Cryptanalysis of RSA-type cryptosystems based on Lucas sequences, Gaussian integers and elliptic curves

Martin Bunder*[1], Abderrahmane Nitaj†[2], Willy Susilo‡[3], and Joseph Tonien§[3]

[1]School of Mathematics and Applied Statistics, University of Wollongong, Australia
[2]Département de Mathématiques, Université de Caen, France
[3]Centre for Computer and Information Security Research, School of Computing and Information Technology, University of Wollongong, Australia

Abstract

In this paper, we apply the continued fraction method to launch an attack on the three RSA-type cryptosystems when the private exponent d is sufficiently small. The first cryptosystem, proposed by Kuwakado, Koyama and Tsuruoka in 1995, is a scheme based on singular cubic curves $y^2 = x^3 + bx^2 \pmod N$ where $N = pq$ is an RSA modulus. The second cryptosystem, proposed by Elkamchouchi, Elshenawy and Shaban in 2002, is an extension of the RSA scheme to the field of Gaussian integers using a modulus $N = PQ$ where P and Q are Gaussian primes such that $p = |P|$ and $q = |Q|$ are ordinary primes. The third cryptosystem, proposed by Castagnos in 2007, is a scheme over quadratic field quotients with an RSA modulus $N = pq$ based on Lucas sequences. In the three cryptosystems, the public exponent e is an integer satisfying the key equation $ed - k(p^2 - 1)(q^2 - 1) = 1$. Our attack is applicable to primes p and q of arbitrary sizes and we do not require the usual assumption that p and q have the same bit size. Thus, this is an extension of our recent result presented at ACISP 2016 conference. Our experiments demonstrate that for a 513-bit prime p and 511-bit prime q, our method works for values of d of up to 520 bits.

Keywords. RSA, elliptic curves, continued fractions.

*mbunder@uow.edu.au
†abderrahmane.nitaj@unicaen.fr
‡wsusilo@uow.edu.au
§joseph_tonien@uow.edu.au

1 Introduction

The public key cryptosystem RSA was introduced by Rivest, Shamir and Adleman [11] in 1978. It is the most popular and widely used public-key cryptosystem. The RSA operations system are based on modular arithmetic. Let p and q be two large primes. The product $N = pq$ is called the RSA modulus and the product $\phi(N) = (p-1)(q-1)$ is the Euler totient function. In RSA, the public exponent e and the private exponent d are integers satisfying $ed \equiv 1 \pmod{\phi(N)}$. A message m is encrypted as $c \equiv m^e \pmod{N}$ and decrypted using $m \equiv c^d \pmod{N}$.

Since its introduction, the RSA cryptosystem has been generalized in various ways, including extensions to singular elliptic curves and Gaussian integers.

In 1995, Kuwakado, Koyama and Tsuruoka [9] presented a new RSA-type scheme based on singular cubic curves with equation $y^2 \equiv x^3 + bx^2 \pmod{N}$ where $N = pq$ is an RSA modulus and $b \in \mathbb{Z}/N\mathbb{Z}$. The public exponent is an integer e such that $\gcd\left(e, \left(p^2-1\right)\left(q^2-1\right)\right) = 1$ and the decryption exponent is the integer $d \equiv e^{-1} \pmod{\left(p^2-1\right)\left(q^2-1\right)}$. From this, we deduce that e and d satisfy a key equation of the form $ed - k\left(p^2-1\right)\left(q^2-1\right) = 1$ where k is a positive integer.

In 2002, Elkamchouchi, Elshenawy and Shaban [6] introduced an extension of RSA to the ring of Gaussian integers. A Gaussian integer is a complex number of the form $a + ib$ where both a and b are integers and $i^2 = -1$. The set of all Gaussian integers is denoted $\mathbb{Z}[i]$. A Gaussian prime number is a Gaussian integer that cannot be represented as a product of non-unit Gaussian integers. The only unit Gaussian integers are ± 1, $\pm i$. Let $P = a + ib$ and $Q = a' + ib'$ be two Gaussian primes. Consider the Gaussian integer $N = PQ$ and the Euler totient function $\phi(N) = (|P| - 1)(|Q| - 1) = \left(a^2 + b^2 - 1\right)\left(a'^2 + b'^2 - 1\right)$. Let e be an integer such that $d \equiv e^{-1} \pmod{\phi(N)}$ exists. Then, in the RSA scheme over the domain of Gaussian integers, a message $m \in \mathbb{Z}[i]$ is encrypted using $c \equiv m^e \pmod{N}$ and decrypted using $m \equiv c^d \pmod{N}$. We note that, in this RSA variant, the key equation is $ed - k(|P| - 1)(|Q| - 1) = 1$ for $N = PQ \in \mathbb{Z}[i]$. In the situation that $N = pq$ is an ordinary RSA modulus, the key equation becomes $ed - k\left(p^2-1\right)\left(q^2-1\right) = 1$, which is the same than in the Kuwakado-Koyama-Tsuruoka elliptic curve variant of RSA.

