




Cryptanalysis of RSA Variants with Modified Euler Quotient

Mengce Zheng¹, Noboru Kunihiro², and Honggang Hu¹

¹ CAS Key Laboratory of Electromagnetic Space Information,
University of Science and Technology of China, Hefei, China
mczheng@mail.ustc.edu.cn, hghu2005@ustc.edu.cn

² The University of Tokyo, Tokyo, Japan
kunihiro@k.u-tokyo.ac.jp

Abstract. The standard RSA scheme provides the key equation $ed \equiv 1 \pmod{\varphi(N)}$ for $N = pq$, where $\varphi(N) = (p-1)(q-1)$ is Euler quotient (or Euler's totient function), e and d are the public and private keys, respectively. It has been extended to the following variants with *modified Euler quotient* $\omega(N) = (p^2-1)(q^2-1)$, which in turn indicates the *modified key equation* is $ed \equiv 1 \pmod{\omega(N)}$.

- An RSA-type scheme based on singular cubic curves $y^2 \equiv x^3 + bx^2 \pmod{N}$ for $N = pq$.
- An extended RSA scheme based on the field of Gaussian integers for $N = PQ$, where P, Q are Gaussian primes with $p = |P|, q = |Q|$.
- A scheme working in quadratic field quotients using Lucas sequences with an RSA modulus $N = pq$.

In this paper, we investigate some key-related attacks on such RSA variants using lattice-based techniques. To be specific, small private key attack, multiple private keys attack, and partial key exposure attack are proposed. Furthermore, we provide the first results for multiple private keys attack and partial key exposure attack when analyzing the RSA variants with modified Euler quotient.

Keywords: RSA variants · Modified Euler quotient · Lattice
Multiple private keys attack · Partial key exposure attack

1 Introduction

1.1 Background

RSA [30] is currently one of the most widely used public key cryptosystems in the world. In the case of the standard RSA, a public modulus N is the product of two large primes p and q of the same bit-size, namely $N = pq$. The key equation is $ed \equiv 1 \pmod{\varphi(N)}$, where $\varphi(N) = (p-1)(q-1)$ is Euler quotient (or Euler's totient function), (N, e) and (p, q, d) are called the public and private keys, respectively. In the encryption process, a message string is transformed into an integer M and then encrypted as $C = M^e \pmod{N}$. The decryption process

computes $C^d \pmod{N}$. Since e and d are always calculated as exponents in the encryption and decryption phases, they are called public and private exponents as well. In the following analyses, we further use α and δ for simplicity, whose values come from $e = N^\alpha$ and $d = N^\delta$.

The standard RSA cryptosystem has been generalized by various approaches such as modifying its modulus [35], modifying Euler quotient [13, 23] and modifying the encryption/decryption process [15, 28] for specific purposes. This paper focuses on the RSA variants with modified Euler quotient $\omega(N) = (p^2 - 1)(q^2 - 1)$ for $N = pq$. We provide the *modified key equation* used in such RSA variants, which shows the relation $ed \equiv 1 \pmod{\omega(N)}$ between $\omega(N)$ and two integers e and d . It can be rewritten as

$$ed = k(p^2 - 1)(q^2 - 1) + 1, \quad (1)$$

where k is an unknown positive integer. In the general cases, we have $0 < \alpha, \delta < 2$ since $0 < e, d < \omega(N) \approx N^2$. But, α and δ can be generated to exceed above range for some security considerations. Next, we briefly introduce three related schemes. One may refer to [7, 13, 23] for more details.

The First Variant. This RSA variant was introduced by Kuwakado et al. [23] in 1995. It is based on singular cubic curves with $y^2 \equiv x^3 + bx^2 \pmod{N}$ for an RSA modulus $N = pq$ and $b \in \mathbb{Z}/N\mathbb{Z}$. The public exponent e and the private exponent d satisfy $\gcd(e, (p^2 - 1)(q^2 - 1)) = 1$ and $d \equiv e^{-1} \pmod{(p^2 - 1)(q^2 - 1)}$. Thus, we have $ed = k(p^2 - 1)(q^2 - 1) + 1$ for a positive integer k from the key generation algorithm.

The Second Variant. This variant was introduced by Elkamchouchi et al. [13] in 2002. It is based on the ring of Gaussian integers $\mathbb{Z}[i]$. A Gaussian integer $a + bi$ is a complex number for integers a, b and $i^2 = -1$, whose norm is defined by $|a + bi| = \sqrt{a^2 + b^2}$. The RSA cryptosystem can be extended over the domain of Gaussian integers because of the similar property and arithmetical operations. Let modulus N be the product of two Gaussian primes P, Q and let e, d be integers satisfying $d \equiv e^{-1} \pmod{(|P|^2 - 1)(|Q|^2 - 1)}$. Note that the key equation is $ed = k(|P|^2 - 1)(|Q|^2 - 1) + 1$ for a positive integer k . When denoting $|P|$ and $|Q|$ by p and q respectively, we have the same modified key equation as derived in the first variant.

The Third Variant. This variant was introduced by Castagnos [7] in 2007. It is based on an RSA modulus $N = pq$ and Lucas sequences working in quadratic field quotients. Let e be an integer satisfying $\gcd(e, (p^2 - 1)(q^2 - 1)) = 1$. Though the inverse $d = e^{-1} \pmod{(p^2 - 1)(q^2 - 1)}$ does not explicitly appear in this scheme, we can analyze its security by solving $ed = k(p^2 - 1)(q^2 - 1) + 1$ for small d .

Small Private Key Attack. In 1990, Wiener [40] showed that one can break the standard RSA scheme when the private key d is less than $\frac{1}{3}N^{0.25}$. Wiener's

attack utilizes the continued fraction approach to deal with the key equation $ed = k(p-1)(q-1) + 1$. If d is small enough, k/d will be one of the convergents of the continued fraction expansion of the public rational fraction e/N . Thus, k and d can be recovered by computing the continued fraction expansion. Furthermore, [6] presented a new improved attack on RSA based on Wiener's technique using continued fraction.

Later in 1999, Boneh and Durfee [3] introduced the small inverse problem and proposed an improved attack using Coppersmith's lattice-based techniques [10] that works for $d < N^{0.292}$. The aim is to find the small roots of the modular equation $x(y + A) + 1 \equiv 0 \pmod{e}$ with known A and e . Herrmann and May [17] presented an optimized algorithm to solve the same equation using the linearization technique, which is applied to obtain smaller dimensional lattices. Though the latter attack does not improve the insecure bound, it simplifies the lattice construction and reduces the practical consumption.

