Cryptanalysis of Variants of RSA with Multiple Small Secret Exponents

Liqiang Peng[1,2], Lei Hu[1,2(✉)], Yao Lu[1,3], Santanu Sarkar[4], Jun Xu[1,2], and Zhangjie Huang[1,2]

[1] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100 093, China
pengliqiang@iie.ac.cn, hu@is.ac.cn

[2] Data Assurance and Communication Security Research Center, Chinese Academy of Sciences, Beijing 100 093, China

[3] The University of Tokyo, Tokyo, Japan
lywhhit@gmail.com

[4] Indian Institute of Technology Madras, Sardar Patel Road, Chennai 600 036, India
sarkar.santanu.bir@gmail.com

Abstract. In this paper, we analyze the security of two variants of the RSA public key cryptosystem where multiple encryption and decryption exponents are used with a common modulus. For the most well known variant, CRT-RSA, assume that n encryption and decryption exponents (e_l, d_{p_l}, d_{q_l}), where $l = 1, \cdots, n$, are used with a common CRT-RSA modulus N. By utilizing a Minkowski sum based lattice construction and combining several modular equations which share a common variable, we prove that one can factor N when $d_{p_l}, d_{q_l} < N^{\frac{2n-3}{8n+2}}$ for all $l = 1, \cdots, n$. We further improve this bound to $d_{p_l}(\text{or } d_{q_l}) < N^{\frac{9n-14}{24n+8}}$ for all $l = 1, \cdots, n$. Moreover, our experiments do better than previous works by Jochemsz-May (Crypto 2007) and Herrmann-May (PKC 2010) when multiple exponents are used. For Takagi's variant of RSA, assume that n key pairs (e_l, d_l) for $l = 1, \cdots, n$ are available for a common modulus $N = p^r q$ where $r \geq 2$. By solving several simultaneous modular univariate linear equations, we show that when $d_l < N^{(\frac{r-1}{r+1})\frac{n+1}{n}}$, for all $l = 1, \cdots, n$, one can factor the common modulus N.

Keywords: RSA · Cryptanalysis · Lattice · Coppersmith's method

1 Introduction

Since its invention [16], the RSA public key scheme has been widely used due to its effective encryption and decryption. To obtain high efficiency, some variants of the original RSA were designed. Wiener [24] proposed an algorithm to use the Chinese Remainder Theorem in the decryption phase to accelerate the decryption operation by using smaller exponents d_p and d_q which satisfy $ed_p \equiv 1 \bmod (p-1)$ and $ed_q \equiv 1 \bmod (q-1)$ for a modulus $N = pq$ and an

A. Biryukov and V. Goyal (Eds.): INDOCRYPT 2015, LNCS 9462, pp. 105–123, 2015.
DOI: 10.1007/978-3-319-26617-6_6

encryption exponent e. This decryption oriented alternative of RSA scheme is usually called as CRT-RSA. Also for gaining a fast decryption implementation, Takagi [21] proposed another variant of RSA with moduli of the form $N = p^r q$, where $r \geq 2$ is an integer. For Takagi's variant, the encryption exponent e and decryption exponent d satisfy $ed \equiv 1 \pmod{p^{r-1}(p-1)(q-1)}$.

In many applications of the RSA scheme and its variants, either d is chosen to be small or d_p and d_q are chosen to be small for efficient modular exponentiation in the decryption process. However, since Wiener [24] showed that the original RSA scheme is insecure when d is small enough, along this direction many researchers have paid much attention to factoring RSA moduli and its variants under small decryption exponents.

Small Secret Exponent Attacks on RSA and Its Variants. For the original RSA with a modulus $N = pq$, Wiener [24] proved that when $d \leq N^{0.25}$, one can factor the modulus N in polynomial time by a Continued Fraction Method. Later, by utilizing a lattice based method, which is usually called Coppersmith's technique [5] for finding small roots of a modular equation, Boneh and Durfee [2] improved the bound to $N^{0.292}$ under several acceptable assumptions. Then, Herrmann and May [6] used a linearization technique to simplify the construction of the lattice involved and obtained the same bound $N^{0.292}$. Until now, $N^{0.292}$ is still the best result for small secret exponent attacks on the original RSA scheme with full size of e.

For CRT-RSA, Jochemsz and May [10] gave an attack for small d_p and d_q, where p and q are balanced and the encryption exponent e is of full size, i.e. about as large as the modulus $N = pq$. By solving an integer equation, they can factor N provided that the small decryption CRT-exponents d_p and d_q are smaller than $N^{0.073}$. Similarly, Herrmann and May [6] used a linearization technique to obtain the same theoretical bound but better results in experiments.

For Takagi's variant of RSA with modulus $N = p^r q$, May [13] applied Coppersmith's method to prove that one can factor the modulus provided that $d \leq N^{(\frac{r-1}{r+1})^2}$. By modifying the collection of polynomials in the construction of the lattice, Lu et al. [12] improved this bound to $d \leq N^{\frac{r(r-1)}{(r+1)^2}}$. Recently, from a new point of view of utilizing the algebraic property $p^r q = N$, Sarkar [17] improved the bound when $r \leq 5$. Especially for the most practical case of $r = 2$, the bound has been significantly improved from $N^{0.222}$ to $N^{0.395}$. The following table lists the existing small decryption exponent attacks on RSA and its variants Table 1.

Multiple Small Secret Exponents RSA. In order to simplify RSA key management, one may be tempted to use a single RSA modulus N for several key pairs (e_i, d_i). Simmons [19] showed that if a massage m is sent to two participants whose public exponents are relatively prime, then m can easily be recovered. However Simmons's attack can not factor N. Hence Howgrave-Graham and Seifert [8] analyzed the case that several available encryption exponents

Table 1. Overview of existing works on small secret exponent attacks on RSA and its variants. The conditions in the last column allow to efficiently factor the modulus N.

Author(s)	Cryptosystem	Bounds
Wiener: 1990 [24]	RSA	$d < N^{0.25}$
Boneh and Durfee: 1999 [2]	RSA	$d < N^{0.292}$
Jochemsz and May: 2007 [10]	CRT-RSA	$d_p, d_q < N^{0.073}$
Herrmann and May: 2010 [6]	CRT-RSA	$d_p, d_q < N^{0.073}$
May: 2004 [13]	Takagi's variant of RSA $N = p^r q$	$d \leq N^{(\frac{r-1}{r+1})^2}$
Lu, Zhang, Peng and Lin: 2014 [12]	Takagi's variant of RSA $N = p^r q$	$d \leq N^{\frac{r(r-1)}{(r+1)^2}}$
Sarkar: 2014 [17]	Takagi's variant of RSA $N = p^2 q$	$d \leq N^{0.395}$

Table 2. Comparison of previous theoretical bounds with respect to the number of decryption exponents.

n	1	2	5	10	20	∞
Howgrave-Graham and Seifert's bound [8]	0.2500	0.3125	0.4677	0.5397	0.6319	1.0000
Sarkar and Maitra's bound [18]	0.2500	0.4167	0.5833	0.6591	0.7024	0.7500
Aono's bound [1]	0.2500	0.4643	0.6250	0.6855	0.7172	0.7500
Takayasu and Kunihiro's bound [23]	0.2929	0.4655	0.6464	0.7460	0.8189	1.0000