In 2007, Castagnos [4] proposed a probabilistic scheme based on an RSA modulus $N = pq$ and using arithmetical operations in quadratic field quotients. Let e be a integer such that $\gcd\left(e, \left(p^2-1\right)\left(q^2-1\right)\right) = 1$. For any integer r, let $V_e(r)$ be the eth term of the Lucas sequence defined by $V_0(r) = 2$, $V_1(r) = r$ and $V_{k+2} = rV_{k+1}(r) - V_k(r)$ for $k \geq 0$. In this scheme, a message $m \in \mathbb{Z}/N\mathbb{Z}$ is encrypted using $c \equiv (1 + mN)V_e(r) \pmod{N^2}$ where r is a random integer with $2 \leq r \leq N - 2$. Then some arithmetical properties, one can decrypt c to get the original message m. Similarly to the Kuwakado-Koyama-Tsuruoka elliptic curve variant of RSA and RSA with Gaussian integers, Castagnos scheme leads

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

The security of the RSA cryptosystem and its variants are based on the difficulty of factoring large integers of the shape $N = pq$. Nevertheless, in some cases, the modulus N can be factored by algebraic methods that are not based on factoring algorithms. For example, in 1990, Wiener [12] showed how to break the RSA when the decryption exponent d satisfies $d < \frac{1}{3}N^{0.25}$. Wiener's method is based on solving the key equation $ed - k(p-1)(q-1) = 1$ by applying the continued fraction algorithm to the public rational fraction $\frac{e}{N}$. When d is small enough, $\frac{k}{d}$ is one of the convergents of the continued fraction expansion of $\frac{e}{N}$. Later, Boneh and Durfee [1] applied lattice reduction and Coppersmith's technique [5] and extended the bound to $d < N^{0.292}$. Recently, using the convergents of the continued fraction expansion of $\frac{e}{N'}$ where N' is a number depending on N, Bunder and Tonien [3] could break the RSA if $d^2e < 8N^{1.5}$.

The complexity of the encryption and decryption algorithms are based on the size of the encryption key e and the size of decryption key d, respectively. In a cryptosystem with a limited resource such as a credit card, it is desirable to have a smaller value of d. In some scenario, for convenience, e is set to a small constant, such as $e = 3$.

In this paper, we consider one of the following scenarios where $N = pq$ is the product of two large primes and the public exponent e satisfies an equation $ed - k\left(p^2-1\right)\left(q^2-1\right) = 1$ with a suitably small secret exponent d:

- an instance of the Kuwakado-Koyama-Tsuruoka cryptosystem [9],
- an instance of the RSA over Gaussian integers [6],
- an instance of Castagnos scheme [4].

Our method is inspired by Bunder and Tonien's technique [3]. We show that when $q < p < \mu q$, if $d^2e < \frac{\mu\ N^3}{(\mu-1)^2}$ then one can find p and q and then factor the modulus N. Our method is based on the continued fraction algorithm as in Bunder and Tonien's attack. Under the condition $d^2e < \frac{\mu\ N^3}{(\mu-1)^2}$, we show that one can find $\frac{k}{d}$ among the convergents of the continued fraction expansion of the public number $\frac{e}{N^2+1-\frac{(\mu+1)^2}{2\mu}N}$. When $\mu = 2$, our condition becomes $d < \frac{\sqrt{2}N(N-\frac{5}{2})}{\sqrt{e(N+4)}}$, which is a slightly improvement of our result in [2].

The paper is organized as follows. In Section 2, we present the Kuwakado-Koyama-Tsuruoka RSA-type scheme, the RSA scheme over Gaussian integers and the Castagnos scheme. In Section 3, we review some facts and lemmas used in our attack. In Section 4, we present our new attack for the general case $q < p < \mu q$. Experiment results for $\mu = 2$ and $\mu = 6$ are presented in Section 5.

