Further Cryptanalysis of a Type of RSA Variants

Gongyu Shi, Geng Wang(✉), and Dawu Gu(✉)

School of Electronic Information and Electrical Engineering,
Shanghai Jiao Tong University, Shanghai 200240, P.R.China
{gy_shi,wanggxx,dwgu}@sjtu.edu.cn

Abstract. To enhance the security or the efficiency of the standard RSA cryptosystem, some variants have been proposed based on elliptic curves, Gaussian integers or Lucas sequences. A typical type of these variants which we called Type-A variants have the specified modified Euler's totient function $\psi(N) = (p^2 - 1)(q^2 - 1)$. But in 2018, based on cubic Pell equation, Murru and Saettone presented a new RSA-like cryptosystem, and it is another type of RSA variants which we called Type-B variants, since their scheme has $\psi(N) = (p^2 + p + 1)(q^2 + q + 1)$. For RSA-like cryptosystems, four key-related attacks have been widely analyzed, i.e., the small private key attack, the multiple private keys attack, the partial key exposure attack and the small prime difference attack. These attacks are well-studied on both standard RSA and Type-A variants. Recently, the small private key attack on Type-B variants has also been analyzed. In this paper, we make further cryptanalysis of Type-B variants, that is, we propose the first theoretical results of multiple private keys attack, partial key exposure attack as well as small prime difference attack on Type-B variants, and the validity of our attacks are verified by experiments. Our results show that for all three attacks, Type-B variants are less secure than standard RSA.

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

1 Introduction

1.1 Background

Rivest, Shamir and Adleman [24] proposed the RSA cryptosystem in 1978, which is one of the oldest public-key cryptosystems and is still widely used nowadays.

In the standard RSA cryptosystem, the public modulus N is a product of two large primes p, q, namely, $N = pq$. Then select two integers e, d such that $ed \equiv 1 \pmod{\varphi(N)}$, where $\varphi(N) = (p-1)(q-1)$ is Euler's totient function. And (N, e) is the public key used to encrypt, (p, q, d) is the private key used to decrypt. To encrypt a message $m < N$, one computes $c := m^e \mod N$, while to decrypt the ciphertext c, one needs to compute $c^d \mod N$. It is recommended to choose p and q of the same size such that $q < p < 2q$, which is called balanced RSA. In this paper, we only consider the balanced cases of the RSA cryptosystem and

its variants. For convenience, we may represent the public exponent e as well as the secret exponent d with $e = N^{\alpha}$ and $d = N^{\beta}$ respectively.

To enhance the security or improve the efficiency, some researchers proposed variants of the standard RSA cryptosystem by modifying the underlying group, e.g., Elliptic curves based [18], Gaussian integers based [11] and Lucas sequences based [7]. In fact, all the variants proposed in [18,11,7] have the same modified Euler's totient function $\psi(N) = (p^2 - 1)(q^2 - 1)$, while the modulus $N = pq$ remains unchanged as the standard RSA. And we call these typical schemes with that specified Euler's totient function Type-A variants in the following texts.

But recently, Murru and Saettone, two Italian researchers from the University of Turin, proposed a new RSA variant with the modified Euler's totient function $\psi(N) = (p^2 + p + 1)(q^2 + q + 1)$ [21]. This cryptosystem is based on the cubic Pell equation, and it defines a non-standard product over a particular group. The authors claimed their scheme is more secure than standard RSA in some circumstances, as this variant scheme is robust against Hastad's broadcast attack [13] and Wiener's small private key attack [30]. And in this paper, we call the variants with $\psi(N) = (p^2 + p + 1)(q^2 + q + 1)$ Type-B variants. Note that one may create new Type-B cryptosystems based on other algebra structure, but it will also suffer from the attacks proposed in this paper, as our attacks do not rely on the structure of the underlying group and are general for Type-B variants.

The following paragraphs introduce four common key-related attacks on RSA-like cryptosystems, e.g., the small private key attack, the multiple private keys attack, the partial key exposure attack and the small prime difference attack.

Small Private Key Attack. In 1990, Wiener showed that if the private key d of an RSA cryptosystem is less than $\frac{1}{3}N^{0.25}$, then one can easily recover d using continued fraction. Specifically, one may find d from the continued fraction expansion of $\frac{e}{N}$. Later, Wiener's bound was improved by Boneh and Durfee [4] to $N^{0.284}$, respectively $N^{0.292}$. They used Coppersmith's lattice-based method [9] to find small roots of the modular equation $x(y + \frac{N+1}{2}) + 1 \equiv 0 \pmod{e}$. In 2010, Herrmann and May [14] obtained the same bound $d < N^{0.292}$, but with a smaller lattice dimension using the technique of unravelled linearization.

The small private key attack on Type-A variants has also been studied. Bunder et al. [6] proposed the first attack based on continued fraction, and the attack was improved in [6,23] using Coppersmith's method, which yields the best bound so far $d < N^{0.585}$.

Recently, the small private key attack on Type-B variants has been analyzed in several papers. In [26,22], it was found that Wiener's method still works. Furthermore, the use of Coppersmith's method has also been explored. Nitaj et al. [22] showed Type-B variants can be broken if $d < N^{0.569}$, and Zheng et al. [32] got a higher bound $d < N^{0.585}$ using an optimized construction.

Multiple Private Keys Attack. Howgrave-Graham and Seifert [16] first studied the case when given multiple public keys with the same modulus ($e_i \approx$

$N^{\alpha}, N)$ that correspond to some small private keys $d_i \approx N^{\beta}$ in 1999. Later, their attack was improved successively by Sarkar and Maitra [25] and Aono [1] using Coppersmith's method. In 2014, Takayasu and Kunihiro [27] proposed the best bound so far, their attack works if $\beta < 1 - \sqrt{\frac{2}{3l+1}}$ and l is the number of obtained keys. When $l = 1$, one can find their attack achieves Boneh and Durfee's stronger bound $\beta < 0.292$.

The multiple private keys attack on Type-A variants has been studied by Zheng et al. [31]. Their attack works if $\beta < 2 - 2\sqrt{\frac{2}{3l+1}}$, and the bound is exactly twice of that on standard RSA.

Partial Key Exposure Attack. In 1998, Boneh et al. [5] first introduced the partial key exposure attack on standard RSA [5], where the attackers are given some most/least significant bits (MSBs/LSBs) of the private key d. The original attack only works for small e, but in 2003, Blömer and May [3] showed that there exists attack for larger e up to $N^{\frac{7}{8}}$. Then, in 2005, Ernst et al. [12] extended the bound to full size e. Later, the partial key exposure attack for small d has been improved by Takayasu and Kunihiro [28], which can achieve Boneh and Durfee's stronger bound in both MSBs and LSBs leakage scenarios.

Zheng et al. [31] studied the partial key exposure attack on Type-A variants. And their attack only covers a weaker bound $d < N^{0.569}$ instead of the best bound of small private key attack on Type-A variants $d < N^{0.585}$.

Small Prime Difference Attack. In 2002, de Weger [10] proposed an attack on standard RSA where the difference of prime factors $|p-q|$ is small. His results showed that under this specified scenario, the small private key attack based on Wiener's method, as well as Boneh and Durfee's method, can both obtain a better bound.

Recently, Cherkaoui-Semmouni et al. [8] studied the small prime difference attack on Type-A variants. And their attack can retrieve the best bound of small private key attack on Type-A variants $d < N^{0.585}$ under the common condition $|p - q| \approx N^{\frac{1}{2}}$.

As stated above, one can find Type-A variants are less secure than standard RSA against all four attacks. And Type-B variants are weaker than standard RSA on small private key attack. Note that the multiple private keys attack, the partial key exposure attack as well as the small prime difference attack on Type-B variants have not been studied yet.

