A generalized attack on RSA type cryptosystems

Martin Bunder, Abderrahmane Nitaj, Willy Susilo, Joseph Tonien

A generalized attack on RSA type cryptosystems

Martin Bunder*, Abderrahmane Nitaj†, Willy Susilo‡, Joseph Tonien§

Abstract

Let $N = pq$ be an RSA modulus with unknown factorization. Some variants of the RSA cryptosystem, such as LUC, RSA with Gaussian primes and RSA type schemes based on singular elliptic curves use a public key e and a private key d satisfying an equation of the form $ed - k\left(p^2-1\right)\left(q^2-1\right) = 1$. In this paper, we consider the general equation $ex - \left(p^2-1\right)\left(q^2-1\right)y = z$ and present a new attack that finds the prime factors p and q in the case that x, y and z satisfy a specific condition. The attack combines the continued fraction algorithm and Coppersmith's technique and can be seen as a generalization of the attacks of Wiener and Blömer-May on RSA.

1 Introduction

In 1978, Rivest, Shamir and Adleman [20] proposed RSA, the first and widely most used public key cryptosystem. The security of RSA is mainly based on the hardness of factoring large composite integers, nevertheless, RSA has been extensively studied for vulnerabilities by various non factorization attacks. The public parameters in RSA are the RSA modulus $N = pq$ which is the product of two large primes of the same bit-size and a public exponent e satisfying $\gcd(e, (p-1)(q-1)) = 1$. The correspondent private exponent is the integer $d < N$ satisfying $ed \equiv 1 \pmod{(p-1)(q-1)}$ which can be rewritten as a key equation $ed - k(p-1)(q-1) = 1$. In RSA, the encryption and decryption time are proportional to the bit-length of the public and the private exponents. To reduce encryption or decryption time, one may be tempted to use small public exponents or private exponents. While a few attacks on RSA with small public exponent e have been launched (see [10]), many attacks on RSA with

*School of Mathematics and Applied Statistics, University of Wollongong, Australia, martin_bunder@uow.edu.au

†Laboratoire de Mathématiques Nicolas Oresme, Université de Caen Normandie, France, abderrahmane.nitaj@unicaen.fr

‡School of Computing and Information Technology, University of Wollongong, Australia, willy_susilo@uow.edu.au

§School of Computing and Information Technology, University of Wollongong, Australia, joseph_tonien@uow.edu.au@uow.edu.au

small or special private exponent d exploit the algebraic properties of the key equation. In 1990, Wiener [24] presented an attack on RSA that solves the key equation and factors N if d is sufficiently small, namely $d < \frac{1}{3}N^{0.25}$. Wiener's attack consists on finding $\frac{k}{d}$ among the convergents of the continued fraction expansion of $\frac{e}{N}$ and then using $\frac{k}{d}$ to factor N. Wiener's attack on RSA has been extended in many ways using lattice reduction and Coppersmith's method [7] (see [2], [11], [17]). In 1997, Boneh and Durfee [4] used lattice reduction and Coppersmith's method to improve the bound to $d < N^{0.292}$. In 2004, Blömer and May studied the variant equation $ex + y \equiv 0 \pmod{(p-1)(q-1)}$ and showed that the RSA modulus can be factored if the unknown parameters satisfy $x < \frac{1}{3}N^{0.25}$ and $|y| \leq cN^{-\frac{3}{4}}ex$ for some constant $c \leq 1$.

In order to improve the implementation of the RSA cryptosystem, many schemes have been presented giving rise to RSA type cryptosystems [3]. One way to extend RSA is to consider a prime-power modulus of the form $N = p^r q$ with $r \geq 2$ (see [22]) or a multi-prime modulus of the form $N = p_1 p_2 \dots p_r$. Another way to extend RSA is to consider the modulus $N = pq$ and the exponent e with specific arithmetical operations such as elliptic curves [14] [13], Gaussian domains [8] and quadratic fields [19].