$(e_1, \cdots, e_n)$ exist for a common modulus N and the corresponding decryption exponents $(d_1, \cdots, d_n)$ are small. From their result, one can factor N when the n decryption exponents satisfy that $d_l < N^\delta$ for all $l = 1, \cdots, n$, where

$$\delta < \begin{cases} \dfrac{(2n+1)2^n - (2n+1)\binom{n}{\frac{n}{2}}}{(2n-1)2^n + (4n+2)\binom{n}{\frac{n}{2}}}, & \text{if } n \text{ is even, and} \\ \dfrac{(2n+1)2^n - 4n\binom{n-1}{\frac{n-1}{2}}}{(2n-2)2^n + 8n\binom{n-1}{\frac{n-1}{2}}}, & \text{if } n \text{ is odd.} \end{cases}$$

In [18], Sarkar and Maitra used the strategy of [9] to solve for small roots of an integer equation and improved the bound to $\delta < \frac{3n-1}{4n+4}$. Aono [1] proposed a method to solve several simultaneous modular equations which share a common unknown variable. Aono combined several lattices into one lattice by a Minkowski sum based lattice construction and obtained that when $\delta < \frac{9n-5}{12n+4}$, N can be factored. Shortly afterwards, Takayasu and Kunihiro [23] modified each lattice and collected more helpful polynomials to improve the bound to $1 - \sqrt{\frac{2}{3n+1}}$. In conclusion, an explicit picture of the comparison of previous work is illustrated in Table 2.

Simultaneous Modular Univariate Linear Equations Modulo an Unknown Divisor. In 2001, Howgrave-Graham first considered the problem of solving an univariate linear equation modulo an unknown divisor of a known composite integer,

$$f(x) = x + a \pmod{p},$$

where a is a given integer, and $p \simeq N^{\beta}$ is an unknown factor of the known N. The size of the root is bounded by $|x| < N^{\delta}$. Howgrave-Graham proved that one can solve for the root in polynomial time provided that $\delta < \beta^2$.

The generalization of this problem has been considered by Cohn and Heninger [4],

$$\begin{cases} f(x_1) = x_1 + a_1 \pmod{p}, \\ f(x_2) = x_2 + a_2 \pmod{p}, \\ \cdots \\ f(x_n) = x_n + a_n \pmod{p}. \end{cases}$$

In the above simultaneous modular univariate linear equations, $a_1, \cdots, a_n$ are given integers, and $p \simeq N^{\beta}$ is an unknown factor of N. Based on their result, one can factor N if

$$\frac{\gamma_1 + \cdots + \gamma_n}{n} < \beta^{\frac{n+1}{n}} \text{ and } \beta \gg \frac{1}{\sqrt{\log N}}$$

where $|x_1| < N^{\gamma_1}, \cdots, |x_n| < N^{\gamma_n}$. Then by considering the sizes of unknown variables and collecting more helpful polynomials which are selected to construct the lattice, Takayasu and Kunihiro [22] further improved the bound to

$$\sqrt[n]{\gamma_1 \cdots \gamma_n} < \beta^{\frac{n+1}{n}} \text{ and } \beta \gg \frac{1}{\sqrt{\log N}}.$$

Our Contributions. In this paper, we give an analysis of CRT-RSA and Takagi's variant of RSA with multiple small decryption exponents, respectively. For CRT-RSA, $(e_1, \cdots, e_n)$ are n encryption exponents and $(d_{p_1}, d_{q_1}), \cdots, (d_{p_n}, d_{q_n})$ are the corresponding decryption exponents for a common CRT-RSA modulus N, where $e_1, \cdots, e_n$ are of full size as N. Based on the Minkowski sum based lattice construction proposed by Aono [1], we combine several modular equations which share a common variable and obtain that one can factor N when

$$d_{p_l}, d_{q_l} < N^{\frac{2n-3}{8n+2}}$$

for all $l = 1, \cdots, n$, where n is the number of decryption exponents.

In order to utilize the Minkowski sum based lattice construction to combine the equations, the equations should share a common variable. Hence, we modified each of the equations considered in [10], which results in a worse bound when there is only one pair of encryption and decryption exponents.

However, note that the modular equations

$$k_{p_l}(p-1) + 1 \equiv 0 \pmod{e_l}, \text{ for } l = 1, \cdots, n,$$

share a common root p. Then we can directly combine these n equations by a Minkowski sum based lattice construction, and moreover introduce a new variable q to minimize the determinant of the combined lattice. We can obtain an improved bound that one can factor N when

$$d_{p_l} < N^{\frac{9n-14}{24n+8}}$$

for all $l = 1, \cdots, n$.

Note that, for combining these equations we modified each of the equations considered in [10]. When there are $n = 2$ decryption exponents, our bound is $N^{0.071}$ which is less than the bound $N^{0.073}$ in [10]. Hence, we only improve the previous bound when there are $n \geq 3$ pairs of encryption and decryption exponents for a common CRT-RSA modulus in theory and obtain $N^{0.375}$ asymptotically in n. However, it is nice to see that we successfully factor N when $d_{p_l} < N^{0.035}$ with 3 pairs of exponents in practice and the original bounds are $N^{0.015}$ in [10] and $N^{0.029}$ in [6].

An explicit description of these bounds is illustrated in Fig. 1.

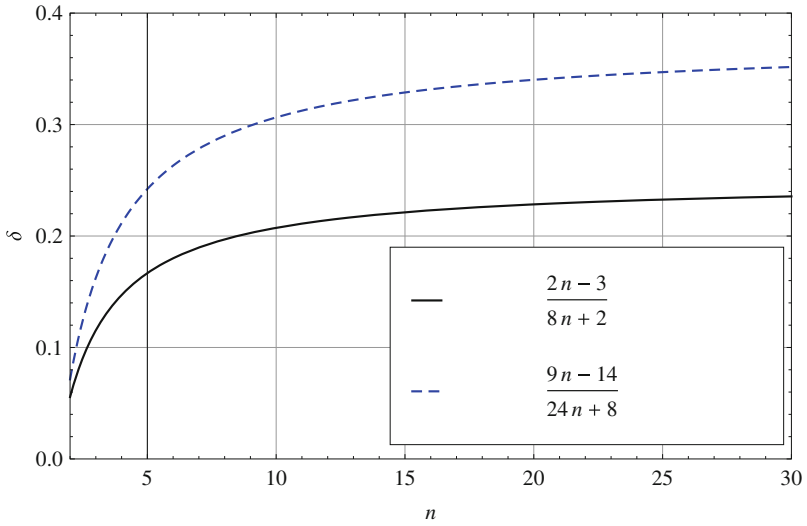

Fig. 1. The recoverable sizes of secret exponents of CRT-RSA. The solid line denotes the range of d_{p_l} and d_{q_l} with respect to n, the dashed line denotes the range of d_{p_l} with respect to n

For Takagi's variant of RSA, assume there exist n encryption and decryption exponents (e_l, d_l), where $l = 1, \cdots, n$ with a common modulus $N = p^r q$, which means there exist l simultaneous modular univariate linear equations. So far, this kind of modular equations is what has been considered in [4,22].