1.2 Our Contributions

In this paper, we make a further cryptanalysis of Type-B RSA variants (i.e., RSA variants with the Euler's totient function $\psi(N) = (p^2+p+1)(q^2+q+1)$), that is, we propose the theoretical bounds of the multiple private keys attack, the partial key exposure attack, as well as the small prime difference attack on Type-B variants for the first time, and we verify the validity of all three attacks

with experiments. What's more, for all three attacks, we consider a more general case for arbitrary α [1].

The results of our three attacks, in addition with the bounds of those attacks as well as the small private key attack on standard RSA and Type-A variants are given in Table 1.

Table 1. Summary of four attacks on standard RSA, Type-A and Type-B variants

	Standard RSA [24]	Type-A [18,11,7]	Type-B [21]
Euler's totient function	$\varphi(N) = (p-1)(q-1)$	$\psi(N) = (p^2-1)(q^2-1)$	$\psi(N) = (p^2+p+1)(q^2+q+1)$
Small Private Key Attack	$\beta < 1 - \frac{\sqrt{2}}{2}$ [4,2]	$\beta < 2 - \sqrt{2}$ [23,31]	$\beta < 2 - \sqrt{2}$ [32]
Multiple Private Keys Attack[1]	$\beta < 1 - \sqrt{\frac{2}{3l+1}}$ [27]	$\beta < 2 - 2\sqrt{\frac{2}{3l+1}}$ [31]	$\beta < \frac{3}{2} - \frac{4}{3l+1}$ [**Section 3**]
Partial Key Exposure Attack[2]	$\beta < \frac{\gamma+2-\sqrt{2-3\gamma^2}}{2}$ [28]	$\beta < \frac{3\gamma+7-2\sqrt{3\gamma+7}}{3}$ [31]	$\beta < \frac{3\gamma+7-2\sqrt{3\gamma+7}}{3}$ [**Section 4**]
Small Prime Difference Attack[3]	$\beta < 1 - \sqrt{2\delta - \frac{1}{2}}$ [10]	$\beta < 2 - 2\sqrt{\delta}$ [8]	$\beta < 2 - \sqrt{8\delta - 2}$ [**Section 5**]

[*] $e = N^\alpha$ is the public exponent, $d = N^\beta$ is the secret exponent. For comparison, we take $\alpha = 1$ for standard RSA, $\alpha = 2$ for Type-A and Type-B variants, since some previous works only give the results for fixed α.
[1] l is the number of keys obtained.
[2] $\tilde{d} = N^\gamma$ and $\bar{d} = N^{\beta-\gamma}$ are the known leaked part and the unknown part of d respectively.
[3] $|p - q| = N^\delta$ is the prime difference.

From the table above, we can learn that Type-B variants are weaker against all four attacks compared with standard RSA, and this property is similar as Type-A variants. Especially for the small prime difference attack, Type-B variants are even less secure than Type-A variants. We will give a detailed analysis and discussion later in the main body.

1.3 Organization

The rest of this paper is organized as follows. In Section 2, we give some notations and describe some important lemmas used in our attacks. From Section 3 to Section 5, we propose our multiple private keys attack, partial key exposure attack and small prime difference attack on Type-B RSA variants respectively. In Section 6, we verify the validity of all three attacks by computer experiments. Finally, we conclude the paper in Section 7.

2 Preliminaries

In this section, we first give some notations, then introduce the lattice reduction technique and Coppersmith's method used in our attack.

Minkowski sum. Let $\mathcal{A}$ and $\mathcal{B}$ be two finite subsets of $\mathbb{Z}^n$, their Minkowski sum is denoted by $\mathcal{A} \boxplus \mathcal{B} := \{(a_1+b_1, \ldots, a_n+b_n) : (a_1, \ldots, a_n) \in \mathcal{A}, (b_1, \ldots, b_n) \in \mathcal{B}\}$. And it can be similarly extended to three or more sets.

[1] Since e is typically of the same order of magnitude as $\psi(N)$ for small d, we can fix $\alpha = 2$ in our case. But Wiener [30] suggests one can add extra $\psi(N)$ to e, which yields larger α.

Multivariate terms order. In this paper, polynomials and monomials are ordered in *lexicographic* order by default. For example, $x_1^{i_1}x_2^{i_2} \prec x_1^{i_1'}x_2^{i_2'} \Leftrightarrow i_1 < i_1'$ or $i_1 = i_1', i_2 < i_2'$. The maximum monomial of each polynomial f in lexicographic order is called the head term, and its coefficient is called the head coefficient, denoted as $\mathrm{HC}(f)$.

Euclidean norm. For a vector $\mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{R}^n$, its Euclidean norm is denoted as $\|\mathbf{b}\| := \sqrt{\sum_{i=1}^{n} b_i^2}$. For a polynomial $f(x_1, \ldots, x_n) := \sum a_{i_1,\ldots,i_n} x_1^{i_1} \ldots x_n^{i_n}$, its Euclidean norm is defined as the Euclidean norm of its coefficients vector: $\|f(x_1, \ldots, x_n)\| := \sqrt{\sum |a_{i_1,\ldots,i_n}|^2}$, while its infinity norm is defined as the maximum term of its coefficients vector: $\|f(x_1, \ldots, x_n)\|_\infty := \max\{|a_{i_1,\ldots,i_n}|\}$.

Lattice. A lattice $\mathcal{L}$ spanned by ω linearly independent row vectors $\mathbf{b}_1, \ldots, \mathbf{b}_\omega \in \mathbb{R}^n$ is the set of their integer linear combinations, denoted as $\mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_\omega) := \{\sum_{i=1}^{\omega} z_i \mathbf{b}_i : z_i \in \mathbb{Z}\}$. The vectors $(\mathbf{b}_1, \ldots, \mathbf{b}_\omega)$ are called a basis of $\mathcal{L}$, and it can be represented with the basis matrix $\mathbf{B} \in \mathbb{R}^{\omega \times n}$ which contains $\mathbf{b}_1, \ldots, \mathbf{b}_\omega$ in each row. We call n the dimension of $\mathcal{L}$, and ω the rank of $\mathcal{L}$. If $\omega = n$, we call $\mathcal{L}$ is a full-rank lattice. The determinant of $\mathcal{L}$ is defined as $\det(\mathcal{L}) := \sqrt{\det(\mathbf{B}\mathbf{B}^T)}$, where $\mathbf{B}^T$ is the transpose of $\mathbf{B}$. We have $\det(\mathcal{L}) = |\det(\mathbf{B})|$ for a full-rank lattice.

In 1982, Lenstra, Lenstra and Lovász [19] proposed the LLL algorithm to find non-zero short lattice vectors in polynomial time, which is widely used in lattice-based cryptanalysis. And according to [20], the output of the LLL algorithm satisfies the following property.

Lemma 1 (LLL algorithm). *Let $\mathcal{L}$ be a lattice spanned by a basis $(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_\omega)$, the LLL algorithm finds a reduced basis $(\tilde{\boldsymbol{b}}_1, \ldots, \tilde{\boldsymbol{b}}_\omega)$ of $\mathcal{L}$ satisfying*

$$\|\tilde{\boldsymbol{b}}_1\| \leq \cdots \leq \|\tilde{\boldsymbol{b}}_i\| \leq 2^{\frac{\omega(\omega-1)}{4(\omega+1-i)}} \det(\mathcal{L})^{\frac{1}{\omega+1-i}}, \text{for } i = 1, 2, \ldots, \omega$$

in time polynomial in the dimension n and the size of entries in the basis matrix of $\mathcal{L}$.

One of the applications of the LLL algorithm in cryptanalysis is Coppersmith's method. In [9], Coppersmith proposed rigorous techniques to find small integer solutions of a univariate modular equation $f(x) = 0 \pmod N$ and a bivariate integer equation $f(x, y) = 0$. Both can be heuristically extended to more multivariate cases with reasonable assumptions.