The small private key attacks on several RSA variants have also been studied in [31–33]. As for the RSA variants with modified Euler quotient $\omega(N) = (p^2 - 1)(q^2 - 1)$, Bunder et al. [5] proposed an attack using the continued fraction approach. They showed that when $d^2e < 2N^3 - 18N^2$, k/d can be found among the convergents of the continued fraction expansion of $e/(N^2 - \frac{9}{4}N + 1)$. Thus, the factorization of N , namely p and q can be deduced from k and d . Peng et al. [27] proposed a better lattice-based attack and improved the insecure bound to $\delta < 2 - \sqrt{\alpha}$ for $\alpha \geq 1$. The attack is reduced to solving small roots $(k, p^2 + q^2)$ of the modular equation $x(N^2 + 1 - y) + 1 \equiv 0 \pmod{e}$ using the linearization technique of [17]. Though Peng et al. gave a refinement on the insecure bound of the small private exponent, they did not present a complete range of solvable α .

Multiple Private Keys Attack. The security of RSA with multiple key pairs was first studied by Howgrave-Graham and Seifert [19] in 1999. In this case, where given n multiple key pairs $(e_1, d_1), \dots, (e_n, d_n)$ for a common public modulus N such that $e_i d_i \equiv 1 \pmod{\varphi(N)}$ for all $i = 1, 2, \dots, n$, the standard RSA can be viewed as the special case for $n = 1$. Similarly, the values of the public and private keys are estimated as N^α and N^δ , respectively.

Later, this attack type was improved by the lattice-based techniques in [1, 36]. The previous works confirm an intuitive inference that RSA becomes more vulnerable when there are more key pairs. Takayasu and Kunihiro [36] proposed the best attack so far that works for $\delta < 1 - \sqrt{2/(3n+1)}$ when given N and public keys $e_1, \dots, e_n \approx N$. If there are even more key pairs, larger secret keys can be recovered, which indicates that full-size private keys i.e. $\delta = 1$ can be recovered with infinitely many key pairs.

The multiple private keys attack has been extended to other RSA variants in several papers like [26, 41]. However, to attack the RSA variant with modified Euler quotient with multiple key pairs is not analyzed before.

Partial Key Exposure Attack. In 1998, Boneh et al. [4] proposed several attacks on RSA given a fraction of the private key bits with small public exponent

e . Their attacks utilized some known most significant bits (MSBs) or some known least significant bits (LSBs) of the private exponent d . In practice, above partial key information can be captured using side channel attacks, e.g. cold boot attacks [16] and others [22, 29]. Therefore, so-called partial key exposure attack has gradually become an important part when estimating the security of RSA.

Blömer and May [2] later improved partial key exposure attacks on RSA using Coppersmith's lattice-based techniques [10]. They showed that RSA is also vulnerable to larger public exponent e given some private key exposure. In 2005, Ernst et al. [14] presented several new attacks that work up to full-size exponents (i.e., $e \approx N$ or $d \approx N$) by three theorems under a common heuristic assumption. The best-known attack was proposed by Takayasu and Kunihiro [37, 39], which can achieve Boneh and Durfee's bound [3] of the small private key attack.

In addition to the partial key exposure attacks on the standard RSA scheme, this attack type has been extended to other RSA variants in several papers like [34]. However, the partial key exposure attack on the RSA variant with modified Euler quotient is not considered before.

1.2 Our Contributions

In this paper, we first derive the crucial modular equation in our analyses from the modified key Eq. 1. We have $ed = k(p^2q^2 - p^2 - q^2 + 1) + 1$, which can be rewritten as $ed = k((N + 1)^2 - (p + q)^2) + 1$. Thus, we are required to solve

$$x(y + A) + 1 \equiv 0 \pmod{e} \quad (2)$$

for $A := (N + 1)^2$ with small roots $x = k$ and $y = -(p + q)^2$. Note that our modular equation is slightly different compared with the root $y = p^2 + q^2$ used in [27].

Then we apply the lattice-based techniques [10] to solve the crucial modular Eq. 2 for some interesting cases. To be specific, we propose three key-related attacks on the RSA variants with modified Euler quotient. We reproduce the small private key attack as the result of [27] using the linearization technique [17] for an accurate range of solvable α .

Proposition 1. *Let $N = pq$ be an RSA modulus with two prime factors p, q of the same bit-size. Let $e = N^\alpha$ be a valid public key and $d = N^\delta$ be its corresponding private key such that $ed \equiv 1 \pmod{(p^2 - 1)(q^2 - 1)}$. Then modulus N of the RSA variants with modified Euler quotient can be efficiently factored if*

$$\delta < 2 - \sqrt{\alpha} \quad \text{for } 1 \leq \alpha < 4.$$

We further provide the result of multiple private keys attack on the RSA variants with modified Euler quotient for the first time.

Proposition 2. *Let $N = pq$ be an RSA modulus with two prime factors p, q of the same bit-size. Let $e_i = N^\alpha$ be a valid public key and $d_i = N^\delta$ be its*

corresponding private key such that $e_i d_i \equiv 1 \pmod{(p^2 - 1)(q^2 - 1)}$ for $1 \leq i \leq n$. Then modulus N of the RSA variants with modified Euler quotient can be efficiently factored if

$$\delta < 2 - \sqrt{\frac{4\alpha}{3n + 1}} \quad \text{for} \quad \frac{4}{3n + 1} < \alpha < 3n + 1.$$

When we have one single key pair, namely $n = 1$, the condition becomes $\delta < 2 - \sqrt{\alpha}$, which is identical to that in Proposition 1.

We also show the result of partial key exposure attack on the RSA variants with modified Euler quotient for the first time.

