A Generalized Attack on Some Variants of the RSA Cryptosystem

Abderrahmane Nitaj, Yanbin Pan, Joseph Tonien

A Generalized Attack on Some Variants of the RSA Cryptosystem

Abderrahmane Nitaj[1], Yanbin Pan[2⋆], and Joseph Tonien[3]

[1] Laboratoire de Mathématiques Nicolas Oresme
Université de Caen Normandie, France
abderrahmane.nitaj@unicaen.fr
[2] Key Laboratory of Mathematics Mechanization, NCMIS, Academy of Mathematics and Systems Science, Chinese Academy of Sciences
panyanbin@amss.ac.cn
[3] School of Computing and Information Technology University of Wollongong, Australia
joseph.tonien@uow.edu.au

Abstract. Let $N = pq$ be an RSA modulus with unknown factorization. The RSA cryptosystem can be attacked by using the key equation $ed - k(p-1)(q-1) = 1$. Similarly, some variants of RSA, such as RSA combined with singular elliptic curves, LUC and RSA with Gaussian primes can be attacked by using the key equation $ed - k\left(p^2-1\right)\left(q^2-1\right) = 1$. In this paper, we consider the more general equation $eu - \left(p^2-1\right)\left(q^2-1\right)v = w$ and present a new attack that finds the prime factors p and q in the case that u, v and w satisfy some specific conditions. The attack is based on Coppersmith's technique and improves the former attacks.

Keywords: RSA variants, Coppersmith's Technique, Lattice reduction

1 Introduction

In 1978, Rivest, Shamir and Adleman [19] invented the RSA cryptosystem. Nowadays, it is the most widely used public key cryptosystem and serves for encryption and signature. The security of RSA is based on the difficulty of factoring specific large integers, called RSA moduli. An RSA modulus is in the form $N = pq$ where p and q are large prime numbers of the same size. The public exponent in RSA is an integer e satisfying $\gcd(e, (p-1)(q-1)) = 1$ while the private exponent is the integer d satisfying $ed \equiv 1 \pmod{(p-1)(q-1)}$. Since its invention, the RSA cryptosystem has been intensively studied for vulnerabilities. Many attacks on RSA exploit the RSA key equation $ed - k(p-1)(q-1) = 1$. A few attacks are based on the continued fraction algorithm such as Wiener's attack [22] and most of the attacks are based on lattice reduction techniques, introduced by Coppersmith [8] (see [3,2,10,15]). Combining both techniques,

⋆ Yanbin Pan was supported by the NNSF of China (No. 61572490 and No. 11471314), and by the National Center for Mathematics and Interdisciplinary Sciences, CAS.

Blömer and May [1] presented an attack using the generalized key equation $ex + y = k(p-1)(q-1)$ for suitably small integers x, k and y.

Many variants of RSA have been proposed for improving the security or reducing the encryption or the decryption time (see [4,21,18]). The variants of RSA in [20,13,9,7] make use of a public exponent e and a private exponent d satisfying the equation

$$ed - k\left(p^2-1\right)\left(q^2-1\right) = 1. \tag{1}$$

In [5], Bunder et al. proposed an attack on these variants by using the continued fraction algorithm approach. Setting $e = N^\beta$, they showed that one can solve the equation 1 and find the prime factors p and q if $d = N^\delta$ and $\delta < \frac{1}{2}(3-\beta)$. This was recently improved to $\delta < 2 - \sqrt{\beta}$ by Peng et al. [17] and by Zheng et al. [23] by using lattice reduction techniques and Coppersmith's method.

In this paper we consider the generalized equation

$$eu - \left(p^2-1\right)\left(q^2-1\right)v = w. \tag{2}$$

This equation can be transformed into the modular equation

$$v(p+q)^2 - (N+1)^2 v - w \equiv 0 \pmod{e}. \tag{3}$$

We set $e = N^\beta$, $u = N^\delta$, $w = N^\gamma$ and using lattice reduction techniques and Coppermith's method, we show that one can solve the equation (3) and find the prime factors p and q under the condition

$$\delta < \frac{7}{3} - \gamma - \frac{2}{3}\sqrt{1+3\beta-3\gamma} - \varepsilon, \tag{4}$$

where ε is a small positive constant. Observe that the key equation (1) is a special case of the equation (3) where $w = 1$ and $\gamma = 0$. In this special case, the condition (4) becomes

$$\delta < \frac{7}{3} - \frac{2}{3}\sqrt{1+3\beta} - \varepsilon,$$

which is slightly worst than the condition $\delta < 2 - \sqrt{\beta}$ derived by the method of Peng et al. [17]. Apart this special case, our method supersedes the method of Peng et al. since their method works only for $w = 1$ while our method works for any $w = N^\gamma$ under the condition (4).