We focus on the modular equation case here. Howgrave-Graham [15] reformulated this method and showed how to judge whether the roots of a modular equation are also roots over integers as follows:

Lemma 2 (Howgrave-Graham). *Let $h(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ be a polynomial with at most ω monomials and M be a positive integer. Suppose that*

1) *$h(x_1', \ldots, x_n') \equiv 0 \pmod M$ where $|x_1'| < X_1, \ldots, |x_n'| < X_n$, and*
2) *$\|h(x_1X_1, \ldots, x_nX_n)\| < \frac{M}{\sqrt{\omega}}$.*

Then $h(x_1', \ldots, x_n') = 0$ holds over the integers.

The main idea of Coppersmith's method is to construct a set of so-called shift polynomials that have the common small roots modular an integer, then apply the LLL algorithm to reduce them to several new polynomials over integers which are easier to solve.

Specifically, we can construct a lattice with the basis containing the coefficients vectors of each shift polynomials, and the LLL reduction algorithm may output several short vectors in the lattice corresponding to the norm of polynomials. If they are small enough to satisfy the bound in Lemma 2, then these equations will hold over integers. Combing with Lemma 1, we obtain

$$2^{\frac{\omega(\omega-1)}{4(\omega+1-i)}} \det(\mathcal{L})^{\frac{1}{\omega+1-i}} < \frac{M}{\sqrt{\omega}}.$$

Since the value of the determinant and M grows significantly faster than the other terms in our case, it can be transformed to the simplified condition

$$\det(\mathcal{L}) < M^{\omega}. \tag{1}$$

Finally, we can use the resultant technique or the Gröbner basis technique to extract the common roots. Note that both techniques require the polynomials we get after reduction are algebraic independent. But no existed method can guarantee the algebraic independence, thus Coppersmith's method is heuristic in this case. In this paper, we make the following assumption just as numerous previous works [4,1,27,32,22].

Assumption 1 *The reduced lattice basis yields algebraically independent polynomials.*

The following lemma proposed by de Weger [10] gives a range of the sum of two integers when their difference is known.

Lemma 3. *Let $N = pq$ be a product of two integers p, q and $\delta = p - q$ is their difference. Then*

$$0 < p + q - 2N^{\frac{1}{2}} < \frac{\delta^2}{4N^{\frac{1}{2}}}.$$

3 Multiple Private Keys Attack

In this section, we propose the multiple private keys attack on Type-B RSA variants.

We consider the situation where the attacker obtained l public key pairs $(e_1, N), \ldots, (e_l, N)$ with a common modulus N, and they correspond to some small $d_1, \ldots, d_l$. All the public exponents e_k and the secret exponents d_k are assumed to be the same size respectively. The goal is to factor N efficiently.

Theorem 1. *Let $N = pq$ be a modulus of Type-B RSA variants with $q < p < 2q$. For integers $l \geq 2$, $1 \leq k \leq l$, let $e_k = N^{\alpha}, d_k = N^{\beta}$ be a valid pair of public*

and secret exponents such that $e_k d_k \equiv 1 \mod (p^2+p+1)(q^2+q+1)$. *Then for* $\frac{1}{2} + \frac{1}{3l-1} < \alpha < \frac{3}{4} + \frac{9l}{4}$, *one can factor* N *in polynomial time if*

$$\beta < \frac{3}{2} - \frac{2\alpha}{3l+1}.$$

Proof. We can rewrite the known equations as

$$\begin{aligned} & e_k d_k \equiv 1 \pmod{(p^2+p+1)(q^2+q+1)} \\ \Rightarrow \quad & e_k d_k = r_k(N^2 + (N+1)(p+q) + p^2 + q^2 + N + 1) + 1 \\ \Rightarrow \quad & e_k d_k = r_k((p+q)^2 + a(p+q) + b) + 1, \end{aligned}$$

where $a := N+1, b := N^2 - N + 1$.

Then we need to solve the following modular equations simultaneously:

$$\begin{cases} f_1(x_1, y) := x_1(y^2 + ay + b) + 1 \equiv 0 \pmod{e_1}, \\ f_2(x_2, y) := x_2(y^2 + ay + b) + 1 \equiv 0 \pmod{e_2}, \\ \qquad \vdots \\ f_l(x_l, y) := x_l(y^2 + ay + b) + 1 \equiv 0 \pmod{e_l}, \end{cases} \tag{2}$$

where the roots $(x_1, x_2, \ldots, x_l, y)$ are $(r_1, r_2, \ldots, r_l, p+q)$, and their values are bounded with $X_1 = X_2 = \cdots = X_l = N^{\alpha+\beta-2}$ and $Y \approx N^{0.5}$.

To solve this problem, we use the Minkowski sum based lattice construction technique proposed by Aono [1].

At first, we define the set of shift polynomials $\mathcal{G}_k (1 \le k \le l)$ and its index set $\mathcal{I}_k$ as

$$\begin{aligned} & j'_k := 2j_k + h_k, \\ & g^{(k)}_{i_k, j'_k}(x_k, y) := x_k^{i_k - j_k} f_k(x_k, y)^{j_k} e_k^{m - j_k} y^{h_k}, \\ & \mathcal{G}_k := \{g^{(k)}_{i_k, j'_k} : 0 \le i_k \le m, 0 \le j_k \le i_k, 0 \le h_k \le 1\}, \\ & \mathcal{I}_k := \{(\underbrace{0, \ldots, 0}_{k-1}, i_k, \underbrace{0, \ldots, 0}_{l-k}, j'_k) : 0 \le i_k \le m, 0 \le j_k \le i_k, 0 \le h_k \le 1\}, \end{aligned}$$

where i_k, j_k, h_k are non-negative integers and m is a fixed positive integer. It is clear that $g^{(k)}_{i_k, j'_k} \equiv 0 \pmod{e_k^m}$. And each index vector stores the maximum exponents of variables x_k, y in the corresponding polynomials.

Then, the Minkowski sum of all index set in our case is defined as

$$\mathcal{I}_+ := \mathcal{I}_1 \boxplus \cdots \boxplus \mathcal{I}_l = \{(i_1, \ldots, i_l, j) : 0 \le i_1, \ldots, i_l \le m, 0 \le j \le 2\sum\nolimits_{k=1}^{l} i_k + l\}.$$

For each $(i_1, \ldots, i_l, j) \in \mathcal{I}_+$, we can define a corresponding polynomial and obtain a new polynomial set:

$$\begin{aligned} g_{i_1, \ldots, i_l, j} &:= \sum_{\sum_{k=1}^{l} j'_k = j} c_{j'_1, \ldots, j'_l} g^{(1)}_{i_1, j'_1} \cdots g^{(l)}_{i_l, j'_l}, \\ \mathcal{G}_+ &:= \{g_{i_1, \ldots, i_l, j} : (i_1, \ldots, i_l, j) \in \mathcal{I}_+\}. \end{aligned}$$

According to the definition of the Minkowski sum lattice, $c_{j'_1,\ldots,j'_l}$ are some selected integers such that the following equation holds:

$$\begin{aligned}\mathrm{HC}(g_{i_1,\ldots,i_l,j}) &= \underset{\sum_{k=1}^{l} j'_k = j}{\mathrm{GCD}} (\mathrm{HC}(g^{(1)}_{i_1,j'_1} \cdots g^{(l)}_{i_l,j'_l})) \\ &= \underset{\sum_{k=1}^{l} j'_k = j}{\mathrm{GCD}} (e_1^{m-\lfloor \frac{j'_1}{2} \rfloor} \cdots e_l^{m-\lfloor \frac{j'_l}{2} \rfloor}),\end{aligned} \tag{3}$$

where $\mathrm{HC}(f)$ means the coefficient of the head term of f in lexicographic order.