In 1995, Kuwakado, Koyama and Tsuruoka [14] presented a scheme based on using an RSA modulus $N = pq$ and a singular cubic equation with equation $y^2 = x^3 + bx^2 \mod N$ where a message $M = (m_x, m_y)$ is represented as a point on the singular cubic equation. In this system, the public exponent e and the private exponent d satisfy an equation of the form $ed - k\left(p^2-1\right)\left(q^2-1\right)$.

In 2002, Elkamchouchi, Elshenawy and Shaban [8] adapted RSA to the Gaussian domain by using a modulus of the form $N = PQ$ where P and Q are two Gaussian primes. The public exponent e and the private exponent d satisfy $ed \equiv 1 \pmod{(|P|-1)(|Q|-1)}$. When $P = p$ and $Q = q$ are integer prime numbers, the equation becomes $ed \equiv 1 \pmod{\left(p^2-1\right)\left(q^2-1\right)} = 1$.

In 1993, Smith and Lennon proposed LUC [21], where the public exponent e and the private exponent d are such that $ed \equiv 1 \pmod{\left(p^2-1\right)\left(q^2-1\right)}$.

In 2007, in connection with LUC, Castagnos [6] proposed a scheme that uses an RSA modulus $N = pq$ and a public exponent e. The two public parameters N and e are such that $\gcd\left(e, \left(p^2-1\right)\left(q^2-1\right)\right) = 1$ which implies the existence of two positive integers d and k satisfying the equation $ed - k\left(p^2-1\right)\left(q^2-1\right) = 1$.

The former four variants of RSA use a modulus $N = pq$ and a public exponent e satisfying an equation of the form $ed - k\left(p^2-1\right)\left(q^2-1\right) = 1$. In [5], an attack is presented that solves the former equation when d satisfies $d < \sqrt{\frac{2N^3 - 18N^2}{e}}$. The attack, which is related to Wiener's attack on RSA, is based on applying the continued fraction algorithm to find $\frac{k}{d}$ among the covergents of the continued fraction expansion of $\frac{e}{N^2 - \frac{9}{4}N + 1}$. In this paper, we consider an extension of this attack by studying the more general equation $ex - \left(p^2-1\right)\left(q^2-1\right)y = z$ where the unknown parameters x, y, z satisfy

$$xy < 2N - 4\sqrt{2}N^{\frac{3}{4}} \quad \text{and} \quad |z| < (p-q)N^{\frac{1}{4}}y.$$

The new attack uses the convergents of the continued fraction expansion of $\frac{e}{N^2+1-\frac{9}{4}N}$ to find $\frac{y}{x}$ and then applies Coppersmith's technique [7] to find p and q.

The remainder of the paper is organized as follows. In section 2, we recall some RSA type schemes that are based on a modulus of the form $N = pq$ with a public exponent satisfying $\gcd\left(e, \left(p^2-1\right)\left(q^2-1\right)\right) = 1$. In Section 3, we briefly review some basic results used in the paper, including continued fractions and Coppersmith's technique. In Section 4, we present some lemmas that will be used in the paper. In Section 5, we present our new method. In Section 6, we give a numerical example. We conclude the paper in Section 7.

2 Variant RSA schemes

Let $N = pq$ be an RSA modulus and e a public integer. In this section, we briefly describe three schemes that are variants of the RSA cryptosystem with a modulus $N = pq$ and with a public key e and a private key d satisfying $ed - k\left(p^2-1\right)\left(q^2-1\right) = 1$. As this equation does not depend on the underlying variant schemes, we then generalize it to the equation $ex - \left(p^2-1\right)\left(q^2-1\right)y = z$ which is the main focus of this paper.