Proposition 3. *Let $N = pq$ be an RSA modulus with two prime factors p, q of the same bit-size. Let $e = N^\alpha$ be a valid public key and $d = N^\delta$ be its corresponding private key such that $ed \equiv 1 \pmod{(p^2 - 1)(q^2 - 1)}$. Given an approximation \tilde{d} with known MSBs $d_M = N^{\gamma_M}$, LSBs $d_L = N^{\gamma_L}$ and unknown $\hat{d} = N^{\delta - \gamma}$ (for $\gamma = \gamma_M + \gamma_L$) such that $d = \tilde{d} + \hat{d}L = d_M M + \hat{d}L + d_L$ for $M := 2^{(\delta - \gamma_M) \log_2 N}$ and $L := 2^{\gamma_L \log_2 N}$. Then modulus N of the RSA variants with modified Euler quotient can be efficiently factored if*

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

We summarize our upper bounds with comparative cryptanalytic results on the standard RSA in Table 1. For simplicity, we set full-size public keys, namely $e \approx N$ in standard RSA and $e \approx N^2$ in RSA variants with $\omega(N)$ to show the respective conditions on δ . More precisely, n indicates the number of given key pairs in multiple private keys attack and γ (or N^γ) indicates the known key exposure in partial key exposure attack.

Table 1. Summary of three key-related attacks on RSA and its variant

	Standard RSA [30]	RSA variants [7, 13, 23]
Small private key attack	$\delta < 0.292$ [3]	$\delta < 0.585$
Multiple private keys attack	$\delta < 1 - \sqrt{\frac{2}{3n+1}}$ [36]	$\delta < 2 - \sqrt{\frac{8}{3n+1}}$
Partial key exposure attack	$\delta < \frac{\gamma+2-\sqrt{2-3\gamma^2}}{2}$ [37]	$\delta < \frac{3\gamma+7-2\sqrt{3\gamma+7}}{3}$

1.3 Organization

The rest of this paper is organized as follows. In Sect. 2, we review some facts and mathematical lemmas of lattice-based attacks. In Sect. 3, we present our small private key attack in details. In Sect. 4, we propose the multiple private keys attack on such RSA variants by applying Minkowski sum technique. In Sect. 5, we propose the partial key exposure attack for such RSA variants. We conclude the paper in Sect. 6.

2 Preliminaries

In this section, we introduce some notions of the lattice-based attacks, which include the LLL algorithm [24], Howgrave-Graham's lemma [18], Coppersmith's techniques [8,9]. One may refer to [10,25] for more details.

A lattice \mathcal{L} spanned by linearly independent vectors $\mathbf{b}_1, \dots, \mathbf{b}_w$ in \mathbb{R}^n is the set of their integer linear combinations, which is denoted by $\mathcal{L}(\mathbf{b}_1, \dots, \mathbf{b}_w) = \{\sum_{i=1}^w z_i \mathbf{b}_i : z_i \in \mathbb{Z}\}$. We call $(\mathbf{b}_1, \dots, \mathbf{b}_w)$ a basis of \mathcal{L} and w is the lattice dimension. If $w = n$, then \mathcal{L} is called full-rank. In another way, \mathbf{b}_i 's can be regarded as row vectors to generate a basis matrix B . The lattice determinant is defined as $\det(\mathcal{L}) := \sqrt{\det(BB^T)}$, where B^T is a transpose of B . We have $\det(\mathcal{L}) = |\det(B)|$ for a full-rank lattice from the definition, which implies that B is a square matrix. Moreover, the determinant of a triangular basis matrix can be easily computed as the product of its diagonal entries.

In 1982, Lenstra et al. [24] proposed the so-called LLL algorithm that is practically used for finding approximately shortest lattice vectors, which plays an important role in the field of lattice-based cryptanalyses.

Lemma 1. *Let \mathcal{L} be a lattice with determinant $\det(\mathcal{L})$ and vectors in \mathbb{R}^n . The LLL algorithm outputs a reduced basis $(\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_w)$ in polynomial time in n, w and input length. For $1 \leq i \leq w$, the reduced vectors \mathbf{v}_i 's satisfy*

$$\|\mathbf{v}_i\| \leq 2^{\frac{w(w-1)}{4(w+1-i)}} \det(\mathcal{L})^{\frac{1}{w+1-i}}.$$

Howgrave-Graham [18] later showed how to judge whether the roots of a modular equation are also roots over the integers. This reformulation is more concise and straightforward compared with Coppersmith's original methods. For a given n -variate polynomial $g(x_1, \dots, x_n) = \sum a_{i_1, \dots, i_n} x_1^{i_1} \cdots x_n^{i_n}$, its norm is defined as $\|g(x_1, \dots, x_n)\| := \sqrt{\sum |a_{i_1, \dots, i_n}|^2}$. We provide the following lemma and then discuss the combination of Lemmas 1 and 2.

Lemma 2. *Let $g(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$ be an integer polynomial that is a sum of at most w monomials. Suppose that*

1. $g(x'_1, \dots, x'_n) = 0 \pmod{R}$, where $|x'_1| < X_1, \dots, |x'_n| < X_n$, and
2. $\|g(x_1 X_1, \dots, x_n X_n)\| < R/\sqrt{w}$.

Then $g(x'_1, \dots, x'_n) = 0$ holds over the integers.

The main idea of the lattice-based attacks is to construct a set of shift polynomials modulo an integer R with the common roots and then reduce them to several equations over the integers by the LLL algorithm. The basis matrix consists of the shift polynomials' coefficient vectors, which come from a given modular equation. It spans a lattice of dimension w and we use the LLL algorithm to obtain short lattice vectors that correspond to the polynomial forms. If the norms of the polynomials are sufficiently small, these equations still hold over the integers. Eventually, we can efficiently extract the common roots by Gröbner

bases computation or resultant computation. Notice that the linearization technique makes it easier to construct a triangular matrix and hence simplifies the whole analysis.

The above fundamental lemmas indicate the final condition, which can be roughly summarized as

$$\det(\mathcal{L}) < R^w. \tag{3}$$

We here do not discuss more how to solve integer polynomial equations since it makes use of the essential idea of solving modular equations by adding an auxiliary parameter. See Coron’s reformulations [11, 12] for the detail. We should note that solving multivariate equations is heuristic because the newly derived polynomials are not guaranteed to be algebraically independent. In this paper, we assume that the polynomials derived from the reduced vectors of the LLL algorithm are algebraically independent as discussed in the literature of lattice-based attacks on RSA and its variants [3, 21]. In fact, there are barely works that contradict this assumption.

3 Small Private Key Attack

In this section, we aim to solve the crucial modular Eq. 2 for sufficient small private key d . Applying the linearization technique, we can reproduce the insecure bound on d for the RSA variants with modified Euler quotient.