In [6], Bunder et al. studied the equation (2) using a combination of the continued fraction algorithm and Coppersmith's method. They showed that this equation can be solved whenever

$$uv < 2N - 4\sqrt{2}N^{\frac{3}{4}} \quad \text{and} \quad |w| < (p-q)N^{\frac{1}{4}}v.$$

The first condition implies the following one

$$\delta < \frac{3-\beta}{2},$$

which is worst than our condition with $\gamma = 0$. As a consequence, our new method can be seen as an extension of the method of Bunder et al. [6].

The rest of the paper is organized as follows. In Section 2, we briefly describe the RSA variants that use exponents satisfying $ed \equiv 1 \pmod{\left(p^2-1\right)\left(q^2-1\right)}$. We also recall some facts on Coppersmith's method and lattice basis reduction. In Section 3, we present our attack. In section 4, we present a comparison with existing attacks. We conclude the paper in Section 5.

2 Preliminaries

In this section, we briefly present some variants of the RSA cryptosystem that use the key equation $ed \equiv 1 \pmod{\left(p^2-1\right)\left(q^2-1\right)}$. We also present Coppersmith's method and lattice basis reduction.

2.1 LUC cryptosystem

LUC cryptosystem, introduced by Smith and Lennon [20] in 1993 is based on Lucas functions. A related cryptosystem was propose by Castagnos [7] in 2007. Both cryptosystems use an RSA modulus $N = pq$, a public exponent e, and a private exponent satisfying a key equation $ed - k\left(p^2-1\right)\left(q^2-1\right) = 1$ which can be generalized by the equation $eu - \left(p^2-1\right)\left(q^2-1\right)v = w$.

2.2 RSA type schemes based on singular cubic curves

In 1995, Kuwakado, Koyama, and Tsuruoka [13] proposed a new cryptosystem based on the singular cubic with equation

$$y^2 = x^3 + bx^2 \mod N.$$

where $N = pq$ is an RSA modulus. In this cryptosystem, the encryption and the decryption keys satisfy an equation of the form $ed - k\left(p^2-1\right)\left(q^2-1\right) = 1$. A generalization of this equation is $eu - \left(p^2-1\right)\left(q^2-1\right)v = w$.

2.3 RSA with Gaussian primes

A variant of RSA was introduced in 2002 by Elkamchouchi, Elshenawy and Shaban [9]. It is an extension of the RSA cryptosystem to the domain of Guassian integers. Gaussian integers are complex number of the form $z = a + bi$ where a and b are integers and $i^2 = -1$. The norm of a Gaussian integer is $|a + bi| = \sqrt{a^2 + b^2}$. In the RSA variant with Gaussian integers, the modulus is $N = PQ$, a product of two Gaussian integer primes P and Q and the public and private exponents satisfy $ed - k\left(|P|^2-1\right)\left(|Q|^2-1\right) = 1$. If $P = p$ and $Q = q$ are integer primes, then $ed - k\left(p^2-1\right)\left(q^2-1\right) = 1$. This can be generalized as $eu - \left(p^2-1\right)\left(q^2-1\right)v = w$.

2.4 Coppersmith's method

In 1996, Coppersmith [8] proposed two methods related to finding small modular roots of univariate polynomials and small integer roots of bivariate polynomials. Since then, many techniques have been proposed for more variables (see [16]). Let

$$h(x,y,z)=\sum_{i,j,k} a_{i,j,k}x^i y^j z^k \in \mathbb{Z}[x,y,z],$$

be a polynomial with ω monomials. Its Euclidean norm is

$$\|h(x,y,z)\|=\sqrt{\sum_{i,j,k} a_{i,j,k}^2}.$$

The following result was proposed by Howgrave-Graham [11] to find the small modular roots of a polynomial.

Theorem 1. *Let e be a positive integer and $h(x,y,z)\in\mathbb{Z}[x,y,z]$ be a polynomial with at most ω monomials. Suppose that*

$$\|h(xX,yY,zZ)\|<\frac{e^m}{\sqrt{\omega}} \quad \textit{and} \quad h\left(x_0,y_0,z_0\right)\equiv 0 \pmod{e^m},$$

where $|x_0|<X$, $|y_0|<Y$, $|z_0|<Z$. Then $h\left(x_0,y_0,z_0\right)=0$ holds over the integers.