2.1 LUC cryptosystem

In 1993, Smith and Lennon [21] proposed a variant of the RSA cryptosystem, called LUC, based on a Lucas functions. In LUC, the modulus is a RSA modulus $N = pq$ and the public exponent e is a positive integer satisfying $\gcd\left(e, \left(p^2-1\right)\left(q^2-1\right)\right)$ which can be rewritten as an equation $ed - k\left(p^2-1\right)\left(q^2-1\right) = 1$. A more general equation is $ex - \left(p^2-1\right)\left(q^2-1\right)y = z$ with the unknown parameters x, y and z.

2.2 Castagnos cryptosystem

In 2007, Castagnos [6] proposed a cryptosystem related to LUC and RSA where the modulus $N = pq$ and the public exponent e satisfy the condition $\gcd\left(e, \left(p^2-1\right)\left(q^2-1\right)\right)$ or equivalently $ed - k\left(p^2-1\right)\left(q^2-1\right) = 1$ for some integers d and k. This equation can be extended to a more general one, namely $ex - \left(p^2-1\right)\left(q^2-1\right)y = z$.

2.3 RSA with Gaussian primes

In 2002, Elkamchouchi, Elshenawy and Shaban [8] proposed a generalization of the RSA cryptosystem to the domain of Guassian integers. A Gaussian integer

is a complexe number $z = a + bi$ where a and b are both integers. A Gaussian prime is a Gaussian integer that is not the product of two non-unit Gaussian integers, the only units being ± 1 and $\pm i$. The Gaussian primes are of one of the following forms

- $P = \pm 1 \pm i$,
- $P = a$ where $|a|$ is an integer prime with $|a| \equiv 3 \pmod 4$,
- $P = ai$ where $|a|$ is an integer prime with $|a| \equiv 3 \pmod 4$,
- $P = a + ib$ where $|P| = a^2 + b^2 \equiv 1 \pmod 4$ is an integer prime.

In the RSA variant with Gaussian integers, the modulus is $N = PQ$, a product of two Gaussian integer primes P and Q. The Euler totient function is $\phi(N) = (|P| - 1)(|Q| - 1)$ and the public exponent e is a positive integer satisfying $\gcd(e, \phi(N)) = 1$. When $P = p$ and $Q = q$ are integer primes, then $\phi(N) = \left(p^2 - 1\right)\left(q^2 - 1\right)$ and the public exponent satisfies the key equation $ed - k\left(p^2 - 1\right)\left(q^2 - 1\right) = 1$ which can be extended to a more general equation $ex - \left(p^2 - 1\right)\left(q^2 - 1\right) y = z$.

2.4 RSA type schemes based on singular cubic curves

Let $N = pq$ be an RSA modulus. For an integer $b \in \mathbb{Z}/n\mathbb{Z}$, consider the cubic curve $E_N(b)$ defined over the ring $\mathbb{Z}/n\mathbb{Z}$ given by the Weierstrass equation

$$E_N(b) : y^2 = x^3 + bx^2 \mod N.$$

In 1995, Kuwakado, Koyama, and Tsuruoka [14] proposed a new cryptosystem based the elliptic curve $E_N(b)$. The encryption key is a positive integer satisfying $\gcd\left(e, \left(p^2 - 1\right)\left(q^2 - 1\right)\right)$ and the decryption key is the integer d satisfying $ed \equiv 1 \pmod{\left(p^2 - 1\right)\left(q^2 - 1\right)}$, or equivalently $ed - k\left(p^2 - 1\right)\left(q^2 - 1\right) = 1$. The encryption and the decryption procedures use operations on the singular cubic curve $E_N(b)$. Using the continued fraction algorithm, it is possible to attack the scheme using the key equation $ed - k\left(p^2 - 1\right)\left(q^2 - 1\right) = 1$. A more general attack on the scheme can be launched by using the equation $ex - \left(p^2 - 1\right)\left(q^2 - 1\right) y = z$ and by combining the continued fraction algorithm and Coppersmith's method.

3 Preliminaries

In this section, we present the mathematical preliminaries.

