A Generalized Wiener-type Attack Against an RSA-like Cryptosystem

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 prime numbers p and q. In 2023, Cotan and Teşeleanu introduced a family of RSA-like cryptosystems based on the key equation $ed - k(p^n - 1)(q^n - 1) = 1$, where $n \geq 1$. Note that when $n = 1$, we obtain the classical RSA system, while $n = 2$ yields the variant proposed by Elkamchouchi, Elshenawy, and Shaban. In this paper, we present a novel attack that combines continued fractions with lattice-based methods for the case $n = 6$. This represents a natural continuation of previous research, which successfully applied similar techniques for $n = 1, 2, 4$.

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

1 Introduction

RSA, one of the most widely used cryptosystems, was introduced by Rivest, Shamir and Adleman in their 1978 paper [23]. The classical RSA scheme works using elements from the group $\mathbb{Z}_N^*$, where N is the product of two large prime numbers p and q. More precisely, to encrypt an element $m \in \mathbb{Z}_N^*$, we have to compute the ciphertext $c \equiv m^e \bmod N$, where e satisfies $\gcd(e, \varphi(N)) = 1$ and $\varphi(N) = (p-1)(q-1)$. To recover the original element, we simply compute $m \equiv c^d \bmod N$, where $d \equiv e^{-1} \bmod \varphi(N)$. The user's public key is (N, e), while (p, q, d) constitutes its secret key. In this paper, we focus only on primes that satisfy $q < p < 2q$ (*i.e.* have the same bit-size), further referred as balanced primes.

Over time, various attacks have been developed to extract the secret key d from the public key (N, e) under certain conditions. Wiener proved in [29] that if $d < N^{0.25}/3$, the secret key d can be recovered from the continued fraction expansion of e/N, hence enabling the factorization of N. Boneh and Durfee [4] improved this bound to $d < N^{0.292}$ using Coppersmith's method [8] and lattice reduction techniques [17]. Herrmann and May [14] later achieved the same bound with simpler methods. For an overview of RSA attacks, see [3, 19, 24].

Elkamchouchi, Elshenawy and Shaban [12] extended the RSA scheme to the ring of Gaussian integers modulo N. Such an integer modulo N has the form $a+bi$, where $a, b \in \mathbb{Z}_N$ and $i^2 = -1$. The set of all Gaussian integers modulo N is denoted by $\mathbb{Z}_N[i]$, and its group order is $\phi(N) = (p^2-1)(q^2-1)$. In this case, the

encryption exponent e satisfies $\gcd(e, \phi(N)) = 1$, and the decryption exponent d is computed as $d \equiv e^{-1} \bmod \phi(N)$. The encryption and decryption processes mirror those of RSA: for $m \in \mathbb{Z}_N[i]$, the ciphertext is $c \equiv m^e \bmod N$, and to recover m we compute $m \equiv c^d \bmod N$. Note that all operations are performed in the ring $\mathbb{Z}_N[i]$.

Elkamchouchi *et al.* [12] argued that their extension has better security compared to traditional RSA. However, Bunder [5] developed a Wiener-type continued fraction attack against this scheme. Using lattice reduction techniques, the authors of [22, 31] improved the bound to $d < N^{0.585}$. For more details on attacks against Elkamchouchi *et al.*'s scheme, see [10, 24].

The rings Z_p and $Z_p[i]$ can be rewritten as $Z_p = \mathbb{Z}_p[t]/(t+1) = GF(p)$ and $Z_p[i] = \mathbb{Z}_p[t]/(t^2+1) = GF(p^2)$, where GF stands for Galois field. Consequently, the underlying RSA group is $\mathbb{Z}_N = GF(p) \times GF(q)$, while in Elkamchouchi *et al.*'s case it is $\mathbb{Z}_N[i] = GF(p^2) \times GF(q^2)$. Using these observations, Cotan and Teşeleanu [10] generalized both schemes to $GF(p^n) \times GF(q^n)$ for $n \geq 1$. In this case, the group order is $\varphi_n(N) = (p^n - 1)(q^n - 1)$, while the encryption and decryption algorithms are direct extensions of RSA and Elkamchouchi *et al.*'s ones.

The motivation for this extension was to evaluate whether Wiener-type attacks apply to the generic setting. The authors of [10] proved that when $d < N^{0.25n}$, a continued fractions attack can always recover the secret exponent, regardless of n. This result was extended to unbalanced primes in [11]. The development of a lattice-based attack was left open in [10, 11], but it was subsequently resolved in [27], thus leading to a better attack bound. Other lattice attacks that could lead to factoring the modulus can be found in [28].