Each j'_k can move from 0 to $\min(2i_k + 1, j)$, so we can transform Eq.(3) to

$$\mathrm{HC}(g_{i_1,\ldots,i_l,j}) = e_1^{m-\min(i_1,\lfloor \frac{j}{2} \rfloor)} \cdots e_l^{m-\min(i_l,\lfloor \frac{j}{2} \rfloor)}. \tag{4}$$

Now, consider the lattice basis matrix of each $\mathcal{G}_k$, which is generated by taking the coefficients vector of $g^{(k)}_{i_k,j'_k}(X_k x_k, Y y)$ for each $g^{(k)}_{i'_k,j'_k} \in \mathcal{G}_k$. By ordering polynomials corresponding to rows and monomials corresponding to columns in lexicographic order, as shown in [22], the basis matrix will be lower triangular. Then, according to [1], the Minkowski sum lattice basis matrix of $\mathcal{G}_+$ is also lower triangular. Furthermore, we can learn the diagonal element in this basis matrix are exactly the result of Eq.(4) multiple with the powers of the bounds of each variable, so the determinant will be

$$\det(\mathcal{L}) = \prod_{(i_1,\ldots,i_l,j)\in\mathcal{I}_+} e_1^{m-\min(i_1,\lfloor \frac{j}{2} \rfloor)} \cdots e_l^{m-\min(i_l,\lfloor \frac{j}{2} \rfloor)} X_1^{i_1} \cdots X_l^{i_l} Y^j.$$

Notice that each polynomial in the form $g^{(k)}_{i_k,j'_k}$ equals to zero modulo e_k^m, thus, for each $g_{i_1,\ldots,i_l,j} \in \mathcal{G}_+$, we have $g_{i_1,\ldots,i_l,j} \equiv 0 \pmod{(e_1 \cdots e_l)^m}$.

Then substitute the above $\det(\mathcal{L})$ into Eq.(1), and set $e_k = N^\alpha$, $X_k = N^{\alpha+\beta-2}$, $Y = N^{0.5}$, $M = (e_1 \cdots e_l)^m$, after some computations (details can be found in Appendix A), we may obtain the condition

$$-\alpha(\frac{l^2}{2} - \frac{l}{6}) + (\alpha + \beta - 2)(\frac{l^2}{2} + \frac{l}{6}) + (\frac{l^2}{4} + \frac{l}{12}) < 0, \tag{5}$$

which yields the bound of β as

$$\beta < \frac{3}{2} - \frac{2\alpha}{3l+1}. \tag{6}$$

On the other hand, we must have $\beta > 0$ and $\alpha + \beta > 2$, which gives the range of valid α as

$$\frac{1}{2} + \frac{1}{3l-1} < \alpha < \frac{3}{4} + \frac{9l}{4}. \tag{7}$$

If the conditions in Eq.(7) and Eq.(6) are satisfied, with Assumption 1, we may construct $l+1$ polynomials over integers from the reduced lattice, then extract the shared common root $(x_1, x_2, \ldots, x_l, y) = (r_1, r_2, \ldots, r_l, p+q)$ using the Gröbner basis method. And the knowledge of $p+q$ yields a factorization of N. This terminates the proof. □

The validity of our multiple private keys attack has been verified by experiments, and the results are given in Table 2 in Section 6.

Comparison with small private key attack using Coppersmith's method on Type-B variants. Set $l = 1$ in our attack, the bound becomes $\beta < \frac{3}{2} - \frac{\alpha}{2}$, which is weaker than the bound in [22,32], thus our attack is not a tight extension of the small private key attack. This is mainly because they use several extra y-shift polynomials and the number is related to a tweakable parameter τ. By optimizing the value of τ, one can always get the best bound. In our attack, we just pick the basic shift polynomials, as many previous works involving the Minkowski sum lattice construction [1,27,31].

Comparison with multiple private keys attack on standard RSA and Type-A variants. According to Table 1, the bound of small private key attack on Type-A and Type-B variants are exactly the same. So we may expect they also have the same bound on multiple private keys attack. However, this is not the case in our attack. Typically, when d is small, e will be of the same order of magnitude as $\psi(N)$, which implies $\alpha = 2$ in our case, the bound of β becomes $\beta < \frac{3}{2} - \frac{4}{3l+1}$, which is exactly twice the bound of multiple private keys attack on standard RSA obtained by Aono [1]. Note that Aono's original attack has been improved by Takayasu and Kunihiro [27] with an optimized construction. Using their method, one may obtain the results of multiple private keys attack on standard RSA and Type-A variants in Table 1. However, we find it is hard to apply their strategy directly on Type-B variants. The main idea of their method is to determine whether a polynomial is helpful or not by comparing its corresponding diagonal value in the lattice basis matrix with the modulus $(e_1 \dots e_l)^m$, then try to collect as many helpful polynomials as possible and as few unhelpful polynomials as possible during the lattice construction. They claimed the lattice basis matrix can still be triangular if $l \geq 3$, and for $l = 1, 2$ one may use the unravelled linearization technique [14] to transform it to be triangular. As a result, they obtain the same result $\beta < 0.292$ as [4] when $l = 1$. But if we apply the same method in our attack, i.e., we add some extra y-shift polynomials into each $\mathcal{G}_k$ and modify the range of j in $\mathcal{I}_+$ from $2\sum_{k=1}^{l} i_k + l$ to $2(2-\beta)\sum_{k=1}^{l} i_k$. When $l \geq 3$, the lattice can not be full-rank even use the unravelled linearization $z_i = x_i y^2 + 1$. Furthermore, we find if setting the upper bound of j as $2\lfloor(2-\beta)\rceil \sum_{k=1}^{l} i_k$, the lattice basis matrix can be triangular again, but we carried out some experiments for small l, m and the results suggest this method gets a lower bound than our original one. Thus, how to improve our attack is still an open problem.

4 Partial Key Exposure Attack

In this section, we propose the partial key exposure attack on Type-B RSA variants. Same as [31], we consider the general case where some MSBs and LSBs of the private key are leaked, so the unknown part is in the middle.

Theorem 2. *Let $N = pq$ be a modulus of Type-B RSA variants with $q < p < 2q$. Let $e = N^{\alpha}, d = N^{\beta}$ be a valid pair of public and secret exponents such that $ed \equiv 1$*

mod $(p^2+p+1)(q^2+q+1)$. *Given some MSBs* $d_M = N^{\gamma_M}$ *and some LSBs* $d_L = N^{\gamma_L}$ *of the secret exponent, and let* $\gamma = \gamma_M + \gamma_L$ *satisfying* $\gamma < \frac{15}{4}$. *Then for* $1-\gamma < \alpha < \frac{15}{4} - \gamma$, *one can factor* N *in polynomial time if*

$$\beta < \frac{3\gamma + 7 - 2\sqrt{3\gamma + 3\alpha + 1}}{3}.$$

Proof. Let $\bar{d}$ denotes the unknown middle part of private key which is bounded by $N^{\beta-\gamma}$, we have

$$d = Md_M + L\bar{d} + d_L,$$

where $M := 2^{(\beta-\gamma_M)\log_2 N}$, $L := 2^{(\beta-\gamma_L)\log_2 N}$.

Thus, we can rewrite the key equation as

$$\begin{aligned} ed &= r((p+q)^2 + a(p+q) + b) + 1 \\ \Rightarrow \quad e(L\bar{d} + \tilde{d}) &= r((p+q)^2 + a(p+q) + b) + 1, \end{aligned}$$

where $a := N+1, b := N^2 - N + 1$, and $\tilde{d} := Md_M + d_L$, which denotes the leaked value of d.

Now, consider the integer equation

$$\bar{f}(x,y,z) := 1 - e\tilde{d} - eLx + y(z^2 + az + b), \tag{8}$$

which has a small root $(x,y,z) = (\bar{d}, r, p+q)$ bounded by $X = N^{\beta-\gamma}, Y = N^{\alpha+\beta-2}, Z \approx N^{0.5}$.

