Attacking an RSA-like Cryptosystem Using Continued Fractions and Lattices

George Teşeleanu

Simion Stoilow Institute of Mathematics of the Romanian Academy
21 Calea Grivitei, Bucharest, Romania

Abstract. Let $N = pq$ be the product of two balanced primes. Cotan and Teşeleanu (2023) introduced a family of RSA-like cryptosystems defined by $ed - k(p^n - 1)(q^n - 1) = 1$, where $n \geq 1$, encompassing classical RSA ($n = 1$) and the Elkamchouchi–Elshenawy–Shaban variant ($n = 2$). We present a new attack for $n = 3$ that integrates continued fractions with lattice-based methods, naturally extending previous results for $n = 1, 2, 4, 6$.

Keywords: continued fraction attack, lattice attack, small private key attack, RSA

1 Introduction

Background. The RSA cryptosystem, introduced by Rivest, Shamir, and Adleman in 1978 [23], remains one of the most deployed public-key encryption schemes. The textbook RSA works in the multiplicative group $\mathbb{Z}_N^*$, where $N = pq$ is a product of two large primes. Encryption of a message $m \in \mathbb{Z}_N^*$ is performed by $c \equiv m^e \bmod N$, with e chosen such that $\gcd(e, \varphi(N)) = 1$, where $\varphi(N) = (p-1)(q-1)$. Decryption is defined as $m \equiv c^d \bmod N$, where $d \equiv e^{-1} \bmod \varphi(N)$. The tuple (N, e) is public, while (p, q, d) remains secret. In what follows, we restrict attention to balanced primes, meaning $q < p < 2q$, so that p and q share the same bit-length.

From the outset, recovering d from (N, e) has been a central target for cryptanalysis. Wiener's classical result [29] shows that if $d < N^{0.25}/3$, it can be recovered from the continued fraction expansion of e/N, which in turn factors N. Boneh and Durfee [4] improved this to $d < N^{0.292}$ via Coppersmith's method [8] and lattice reduction [17], with Herrmann and May [14] later achieving the same bound using simpler tools. Broader surveys of such attacks are given in [3,19,24].

RSA over Gaussian Integers. In 2002, Elkamchouchi, Elshenawy, and Shaban [12] proposed an RSA analogue over the ring of Gaussian integers modulo N. Elements have the form $a + bi$ with $a, b \in \mathbb{Z}_N$ and $i^2 = -1$. The multiplicative group $\mathbb{Z}_N[i]$ has order $\phi(N) = (p^2 - 1)(q^2 - 1)$, and the exponents satisfy $\gcd(e, \phi(N)) = 1$ with $d \equiv e^{-1} \bmod \phi(N)$. Encryption and decryption proceed exactly as in RSA, except all arithmetic is carried out in $\mathbb{Z}_N[i]$.

Although this extension was claimed to offer greater security, Bunder *et al.* [5] showed a Wiener-type attack via continued fractions. Later improvements [22,31] using lattice reduction techniques pushed the bound to $d < N^{0.585}$. Additional analysis can be found in [10, 24].

Generalizing via Galois Fields. The rings Z_p and $Z_p[i]$ can be identified as $Z_p \cong GF(p)$ and $Z_p[i] \cong GF(p^2)$, where GF denotes a Galois field. Thus, classical RSA operates over $GF(p) \times GF(q)$, while the Gaussian variant corresponds to $GF(p^2) \times GF(q^2)$. This perspective led Cotan and Teşeleanu [10] to define a family of RSA-like systems over $GF(p^n) \times GF(q^n)$, for $n \geq 1$, with group order $\varphi_n(N) = (p^n - 1)(q^n - 1)$. Encryption and decryption generalize directly from the $n = 1, 2$ cases.

The main motivation was to determine whether Wiener-type cryptanalysis extends to this broader class. Indeed, [10] showed that for $d < N^{0.25n}$, continued fractions recover d for any n. The unbalanced prime case was later covered in [11]. A lattice-based extension, left as an open question in these works, was resolved in [26], yielding stronger bounds. Other related lattice techniques appear in [28].

Related work. The approach of Blomer and May [1] combined continued fractions with Coppersmith's method. They showed that if

$$ae + b = k\varphi_1(N),$$

and

$$0 < a \leq \frac{1}{3}N^{\frac{1}{4}} \quad \text{and} \quad |b| = \mathcal{O}(N^{-\frac{3}{4}}ae),$$

then we can factor N in polynomial time.