By an application of their results, we obtain that the modulus can be factored when $d_l \leq N^{\delta}$ for all $l = 1, \cdots, n$, where

$$\delta < \left(\frac{r-1}{r+1}\right)^{\frac{n+1}{n}}.$$

The rest of this paper is organized as follows. Section 2 is some preliminary knowledge on lattices and the CRT-RSA variant. In Sect. 3, we analyze CRT-RSA with multiple small decryption exponents. Section 4 presents an analysis on Takagi's variant RSA with multiple small decryption exponents. Finally, Sect. 5 is the conclusion.

2 Preliminaries

Let $w_1, w_2, \cdots, w_k$ be k linearly independent vectors in $\mathbb{R}^n$. A lattice $\mathcal{L}$ spanned by $\{w_1, \cdots, w_k\}$ is the set of all integer linear combinations, $c_1 w_1 + \cdots + c_k w_k$, of $w_1, \cdots, w_k$, where $c_1, \cdots, c_k \in \mathbb{Z}$. The k-dimensional lattice $\mathcal{L}$ is a discrete additive subgroup of $\mathbb{R}^n$. The set of vectors $w_1, \cdots, w_k$ is called a basis of the lattice $\mathcal{L}$. The lattice bases are not unique, one can obtain another basis by multiplying any matrix with determinant ± 1, it means that any lattice of dimension larger than 1 has infinitely many bases [15]. Hence, how to find a lattice basis with good properties has been an important problem.

Lenstra et al. [11] introduced the famous L^3 lattice basis reduction algorithm which can output a relatively short and nearly orthogonal lattice basis in polynomial time. Instead of finding the shortest vectors in a lattice, the algorithm finds the L^3 reduced basis with the following useful properties.

Lemma 1 *(L^3, [11]). Let $\mathcal{L}$ be a lattice of dimension k. Applying the L^3 algorithm to $\mathcal{L}$, the outputted reduced basis vectors $v_1, \cdots, v_k$ satisfy that*

$$\|v_i\| \leq 2^{\frac{k(k-i)}{4(k+1-i)}} \det(\mathcal{L})^{\frac{1}{k+1-i}}, \text{ for any } 1 \leq i \leq k.$$

Coppersmith [5] applied the L^3 lattice basis reduction algorithm in order to find small solutions of integer equations and modular equations. Later, Jochemsz and May [9] extended this technique and gave general results to find roots of multivariate polynomials.

For a given polynomial $g(x_1, \cdots, x_k) = \sum_{(i_1, \cdots, i_k)} a_{i_1, \cdots, i_k} x_1^{i_1} \cdots x_k^{i_k}$, we define the norm of g as

$$\|g(x_1, \cdots, x_k)\| = \Big(\sum_{(i_1, \cdots, i_k)} a_{i_1, \cdots, i_k}^2 \Big)^{\frac{1}{2}}.$$

The following lemma due to Howgrave-Graham [7] gives a sufficient condition under which a modular equation can be converted into an integer equation.

Lemma 2 *(Howgrave-Graham, [7]). Let* $g(x_1, \cdots, x_k) \in \mathbb{Z}[x_1, \cdots, x_k]$ *be an integer polynomial with at most* w *monomials. Suppose that*

$$g(y_1, \cdots, y_k) \equiv 0 \pmod{p^m} \text{ for } |y_1| \leq X_1, \cdots, |y_k| \leq X_k, \text{ and}$$
$$\|g(x_1X_1, \cdots, x_kX_k)\| < \frac{p^m}{\sqrt{w}}.$$

Then $g(y_1, \cdots, y_k) = 0$ *holds over the integers.*

Suppose we have $w(> k)$ polynomials $b_1, \cdots, b_w$ in the variables $x_1, \ldots, x_k$ such that $b_1(y_1, \ldots, y_k) = \cdots = b_w(y_1, \ldots, y_k) = 0 \, mod p^m$ with $|y_1| \leq X_1, \ldots, |y_k| \leq X_k$. Now we construct a lattice $\mathcal{L}$ with the coefficient vectors of $b_1(x_1X_1, \ldots, x_kX_k)$, $\ldots$, $b_w(x_1X_1, \ldots, x_kX_k)$. After lattice reduction, we get k polynomials $v_1(x_1, \ldots, x_k), \ldots, v_k(x_1, \ldots, x_k)$ such that

$$v_1(y_1, \ldots, y_k) = \cdots = v_k(y_1, \ldots, y_k) = 0 \, mod p^m$$

which correspond to the first k vectors of the reduced basis. Also by the property of the L^3 algorithm, we have

$$||v_1(x_1X_1, \ldots, x_kX_k)|| \leq \cdots \leq ||v_k(x_1X_1, \ldots, x_kX_k)|| \leq 2^{\frac{w(w-1)}{4(w+1-k)}} \det(\mathcal{L})^{\frac{1}{w+1-k}}.$$

Hence by Lemma 2, if

$$2^{\frac{w(w-1)}{4(w+1-k)}} \det(\mathcal{L})^{\frac{1}{w+1-k}} < \frac{p^m}{\sqrt{w}},$$

then we have $v_1(y_1, \ldots, y_k) = \cdots = v_k(y_1, \ldots, k_k) = 0$. Next we want to find $y_1, \ldots, y_k$ from $v_1, \ldots, v_k$.

Once we obtain several polynomial equations over the integers from the L^3 lattice basis reduction algorithm, we can solve for the roots over the integers by calculating the resultants or the Gröbner basis of the polynomials based on the following heuristic assumption. In practical experiments, the following heuristic assumption usually holds.

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.*

Similarly as other lattice reduction works [1,9,10,23], while we present experimental results in support of our attacks, we also like to point out the theoretical results are asymptotic, as we neglect constants in certain cases in the calculations of our attacks.

Minkowski Sum Based Lattice Construction. In [1], Aono proposed a method to construct a lattice for Coppersmith's technique for simultaneous modular equations. In order to make this clear, let us illustrate it by an example. There are two modular equations $f_1 \equiv 0 \, (\mathrm{mod}\, W_1)$ and $f_2 \equiv 0 \, (\mathrm{mod}\, W_2)$.

Based on Coppersmith's technique, to solve for the solutions of f_1 we first select some polynomials $g_1, \cdots, g_n$ which share the same solutions modulo W_1^m. Similarly, we construct polynomials $g'_1, \cdots, g'_n$ which share same solutions modulo W_2^m. It is obvious that any polynomial $g_i g'_j$ where $1 \leq i, j \leq n$ has the desired solutions modulo $W_1^m W_2^m$. Then we arrange these polynomials and construct a new lattice with polynomials which have the desired solutions modulo $W_1^m W_2^m$. By an integer linear combination, some of these polynomials which have the same leading monomial can be written as $\sum_{i,j} a_{i,j} g_i g'_j$. To keep the determinant of the lattice small, the integers $a_{i,j}$ are chosen appropriately. This lattice is called a combined lattice obtained from the two lattices, one of which is constructed by the polynomials $g_1, \cdots, g_n$ and another one of which is constructed by the polynomials $g'_1, \cdots, g'_n$. Aono proved that the combined lattice is triangular, if each lattice has a triangular basis matrix. The above conclusion could be extend to an arbitrary number of modular equations.

