HAL
open science

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

Martin Bunder, Abderrahmane Nitaj, Willy Susilo, Joseph Tonien

## To cite this version:

Martin Bunder, Abderrahmane Nitaj, Willy Susilo, Joseph Tonien. Cryptanalysis of RSA-type cryptosystems based on Lucas sequences, Gaussian integers and elliptic curves. Journal of information security and applications, 2018, 10.1016/j.jisa.2018.04.006 . hal-02320970

HAL Id: hal-02320970<br>https://normandie-univ.hal.science/hal-02320970

Submitted on 20 Oct 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# Cryptanalysis of RSA-type cryptosystems based on Lucas sequences, Gaussian integers and elliptic curves ${ }^{\star}$ 

Martin Bunder ${ }^{1}$, Abderrahmane Nitaj ${ }^{2}$, Willy Susilo ${ }^{3}$, and Joseph Tonien ${ }^{3}$<br>${ }^{1}$ School of Mathematics and Applied Statistics, University of Wollongong, Australia<br>mbunder@uow.edu.au<br>${ }^{2}$ Département de Mathématiques, Université de Caen, France abderrahmane.nitaj@unicaen.fr<br>${ }^{3}$ Centre for Computer and Information Security Research, School of Computing and Information Technology, University of Wollongong, Australia<br>[wsusilo, joseph_tonien]@uow.edu.au


#### Abstract

In 1995, Kuwakado, Koyama and Tsuruoka presented a new RSA-type scheme based on singular cubic curves $y^{2} \equiv x^{3}+b x^{2}(\bmod N)$ where $N=p q$ 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 $N=P Q$ where $P$ and $Q$ are Gaussian primes such that $p=|P|$ and $q=|Q|$ are ordinary primes. Later, in 2007, Castagnos proposed a scheme over quadratic field quotients with an RSA modulus $N=p q$ based on Lucas sequences. In the three schemes, the public exponent $e$ is an integer satisfying the key equation $e d-k\left(p^{2}-1\right)\left(q^{2}-1\right)=1$. 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 experiments demonstrate that for a 1024-bit modulus, our method works for values of $d$ of up to 520 bits. We also examine the effect of dropping the usual assumption that $p$ and $q$ have the same bit size.


Keywords: RSA, elliptic curves, continued fractions.

[^0]
## 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 $N=p q$ 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 $e d \equiv 1(\bmod \phi(N))$. A message $m$ is encrypted as $c \equiv m^{e}(\bmod N)$ and decrypted using $m \equiv c^{d}$ $(\bmod N)$.

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 $y^{2} \equiv x^{3}+b x^{2}(\bmod N)$ where $N=p q$ is an RSA modulus and $b \in \mathbb{Z} / N \mathbb{Z}$. The public exponent is an integer $e$ such that $\operatorname{gcd}\left(e,\left(p^{2}-1\right)\left(q^{2}-1\right)\right)=1$ and the decryption exponent is the integer $d \equiv e^{-1}\left(\bmod \left(p^{2}-1\right)\left(q^{2}-1\right)\right)$. From this, we deduce that $e$ and $d$ satisfy a key equation of the form $e d-k\left(p^{2}-1\right)\left(q^{2}-1\right)=1$ 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 $a+i b$ 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 $\pm 1, \pm i$. Let $P=a+i b$ and $Q=a^{\prime}+i b^{\prime}$ be two Gaussian primes. Consider the Gaussian integer $N=P Q$ and the Euler totient function $\phi(N)=(|P|-1)(|Q|-1)=\left(a^{2}+b^{2}-1\right)\left(a^{\prime 2}+b^{\prime 2}-1\right)$. Let $e$ be an integer such that $d \equiv e^{-1}(\bmod \phi(N))$ exists. Then, in the RSA scheme over the domain of Gaussian integers, a message $m \in \mathbb{Z}[i]$ is encrypted using $c \equiv m^{e}$ $(\bmod N)$ and decrypted using $m \equiv c^{d}(\bmod N)$. We note that, in this RSA variant, the key equation is $e d-k(|P|-1)(|Q|-1)=1$ for $N=P Q \in \mathbb{Z}[i]$. In the situation that $N=p q$ 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 $N=p q$ and using arithmetical operations in quadratic field quotients. Let $e$ be a integer such that $\operatorname{gcd}\left(e,\left(p^{2}-1\right)\left(q^{2}-1\right)\right)=1$. For any integer $r$, let $V_{e}(r)$ be the $e$ th term of the Lucas sequence defined by $V_{0}(r)=2, V_{1}(r)=r$ and $V_{k+2}=r V_{k+1}(r)-V_{k}(r)$ for $k \geq 0$. In this scheme, a message $m \in \mathbb{Z} / N \mathbb{Z}$ is encrypted using $c \equiv(1+m N) V_{e}(r)\left(\bmod N^{2}\right)$ 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 $e d-k\left(p^{2}-1\right)\left(q^{2}-1\right)=1$.

