} + N^{\delta + \frac{r}{r+1} - 1} \\
&= N^{\beta} + N^{\delta - \frac{1}{r+1}} \\
&\approx N^{\lambda}.
\end{aligned}$$

Hence the result. □

So from an approximation of d, one can find an approximation of b. We will use this idea to prove the following result.

Theorem 3. *Let $N = p^r q$ be an RSA modulus with $p \approx q \approx N^{\frac{1}{r+1}}$. Let the public exponent $e(\approx N)$ and private exponent $d(\approx N^{\delta})$ satisfies $ed = 1 + b\phi(N)$. Given an approximation d_0 of d with $|d - d_0| < N^{\beta}$, one can factor N in polynomial time under Assumption 1 if*

$$\lambda < \frac{3r - 2\sqrt{3r+3} + 3}{3\ (r+1)},$$

where $\lambda = \max\left\{\beta, \delta - \frac{r}{r+1}\right\}$.

Proof. We have $ed \equiv 1 \bmod \phi(N)$ where $N = p^r q$. So we can write $ed = 1 + b(N - p^r - p^{r-1}q + p^{r-1})$. From Lemma 1, we can find an approximation b_0 of b. Let $b_1 = b - b_0$. Hence we have $ed = 1 + (b_0 + b_1)(N - p^r - p^{r-1}q + p^{r-1})$. Now we want to find the root $(x_0, y_0, z_0) = (b_1, p, q)$ modulo e of the polynomial

$$f_e(x, y, z) = 1 + (b_0 + x)\left(N - y^r - y^{r-1}z + y^{r-1}\right).$$

Let $X = N^{\lambda}, Y = Z = N^{\frac{1}{r+1}}$. Clearly, (X, Y, Z) provides the upper bounds of the elements in the root (x_0, y_0, z_0), neglecting any small constant.

For integers m, a, t, we consider the following polynomials

$$g_{v,i,0}(x, y, z) = y^{i+rv} z^a f_e^{(m-v)} \quad \text{where } v = 0, \ldots, m,\ i = 0, \ldots, t \quad \text{and}$$
$$g_{v,i,j}(x, y, z) = x^{j - \min\{j,v\}} y^{i-j+r\max\{j,v\}} z^{j+a} f_e^{m - \max\{j,v\}} \quad \text{where } v = 0, \ldots, m,\ j = 1, \ldots, m,\ i = 0, \ldots, r.$$

Now we replace each occurrence of the monomial $y^r z$ in $g_{v,i,0}$ by N. Let the new polynomial be $h'_{v,i,0}$. Now we want to make the coefficient of the monomial $x^{m-v}\ y^{i+rm-rl} z^{a-l}$ in $h'_{v,i,0}$ to be 1, where $l = \min\left\{\left\lfloor \frac{i+rm}{r} \right\rfloor, a\right\}$. Let A be its coefficient in $h'_{v,i,0}$. Assume $\gcd(A, e) = 1$. Let $AB \equiv 1 \bmod e^m$.

Table 4
Numerical values of δ for different parameters.

r	m	a	t	λ	Lattice dimension
2	10	4	0	0.23	341
3	7	5	2	0.26	248
4	10	10	13	0.37	704
5	15	16	29	0.45	1920
6	27	35	89	0.52	7812

Now consider the set of polynomials

$$h_{v,i,0}(x, y, z) = Bh'_{v,i,0}(x, y, z)e^v.$$

Similarly construct $h_{v,i,j}(x, y, z) = Bh'_{v,i,j}(x, y, z)e^{\max\{j,v\}}$.

Next, we form a lattice L by taking the coefficient vectors of the shift polynomials $h_{v,i,j}(xX, yY, zZ)$ as basis.

Now dimension w of L is given by $w = \sum_{v=0}^{m}\sum_{i=0}^{t} 1+\sum_{v=0}^{m}\sum_{j=1}^{m}\sum_{i=0}^{r} 1 = (r+1)m^2+mt+o(m^2)$. Let the determinant of L be $\det(L) = X^{s_x}Y^{s_y}Z^{s_z}e^{s_e}$.

Now $s_x = \sum_{v=0}^{m}\sum_{i=0}^{t}(m-v) + \sum_{v=0}^{m}\sum_{j=1}^{m}\sum_{i=0}^{r}\big(m+j-\min\{j,v\}-\max\{j,v\}\big) = \frac{m^3(r+1)}{2} + \frac{m^2t}{2} + o(m^3)$. Similarly, $s_e = \frac{2m^3(r+1)}{3} + \frac{m^2t}{2} + o(m^3)$.