CRT-RSA. Since the RSA public key cryptosystem has been invented [16], this public key scheme has been widely used due to its succinct and effective encryption and decryption. Wiener [24] proposed to use the Chinese Remainder Theorem in the decryption phase. This scheme is usually called CRT-RSA. Based on the work of Sun and Wu [20], one version of this variant can be described as follows:

Algorithm 1. Key generation of CRT-RSA

Input:

(n, δ_1, δ_2), where $n, \delta_1 n$ and $\delta_2 n$ denote the bitlengths of N, d_p and d_q, respectively.

Output:

CRT-RSA-instance (N, p, q, e, d_p, d_q).

1: Randomly choose two $\frac{n}{2}$-bit primes $p = 2p_1 + 1$ and $q = 2q_1 + 1$ such that $\gcd(p_1, q_1) = 1$.
2: Randomly generate $(\delta_1 n)$-bit integer d_p and $(\delta_2 n)$-bit integer d_q such that $\gcd(d_p, p-1) = 1$ and $\gcd(d_q, q-1) = 1$.
3: Compute $\bar{d} \equiv (d_q - d_p)(p_1^{-1} (\mathrm{mod}\ q_1))$.
4: Compute $d = d_p + p_1 \cdot \bar{d}$.
5: Compute the encryption exponent e satisfying $ed \equiv (\mathrm{mod}\,(p-1)(q-1))$.
6: The RSA modulus is $N = pq$, the secret key is (d_p, d_q, p, q) and the public key is (N, e).

As described in the key generation algorithm of CRT-RSA, the case that more than one valid encryption and decryption exponents for the same CRT-RSA modulus $N = pq$ may exist, that is, when we are done with Step 1 for choosing a pair (p, q), we generate several different d_p and d_q in the remaining steps. Next, we analyze the weakness in the case that multiple encryption and decryption exponents share a common CRT-RSA modulus.

3 Multiple Encryption and Decryption Exponents Attack of CRT-RSA

In this section, along the idea of [1,8,18,23] we give the following theorems when multiple encryption and decryption exponents are used for a common CRT-RSA modulus. By making a comparison between our results and Jochemsz and May's result [10], we improve the bound when there are 3 or more pairs of encryption and decryption exponents for a common CRT-RSA modulus. And we also improve the experimental results $N^{0.015}$ in [10] and $N^{0.029}$ in [6] to $N^{0.035}$ with 3 pairs of exponents.

Theorem 1. *Let $(e_1, e_2, \cdots, e_n)$ be n CRT-RSA encryption exponents with a common modulus $N = pq$, where $n \geq 3$ and $e_1, e_2, \cdots, e_n$ have roughly the same bitlength as N. Consider that $d_{p_i}, d_{q_i} \leq N^{\delta}$ for $i = 1, 2, \cdots, n$ are the corresponding decryption exponents. Then under Assumption 1, one can factor N in polynomial time when*

$$\delta < \frac{2n-3}{8n+2}.$$

Proof. For one pair of keys (e_l, d_{p_l}, d_{q_l}), we have

$$\begin{aligned} e_l d_{p_l} - 1 &= k_{p_l}(p-1), \\ e_l d_{q_l} - 1 &= k_{q_l}(q-1), \end{aligned}$$

where k_{p_l} and k_{q_l} are some integers.

Moreover, by multiplying these two equations, we have that

$$e_l^2 d_{p_l} d_{q_l} - e_l(d_{p_l} + d_{q_l}) + 1 = k_{p_l} k_{q_l}(N - s),$$

where $s = p + q - 1$.

Then $(k_{p_l} k_{q_l}, s, d_{p_l} + d_{q_l})$ is a solution of

$$f_l(x_l, y, z_l) = x_l(N - y) + e_l z_l - 1 \pmod{e_l^2}.$$

Moreover, consider the n modular polynomials

$$f_l(x_l, y, z_l) = x_l(N - y) + e_l z_l - 1 \pmod{e_l^2}, \text{ for } l = 1, \cdots, n. \tag{1}$$

These polynomials have the common root $(x_1, \cdots, x_n, y, z_1, \cdots, z_n) = (k_{p_1} k_{q_1}, \cdots, k_{p_n} k_{q_n}, s, d_{p_1} + d_{q_1}, \cdots, d_{p_n} + d_{q_n})$, and the values of its coefficients can be roughly bounded as $k_{p_l} k_{q_l} \simeq X_l = N^{1+2\delta}$, $s \simeq Y = N^{\frac{1}{2}}$ and $d_{p_l} + d_{q_l} \simeq N^{\delta} = Z$ for $l = 1, \cdots, n$.

In order to solve for the desired solution of the modular equations $f_l(x_l, y, z_l) = 0 \pmod{e_l^2}$, for $l = 1, \cdots, n$, based on Aono's idea [1], we first selected the following set of polynomials to solve each single equation,

$$S_l = \{x_l^{i_l} z_l^{j_l} f_l^{k_l}(x_l, y, z_l)(e_l^2)^{m-k_l} | 0 \leq k_l \leq m, 0 \leq i_l \leq m - k_l, 0 \leq j_l \leq m - i_l - k_l\},$$

where $l = 1, \cdots, n$ and m is a positive integer.

Each selection for the corresponding equation in (1) generates a triangular basis matrix. Likewise, for each $l = 1, 2, \cdots, n$, we can respectively construct a triangular matrix. Based on the technique of Minkowski sum based lattice construction, these n lattices corresponding to the n triangular matrices can be combined as a new lattice $\mathcal{L}'$ and the basis matrix with polynomials which have the same root as the solutions of the modular equation modulo $(e_1^2 \cdots e_n^2)^m$. Since each basis matrix is triangular, the combined lattice is also triangular. The combined basis matrix has diagonal entries

$$X_1^{i_1} \cdots X_n^{i_n} Y^k Z_1^{j_1} \cdots Z_n^{j_n} (e_1^2)^{m-\min(i_1,k)} \cdots (e_n^2)^{m-\min(i_n,k)},$$

where

$$0 \le i_1, \cdots, i_n \le m,\ 0 \le k \le i_1 + i_2 + \cdots + i_n,\ 0 \le j_1 \le i_1, \cdots,\ 0 \le j_n \le i_n.$$