Coppersmith's method enables to find several polynomials that can be used in Howgrave-Graham's Theorem 1. This is possible by applying a lattice reduction technique such as the LLL algorithm [14] to a lattice with a given basis. In general, the LLL algorithm produces a reduced basis with relatively small norms such as in the following result (see [15]).

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

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

where $\det(\mathcal{L})$ is the determinant of the lattice.

We assume that if $h_1,h_2,h_3\in\mathbb{Z}[x,y,z]$ are three polynomials produced by Coppersmith's method, then the ideal generated by the polynomial equations $h_1(x,y,z)=0$, $h_2(x,y,z)=0$, $h_3(x,y,z)=0$ has dimension zero. Then, a system of polynomials sharing the root can be solved by using Gröbner basis computation or resultant techniques.

3 The attack

Theorem 3. *Let $N=pq$ be an RSA modulus and $e=N^\beta$ be a public exponent. Suppose that e satisfies the equation $eu-\left(p^2-1\right)\left(q^2-1\right)v=w$ with $u<N^\delta$ and $|w|<N^\gamma$. If*

$$\delta<\frac{7}{3}-\gamma-\frac{2}{3}\sqrt{1+3\beta-3\gamma}-\varepsilon,$$

then one can factor N in polynomial time.

Proof. Let $N = pq$ be an RSA modulus. Let e be a public exponent satisfying $eu - \left(p^2-1\right)\left(q^2-1\right)v = w$ with $|w| < eu$. Suppose that $e = N^{\beta}$, $u < N^{\delta}$ and $|w| < N^{\gamma}$. Then

$$v = \frac{eu - w}{\left(p^2-1\right)\left(q^2-1\right)} < \frac{eu + |w|}{\left(p^2-1\right)\left(q^2-1\right)} < 2N^{\beta+\delta-2},$$

where we used $\left(p^2-1\right)\left(q^2-1\right) \approx N^2$. It follows that the solution (u, v, w) of the equation $eu - \left(p^2-1\right)\left(q^2-1\right)v = w$ satisfies $u < N^{\delta}$, $v < 2N^{\beta+\delta-2}$ and $|w| < N^{\gamma}$. We set

$$X = 2N^{\beta+\delta-2}, Y = 3N^{\frac{1}{2}}, Z = N^{\gamma}. \tag{5}$$

This means that the solution (u, v, w) satisfies $u < N^{\delta}$, $v < X$ and $|w| < Z$. Moreover, since p and q are of the same size, then we have $p + q < 3N^{\frac{1}{2}} = Y$.

Transforming the equation $eu - \left(p^2-1\right)\left(q^2-1\right)v = w$, we get a modular one, namely $-v\left((N+1)^2 - (p+q)^2\right) - w \equiv 0 \pmod{e}$. This can be rewritten as

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

Consider the polynomial

$$f(x, y, z) = xy^2 + a_1 x + z,$$

where $a_1 = -(N+1)^2$. Then $(x, y, z) = (v, p+q, -w)$ is a solution of the polynomial modular equation $f(x, y, z) \equiv 0 \pmod{e}$. To find the small solutions of the equation $f(x, y, z) \equiv 0 \pmod{e}$, we apply Coppersmith's method combined with the extended strategy of Jochemsz and May [12] for finding small modular roots.

Let m and t be positive integers to be specified later. For $0 \le k \le m$, define the set

$$M_k = \bigcup_{0 \le j \le t} \{x^{i_1} y^{2i_2+j} z^{i_3} \;\Big|\; x^{i_1} y^{2i_2} z^{i_3} \quad \text{is a monomial of} \quad f^m(x, y, z) \quad \text{and} \quad \frac{x^{i_1} y^{2i_2} z^{i_3}}{(xy^2)^k} \quad \text{is a monomial of} \quad f^{m-k}\}.$$

A straightforward calculation shows that $f^m(x, y, z)$ is

$$f^m(x, y, z) = \sum_{i_1=0}^{m} \sum_{i_2=0}^{i_1} \binom{m}{i_1} \binom{i_1}{i_2} a_1^{i_1-i_2} x^{i_1} y^{2i_2} z^{m-i_1}.$$