Also

$$\begin{aligned} s_y &= \sum_{v=0}^{m}\sum_{i=0}^{t}\Big(i+rm-r\min\Big\{\Big\lfloor\frac{i+rm}{r}\Big\rfloor, a\Big\}\Big) + \\ &\quad \sum_{v=0}^{m}\sum_{j=1}^{m}\sum_{i=0}^{r}\Big(i-j+rm-r\min\Big\{\Big\lfloor\frac{i-j+rm}{r}\Big\rfloor, j+a\Big\}\Big) \\ &= \frac{1}{2}m^3r^2 - m^2ar^2 + \frac{1}{2}ma^2r^2 + m^2tr - matr + \frac{1}{2}mt^2 + o(m^3), \quad (\text{if } a < m \text{ or } a > m \,\&\, t > r(a-m)) \end{aligned}$$

and

$$\begin{aligned} s_z &= \sum_{v=0}^{m}\sum_{i=0}^{t}\Big(a-\min\Big\{\Big\lfloor\frac{i+rm}{r}\Big\rfloor, a\Big\}\Big) + \\ &\quad \sum_{v=0}^{m}\sum_{j=1}^{m}\sum_{i=0}^{r}\Big(j+a-\min\Big\{\Big\lfloor\frac{i-j+rm}{r}\Big\rfloor, j+a\Big\}\Big) \\ &= \frac{ma^2r^2 + 2m^2ar + m^3}{2r} + o(m^3) \quad (\text{if } a < m \text{ or } a > m \,\&\, t > r(a-m)). \end{aligned}$$

To find (x_0, y_0, z_0) using lattice reduction over L, we need $\det(L) < e^{mw}$. Let $a = \tau_1 m$ and $t = \tau_2 m$, where τ_1, τ_2 are non-negative real numbers.

Now putting the values of $\det(L)$ and w in the condition $\det(L) < e^{mw}$, required condition is

$$\begin{aligned} \eta(\tau_1, \tau_2) &= -\frac{\tau_1^2}{2r} + \frac{2r^3\tau_1 + 2r^2\tau_1\tau_2 - r^3\lambda - r^2\tau_2\lambda - \frac{r^3}{3} - r^2\tau_2 - r\tau_2^2 - 2r^2\lambda - r\tau_2\lambda}{2r^2+2r} \\ &\quad + \frac{\frac{4}{3}r^2 - 2r\tau_1 + r\tau_2 - r\lambda + \frac{2}{3}r - 1}{2r^2+2r} > 0. \end{aligned}$$

For a fixed δ, we will take the partial derivative of η with respect to τ_1, τ_2 and equate each of them to 0, we get $\tau_1 = -\frac{(\lambda-1)r^2+(\lambda-1)r+2}{2r}$ and $\tau_2 = -\frac{r^2}{2}(\lambda-1) - \lambda r - \frac{\lambda}{2} - \frac{1}{2}$. Now put these values of τ_1, τ_2 in η, we have $\lambda < \frac{3r-2\sqrt{3r+3}+3}{3(r+1)}$. □

In Table 4 we present few numerical values of λ for different values of r, m, a, t.

Note that cryptanalysis using our method is possible if $\lambda < \frac{3r-2\sqrt{3r+3}+3}{3(r+1)}$, with $\lambda = \max\Big\{\beta, \delta - \frac{1}{r+1}\Big\}$. As $\lambda < \frac{3r-2\sqrt{3r+3}+3}{3(r+1)}$, we have $\beta < \frac{3r-2\sqrt{3r+3}+3}{3(r+1)}$ and $\delta < \frac{1}{r+1} + \frac{3r-2\sqrt{3r+3}+3}{3(r+1)}$.

In [18], it is proved that if $|d-d_0| < N^{\beta}$ where $\beta = \max\Big\{\frac{r}{(r+1)^2}, (\frac{r-1}{r+1})^2\Big\}$ and d_0 is known, one can factor N in polynomial time. Lu et al. [16] improve this bound to $|d-d_0| < N^{\frac{r(r-1)}{(r+1)^2}}$. Approach of [18,16] works even when d is of order N. However our approach does not work in these cases.

Table 5
Numerical upper bound of β and δ for different values of r.

r		2	3	4	5	6	7	8	9	10
[18]:	β	0.222	0.250	0.360	0.444	0.510	0.562	0.605	0.640	0.669
[16]:	β	0.222	0.375	0.480	0.555	0.612	0.656	0.691	0.720	0.744
Our	β	0.333	0.423	0.484	0.528	0.563	0.592	0.615	0.635	0.652
	δ	0.667	0.673	0.684	0.695	0.706	0.717	0.726	0.735	0.743

In Table 5, we have compared our bounds with the work of [16,18]. From Table 5, it is clear that when $\delta < \frac{1}{r+1} + \frac{3r-2\sqrt{3r+3}+3}{3(r+1)}$, our approach is better than the work of [18] if $r \leq 8$. However, our idea is better than [16] when $r < 5$. We could not attempt experiments as the lattice dimension is becoming quite high to show the improvements.