Another variation, due to Nitaj [21], considered

$$ae - b(p - u)(q - v) = 1,$$

under specific bounds on a, b, u, v and with small prime factors for $p - u$ and $q - v$.

The $n = 2, 4, 6$ cases were analyzed in [6, 20, 27], where factorization follows if a, b and c from $ae - b\varphi_n(N) = c$ satisfy specific conditions. We summarize these results in Table 1.

Our Contributions. We investigate the previously untreated case $n = 3$, by combining continued fractions with lattice reduction techniques. Our method begins by recovering integers a, b from $ae - b\varphi_3(N) = c$ via a continued fraction approximation. These values yield an estimate $\hat{p}$ for p, which can then be recovered exactly using Coppersmith's method. Knowing the upper bound on d from $ed - k\varphi_3(N) = 1$ also allows us, through [20], to deduce a corresponding lower bound.

	Upper bound
$n = 2$ [6]	$2N - 4\sqrt{2}N^{3/4}$
$n = 3$ (this work)	$\frac{N^3 - 10N\sqrt{N} + 1}{22N\sqrt{N} + N^{3/4}}$
$n = 4$ [20]	$\frac{2N^4 - 49N^2 + 2}{170N^2 + 4N}$
$n = 6$ [27]	$\frac{N^6 - 162N^3 + 1}{1100N^3 + 2N\sqrt{N}}$

Table 1. Summary on upper bounds for ab.

Structure of the Paper. Preliminaries are reviewed in Section 2. The attack is detailed in Section 3, followed by an example in Section 4 and final remarks in Section 5.

2 Preliminaries

Notations. Throughout the paper, λ denotes a security parameter. Also, the notation $|S|$ denotes the cardinality of a set S. The action of selecting a random element x from a sample space X is denoted by $x \xleftarrow{\$} X$.

2.1 Continued fraction

For any real number ζ there exists a unique sequence $(a_n)_n$ of integers such that

$$\zeta = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cdots}}}},$$

where $a_k > 0$ for any $k \geq 1$. This sequence represents the continued fraction expansion of ζ and is denoted by $\zeta = [a_0, a_1, a_2, \ldots]$. Remark that ζ is a rational number if and only if its corresponding representation as a continued fraction is finite.

For any real number $\zeta = [a_0, a_1, a_2, \ldots]$, the sequence of rational numbers $(A_n)_n$, obtained by truncating this continued fraction, $A_k = [a_0, a_1, a_2, \ldots, a_k]$, is called the convergents sequence of ζ.

According to [13], the following bound allows us to check if a rational number u/v is a convergent of ζ.

Theorem 1. *Let $\zeta = [a_0, a_1, a_2, \ldots]$ be a positive real number. If u, v are positive integers such that $\gcd(u, v) = 1$ and*

$$\left|\zeta - \frac{u}{v}\right| < \frac{1}{2v^2},$$

then u/v is a convergent of $[a_0, a_1, a_2, \ldots]$.

2.2 Finding Small Roots

In this section, we outline some tools used for solving the problem of finding small roots, both in the modular and integer cases.

Coppersmith [7–9] provided rigorous techniques for computing small integer roots of single-variable polynomials modulo an integer, as well as bivariate polynomials over the integers. In the case of modular roots, Coppersmith's ideas were reinterpreted by Howgrave-Graham [15]. We further provide Howgrave-Graham result.

Theorem 2. *Let $f(x_1, \ldots, x_n) = \sum a_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n} \in \mathbb{Z}[x_1, \ldots, x_n]$ be a polynomial with at most ω monomials, α be an integer and let*

$$||f(x_1, \ldots, x_n)|| = \sqrt{\sum |a_{i_1 \ldots i_n}|^2}$$

be its norm. Suppose that

- *$f(y_1, \ldots, y_n) \equiv 0 \bmod \alpha$ for some $|y_1| < X_1, \ldots, |y_n| < X_n$,*
- *$||f(y_1 X_1, \ldots, y_n X_n)|| < \alpha/\sqrt{\omega}$,*

then $f(y_1, \ldots, y_n) = 0$ holds over integers.

Lenstra, Lenstra and Lovász [17] proposed a lattice reduction algorithm (LLL) that is widely used in cryptanalysis and is typically combined with Howgrave-Graham's lemma. We further provide the version presented in [16, 18].