To solve Eq.(8) using Coppersmith's method, we apply Jochemsz and May's strategy [17]. First, we need to define a parameter as $W := \|f(Xx, Yy, Zz)\|_\infty$, and in our case, that's

$$W = \max\{|1 - e\tilde{d}|, eLX, YZ^2, aYZ, bY\} = bY = N^{\alpha+\beta}.$$

Then, set $R := WX^{m-1}Y^{m-1}Z^{2(m-1)+\tau m}$, where m is a fixed positive integer and $0 \le \tau \le 1$ is a parameter to be optimized later. And we can transform Eq.(8) to the modular equation

$$f(x,y,z) := (1 - e\tilde{d})^{-1} f(x,y,z) \pmod{R}. \tag{9}$$

We define the set of shift polynomials as

$$\begin{aligned} &g_{i,j,k}(x,y,z) := x^i y^j z^k f(x,y,z) X^{m-1-i} Y^{m-1-j} Z^{2(m-1)-k+\tau m}, \\ &h_{i,j,k}(x,y,z) := x^i y^j z^k R, \\ &\mathcal{G} := \{g_{i,j,k} : 0 \le i \le m-1, 0 \le j \le m-1-i, 0 \le k \le 2j + \tau m\}, \\ &\mathcal{H} := \{h_{i,j,k} : 0 \le i \le m, j = m-i, 0 \le k \le 2j + \tau m\}, \\ &\mathcal{F} := \mathcal{G} \cup \mathcal{H}, \end{aligned}$$

where i, j, k are non-negative integers. Note that all polynomials in $\mathcal{F}$ share the common root $(\bar{d}, r, p+q)$ modular R.

Consider the basis matrix generated by taking the coefficients vector of $F(Xx, Yy, Zz)$ for each $F \in \mathcal{F}$. By sorting all the monomials (each corresponds to a column in the matrix) with the order mentioned in [17], we may get an upper triangular matrix.

Let $\mathcal{L}$ be the lattice corresponding to that triangular basis matrix and ω be its dimension. In our construction, the diagonal entries of this matrix are $X^{m-1}Y^{m-1}Z^{2(m-1)+\tau m}$ for polynomials in $\mathcal{G}$ and $WX^{m-1+i}Y^{m-1+j}Z^{2(m-1)+\tau m+k}$ for polynomials in $\mathcal{H}$. So, we have

$$\det(\mathcal{L}) = \prod_{\substack{(i,j,k):\\ g_{i,j,k}\in\mathcal{G}}} X^{m-1}Y^{m-1}Z^{2(m-1)+\tau m} \prod_{\substack{(i,j,k):\\ h_{i,j,k}\in\mathcal{H}}} WX^{m-1+i}Y^{m-1+j}Z^{2(m-1)+\tau m+k}.$$

Next, we can set $X = N^{\beta-\gamma}, Y = N^{\alpha+\beta-2}, Z = N^{0.5}, W = N^{\alpha+\beta}$, $M = WX^{m-1}Y^{m-1}Z^{2(m-1)+\tau m}$, and the condition in Eq.(1) can be simplified to (details of computation are given in Appendix B)

$$3\tau^2 + (6\beta - 6\gamma - 6)\tau + 4\alpha + 8\beta - 4\gamma - 12 < 0. \tag{10}$$

By setting $\tau = 1 - \beta + \gamma$, the left-hand side of Eq.(10) reaches its minimum, and we get

$$-3(1 - \beta + \gamma)^2 + 4\alpha + 8\beta - 4\gamma - 12 < 0.$$

Thus, we get the bound of β as

$$\beta < \frac{3\gamma + 7 - 2\sqrt{3\gamma + 3\alpha + 1}}{3}. \tag{11}$$

On the other hand, we require $0 \leq \tau \leq 1$, which indicates $0 \leq \beta \leq 1+\gamma$. We consider the case $\beta < \min(\frac{3\gamma+7-2\sqrt{3\gamma+3\alpha+1}}{3}, 1+\gamma) = \frac{3\gamma+7-2\sqrt{3\gamma+3\alpha+1}}{3}$, which implies $\alpha > 1 - \gamma$. Combing with the condition $0 < \gamma \leq \beta$ and $\alpha + \beta \geq 2$, we can get the range of valid α as

$$1 - \gamma < \alpha < \frac{15}{4} - \gamma. \tag{12}$$

If the conditions in Eq.(11) and Eq.(12) are satisfied, with Assumption 1, similar as the previous attack, we can extract the shared common root $(x, y, z) = (\bar{d}, r, p+q)$. And the knowledge of $p+q$ yields a factorization of N. This terminates the proof. □

We verify the validity of our partial key exposure attack with experiments, and the results can be found in Table 3 of Section 6.

Comparison with small private key attack using Coppersmith's method on Type-B variants. Set $\gamma = 0, \alpha = 2$ in our attack, the bound becomes $\beta < \frac{7-2\sqrt{7}}{3} \approx 0.569$, which is same as the bound obtained by Nitaj et al. [22]. This implies our construction can only achieve the weaker bound instead of the stronger bound $\beta < 0.585$, so it is an open problem for how to optimize

our attack to cover the stronger bound. As our attack corresponds to the general case when both some MSBs and LSBs are leaked, there may be some loss of precision. One can consider the MSBs and LSBs cases separately with some different ad-hoc optimized constructions.

Comparison with partial key exposure attack on standard RSA and Type-A variants. According to Table 1, our attack yields the same bound as that on Type-A variants. This is mainly because the $\psi(N)$ of both Type-A and Type-B variants are of the same order of magnitude as N^2 and Zheng et al. [31] as well as we use the general construction proposed by Jochemsz and May [17]. But this result is not twice as the partial key exposure attack bound on standard RSA. Just as the former analysis, Takayasu and Kunihiro [28] choose some ad-hoc and well-optimized constructions instead of general constructions, which makes it possible to fully cover Boneh and Durfee's bound.

5 Small Prime Difference Attack

In this section, we propose the small prime difference attack on Type-B RSA variants with a modulus $N = pq$ where the primes difference $|p-q|$ is sufficiently small.

Note that when $|p - q| \leq N^{\frac{1}{4}}$, the attack is trivial, since one may find $p + q$ is equal to $2N^{\frac{1}{2}}$ according to Lemma 3, which yields a factorization. So, we only consider the case $\delta > \frac{1}{4}$.

Theorem 3. *Let $N = pq$ be a modulus of Type-B RSA variants with $q < p < 2q$ and $p - q < N^{\delta}$ where $\frac{1}{4} < \delta < \frac{1}{2}$. Let $e = N^{\alpha}, d = N^{\beta}$ be a valid pair of public and secret exponents such that $ed \equiv 1 \mod (p^2 + p + 1)(q^2 + q + 1)$. Then for $4\delta - 1 < \alpha < 9\delta - \frac{36\delta-9}{4}$, one can factor N in polynomial time if*

$$\beta < 2 - \sqrt{\alpha(4\delta - 1)}.$$

Proof. Similar as the multiple private keys attack, the key equation is

$$ed = r((p + q)^2 + a(p + q) + b) + 1,$$

where $a := N + 1, b := N^2 - N + 1$. And it corresponds to the modular equation

$$\bar{f}(x, y) := x(y^2 + ay + b) + 1 \equiv 0 \pmod{e},$$

which has a root $(x, y) = (r, p + q)$.

According to Lemma 3, we have $p + q = c + \Delta$ where $c := 2N^{\frac{1}{2}}, \Delta < \frac{N^{2\delta}}{4N^{\frac{1}{2}}} \approx N^{2\delta-\frac{1}{2}}$. To make the desired root of variable y becomes Δ, we just replace y in $\bar{f}(x, y)$ with $y + c$, and obtain the new equation

$$f(x, y) := x(y^2 + Ay + B) + 1 \equiv 0 \pmod{e},$$

where $A := 2c + a, B := c^2 + ac + b$. Obviously, $f(x, y)$ has a small root (r, Δ), which are bounded by $X = N^{\alpha+\beta-2}$ and $Y = N^{2\delta-\frac{1}{2}}$.