Then the determinant of the lattice can be calculated as

$$\begin{aligned}\det(\mathcal{L}') = \prod_{i_1=0}^{m} \cdots \prod_{i_n=0}^{m} \prod_{k=0}^{i_1+\cdots+i_n} \prod_{j_1=0}^{m-i_1} \cdots \prod_{j_n=0}^{m-i_n} \Big(& X_1^{i_1} \cdots X_n^{i_n} Y^k Z_1^{j_1} \cdots Z_n^{j_n} \\ & (e_1^2)^{m-\min(i_1,k)} \cdots (e_n^2)^{m-\min(i_n,k)} \Big) \\ = X_1^{S_{x_1}} \cdots X_n^{S_{x_n}} Y^{S_y} Z_1^{S_{z_1}} \cdots Z_n^{S_{z_n}} & (e_1^2)^{S_{e_1}} \cdots (e_n^2)^{S_{e_n}},\end{aligned}$$

where

$$\begin{aligned} S_{x_1} + S_{x_2} + \cdots + S_{x_n} &= (\frac{n^2}{18} + \frac{n}{36}) \frac{m^{2n+2}}{2^{n-1}} + o(m^{2n+2}), \\ S_y &= (\frac{n^2}{36} + \frac{n}{72}) \frac{m^{2n+2}}{2^{n-1}} + o(m^{2n+2}), \\ S_{z_1} + S_{z_2} + \cdots + S_{z_n} &= (\frac{n^2}{18} - \frac{n}{72}) \frac{m^{2n+2}}{2^{n-1}} + o(m^{2n+2}), \\ S_{e_1} + S_{e_2} + \cdots + S_{e_n} &= (\frac{n^2}{9} - \frac{n}{72}) \frac{m^{2n+2}}{2^{n-1}} + o(m^{2n+2}). \end{aligned}$$

On the other hand, the dimension is

$$\dim(\mathcal{L}') = \sum_{i_1=0}^{m} \cdots \sum_{i_n=0}^{m} \sum_{k=0}^{i_1+\cdots+i_n} \sum_{j_1=0}^{m-i_1} \cdots \sum_{j_n=0}^{m-i_n} 1 = \frac{n}{6 \cdot 2^{n-1}} m^{2n+1} + o(m^{2n+1}).$$

Please refer to the appendix to see the detailed calculations.

From Lemmas 1 and 2, we can obtain integer equations when

$$\det(\mathcal{L}')^{\frac{1}{\dim(\mathcal{L}')}} < (e_1^2 \cdots e_n^2)^m. \tag{2}$$

Neglecting the low order terms of m and putting $X_l = N^{1+2\delta}, Y = N^{\frac{1}{2}}, Z_l = N^{\delta}$ and $e_l^2 \simeq N^2$ into the above inequality (2), the necessary condition can be written as

$$(1+2\delta)(\frac{n^2}{18} + \frac{n}{36}) + \frac{1}{2}(\frac{n^2}{36} + \frac{n}{72}) + \delta(\frac{n^2}{18} - \frac{n}{72}) + 2(\frac{n^2}{9} + \frac{n}{72}) \le \frac{n^2}{3},$$

namely,

$$\delta < \frac{2n-3}{8n+2}.$$

Then we get $2n+1$ polynomials which share the root $(x_1, \ldots, x_n, y, z_1, \ldots, z_n)$. Under Assumption 1, we can find $x_1, \ldots, x_n, y, z_1, \ldots, z_n$ from these polynomials. This concludes the proof of Theorem 1. □

Moreover, as well as by using Minkowski sum based lattice construction to combine the polynomials $e_l d_{p_l} = k_{p_l}(p-1)+1$, for $l = 1, \cdots, n$, we also introduce an additional variable q to reduce the determinant of our lattice and finally improve our bound of Theorem 1.

More precisely, we firstly construct a lattice which combines the polynomials $f_l(x_l, y) = x_l(y-1) + 1 \pmod{e_l}$, for $l = 1, \cdots, n$ by utilizing Minkowski sum lattice based construction. Then based on an observation of the monomials which appear in the lattice, we found that the desired root p of variable y is a factor of N. Thus, to reduce the determinant of our constructed lattice we can introduce a new variable z which corresponds to q. Since $pq = N$, we can replace yz by N and then by multiplying the inverse of N modulo $e_1 \cdots e_n$. Above all, we can obtain the following theorem.

Theorem 2. *Let $(e_1, e_2, \cdots, e_n)$ be n CRT-RSA encryption exponents with a common modulus $N = pq$, where $n \geq 2$ and $e_1, e_2, \cdots, e_n$ have the roughly same bitlengths as N. Consider that d_{p_l}, d_{q_l} for $l = 1, 2, \cdots, n$ are the corresponding decryption exponents. Assumed that $d_{p_l} < N^{\delta}$ for $l = 1, 2, \cdots, n$, then under Assumption 1, one can factor N in polynomial time when*

$$\delta < \frac{9n-14}{24n+8}.$$

Proof. For each of the key pairs (e_l, d_{p_l}, d_{q_l}), we have that

$$e_l d_{p_l} = k_{p_l}(p-1) + 1,$$

where k_{p_l} is an integer.

Then (k_{p_l}, p) is a solution of

$$f_l(x_l, y) = x_l(y-1) + 1 \pmod{e_l}.$$

Consider the n modular polynomials

$$f_l(x_l, y) = x_l(y-1) + 1 \pmod{e_l}, \text{ for } l = 1, \cdots, n.$$

Obviously, these polynomials have the common root $(x_1, \cdots, x_n, y) = (k_{p_1}, \cdots, k_{p_n}, p)$, and the sizes of its coefficients can be roughly determined as $k_{p_l} \simeq X_l = N^{\frac{1}{2}+\delta}$, for $l = 1, \cdots, n$ and $p \simeq Y = N^{\frac{1}{2}}$.

In order to solve for the desired solution, similarly we firstly selected the following set of polynomials to solve each single modular equation,

$$S_l = \{x_l^{i_l} f_l^{k_l}(x_l, y)(e_l)^{m-k_l} | 0 \leq k_l \leq m, 0 \leq i_l \leq m - k_l\},$$

where $l = 1, \cdots, n$ and m is a positive integer.

Each selection generates a triangular basis matrix. Then, for $l = 1, \cdots, n$ we construct a triangular matrix respectively. We constructed the basis matrix with polynomials which have the same roots as the solutions of the modular equation modulo $(e_1 \cdots e_n)^m$. By combining these n lattices based on a Minkowski sum based lattice construction, the matrix corresponding to the combined lattice $\mathcal{L}_1'$ is triangular and has diagonal entries

$$X_1^{i_1} \cdots X_n^{i_n} Y^k e_1^{m-\min(i_1,k)} \cdots e_n^{m-\min(i_n,k)},$$

where

$$0 \le i_1, \cdots, i_n \le m,\ 0 \le k \le i_1 + i_2 + \cdots + i_n.$$

Moreover, note that the desired small solution contains the prime factor p, which is a factor of the modulus $N = pq$. Then we introduce a new variable z for another prime factor q, and multiply each polynomial corresponding to each row vector in the $\mathcal{L}_1'$ by a power z^s for some s that will be optimized later. Then, we replace every occurrence of the monomial yz by N because $N = pq$. Therefore, compared to the unchanged polynomials, every monomial $x_1^{i_1} \cdots x_n^{i_n} y^k z^s$ and $k \ge s$ with coefficient $a_{i_1,\cdots,i_n,k}$ is transformed into a monomial $x_1^{i_1} \cdots x_n^{i_n} y^{k-s}$ with coefficient $a_{i_1,\cdots,i_n,k} N^s$. Similarly, when $k < s$, the monomial $x_1^{i_1} \cdots x_n^{i_n} y^k z^s$ with coefficient $a_{i_1,\cdots,i_n,k}$ is transformed into monomial $x_1^{i_1} \cdots x_n^{i_n} z^{s-k}$ with coefficient $a_{i_1,\cdots,i_n,k} N^k$. Let $Z = N^{\frac{1}{2}}$ denote the upper bound of the unknown variable z.