3.1 Continued fractions

Let x be a real number. Define the sets $(x_0, x_1, \ldots)$ and $[a_0, a_1, \ldots]$ by $x_0 = x$ and by the recurrences

$$a_i = \lfloor x_i \rfloor, \quad x_{i+1} = \frac{1}{x_i - a_i}, \quad i = 0, 1, \ldots .$$

The set $[a_0, a_1, \cdots]$ is the continued fraction expansion of x and satisfies

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}.$$

The convergents of x are the rational numbers $\frac{p_n}{q_n}$, $n = 0, 1, \ldots$ satisfying

$$\frac{p_n}{q_n} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}.$$

Continued fractions have numerous properties and applications in cryptography. The following useful result characterizes the approximations to a real number x (see Theorem 184 of [9]).

Theorem 1 (Legendre) *If a, b be positive integers and*

$$0 < \left| x - \frac{a}{b} \right| < \frac{1}{2b^2}$$

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

Note that when $x = \frac{r}{s}$ is a rational number, then the list of the convergents of the continued fraction expansion of $\frac{r}{s}$ can be done in polynomial time in $\log(\max(a, b))$.

3.2 Coppersmith's method

In 1997, Coppersmith [7] introduced an algorithm to find small solutions of univariate modular polynomial equations and another algorithm to find small roots of bivariate polynomial equations. Since then, Coppersmith's method has been applied in various applications in cryptography, mainly to attack the RSA cryptosystem. A typical example is the following result.

Theorem 2 *Let $N = pq$ be the product of two unknown primes such that $q < p < 2q$. Given an approximation $\tilde{p}$ of p with an additive error term at most $N^{\frac{1}{4}}$, one can find p and q in polynomial time in* $\log(N)$.

As a consequence of Coppersmith's Theorem, one can show that if $N = pq$ with $|p - q| < N^{\frac{1}{4}}$, then N can be factored (see [18]). Thus, throughout this paper, we will consider that the prime difference $p - q$ satisfies $|p - q| > N^{\frac{1}{4}}$.

4 Useful Lemmas

One of the main RSA standard recommendations for safe parameters is to choose the prime factors factors p, q of the same bit-size. More precisely, p and q should satisfy $1 < \frac{p}{q} < 2$ or equivalently $q < p < 2q$. Under this assumption, one can find intervals for p, q, $p - q$, $p + q$ and $p^2 + q^2$ in terms of N. We begin by the following results (see [18]).

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

$$\frac{\sqrt{2}}{2}\sqrt{N} < q < \sqrt{N} < p < \sqrt{2}\sqrt{N} \quad \textit{and} \quad 0 < p - q < \frac{\sqrt{2}}{2}\sqrt{N}.$$

We will need the following result.

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

$$2\sqrt{N} < p + q < \frac{3\sqrt{2}}{2}\sqrt{N} \quad \textit{and} \quad 2N < p^2 + q^2 < \frac{5}{2}N.$$

Proof. Assume that $N = pq$ with $q < p < 2q$. Then $1 < \frac{p}{q} < 2$. The function $f(x) = x + \frac{1}{x}$ is increasing on $[1, +\infty)$. Hence, $f(1) < f(\frac{p}{q}) < f(2)$, that is

$$2 < \frac{p}{q} + \frac{q}{p} < \frac{5}{2}.$$

Multiplying by $N = pq$, we get

$$2N < p^2 + q^2 < \frac{5}{2}N.$$

Similarly, since $1 < \sqrt{\frac{p}{q}} < \sqrt{2}$, then $f(1) < f(\sqrt{\frac{p}{q}}) < f(\sqrt{2})$, or equivalently

$$2 < \sqrt{\frac{p}{q}} + \sqrt{\frac{p}{q}} < \frac{3\sqrt{2}}{2}.$$

Hence, multiplying by $\sqrt{N} = \sqrt{pq}$, we get

$$2\sqrt{N} < p + q < \frac{3\sqrt{2}}{2}\sqrt{N}.$$

This terminates the proof. ■

5 The New Attack

In this section, we present our new attack to solve the equation $ex-\left(p^2-1\right)\left(q^2-1\right)y = z$ when x, y and z are suitably small. The new method combines two techniques, the continued fraction algorithm and Coppersmith's method.