The security of the RSA cryptosystem and its variants are based on the difficulty of factoring large integers of the shape $N=p q$. 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 $e d-k(p-1)(q-1)=1$ 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 $\frac{e}{N^{\prime}}$ where $N^{\prime}$ is a number depending on $N$, Bunder and Tonien [3] could break the RSA if $d^{2} e<8 N^{1.5}$.

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 $N=p q$ is the product of two large primes and the public exponent $e$ satisfies an equation $e d-k\left(p^{2}-1\right)\left(q^{2}-1\right)=1$ 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 in the case when $p$ and $q$ has equal bit length, if $d^{2} e<2 N^{3}-18 N^{2}$ 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 $d<\sqrt{\frac{2 N^{3}-18 N^{2}}{e}}$, we show that one can find $\frac{k}{d}$ among the convergents of the continued fraction expansion of the public rational number $\frac{e}{N^{2}-\frac{9}{4} N+1}$. In the general case, where $q<p<\mu q$, if $d^{2} e<\frac{\mu N^{3}}{(\mu-1)^{2}}$ then we can find $\frac{k}{d}$ among the convergents of the continued fraction expansion of $\frac{e}{N^{2}+1-\frac{(\mu+1)^{2}}{2 \mu} N}$.

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 case $q<p<2 q$ and in Section 5, our attack for the general case $q<p<\mu q$. Experiment results for $\mu=2$ and $\mu=6$ are presented in Section 6 . Note that the contents of Section 5 and Section 6 are new and have not been included in our conference paper [2].

## 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 $N=p q$ 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 $\operatorname{gcd}(a b, N)=1$ and $\operatorname{gcd}\left(4 a^{3}+27 b^{2}, N\right)=1$. 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

$$
y^{2}+a x y \equiv x^{3}+b x^{2} \quad(\bmod N)
$$

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

$$
E_{p}(a, b): y^{2}+a x y \equiv x^{3}+b x^{2} \quad(\bmod p)
$$

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 $-P=(x,-a x-y)$.
- If $P=(x, y)$, then $2 P=P_{3}=\left(x_{3}, y_{3}\right)$ with

$$
\begin{aligned}
& x_{3}=\left(\frac{3 x^{2}+2 b x-a y}{2 a y+a x}\right)^{2}+a\left(\frac{3 x^{2}+2 b x-a y}{2 a y+a x}\right)-b-2 x, \\
& y_{3}=-\left(\frac{3 x^{2}+2 b x-a y}{2 a y+a x}+a\right) x_{3}-\frac{-x^{3}}{2 a y+a x} .
\end{aligned}
$$

- If $P_{1}=\left(x_{1}, y_{1}\right)$ and $P_{2}=\left(x_{2}, y_{2}\right)$ with $P_{1} \neq \pm P_{2}$, then $P_{1}+P_{2}=P_{3}=$ $\left(x_{3}, y_{3}\right)$ with

$$
\begin{aligned}
x_{3} & =\left(\frac{y_{2}-y_{1}}{x_{2}-x_{1}}\right)^{2}+a\left(\frac{y_{2}-y_{1}}{x_{2}-x_{1}}\right)-b-x_{1}-x_{2}, \\
y_{3} & =-\left(\frac{y_{2}-y_{1}}{x_{2}-x_{1}}+a\right) x_{3}-\frac{y_{1} x_{2}-y_{2} x_{1}}{x_{2}-x_{1}} .
\end{aligned}
$$

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 $N=p q$.
- Choose $e$ such that $\operatorname{gcd}\left(e,\left(p^{2}-1\right)\left(q^{2}-1\right)\right)=1$.
- Compute $d=e^{-1}\left(\bmod \left(p^{2}-1\right)\left(q^{2}-1\right)\right)$.
- Keep $p, q, d$ secret and publish $N, e$.


## 2. Encryption:

- Transform the message as $m=\left(m_{x}, m_{y}\right) \in \mathbb{Z}_{N} \times \mathbb{Z}_{N}$.
- Compute $b=\frac{m_{y}^{2}-m_{x}^{3}}{m_{x}^{2}}(\bmod N)$.
- Compute the ciphertext point $\left(c_{x}, c_{y}\right)=e\left(m_{x}, m_{y}\right)$ on the elliptic curve $y^{2}=x^{3}+b x^{2}(\bmod N)$.