Hence, $x^{i_1} y^{2i_2} z^{i_3}$ is a monomial of $f^m(x, y, z)$ if

$$i_1 = 0, \ldots, m, \quad i_2 = 0, \ldots, i_1, \quad i_3 = m - i_1.$$

Similarly, $x^{i_1}y^{2i_2}z^{i_3}$ is a monomial of $f^{m-k}(x,y,z)$ if

$$i_1 = 0, \ldots, m-k, \quad i_2 = 0, \ldots, i_1, \quad i_3 = m-k-i_1.$$

From this, we deduce that for $0 \le k \le m$, if $x^{i_1}y^{2i_2}z^{i_3}$ is a monomial of $f^m(x,y,z)$, then $\frac{x^{i_1}y^{2i_2}z^{i_3}}{(xy^2)^k}$ is a monomial of $f^{m-k}(x,y,z)$ if

$$i_1 = k, \ldots, m, \quad i_2 = k, \ldots, i_1, \quad i_3 = m-i_1.$$

This leads to a characterization of the set M_k. For $0 \le k \le m$, we obtain

$$x^{i_1}y^{i_2}z^{i_3} \in M_k \text{ if } i_1 = k, \ldots, m,\ i_2 = 2k, \ldots, 2i_1+t,\ i_3 = m-i_1.$$

Replacing k by $k+1$, we get

$$\begin{aligned} &x^{i_1}y^{i_2}z^{i_3} \in M_{k+1} \text{ if} \\ &i_1 = k+1, \ldots, m,\ i_2 = 2k+2, \ldots, 2i_1+t,\ i_3 = m-i_1. \end{aligned}$$

For $0 \le k \le m$, define the polynomials

$$g_{k,i_1,i_2,i_3}(x,y,z) = \frac{x^{i_1}y^{i_2}z^{i_3}}{(xy^2)^k} f(x,y,y)^k e^{m-k} \quad \text{with} \quad x^{i_1}y^{i_2}z^{i_3} \in M_k \setminus M_{k+1}.$$

Since for $t \ge 1$, we have

$$\begin{aligned} &x^{i_1}y^{i_2}z^{i_3} \in M_k \setminus M_{k+1} \\ &\text{if } i_1 = k, \ldots, m,\ i_2 = 2k, 2k+1,\ i_3 = m-i_1, \\ &\text{or } i_1 = k,\ i_2 = 2k+2, \ldots, 2i_1+t,\ i_3 = m-i_1, \end{aligned}$$

then the polynomials $g_{k,i_1,i_2,i_3}(x,y,z)$ reduce to the polynomials $G_{k,i_1,i_2,i_3}(x,y,z)$ and $H_{k,i_1,i_2,i_3}(x,y,z)$ where

$$\begin{aligned} G_{k,i_1,i_2,i_3}(x,y,z) &= x^{i_1-k}y^{i_2-2k}z^{i_3} f(x,y,z)^k e^{m-k}, \\ &\quad \text{for} \quad k = 0, \ldots m,\ i_1 = k, \ldots, m,\ i_2 = 2k, 2k+1,\ i_3 = m-i_1, \\ H_{k,i_1,i_2,i_3}(x,y,z) &= y^{i_2-2k}z^{i_3} f(x,y,z)^k e^{m-k}, \\ &\quad \text{for} \quad k = 0, \ldots m,\ i_1 = k,\ i_2 = 2k+2, \ldots, 2i_1+t,\ i_3 = m-i_1. \end{aligned}$$

Observe that for the target solution $(x,y,z) = (v, p+q, -w)$, the former polynomials satisfy

$$G_{k,i_1,i_2,i_3}(x,y,z) \equiv H_{k,i_1,i_2,i_3}(x,y,z) \equiv 0 \pmod{e^m}.$$

Let $\mathcal{L}$ denote the lattice spanned by the coefficient vectors of the polynomials $G_{k,i_1,i_2,i_3}(xX, yY, zZ)$ and $H_{k,i_1,i_2,i_3}(xX, yY, zZ)$ where X, Y and Z are positive integers to be defined later. The ordering of rows is such that any polynomial

$G_{k,i_1,i_2,i_3}(xX, yY, zZ)$ is prior to any polynomial $H_{k,i_1,i_2,i_3}(xX, yY, zZ)$. Inside each type of polynomial, the ordering of the tuples (k, i_1, i_2, i_3) follows rule

$$(k, i_1, i_2, i_3) \prec (k', i'_1, i'_2, i'_3) \text{ if } \begin{cases} k < k', \\ k = k', i_1 < i'_1 \\ k = k', i_1 = i'_1, i_2 < i'_2, \\ k = k', i_1 = i'_1, i_2 = i'_2, i_3 < i'_3. \end{cases}$$