In order to find all small roots (x, y) of the bivariate modular equation $xy + Ax + 1 \equiv 0 \pmod{e}$. We first transform the original polynomial $xy + Ax + 1$ into $Ax + z$ by letting $z := xy + 1$. The shift polynomials $g_{[i,j,k]}(x, y, z)$ are defined in the following form for $f(x, y, z) := Ax + z$,

$$g_{[i,j,k]}(x, y, z) := x^i y^j f^k(x, y, z) e^{s-k} = x^i y^j (Ax + z)^k e^{s-k},$$

where s is a fixed positive integer and $i, j, k \in \mathbb{N}$. We denote the set of shift polynomials by $\mathcal{G} \cup \mathcal{H}$ for

$$\begin{aligned} \mathcal{G} &:= \{g_{[i,j,k]}(x, y, z) : (i, j, k) \in \mathcal{I}_{\mathcal{G}}\}, \\ \mathcal{H} &:= \{g_{[i,j,k]}(x, y, z) : (i, j, k) \in \mathcal{I}_{\mathcal{H}}\}, \end{aligned}$$

where two index sets $\mathcal{I}_{\mathcal{G}}$ and $\mathcal{I}_{\mathcal{H}}$ are defined by

$$\begin{aligned} \mathcal{I}_{\mathcal{G}} &:= \{(i, j, k) : j = 0; i = 0, \dots, s; k = 0, \dots, s - i\}, \\ \mathcal{I}_{\mathcal{H}} &:= \{(i, j, k) : i = 0; k = 0, \dots, s; j = 1, \dots, \tau k\}, \end{aligned}$$

for a parameter $0 \leq \tau \leq 1$ to be optimized later. It is clear that all the shift polynomials share the small roots modulo e^s . The polynomial and monomial orders \prec are defined as $g_{[i,j,k]} \prec g_{[i',j',k']}$ and $x^i y^j z^k \prec x^{i'} y^{j'} z^{k'}$, respectively if (1) $i + k < i' + k'$; or (2) $i + k = i' + k'$ and $k < k'$; or (3) $i = i'$, $k = k'$ and $j < j'$.

We can substitute each occurrence of xy by the term $z - 1$. The lattice basis matrix is generated by taking the coefficient vectors of $g_{[i,j,k]}(xX, yY, zZ)$ as

row vectors, where X, Y and Z denote the upper bounds on the roots (x, y, z) . Additionally, the rows and columns are arranged according to above orders \prec , which guarantees that the lattice basis matrix is triangular. Table 2 shows a toy example for two parameters $s = 2$ and $\tau = 1$, where symbols “-” indicate the non-zero off-diagonal entries, and f denotes $AxX + zZ$.

Table 2. A toy example of the lattice basis matrix for $s = 2$ and $\tau = 1$

	1	x	z	yz	x^2	xz	z^2	yz^2	y^2z^2
$g_{[0,0,0]}$ e^2	e^2								
$g_{[1,0,0]}$ xXe^2	e^2X								
$g_{[0,0,1]}$ fe	-	eZ							
$g_{[0,1,1]}$ yYf	-		YZ						
$g_{[2,0,0]}$ $(xX)^2e^2$					e^2X^2				
$g_{[1,0,1]}$ $xXfe$					-	eXZ			
$g_{[0,0,2]}$ f^2					-	-	Z^2		
$g_{[0,1,2]}$ yYf^2		-	-			-	-	YZ^2	
$g_{[0,2,2]}$ $(yY)^2f^2$	-		-	-			-	-	Y^2Z^2

Since we have $e = N^\alpha$ and $d = N^\delta$, we can figure out $X = N^{\alpha+\delta-2}, Y = N$ and $Z = N^{\alpha+\delta-1}$. We are able to compute the determinant $\det(\mathcal{L})$ by counting the numbers of X, Y, Z and e appearing in the diagonal entries respectively, which signify the contributions of the shift polynomials to $\det(\mathcal{L})$. We omit the rounding of τk since it is negligible in our asymptotic analysis for sufficiently large s .

We compute the dimension w of the full-rank lattice and the contributions of the shift polynomials denoted by n_X, n_Y, n_Z and n_e , respectively.

$$\begin{aligned}
 w &= \sum_{(i,j,k) \in \mathcal{I}_G \cup \mathcal{I}_H} 1 = \sum_{i=0}^s \sum_{k=0}^{s-i} 1 + \sum_{k=0}^s \sum_{j=1}^{\tau k} 1 = \frac{1+\tau}{2}s^2 + o(s^2), \\
 n_X &= \sum_{(i,j,k) \in \mathcal{I}_G \cup \mathcal{I}_H} i = \sum_{i=0}^s \sum_{k=0}^{s-i} i = \frac{1}{6}s^3 + o(s^3), \\
 n_Y &= \sum_{(i,j,k) \in \mathcal{I}_G \cup \mathcal{I}_H} j = \sum_{k=0}^s \sum_{j=1}^{\tau k} j = \frac{\tau^2}{6}s^3 + o(s^3), \\
 n_Z &= \sum_{(i,j,k) \in \mathcal{I}_G \cup \mathcal{I}_H} k = \sum_{i=0}^s \sum_{k=0}^{s-i} k + \sum_{k=0}^s \sum_{j=1}^{\tau k} k = \frac{1+2\tau}{6}s^3 + o(s^3), \\
 n_e &= \sum_{(i,j,k) \in \mathcal{I}_G \cup \mathcal{I}_H} (s-k) = \sum_{i=0}^s \sum_{k=0}^{s-i} (s-k) + \sum_{k=0}^s \sum_{j=1}^{\tau k} (s-k) = \frac{2+\tau}{6}s^3 + o(s^3).
 \end{aligned}$$

From above rough condition 3 $\det(\mathcal{L}) < R^w$ for $\det(\mathcal{L}) = X^{n_x} Y^{n_y} Z^{n_z} e^{n_e}$ and $R = e^s$, we have

$$(\alpha + \delta - 2) + \tau^2 + (1 + 2\tau)(\alpha + \delta - 1) + (2 + \tau)\alpha < 3(1 + \tau)\alpha,$$

when dealing with the exponents and omitting other lower order terms of s . It can be simplified to

$$\tau^2 + (2\delta - 2)\tau + \alpha + 2\delta - 3 < 0.$$

The value of the left side reaches its minimum by setting $\tau = 1 - \delta$ and then the inequality becomes

$$\delta^2 - 4\delta - \alpha + 4 > 0.$$

Therefore, we obtain the final condition

$$\delta < 2 - \sqrt{\alpha}.$$

Note that $0 \leq \tau = 1 - \delta \leq 1$ and hence we have $0 \leq \delta \leq 1$. Combining it with $\alpha + \delta \geq 2$ and $\delta < 2 - \sqrt{\alpha}$, we have $1 \leq \alpha < 4$ that is our complete solvable range of α . Thus, we attain the bound of Proposition 1 as required.