## 3. Decryption:

- Compute $b=\frac{c_{y}^{2}-c_{x}^{3}}{c_{x}^{2}}(\bmod N)$.
- Compute the plaintext point $\left(m_{x}, m_{y}\right)=d\left(c_{x}, c_{y}\right)$ on the elliptic curve $y^{2}=x^{3}+b x^{2}(\bmod N)$.

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

$$
e d-k\left(p^{2}-1\right)\left(q^{2}-1\right)=1
$$

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 $a+b i$ where $a, b \in \mathbb{Z}$ and $i^{2}=-1$. The set of all Gaussian integers is the ring $\mathbb{Z}[i]$. Let $\alpha$ and $\beta \neq 0$ be two Gaussian integers. We say that $\beta$ divides $\alpha$ if there exists a Gaussian integer $\gamma$ such that $\alpha=\beta \gamma$. The norm of a Gaussian integer $a+b i$ is $|a+b i|=a^{2}+b^{2}$. A Gaussian prime is a Gaussian integer which is divisible only by a unit. The units in $\mathbb{Z}[i]$ are $\pm 1$ and $\pm i$ and have norm 1 . As a consequence, if $a^{2}+b^{2}$ is a prime number in $\mathbb{Z}$, then $a+i b$ is a Gaussian prime. Conversely, if $p \in Z$ is an ordinary prime number, then Gaussian integers $p$ and $p i$ are Gaussian primes if and only if $p \equiv 3(\bmod 4)$. The existence of prime factorization in $\mathbb{Z}[i]$ allows us to consider Gaussian integers of the form $N=P Q$ 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 $\alpha^{|P|-1} \equiv 1(\bmod P)$ whenever $\alpha \not \equiv 0$ $(\bmod P)$. Similarly, if $N=P Q$ is the product of two Gaussian primes, then $\alpha^{(|P|-1)(|Q|-1)} \equiv 1(\bmod N)$ whenever $\alpha \not \equiv 0(\bmod N)$. In particular, if $N=$ $p q \in \mathbb{Z}$ is the product of two ordinary primes, then $\alpha^{\left(p^{2}-1\right)\left(q^{2}-1\right)} \equiv 1(\bmod N)$ whenever $\alpha \not \equiv 0(\bmod N)$.

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 $N=P Q$.
- Choose $e$ such that $\operatorname{gcd}(e,(|P|-1)(|Q|-1))=1$.
- Determine $\left.d=e^{-1}(\bmod (|P|-1)(|Q|-1))\right)$.
- Keep $P, Q, d$ secret, publish $N, e$.


## 2. Encryption:

- Transform the message as a Gaussian integer $M \in \mathbb{Z}[i]$.
- Compute $C \equiv M^{e}(\bmod N)$.


## 3. Decryption:

- Compute $M \equiv C^{d}(\bmod N)$.

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

$$
e d-k\left(p^{2}-1\right)\left(q^{2}-1\right)=1
$$

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 $N=p q$ and a public exponent $e$ such that $\operatorname{gcd}\left(e,\left(p^{2}-1\right)\left(q^{2}-1\right)\right)=1$. 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 $V_{k+2}=r V_{k+1}(r)-V_{k}(r)$. 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 $N=p q$.
- Choose $e$ such that $\operatorname{gcd}\left(e,\left(p^{2}-1\right)\left(q^{2}-1\right)\right)=1$.
- 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 $c \equiv(1+m N) V_{e}(r)\left(\bmod N^{2}\right)$.


## 3. Decryption:

- Compute $i_{p}=\left(\frac{c^{2}-4}{p}\right)$ and $d\left(p, i_{p}\right) \equiv e^{-1}\left(\bmod p-i_{p}\right)$.
- Compute $i_{q}=\left(\frac{c^{2}-4}{q}\right)$ and $d\left(q, i_{q}\right) \equiv e^{-1}\left(\bmod q-i_{q}\right)$.
- Compute $r_{p} \equiv V_{d\left(p, i_{p}\right)}(\bmod p)$ and $r_{q} \equiv V_{d\left(q, i_{q}\right)}(\bmod q)$.
- Compute $p^{\prime} \equiv p^{-1}(\bmod q)$ and $r=r_{p}+p\left(r_{p}-r_{q}\right) p^{\prime}(\bmod N)$.
- Compute $t_{p} \equiv \frac{c}{V_{e}(r)}\left(\bmod p^{2}\right)$ and $m_{p} \equiv \frac{t_{p}-1}{p} \cdot q^{-1}(\bmod p)$.
- Compute $t_{q} \equiv \frac{c}{V_{e}(r)}\left(\bmod q^{2}\right)$ and $m_{q} \equiv \frac{t_{q}-1}{q} \cdot p^{-1}(\bmod q)$.
- Compute the plaintext $m \equiv m_{p}+p\left(m_{q}-m_{p}\right) p^{\prime}(\bmod N)$.