2 Preliminaries

In this section, we present the three variants of the RSA cryptosystem for which our attack works, namely the Kuwakado-Koyama-Tsuruoka RSA-type scheme, the RSA scheme over Gaussian integers and the Castagnos scheme.

2.1 The Kuwakado-Koyama-Tsuruoka RSA-type scheme

The Kuwakado-Koyama-Tsuruoka RSA-type scheme is based on the use of an RSA modulus $N = pq$ as the modulus of a singular elliptic curve. Let $\mathbb{Z}_N = \mathbb{Z}/N\mathbb{Z}$ be the ring of integers modulo N and $\mathbb{F}_p$ be the finite field. Let a and b be integers with $\gcd(ab, N) = 1$ and $\gcd(4a^3 + 27b^2, N) = 1$. A singular elliptic curve $E_N(a, b)$ over the ring $\mathbb{Z}_N$ is the concatenation of a point $\mathcal{O}_N$, called the point at infinity, and the set of points $(x, y) \in \mathbb{Z}_N^2$ satisfying the Weierstrass equation

$$y^2 + axy \equiv x^3 + bx^2 \pmod{N}.$$

If we consider this form modulo p, we get an elliptic curve $E_p(a, b)$ over $\mathbb{F}_p$

$$E_p(a, b) : y^2 + axy \equiv x^3 + bx^2 \pmod{p},$$

with the point at infinity $\mathcal{O}_p$. It is well known that the chord-and-tangent method defines an addition law on singular elliptic curves, as for all elliptic curves on $\mathbb{F}_p$. The addition law can be summarized as follows.

- For any point $P \in E_p(a, b)$, $P + \mathcal{O}_p = \mathcal{O}_p + P = P$.
- If $P = (x, y) \in E_p(a, b)$, then $-P = (x, -ax - y)$.
- If $P = (x, y)$, then $2P = P_3 = (x_3, y_3)$ with

$$x_3 = \left(\frac{3x^2 + 2bx - ay}{2ay + ax}\right)^2 + a\left(\frac{3x^2 + 2bx - ay}{2ay + ax}\right) - b - 2x,$$
$$y_3 = -\left(\frac{3x^2 + 2bx - ay}{2ay + ax} + a\right)x_3 - \frac{-x^3}{2ay + ax}.$$

- If $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ with $P_1 \neq \pm P_2$, then $P_1 + P_2 = P_3 = (x_3, y_3)$ with

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 + a\left(\frac{y_2 - y_1}{x_2 - x_1}\right) - b - x_1 - x_2,$$
$$y_3 = -\left(\frac{y_2 - y_1}{x_2 - x_1} + a\right)x_3 - \frac{y_1x_2 - y_2x_1}{x_2 - x_1}.$$

The addition law can be extended to the elliptic curve $E_N(a, b)$ in the same way as the addition in $E_p(a, b)$ by replacing computations modulo p by computations

modulo N. In $E_N(a,b)$, a specific problem can occur. Sometimes, the inverse modulo N does not exist. In this case, this could lead to finding a prime factor of N, which is unlikely to happen when p and q are large. Note that this is one of the principles of Elliptic Curve Method of factorization [10].

In 1995, Kuwakado, Koyama and Tsuruoka [9] proposed a system based on singular elliptic curves modulo an RSA modulus, which can be summarized as follows.

1. **Key Generation:**
   - Choose two distinct prime numbers p and q of similar bit-length.
   - Compute $N = pq$.
   - Choose e such that $\gcd\left(e, \left(p^2-1\right)\left(q^2-1\right)\right) = 1$.
   - Compute $d = e^{-1} \pmod{\left(p^2-1\right)\left(q^2-1\right)}$.
   - Keep p, q, d secret and publish N, e.

2. **Encryption:**
   - Transform the message as $m = (m_x, m_y) \in \mathbb{Z}_N \times \mathbb{Z}_N$.
   - Compute $b = \frac{m_y^2 - m_x^3}{m_x^2} \pmod{N}$.
   - Compute the ciphertext point $(c_x, c_y) = e(m_x, m_y)$ on the elliptic curve $y^2 = x^3 + bx^2 \pmod{N}$.

3. **Decryption:**
   - Compute $b = \frac{c_y^2 - c_x^3}{c_x^2} \pmod{N}$.
   - Compute the plaintext point $(m_x, m_y) = d(c_x, c_y)$ on the elliptic curve $y^2 = x^3 + bx^2 \pmod{N}$.