To keep the determinant of the lattice as small as possible, we try to eliminate the factor of N^s and N^k in the coefficients of the diagonal entries. Since $(N, e_1 \cdots e_n) = 1$, we only need to multiply the corresponding polynomial with the inverse of N^s or N^k modulo $(e_1 \cdots e_n)^m$.

Then the determinant of the lattice can be calculated as follows,

$$\det(\mathcal{L}_1') = X_1^{S_{x_1}} \cdots X_n^{S_{x_n}} Y^{S_y} Z^{S_z} e_1^{S_{e_1}} \cdots e_n^{S_{e_n}},$$

where

$$\begin{aligned}
S_{x_1} + S_{x_2} + \cdots + S_{x_n} &= \sum_{i_1=0}^{m} \cdots \sum_{i_n=0}^{m} \sum_{k=0}^{i_1+\cdots+i_n} (i_1 + \cdots i_n), \\
S_y &= \sum_{i_1=0}^{m} \cdots \sum_{i_n=0}^{m} \sum_{k=s}^{i_1+\cdots+i_n} (k - s), \\
S_z &= \sum_{i_1=0}^{m} \cdots \sum_{i_n=0}^{m} \sum_{k=0}^{s-1} (s - k), \\
S_{e_1} + S_{e_2} + \cdots + S_{e_n} &= \sum_{i_1=0}^{m} \cdots \sum_{i_n=0}^{m} \sum_{k=0}^{i_1+\cdots+i_n} \big(nm - \\
&\qquad \min(i_1, k) - \cdots - \min(i_n, k)\big).
\end{aligned}$$

Since the following formulas hold for any $0 \leq a, b \leq n$,

$$\sum_{i_1=0}^{m} \cdots \sum_{i_n=0}^{m} i_a i_b = \begin{cases} \frac{1}{3}m^{n+2} + o(m^{n+2}), & (a = b), \\ \frac{1}{4}m^{n+2} + o(m^{n+2}), & (a \neq b), \end{cases}$$

we have that

$$\begin{aligned} S_{x_1} + S_{x_2} + \cdots + S_{x_n} &= (\frac{n^2}{4} + \frac{n}{12})m^{n+2} + o(m^{n+2}), \\ S_y &= (\frac{\sigma^2 n^2}{2} - \frac{\sigma n^2}{2} + \frac{n^2}{8} + \frac{n}{24})m^{n+2} + o(m^{n+2}), \\ S_z &= (\frac{\sigma^2 n^2}{2})m^{n+2} + o(m^{n+2}), \\ S_{e_1} + S_{e_2} + \cdots + S_{e_n} &= (\frac{n^2}{4} + \frac{n}{12})m^{n+2} + o(m^{n+2}). \end{aligned}$$

where $s = \sigma nm$ and $0 \leq \sigma < 1$.

On the other hand, the dimension of the lattice is

$$\dim(\mathcal{L}_1') = \sum_{i_1=0}^{m} \cdots \sum_{i_n=0}^{m} \sum_{k=0}^{i_1+\cdots+i_n} 1 = \frac{n}{2}m^{n+1} + o(m^{n+1}).$$

From Lemmas 1 and 2, we can obtain integer equations when

$$\det(\mathcal{L}_1')^{\frac{1}{\dim(\mathcal{L}_1')}} < (e_1 \cdots e_n)^m. \tag{3}$$

Neglecting the low order terms of m and putting $X_l = N^{\frac{1}{2}+\delta}, Y = N^{\frac{1}{2}}, Z = N^{\frac{1}{2}}$ and $e_l \simeq N$ into the above inequality (3) for $l = 1, \cdots, n$, the necessary condition can be written as

$$(\frac{1}{2} + \delta)(\frac{n^2}{4} + \frac{n}{12}) + \frac{1}{2}(\frac{\sigma^2 n^2}{2} - \frac{\sigma n^2}{2} + \frac{n^2}{8} + \frac{n}{24}) + \frac{1}{2}(\frac{\sigma^2 n^2}{2}) + (\frac{n^2}{4} + \frac{n}{12}) \leq \frac{n^2}{2}.$$

By optimizing $\sigma = \frac{1}{4}$, we finally obtain the following bound on δ

$$\delta < \frac{9n - 14}{24n + 8}.$$

Then under Assumption 1, one can factor N in polynomial time. This concludes the proof of Theorem 2. □

The reason that our result improves over previous work in the literature is based on the following two observations. Firstly, we can combine n polynomials by utilizing the Minkowski sum lattice based construction. Secondly, from the knowledge of $N = pq$, we can optimize the determinant of the lattice by introducing some factor z^s to every polynomials, where z is a new variable corresponding to q and s is an integer which will be optimized during the calculations.

Experimental Results. Note that in the calculations of Theorem 2, we assume that m goes to infinity. Then our result is an asymptotic bound, as we neglect lower order terms of m. If m and n are fixed, the maximum δ satisfying the inequality of condition (3) is easily computed. In Table 3, for each fixed m and n, we list the maximum δ satisfying (3) and the dimension of lattice. The column limit denotes the asymptotic bound.

Table 3. Theoretical bound and lattice dimension for small δ with fixed m.

$n = 2$							
m	5	6	7	8	9	10	∞
s	2	3	3	4	4	5	∞
δ	0.0081	0.0200	0.0244	0.0313	0.0340	0.0385	0.0714
$\dim(\mathcal{L}')$	216	343	512	729	1000	1331	∞
$n = 3$							
m	2	3	4	5	6	7	∞
s	1	2	3	4	4	5	∞
δ	0.0357	0.0746	0.0938	0.1052	0.1127	0.1200	0.1625
$\dim(\mathcal{L}'_1)$	108	352	875	1836	3430	5888	∞

We have implemented the experiment program in Magma 2.11 computer algebra system [3] on a PC with Intel(R) Core(TM) Duo CPU (2.53 GHz, 1.9 GB RAM Windows 7) and carried out the L^3 algorithm [14]. Experimental results are provided in Table 4.

Table 4. Experimental results.

N (bits)	n	theo. of δ	expt. of δ	parameters of lattice	time (in sec.)
1000	3	0.0357	0.0350	$m = 2$, $s = 1$, $\dim(\mathcal{L}'_1) = 108$	3978.213

In the experiments we successfully factored the common modulus N in practice, when there are three decryption exponents and all of them are less than $N^{0.035}$. For this given problem which factor N with small decryption exponent, Jochemsz and May [10] successfully factored N with one small decryption exponent and the bound is $N^{0.015}$, later the bound has been improved to $N^{0.029}$ by utilizing the unraveled linearization technique introduced by Herrmann and May [6]. In other words, we improve both the theoretical and the experimental bound by using more decryption exponents with a common modulus.

