Cryptanalysis of RSA Variants with Primes Sharing Most Significant Bits

Meryem Cherkaoui-Semmouni[1], Abderrahmane Nitaj[2(✉)], Willy Susilo[3], and Joseph Tonien[3]

[1] ICES Team, ENSIAS, Mohammed V University in Rabat, Morocco
meryem.semmouni@um5s.net.ma
[2] Normandie Univ, UNICAEN, CNRS, LMNO, 14000 Caen, France
abderrahmane.nitaj@unicaen.fr
[3] Institute of Cybersecurity and Cryptology, School of Computing and Information Technology, University of Wollongong, Australia
{willy.susilo,joseph.tonien}@uow.edu.au

Abstract. We consider four variants of the RSA cryptosystem with an RSA modulus $N = pq$ where the public exponent e and the private exponent d satisfy an equation of the form $ed - k\left(p^2-1\right)\left(q^2-1\right) = 1$. We show that, if the prime numbers p and q share most significant bits, that is, if the prime difference $|p-q|$ is sufficiently small, then one can solve the equation for larger values of d, and factor the RSA modulus, which makes the systems insecure.

Keywords: RSA variants, Continued fractions, Coppersmith's method, Lattice reduction.

1 Introduction

The RSA cryptosystem [16] is one of the most used public key cryptosystems. The arithmetic of RSA is based on a few parameters, namely a modulus of the form $N = pq$ where p and q are large primes, a public exponent e satisfying $\gcd(e, \phi(N)) = 1$ where $\phi(N) = (p-1)(q-1)$, and a private exponent d satisfying $ed \equiv 1 \pmod{\phi(N)}$. To encrypt a message m, one simply computes the ciphertext $c \equiv m^e \pmod{N}$, and to decrypt it, one computes $m \equiv c^d \pmod{N}$.

To ease the exponentiation in the decryption phase, a natural way is to choose a mall private exponent. Unfortunately, Wiener [21] showed that if $d < \frac{1}{3}N^{\frac{1}{4}}$, then one can factor N by computing the convergents of the continued fraction expansion of $\frac{e}{N}$. Later on, Boneh and Durfee [1] extended the bound up to $d < N^{0.292}$ by applying Coppersmith's method [7] and lattice reduction techniques. Also, there are plenty of attacks on RSA that depend on the arithmetical structure of its parameters [2,10]. A typical attack on RSA with a specific structure, presented by de Weger [20] in 2002, exploits the size of the difference of the prime factors $|p-q|$. It notably improves the attack of Wiener, as well as the attack of Boneh and Durfee when $|p-q|$ is suitably small.

Since its invention by Rivest, Shamir and Adleman in 1978, many variants of RSA have been proposed such as Multi-prime RSA [6], Rebalanced RSA [21], and RSA-CRT [19]. These variants use more or less the same arithmetic. However, some variants of RSA with notably different structures have been proposed in the literature. In the following, we present four of such variants having similar moduli and key equations.

1) In 1993, Smith and Lennon [17] proposed a system, called LUC, based on Lucas sequences. The modulus is $N = pq$, and the public and the private exponents are positive integers e and d satisfying $ed \equiv 1 \pmod{\left(p^2-1\right)\left(q^2-1\right)}$.
2) In 1995, Kuwakado et al. [12] presented a cryptosystem based on the singular cubic curve with the equation $y^2 \equiv x^3 + ax^2 \pmod{N}$ where $N = pq$ is an RSA modulus, and $a, x, y \in \mathbb{Z}/N\mathbb{Z}$. In this system, the public exponent e and the private exponent d satisfy $ed \equiv 1 \pmod{\left(p^2-1\right)\left(q^2-1\right)}$.
3) In 2002, Elkamchouchi et al. [8] proposed a cryptosystem in the ring of Gaussian integers. The operations are performed modulo $N = PQ$ where P and Q are two Gaussian primes. The public exponent e and the private exponent d are positive integers satisfying $ed \equiv 1 \pmod{\left(|P|^2-1\right)\left(|Q|^2-1\right)}$ where $|P|$ and $|Q|$ are prime integers.
4) In 2006, Castagnos [5] presented a probabilistic cryptosystem over quadratic field quotients. As in LUC, this cryptosystem uses Lucas sequences, and the modulus is in the form $N = pq$. As in the previous cryptosystems, the public exponent e, and the private exponent d are positive integers satisfying $ed \equiv 1 \pmod{\left(p^2-1\right)\left(q^2-1\right)}$.