Observe the modular inverse $d = e^{-1} \pmod{\left(p^2-1\right)\left(q^2-1\right)}$ can be transformed as a key equation

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

which will be the starting equation of our new attack.

2.2 RSA over the domain of Gaussian integers

We now focus on how to extend the RSA cryptosystem to the ring of Gaussian integers. We begin by reviewing the main properties of Gaussian integers.

A Gaussian integer is a complex number of the form $a + bi$ where $a, b \in \mathbb{Z}$ and $i^2 = -1$. The set of all Gaussian integers is the ring $\mathbb{Z}[i]$. Let α and $\beta \neq 0$ be two Gaussian integers. We say that β divides α if there exists a Gaussian integer γ such that $\alpha = \beta\gamma$. The norm of a Gaussian integer $a+bi$ is $|a+bi| = a^2+b^2$. A Gaussian prime is a Gaussian integer which is divisible only by a unit. The units in $\mathbb{Z}[i]$ are ± 1 and $\pm i$ and have norm 1. As a consequence, if $a^2 + b^2$ is a prime number in $\mathbb{Z}$, then $a+ib$ is a Gaussian prime. Conversely, if $p \in Z$ is an ordinary prime number, then Gaussian integers p and pi are Gaussian primes if and only if $p \equiv 3 \pmod 4$. The existence of prime factorization in $\mathbb{Z}[i]$ allows us to consider Gaussian integers of the form $N = PQ$ where P and Q are Gaussian primes with large norm. Similarly, the existence of Euclidean division and Euclidean algorithm in $\mathbb{Z}[i]$ allow us to consider arithmetic operations modulo N. On the other hand, if P is a Gaussian prime, then $\alpha^{|P|-1} \equiv 1 \pmod P$ whenever $\alpha \not\equiv 0 \pmod P$. Similarly, if $N = PQ$ is the product of two Gaussian primes, then $\alpha^{(|P|-1)(|Q|-1)} \equiv 1 \pmod N$ whenever $\alpha \not\equiv 0 \pmod N$. In particular, if $N = pq \in \mathbb{Z}$ is the product of two ordinary primes, then $\alpha^{(p^2-1)(q^2-1)} \equiv 1 \pmod N$ whenever $\alpha \not\equiv 0 \pmod N$.

Using the arithmetical operations on the ring $\mathbb{Z}[i]$, Elkamchouchi, Elshenawy and Shaban [6] proposed an extension of the RSA cryptosystem to Gaussian integers. The scheme can be summarized as follows.

1. **Key Generation:**
   - Choose two distinct Gaussian primes P and Q of similar norm.
   - Compute $N = PQ$.
   - Choose e such that $\gcd(e, (|P| - 1)(|Q| - 1)) = 1$.
   - Determine $d = e^{-1} \pmod{(|P| - 1)(|Q| - 1)}$.
   - Keep P, Q, d secret, publish N, e.

2. **Encryption:**
   - Transform the message as a Gaussian integer $M \in \mathbb{Z}[i]$.
   - Compute $C \equiv M^e \pmod N$.

3. **Decryption:**

- Compute $M \equiv C^d \pmod{N}$.

When $N = pq \in \mathbb{Z}$ where p and q are ordinary prime numbers of the form $4m+3$, the modular inverse of e becomes $d = e^{-1} \pmod{\left(p^2-1\right)\left(q^2-1\right)}$ and can be rewritten as

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

This is the same key equation that comes up in the Kuwakado-Koyama-Tsuruoka RSA-type scheme.

2.3 Castagnos scheme

Castagnos scheme [4] was proposed in 2007 and uses an RSA modulus $N = pq$ and a public exponent e such that $\gcd\left(e, \left(p^2-1\right)\left(q^2-1\right)\right) = 1$. The encryption and the decryption algorithms make use of the Lucas series. Let r be an integer. Define $V_0(r) = 2$ and $V_1(r) = r$. For $k \geq 0$, the $k+2$th term of the Lucas sequence is defined by $V_{k+2} = rV_{k+1}(r) - V_k(r)$. The Lucas series can be computed efficiently by the square and multiply algorithm. The Castagnos scheme can be summarized as follows, where $\left(\frac{x}{p}\right)$ is the Jacobi symbol.

1. **Key Generation:**
   - Choose two distinct prime numbers p and q of similar bit-length.
   - Compute $N = pq$.
   - Choose e such that $\gcd\left(e, \left(p^2-1\right)\left(q^2-1\right)\right) = 1$.
   - Keep p, q secret and publish N, e.