Theorem 3 *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let e be a public exponent satisfying an equation $ex-\left(p^2-1\right)\left(q^2-1\right)y = z$ with coprime positive integers x and y. If*

$$xy < 2N - 4\sqrt{2}N^{\frac{3}{4}} \quad \textit{and} \quad |z| < (p-q)N^{\frac{1}{4}}y,$$

then one can find p and q in polynomial time in $\log(N)$.

Proof. Suppose that $N = pq$ with $q < p < 2q$ and that a public exponent e satisfies the equation

$$ex - \left(p^2-1\right)\left(q^2-1\right)y = z, \tag{1}$$

with $x > 0$, $y > 0$ and $\gcd(x, y) = 1$. Then

$$\begin{aligned} ex - \left(N^2 + 1 - \frac{9}{4}N\right)y &= ex - (p^2-1)(q^2-1)y - \left(p^2+q^2-\frac{9}{4}N\right)y \\ &= z - \left(p^2+q^2-\frac{9}{4}N\right)y. \end{aligned} \tag{2}$$

From this we deduce

$$\left|\frac{e}{N^2+1-\frac{9}{4}N} - \frac{y}{x}\right| \leq \frac{|z|}{x\left(N^2+1-\frac{9}{4}N\right)} + \frac{\left|p^2+q^2-\frac{9}{4}N\right|y}{x\left(N^2+1-\frac{9}{4}N\right)}. \tag{3}$$

Using Lemma 2, we get that $\left|p^2+q^2-\frac{9}{4}N\right| < \frac{1}{4}N$. Suppose in addition that $|z| < |p-q|N^{\frac{1}{4}}y$. Then, using Lemma 1, we get

$$|z| < |p-q|N^{\frac{1}{4}}y < \frac{\sqrt{2}}{2}\sqrt{N}\cdot N^{\frac{1}{4}}y = \frac{\sqrt{2}}{2}N^{\frac{3}{4}}y. \tag{4}$$

Hence (3) leads to

$$\begin{aligned} \left|\frac{e}{N^2+1-\frac{9}{4}N} - \frac{y}{x}\right| &< \frac{\frac{\sqrt{2}}{2}N^{\frac{3}{4}}}{N^2+1-\frac{9}{4}N}\cdot\frac{y}{x} + \frac{\frac{1}{4}N}{N^2+1-\frac{9}{4}N}\cdot\frac{y}{x} \\ &= \frac{N+2\sqrt{2}N^{\frac{3}{4}}}{4N^2+4-9N}\cdot\frac{y}{x}. \end{aligned} \tag{5}$$

Now, suppose that $xy < 2N - 4\sqrt{2}N^{\frac{3}{4}}$. A straightforward calculation shows that

$$2N - 4\sqrt{2}N^{\frac{3}{4}} < \frac{4N^2+4-9N}{2N+4\sqrt{2}N^{\frac{3}{4}}}.$$

Then $xy < \frac{4N^2+4-9N}{2\left(N+2\sqrt{2}N^{\frac{3}{4}}\right)}$ and $\frac{N+2\sqrt{2}N^{\frac{3}{4}}}{4N^2+4-9N} < \frac{1}{2xy}$. Using this in (5), we get

$$\left|\frac{e}{N^2+1-\frac{9}{4}N} - \frac{y}{x}\right| < \frac{N+2\sqrt{2}N^{\frac{3}{4}}}{4N^2+4-9N} \cdot \frac{y}{x} < \frac{1}{2xy} \cdot \frac{y}{x} = \frac{1}{2x^2}.$$