Similarly, the monomials $x^{i_1}y^{i_1}z^{i_1}$ in the columns are ordered following the rule

$$x^{i_1}y^{i_1}z^{i_1} \prec x^{i'_1}y^{i'_2}z^{i'_3} \text{ if } \begin{cases} i_1 < i'_1 \\ i_1 = i'_1, i_2 < i'_2, \\ i_1 = i'_1, i_2 = i'_2, i_3 < i'_3. \end{cases}$$

This leads to a left triangular matrix. As an example, for $m = 2$ and $t = 3$, the matrix is presented in the following triangular table where the non-zero terms are denoted $*$.

Polynomial	z^2	yz^2	xz	xyz	x^2	x^2y	xy^2z	xy^3z	x^2y^2	x^2y^3	x^2y^4	x^2y^5	y^2z^2	y^3z^2	xy^4z	xy^5z	x^2y^6	x^2y^7
$G_{0,0,0,2}$	Z^2e^2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$G_{0,0,1,2}$	0	YZ^2e^2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$G_{0,1,0,1}$	0	0	XZe^2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$G_{0,1,1,1}$	0	0	0	$XYZe^2$	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$G_{0,2,0,0}$	0	0	0	0	X^2e^2	0	0	0	0	0	0	0	0	0	0	0	0	0
$G_{0,2,1,0}$	0	0	0	0	0	X^2Ye^2	0	0	0	0	0	0	0	0	0	0	0	0
$G_{1,1,2,1}$	*	0	*	0	0	0	ZXY^2e	0	0	0	0	0	0	0	0	0	0	0
$G_{1,1,3,1}$	0	*	0	*	0	0	0	Y^3ZXe	0	0	0	0	0	0	0	0	0	0
$G_{1,2,2,0}$	0	0	*	0	*	0	0	0	X^2Y^2e	0	0	0	0	0	0	0	0	0
$G_{1,2,3,0}$	0	0	0	*	0	*	0	0	0	X^2Y^3e	0	0	0	0	0	0	0	0
$G_{2,2,4,0}$	*	0	*	0	*	0	*	0	*	0	X^2Y^4	0	0	0	0	0	0	0
$G_{2,2,5,0}$	0	*	0	*	0	*	0	*	0	*	0	X^2Y^5	0	0	0	0	0	0
$H_{0,0,2,2}$	0	0	0	0	0	0	0	0	0	0	0	0	$Y^2Z^2e^2$	0	0	0	0	0
$H_{0,0,3,2}$	0	0	0	0	0	0	0	0	0	0	0	0	0	$Y^3Z^2e^2$	0	0	0	0
$H_{1,1,4,1}$	0	0	0	0	0	0	*	0	0	0	0	0	*	0	Y^4ZXe	0	0	0
$H_{1,1,5,1}$	0	0	0	0	0	0	0	*	0	0	0	0	0	*	0	Y^5ZXe	0	0
$H_{2,2,6,0}$	0	0	0	0	0	0	*	0	*	0	*	0	*	0	*	0	Y^6X^2	0
$H_{2,2,7,0}$	0	0	0	0	0	0	0	*	0	*	0	*	0	*	0	*	0	Y^7X^2

Since the matrix is triangular, then only the diagonal terms contribute to the determinant. On the other hand, only e, X, Y and Z contribute to the determinant and we get the form

$$\det(\mathcal{L}) = e^{n_e} X^{n_X} Y^{n_Y} Z^{n_Z}. \tag{6}$$

Using the construction of the polynomials $G_{k,i_1,i_2,i_3}(x,y,z)$ and $H_{k,i_1,i_2,i_3}(x,y,z)$, the exponents n_e, n_X, n_Y, n_Z, and the dimension ω of the lattice are as follows