2. **Encryption:**
   - Transform the message as an integer $m \in \mathbb{Z}/N\mathbb{Z}$.
   - Choose a random integer $r \in [2, n-2]$.
   - Compute the ciphertext $c \equiv (1+mN)V_e(r) \pmod{N^2}$.

3. **Decryption:**
   - Compute $i_p = \left(\frac{c^2-4}{p}\right)$ and $d(p, i_p) \equiv e^{-1} \pmod{p - i_p}$.
   - Compute $i_q = \left(\frac{c^2-4}{q}\right)$ and $d(q, i_q) \equiv e^{-1} \pmod{q - i_q}$.
   - Compute $r_p \equiv V_{d(p,i_p)} \pmod{p}$ and $r_q \equiv V_{d(q,i_q)} \pmod{q}$.
   - Compute $p' \equiv p^{-1} \pmod{q}$ and $r = r_p + p(r_p - r_q)p' \pmod{N}$.
   - Compute $t_p \equiv \frac{c}{V_e(r)} \pmod{p^2}$ and $m_p \equiv \frac{t_p - 1}{p} \cdot q^{-1} \pmod{p}$.

- Compute $t_q \equiv \frac{c}{V_e(r)} \pmod{q^2}$ and $m_q \equiv \frac{t_q - 1}{q} \cdot p^{-1} \pmod{q}$.
- Compute the plaintext $m \equiv m_p + p(m_q - m_p)p' \pmod{N}$.

Despite the inverse $d \equiv e^{-1} \pmod{\left(p^2-1\right)\left(q^2-1\right)}$ is not being used directly in the scheme, we use the key equation $ed - k\left(p^2-1\right)\left(q^2-1\right) = 1$ to launch an attack on Castagnos scheme when d is suitably small.

3 Useful lemmas

In this section, we review the main properties of the continued fractions and state a useful lemma that will be used in the attack.

A **continued fraction** is an expression of the form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}$$

The continued fraction expansion of a number is formed by subtracting away the integer part of it and inverting the remainder and then repeating this process again and again. The coefficients a_i of the continued fraction of a number x are constructed as follows:

$$x_0 = x,\ a_n = [x_n],\ x_{n+1} = \frac{1}{x_n - a_n}$$

We use the following notation to denote the continued fraction

$$x = [a_0, a_1, \ldots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}$$

If $k \leq n$, the continued fraction $[a_0, a_1, \ldots, a_k]$ is called the k^{th} *convergent* of x. The following theorem gives us the *fundamental recursive formulas* to calculate the convergents.

Theorem 1 *[7] The k^{th} convergent can be determined as*

$$[a_0, \ldots, a_k] = \frac{p_k}{q_k}$$

where the sequences $\{p_n\}$ and $\{q_n\}$ are specified as follows:

$$\begin{aligned} p_{-2} &= 0, \quad p_{-1} = 1, \quad p_n = a_n p_{n-1} + p_{n-2}, \quad \forall n \geq 0, \\ q_{-2} &= 1, \quad q_{-1} = 0, \quad q_n = a_n q_{n-1} + q_{n-2}, \quad \forall n \geq 0. \end{aligned}$$

Theorem 2 *[7] Let p, q be positive integers such that*

$$0 < \left| x - \frac{p}{q} \right| < \frac{1}{2q^2}$$

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

Now, we present a useful result that will be used throughout the paper.

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

$$\phi_1 = N^2 + 1 - (\mu + \frac{1}{\mu})N,$$
$$\phi_2 = N^2 + 1 - 2N.$$

Then

$$\phi_1 < (p^2 - 1)(q^2 - 1) < \phi_2.$$

Proof. We have $1 < \frac{p}{q} < \mu$, so based on the increasing property of the function $f(x) = x + \frac{1}{x}$ on $[1, +\infty)$, we get $f(1) < f\left(\frac{p}{q}\right) < f(\mu)$, that is

$$2 < \frac{p}{q} + \frac{q}{p} < \mu + \frac{1}{\mu}.$$

Multiplying by N, we get

$$2N < p^2 + q^2 < (\mu + \frac{1}{\mu})N.$$

Since $\left(p^2 - 1\right)\left(q^2 - 1\right) = N^2 + 1 - \left(p^2 + q^2\right)$, we get

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

This terminates the proof. ■

4 A new attack based on continued fractions for arbitrary bit size primes

In [2], we consider the case where the two primes p and q are of the same bit size, i.e. $q < p < 2q$ and we have the following result