Hence, if this condition is fulfilled, then one can find $\frac{y}{x}$ amongst the convergents of the continued fraction expansion of $\frac{e}{N^2+1-\frac{9}{4}N}$ as stated in Theorem 1. Moreover, since $\gcd(x, y) = 1$, the values of x and y are the denominator and numerator of the convergent. Plugging x and y in (1), we get

$$p^2 + q^2 = N^2 + 1 - \frac{ex}{y} + \frac{z}{y}. \tag{6}$$

Adding $2N$ to both sides of (6), we get

$$(p+q)^2 = (N+1)^2 - \frac{ex}{y} + \frac{z}{y}. \tag{7}$$

Similarly, subtracting $2N$ to both sides of (6), we get

$$(p-q)^2 = (N-1)^2 - \frac{ex}{y} + \frac{z}{y}. \tag{8}$$

Observe that (7) can be transformed into

$$\left|p+q-\sqrt{\left|(N+1)^2 - \frac{ex}{y}\right|}\right| \times \left|p+q+\sqrt{\left|(N+1)^2 - \frac{ex}{y}\right|}\right| = \frac{|z|}{y},$$

from which we deduce

$$\left|p+q-\sqrt{\left|(N+1)^2 - \frac{ex}{y}\right|}\right| = \frac{|z|}{\left|p+q+\sqrt{\left|(N+1)^2 - \frac{ex}{y}\right|}\right| y} < \frac{|z|}{(p+q)y}.$$

By (4) we have $|z| < \frac{\sqrt{2}}{2}N^{\frac{3}{4}}y$ and by Lemma 2 we have $p+q > 2\sqrt{N}$. Then

$$\left|p+q-\sqrt{\left|(N+1)^2 - \frac{ex}{y}\right|}\right| < \frac{\frac{\sqrt{2}}{2}N^{\frac{3}{4}}}{2\sqrt{N}} = \frac{\sqrt{2}}{4}N^{\frac{1}{4}} < N^{\frac{1}{4}}.$$

This means that $\sqrt{\left|(N+1)^2 - \frac{ex}{y}\right|}$ is an approximation of $p+q$ with error term less than $N^{\frac{1}{4}}$. In a similar way, using (8), we get

$$\left|p-q-\sqrt{\left|(N-1)^2 - \frac{ex}{y}\right|}\right| \times \left|p-q+\sqrt{\left|(N-1)^2 - \frac{ex}{y}\right|}\right| = \frac{|z|}{y},$$

which leads to

$$\left|p-q-\sqrt{\left|(N-1)^2-\frac{ex}{y}\right|}\right| = \frac{|z|}{\left|p-q+\sqrt{\left|(N+1)^2-\frac{ex}{y}\right|}\right| y} < \frac{|z|}{(p-q)y}.$$

Using the assumption $|z| < (p-q)N^{\frac{1}{4}}y$, we get

$$\left|p-q-\sqrt{\left|(N-1)^2-\frac{ex}{y}\right|}\right| < \frac{(p-q)N^{\frac{1}{4}}y}{(p-q)y} = N^{\frac{1}{4}}.$$

Hence, $\sqrt{\left|(N-1)^2-\frac{ex}{y}\right|}$ is an approximation of $p-q$ with an error term less than $N^{\frac{1}{4}}$. Combing the approximations of $p+q$ and $p-q$, we get

$$\begin{aligned}
&\left|p-\frac{1}{2}\left(\sqrt{\left|(N+1)^2-\frac{ex}{y}\right|}+\sqrt{\left|(N-1)^2-\frac{ex}{y}\right|}\right)\right| \\
&< \frac{1}{2}\left|p+q-\sqrt{\left|(N+1)^2-\frac{ex}{y}\right|}\right| + \frac{1}{2}\left|p-q-\sqrt{\left|(N-1)^2-\frac{ex}{y}\right|}\right| \\
&< \frac{1}{2}N^{\frac{1}{4}} + \frac{1}{2}N^{\frac{1}{4}} \\
&= N^{\frac{1}{4}}.
\end{aligned}$$