Theorem 3. *Let L be a lattice of dimension ω. In polynomial time, the LLL algorithm outputs a reduced basis $(b_1, \ldots, b_\omega)$ that satisfies*

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

where $det(L)$ is the determinant of lattice L.

Note that the condition

$$2^{\frac{\omega(\omega-1)}{4(\omega+1-i)}} det(L)^{\frac{1}{\omega+1-i}} < \alpha/\sqrt{\omega}$$

implies that the polynomials corresponding to b_i match Howgrave-Graham's bound. This leads to

$$det(L) \leq \varepsilon \alpha^{\omega+1-i},$$

where ε is an error term that is usually ignored.

In order to find a solution $(y_1, \ldots, y_n)$ we need the following assumption to be true.

Assumption 4 *The LLL reduced basis polynomials are algebraically independent*[1]*, and the resultant computations for b_i yield the common roots of these polynomials.*

In [2], the authors present a more flexible formulation of Coppersmith's result [8]. Their method first constructs a specific lattice basis, applies the LLL algorithm [17] to reduce it, and finally uses Howgrave-Graham's lemma [15] to derive the solutions.

Theorem 5. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Suppose we are given an approximation of p with additive error at most $N^{1/4}$. Then N can be factored in polynomial time.*

Once an attack is obtained for a given upper bound on small private exponents, the result of [20] implies the existence of a corresponding attack for a given lower bound on large private exponents. For results concerning φ_1, φ_2, φ_4 and φ_6, we refer the reader to [20, 27].

Theorem 6. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Let $\psi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Suppose we are given an algorithm $\mathcal{A}$ that is able to factor N in polynomial time given N and a public exponent $0 < e < \psi(p, q)$ such that there exists positive integers x and y satisfying*

$$ex - y\psi(p, q) = z, \text{ with } xy < \mathcal{B}_1 \text{ and } |z| < \mathcal{B}_2,$$

for $\mathcal{B}_1 > 0$ and $\mathcal{B}_2 \geq 1$. Then, using algorithm $\mathcal{A}$, N can be factored in polynomial time given N and a public exponent $0 < e' < \psi(p, q)$ such that the corresponding private exponent is $d' = \psi(p, q) - d$ for some $d < \sqrt{\mathcal{B}_1}$.

2.3 Quotient Groups

In this section we provide the group theory needed to introduce the RSA-like family. Therefore, let $(\mathbb{F}, +, \cdot)$ be a field and $t^n - r$ an irreducible polynomial in $\mathbb{F}[t]$. Then

$$\mathbb{A}_n = \mathbb{F}[t]/(t^n - r) = \{a_0 + a_1 t + \ldots + a_{n-1} t^{n-1} \mid a_0, a_1, \ldots, a_{n-1} \in \mathbb{F}\}$$

is the corresponding quotient field. Let $a(t), b(t) \in \mathbb{A}_n$. Remark that the quotient field induces a natural product

$$\begin{aligned} a(t) \circ b(t) &= \left(\sum_{i=0}^{n-1} a_i t^i\right) \circ \left(\sum_{j=0}^{n-1} b_j t^j\right) \\ &= \sum_{i=0}^{n-2} \left(\sum_{j=0}^{i} a_j b_{i-j} + r \sum_{j=0}^{i+n} a_j b_{i-j+n}\right) t^i + \sum_{j=0}^{n-1} a_j b_{n-1-j} t^{n-1}. \end{aligned}$$

[1] They do not share a non-trivial gcd.

2.4 RSA-like Cryptosystems

Let p be a prime number. When we instantiate $\mathbb{F} = \mathbb{Z}_p$, we have that $\mathbb{A}_n = GF(p^n)$ is the Galois field of order p^n. Moreover, $\mathbb{A}_n^*$ is a cyclic group of order $\varphi_n(\mathbb{Z}_p) = p^n - 1$. Remark that an analogous of Fermat's little theorem holds

$$a(t)^{\varphi_n(\mathbb{Z}_p)} \equiv 1 \bmod p,$$

where $a(t) \in \mathbb{A}_n^*$ and the power is evaluated by $\circ$-multiplying $a(t)$ by itself $\varphi_n(\mathbb{Z}_p) - 1$ times. Based on these observations, the authors of [10] built an encryption scheme that is similar to RSA by using the $\circ$ operation as the product.