Notice that f and $\bar{f}$ only differ at some coefficients, thus, to find the small roots of f, we may refer to the lattice construction used to find the small roots of $\bar{f}$ in [32] by Zheng et al..

Let $z := xy^2 + 1$, then we transform $f(x, y)$ into

$$f^*(x, y, z) := z + x(Ay + B) \equiv 0 \pmod{e}.$$

We define the set of shift polynomials as

$$\begin{aligned}
&g_{i,j,k}(x, y, z) := x^{i-j} f^*(x, y, z)^j e^{m-j} y^k, \\
&h_{j,k}(x, y, z) := f^*(x, y, z)^j e^{m-j} y^k, \\
&\mathcal{G} := \{g_{i,j,k} : 0 \le i \le m, 0 \le j \le i, 0 \le k \le 1\}, \\
&\mathcal{H} := \{h_{j,k} : 0 \le j \le m, 2 \le k \le \tau m\}, \\
&\mathcal{F} := \mathcal{G} \cup \mathcal{H},
\end{aligned}$$

where i, j, k are non-negative integers, m is a fixed positive integer and $0 \le \tau \le 1$ is a parameter to be optimized later.

Now, for each polynomial $F \in \mathcal{F}$, we just apply the unravelled linearization technique, by replacing terms in the form $(xy^2)^t$ to $(z - 1)^t$ for any $t \in \mathbb{N}$ to get F'. Consider the basis matrix generated by taking the coefficients vector of each $F'(Xx, Yy, Zz)$, by sorting the rows and columns using the rules described in [32], we may obtain a triangular matrix.

Let $\mathcal{L}$ be the lattice corresponding to that triangular matrix, following a similar computation in previous attacks, we get its dimension ω and its determinant:

$$\begin{aligned}
\omega &= \frac{\tau + 2}{2} m^2 + o(m^2), \\
\det(\mathcal{L}) &= X^{\frac{1}{3}m^3 + o(m^3)} Y^{\frac{\tau^2}{6}m^3 + o(m^3)} Z^{\frac{\tau+1}{3}m^3 + o(m^3)} e^{\frac{\tau+4}{6}m^3 + o(m^3)}.
\end{aligned}$$

In our construction, each polynomial F' satisfies that $F'(r, \Delta, r\Delta^2 + 1) \equiv 0 \pmod{e^m}$. Thus, substitute the above $\det(\mathcal{L})$ into Eq.1, and set $e = N^\alpha$, $X = N^{\alpha+\beta-2}$, $Y = N^{2\delta-\frac{1}{2}}$, $Z = N^{\alpha+\beta+4\delta-3}$, $M = e^m$, we will obtain the condition

$$\begin{aligned}
&N^{(\alpha+\beta-2)(\frac{1}{3}m^3 + o(m^3))} \cdot N^{(2\delta-\frac{1}{2})(\frac{\tau^2}{6}m^3 + o(m^3))}. \\
&N^{(\alpha+\beta+4\delta-3)(\frac{\tau+1}{3}m^3 + o(m^3))} \cdot N^{\alpha(\frac{\tau+4}{6}m^3 + o(m^3))} < N^{\alpha(\frac{\tau+2}{2}m^3 + o(m^3))}.
\end{aligned}$$

When m is sufficient large, we may omit all terms in $o(m^3)$, then take the exponents part of N, and we can transform the condition to

$$(4\delta - 1)\tau^2 + (4\beta + 16\delta - 12)\tau + 4\alpha + 8\beta + 16\delta - 20 < 0. \tag{13}$$

By setting $\tau = \frac{-2\beta - 8\delta + 6}{4\delta - 1}$, the left-hand side of Eq.(13) reaches its minimum, and we obtain

$$\beta^2 - 4\beta - 4\alpha\delta + \alpha + 4 > 0,$$

which gives the upper bound of β as

$$\beta < 2 - \sqrt{\alpha(4\delta - 1)}. \tag{14}$$

On the other hand, we require $0 \leq \tau \leq 1$, which implies $\frac{7}{2} - 6\delta \leq \beta \leq 3 - 4\delta$. We consider the case $\beta < \min(2 - \sqrt{\alpha(4\delta - 1)}, 3 - 4\delta) = 2 - \sqrt{\alpha(4\delta - 1)}$, which always holds if $\alpha > 4\delta - 1$. Combing with $\alpha + \beta > 2$, we can get the range of solvable α as

$$4\delta - 1 < \alpha < 9\delta - \frac{9}{4}. \tag{15}$$

If the conditions in Eq.(14) and Eq.(15) are satisfied, with Assumption 1, similar as the previous attack, we may extract the shared common root $(x, y, z) = (r, \Delta, r\Delta^2 + 1)$. Then, we get $p + q$ as $p + q = c + \Delta$, which yields a factorization of N. This terminates the proof. □

We carried out some experiments to verify the validity of our small prime difference attack, one may check Table 4 in Section 6 for details.

Comparison with small private key attack using Coppersmith's method on Type-B variants. Set $\delta = \frac{1}{2}, \alpha = 2$ in our attack, the bound becomes $\beta < 2 - \sqrt{2}$, which is same as the best bound so far obtained by Zheng et al. [32]. This is reasonable, as one can find the modular equation we construct (i.e., equation f in Therorem 3) only differs from that constructed in [32] (i.e., equation $\bar{f}$ in Therorem 3) at two coefficients and the same lattice constructions are used in these two attacks. Thus, for Type-B variants, the small prime difference attack is a tight extension of the small private key attack.

Comparison with small prime difference attack on standard RSA and Type-A variants. If we set $\alpha = 2$, one can verify that our bound is exactly twice as the bound on standard RSA obtained by de Weger [10]. This is reasonable, as the small primes difference attack is a specified version of the small private key attack. But one may find the bound on Type-A and Type-B variants are different. This is mainly due to the difference between the modular equation construction. The $\psi(N)$ of Type-A variants can be represented as a function of $p - q$ directly (i.e., $\psi(N) = (p^2 - 1)(q^2 - 1) = -(p - q)^2 + N^2 - 2N + 1$), while for Type-B we can only represent $\psi(N)$ as a function of $p + q$. Specifically, Type-B variants are weaker than Type-A variants on small prime difference attack, since the upper bound of solvable β in our attack on Type-B is always higher than the bound obtained by Cherkaoui-Semmouni et al. [8] on Type-A for any valid $\frac{1}{4} < \delta < \frac{1}{2}$ with the same valid α.

6 Experimental Results

In this section, we verify the validity of the all three attacks proposed in this paper.

Experiments are carried out using SageMath 9.4 [29] with a single process on an Ubuntu 20.04.3 LTS workstation with Intel(R) Xeon(R) Gold 5218 CPU @ 2.30GHz.

For each test, we first generate two 512-bit primes p, q and compute the 1024-bit modulus $N = pq$, then randomly choose secret exponent(s) bounded by N^β and computes the corresponding public exponent(s).

In the following tables, ω is the lattice dimension, β_{thm} means the bound computed from the theorems, β_{exp} indicates the experimental bounds, that's if we increase β_{exp} by 0.01, our attacks will fail to factor the modulus N. And Time_{LLL}, Time_{GB} are the time cost of the LLL reduction and the Gröbner basis computation respectively.