$$\begin{aligned}
n_e &= \sum_{k=0}^{m}\sum_{i_1=k}^{m}\sum_{i_2=2k}^{2k+1}\sum_{i_3=m-i_1}^{m-i_1}(m-k) + \sum_{k=0}^{m}\sum_{i_1=k}^{k}\sum_{i_2=2k+2}^{2i_1+t}\sum_{i_3=m-i_1}^{m-i_1}(m-k)\\
&= \frac{1}{6}m(m+1)(4m+3t+5),\\
n_X &= \sum_{k=0}^{m}\sum_{i_1=k}^{m}\sum_{i_2=2k}^{2k+1}\sum_{i_3=m-i_1}^{m-i_1} i_1 + \sum_{k=0}^{m}\sum_{i_1=k}^{k}\sum_{i_2=2k+2}^{2i_1+t}\sum_{i_3=m-i_1}^{m-i_1} i_1\\
&= \frac{1}{6}m(m+1)(4m+3t+5),\\
n_Y &= \sum_{k=0}^{m}\sum_{i_1=k}^{m}\sum_{i_2=2k}^{2k+1}\sum_{i_3=m-i_1}^{m-i_1} i_2 + \sum_{k=0}^{m}\sum_{i_1=k}^{k}\sum_{i_2=2k+2}^{2i_1+t}\sum_{i_3=m-i_1}^{m-i_1} i_2\\
&= \frac{1}{6}(m+1)\left(4m^2+6mt+3t^2+5m+3t\right),\\
n_Z &= \sum_{k=0}^{m}\sum_{i_1=k}^{m}\sum_{i_2=2k}^{2k+1}\sum_{i_3=m-i_1}^{m-i_1} i_3 + \sum_{k=0}^{m}\sum_{i_1=k}^{k}\sum_{i_2=2k+2}^{2i_1+t}\sum_{i_3=m-i_1}^{m-i_1} i_3\\
&= \frac{1}{6}m(m+1)(2m+3t+1).\\
\omega &= \sum_{k=0}^{m}\sum_{i_1=k}^{m}\sum_{i_2=2k}^{2k+1}\sum_{i_3=m-i_1}^{m-i_1} 1 + \sum_{k=0}^{m}\sum_{i_1=k}^{k}\sum_{i_2=2k+2}^{2i_1+t}\sum_{i_3=m-i_1}^{m-i_1} 1\\
&= (m+1)(m+t+1).
\end{aligned} \tag{7}$$

For $t=\tau m$ and sufficiently large m, we can approximate the exponents n_e, n_X, n_Y, n_Z by their leading term and get

$$\begin{aligned}
n_e &= \frac{1}{6}(3\tau+4)m^3 + o(m^3),\\
n_X &= \frac{1}{6}(3\tau+4)m^3 + o(m^3),\\
n_Y &= \frac{1}{6}(3\tau^2+6\tau+4)m^3 + o(m^3),\\
n_Z &= \frac{1}{6}(3\tau+2)m^3 + o(m^3),\\
\omega &= (\tau+1)m^2 + o(m^2).
\end{aligned} \tag{8}$$

Applying the LLL algorithm to the lattice $\mathcal{L}$, we get a reduced basis where the three first vectors $h_i(Xx, Yy, Zz)$, $i = 1, 2, 3$ satisfy the conditions $\|h_1(Xx, Yy, Zz)\| \leq \|h_2(Xx, Yy, Zz)\| \leq \|h_3(Xx, Yy, Zz)\|$, and

$$\|h_3(Xx, Yy, Zz)\| \leq 2^{\frac{\omega(\omega-1)}{4(\omega-2)}} \det(\mathcal{L})^{\frac{1}{\omega-2}}.$$

For comparison, Theorem 1 can be applied if

$$\|h_3(Xx, Yy, Zz)\| < \frac{e^m}{\sqrt{\omega}}.$$

To this end, we set

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

or equivalently

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

Hence, using (6), we get

$$e^{n_e - m\omega} X^{n_X} Y^{n_Y} Z^{n_Z} < \frac{2^{-\frac{\omega(\omega-1)}{4}}}{(\sqrt{\omega})^{\omega-2}} e^{-2m}, \tag{9}$$

where the right side term is a small constant depending only on e and m. Plugging the values of n_e, n_X, n_Y, n_Z and ω from (8) as well as the values $e = N^\beta$, $X = 2N^{\beta+\delta-2}$, $Y = 3N^{\frac{1}{2}}$, $Z = N^\gamma$ in each term of (9), we get