Setup(λ): Let $n \geq 1$ be an integer. Randomly generate two distinct large prime numbers p, q such that $p, q \geq 2^\lambda$ and compute their product $N = pq$. Select $r \in \mathbb{Z}_N$ such that the polynomial $t^n - r$ is irreducible in $\mathbb{Z}_p[t]$ and $\mathbb{Z}_q[t]$. Let

$$\varphi_n(\mathbb{Z}_N) = \varphi_n(N) = (p^n - 1) \cdot (q^n - 1).$$

Choose an integer e such that $\gcd(e, \varphi_n(N)) = 1$ and compute d such that $ed \equiv 1 \bmod \varphi_n(N)$. Output the public key $pk = (n, N, r, e)$. The corresponding secret key is $sk = (p, q, d)$.

Encrypt(pk, m): To encrypt a message $m = (m_0, \ldots, m_{n-1}) \in \mathbb{Z}_N^n$ we first construct the polynomial $m(t) = m_0 + \ldots + m_{n-1}t^{n-1} \in \mathbb{A}_n^*$ and then we compute $c(t) \equiv [m(t)]^e \bmod N$. Output the ciphertext $c(t)$.

Decrypt$(sk, c(t))$: To recover the message, simply compute $m(t) \equiv [c(t)]^d \bmod N$ and reassemble $m = (m_0, \ldots, m_{n-1})$.

Remark 1. When $n = 1$ we get the RSA scheme [23]. Also, when $n = 2$, we obtain the Elkamchouchi *et al.* cryptosystem [12].

3 A Generalized Wiener-type Attack

In this section, we investigate the generalized equation $ae - b\varphi_3(N) = c$, where e is the public exponent and c is a known value. Our approach unfolds in two main stages: initially, we derive the coefficients a and b through a continued fraction expansion; subsequently, we approximate p, and use Coppersmith's result to factor N. We start by examining the lattice-based approach and then proceed to the continued fractions method.

3.1 Application of Lattices

We begin this subsection with a lemma that provides bounds for the sum $p^3 + q^3$.

Lemma 1. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Then the following property holds*

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

Proof. From the inequality $q < p < 2q$ we derive $1 < p\sqrt{p}/(q\sqrt{q}) < 2\sqrt{2}$. Since the function $f(x) = x + 1/x$ is increasing on $[1, +\infty)$, we have that

$$2 < \frac{p\sqrt{p}}{q\sqrt{q}} + \frac{q\sqrt{q}}{p\sqrt{p}} < \frac{9\sqrt{2}}{4}.$$

Multiplying the inequality with $N\sqrt{N}$, we obtain

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

just as desired. □

Using the following lemma (provided in [21, Lemma 1]), we prove that $p-q = \Omega(N\sqrt{N})$.

Lemma 2. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Then the following property holds*

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

Lemma 3. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Then the following property holds*

$$0 < p^3 - q^3 < \frac{7\sqrt{2}}{4}N\sqrt{N}.$$

Proof. According to Lemma 2 we obtain

$$\frac{\sqrt{2}}{4}N\sqrt{N} < q^3 < N\sqrt{N} < p^3 < 2\sqrt{2}N\sqrt{N}.$$

Therefore, we have

$$0 < p^3 - q^3 < 2\sqrt{2}N\sqrt{N} - \frac{\sqrt{2}}{4}N\sqrt{N}.$$

just as desired. □

Let $S_3 = p^3 + q^3$ and $D_3 = p^3 - q^3$. Using the value for φ_3, namely

$$\varphi_3 = N^3 - S_3 + 1,$$

and the relation

$$p^3 - q^3 = \sqrt{(p^3 + q^3)^2 - 4N^3}$$

we further derive some approximations for $p^3 + q^3$ and $p^3 - q^3$.

Lemma 4. *Let $0 < \delta < 7\sqrt{2}/4$ and $N = pq > (3\sqrt{2}/4\delta)^{4/3}$ be the product of two unknown primes with $q < p < 2q$ and $p^3 - q^3 \geq \delta N\sqrt{N}$. Also, let e be a public exponent satisfying $ae - b\varphi_3(N) = c$ such that $6|c| < \delta b N^{3/4}$. We define $S_3 = p^3 + q^3$, $D_3 = p^3 - q^3$,*

$$\hat{S}_3 = N^3 - 1 - \frac{ae}{b} \quad \text{and} \quad \hat{D}_3 = \sqrt{\hat{S}_3^2 - 4N^3}$$