Table 2. Experiment results of multiple private keys attack

l	m	ω	β_{thm}	β_{exp}	Time_{LLL}	Time_{GB}
2	1	20	0.93	0.54	0.14s	0.01s
2	2	63	0.93	0.69	64.69s	0.09s
2	3	144	0.93	0.75	18608.71s	2.77s
3	1	56	1.10	0.76	3.41s	0.30s
3	2	270	1.10	0.82	98643.22s	38.31s
4	1	144	1.19	0.86	226.32s	6.73s
5	1	352	1.25	0.93	19154.73s	3919.37s

Table 3. Experiment results of partial key exposure attack

γ	m	ω	β_{thm}	β_{exp}	Time_{LLL}	Time_{GB}
0.05	3	50	0.60	0.43	28.16s	0.01s
0.10	3	50	0.63	0.45	27.65s	0.01s
0.20	3	60	0.69	0.49	56.14s	0.01s
0.40	3	60	0.82	0.59	60.18s	0.01s
0.40	4	115	0.82	0.63	1538.38s	0.02s
0.40	5	175	0.82	0.66	18763.19s	0.05s
0.80	3	60	1.09	0.81	48.91s	0.02s

Table 4. Experiment results of small prime difference attack

δ	m	ω	β_{thm}	β_{exp}	Time_{LLL}	Time_{GB}
0.30	3	26	1.37	1.10	1.49s	0.03s
0.30	5	57	1.37	1.12	73.04s	0.12s
0.30	7	100	1.37	1.14	1385.02s	0.39s
0.30	9	155	1.37	1.16	17616.57s	1.12s
0.34	5	57	1.15	0.99	67.36s	0.10s
0.38	5	57	0.98	0.86	65.34s	0.10s
0.42	5	57	0.83	0.73	53.96s	0.08s
0.46	5	57	0.70	0.60	120.49s	0.07s

For all three attacks, we can find that there are some differences between the theoretical bounds and our experimental results. In fact, this is reasonable, since we assume m can be sufficiently large and employ lots of approximation when computing the theoretical bound.

Due to the constrained computer resources, the lattice reduction process becomes the bottleneck of our attacks, for the time cost of the Gröbner basis computation is substantially less than that of the LLL algorithm. Even if we slightly increase m, the time cost will increase significantly, making it difficult to reach the bound β_{thm} in practice.

7 Conclusion

In this paper, we study the multiple private keys attack, the partial key exposure attack, as well as the small prime difference attack on a new type of RSA variants with the modified Euler's totient function $\psi(N) = (p^2+p+1)(q^2+q+1)$ for the first time. Our results imply this type of variants are less secure than standard RSA under these attacks. And according to the previous researches, one can find another typical type of RSA variants with $\psi(N) = (p^2-1)(q^2-1)$ are also weaker than standard RSA against these attacks. Thus, it seems that one should not pick the groups with larger Euler's totient function when designing RSA-like cryptosystems, since this will reduce the security against some key-related attacks.

Acknowledgments

We thank the anonymous reviewers for insightful comments. This work was partially supported by the National Natural Science Foundation of China (Grant Number 62072307), the National Key Research and Development Project of China (Grant Number 2020YFA0712300) as well as the Science and Technology Innovation Action Plan of Shanghai (Grant Number 22511101300).

References

1. Aono, Y.: Minkowski sum based lattice construction for multivariate simultaneous Coppersmith's technique and applications to RSA. In: Australasian Conference on Information Security and Privacy. pp. 88–103. Springer (2013)
2. Blömer, J., May, A.: Low secret exponent RSA revisited. In: International Cryptography and Lattices Conference. pp. 4–19. Springer (2001)
3. Blömer, J., May, A.: New partial key exposure attacks on RSA. In: Annual International Cryptology Conference. pp. 27–43. Springer (2003)
4. Boneh, D., Durfee, G.: Cryptanalysis of RSA with private key d less than $N^{0.292}$. IEEE transactions on Information Theory **46**(4), 1339–1349 (2000)
5. Boneh, D., Durfee, G., Frankel, Y.: An attack on RSA given a small fraction of the private key bits. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 25–34. Springer (1998)
6. Bunder, M., Nitaj, A., Susilo, W., Tonien, J.: A new attack on three variants of the RSA cryptosystem. In: Australasian Conference on Information Security and Privacy. pp. 258–268. Springer (2016)
7. Castagnos, G.: An efficient probabilistic public-key cryptosystem over quadratic fields quotients. Finite Fields and Their Applications **13**(3), 563–576 (2007)
8. Cherkaoui-Semmouni, M., Nitaj, A., Susilo, W., Tonien, J.: Cryptanalysis of RSA variants with primes sharing most significant bits. In: International Conference on Information Security. pp. 42–53. Springer (2021)
9. Coppersmith, D.: Small solutions to polynomial equations, and low exponent RSA vulnerabilities. Journal of cryptology **10**(4), 233–260 (1997)
10. De Weger, B.: Cryptanalysis of RSA with small prime difference. Applicable Algebra in Engineering, Communication and Computing **13**(1), 17–28 (2002)

11. Elkamchouchi, H., Elshenawy, K., Shaban, H.: Extended RSA cryptosystem and digital signature schemes in the domain of Gaussian integers. In: The 8th International Conference on Communication Systems, 2002. ICCS 2002. vol. 1, pp. 91–95. IEEE (2002)
12. Ernst, M., Jochemsz, E., May, A., Weger, B.d.: Partial key exposure attacks on RSA up to full size exponents. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 371–386. Springer (2005)
13. Hastad, J.: N using RSA with low exponent in a public key network. In: Conference on the Theory and Application of Cryptographic Techniques. pp. 403–408. Springer (1985)
14. Herrmann, M., May, A.: Maximizing small root bounds by linearization and applications to small secret exponent RSA. In: International Workshop on Public Key Cryptography. pp. 53–69. Springer (2010)
15. Howgrave-Graham, N.: Finding small roots of univariate modular equations revisited. In: IMA International Conference on Cryptography and Coding. pp. 131–142. Springer (1997)
16. Howgrave-Graham, N., Seifert, J.P.: Extending wiener's attack in the presence of many decrypting exponents. In: International Exhibition and Congress on Network Security. pp. 153–166. Springer (1999)
17. Jochemsz, E., May, A.: A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 267–282. Springer (2006)
18. Kuwakado, H., Koyama, K., Tsuruoka, Y.: A new RSA-type scheme based on singular cubic curves $y^2 \equiv x^3 + bx^2 \pmod{n}$. IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences **78**(1), 27–33 (1995)
19. Lenstra, A.K., Lenstra, H.W., Lovász, L.: Factoring polynomials with rational coefficients. Mathematische annalen **261**, 515–534 (1982)
20. May, A.: New RSA vulnerabilities using lattice reduction methods. Ph.D. thesis, Citeseer (2003)
21. Murru, N., Saettone, F.M.: A novel RSA-like cryptosystem based on a generalization of the Rédei rational functions. In: International Conference on Number-Theoretic Methods in Cryptology. pp. 91–103. Springer (2018)
22. Nitaj, A., Ariffin, M.R.B.K., Adenan, N.N.H., Abu, N.A.: Classical attacks on a variant of the RSA cryptosystem. In: International Conference on Cryptology and Information Security in Latin America. pp. 151–167. Springer (2021)
23. Peng, L., Hu, L., Lu, Y., Wei, H.: An improved analysis on three variants of the RSA cryptosystem. In: International Conference on Information Security and Cryptology. pp. 140–149. Springer (2016)
24. Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM **21**(2), 120–126 (1978)
25. Sarkar, S., Maitra, S.: Cryptanalysis of RSA with more than one decryption exponent. Information Processing Letters **110**(8-9), 336–340 (2010)
26. Susilo, W., Tonien, J.: A Wiener-type attack on an RSA-like cryptosystem constructed from cubic Pell equations. Theoretical Computer Science **885**, 125–130 (2021)
27. Takayasu, A., Kunihiro, N.: Cryptanalysis of RSA with multiple small secret exponents. In: Australasian Conference on Information Security and Privacy. pp. 176–191. Springer (2014)

28. Takayasu, A., Kunihiro, N.: Partial key exposure attacks on RSA: achieving the boneh-durfee bound. In: International Conference on Selected Areas in Cryptography. pp. 345–362. Springer (2014)
29. The Sage Developers: SageMath, the Sage Mathematics Software System (Version 9.4) (2021), https://www.sagemath.org
30. Wiener, M.J.: Cryptanalysis of short RSA secret exponents. IEEE Transactions on Information theory **36**(3), 553–558 (1990)
31. Zheng, M., Kunihiro, N., Hu, H.: Cryptanalysis of RSA variants with modified Euler quotient. In: International Conference on Cryptology in Africa. pp. 266–281. Springer (2018)
32. Zheng, M., Kunihiro, N., Yao, Y.: Cryptanalysis of the RSA variant based on cubic Pell equation. Theoretical Computer Science **889**, 135–144 (2021)