Note that in the experiments, we always find many polynomial equations which share the desired solutions over the integers. Moreover we have another

equation $yz = N$. Then by calculating the Gröbner basis of these polynomials, we can successfully solve for the desired solutions in less than two hours.

In all experiments we have done for verification of our proposed attack, we indeed successfully collected the roots by using Gröbner basis technique and there was no experimental result to contradict Assumption 1. On the other hand, however, it seems very difficult to prove or demonstrate its validity.

4 Multiple Encryption and Decryption Exponents Attack of Takagi's Variant RSA

Theorem 3. *Let $(e_1, e_2, \cdots, e_n)$ be n encryption exponents of Takagi's variant of RSA with common modulus $N = p^r q$. Consider that $d_1, d_2, \cdots, d_n$ are the corresponding decryption exponents. Then under Assumption 1, one can factor N in polynomial time when*

$$\delta < \left(\frac{r-1}{r+1}\right)^{\frac{n+1}{n}},$$

where $d_l \leq N^\delta$, for $l = 1, \cdots, n$.

Proof. For one modulus $N = p^r q$, there exist n encryption and decryption exponents (e_l, d_l), thus, we have that

$$\begin{aligned} e_1 d_1 &= k_1 p^{r-1}(p-1)(q-1) + 1, \\ e_2 d_2 &= k_2 p^{r-1}(p-1)(q-1) + 1, \\ &\cdots \\ e_n d_n &= k_n p^{r-1}(p-1)(q-1) + 1. \end{aligned}$$

Hence, for the unknown $(d_1, \cdots, d_n)$ we have the following modular equations,

$$\begin{aligned} f(x_1) &= e_1 x_1 - 1 \pmod{p^{r-1}}, \\ f(x_2) &= e_2 x_2 - 1 \pmod{p^{r-1}}, \\ &\cdots \\ f(x_n) &= e_n x_n - 1 \pmod{p^{r-1}}. \end{aligned}$$

As it is shown, $(d_1, d_2, \cdots, d_n)$ is a root of simultaneous modular univariate linear equations modulo an unknown divisor, and the size is bounded as $d_l \leq N^\delta$, for $l = 1, \cdots, n$.

Using the technique of [4,22], it can be shown that if

$$\delta < \left(\frac{r-1}{r+1}\right)^{\frac{n+1}{n}},$$

these simultaneous modular univariate linear equations can be solved under Assumption 1, which means $(d_1, \cdots, d_n)$ can be recovered. Then one can easily factor N by calculating the common factor. □

Table 5. Factoring N with multiple decryption exponents.

r	$\log_2 N$	$\log_2 p$	$n = 2$				$n = 3$			
			theo.	expt.	dim($\mathcal{L}$)	time (in sec.)	theo.	expt.	dim($\mathcal{L}$)	time (in sec.)
2	1500	500	0.272	0.230	66	2022.834	0.291	0.240	84	1537.078

Experimental Results. We have implemented the experiment program in Magma 2.11. In all experiments, we successfully solved for desired solutions $(d_1, d_2, \cdots, d_n)$. Similarly, there was no experimental result to contradict Assumption 1 Table 5.

Notice that, the previous Theorem 3 can be applied for encryption exponents $(e_1, \cdots, e_n)$ of arbitrary sizes. However, if there exist two valid key pairs (e_1, d_1) and (e_2, d_2), where e_1 and e_2 have roughly the same size as the modulus N or some larger values as N^α. Assume that $d_1 \simeq d_2 \simeq N^\delta$, then we can give an analysis as follows.

Given two equations $e_1 d_1 = k_1 p^{r-1}(p-1)(q-1) + 1$ and $e_2 d_2 = k_2 p^{r-1}(p-1)(q-1) + 1$, we eliminate $p^{r-1}(p-1)(q-1)$ and obtain the following equality,

$$k_2(e_1 d_1 - 1) = k_1(e_2 d_2 - 1)$$

which suggests that we look for small solutions of the polynomial

$$f(x, y) = e_2 x + y \pmod{e_1}. \tag{4}$$

Since $(d_2 k_1, k_2 - k_1)$ is a root of $f(x, y) \bmod e_1$. The bound of k_1 can be estimated as $N^{\alpha+\delta-1}$, hence we define the bounds $|d_2 k_1| \simeq X = N^{\alpha+2\delta-1}$ and $|k_2 - k_1| \simeq Y = N^{\alpha+\delta-1}$. For this linear modular equation, we can recover $(d_2 k_1, k_2 - k_1)$ for sufficiently large N provided that $XY < e$, or $\alpha + 2\delta - 1 + \alpha + \delta - 1 < \alpha$.

Thus, to recover $d_2 k_1$ and $k_2 - k_1$ from this lattice-based method, the size of the encryption and decryption exponents should satisfy

$$\alpha + 3\delta < 2,$$

where $\alpha + \delta > 1$.

5 Conclusion

In this paper, we presented some applications of Minkowski sum based lattice construction and gave analyses of the case that multiple pairs of encryption and decryption exponents are used with the common CRT-RSA modulus N. We showed that one can factor N when both $d_{p_i}, d_{q_i} \leq N^{\frac{2l-3}{8l+2}}$ or either d_{p_i} or d_{q_i} is less than $N^{\frac{9l-14}{24l+8}}$, for $i = 1, 2, \cdots, l$. Moreover, we also analyzed the situation when more than one encryption and decryption exponents are used in Takagi's variant of RSA with modulus $N = p^r q$.

Acknowledgements. The authors would like to thank anonymous reviewers for their helpful comments and suggestions. The work of this paper was supported by the National Key Basic Research Program of China (Grants 2013CB834203 and 2011CB302400), the National Natural Science Foundation of China (Grants 61472417, 61402469, 61472416 and 61272478), the Strategic Priority Research Program of Chinese Academy of Sciences under Grant XDA06010702 and XDA06010703, and the State Key Laboratory of Information Security, Chinese Academy of Sciences. Y. Lu is supported by Project CREST, JST.

Appendix

Here we present the detailed calculations of $S_{X_1}, S_Y, S_{Z_1}, S_{e_1}$.