Despite the inverse $d \equiv e^{-1}\left(\bmod \left(p^{2}-1\right)\left(q^{2}-1\right)\right)$ is not being used directly in the scheme, we use the key equation $e d-k\left(p^{2}-1\right)\left(q^{2}-1\right)=1$ 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

$$
a_{0}+\frac{1}{a_{1}+\frac{1}{a_{2}+\frac{1}{\ddots}}}
$$

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:

$$
x_{0}=x, a_{n}=\left[x_{n}\right], x_{n+1}=\frac{1}{x_{n}-a_{n}}
$$

We use the following notation to denote the continued fraction

$$
x=\left[a_{0}, a_{1}, \ldots, a_{n}\right]=a_{0}+\frac{1}{a_{1}+\frac{1}{\ddots \cdot+\frac{1}{a_{n}}}}
$$

If $k \leq n$, the continued fraction $\left[a_{0}, a_{1}, \ldots, a_{k}\right]$ is called the $k^{\text {th }}$ convergent of $x$. The following theorem gives us the fundamental recursive formulas to calculate the convergents

Theorem 1. [7] The $k^{\text {th }}$ convergent can be determined as

$$
\left[a_{0}, \ldots, a_{k}\right]=\frac{p_{k}}{q_{k}}
$$

where the sequences $\left\{p_{n}\right\}$ and $\left\{q_{n}\right\}$ 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

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

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

$$
\phi_{1}<\left(p^{2}-1\right)\left(q^{2}-1\right)<\phi_{2} .
$$

Proof. Suppose that $q<p<2 q$. 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

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

Multiplying by $N$, we get

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

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

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

that is $\phi_{1}<\left(p^{2}-1\right)\left(q^{2}-1\right)<\phi_{2}$. 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 the Castagnos scheme in the situation that the key equation $e d-k\left(p^{2}-1\right)\left(q^{2}-1\right)=1$ 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 the Castagnos scheme with $N=p q$ and $q<p<2 q$. 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

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

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

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

and one can factor $N$ in polynomial time.
Proof. Let $\phi_{1}=N^{2}+1-\frac{5}{2} N$ and $\phi_{2}=N^{2}+1-2 N$. Then $N^{\prime}=N^{2}-\frac{9}{4} N+1$ is the midpoint of the interval $\left[\phi_{1}, \phi_{2}\right]$. Since $\left(p^{2}-1\right)\left(q^{2}-1\right) \in\left[\phi_{1}, \phi_{2}\right]$, then

$$
\begin{equation*}
\left|\left(p^{2}-1\right)\left(q^{2}-1\right)-N^{\prime}\right|<\frac{1}{2}\left(\phi_{2}-\phi_{1}\right)=\frac{1}{4} N . \tag{1}
\end{equation*}
$$

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

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

Then, using $d=\frac{k\left(p^{2}-1\right)\left(q^{2}-1\right)+1}{e}$ and (3), we get

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

Now, using Lemma 1 , we get

$$
\begin{equation*}
\left|\frac{e}{N^{\prime}}-\frac{k}{d}\right|<\frac{e N}{4 \phi_{1}^{2}}+\frac{e}{\phi_{1}^{2}}<\frac{e(N+4)}{4\left(\phi_{1}-1\right)^{2}}=\frac{e(N+4)}{4\left(N^{2}-\frac{5}{2} N\right)^{2}} . \tag{2}
\end{equation*}
$$

A straightforward calculation shows that

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

Combining this with (2), we get

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

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

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

Combining with $N=p q$, 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.

## 5 Different bit size primes

In Section 4, we consider the case where the two primes $p$ and $q$ are of the same bit size, i.e. $q<p<2 q$. In this section, we give a generalised attacked 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 $\mu$ 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.
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 $N=p q$ 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

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

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. 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

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

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

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

Let

$$
\begin{aligned}
& \phi_{1}=N^{2}+1-\left(\mu+\frac{1}{\mu}\right) N \\
& \phi_{2}=N^{2}+1-2 N \\
& N^{\prime}=N^{2}+1-\frac{(\mu+1)^{2}}{2 \mu} N .
\end{aligned}
$$