Appendix A: Details of the computation of Eq.(5)

According to Eq.(1), we have

$$\begin{aligned}
&\prod_{(i_1,\ldots,i_l,j)\in\mathcal{I}_+} e_1^{m-\min(i_1,\lfloor\frac{j}{2}\rfloor)}\cdots e_l^{m-\min(i_l,\lfloor\frac{j}{2}\rfloor)} X_1^{i_1}\cdots X_l^{i_l}Y^j && < (e_1\ldots e_l)^{m|\mathcal{I}_+|}\\
\Rightarrow &\prod_{(i_1,\ldots,i_l,j)\in\mathcal{I}_+} N^{-\alpha\sum_{k=1}^{l}\min(i_k,\lfloor\frac{j}{2}\rfloor)} N^{(\alpha+\beta-2)\sum_{t=1}^{l} i_t} N^{0.5j} && < 1\\
\Rightarrow &\sum_{(i_1,\ldots,i_l,j)\in\mathcal{I}_+} -\alpha\sum_{k=1}^{l}\min(i_k,\lfloor\frac{j}{2}\rfloor)+(\alpha+\beta-2)\sum_{t=1}^{l} i_t + 0.5j < 0. && (16)
\end{aligned}$$

Let $\overset{\bullet}{\sum}$ denotes the sum $\sum_{i_1=0}^{m}\cdots\sum_{i_l=0}^{m}$, $\bar{i}$ denotes the sum $\sum_{k=1}^{l} i_k$.

For any $l, m \in \mathbb{N}$ and $1 \le a \le b \le l$, the following formulas hold:

$$\overset{\bullet}{\sum} i_a i_b = \begin{cases} m^{l-1}\dfrac{m(m+1)(2m+1)}{6} & = \dfrac{m^{l+2}}{3} + o(m^{l+2}) \quad (a=b),\\ m^{l-2}\dfrac{m^2(m+1)^2}{4} & = \dfrac{m^{l+2}}{4} + o(m^{l+2}) \quad (a\neq b). \end{cases}$$

Then,

$$\overset{\bullet}{\sum}\bar{i}^2 = (\frac{l^2}{4}+\frac{l}{12})m^{l+2} + o(m^{l+2}).$$

Thus,

$$\sum_{(i_1,\ldots,i_l,j)\in\mathcal{I}_+} j = \overset{\bullet}{\sum}\sum_{j=0}^{l+2\bar{i}} j = \overset{\bullet}{\sum}(2\bar{i}^2 + o(m)) = (\frac{l^2}{2}+\frac{l}{6})m^{l+2} + o(m^{l+2}),$$

$$\sum_{(i_1,\ldots,i_l,j)\in\mathcal{I}_+} \bar{i} = \overset{\bullet}{\sum}\sum_{j=0}^{l+2\bar{i}} \bar{i} = \overset{\bullet}{\sum}(2\bar{i}^2 + o(m)) = (\frac{l^2}{2}+\frac{l}{6})m^{l+2} + o(m^{l+2}),$$

$$\begin{aligned}\sum_{(i_1,\ldots,i_l,j)\in\mathcal{I}_+}\sum_{k=1}^{l}\min(i_k,\lfloor\frac{j}{2}\rfloor) &= l\sum_{(i_1,\ldots,i_l,j)\in\mathcal{I}_+}\min(i_1,\lfloor\frac{j}{2}\rfloor) = l\overset{\bullet}{\sum}\sum_{j=0}^{l+2\bar{i}}\min(i_1,\lfloor\frac{j}{2}\rfloor)\\ &= l\overset{\bullet}{\sum}(\sum_{j=0}^{2i_1}\lfloor\frac{j}{2}\rfloor + \sum_{j=2i_1+1}^{l+2\bar{i}} i_1) = l\overset{\bullet}{\sum}(i_1(i_1+1)+i_1(l+2\sum_{t=2}^{l} i_t))\\ &= (\frac{l^2}{2}-\frac{l}{6})m^{l+2} + o(m^{l+2}).\end{aligned}$$

Now, just substitute the above results into the left-hand side of Eq.(16), we get

$$-\alpha(\frac{l^2}{2}-\frac{l}{6})m^{l+2} + (\alpha+\beta-2)(\frac{l^2}{2}+\frac{l}{6})m^{l+2} + (\frac{l^2}{4}+\frac{l}{12})m^{l+2} + o(m^{l+2}) < 0.$$

When m is sufficient large, we may omit the term $o(m^{l+2})$, which yields the new condition in Eq.(5)

Appendix B: Details of the computation of Eq.(10)

First, we can rewrite the condition in Eq.(1) as

$$X^{n_X}Y^{n_Y}Z^{n_Z} < W^{n_W}. \tag{17}$$

We can compute the value of $\omega, n_X, n_Y, n_Z, n_W$ as follows:

$$\omega = |\mathcal{G}| + |\mathcal{H}| = \sum_{\substack{(i,j,k):\\ g_{i,j,k}\in\mathcal{G}}} 1 + \sum_{\substack{(i,j,k):\\ h_{i,j,k}\in\mathcal{H}}} 1 = \frac{3\tau+2}{6}m^3 + o(m^3)$$

$$n_X = \sum_{\substack{(i,j,k):\\ g_{i,j,k}\in\mathcal{G}}} (m-1) + \sum_{\substack{(i,j,k):\\ h_{i,j,k}\in\mathcal{H}}} (m-1+i) - (m-1)\omega = \sum_{\substack{(i,j,k):\\ h_{i,j,k}\in\mathcal{H}}} i = \frac{3\tau+2}{6}m^3 + o(m^3)$$

$$n_Y = \sum_{\substack{(i,j,k):\\ g_{i,j,k}\in\mathcal{G}}} (m-1) + \sum_{\substack{(i,j,k):\\ h_{i,j,k}\in\mathcal{H}}} (m-1+j) - (m-1)\omega = \sum_{\substack{(i,j,k):\\ h_{i,j,k}\in\mathcal{H}}} j = \frac{3\tau+4}{6}m^3 + o(m^3)$$

$$\begin{aligned} n_Z &= \sum_{\substack{(i,j,k):\\ g_{i,j,k}\in\mathcal{G}}} (2(m-1)+\tau m) + \sum_{\substack{(i,j,k):\\ h_{i,j,k}\in\mathcal{H}}} (2(m-1)+\tau m+k) - (2(m-1)+\tau m)\omega \\ &= \sum_{\substack{(i,j,k):\\ h_{i,j,k}\in\mathcal{H}}} k = \frac{3\tau^2+6\tau+4}{6}m^3 + o(m^3) \end{aligned}$$

$$n_W = \omega - \sum_{\substack{(i,j,k):\\ h_{i,j,k}\in\mathcal{H}}} 1 = \frac{3\tau+2}{6}m^3 + o(m^3)$$

Substitute the above results and $X = N^{\beta-\delta}, Y = N^{\alpha+\beta-2}, Z = N^{0.5}, W = N^{\alpha+\beta}$ into Eq.(17), then take the exponents part, we can obtain

$$\begin{aligned} &(\beta-\delta)(\frac{3\tau+2}{6}m^3 + o(m^3)) + (\alpha+\beta-2)(\frac{3\tau+4}{6}m^3 + o(m^3)) \\ &\quad + 0.5(\frac{3\tau^2+6\tau+4}{6}m^3 + o(m^3)) < (\alpha+\beta)(\frac{3\tau+2}{6}m^3 + o(m^3)). \end{aligned}$$

When m is sufficient large, we may omit the term $o(m^3)$, and get the new condition in Eq.(10).