Theorem 3 *[2] Let (N, e) be a public key in the Kuwakado-Koyama-Tsuruoka cryptosystem or in the RSA cryptosystem with Gaussian integers or in the*

Castagnos scheme with $N = pq$ and $q < p < 2q$. If $e < \left(p^2-1\right)\left(q^2-1\right)$ satisfies an equation $ed - k\left(p^2-1\right)\left(q^2-1\right) = 1$ with

$$d < \sqrt{\frac{2N^3 - 18N^2}{e}},$$

then $\frac{k}{d}$ is a convergent of the continued fraction expansion of

$$\frac{e}{N^2 + 1 - \frac{9}{4}N}$$

and one can factor N in polynomial time.

In this section, we give a generalised attack by considering two primes p and q of arbitrary sizes. We will not require p and p to have the same bit size, but instead, we consider the case $q < p < \mu q$ where μ is a parameter. We show that if

$$d^2 e < \frac{\mu\ N^3}{(\mu-1)^2}$$

then the three RSA-variant schemes can be broken. When $\mu = 2$ then p and q have the same bit size and our result is a slightly improvement of [2]. When $\mu = 2^s$ then the two primes p and q can have their bit sizes differ up to s bits.

Theorem 4 *Let (N, e) be a public key in the Kuwakado-Koyama-Tsuruoka cryptosystem or in the RSA cryptosystem with Gaussian integers or in the Castagnos scheme with $N = pq$ and $q < p < \mu q$. If $e < \left(p^2-1\right)\left(q^2-1\right)$ satisfies an equation $ed - k\left(p^2-1\right)\left(q^2-1\right) = 1$ with*

$$d < \frac{N(N - (\mu + \frac{1}{\mu}))}{\sqrt{e(\frac{(\mu-1)^2}{\mu}N + 2)}} \approx \frac{\sqrt{\mu}\ N^{\frac{3}{2}}}{(\mu-1)\ \sqrt{e}}$$

then $\frac{k}{d}$ is a convergent of the continued fraction expansion of

$$\frac{e}{N^2 + 1 - \frac{(\mu+1)^2}{2\mu}N}$$

and one can factor N in polynomial time.

Proof. By Lemma 1,

$$\phi_1 < (p^2-1)(q^2-1) < \phi_2$$

where

$$\phi_1 = N^2 + 1 - (\mu + \frac{1}{\mu})N,$$
$$\phi_2 = N^2 + 1 - 2N.$$

Let

$$N' = N^2 + 1 - \frac{(\mu+1)^2}{2\mu}N$$

then N' is the midpoint of the interval $[\phi_1, \phi_2]$. Since $\left(p^2-1\right)\left(q^2-1\right) \in [\phi_1, \phi_2]$, we have

$$\left|\left(p^2-1\right)\left(q^2-1\right) - N'\right| < \frac{1}{2}(\phi_2 - \phi_1) = \frac{(\mu-1)^2}{2\mu}N. \tag{1}$$

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

$$\begin{aligned}
\left|\frac{e}{N'} - \frac{k}{d}\right| &\leq e\left|\frac{1}{N'} - \frac{1}{(p^2-1)(q^2-1)}\right| + \left|\frac{e}{(p^2-1)(q^2-1)} - \frac{k}{d}\right| \\
&= e\frac{\left|\left(p^2-1\right)\left(q^2-1\right) - N'\right|}{N'(p^2-1)(q^2-1)} + \frac{1}{(p^2-1)(q^2-1)d} \\
&= e\frac{\left|\left(p^2-1\right)\left(q^2-1\right) - N'\right|}{N'(p^2-1)(q^2-1)} + \frac{e}{(p^2-1)(q^2-1)(k(p^2-1)(q^2-1)+1)}
\end{aligned}$$

Then, using (1), we get

$$\begin{aligned}
\left|\frac{e}{N'} - \frac{k}{d}\right| &< \frac{e\frac{(\mu-1)^2}{2\mu}N}{(\phi_1-1)^2} + \frac{e}{(\phi_1-1)^2} \\
&= \frac{e(\frac{(\mu-1)^2}{2\mu}N + 1)}{(\phi_1-1)^2} \\
&= \frac{e(\frac{(\mu-1)^2}{\mu}N + 2)}{2N^2(N - (\mu + \frac{1}{\mu}))^2}.
\end{aligned}$$

Combining with the condition

$$d < \frac{N(N - (\mu + \frac{1}{\mu}))}{\sqrt{e(\frac{(\mu-1)^2}{\mu}N + 2)}}$$

we have

$$\left|\frac{e}{N'} - \frac{k}{d}\right| < \frac{1}{2d^2}$$

So by Theorem 2, $\frac{k}{d}$ is a convergent of the continued fraction expansion of $\frac{e}{N'}$, and thus, we can find the factorization of N in polynomial time. This terminates the proof. ■

When $\mu = 2$, the condition $q < p < 2q$ implies that the two primes p and q have the same bit size, we have the following result. This is a slightly improvement of [2].