4 Multiple Private Keys Attack

In this section, we propose the multiple private keys attack on the RSA variants with modified Euler quotient. To specify the analytic situation for given n key pairs, we define the following general multiple private keys attack scenario.

Let N be the product of two primes p, q of the same bit-size. Let $e_i = N^\alpha$ and $d_i = N^\delta$ for $1 \leq i \leq n$ such that $e_i d_i \equiv 1 \pmod{\omega(N)}$, where $\omega(N) = (p^2 - 1)(q^2 - 1)$. Given N and n key pairs (e_i, d_i) (for $1 \leq i \leq n$), the goal is to efficiently factor N .

In this case, we need to solve the simultaneous modular equations

$$\begin{cases} f_1(x_1, y) := x_1(y + A) + 1 \equiv 0 \pmod{e_1} \\ f_2(x_2, y) := x_2(y + A) + 1 \equiv 0 \pmod{e_2} \\ \vdots \\ f_n(x_n, y) := x_n(y + A) + 1 \equiv 0 \pmod{e_n} \end{cases} \tag{4}$$

for $A := (N + 1)^2$ and the roots $(x_1, x_2, \dots, x_n, y) = (k_1, k_2, \dots, k_n, -(p + q)^2)$ whose values are bounded by $X_1 = \dots = X_n = N^{\alpha+\delta-2}$ and $Y = N$.

To deal with above simultaneous modular Eq.4, Aono [1] proposed Minkowski sum based lattice constructions. We also apply this tool to provide the generation of the shift polynomials. The underlying shift polynomials are defined by

$$g_{i_k, j_k}^{(k)}(x_k, y) := x_k^{i_k - j_k} f_k^{j_k}(x_k, y) e_k^{s - j_k}$$

with $0 \leq j_k \leq i_k \leq s$ and $i_k, j_k \in \mathbb{N}$ for $1 \leq k \leq n$. It is clear that we have $g_{i_k, j_k}^{(k)}(x_k, y) \equiv 0 \pmod{e_k^s}$ for each k . We define the same Minkowski sum based shift polynomials as [1] by

$$g_{i_1, \dots, i_n, j}(x_1, \dots, x_n, y) := \sum_{j_1 + \dots + j_n = j} a_{j_1, \dots, j_n} g_{i_1, j_1}^{(1)} g_{i_2, j_2}^{(2)} \dots g_{i_n, j_n}^{(n)}$$

for a particular a_{j_1, \dots, j_n} such that the corresponding diagonal entry in the basis matrix is

$$X_1^{i_1} \dots X_n^{i_n} Y^j e_1^{s - \min\{i_1, j\}} \dots e_n^{s - \min\{i_n, j\}}.$$

Thus, all the shift polynomials share the common roots $(x_1, x_2, \dots, x_n, y) = (k_1, \dots, k_n, -(p + q)^2)$ modulo $(e_1 \dots e_n)^s$. We consider the shift polynomials with $\max\{i_1, \dots, i_n\} \leq j$. Applying a useful criterion from [36], we compare the sizes of the diagonal entries with the size of the modulus to choose as many helpful polynomials as possible. It requires that

$$X_1^{i_1} \dots X_n^{i_n} Y^j e_1^{s - i_1} \dots e_n^{s - i_n} \leq (e_1 \dots e_n)^s,$$

which leads to

$$(\alpha + \delta - 2) \sum_{k=1}^n i_k + j + \alpha ns - \alpha \sum_{k=1}^n i_k \leq \alpha ns.$$

That is $j \leq (2 - \delta) \sum_{k=1}^n i_k$. Therefore, we select the shift polynomials over the index set

$$\mathcal{I} := \{(i_1, \dots, i_n, j) : 0 \leq i_1, i_2, \dots, i_n \leq s; 0 \leq j \leq (2 - \delta) \sum_{k=1}^n i_k\}.$$

The lattice basis matrix is triangular as discussed in [1, 36]. We follow a similar analysis in Sect. 3 (ignoring lower order terms of s) to compute the lattice dimension

$$w = \sum_{(i_1, \dots, i_n, j) \in \mathcal{I}} 1 = \frac{n(2 - \delta)}{2} s^{n+1},$$

and respective contributions of the diagonal entries to the determinant that are denoted by n_{X_k}, n_Y and n_{e_k} for $1 \leq k \leq n$,

$$n_{X_1} = \dots = n_{X_n} = \sum_{(i_1, \dots, i_n, j) \in \mathcal{I}} i_k = \frac{(3n + 1)(2 - \delta)}{12} s^{n+2},$$

$$n_Y = \sum_{(i_1, \dots, i_n, j) \in \mathcal{I}} j = \frac{n(3n + 1)(2 - \delta)^2}{24} s^{n+2},$$

$$n_{e_1} = \dots = n_{e_n} = \sum_{(i_1, \dots, i_n, j) \in \mathcal{I}} (s - \min\{i_n, j\}) = \frac{2 + (3n - 1)(2 - \delta)}{12} s^{n+2}.$$

We can find solutions of the simultaneous modular Eq. 4 if the condition 3 holds, that is

$$X_1^{n_{x_1}} \dots X_n^{n_{x_n}} Y^{n_y} e_1^{n_{e_1}} \dots e_n^{n_{e_n}} < (e_1 \dots e_n)^{sw},$$

which leads to

$$2n(3n + 1)(2 - \delta)(\alpha + \delta - 2) + n(3n + 1)(2 - \delta)^2 + n(4 - (6n + 2)(2 - \delta))\alpha < 0.$$

It can be reduced to

$$-(3n + 1)(2 - \delta)^2 + 4\alpha < 0.$$

Finally, we derive the condition for the multiple private keys attack scenario

$$\delta < 2 - \sqrt{\frac{4\alpha}{3n + 1}}.$$

The range of solvable α is determined by $2 - \sqrt{\frac{4\alpha}{3n+1}} > 0$ and $\alpha + 2 - \sqrt{\frac{4\alpha}{3n+1}} > 2$, which imply

$$\frac{4}{3n + 1} < \alpha < 3n + 1$$

as claimed in Proposition 2.