A common characteristic of the former cryptosystems is that they share the key equation $ed \equiv 1 \pmod{\left(p^2-1\right)\left(q^2-1\right)}$. The cryptanalysis of such systems started in 2016 with the work of Bunder et al. [3]. They transformed the key equation into an equation of the form $ed - k\left(p^2-1\right)\left(q^2-1\right) = 1$, and showed that $\frac{k}{d}$ can be computed by a convergent of the continued fraction expansion of $\frac{e}{N^2-\frac{9}{4}N+1}$ if $d < \sqrt{\frac{2N^3-18N^2}{e}}$. Then, in 2017, Bunder et al. [4] studied the case when $N = pq$, and the public exponent e satisfies an equation of the form $ex - \left(p^2-1\right)\left(q^2-1\right)y = z$. They combined Coppersmith's technique, and the continued fraction method and showed that one can factor N if $xy < 2N - 4\sqrt{2}N^{\frac{3}{4}}$ and $|z| < |p-q|N^{\frac{1}{4}}y$. For $z = 1$, the equation becomes $ed - k\left(p^2-1\right)\left(q^2-1\right) = 1$, and the bound on d is $d < \sqrt{2N - 4\sqrt{2}N^{\frac{3}{4}}}$. The same equation $ex - \left(p^2-1\right)\left(q^2-1\right)y = z$ was later considered by Nitaj et al. [15]. For $e = N^{\alpha}$, and $d = N^{\delta}$, they showed that the equation $ed - k\left(p^2-1\right)\left(q^2-1\right) = 1$ can be solved and N can be factored if $\delta < \frac{7}{3} - \frac{2}{3}\sqrt{1+3\alpha}$. In [18], Peng et al. obtained the better bound $\delta < 2 - \sqrt{\alpha}$ by mixing Coppersmith's method and unravelled linearization techniques. Finally, Zheng et al. [22] reconsidered the key equation $ed - k\left(p^2-1\right)\left(q^2-1\right) = 1$, and obtained a similar bound on d which is applicable for $1 \leq \alpha < 4$.

In this paper, we study the cryptanalysis of the former four variants of RSA if the RSA modulus $N = pq$ is such that $q < p < 2q$, and $p - q = N^{\beta}$. We note here

that, for $q < p < 2q$, we have always $0 < \beta < \frac{1}{2}$. However, if $\beta < \frac{1}{4}$, then one can find p and q by Fermat's method (see [20]), or by Coppersmith's method [7]. Our starting point is the key equation $ed - k\left(p^2-1\right)\left(q^2-1\right) = 1$ which is common to the four variants. More precisely, for $q < p < 2q$, we set $e = N^\alpha$, $p - q = N^\beta$, $d = N^\delta$. Then, by applying the continued fraction algorithm, we show that, under the condition $\delta < 2 - \beta - \frac{1}{2}\alpha$, the rational number $\frac{k}{d}$ is a convergent of the continued fraction expansion of $\frac{e}{(N-1)^2}$. This leads us to find p and q, and break the system. Also, we show that the key equation can be transformed to a modular polynomial equation of the form $f(x,y) = xy + Ax + 1 \equiv 0 \pmod{e}$, with $A = -(N-1)^2$, where $(x,y) = \left(-k, (p-q)^2\right)$ is a solution. Then by applying Coppersmith's method and lattice reduction techniques, we show that, under the condition $\delta < 2 - \sqrt{2\alpha\beta}$, one can factor the RSA modulus N. If we apply our attacks to the case where p and q are randomly chosen, that is $p - q = \mathcal{O}\left(N^\beta\right)$ with $\beta = \frac{1}{2}$, then our bounds on δ and d retrieve the existing bounds in the previous attacks in [3,15,18,22].

The paper is organized as follows. Section 2 presents the preliminaries to the next sections. In Section 3, we present our first attack based on the continued fraction algorithm. In Section 4, we present our second attack based on Coppersmith's method and lattice reduction techniques. In Section 5, we compare the new results to existing ones in the literature. We conclude the paper in Section 6.

2 Preliminaries

In this section, we present some fundamental concepts and results relevant to our methods.

2.1 A useful lemma

We start by the following result (see [3]).

Lemma 1. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Then*

$$N^2 - \frac{5}{2}N + 1 < \left(p^2-1\right)\left(q^2-1\right) < N^2 - 2N + 1.$$

2.2 Continued fractions

Let ξ be real number. The continued fraction expansion of ξ is an expression of the form

$$\xi = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}},$$

where $a_0 \in \mathbb{Z}$, and $a_i \in \mathbb{N}^*$ for $i \geq 1$. If ξ is a rational number, the list $[a_0, a_1, a_2, \ldots]$ of partial quotients is finite and can be computed in polynomial

time. For $n \geq 0$, $[a_0, a_1, a_2, \ldots, a_n]$ is a rational number and is called a convergent of the continued fraction expansion of ξ. There are various properties of the continued fraction expansion of real numbers, and the following is useful to check whether a rational number $\frac{a}{b}$ is a convergent of a real number ξ [9].

Theorem 1. *Let ξ be a positive real number. If a and b are integers satisfying* $\gcd(a, b) = 1$ *and*

$$\left|\xi - \frac{a}{b}\right| < \frac{1}{2b^2},$$

then $\frac{a}{b}$ is a convergent of the continued fraction expansion of ξ.