$$\begin{aligned}
e^{n_e - m\omega} &= N^{\left(-\frac{1}{2}\tau - \frac{1}{3}\right)\beta m^3 + o(m^3)}, \\
X^{n_X} &= N^{\left(\frac{1}{2}\tau + \frac{2}{3}\right)(\beta+\delta-2)m^3 + o(m^3)} \cdot 2^{\left(\frac{1}{2}\tau + \frac{2}{3}\right)m^3 + o(m^3)} \\
&= N^{\left(\frac{1}{2}\tau + \frac{2}{3}\right)(\beta+\delta-2)m^3 + o(m^3) + \varepsilon_1}, \\
Y^{n_Y} &= N^{\frac{1}{2}\left(\frac{1}{2}\tau^2 + \tau + \frac{2}{3}\right)m^3 + o(m^3)} \cdot 3^{\left(\frac{1}{2}\tau^2 + \frac{1}{2}\tau + \frac{1}{6}\right)m^3 + o(m^3)} \\
&= N^{\frac{1}{2}\left(\frac{1}{2}\tau^2 + \tau + \frac{2}{3}\right)m^3 + o(m^3) + \varepsilon_2}, \\
Z^{n_Z} &= N^{\left(\frac{1}{2}\tau + \frac{1}{3}\right)\gamma m^3 + o(m^3)}, \\
\frac{2^{-\frac{\omega(\omega-1)}{4}}}{(\sqrt{\omega})^{\omega-2}} e^{-2m} &= N^{-2\beta m - \varepsilon_3},
\end{aligned}$$

where ε_1, ε_2 and ε_3 are small positive constants depending on m, and N. It follows that the inequality (9) can be rewritten in terms of the exponents as

$$\begin{aligned}
&\left(-\frac{1}{2}\tau - \frac{1}{3}\right)\beta + \left(\frac{1}{2}\tau + \frac{2}{3}\right)(\beta + \delta - 2) \\
&\qquad + \frac{1}{2}\left(\frac{1}{2}\tau^2 + \tau + \frac{2}{3}\right) + \left(\frac{1}{2}\tau + \frac{1}{3}\right)\gamma < \frac{-2\beta m - \varepsilon_3 - \varepsilon_1 - \varepsilon_2}{m^3}.
\end{aligned}$$

Setting $\frac{-2\beta m-\varepsilon_3-\varepsilon_3-\varepsilon_1\varepsilon_2}{m^3} = -\varepsilon_4$ and rearranging, we get

$$3\tau^2 + 6(\delta+\gamma-1)\tau + 4\beta + 8\delta + 4\gamma - 12 < -12\varepsilon_4. \tag{10}$$

The left side of (10) is optimal for $\tau_0 = 1-\delta-\gamma$. Plugging τ_0 in (10), we get

$$-3\delta^2 + (14-6\gamma)\delta - \gamma^2 + 4\beta + 10\gamma - 15 < -12\varepsilon_4.$$

This inequality is valid if

$$\delta < \frac{7}{3} - \gamma - \frac{2}{3}\sqrt{1+3\beta-3\gamma} - \varepsilon, \tag{11}$$

where ε is a small positive constant depending on m and N. This terminates the proof. □

4 Comparison with existing results

In [6], Bunder et al. combined the continued fraction algorithm and Coppersmith's method to study the equation $eu - \left(p^2-1\right)\left(q^2-1\right)v = w$. They showed that it is possible to solve it if

$$uv < 2N - 4\sqrt{2}N^{\frac{3}{4}} \quad \text{and} \quad |w| < (p-q)N^{\frac{1}{4}}v.$$

In terms of $e = N^\beta$, $u = N^\delta$ and $|w| = N^\gamma$, the first condition implies the following one

$$\delta < \frac{3-\beta}{2}.$$

For $\gamma = 0$, that is $w = 1$, the bound of Theorem 3 becomes

$$\delta < \frac{7}{3} - \frac{2}{3}\sqrt{1+3\beta} - \varepsilon.$$

Neglecting the ε term, the difference between the former bound and the bound of [6] is

$$\delta_1 = \frac{7}{3} - \frac{2}{3}\sqrt{1+3\beta} - \frac{3-\beta}{2} = \frac{5}{6} + \frac{b}{2} - \frac{2}{3}\sqrt{1+3\beta}.$$

A straightforward calculation shows that $\delta_1 \geq 0$. This shows that the bound of Theorem 3 is better than the bound of [6].