5 Partial Key Exposure Attack

In this section, we propose the partial key exposure attack on the RSA variants with modified Euler quotient. To specify the analytic situation for given leakage of the private key, we define the following general partial key exposure attack scenario.

Let N be the product of two primes p, q of the same bit-size. Let $e = N^\alpha$ and $d = N^\delta$ such that $ed \equiv 1 \pmod{\omega(N)}$, where $\omega(N) = (p^2 - 1)(q^2 - 1)$. Given N, e and \tilde{d} (i.e. MSBs d_M and LSBs d_L) that is a known approximation of d satisfying

$$d = \tilde{d} + \hat{d}L = d_M M + \hat{d}L + d_L$$

for $M := 2^{(\delta - \gamma_M) \log_2 N}$ and $L := 2^{\gamma_L \log_2 N}$, which implies that $|\hat{d}| < N^{\delta - \gamma}$ for $\gamma := \gamma_M + \gamma_L$, the target is to efficiently factor N .

Recall that the modified key Eq. 1 is $ed = k(p^2 - 1)(q^2 - 1) + 1$. Since $d = \tilde{d} + \hat{d}L$, we substitute it with its approximation and obtain

$$e(\tilde{d} + \hat{d}L) = k(p^2 - 1)(q^2 - 1) + 1.$$

We now focus on the integer equation

$$f(x, y, z) := 1 - e\tilde{d} + eLx + y((N + 1)^2 + z) \tag{5}$$

with small roots $x = -\hat{d}$, $y = k$ and $z = -(p + q)^2$, whose values are bounded by $X = N^{\delta - \gamma}$, $Y = N^{\alpha + \delta - 2}$ and $Z = N$, respectively. If we discover the small roots of $f(x, y, z)$, we can factor the RSA modulus N .

We turn to solving the integer polynomial 5 by applying Jochemsz and May’s strategy [20]. A similar construction is also described in [39]. We first give the definition of the auxiliary parameter $W := \|f(xX, yY, zZ)\|_\infty$, namely l_∞ -norm of a certain polynomial. For our integer polynomial 5, we have

$$W = \max\{|1 - e\tilde{d}|, |eLX|, |Y(N + 1)^2|, |YZ|\} = N^{\alpha+\delta}.$$

We set a suitable integer $R := WX^{s-1}Y^{s-1}Z^{s-1+\tau s}$ (as a modulus) for a fixed positive integer s and $\tau \geq 0$ to be optimized later. We then perform a transformation on the original polynomial 4 by

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

The shift polynomials $g_{[i,j,k]}^{\mathcal{G}}(x, y, z)$ and $g_{[i,j,k]}^{\mathcal{H}}(x, y, z)$ are defined in the following forms,

$$\begin{aligned} g_{[i,j,k]}^{\mathcal{G}}(x, y, z) &:= x^i y^j z^k f'(x, y, z) X^{s-1-i} Y^{s-1-j} Z^{s-1+\tau s-k}, \\ g_{[i,j,k]}^{\mathcal{H}}(x, y, z) &:= x^i y^j z^k R, \end{aligned}$$

for $i, j, k \in \mathbb{N}$. We denote the set of shift polynomials by $\mathcal{G} \cup \mathcal{H}$, where

$$\begin{aligned} \mathcal{G} &:= \{g_{[i,j,k]}^{\mathcal{G}}(x, y, z) : (i, j, k) \in \mathcal{I}_{\mathcal{G}}\}, \\ \mathcal{H} &:= \{g_{[i,j,k]}^{\mathcal{H}}(x, y, z) : (i, j, k) \in \mathcal{I}_{\mathcal{H}} \setminus \mathcal{I}_{\mathcal{G}}\}, \end{aligned}$$

for two index sets $\mathcal{I}_{\mathcal{G}}$ and $\mathcal{I}_{\mathcal{H}}$ defined by

$$\begin{aligned} \mathcal{I}_{\mathcal{G}} &:= \{(i, j, k) : i = 0, \dots, s - 1; j = 0, \dots, s - 1 - i; k = 0, \dots, j + \tau s\}, \\ \mathcal{I}_{\mathcal{H}} &:= \{(i, j, k) : i = 0, \dots, s; j = 0, \dots, s - i; k = 0, \dots, j + \tau s\}. \end{aligned}$$

It is noticeable that all the shift polynomials share the common roots $(x, y, z) = (-\hat{d}, k, -(p + q)^2)$ modulo R . The polynomial and monomial orders are quite straightforward as mentioned in [20]. Therefore, we can construct a triangular basis matrix with diagonal entries $X^{s-1}Y^{s-1}Z^{s-1+\tau s}$ for \mathcal{G} and $X^i Y^j Z^k R = WX^{s-1+i}Y^{s-1+j}Z^{s-1+\tau s+k}$ for \mathcal{H} . We then follow a similar analysis in Sect. 3 (ignoring lower order terms of s) to compute the lattice dimension

$$w = \sum_{(i,j,k) \in \mathcal{I}_{\mathcal{G}}} 1 + \sum_{(i,j,k) \in \mathcal{I}_{\mathcal{H}} \setminus \mathcal{I}_{\mathcal{G}}} 1 = \frac{1 + 3\tau}{6} s^3.$$

Recall that the rough condition 3 $\det(\mathcal{L}) < R^w$ indicates

$$\begin{aligned} &\prod_{(i,j,k) \in \mathcal{I}_{\mathcal{G}}} X^{s-1} Y^{s-1} Z^{s-1+\tau s} \prod_{(i,j,k) \in \mathcal{I}_{\mathcal{H}} \setminus \mathcal{I}_{\mathcal{G}}} W X^{s-1+i} Y^{s-1+j} Z^{s-1+\tau s+k} \\ &< (W X^{s-1} Y^{s-1} Z^{s-1+\tau s})^w. \end{aligned}$$