2.3 Lattice reduction

Let $b_1, b_2, \ldots, b_\omega$ be ω linearly independent vectors of $\mathbb{R}^n$ with $n \geq \omega$. The lattice $\mathcal{L}$ spanned by the vectors $b_1, b_2, \ldots, b_\omega$ is the set of their integer linear combinations, that is

$$\mathcal{L} = \left\{ \sum_{i=1}^{\omega} x_i b_i,\ x_1, \ldots, x_\omega \in \mathbb{Z} \right\}.$$

The list $(b_1, b_2, \ldots, b_\omega)$ is called a basis of the lattice $\mathcal{L}$, ω is its dimension, and n is its rank. When $\omega = n$, the lattice is called full-rank. A basis matrix B for the lattice can be constructed by expanding the vectors b_i in the rows. The lattice determinant is then defined by $\det(\mathcal{L}) = \sqrt{\det(BB^t)}$, where B^t is the transpose of B. When the lattice if full-rank, B is a square matrix and $\det(\mathcal{L}) = |\det(B)|$.

Lattices are used in several domains, especially in cryptography for creating new systems and for cryptanalysis. As a lattice has infinitely many bases, it is crucial to find a basis with good properties, typically with short vectors. In 1982, Lenstra, Lenstra, and Lovász [13] proposed an algorithm, called LLL, to find a good basis and short vectors in a lattice. A useful property of the LLL algorithm is the following result [14]

Theorem 2. *Let $\mathcal{L}$ be a lattice spanned by a basis $(u_1, u_2, \ldots, u_\omega)$. The LLL algorithm produces a new basis $(b_1, b_2, \ldots, b_\omega)$ satisfying*

$$\|b_1\| \leq \ldots \leq \|b_i\| \leq 2^{\frac{\omega(\omega-1)}{4(\omega+1-i)}} \det(\mathcal{L})^{\frac{1}{\omega+1-i}}, \quad i = 1, \ldots, \omega.$$

Let e be an integer and $f(x_1, x_2, \ldots, x_n) = \sum_{i_1, i_2, \ldots, i_n} a_{i_1, i_2, \ldots, i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$ with $a_{i_1, i_2, \ldots, i_n} \in \mathbb{Z}$. The Euclidean norm of the polynomial f is defined by $\|f(x_1, x_2, \ldots, x_n)\| = \sqrt{\sum a_{i_1, i_2, \ldots, i_n}^2}$. In 1997, Coppersmith [7] developed a technique to find the small solutions of the modular polynomial equation $f(x_1) \equiv 0 \pmod{N}$ with one variable, and the small roots of the polynomial $f(x_1, x_2) = 0$ with two variables, by applying lattice reduction. Later, the technique has been extended to more variables, especially to find the small solutions of the modular polynomial equation $f(x_1, x_2, \ldots, x_n) \equiv 0 \pmod{e}$. The following result, due to Howgrave-Graham [11], is a cornerstone in Coppersmith's method.

Theorem 3 (Howgrave-Graham). *Let $f(x_1, x_2, \ldots, x_n) \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$ be a polynomial with at most ω monomials, and e a positive integer. Suppose that*

$$f(x'_1, x'_2, \ldots, x'_n) \equiv 0 \pmod{e} \text{ and } \|f(x_1X_1, x_2X_2, \ldots, x_nX_n))\| < \frac{e}{\sqrt{\omega}},$$

where $|x'_1| < X_1, |x'_2| < X_2, \ldots, |x'_n| < X_n$. Then $f(x'_1, x'_2, \ldots, x'_n) = 0$ holds over the integers.

The starting step in Coppersmith's method for finding the small solutions of the modular polynomial equation $f(x_1, x_2, \ldots, x_n) \equiv 0 \pmod{e}$ is to generate ω polynomials $g_i(x_1, x_2, \ldots, x_n)$ satisfying $g_i(x'_1, x'_2, \ldots, x'_n) \equiv 0 \pmod{e}$ for $1 \leq i \leq \omega$. The coefficients of the polynomials $g_i(x_1, x_2, \ldots, x_n)$ are then used to build a matrix of a lattice $\mathcal{L}$. Applying the LLL algorithm to the lattice produces a new matrix from which ω new polynomials $h_i(x_1, x_2, \ldots, x_n)$ are extracted such that $h_i(x'_1, x'_2, \ldots, x'_n) \equiv 0 \pmod{e}$. If, in addition, at least n of such polynomials satisfy Theorem 3, then using resultant techniques or Gröbner basis method, one can extract the small solution $(x'_1, x'_2, \ldots, x'_n)$. We note that for $n \geq 3$, Coppersmith's method to extract the solutions is heuristic. It depends on the assumption that the polynomials derived from the reduced basis are algebraically independent. In this paper, we always successfully extracted the solutions by Gröbner basis computation.

3 The Attack Based on Continued Fraction Algorithm

In this section, we present our first attack which is based on the continued fraction algorithm.