Related work. The first generalized Wiener attack was proposed in [1]. By combining continued fractions with Coppersmith's result, the authors showed that if the public exponent e satisfies

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

where

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

then we can factor N in polynomial time. Another generalized attack on RSA was proposed in [21]. More precisely, the author proved that if the public exponent e satisfies

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

where

$$1 \leq b < a < 2^{-\frac{1}{4}} N^{\frac{1}{4}}, \quad |u| < N^{\frac{1}{4}} \quad \text{and} \quad v = \left\lfloor -\frac{qu}{p-u} \right\rceil,$$

then we can factor N in polynomial time if all the prime factors of $p-u$ and $q-v$ are less than 10^{50}.

The case $n=2$ was studied in [6], where the authors proved that if the public exponent e satisfies

$$ae - b\varphi_2(N) = c,$$

then we can factor N in polynomial time if a, b and c satisfy a specific condition.

The final case, $n=4$, was tackled in [20]. More precisely, the authors proved that if the public exponent e satisfies

$$ae - b\varphi_4(N) = c,$$

where

$$ab < \frac{2N^4 - 49N^2 + 2}{170N^2 + 4N} \quad \text{and} \quad |c| < bN,$$

then we can factor N in polynomial time.

Our Contributions. In this paper, we continue the work started in [1, 6, 20] by developing a generalized Wiener attack for the case $n = 6$. The first step in developing such an attack is to find a good approximation $\hat{p}$ of p, such that we can apply a result due to Coppersmith to recover the actual value of p. To compute $\hat{p}$, we first use a continued fractions approximation to determine the terms a and b from the equation $ae - b\varphi_6(N) = c$. Then, we compute $\hat{p}$ as a function of a, b, and N. Once we know the attack's upper bound for d (from the equation $ed - k\varphi_6(N) = 1$), we can also derive a lower bound using a result from [20].

Structure of the Paper. Preliminary notions are provided in Section 2. In Section 3 we describe our attack. An example is given in Section 4 and we conclude our paper 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 Cubic Roots

We start this section by providing a solution to the depressed cubic equation $t^3 + Pt + Q$ (see [25]).

Theorem 2 (Cardano's Formula). *Given the depressed cubic $t^3 + Pt + Q$, one of its roots is given by*

$$\sqrt[3]{-\frac{Q}{2} + \sqrt{\frac{Q^2}{4} + \frac{P^3}{27}}} + \sqrt[3]{-\frac{Q}{2} - \sqrt{\frac{Q^2}{4} + \frac{P^3}{27}}}.$$

In one of our proofs, we also need an equivalent of $\sqrt{u} - \sqrt{v} < \sqrt{u \pm v} < \sqrt{u} + \sqrt{v}$ for cubic roots. Therefore, we prove such an equivalent.

Lemma 1. *Let $u > v > 0$. The following inequality holds*

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

Proof. Since $u > v > 0$ we have that

$$\begin{aligned}
(\sqrt[3]{u} - \sqrt[3]{v})^3 &= u - v - 3\sqrt[3]{uv}(\sqrt[3]{u} - \sqrt[3]{v}) < u - v, \\
(\sqrt[3]{u} + \sqrt[3]{v})^3 &= u + v + 3\sqrt[3]{uv}(\sqrt[3]{u} + \sqrt[3]{v}) > u + v,
\end{aligned}$$

which is equivalent to

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

just as desired. □

2.3 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 3. *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 4. *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 5 *The LLL reduced basis polynomials are algebraically independent*[1]*, and the resultant computations for* b_i *yield the common roots of these polynomials.*

[1] they do not share a non-trivial gcd

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 6. *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 we derive an attack that works for a given upper bound on small private exponents, the following result from [20] tells us that there exists an attack that works for a given lower bound on large private exponents. We refer the reader to [20] for results concerning φ_1, φ_2 and φ_4.

Theorem 7. *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 $d < \sqrt{\mathcal{B}_1}$.

2.4 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

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

2.5 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 study the generalized equation $ae - b\varphi_6(N) = c$, where e is a public exponent and c is known. Our attack consists of two steps: first, we compute a and b from a continued fraction expansion; then we find an appropriate approximation for p, and finally, we use Coppersmith's result to factor N. We begin with the lattice-based part of our attack and conclude with the continued fractions-based part.