Thus, we can find solutions of the integer Eq. 5 when $X^{n_X} Y^{n_Y} Z^{n_Z} < W^{n_W}$ (ignoring lower order terms of s) for

$$\begin{aligned}
 n_X &= \sum_{(i,j,k) \in \mathcal{I}_G} (s-1) + \sum_{(i,j,k) \in \mathcal{I}_H \setminus \mathcal{I}_G} (s-1+i) - (s-1)w = \frac{1+3\tau}{6} s^3, \\
 n_Y &= \sum_{(i,j,k) \in \mathcal{I}_G} (s-1) + \sum_{(i,j,k) \in \mathcal{I}_H \setminus \mathcal{I}_G} (s-1+j) - (s-1)w = \frac{2+3\tau}{6} s^3, \\
 n_Z &= \sum_{(i,j,k) \in \mathcal{I}_G} (s-1+\tau s) + \sum_{(i,j,k) \in \mathcal{I}_H \setminus \mathcal{I}_G} (s-1+\tau s+k) - (s-1+\tau s)w \\
 &= \frac{1+3\tau+3\tau^2}{6} s^3, \\
 n_W &= w - \sum_{(i,j,k) \in \mathcal{I}_H \setminus \mathcal{I}_G} 1 = \sum_{(i,j,k) \in \mathcal{I}_G} 1 = \frac{1+3\tau}{6} s^3.
 \end{aligned}$$

Substituting them for the inequality, we obtain

$$(1+3\tau)(\delta-\gamma) + (2+3\tau)(\alpha+\delta-2) + (1+3\tau+3\tau^2) < (1+3\tau)(\alpha+\delta),$$

which leads to

$$3\tau^2 + (3\delta - 3\gamma - 3)\tau + \alpha + 2\delta - \gamma - 3 < 0.$$

The value of the left side reaches its minimum by setting $\tau = (1 + \gamma - \delta)/2$ and we have

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

as claimed in Proposition 3.

It is also possible to apply known bounds given in [20, Appendix B] to solve an integer polynomial of special forms including our integer polynomial 5. We provide a useful lemma as follows.

Lemma 3. *Let $f(x_1, x_2, x_3) = a_0 + a_1x_1 + x_2(a_2 + x_3) \in \mathbb{Z}[x_1, x_2, x_3]$ be an integer polynomial. Suppose that x_1, x_2, x_3 are bounded by X_1, X_2, X_3 respectively, and $W = \max\{|a_0|, |a_1|X_1, |a_2|X_2, X_2X_3\}$. Then the roots can be found for an optimized $\tau \geq 0$ if*

$$X_1^{1+3\tau} X_2^{2+3\tau} X_3^{1+3\tau+3\tau^2} < W^{1+3\tau}.$$

We directly apply Lemma 3 with $X_1 = N^{\delta-\gamma}$, $X_2 = N^{\alpha+\delta-2}$, $X_3 = N$ and $W = N^{\alpha+\delta}$ for our attack and have

$$(1+3\tau)(\delta-\gamma) + (2+3\tau)(\alpha+\delta-2) + (1+3\tau+3\tau^2) < (1+3\tau)(\alpha+\delta),$$

that is equivalent to

$$3\tau^2 + (3\delta - 3\gamma - 3)\tau + \alpha + 2\delta - \gamma - 3 < 0,$$

which gives the same result as stated in Proposition 3.

6 Concluding Remarks

We study some key-related attacks on the RSA variants with modified Euler quotient $\omega(N) = (p^2 - 1)(q^2 - 1)$ in this paper. Some interesting cases such as given more key pairs and given some key exposure are analyzed like previous works in the literature. We propose the multiple private keys attack that extends the small private key attack for n key pairs. Since the case of $n = 1$ corresponds to the small private key attack, it is a meaningful extension of the latter.

For the partial key exposure attack, a preliminary result is provided assuming we already know some most and least significant bits of the private key. However, there exist several methods to improve the results for given only the most significant bits or the least significant bits like [39]. A combined scenario i.e. partial key exposure attack with multiple key pairs has also been analyzed in [38]. To generalize partial key exposure attacks with only MSBs, LSBs or multiple key pairs on the RSA variants with modified Euler quotient remains as future work.

Acknowledgments. The authors would like to thank the anonymous reviewers for their valuable comments and suggestions. This work was partially supported by National Natural Science Foundation of China (Grant Nos. 61522210, 61632013).

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 2013. LNCS, vol. 7959, pp. 88–103. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-39059-3_7
2. Blömer, J., May, A.: New partial key exposure attacks on RSA. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 27–43. Springer, Heidelberg (2003). https://doi.org/10.1007/978-3-540-45146-4_2
3. Boneh, D., Durfee, G.: Cryptanalysis of RSA with private key d less than $N^{0.292}$. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 1–11. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48910-X_1
4. Boneh, D., Durfee, G., Frankel, Y.: An attack on RSA given a small fraction of the private key bits. In: Ohta, K., Pei, D. (eds.) ASIACRYPT 1998. LNCS, vol. 1514, pp. 25–34. Springer, Heidelberg (1998). https://doi.org/10.1007/3-540-49649-1_3
5. Bunder, M., Nitaj, A., Susilo, W., Tonien, J.: A new attack on three variants of the RSA cryptosystem. In: Liu, J.K., Steinfeld, R. (eds.) ACISP 2016. LNCS, vol. 9723, pp. 258–268. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-40367-0_16
6. Bunder, M., Tonien, J.: New attack on the RSA cryptosystem based on continued fractions. Malays. J. Math. Sci. **11**(S3), 45–57 (2017)
7. Castagnos, G.: An efficient probabilistic public-key cryptosystem over quadratic fields quotients. Finite Fields Appl. **13**(3), 563–576 (2007)
8. Coppersmith, D.: Finding a small root of a bivariate integer equation; factoring with high bits known. In: Maurer, U. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 178–189. Springer, Heidelberg (1996). https://doi.org/10.1007/3-540-68339-9_16

