A new attack on three variants of the RSA cryptosystem

Martin Bunder, Abderrahmane Nitaj, Willy Susilo, Joseph Tonien

A new attack on three variants of the RSA cryptosystem

Martin Bunder[1], Abderrahmane Nitaj[2], Willy Susilo[3], and Joseph Tonien[3]

[1]School of Mathematics and Applied Statistics, University of Wollongong, Australia, *mbunder@uow.edu.au*
[2]Université de Caen, France, *abderrahmane.nitaj@unicaen.fr*
[3]Centre for Computer and Information Security Research, School of Computing and Information Technology, University of Wollongong, Australia, [*wsusilo,joseph tonien*]*@uow.edu.au*

Abstract

In 1995, Kuwakado, Koyama and Tsuruoka presented a new RSA-type scheme based on singular cubic curves $y^2 \equiv x^3 + bx^2 \pmod N$ where $N = pq$ is an RSA modulus. Then, in 2002, Elkamchouchi, Elshenawy and Shaban introduced 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. Later, in 2007, Castagnos's proposed a scheme over quadratic fields quotients with an RSA modulus $N = pq$. In the three schemes, the public exponent e is an integer satisfying the key equation $ed - k\left(p^2 - 1\right)\left(q^2 - 1\right) = 1$. In this paper, we apply the continued fraction method to launch an attack on the three schemes when the private exponent d is sufficiently small. Our attack can be considered as an extension of the famous Wiener attack on RSA.

Keywords. RSA, Elliptic curves, continued fractions

Mathematics Subject Classification. 94A60, 68P25, 11A55.

1 Introduction

The public key cryptosystem RSA was introduced by Rivest, Shamir and Adleman [10] 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 in 1978 by Rivest, Shamir and Adleman [10], the RSA cryptosystem has been generalized in various ways, including extensions to singular elliptic curves and Gaussian integers.

In 1995, Kuwakado, Koyama and Tsuruoka [8] 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 $\gcd(e, (p^2-1)(q^2-1)) = 1$ and the decryption exponent is the integer $d \equiv e^{-1} \pmod{(p^2-1)(q^2-1)}$. From this, we deduce that e and d satisfy a key equation of the form $ed - k(p^2-1)(q^2-1) = 1$ where k is a positive integer.

In 2002, Elkamchouchi, Elshenawy and Shaban [5] 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 is such that $i^2 = -1$. The set of all Gaussian integers is denoted $\mathbb{Z}[i]$. A Gaussian prime number is a Gaussian integer that can not be 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 $\phi(N) = (|P|-1)(|Q|-1) = (a^2+b^2-1)(a'^2+b'^2-1)$. 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 $ed - k(p^2-1)(q^2-1) = 1$, which is the same than in the Kuwakado-Koyama-Tsuruoka elliptic curve variant of RSA.

In 2007, Castagnos [3] proposed a probabilistic scheme based on an RSA modulus $N = pq$ and using arithmetic operations in quadratic field quotients. Let e be a integer such that $\gcd(e, (p^2-1)(q^2-1)) = 1$. 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 arithmetic 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 intgers, Castagnos scheme leads to the key equation $ed - k(p^2-1)(q^2-1) = 1$.

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 [11] showed how to break 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 [4] and extended the bound to $d < N^{0.292}$.

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 $ed - k(p^2-1)(q^2-1) = 1$ with suitably small secret exponent d.

- an instance of the Kuwakado-Koyama-Tsuruoka cryptosystem [8],
- an instance of the RSA over Gaussian integers [5],
- an instance of Castagnos scheme [3].

Our attack works for certain small sizes of d. We show that when d is sufficiently small, namely $d < \sqrt{\frac{2N^3 - 18N^2}{e}}$, then one can find p and q an

then factor the modulus N. Our method is based on the continued fraction algorithm as in Wiener's attack. Under the condtion $d < \sqrt{\frac{2N^3-18N^2}{e}}$, we show that one can find $\frac{k}{d}$ among the covergents of the continued fraction expansion of the public rational number $\frac{e}{N^2-\frac{9}{4}N+1}$.

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 Castagnos scheme. In Section 3, we review some facts and lemmas used in our attack. In Section 4, we present our new attack with a numerical example. We conclude the paper in Section 5.

2 Preliminaries

In this section, we present the two 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 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 [9].