Corollary 1 *Let (N, e) be a public key in the Kuwakado-Koyama-Tsuruoka cryptosystem or in the RSA cryptosystem with Gaussian integers or in the Castagnos scheme with $N = pq$ and $q < p < 2q$. If $e < \left(p^2 - 1\right)\left(q^2 - 1\right)$ satisfies an equation $ed - k\left(p^2 - 1\right)\left(q^2 - 1\right) = 1$ with*

$$d < \frac{\sqrt{2}N(N - \frac{5}{2})}{\sqrt{e(N+4)}} \approx \frac{\sqrt{2}\ N^{\frac{3}{2}}}{\sqrt{e}}$$

then $\frac{k}{d}$ is a convergent of the continued fraction expansion of

$$\frac{e}{N^2 + 1 - \frac{9}{4}N}$$

and one can factor N in polynomial time.

5 Experiment results

5.1 Same bit primes

We consider two RSA primes p and q, both of 512 bits, which give us a 1024-bit modulus N. The public exponent e is 2029-bit and the secret exponent d is 520-bit.

$p =$1009926345 7471330007 1984329453 1837129144 5329854502
1579205949 1972427206 6832404994 0387919056 4150845276
8065924106 7922890816 2666245720 1616730699 1117239731 85481

$q =$9201052432 2086390067 1386866266 0639973895 0237269245
6878261382 5773843108 2681621528 1513707044 8098390827
1161420676 8781444754 1784724352 5840645389 7707377855 3491

$N =$9292385259 8882409829 3162082225 5290648240 2932610895
2796745930 4569281602 2535261774 6000624542 0686015350
5820019086 9644402726 0931963319 2462241182 6579351302
0782053736 0725528276 5503973157 0642939798 0805113181
1631153462 5580255681 0453116780 9138251914 8143650220
1487534725 1944638440 3016589748 5133626528 3338290596 23064171

e =5610945328 2671796041 5829077437 9519142056 5955456458
7016831195 6891736518 8405496534 0274145492 4223492328
5533946739 3132613402 2802793166 8707714667 2017196874
2057028761 3007844191 6424007923 8588782842 5888389498
2399842002 8312226377 0538147674 6869931106 0864836776
4239757895 9256035850 8693271128 6691302868 6894236736
3858899449 4578621026 8249617044 5653141105 6506148300
2531330952 9779988125 0306197976 3903833872 8515848925
1679290735 1472231296 9415530850 4617614777 4425005468
7389111903 1488774848 5654348435 7158394635 1774298241
7614264452 0801690300 4327479471 1402065512 8418504644
3456306876 4694318782 5003370247 1823625867 3480338561 6726117398 7

We found $\frac{k}{d}$ at the 306th convergent of $\frac{e}{N^2-\frac{9}{4}N+1}$

k =2230382597 4699469998 8596682209 1052908389 5670986870
3180114419 9709650127 6686575639 3075936836 3045074562
2035858758 0823897378 9584493028 0368787713 7164782033 05
d =3432398830 0653048574 9095039954 0696608634 7176500716
5270469723 1729592771 5916988280 2606127982 0330727277
4886481556 9574042901 8560993999 8583219062 8701414555 7262923

5.2 Different bit primes

In this section, we present our experimental result with Theorem 4 for the case $\mu = 6$. We pick two RSA primes p and q such that $q < p < 6q$. The prime p is 513-bit and the prime q is 511-bit. The public exponent e is 2025-bit and the secret exponent d is 520-bit. We can verify that the condition of $d < \frac{N(N-(\mu+\frac{1}{\mu}))}{\sqrt{e(\frac{(\mu-1)^2}{\mu}N+2)}}$ is satisfied as required by Theorem 4.

p =2251084283 5399690392 8700279533 0660713571 6421309613
1606252397 0689624877 5416713946 7115639068 3214685532
3666826003 6319257221 4371382498 2817351298 6759602510 57551
q =4309404521 9164250721 4408330391 2371174042 4509359250
1101852828 8585049357 7444908497 8816733294 5916734904
4534762750 3939424631 2488030728 2485748601 6547649010 5607