This gives an approximation of p with an error term of at most $N^{\frac{1}{4}}$. Hence, using Coppersmith's Theorem 2, one can find p which leads to $q = \frac{N}{p}$. Since every step in the proof can be done in polynomial time in $\log(N)$, then the factorization of N can be obtained in polynomial time in $\log(N)$. ■

We note that, when $\gcd\left(ex, \left(p^2-1\right)\left(q^2-1\right)\right) = 1$, the diophantine equation $ex - \left(p^2-1\right)\left(q^2-1\right)y = z$ is equivalent to the modular equation $ex \equiv z \pmod{\left(p^2-1\right)\left(q^2-1\right)}$. Moreover, the exponent e satisfies

$$e \equiv \frac{z}{x} \pmod{\left(p^2-1\right)\left(q^2-1\right)}.$$

Hence, Theorem 3 implies that one can factor $N = pq$ for such exponents e in the case where $xy < 2N - 4\sqrt{2}N^{\frac{3}{4}}$ and $|z| < (p-q)N^{\frac{1}{4}}y$.

We now consider an application of Theorem 3 to the private exponent d. We recall that d satisfies $ed \equiv 1 \pmod{\left(p^2-1\right)\left(q^2-1\right)}$. Instead of this modular equation, we consider the key equation

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

Corollary 1 *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let $e < \left(p^2-1\right)\left(q^2-1\right)$ be a public exponent. If the private exponent d satisfies*

$$d < \sqrt{2N - 4\sqrt{2}N^{\frac{3}{4}}},$$

then one can find p and q in polynomial time in $\log(N)$.

Proof. Suppose that $q < p < 2q$ and $e < \left(p^2-1\right)\left(q^2-1\right)$. Since the private exponent d satisfies $ed - k\left(p^2-1\right)\left(q^2-1\right) = 1$ for a positive integer k, then

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

Then $dk < d^2$. Now, assume that $d^2 < 2N - 4\sqrt{2}N^{\frac{3}{4}}$. Then, $dk < 2N - 4\sqrt{2}N^{\frac{3}{4}}$ and d, k fulfill the conditions of Theorem 3 wich leads to the factorization of N in polynomial time in $\log(N)$. ■

6 A Numerical Example

In this section we give a detailed numerical example to explain our method as developed in Theorem 3. Let us consider the small public key

$$\begin{aligned} N &= 204645825996541, \\ e &= 26384989321053458213237. \end{aligned}$$

It is obvious that equation $ex - \left(p^2-1\right)\left(q^2-1\right)y = z$ has infinitely many solutions (x, y, z) with positive integers x, y and non zero integer z. Our aim is to find the solution that satisfies the conditions of Theorem 3, if any. Define We want to find $\frac{y}{x}$ among the convergents of the continued fraction expansion of $\frac{e}{N^2+1-\frac{9}{4}N}$. Following the technique of Theorem 3, for each convergent $\frac{y}{x}$ of $\frac{e}{N^2+1-\frac{9}{4}N}$ with $xy < 2N - 4\sqrt{2}N^{\frac{3}{4}} \approx 4.089 \times 10^{14}$, we compute an approximation $\tilde{p}$ of p using

$$\tilde{p} = \frac{1}{2}\left(\sqrt{\left|(N+1)^2 - \frac{ex}{y}\right|} + \sqrt{\left|(N-1)^2 - \frac{ex}{y}\right|}\right),$$

and apply Coppersmith's Theorem 2 with $\tilde{p}$. Using the convergent

$$\frac{y}{x} = \frac{16052}{25478743725},$$

we get $\tilde{p} \approx 19126518$. Coppersmith's Theorem outputs the prime factor $p = 19126831$ from which we deduce the second prime factor $q = \frac{N}{p} = 10699411$. This completes the factorization of N.