In 1995, Kuwakado, Koyama and Tsuruoka [8] 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 $\gcd(e, (p^2-1)(q^2-1)) = 1$.
   - Compute $d = e^{-1} \pmod{(p^2-1)(q^2-1)}$.
   - 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 $d = e^{-1} \pmod{(p^2-1)(q^2-1)}$ 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 is such that $i^2 = -1$. 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 $\alpha^{\left(p^2-1\right)\left(q^2-1\right)} \equiv 1 \pmod{N}$ whenever $\alpha \not\equiv 0 \pmod{N}$.

Using the arithmetic operations on the ring $\mathbb{Z}[i]$, Elkamchouchi, Elshenawy and Shaban [5] 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 [3] was proposed in 2007 and uses an RSA modulus $N = pq$ and a public exponent e such that $\gcd(e, (p^2-1)(q^2-1)) = 1$. 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. 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 $\gcd(e, (p^2-1)(q^2-1)) = 1$.
   - 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 $d \equiv e^{-1} \pmod{(p^2-1)(q^2-1)}$ is not used directly in the scheme, we use the key equation $ed - k(p^2-1)(q^2-1) = 1$ 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. For example,

$$\begin{aligned}\frac{2015}{444} &= 4 + \frac{239}{444} = 4 + \frac{1}{\frac{444}{239}} = 4 + \cfrac{1}{1 + \frac{205}{239}} = 4 + \cfrac{1}{1 + \cfrac{1}{\frac{239}{205}}} \\ &= 4 + \cfrac{1}{1 + \cfrac{1}{1 + \frac{34}{205}}} = 4 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{\frac{205}{34}}}} = 4 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{6 + \frac{1}{34}}}}\end{aligned}$$

As we have seen above, 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. *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[1]*:*

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

Theorem 2. *Let p, q be positive integers such that $\frac{p}{q} \notin \mathbb{N}$ and $(p, q) = 1$. If*

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

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

Proofs of Theorem 1 and Theorem 2 can be found in most of standard textbooks on number theory such as [6].

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

Lemma 1. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let $\phi_1 = N^2 + 1 - \frac{5}{2}N$ and $\phi_2 = N^2 + 1 - 2N$. Then*

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

Proof. Suppose that $q < p < 2q$. Then $1 < \frac{p}{q} < 2$, so since the function $f(x) = x + \frac{1}{x}$ is increasing on $[1, +\infty)$, we get $f(1) < f\left(\frac{p}{q}\right) < f(2)$, that is

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

[1]The convergents start with $\frac{p_0}{q_0}$, but it is a convention to extend the sequence index to -1 and -2 to allow the recursive formula to hold for $n = 0$ and $n = 1$

Multiplying by N, we get

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

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

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

that is $\phi_1 < (p^2-1)(q^2-1) < \phi_2$. This terminates the proof. □

4 A New Attack on RSA Variants Based on Continued Fractions

In this section, we propose a new attack on the Kuwakado-Koyama-Tsuruoka cryptosystem as well as RSA over the Gaussian integer domain and Castagnos scheme in the situation that the key equation $ed - k(p^2-1)(q^2-1) = 1$ is satisfied with a suitably small secret exponent d.

Theorem 3. *Let (N, e) be a public key in the Kuwakado-Koyama-Tsuruoka cryptosystem or in the RSA cryptosystem with Gaussian integers or in Castagnos scheme with $N = pq$ and $q < p < 2q$. If $e < (p^2-1)(q^2-1)$ satisfies an equation $ed - k(p^2-1)(q^2-1) = 1$ with*

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

then one can factor N in polynomial time.

Proof. Let $\phi_1 = N^2 + 1 - \frac{5}{2}N$ and $\phi_2 = N^2 + 1 - 2N$. Then $N' = N^2 - \frac{9}{4}N + 1$ is the midpoint of the interval $[\phi_1, \phi_2]$. Since $(p^2-1)(q^2-1) \in [\phi_1, \phi_2]$, then

$$\left|(p^2-1)(q^2-1) - N'\right| < \frac{1}{2}(\phi_2 - \phi_1) = \frac{1}{4}N. \tag{1}$$

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

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

Then, using $d = \frac{k\left(p^2-1\right)\left(q^2-1\right)+1}{e}$ and (1), we get

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

Now, using Lemma 1, we get

$$\left|\frac{e}{N'} - \frac{k}{d}\right| < \frac{eN}{4\phi_1^2} + \frac{e}{\phi_1^2} < \frac{e(N+4)}{4(\phi_1-1)^2} = \frac{e(N+4)}{4\left(N^2 - \frac{5}{2}N\right)^2}. \tag{2}$$