N =9700832790 7021385390 4896466540 1601016697 9018555029
9703057514 5759061053 3697035051 2074639275 6847870272
0665951962 7031014290 6416502632 7630838653 8473467834
7894193231 7363670403 6746823112 7635148598 2833618775
9537769355 3973649039 4878199679 3768212843 1912875915
5743213282 9142414646 2589790816 1555160091 6544617094 24788457

e =2671630446 5047922612 1252742215 1475559753 7241860791
2093132740 5641923165 9718687137 9309258926 2478467217
6240162209 8399694799 3431771506 3146187336 5667839242
9797136667 0172935196 7047211436 7473569771 6376048156
6682301440 4366414431 8903690242 5361894565 8356426103
1590986355 9710607287 9200098536 4620383116 0061469153
1021296633 3242652768 5015393792 5758080833 8675858392
6006508016 4569283723 6478429721 9444664288 7134749805
8459839679 1047808065 9191027176 5899435088 0770410882
2622162123 1125991843 0044728097 1298291167 5436520870
8063051557 0718647958 9297699102 8690718545 8180532010
5143027320 1226957906 0997422184 9734372569 9623973425 7519040887

We found $\frac{k}{d}$ at the 291th convergent of $\frac{e}{N^2+1-\frac{(\mu+1)^2}{2\mu}N} = \frac{e}{N^2+1-\frac{49}{12}N}$

k =9744422179 7382625455 6522084013 6478311497 0194986256
1788936640 5212659933 2382608493 4392942988 2877863728
9298553572 7992595886 9245052334 7340515904 3019272879
d =3432398830 0653048574 9095039954 0696608634 7176500716
5270469723 1729592771 5916988280 2606127982 0330727277
4886481556 9574042901 8560993999 8583219062 8701414555 7412423

6 Conclusion

We have proposed an attack on three variants of the RSA cryptosystem, namely the Kuwakado-Koyama-Tsuruoka extension for singular elliptic curves, Elkamchouchi et al.'s extension of RSA to the Gaussian integer ring and Castagnos

scheme. For the three extensions, we showed that the RSA modulus $N = pq$ can be factored in polynomial time if the public exponent e is related to a suitably small secret exponent d. The attack is based on the theory of continued fractions and can be seen as an extension of Wiener's [12] and Bunder-Tonien's [3] attacks on the RSA.

References

[1] Boneh, D., Durfee, G.: Cryptanalysis of RSA with private key d less than $N^{0.292}$, Eurocrypt'99, Lecture Notes in Computer Science **1592**, 1–11, 1999.

[2] Bunder, M., Nitaj, A., Susilo, W., Tonien, J.: A new attack on three variants of the RSA cryptosystem, Proceedings of the 21st Australasian Conference on Information Security and Privacy, Lecture Notes in Computer Science 9723, 2016, 258-268.

[3] Bunder, M., Tonien, J.: A new improved attack on RSA, Proceedings of the 5th International Cryptology and Information Security Conference, 2016, 101-110.

[4] Castagnos, G.: An efficient probabilistic public-key cryptosystem over quadratic field quotients, *Finite Fields and Their Applications* **13**, 563–576, 2007.

[5] Coppersmith, D.: Small solutions to polynomial equations, and low exponent RSA vulnerabilities, *Journal of Cryptology* **10**, 233–260, 1997.

[6] Elkamchouchi, H., Elshenawy, K., Shaban, H.: Extended RSA cryptosystem and digital signature schemes in the domain of Gaussian integers, Proceedings of the 8th International Conference on Communication Systems, 91–95, 2002.

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

[8] Koyama, K., Maurer, U.M., Okamoto, T., Vanstone, S.A.: New public-key schemes based on elliptic curves over the ring Z_n, CRYPTO'91, Lecture Notes in Computer Science **576**, 252–266, 1991.

[9] 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* **E78-A**,27–33, 1995.

[10] Lenstra, H.: Factoring integers with elliptic curves, *Annals of Mathematics* **126**, 649–673, 1987.

[11] Rivest, R., Shamir, A., Adleman, L.: A Method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM* **21**, 120–126, 1978.

[12] Wiener, M.: Cryptanalysis of short RSA secret exponents, *IEEE Transactions on Information Theory* **36**, 553–558, 1990.