Then the following hold

$$|S_3 - \hat{S}_3| < \frac{3}{6}N^{3/4} \quad \text{and} \quad |D_3 - \hat{D}_3| < \frac{9}{6}N^{3/4}.$$

Proof. We know that

$$\varphi_3 = N^3 - p^3 - q^3 + 1 = (ae - c)/b,$$

and thus, we have that

$$S_3 = N^3 + 1 - \frac{ae - c}{b}.$$

Therefore, we obtain the following

$$|S_3 - \hat{S}_3| = \frac{|c|}{b} < \frac{\delta}{6}N^{3/4} < \frac{3}{6}N^{3/4}.$$

For the second part of the proof, we first observe that

$$\hat{S}_3^2 - 4N^3 = D_3^2 - 2S_3\frac{c}{b} + \frac{c^2}{b^2}.$$

To prove that $\hat{D}_3$ is well defined, it suffices to show that $D_3^2 \geq 2S_3\frac{|c|}{b}$. We observe that

$$2S_3\frac{|c|}{b} < 2 \cdot \frac{9\sqrt{2}}{4}N\sqrt{N} \cdot \frac{\delta}{6}N^{3/4} = \frac{3\sqrt{2}}{4}\delta N^{9/4} < \delta^2 N^3 < (p^3 - q^3)^2.$$

Note that $\delta N^{3/4}/6 < N\sqrt{N}/2 < (p^3 + q^3)/4$ and thus $|\hat{S}_3| < 5S_3/4$. Using

$$\hat{D}_3 - D_3 = \sqrt{\hat{S}_3^2 - 4N^3} - D_3 = \frac{(\hat{S}_3 - S_3)(\hat{S}_3 + S_3)}{\hat{D}_3 + D_3}$$

we obtain that

$$\hat{D}_3 - D_3 < \frac{\delta}{6}N^{3/4} \cdot \frac{9}{4} \cdot 4N\sqrt{N} \cdot \frac{1}{D_3} < \frac{9}{6}N^{3/4},$$

just as desired. □

The following lemma proven in [27] will be useful to prove the subsequent theorem.

Lemma 5. *Let $u > v > 0$. The following inequality holds*

$$\sqrt[3]{u} - \sqrt[3]{v} < \sqrt[3]{u \pm v} < \sqrt[3]{u} + \sqrt[3]{v}.$$

We are now in a position to apply Coppersmith's result to factor N.

Theorem 7. *Let $0 < \delta < 7\sqrt{2}/4$ and $N = pq > (3\sqrt{2}/4\delta)^{4/3}$ be the product of two unknown primes with $q < p < 2q$ and $p^3 - q^3 \geq \delta N\sqrt{N}$. Also, let e be a public exponent satisfying $ae - b\varphi_3(N) = c$ such that $6|c| < b\delta N^{3/4}$. Given e, N, a and b we can factor N in polynomial time.*

Proof. Using the approximations derived in Lemma 4 we have that

$$\begin{aligned}\left|p - \sqrt[3]{\frac{1}{2}(\hat{S}_3 + \hat{D}_3)}\right| &= \left|\sqrt[3]{\frac{1}{2}(S_3 + D_3)} - \sqrt[3]{\frac{1}{2}(\hat{S}_3 + \hat{D}_3)}\right| \\ &\leq \sqrt[3]{\frac{1}{2}|S_3 - \hat{S}_3| + \frac{1}{2}|D_3 - \hat{D}_3|} \\ &< \sqrt[3]{\frac{3}{12}N^{3/4} + \frac{9}{12}N^{3/4}} = N^{1/4},\end{aligned}$$

where for the first inequality we used Lemma 5. Therefore,

$$\hat{p} = \sqrt[3]{0.5(\hat{S} + \hat{D})}$$

is a good approximation of p. Now according to Theorem 5, we can factor N in polynomial time. □

3.2 Application of Continued Fractions

We begin this subsection with a lemma (provided in [6, Lemma 3]) that provides lower and upper bounds for p and q.

Lemma 6. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Then the following property holds*

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

We further derive an useful bound for the continued fraction part of our attack.

Lemma 7. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Then the following property holds*

$$\left|S^3 - 3NS - 10N\sqrt{N}\right| < 11N\sqrt{N}$$

where $S = p + q$.