Let $\sum^*$ denotes $\sum_{i_1=0}^{m} \cdots \sum_{i_n=0}^{m} \sum_{j_1=0}^{m-i_1} \cdots \sum_{j_n=0}^{m-i_n}$, for any $0 \le a, b \le n$, we have that

$$\sum^* i_a i_b = \begin{cases} \frac{1}{12*2^{n-1}} * m^{2n+2} + o(m^{2n+2}), & (a = b), \\ \frac{1}{18*2^{n-1}} * m^{2n+2} + o(m^{2n+2}), & (a \neq b), \end{cases}$$

and

$$\sum^* i_a j_b = \begin{cases} \frac{1}{24*2^{n-1}} * m^{2n+2} + o(m^{2n+2}), & (a = b), \\ \frac{1}{18*2^{n-1}} * m^{2n+2} + o(m^{2n+2}), & (a \neq b). \end{cases}$$

Then we obtain that

$$\sum^* \sum_{k=0}^{i_1+\cdots+i_n} i_1 + \cdots + i_n = (\frac{n^2}{18} + \frac{n}{36}) * \frac{m^{2n+2}}{2^{n-1}} + o(m^{2n+2}),$$

$$\sum^* \sum_{k=0}^{i_1+\cdots+i_n} j_1 + \cdots + j_n = (\frac{n^2}{18} - \frac{n}{72}) * \frac{m^{2n+2}}{2^{n-1}} + o(m^{2n+2}),$$

$$\begin{aligned} \sum^* \sum_{k=0}^{i_1+\cdots+i_n} k &= \sum^* \frac{(i_1 + \cdots + i_n)^2}{2} + \frac{i_1 + \cdots + i_n}{2} \\ &= (\frac{n^2}{36} + \frac{n}{72}) * \frac{m^{2n+2}}{2^{n-1}} + o(m^{2n+2}). \end{aligned}$$

Moreover,

$$\begin{aligned} \sum^* \sum_{k=0}^{i_1+\cdots+i_n} \min(i_1, k) &= \sum^* (\sum_{k=0}^{i_1} k + \sum_{k=i_1+1}^{i_1+\cdots+i_n} i_1) \\ &= \sum^* (\frac{i_1(i_1+1)}{2} + i_1(i_2 + \cdots + i_n)) \\ &= (\frac{n}{18} - \frac{1}{72}) * \frac{m^{2n+2}}{2^{n-1}} + o(m^{2n+2}). \end{aligned}$$

By symmetry, we have

$$\sum^{*} \sum_{k=0}^{i_1+\cdots+i_n} \min(i_1,k)+\cdots+\min(i_n,k) = (\frac{n^2}{18}-\frac{n}{72}) * \frac{m^{2n+2}}{2^{n-1}} + o(m^{2n+2}).$$

The dimension of lattice $\mathcal{L}'$ is

$$\dim(\mathcal{L}') = \sum^{*} \sum_{k=0}^{i_1+\cdots+i_n} 1 = \frac{n}{6*2^{n-1}} * m^{2n+1} + o(m^{2n+1}).$$

References

1. Aono, Y.: Minkowski sum based lattice construction for multivariate simultaneous Coppersmith's technique and applications to RSA. In: Boyd, C., Simpson, L. (eds.) ACISP. LNCS, vol. 7959, pp. 88–103. Springer, Heidelberg (2013)
2. Boneh, D., Durfee, G.: Cryptanalysis of RSA with private key d less than $N^{0.292}$. IEEE IEEE Trans. Inf. Theory **46**(4), 1339–1349 (2000)
3. Bosma, W., Cannon, J.J., Playoust, C.: The MAGMA algebra system I: the user language. J. Symbolic Comput. **24**(3/4), 235–265 (1997)
4. Cohn, H., Heninger, N.: Approximate common divisors via lattices. CoRR abs/1108.2714 (2011)
5. Coppersmith, D.: Small solutions to polynomial equations, and low exponent RSA vulnerabilities. J. Cryptology **10**(4), 233–260 (1997)
6. Herrmann, M., May, A.: Maximizing small root bounds by linearization and applications to small secret exponent RSA. In: Nguyen, P.Q., Pointcheval, D. (eds.) PKC 2010. LNCS, vol. 6056, pp. 53–69. Springer, Heidelberg (2010)
7. Howgrave-Graham, N.: Finding small roots of univariate modular equations revisited. In: Darnell, M.J. (ed.) Cryptography and Coding 1997. LNCS, vol. 1355. Springer, Heidelberg (1997)
8. Howgrave-Graham, N., Seifert, J.-P.: Extending Wiener's attack in the presence of many decrypting exponents. In: Baumgart, R. (ed.) CQRE 1999. LNCS, vol. 1740, pp. 153–166. Springer, Heidelberg (1999)
9. Jochemsz, E., May, A.: A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants. In: Lai, X., Chen, K. (eds.) ASIACRYPT 2006. LNCS, vol. 4284, pp. 267–282. Springer, Heidelberg (2006)
10. Jochemsz, E., May, A.: A polynomial time attack on RSA with private CRT-exponents smaller than $N^{0.073}$. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 395–411. Springer, Heidelberg (2007)
11. Lenstra, A.K., Lenstra, H.W., Lovász, L.: Factoring polynomials with rational coefficients. Mathematische Annalen **261**(4), 515–534 (1982)
12. Lu, Y., Zhang, R., Peng, L., Lin, D.: Solving linear equations modulo unknown divisors: revisited. In: ASIACRYPT 2015 (2015) (to appear). https://eprint.iacr.org/2014/343
13. May, A.: Secret exponent attacks on RSA-type schemes with moduli $N = p^r q$. In: Bao, F., Deng, R., Zhou, J. (eds.) PKC 2004. LNCS, vol. 2947, pp. 218–230. Springer, Heidelberg (2004)
14. Nguên, P.Q., Stehlé, D.: Floating-point LLL revisited. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 215–233. Springer, Heidelberg (2005)

15. Nguyen, P.Q., Vallée, B. (eds.): The LLL Algorithm - Survey and Applications. Information Security and Cryptography. Springer, Heidelberg (2010)
16. Rivest, R.L., Shamir, A., Adleman, L.M.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **21**(2), 120–126 (1978)
17. Sarkar, S.: Small secret exponent attack on RSA variant with modulus $N = p^r q$. Des. Codes Crypt. **73**(2), 383–392 (2014)
18. Sarkar, S., Maitra, S.: Cryptanalysis of RSA with more than one decryption exponent. Inf. Process. Lett. **110**(8–9), 336–340 (2010)
19. Simmons, G.J.: A weak privacy protocol using the RSA cryptalgorithm. Cryptologia **7**(2), 180–182 (1983)
20. Sun, H., Wu, M.: An approach towards rebalanced RSA-CRT with short public exponent. IACR Cryptology ePrint Archive **2005**, 53 (2005)
21. Takagi, T.: Fast RSA-type cryptosystem modulo $p^k q$. In: CRYPTO 1998. vol. 1462, pp. 318–326 (1998)
22. Takayasu, A., Kunihiro, N.: Better lattice constructions for solving multivariate linear equations modulo unknown divisors. In: Boyd, C., Simpson, L. (eds.) ACISP. LNCS, vol. 7959, pp. 118–135. Springer, Heidelberg (2013)
23. Takayasu, A., Kunihiro, N.: Cryptanalysis of RSA with multiple small secret exponents. In: Susilo, W., Mu, Y. (eds.) ACISP 2014. LNCS, vol. 8544, pp. 176–191. Springer, Heidelberg (2014)
24. Wiener, M.J.: Cryptanalysis of short RSA secret exponents. IEEE Trans. Inf. Theory **36**(3), 553–558 (1990)