5. Conclusion

In this paper, we have considered the Prime Power RSA, i.e, when RSA modulus is of the form $N = p^r q$. Our new lattice construction improves the existing attacks for small decryption exponent when $r = 3, 4$. We also have studied partial key exposure attack on Prime Power RSA. Our new approach improves the existing works when $2 \leq r \leq 4$ if $d < N^{\frac{1}{r+1} + \frac{3r-2\sqrt{3r+3}+3}{3(r+1)}}$.

References

[1] J. Blömer, A. May, New partial key exposure attacks on RSA, in: Crypto 2003, in: LNCS, vol. 2729, 2003, pp. 27–43.
[2] D. Boneh, R.A. DeMillo, R.J. Lipton, On the importance of eliminating errors in cryptographic computations, J. Cryptology 14 (2) (2001) 101–119.
[3] D. Boneh, G. Durfee, Cryptanalysis of RSA with private key d less than $N^{0.292}$, IEEE Trans. Inform. Theory 46 (4) (2000) 1339–1349.
[4] D. Boneh, G. Durfee, Y. Frankel, Exposing an RSA private key given a small fraction of its bits, in: Asiacrypt 1998, in: LNCS, vol. 1514, 1998, pp. 25–34.
[5] D. Boneh, G. Durfee, N. Howgrave-Graham, Factoring $N = p^r q$ for large r, in: Crypto 1999, in: LNCS, vol. 1666, 1999, pp. 326–337.
[6] D. Coppersmith, Small solutions to polynomial equations and low exponent vulnerabilities, J. Cryptol. 10 (4) (1997) 223–260.
[7] D. Cox, J. Little, D. O'Shea, Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra, third ed., Springer, New York, 2007.
[8] M. Ernst, E. Jochemsz, A. May, B. de Weger, Partial key exposure attacks on RSA up to full size exponents, in: Eurocrypt 2005, in: LNCS, vol. 3494, 2005, pp. 371–386.
[9] A. Fujioka, T. Okamoto, S. Miyaguchi, ESIGN: An efficient digital signature implementation for smard cards, in: Eurocrypt 1991, in: LNCS, vol. 547, 1991, pp. 446–457.
[10] N. Howgrave-Graham, Finding small roots of univariate modular equations revisited, in: Proceedings of IMA International Conference on Cryptography and Coding, LNCS, vol. 1355, 1997, pp. 131–142.
[11] K. Itoh, N. Kunihiro, K. Kurosawa, Small secret key attack on a variant of RSA (Due to Takagi), in: CT-RSA 2008, in: LNCS, vol. 4964, 2008, pp. 387–406.
[12] P. Kocher, Timing attacks on implementations of Diffie-Hellman, RSA, DSS and other systems, in: Crypto 1996, in: LNCS, vol. 1109, 1996, pp. 104–113.
[13] P.C. Kocher, J. Jaffe, B. Jun, Differential power analysis, in: Crypto 1999, in: LNCS, vol. 1666, 1999, pp. 388–397.
[14] H.W. Lenstra Jr., Factoring integers with elliptic curves, Ann. of Math. 126 (1987) 649–673.
[15] A.K. Lenstra, H.W. Lenstra Jr., L. Lovász, Factoring polynomials with rational coefficients, Math. Ann. 261 (1982) 515–534.
[16] Y. Lu, R. Zhang, D. Lin, New Results on Solving Linear Equations Modulo Unknown Divisors and its Applications. IACR Cryptology ePrint Archive, 2014.
[17] Y. Lu, R. Zhang, L. Peng, D. Lin, Solving linear equations modulo unknown divisors: revisited. Accepted in ASIACRYPT 2015.
[18] A. May, Secret exponent attacks on RSA-type schemes with moduli $N = p^r q$, in: PKC 2004, in: LNCS, vol. 2947, 2004, pp. 218–230.
[19] T. Okamoto, S. Uchiyama, A new public key cryptosystem as secure as factoring, in: Eurocrypt 1998, in: LNCS, vol. 1403, 1998, pp. 308–318.
[20] S. Sarkar, Small secret exponent attack on RSA variant with modulus $N = p^r q$, Des. Codes Cryptogr. 73 (2) (2014) 383–392.
[21] T. Takagi, Fast RSA-type cryptosystem modulo $p^k q$, in: Crypto 1998, in: LNCS, vol. 1462, 1998, pp. 318–326.
[22] M. Wiener, Cryptanalysis of short RSA secret exponents, IEEE Trans. Inform. Theory 36 (3) (1990) 553–558.