Theorem 4. *Let $N = pq$ be an RSA modulus with $q < p < 2q$ and $|p-q| = N^\beta$. Let $e = N^\alpha$ be a public exponent satisfying the equation $ed - k\left(p^2-1\right)\left(q^2-1\right) = 1$ with $d = N^\delta$. If*

$$\delta < 2 - \beta - \frac{1}{2}\alpha,$$

then one can find p and q in polynomial time.

Proof. Suppose that $N = pq$ with $q < p < 2q$ and that a public exponent e satisfies the key equation $ed - k\left(p^2-1\right)\left(q^2-1\right) = 1$. Then

$$\begin{aligned} ed - (N-1)^2 k &= k\left(p^2-1\right)\left(q^2-1\right) + 1 - (N-1)^2 k \\ &= 1 + k\left(\left(p^2-1\right)\left(q^2-1\right) - (N-1)^2\right) \\ &= 1 - k(p-q)^2. \end{aligned}$$

This leads to

$$\left|\frac{e}{(N-1)^2} - \frac{k}{d}\right| = \frac{\left|1 - k(p-q)^2\right|}{d(N-1)^2} < \frac{k(p-q)^2}{d(N-1)^2}.$$

Using the key equation, we get $k\left(p^2-1\right)\left(q^2-1\right) = ed-1 < ed$. Then

$$\frac{k}{d} < \frac{e}{(p^2-1)(q^2-1)},$$

and

$$\left|\frac{e}{(N-1)^2} - \frac{k}{d}\right| < \frac{e(p-q)^2}{(N-1)^2(p^2-1)(q^2-1)}.$$

By Lemma 1, we have

$$\begin{aligned}(N-1)^2\left(p^2-1\right)\left(q^2-1\right) &> (N-1)^2\left(N^2-\frac{5}{2}N+1\right)\\ &= N^4-\frac{9}{2}N^3+7N^2-\frac{9}{2}N+1\\ &> \frac{1}{2}N^4,\end{aligned}$$

where the last inequality is valid for $N \geq 8$. Hence using $e = N^\alpha$, $|p-q| = N^\beta$, and $d = N^\delta$, we get

$$\left|\frac{e}{(N-1)^2} - \frac{k}{d}\right| < \frac{e(p-q)^2}{(N-1)^2(p^2-1)(q^2-1)} < 2N^{\alpha+2\beta-4}.$$

If $2N^{\alpha+2\beta-4} < \frac{1}{2}N^{-2\delta}$, that is $\delta < 2-\beta-\frac{1}{2}\alpha$, then

$$\left|\frac{e}{(N-1)^2} - \frac{k}{d}\right| < \frac{1}{2}N^{-2\delta} = \frac{1}{2d^2}.$$

It follows that one can find $\frac{k}{d}$ amongst the convergents of the continued fraction expansion of $\frac{e}{(N-1)^2}$. Then, using the values of k and d in the key equation $ed - k\left(p^2-1\right)\left(q^2-1\right) = 1$, we get $p^2+q^2 = N^2+1-\frac{ed-1}{k}$. Combining this with $N = pq$, we find p and q. □

We note that if p and q are such that $p-q \approx N^{\frac{1}{2}}$, then $\beta \approx \frac{1}{2}$, and the bound on δ in Theorem 4 is $\delta < \frac{3}{2}-\frac{\alpha}{2}$. This retrieves the results of [3].

4 The Attack Based on Coppersmith's Method

In this section, we apply Coppersmith's method and lattice reduction techniques to launch an attack on the RSA variants with a modulus $N = pq$ where the prime difference $|p-q|$ is sufficiently small, and the exponents e and d satisfy the equation $ed - k\left(p^2-1\right)\left(q^2-1\right) = 1$.

Theorem 5. *Let (N,e) be a public key for the RSA variants where $N = pq$ with $q < p < 2q$, and $e = N^\alpha$. Suppose that e satisfies the equation $ed - k\left(p^2-1\right)\left(q^2-1\right) = 1$ with $d = N^\delta$ and $|p-q| < N^\beta$. If*

$$\delta < 2-\sqrt{2\alpha\beta}-\varepsilon,$$

for a small positive constant ε, then one can factor N in polynomial time.

Proof. Suppose that $N = pq$ and $e = N^\alpha$ satisfy the equation $ed - k\left(p^2-1\right)\left(q^2-1\right) = 1$ with $d = N^\delta$ and $|p-q| = N^\beta$. By Lemma 1, for $N \geq 5$, we have

$$\left(p^2-1\right)\left(q^2-1\right) > N^2 + 1 - \frac{5}{2}N > \frac{1}{2}N^2.$$

Then

$$k = \frac{ed-1}{(p^2-1)(q^2-1)} < \frac{2ed}{N^2} = 2N^{\alpha+\delta-2},$$

which gives an upper bound for k. On the other hand, the key equation can be rewritten as

$$(-k)(p-q)^2 - (N-1)^2(-k) + 1 \equiv 0 \pmod{e}.$$

Consider the polynomial $f(x,y) = xy + Ax + 1$, with $A = -(N-1)^2$. Then $(x,y) = \left(-k, (p-q)^2\right)$ is a solution of the modular polynomial equation $f(x,y) \equiv 0 \pmod{e}$. To find the small solutions, we apply Coppersmith's method [7] to the polynomial $F(x,u) = u + Ax$ where $u = xy + 1$ with the bounds

$$|x| < 2N^{\alpha+\delta-2}, \quad |y| < N^{2\beta}, \quad |u| < 2N^{\alpha+\delta+2\beta-2}.$$