Proof. Using Lemma 6 we obtain that

$$8N\sqrt{N} < S^3 < 27N\sqrt{N}.$$

Therefore, we have

$$-N\sqrt{N} = (8 - 3 \cdot 3)N\sqrt{N} < S^3 - 3NS < (27 - 3 \cdot 2)N\sqrt{N} = 21N\sqrt{N}.$$

Thus, we obtain

$$-11N\sqrt{N} < A - 10N\sqrt{N} < 11N\sqrt{N},$$

just as desired. □

Theorem 8. *Let $0 < \delta < 7\sqrt{2}/4$ and $N = pq > (3\sqrt{2}/4\delta)^{4/3}$ be the product of two unknown primes with $q < p < 2q$ and $p^3 - q^3 \geq \delta N\sqrt{N}$. Also, let e be a public exponent satisfying $ae - b\varphi_3(N) = c$ such that $6|c| < \delta b N^{3/4}$. Given e, N we can factor N in polynomial time if*

$$ab < \frac{N^3 - 10N\sqrt{N} + 1}{N^{3/4} + 22N\sqrt{N}}.$$

Proof. According to [26] we have

$$\varphi_3 = N^3 + 3NS - S^3 + 1.$$

We denote by

$$A = S^3 - 3NS - 10N\sqrt{N}.$$

We know that

$$ae - b\left(N^3 - A - 10N\sqrt{N} + 1\right) = c$$

which is equivalent to

$$ae - b\left(N^3 - 10N\sqrt{N} + 1\right) = c - bA.$$

Dividing everything by $a(N^3 - 10N\sqrt{N} + 1)$ we obtain

$$\frac{e}{N^3 - 10N\sqrt{N} + 1} - \frac{b}{a} = \frac{c - bA}{a(N^3 - 10N\sqrt{N} + 1)}.$$

Taking the absolute value we obtain

$$\begin{aligned}
\left|\frac{e}{N^3 - 10N\sqrt{N} + 1} - \frac{b}{a}\right| &\leq \frac{|c| + |bA|}{a(N^3 - 10N\sqrt{N} + 1)} \\
&\leq \frac{\delta N^{3/4} + 6|A|}{6(N^3 - 10N\sqrt{N} + 1)} \cdot \frac{b}{a} \\
&\leq \frac{N^{3/4} + 22N\sqrt{N}}{N^3 - 10N\sqrt{N} + 1} \cdot \frac{b}{2a} \\
&< \frac{1}{ab} \cdot \frac{b}{2a} = \frac{1}{2a^2}.
\end{aligned}$$

where for the third inequality we used Lemma 7 and for the last inequality we used our hypothesis. Since

$$\left| \frac{e}{N^3 - 10N\sqrt{N} + 1} - \frac{b}{a} \right| < \frac{1}{2a^2}.$$

then according to Theorem 1 b/a appears among the convergents of $e/(N^3 - 10N\sqrt{N}+1)$. Once we obtain a and b we apply Theorem 7, and thus we conclude our proof. □

To conclude, we apply our general result to the RSA-like cryptosystem in the case $n = 3$. The second corollary follows from Theorem 6.

Corollary 1. *Let $0 < \delta < 7\sqrt{2}/4$ and $N = pq > (3\sqrt{2}/4\delta)^{4/3}$ be the product of two unknown primes with $q < p < 2q$ and $p^3 - q^3 \geq \delta N\sqrt{N}$. Also, let $e < \varphi_3(N)$ be a public exponent satisfying $ed - k\varphi_3(N) = 1$. Given e, N we can factor N in polynomial time if*

$$d < \sqrt{\frac{N^3 - 10N\sqrt{N} + 1}{N^{3/4} + 22N\sqrt{N}}}.$$

Proof. We notice that

$$k = \frac{ed - 1}{\varphi_3(N)} < \frac{ed}{\varphi_3(N)} < d$$

and

$$kd < d^2 < \frac{N^3 - 10N\sqrt{N} + 1}{N^{3/4} + 22N\sqrt{N}}$$

According to Theorem 8 we can factor N in polynomial time. □

Corollary 2. *Let $0 < \delta < 7\sqrt{2}/4$ and $N = pq > (3\sqrt{2}/4\delta)^{4/3}$ be the product of two unknown primes with $q < p < 2q$ and $p^3 - q^3 \geq \delta N\sqrt{N}$. Also, let $e < \varphi_3(N)$ be a public exponent satisfying $ed - k\varphi_3(N) = 1$. Given e, N we can factor N in polynomial time if*

$$d > \varphi_3(N) - \sqrt{\frac{N^3 - 10N\sqrt{N} + 1}{N^{3/4} + 22N\sqrt{N}}}.$$

4 Experimental Results

To validate our result, we executed the code for our attack [25] on a workstation running Ubuntu 20.04.1, equipped with an Intel(R) Core(TM) i7-1165G7 CPU at 2.80 GHz (8 cores) and 16 GB of RAM. The implementation was carried out in SageMath 10.3, based on the Coppersmith attack code from [30].