9. Coppersmith, D.: Finding a small root of a univariate modular equation. In: Maurer, U. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 155–165. Springer, Heidelberg (1996). https://doi.org/10.1007/3-540-68339-9_14
10. Coppersmith, D.: Small solutions to polynomial equations, and low exponent RSA vulnerabilities. *J. Cryptol.* **10**(4), 233–260 (1997)
11. Coron, J.-S.: Finding small roots of bivariate integer polynomial equations revisited. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 492–505. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-24676-3_29
12. Coron, J.-S.: Finding small roots of bivariate integer polynomial equations: a direct approach. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 379–394. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-74143-5_21
13. Elkamchouchi, H., Elshenawy, K., Shaban, H.: Extended RSA cryptosystem and digital signature schemes in the domain of Gaussian integers. In: ICCS 2002, vol. 1, pp. 91–95. IEEE (2002)
14. Ernst, M., Jochemsz, E., May, A., de Weger, B.: Partial key exposure attacks on RSA up to full size exponents. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 371–386. Springer, Heidelberg (2005). https://doi.org/10.1007/11426639_22
15. Fiat, A.: Batch RSA. In: Brassard, G. (ed.) CRYPTO 1989. LNCS, vol. 435, pp. 175–185. Springer, New York (1990). https://doi.org/10.1007/0-387-34805-0_17
16. Halderman, J.A., Schoen, S.D., Heninger, N., Clarkson, W., Paul, W., Calandrino, J.A., Feldman, A.J., Appelbaum, J., Felten, E.W.: Lest we remember: cold-boot attacks on encryption keys. *Commun. ACM* **52**(5), 91–98 (2009)
17. 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). https://doi.org/10.1007/978-3-642-13013-7_4
18. Howgrave-Graham, N.: Finding small roots of univariate modular equations revisited. In: Darnell, M. (ed.) Cryptography and Coding 1997. LNCS, vol. 1355, pp. 131–142. Springer, Heidelberg (1997). <https://doi.org/10.1007/BFb0024458>
19. Howgrave-Graham, N., Seifert, J.-P.: Extending Wiener’s attack in the presence of many decrypting exponents. *CQRE* 1999. LNCS, vol. 1740, pp. 153–166. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-46701-7_14
20. 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). https://doi.org/10.1007/11935230_18
21. 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). https://doi.org/10.1007/978-3-540-74143-5_22
22. Kocher, P.C.: Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In: Kobitz, N. (ed.) CRYPTO 1996. LNCS, vol. 1109, pp. 104–113. Springer, Heidelberg (1996). https://doi.org/10.1007/3-540-68697-5_9
23. Kuwakado, H., Koyama, K., Tsuruoka, Y.: New RSA-type scheme based on singular cubic curves $y^2 \equiv x^3 + bx^2 \pmod{n}$. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **E78-A**(1), 27–33 (1995)
24. Lenstra, A.K., Lenstra, H.W., Lovász, L.: Factoring polynomials with rational coefficients. *Math. Ann.* **261**(4), 515–534 (1982)

25. May, A.: Using LLL-reduction for solving RSA and factorization problems. In: Nguyen, P.Q., Vallée, B. (eds.) *The LLL Algorithm - Survey and Applications*. ISC, pp. 315–348. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-02295-1_10
26. Peng, L., Hu, L., Lu, Y., Sarkar, S., Xu, J., Huang, Z.: Cryptanalysis of variants of RSA with multiple small secret exponents. In: Biryukov, A., Goyal, V. (eds.) *INDOCRYPT 2015*. LNCS, vol. 9462, pp. 105–123. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-26617-6_6
27. Peng, L., Hu, L., Lu, Y., Wei, H.: An improved analysis on three variants of the RSA cryptosystem. In: Chen, K., Lin, D., Yung, M. (eds.) *Inscrypt 2016*. LNCS, vol. 10143, pp. 140–149. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-54705-3_9
28. Quisquater, J.J., Couvreur, C.: Fast decipherment algorithm for RSA public-key cryptosystem. *Electron. Lett.* **18**(21), 905–907 (1982)
29. Ristenpart, T., Tromer, E., Shacham, H., Savage, S.: Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In: Al-Shaer, E., Jha, S., Keromytis, A.D. (eds.) *ACM CCS 2009*, pp. 199–212. ACM Press, Chicago (2009)
30. Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **21**(2), 120–126 (1978)
31. Sarkar, S.: Small secret exponent attack on RSA variant with modulus $N = p^r q$. *Des. Codes Cryptogr.* **73**(2), 383–392 (2014)
32. Sarkar, S.: Revisiting prime power RSA. *Discrete Appl. Math.* **203**, 127–133 (2016)
33. Sarkar, S., Maitra, S.: Cryptanalytic results on ‘Dual CRT’ and ‘Common Prime’ RSA. *Des. Codes Cryptogr.* **66**(1–3), 157–174 (2013)
34. Sarkar, S., Venkateswarlu, A.: Partial key exposure attack on CRT-RSA. In: Meier, W., Mukhopadhyay, D. (eds.) *INDOCRYPT 2014*. LNCS, vol. 8885, pp. 255–264. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-13039-2_15
35. Takagi, T.: Fast RSA-type cryptosystem modulo $p^k q$. In: Krawczyk, H. (ed.) *CRYPTO 1998*. LNCS, vol. 1462, pp. 318–326. Springer, Heidelberg (1998). <https://doi.org/10.1007/BFb0055738>
36. 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, Cham (2014). https://doi.org/10.1007/978-3-319-08344-5_12
37. Takayasu, A., Kunihiro, N.: Partial key exposure attacks on RSA: achieving the Boneh-Durfee bound. In: Joux, A., Youssef, A. (eds.) *SAC 2014*. LNCS, vol. 8781, pp. 345–362. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-13051-4_21
38. Takayasu, A., Kunihiro, N.: Partial key exposure attacks on RSA with multiple exponent pairs. In: Liu, J.K., Steinfeld, R. (eds.) *ACISP 2016*. LNCS, vol. 9723, pp. 243–257. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-40367-0_15
39. Takayasu, A., Kunihiro, N.: A tool kit for partial key exposure attacks on RSA. In: Handschuh, H. (ed.) *CT-RSA 2017*. LNCS, vol. 10159, pp. 58–73. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-52153-4_4
40. Wiener, M.J.: Cryptanalysis of short RSA secret exponents. *IEEE Trans. Inf. Theory* **36**(3), 553–558 (1990)
41. Zheng, M., Hu, H.: Cryptanalysis of prime power RSA with two private exponents. *Sci. China Inf. Sci.* **58**(11), 1–8 (2015)