Let m and t be two positive integers to be specified later. Consider the polynomials

$$\begin{aligned}
&G_{k,i_1,i_2,i_3}(x,y,u) = x^{i_1}F(x,u)^k e^{m-k},\\
&\text{with } k = 0,\ldots m,\ i_1 = 0,\ldots,m-k,\ i_2 = 0,\ i_3 = k,\\
&H_{k,i_1,i_2,i_3}(x,y,u) = y^{i_2}F(x,u)^k e^{m-k},\\
&\text{with } i_1 = 0, i_2 = 1,\ldots t,\ k = \left\lfloor \frac{m}{t} \right\rfloor i_2,\ldots,m,\ i_3 = k.
\end{aligned}$$

In the expansion of the polynomial $H_{k,i_1,i_2,i_3}(x,y,u)$, each term xy is replaced by $u-1$. The monomials of $G_{k,i_1,i_2,i_3}(x,y,u)$ and $H_{k,i_1,i_2,i_3}(x,y,u)$ are ordered by the following rule

- A monomial of $G_{k,i_1,i_2,i_3}(x,y,u)$ is prior to every monomial of $H_{k,i_1,i_2,i_3}(x,y,u)$.
- The monomials of $G_{k,i_1,i_2,i_3}(x,y,u)$ are ordered following the output of the procedure
  for $k = 0,\ldots m$, for $i_1 = 0,\ldots,m-k$, for $i_2 = 0$, for $i_3 = k$, output $x^{i_1}y^{i_2}u^{i_3}$.
- The monomials of $H_{k,i_1,i_2,i_3}(x,y,u)$ are ordered following the output of the procedure
  for $i_1 = 0$, for $i_2 = 1,\ldots t$, for $k = \left\lfloor \frac{m}{t} \right\rfloor i_2,\ldots,m$, for $i_3 = k$, output $x^{i_1}y^{i_2}u^{i_3}$.

The polynomials are ordered by similar rules. We set

$$X = 2N^{\alpha+\delta-2},\ Y = N^{2\beta},\ U = 2N^{\alpha+\delta+2\beta-2}. \tag{1}$$

We consider the lattice $\mathcal{L}$ where the rows of the basis matrix is built by considering the coefficients of the monomials of the polynomials $G_{k,i_1,i_2,i_3}(Xx, Yy, Uu)$ and $H_{k,i_1,i_2,i_3}(Xx, Yy, Uu)$. We note that the lattice $\mathcal{L}$ is different from the

lattices used in [18,22,15]. Table 1 shows the lattice basis matrix generated by $m = 2$ and $t = 2$.

	1	x	x^2	u	xu	u^2	yu	yu^2	y^2u^2
$G_{0,0,0,0}(x,y,u)$	e^2	0	0	0	0	0	0	0	0
$G_{0,1,0,0}(x,y,u)$	0	Xe^2	0	0	0	0	0	0	0
$G_{,2,0,0}(x,y,u)$	0	0	X^2e^2	0	0	0	0	0	0
$G_{1,0,0,1}(x,y,u)$	0	Xa_1e	0	Ue	0	0	0	0	0
$G_{1,1,0,1}(x,y,u)$	0	0	X^2a_1e	0	XUe	0	0	0	0
$G_{2,0,0,2}(x,y,u)$	0	0	$X^2a_1^2$	0	$2UXa_1$	U^2	0	0	0
$H_{1,0,1,1}(x,y,u)$	$-a_1e$	0	0	Ua_1e	0	0	UYe	0	0
$H_{2,0,1,2}(x,y,u)$	0	$-a_1^2X$	0	$-2Ua_1$	a_1^2UX	$2U^2a_1$	0	U^2Y	0
$H_{2,0,2,2}(x,y,u)$	a_1^2	0	0	$-2Ua_1^2$	0	$U^2a_1^2$	$-2Ua_1Y$	$2U^2a_1Y$	U^2Y^2

Table 1. The lattice basis matrix for $m = 2$ and $t = 2$.