We used the following parameters

$$\begin{aligned} N &= 348965558859919659799872778156428368196003826103849376373 1, \\ e &= 914388687895768317115801481073211755133354550733330425214416055 \\ &\quad 247322855089745802781880650112500450644009507380804851765908646 \\ &\quad 474776489258324710201007396549253335751630927 7. \end{aligned}$$

Computing the continued fraction expansion of $e/(N^3 - 10N\sqrt{N} + 1)$, we get the first 25 partial quotients

$$[0, 4, 1, 1, 1, 5, 8, 5, 2, 12, 2, 5, 1, 2, 1, 12, 42, 10, 2, 1, 1, 9, 1, 2, 1, \ldots].$$

Looking at the $82th$ convergent we obtain

$$\begin{aligned} a &= 139379657490816394634598239204052259412 3813 \\ b &= 299904193479875310237724396865170476455978, \end{aligned}$$

which satisfy the condition of Theorem 8. Therefore, we obtain the following approximations of S_3 and D_3

$$\begin{aligned} \hat{S}_3 &= 233338672780168639333586294670548066997335251906712757949 \\ &\quad 944567539727771990747907949748 9 \\ \hat{D}_3 &= 229667362942519266201139773721266646133097156290727851611 \\ &\quad 604786408601887555172406912254 6. \end{aligned} \tag{1}$$

Once we know $\hat{S}_3$ and $\hat{D}_3$ we can compute p's approximation

$$\hat{p} = 132287523294776463864922187740.$$

Using Coppersmith's algorithm we find

$$p = 132287523294776463864922187741,$$

and then we can compute

$$q = N/p = 263793251372859435495403773 91.$$

5 Conclusions

In this paper, we have presented a generalized Wiener-type attack against RSA-like cryptosystems. Our approach begins by analyzing the general equation $ae - b\varphi_3(N) = c$, followed by the application of a result due to Coppersmith [2, 8]. We demonstrate that when d is either sufficiently small or sufficiently large, N can be factored in polynomial time.

Future work. An interesting direction for future work would be to develop a method applicable to $\varphi_i(N)$ for arbitrary i, rather than only for specific cases (*i.e.* for $n = 1, 2, 3, 4, 6$).

References

1. Blömer, J., May, A.: A Generalized Wiener Attack on RSA. In: PKC 2004. Lecture Notes in Computer Science, vol. 2947, pp. 1–13. Springer (2004)
2. Blömer, J., May, A.: A Tool Kit for Finding Small Roots of Bivariate Polynomials over the Integers. In: EUROCRYPT 2005. Lecture Notes in Computer Science, vol. 3494, pp. 251–267. Springer (2005)
3. Boneh, D.: Twenty Years of Attacks on the RSA Cryptosystem. Notices of the AMS **46**(2), 203–213 (1999)
4. Boneh, D., Durfee, G.: Cryptanalysis of RSA with Private Key d Less than $N^{0.292}$. In: EUROCRYPT 1999. Lecture Notes in Computer Science, vol. 1592, pp. 1–11. Springer (1999)
5. Bunder, M., Nitaj, A., Susilo, W., Tonien, J.: A New Attack on Three Variants of the RSA Cryptosystem. In: ACISP 2016. Lecture Notes in Computer Science, vol. 9723, pp. 258–268. Springer (2016)
6. Bunder, M., Nitaj, A., Susilo, W., Tonien, J.: A Generalized Attack on RSA Type Cryptosystems. Theoretical Computer Science **704**, 74–81 (2017)
7. Coppersmith, D.: Finding a Small Root of a Bivariate Integer Equation; Factoring with High Bits Known. In: EUROCRYPT 1996. Lecture Notes in Computer Science, vol. 1070, pp. 178–189. Springer (1996)
8. Coppersmith, D.: Finding a Small Root of a Univariate Modular Equation. In: EUROCRYPT 1996. Lecture Notes in Computer Science, vol. 1070, pp. 155–165. Springer (1996)
9. Coppersmith, D.: Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities. Journal of Cryptology **10**(4), 233–260 (1997)
10. Cotan, P., Teşeleanu, G.: Small Private Key Attack Against a Family of RSA-Like Cryptosystems. In: NordSEC 2023. Lecture Notes in Computer Science, vol. 14324, pp. 57–72. Springer (2023)
11. Cotan, P., Teşeleanu, G.: A Security Analysis of Two Classes of RSA-Like Cryptosystems. Journal of Mathematical Cryptology **18**(1), 20240013 (2024)
12. Elkamchouchi, H., Elshenawy, K., Shaban, H.: Extended RSA Cryptosystem and Digital Signature Schemes in the Domain of Gaussian Integers. In: ICCS 2002. vol. 1, pp. 91–95. IEEE Computer Society (2002)
13. Hardy, G.H., Wright, E.M., et al.: An Introduction to the Theory of Numbers. Oxford University Press (1979)
14. Herrmann, M., May, A.: Maximizing Small Root Bounds by Linearization and Applications to Small Secret Exponent RSA. In: PKC 2010. Lecture Notes in Computer Science, vol. 6056, pp. 53–69. Springer (2010)
15. Howgrave-Graham, N.: Finding small roots of univariate modular equations revisited. In: IMA 1997. Lecture Notes in Computer Science, vol. 1355, pp. 131–142. Springer (1997)
16. Jochemsz, E., May, A.: A Strategy for Finding Roots of Multivariate Polynomials with New Applications in Attacking RSA Variants. In: ASIACRYPT 2006. Lecture Notes in Computer Science, vol. 4284, pp. 267–282. Springer (2006)