A straightforward calculation shows that

$$\frac{N+4}{4\left(N^2 - \frac{5}{2}N\right)^2} < \frac{1}{4N^3 - 36N^2}.$$

Combining this with (2), we get

$$\left|\frac{e}{N'} - \frac{k}{d}\right| < \frac{1}{4N^3 - 36N^2}.$$

If $d < \sqrt{\frac{2N^3-18N^2}{e}}$, then $\left|\frac{e}{N'} - \frac{k}{d}\right| < \frac{1}{2d^2}$ and by Theorem 2, $\frac{k}{d}$ is a convergent of the continued fraction expansion of $\frac{e}{N'}$. Using k and d, we get

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

Combining with $N = pq$, we get the values of p and q which leads to the factorization of N. Observe that every step in the proof can be done in polynomial time. This terminates the proof. □

Remark 1. Observe that in most of the cases, the public exponent e is full-sized, that is $e \approx N^2$. Then our method of Theorem can be applied to factor N whenever $d < \sqrt{2N-18} \approx \sqrt{2}\sqrt{N}$.

Remark 2. Since e satisfies the key equation $ed - k\left(p^2-1\right)\left(q^2-1\right) = 1$, then $ed > \left(p^2-1\right)\left(q^2-1\right) > N^2 + 1 - \frac{5}{2}N$. In connection with Theorem 3, to ensure $d < \sqrt{\frac{2N^3-18N^2}{e}}$, the exponent e should satisfy

$$e > \frac{N^2 + 1 - \frac{5}{2}N}{\sqrt{\frac{2N^3-18N^2}{e}}},$$

from which we deduce the lower bound for e

$$e > \frac{\left(N^2 + 1 - \frac{5}{2}N\right)^2}{2N^3 - 18N^2} \approx \frac{1}{2}N.$$

Consequently, our method can not be applied for small values of e such as $e = 3$.

4.1 A numerical example

In connection with Theorem 3, we present an experimental result. We consider the RSA modulus N and the public exponent e as follows.

$$\begin{aligned} N &= 26179392205533153027454620 91, \\ e &= 56560393323059524365594244618317839555728723511570041 85. \end{aligned}$$

The first partial quotients of $\frac{e}{N^2 - \frac{9}{4}N + 1}$ are

$$0, 1, 4, 1, 2, 1, 1, 1, 1, 3, 1, 1, 1, 46, 3, 5, 1, 1, 2, 26, 2, 2, 39, 1, 3, 2, 3, 1, 23104, 1, 9,$$
$$1, 1, 2, 1, 3, 2, 2, ...$$

We can see that the 29th partial quotient is more larger than the previous ones. This means that the 28th convergent is a promising candidate for $\frac{k}{d}$. Indeed, using $\frac{k}{d} = \frac{981582747476}{1189415557289}$, we get

$$\begin{aligned} &\left(p^2 - 1\right)\left(q^2 - 1\right) = \frac{ed - 1}{k} \\ &= 685360576251130006447319558821209509635136192846981 6064. \end{aligned}$$

Combining with the equation $N = pq$, we get

$$\begin{aligned} p &= 68410308889243, \\ q &= 38268197630737. \end{aligned}$$

which completes the factorization of N. In this example, we can check that the condition $d < \sqrt{\frac{2N^3 - 18N^2}{e}}$ is satisfied as required in Theorem 3.

5 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 attack on RSA and Bunder-Tonien's [2] attacks on the RSA.

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] M. Bunder, J. Tonien, A new improved attack on RSA based on Wiener's technique of continued fractions, submitted manuscript.

[3] 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`

[4] Coppersmith, D.: Small solutions to polynomial equations, and low exponent RSA vulnerabilities. Journal of Cryptology, 10(4), pp. 233–260 (1997)

[5] 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.

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

[7] K. Koyama, U.M. Maurer, T. Okamoto, S.A. Vanstone, New Public-Key Schemes Based on Elliptic Curves over the Ring Z_n, CRYPTO 1991, Lecture Notes in Computer Science 576, 252-266.

[8] 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.

[9] Lenstra, H.: Factoring integers with elliptic curves, Annals of Mathematics, Vol. 126, pp. 649–673 (1987)

[10] 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)

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