The lattice basis matrix is triangular and the determinant of the lattice is of the form

$$\det(\mathcal{L}) = X^{n_X}Y^{n_Y}U^{n_U}e^{n_e}, \tag{2}$$

and the dimension is ω with

$$\begin{aligned}
n_X &= \sum_{k=0}^{m}\sum_{i_1=0}^{m-k} i_1 = \frac{1}{6}m^3 + o(m^3),\\
n_Y &= \sum_{i_2=1}^{t}\sum_{k=\lfloor \frac{m}{t} \rfloor}^{m} i_2 = \frac{1}{2}mt^2 - \frac{1}{3}\left\lfloor \frac{m}{t} \right\rfloor t^3 + o(mt^2),\\
n_U &= \sum_{k=0}^{m}\sum_{i_1=0}^{m-k} k + \sum_{i_2=1}^{t}\sum_{k=\lfloor \frac{m}{t} \rfloor}^{m} k = \frac{1}{6}m^3 + \frac{1}{2}m^2t - \frac{1}{6}\left\lfloor \frac{m}{t} \right\rfloor^2 t^3 + o(m^3),\\
n_e &= \sum_{k=0}^{m}\sum_{i_1=0}^{m-k} (m-k) + \sum_{i_2=1}^{t}\sum_{k=\lfloor \frac{m}{t} \rfloor}^{m} (m-k)\\
&= \frac{1}{3}m^3 + \frac{1}{2}m^2t + \frac{1}{6}\left\lfloor \frac{m}{t} \right\rfloor^2 t^3 - \frac{1}{2}\left\lfloor \frac{m}{t} \right\rfloor mt^2 + o(m^3).\\
\omega &= \sum_{k=0}^{m}\sum_{i_1=0}^{m-k} 1 + \sum_{i_2=1}^{t}\sum_{k=\lfloor \frac{m}{t} \rfloor}^{m} 1 = \frac{1}{2}m^2 + mt - \frac{1}{2}\left\lfloor \frac{m}{t} \right\rfloor t^2 + o(m^2).
\end{aligned}$$

If we set $t = m\tau$ and replace $\lfloor \frac{m}{t} \rfloor$ by $\frac{1}{\tau}$ in the above approximations, we get

$$\begin{aligned} n_X &= \frac{1}{6}m^3 + o(m^3), \\ n_Y &= \frac{1}{6}\tau^2 m^3 + o(m^3), \\ n_U &= \frac{1}{6}(2\tau+1)m^3 + o(m^3), \\ n_e &= \frac{1}{6}(\tau+2)m^3 + o(m^3), \\ \omega &= \frac{1}{2}(\tau+1)m^2 + o(m^2). \end{aligned} \tag{3}$$

Applying the LLL algorithm to the lattice $\mathcal{L}$, we get a new matrix satisfying the inequalities of Theorem 2. To combine it with Theorem 3, we set

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

or equivalently $\det(\mathcal{L}) < 2^{-\frac{\omega(\omega-1)}{4}} (\sqrt{\omega})^{2-\omega} e^{m(\omega-2)}$. Using (2), we get

$$X^{n_X} Y^{n_Y} U^{n_U} e^{n_e} < 2^{-\frac{\omega(\omega-1)}{4}} \left(\sqrt{\omega}\right)^{2-\omega} e^{m(\omega-2)}.$$

Then, using (3), and by a straightforward calculation, we get the inequality

$$\begin{aligned} \frac{1}{6}(\alpha+\delta-2) + \frac{1}{6}\tau^2(2\beta) + \frac{1}{6}(2\tau+1)(\alpha+\delta+2\beta-2) \\ + \frac{1}{6}(\tau+2)\alpha - \frac{1}{2}(\tau+1)\alpha < -\varepsilon_1, \end{aligned}$$

where ε_1 is a small positive constant that depends only on N and m. The left side is optimized for $\tau_0 = \frac{2-\delta-2\beta}{2\beta}$. Plugging τ_0 in the former inequality, we get

$$-\delta^2 + 4\delta + 2\alpha\beta - 4 < -\varepsilon_2,$$

with a small positive constant ε_2. This leads to the inequality

$$\delta < 2 - \sqrt{2\alpha\beta} - \varepsilon,$$

where ε is a small positive constant. Note that we also need $\tau_0 \geq 0$, that is $2 - \delta - 2\beta \geq 0$ and $\delta \leq 2 - 2\beta$. Consequently, δ should satisfy

$$\delta < \min\left(2 - \sqrt{2\alpha\beta} - \varepsilon, 2 - 2\beta\right)$$

For $\alpha \geq 2\beta$, that is $e \geq |p-q|^2$, we have $2 - \sqrt{2\alpha\beta} \leq 2 - 2\beta$, and the condition becomes $\delta < 2 - \sqrt{2\alpha\beta} - \varepsilon$. Under these conditions, the reduced lattice has three polynomials $h_1(x, y, u)$, $h_2(x, y, u)$ and $h_2(x, y, u)$ sharing the root $(x, y, u) = (-k, (p-q)^2, -k(p-q)^2 + 1)$. Then, applying Gröbner basis or resultant computations, we can extract the solution from which we deduce $p - q = \sqrt{y}$. Combining with the equation $pq = N$, this leads to the factorization of $N = pq$, and terminates the proof. □