Then $N^{\prime}$ is the midpoint of the interval $\left[\phi_{1}, \phi_{2}\right]$. Since $\left(p^{2}-1\right)\left(q^{2}-1\right) \in\left[\phi_{1}, \phi_{2}\right]$, we have

$$
\begin{equation*}
\left|\left(p^{2}-1\right)\left(q^{2}-1\right)-N^{\prime}\right|<\frac{1}{2}\left(\phi_{2}-\phi_{1}\right)=\frac{(\mu-1)^{2}}{2 \mu} N \tag{3}
\end{equation*}
$$

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

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

Then, using (3), we get

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

Combining with the condition

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

we have

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

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

## 6 Experiment results

### 6.1 Same bit primes

In connection with Theorem 3, we present an experimental result. 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. We can verify that the condition $d<\sqrt{\frac{2 N^{3}-18 N^{2}}{e}}$ is satisfied as required by Theorem 3 .

$$
\begin{array}{rl}
p= & 10099263457471330007 \\
& 1579205949 \\
& 1972427206 \\
8065924106 & 7922890816 \\
q & 2666245729453
\end{array} 1616371291445398554502
$$

$e=56109453282671796041582907743795191420565955456458$
70168311956891736518840549653402741454924223492328
55339467393132613402280279316687077146672017196874
20570287613007844191642400792385887828425888389498
23998420028312226377053814767468699311060864836776
42397578959256035850869327112866913028686894236736
38588994494578621026824961704456531411056506148300
25313309529779988125030619797639038338728515848925
16792907351472231296941553085046176147774425005468
73891119031488774848565434843571583946351774298241
76142644520801690300432747947114020655128418504644
3456306876469431878250033702471823625867348033856167261173987

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

$$
\begin{aligned}
k= & 22303825974699469998859668220910529083895670986870 \\
& 31801144199709650127668657563930759368363045074562 \\
& 2035858758082389737895844930280368787713716478203305 \\
d= & 34323988300653048574909503995406966086347176500716 \\
& 52704697231729592771591698828026061279820330727277 \\
& 488648155695740429018560993999858321906287014145557262923
\end{aligned}
$$

### 6.2 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 $q<p<6 q$. The prime $p$ is 513bit 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 $d<\frac{N\left(N-\left(\mu+\frac{1}{\mu}\right)\right)}{\sqrt{e\left(\frac{(\mu-1)^{2}}{\mu} N+2\right)}}$ is satisfied as required by Theorem 4.

```
p=22510842835399690392 8700279533 0660713571 6421309613
    1606252397 0689624877 5416713946 7115639068 3214685532
    366682600363192572214371382498 28173512986759602510 57551
q=43094045219164250721440833039123711740424509359250
    1101852828 8585049357 7444908497 88167332945916734904
    453476275039394246312488030728 2485748601 65476490105607
```

```
N=9700832790 7021385390 4896466540 1601016697 9018555029
        970305751457590610533697035051 20746392756847870272
        0665951962703101429064165026327630838653 8473467834
        7894193231736367040367468231127635148598 2833618775
        9537769355 39736490394878199679 37682128431912875915
        57432132829142414646 258979081615551600916544617094 24788457
```

```
e=2671630446 5047922612125274221514755597537241860791
    209313274056419231659718687137 9309258926 2478467217
    6240162209 83996947993431771506 31461873365667839242
    9797136667 0172935196 7047211436 74735697716376048156
    6682301440 436641443189036902425361894565 8356426103
    1590986355 9710607287 920009853646203831160061469153
    1021296633 324265276850153937925758080833 8675858392
    6006508016 4569283723647842972194446642887134749805
    8459839679 1047808065 91910271765899435088 0770410882
    2622162123 1125991843 004472809712982911675436520870
    80630515570718647958 92976991028690718545 8180532010
    51430273201226957906 0997422184973437256996239734257519040887
```

We found $\frac{k}{d}$ at the 291th convergent of $\frac{e}{N^{2}+1-\frac{(\mu+1)^{2}}{2 \mu} N}=\frac{e}{N^{2}+1-\frac{49}{12} N}$
$k=97444221797382625455652208401364783114970194986256$ 17889366405212659933238260849343929429882877863728 92985535727992595886924505233473405159043019272879
$d=34323988300653048574909503995406966086347176500716$ 52704697231729592771591698828026061279820330727277 488648155695740429018560993999858321906287014145557412423

## 7 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 $N=p q$ 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, 2016.
3. Bunder, M., Tonien, J.: A new improved attack on RSA, Proceedings of the 5th International Cryptology and Information Security Conference, 2016.
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 $y^{2}=x^{3}+b x^{2}(\bmod n)$, 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.

[^0]:    * This paper is the extended version of "A new attack on three variants of the RSA cryptosystem" [2] presented at ACISP 2016