7 Conclusion

In this paper, we considered some variants of the RSA cryptosystem that use a modulus $N = pq$ and a public exponent d satisfying $\gcd\left(e, \left(p^2-1\right)\left(q^2-1\right)\right)$. We studied the general equation $ex - \left(p^2-1\right)\left(q^2-1\right)y = z$ and combined the continued fraction algorithm with Coppersmith's technique to find x and y and then to factor the RSA modulus N. Our new method can considered as an extension to some RSA type schemes of two former methods that work for RSA, namely Wiener's attack and Blömer-May attack.

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, 1–13. Springer-Verlag (2004)

[2] Boneh, D.: Twenty years of attacks on the RSA cryptosystem, Notices Amer. Math. Soc. 46 (2), pp. 203–213, (1999)

[3] Boneh, D., Shacham, H.: Fast Variants of RSA, CryptoBytes, Vol. 5, No. 1, pp. 1–9, (2002)

[4] 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)

[5] Bunder, M., Nitaj, A., Susilo, W., Tonien, J.: A new attack on three variants of the RSA cryptosystem, Information Security and Privacy, 21st Australasian Conference, ACISP 2016, Melbourne, VIC, Australia, July 4-6, 2016, Proceedings, Volume 9723 of the series Lecture Notes in Computer Science pp. 258-268 (2016)

[6] 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. `http://www.math.u-bordeaux1.fr/~gcastagn/publi/crypto_quad.pdf`

[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] Hardy, G.H., Wright, E.M.: An Introduction to the Theory of Numbers, Oxford University Press, London, 1965.

[10] Hastad, J., Solving simultaneous modular equations of low degree, SIAM J. of Computing, Vol. 17, p.336-341, 1988.

[11] Hinek, M.J.: Cryptanalysis of RSA and its variants. Chapman & Hall/CRC Cryptography and Network Security. CRC Press, Boca Raton, FL, (2010)

[12] Konrad, K.: The Gaussian integers, preprint, available at `http://www.math.uconn.edu/~kconrad/blurbs/ugradnumthy/Zinotes.pdf`.

[13] K. Koyama, U.M. Maurer, T. Okamoto, S.A. Vanstone, New public-key schemes based on elliptic curves over the ring Zn, Advances in Cryptology – Proc. Crypto'91, Lecture Notes in Computer Science, vol. 576, Springer, Berlin, 1992, pp. 252–266.

[14] 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.

[15] Lenstra, A.K., Lenstra, H.W., Lovász, L.: Factoring polynomials with rational coefficients, Mathematische Annalen, Vol. 261, pp. 513–534, (1982)

[16] Ibrahimpašić, B.: A cryptanalytic attack on the LUC cryptosystem using continued fractions, Math. Commun., Vol. 14, No. 1, pp. 103-118 (2009)

[17] 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`

[18] Nitaj, A.: Another generalization of Wiener's attack on RSA, in Vaudenay, S. (ed.) Africacrypt 2008. Lecture Notes in Computer Science, Springer-Verlag Vol. 5023, pp. 174–190 (2008)

[19] Paulus, S., Takagi, T.: A new public key cryptosystem over quadratic orders with quadratic decryption time. J. Cryptology 13, 263–272 (2000)

[20] 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)

[21] Smith, P.J., Lennon, G.J.J.: LUC: a new public–key cryptosystem, Ninth IFIP Symposium on Computer Science Security, Elseviver Science Publishers, 1993, 103–117.

[22] Takagi, T.: Fast RSA-type cryptosystem modulo $p^k q$. In Advances in Cryptology–Crypto'98, pp. 318–326. Springer, (1998)

[23] de Weger, B.: Cryptanalysis of RSA with small prime difference, Applicable Algebra in Engineering, Communication and Computing,Vol. 13(1), pp. 17–28 (2002)

[24] Wiener, M.: Cryptanalysis of short RSA secret exponents, IEEE Transactions on Information Theory, Vol. 36, pp. 553–558 (1990)