In [17], Peng et al. proposed a lattice based method to solve the equation $ed - k\left(p^2-1\right)\left(q^2-1\right) = 1$ under the condition $\delta < 2-\sqrt{\beta}$ and $\beta > 1$. This is a special case of the general equation $eu - \left(p^2-1\right)\left(q^2-1\right)v = w$. In this special case, we have $w = N^\gamma = 1$ and $\gamma = 0$, and the difference between the bound of Theorem 3 and the bound of [17] is

$$\delta_2 = 2 - \sqrt{\beta} - \left(\frac{7}{3} - \frac{2}{3}\sqrt{1+3\beta}\right) = \frac{2}{3}\sqrt{1+3\beta} - \frac{1}{3} - \sqrt{\beta}.$$

Again, a straightforward calculation shows that $\delta_2 \geq 0$. This means that the condition of Theorem 3 is not better than Peng al.'s bound. Nevertheless, our method is more general and can solve a variety of equations with $w \neq 1$.

5 Conclusion

In this paper, we have studied the equation $eu-\left(p^2-1\right)\left(q^2-1\right)v=w$ which is a generalization of the equation $ed-k\left(p^2-1\right)\left(q^2-1\right)=1$. The latter equation is the key equation of some variants of the RSA cryptosystem with modulus $N=pq$, public exponent e and private key d. We have showed that, under some conditions, it is possible to solve the equation $eu-\left(p^2-1\right)\left(q^2-1\right)v=w$ and break the cryptosystem. The attack is based on applying Coppersmith's method to a multivariate modular equation and can be seen as an extension of former attacks on such cryptosystems.

References

1. Blömer, J., May, A.: A generalized Wiener attack on RSA. In Public Key Cryptography - PKC 2004, volume 2947 of Lecture Notes in Computer Science, Springer-Verlag, pp. 1–13 (2004)
2. 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)
3. Boneh, D.: Twenty years of attacks on the RSA cryptosystem, Notices Amer. Math. Soc. 46 (2), pp. 203–213, (1999)
4. Boneh, D., Shacham, H.: Fast Variants of RSA, CryptoBytes, Vol. 5, No. 1, pp. 1–9, (2002)
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, Part II. LNCS, vol. 9723, pp. 258–268. Springer (2016)
6. Bunder, M., Nitaj, A., Susilo, W., Tonien, J.: A generalized attack on RSA type cryptosystems, Theoretical Computer Science Volume 704, 15 December 2017, pp. 74–81 (2017)
7. Castagnos, G.: An efficient probabilistic public-key cryptosystem over quadratic field quotients, 2007, Finite Fields and Their Applications, 07/2007, 13(3-13), p. 563-576 (2007)
8. Coppersmith, D.: Small solutions to polynomial equations, and low exponent RSA vulnerabilities. Journal of Cryptology, 10(4), pp. 233–260 (1997)
9. 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, pp. 91–95 (2002)
10. Hinek, M.J.: Cryptanalysis of RSA and its Variants. Chapman & Hall/CRC Cryptography and Network Security. CRC Press, Boca Raton, FL, (2010)
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. 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)
13. Kuwakado, H., Koyama, K., Tsuruoka, Y.: 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 (1995)

14. Lenstra, A.K., Lenstra, H.W., Lovász, L.: Factoring polynomials with rational coefficients, Mathematische Annalen, Vol. 261, pp. 513–534, (1982)
15. May, A.: New RSA Vulnerabilities Using Lattice Reduction Methods. PhD thesis, University of Paderborn (2003) available at `http://www.cits.rub.de/imperia/md/content/may/paper/bp.ps`
16. May A.: Using LLL-reduction for solving RSA and factorization problems: a survey. In: LLL+25 Conference in Honour of the 25th Birthday of the LLL Algorithm. Springer, Berlin, Heidelberg (2007)
17. 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. vol. 10143, pp. 140–149. Springer (2017)
18. Quisquater, J. J., Couvreur, C.: Fast Decipherment Algorithm for RSA Public-Key Cryptosystem. Electronics Letters, 18(21), pp. 905–907 (1982)
19. 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)
20. Smith, P.J., Lennon, G.J.J.: LUC: a new publickey cryptosystem, Ninth IFIP Symposium on Computer Science Security, Elseviver Science Publishers, 1993, pp. 103–117 (1993)
21. Takagi, T.: Fast RSA-type cryptosystem modulo $p^k q$. In Advances in Cryptology–Crypto'98, pp. 318–326. Springer, (1998)
22. Wiener, M.: Cryptanalysis of short RSA secret exponents, IEEE Transactions on Information Theory, Vol. 36, pp. 553–558 (1990)
23. Zheng, M., Kunihiro, N., Hu, H.: Cryptanalysis of RSA variants with modified Euler quotient, A. Joux et al. (Eds.): AFRICACRYPT 2018, LNCS 10831, pp. 266–281 (2018)