5 Comparison with Former Attacks

Before starting comparing our results to existing ones, we notice that the bound on δ in Theorem 5 is always better than the bound in Theorem 4. To ease the comparison, we neglect the term ε in Theorem 5. For the same parameters α and β, the difference between the bounds in Theorem 5 and Theorem 4 is

$$\begin{aligned} 2-\sqrt{2\alpha\beta}-\left(2-\beta-\frac{1}{2}\alpha\right) &= \beta+\frac{1}{2}\alpha-\sqrt{2\alpha\beta} \\ &= \frac{\left(\beta+\frac{1}{2}\alpha\right)^2-2\alpha\beta}{\beta+\frac{1}{2}\alpha+\sqrt{2\alpha\beta}} \\ &= \frac{\left(\beta-\frac{1}{2}\alpha\right)^2}{\beta+\frac{1}{2}\alpha+\sqrt{2\alpha\beta}} \\ &\geq 0, \end{aligned}$$

which implies that $2-\sqrt{2\alpha\beta} \geq 2-\beta-\frac{1}{2}\alpha$.

In [3], Bunder et al. studied the key equation $ed-k\left(p^2-1\right)\left(q^2-1\right)=1$ by the method of the continued fractions. They showed that if d satisfies $d<\sqrt{\frac{2N^3-18N^2}{e}}$, then $\frac{k}{d}$ is a convergent of the continued fraction expansion of $\frac{e}{N^2-\frac{9}{4}N+1}$, the key equation can be solved and N can be factored. If we set $d=N^\delta$, and $e=N^\alpha$, then the former inequality gives $\delta<\frac{3}{2}-\frac{1}{2}\alpha$ which is the same than the bound of Theorem 4 with $|p-q|=N^\beta$ and $\beta=\frac{1}{2}$. As a consequence, the results of [3] can be retrieved by our method as in Theorem 4.

In [15], Nitaj et al. studied the variant equation $eu-\left(p^2-1\right)\left(q^2-1\right)v=w$ with $e=N^\alpha$, $u<N^\delta$, $|w|<N^\gamma$, and showed that under the conditions $\delta<\frac{7}{3}-\gamma-\frac{2}{3}\sqrt{1+3\alpha-3\gamma}$, one can factor the RSA modulus $N=pq$. If we take $\gamma=0$, then the equation becomes $eu-\left(p^2-1\right)\left(q^2-1\right)v=1$, and the condition is $\delta<\frac{7}{3}-\frac{2}{3}\sqrt{1+3\alpha}$. To compare it with the bound of Theorem 5, we take $|p-q|=N^\beta$ with $\beta=\frac{1}{2}$, and the bound becomes $\delta<2-\sqrt{\alpha}$. Then

$$\begin{aligned} 2-\sqrt{\alpha}-\left(\frac{7}{3}-\frac{2}{3}\sqrt{1+3\alpha}\right) &= \frac{2}{3}\sqrt{1+3\alpha}-\sqrt{\alpha}-\frac{1}{3} \\ &= \frac{\frac{4}{9}(1+3\alpha)-\left(\sqrt{\alpha}+\frac{1}{3}\right)^2}{\frac{2}{3}\sqrt{1+3\alpha}+\sqrt{\alpha}+\frac{1}{3}} \\ &= \frac{\frac{1}{3}+\frac{1}{3}\alpha-\frac{2}{3}\sqrt{\alpha}}{\frac{2}{3}\sqrt{1+3\alpha}+\sqrt{\alpha}+\frac{1}{3}} \\ &= \frac{\frac{1}{3}\left(1-\sqrt{\alpha}\right)^2}{\frac{2}{3}\sqrt{1+3\alpha}+\sqrt{\alpha}+\frac{1}{3}} \\ &\geq 0, \end{aligned}$$

which shows that our bound in Theorem 5 is always better than the bound of [15].

In [18], Peng et al. studied the key equation $ed - k\left(p^2-1\right)\left(q^2-1\right) = 1$ by Coppersmith's method, with $e = N^\alpha$, and $d = N^\delta$. The key equation is first transformed to the modular equation $k\left(N^2+1-p^2-q^2\right)+1 \equiv 0 \pmod{e}$, and then to the modular equation $x(y+A)+1 \equiv 0 \pmod{e}$ with $A = N^2+1$, $x = k$, and $y = -\left(p^2+q^2\right)$. They showed that one can factor the RSA modulus if $\delta < 2-\sqrt{\alpha}$. In Theorem 5, if we set $|p-q| = N^\beta$ with $\beta = \frac{1}{2}$, we get the same condition. This shows that our method can be considered as an extension of the work in [18].

In [22], Zheng et al. studied the key equation $ed - k\left(p^2-1\right)\left(q^2-1\right) = 1$ and transformed it to $k\left((N+1)^2-(p+q)^2\right)+1 \equiv 0 \pmod{e}$, and also to $x(y+A)+1 \equiv 0 \pmod{e}$ with $A = (N+1)^2$, $x = k$, and $y = -(p+q)^2$. They showed that one can solve the equation and factor N if $d = N^\delta$, $e = N^\alpha$, and $\delta < 2-\sqrt{\alpha}$. As specified before, this result can be retrieved by our method of Theorem 5.