17. Lenstra, A.K., Lenstra, H.W., Lovász, L.: Factoring Polynomials with Rational Coefficients. Mathematische Annalen **261**, 515–534 (1982)
18. May, A.: New RSA Vulnerabilities Using Lattice Reduction Methods. Ph.D. thesis, University of Paderborn (2003)
19. May, A.: Using LLL-Reduction for Solving RSA and Factorization Problems. In: The LLL Algorithm: Survey and Applications, pp. 315–348. Information Security and Cryptography, Springer (2010)
20. Michel, S., Niang, O., Sow, D.: A new generalized attack on rsa-like cryptosystems. IACR Cryptology ePrint Archive **2025/380** (2025)
21. Nitaj, A.: Another Generalization of Wiener's Attack on RSA. In: AFRICACRYPT 2008. Lecture Notes in Computer Science, vol. 5023, pp. 174–190. Springer (2008)
22. Peng, L., Hu, L., Lu, Y., Wei, H.: An Improved Analysis on Three Variants of the RSA Cryptosystem. In: Inscrypt 2016. Lecture Notes in Computer Science, vol. 10143, pp. 140–149. Springer (2016)
23. Rivest, R.L., Shamir, A., Adleman, L.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM **21**(2), 120–126 (1978)
24. Shi, G., Wang, G., Gu, D.: Further Cryptanalysis of a Type of RSA Variants. In: ISC 2022. Lecture Notes in Computer Science, vol. 13640, pp. 133–152. Springer (2022)
25. Teşeleanu, G.: Generalized Wiener-type Attacks Against Some Particular Cases of the Generalised Elkamchouchi et al. Scheme. https://github.com/teseleanu/generalized-wiener-type-attacks
26. Teşeleanu, G.: A Lattice Attack Against a Family of RSA-Like Cryptosystems. In: CSCML 2024. Lecture Notes in Computer Science, vol. 15349, pp. 343–355. Springer (2024)
27. Teşeleanu, G.: A Generalized Wiener-type Attack Against an RSA-like Cryptosystem. In: CSCML. Lecture Notes in Computer Science, vol. ??, p. ?? Springer (2025)
28. Teşeleanu, G.: Partial Exposure Attacks Against a Family of RSA-like Cryptosystems. Cryptography **9**(1) (2025)
29. Wiener, M.J.: Cryptanalysis of Short RSA Secret Exponents. IEEE Trans. Inf. Theory **36**(3), 553–558 (1990)
30. Wong, D.: Lattice Based Attacks on RSA. https://github.com/mimoo/RSA-and-LLL-attacks
31. Zheng, M., Kunihiro, N., Hu, H.: Cryptanalysis of RSA Variants with Modified Euler Quotient. In: AFRICACRYPT 2018. Lecture Notes in Computer Science, vol. 10831, pp. 266–281. Springer (2018)