6 Conclusion

In this paper, we studied the key equation $ed - k\left(p^2-1\right)\left(q^2-1\right) = 1$ derived from four variants of the RSA cryptosystem with a modulus $N = pq$, a public exponent e, and a private exponent d. Moreover, we considered the situation where the prime factors p and q are of equal bitsize, and share an amount of their most significant bits. We presented two different attacks on such variants. The first attack is based on the continued fraction algorithm, and the second attack is based on lattice reduction. For both attacks, we showed that the variants are insecure if the prime difference $p-q$, and the private exponent d are suitably small. Finally, we compared our new attacks to existing ones, and showed that our methods are more suitable for the cryptanalysis of the RSA variants.

References

1. Boneh, D., Durfee, G.: Cryptanalysis of RSA with private key d less than $N^{0.292}$, Advances in Cryptology-Eurocrypt'99, Lecture Notes in Computer Science Vol. 1592, Springer-Verlag, pp. 1–11 (1999)
2. Boneh, D.: Twenty years of attacks on the RSA cryptosystem, Notices Amer. Math. Soc. 46 (2), 203–213, (1999)
3. 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. 258268. Springer, Cham (2016).
4. M. Bunder, A. Nitaj, W. Susilo, and J. Tonien: A generalized attack on RSA type cryptosystems, Theoretical Computational Science, vol. 704, pp. 7481, 2017
5. G. Castagnos, An efficient probabilistic public-key cryptosystem over quadratic field quotients, 2007, Finite Fields and Their Applications, 07/2007, 13(3-13), p. 563-576. http://www.math.u-bordeaux1.fr/~gcastagn/publi/crypto_quad.pdf
6. T. Collins, D. Hopkins, S. Langford, and M. Sabin. Public key cryptographic apparatus and Method. US Patent #5,848,159, Jan. 1997.

7. Coppersmith, D.: Small solutions to polynomial equations, and low exponent RSA vulnerabilities. Journal of Cryptology, 10(4), pp. 233–260 (1997)
8. Elkamchouchi, H., Elshenawy, K., Shaban, H.: Extended RSA cryptosystem and digital signature schemes in the domain of Gaussian integers, in Proceedings of the 8th International Conference on Communication Systems, (2002) pp. 91–95.
9. G. H. Hardy and E. M. Wright: An Introduction to Theory of Numbers, 5th Edition, The Clarendon Press Oxford University Press, New York, 1979.
10. Hinek, M.: Cryptanalysis of RSA and Its Variants, Chapman & Hall/CRC, Cryptography and Network Security Series, Boca Raton, (2009)
11. Howgrave-Graham, N.: Finding small roots of univariate modular equations revisited, In Cryptography and Coding, LNCS 1355, pp. 131-142, Springer-Verlag (1997)
12. H. Kuwakado, K. Koyama, and Y. Tsuruoka: A new RSA-type scheme based on singular cubic curves $y^2 = x^3+bx^2 \pmod n$, IEICE Transactions on Fundamentals, vol. E78-A (1995) pp. 27–33.
13. Lenstra, A.K., Lenstra, H.W., Lovász, L.: Factoring polynomials with rational coefficients, Mathematische Annalen, Vol. 261, pp. 513–534, (1982)
14. May, A.: New RSA Vulnerabilities Using Lattice Reduction Methods, PhD Thesis, University of Paderborn (2003) `https://digital.ub.uni-paderborn.de/ubpb/urn/urn:nbn:de:hbz:466-20030101205`
15. Nitaj A., Pan Y., Tonien J.: a generalized attack on some variants of the RSA cryptosystem. In: Cid C., Jacobson Jr. M. (eds) Selected Areas in Cryptography - SAC 2018. SAC 2018. Lecture Notes in Computer Science, vol 11349. Springer, Cham (2018)
16. Rivest, R., Shamir, A., Adleman, L.: A Method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM, Vol. 21 (2), pp. 120–126 (1978)
17. P. J. Smith, G. J. J. Lennon, LUC: a new public-key cryptosystem, Ninth IFIP Symposium on Computer Science Security, Elsevier Science Publishers (1993), 103-117.
18. 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. 140149. Springer, Cham (2017)
19. J. J. Quisquater and C. Couvreur: Fast decipherment algorithm for RSA public key cryptosystem, Electronic Letters, vol. 18, pp.905-907, 1982
20. de Weger, B.: Cryptanalysis of RSA with small prime difference, Applicable Algebra in Engineering, Communication and Computing,Vol. 13(1), pp. 17–28 (2002)
21. Wiener, M.: Cryptanalysis of short RSA secret exponents, IEEE Transactions on Information Theory, Vol. 36, pp. 553–558 (1990)
22. Zheng, M., Kunihiro, N., Hu, H.: Cryptanalysis of RSA Variants with Modified Euler Quotient. In: Joux A., Nitaj A., Rachidi T. (eds) Progress in Cryptology-AFRICACRYPT 2018. AFRICACRYPT 2018. Lecture Notes in Computer Science, vol 10831. Springer, Cham (2018)