3.1 Application of Lattices

Let $S = p + q$ and $D = p - q$. Using the value for φ_6 provided in [27], namely

$$\begin{aligned}\varphi_6 &= N^6 + 2N^3 - 9N^2S^2 + 6NS^4 - S^6 + 1 \\ &= N^6 - 2N^3 - 9N^2D^2 - 6ND^4 - D^6 + 1,\end{aligned}$$

we further derive some inequalities for $p + q$ and $p - q$.

Lemma 2. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Also, let e be a public exponent satisfying $ae - b\varphi_6(N) = c$ such that $|c| < bN\sqrt{N}$. We define $S = p + q$ and*

$$\hat{S} = \sqrt[3]{\frac{1}{2} \cdot \left(\sqrt{(N^3 + 1)^2 - \frac{ae}{b}} + \sqrt{(N^3 - 1)^2 - \frac{ae}{b}} \right)} + \beta,$$

where

$$\beta = \sqrt[3]{\frac{1}{2}\left(\sqrt{(N^3+1)^2 - \frac{ae-c}{b}} - \sqrt{(N^3-1)^2 - \frac{ae-c}{b}}\right)}.$$

Then the following holds

$$|S - \hat{S}| < N^{1/4}.$$

Proof. We first start by noticing that we can rewrite φ_6 as follows

$$\begin{aligned}\varphi_6 &= N^6 + 2N^3 - 9N^2S^2 + 6NS^4 - S^6 + 1\\ &= -S^2(S^4 - 6NS^2 + 9N^2) + (N^3+1)^2\\ &= -S^2(S^2 - 3N)^2 + (N^3+1)^2\\ &= -t^2 + (N^3+1)^2,\end{aligned}$$

where $t = S^3 - 3NS$.

On the other hand, we have that $\varphi_6(N) = (ae-c)/b$. Therefore, we have that

$$-t^2 + (N^3+1)^2 - \frac{ae-c}{b} = 0,$$

and we observe that

$$t = \sqrt{(N^3+1)^2 - \frac{ae-c}{b}}.$$

Therefore, S satisfies the equation

$$S^3 - 3NS - \sqrt{(N^3+1)^2 - \frac{ae-c}{b}} = 0.$$

Using Cardano's formula, we obtain that $S = \alpha + \beta$, where

$$\begin{aligned}\alpha &= \sqrt[3]{\frac{1}{2}\sqrt{(N^3+1)^2 - \frac{ae-c}{b}} + \sqrt{\frac{1}{4}\left((N^3+1)^2 - \frac{ae-c}{b}\right) - N^3}}\\ &= \sqrt[3]{\frac{1}{2}\left(\sqrt{(N^3+1)^2 - \frac{ae-c}{b}} + \sqrt{(N^3-1)^2 - \frac{ae-c}{b}}\right)}.\end{aligned}$$

Let

$$\hat{\alpha} = \sqrt[3]{\frac{1}{2}\sqrt{(N^3+1)^2 - \frac{ae}{b}} + \sqrt{\frac{1}{4}\left((N^3-1)^2 - \frac{ae}{b}\right)}}.$$

Using Lemma 1 and the fact that for positive integers $u > v > 0$ we have $\sqrt{u} - \sqrt{v} < \sqrt{u \pm v} < \sqrt{u} + \sqrt{v}$, we obtain the following

$$|\alpha - \hat{\alpha}| < \sqrt[3]{\frac{1}{2}\sqrt{\frac{|c|}{b}} + \frac{1}{2}\sqrt{\frac{|c|}{b}}} = \left(\frac{|c|}{b}\right)^{1/6}. \tag{1}$$

Using Equation (1), we obtain the following

$$|S - \hat{S}| = |\alpha + \beta - \hat{\alpha} - \beta| = |\alpha - \hat{\alpha}| \leq \left(\frac{|c|}{b}\right)^{1/6} < N^{1/4},$$

just as desired. □

Lemma 3. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Also, let e be a public exponent satisfying $ae - b\varphi_6(N) = c$ such that $|c| < bN\sqrt{N}$. We define $D = p - q$ and*

$$\hat{D} = \sqrt[3]{\frac{1}{2} \cdot \left(\sqrt{(N^3-1)^2 - \frac{ae}{b}} + \sqrt{(N^3+1)^2 - \frac{ae}{b}}\right)} - \beta,$$

where

$$\beta = \sqrt[3]{\frac{1}{2}\left(\sqrt{(N^3+1)^2 - \frac{ae-c}{b}} - \sqrt{(N^3-1)^2 - \frac{ae-c}{b}}\right)}.$$

Then the following holds

$$|D - \hat{D}| < N^{1/4}.$$

Proof. We first start by noticing that we can rewrite φ_6 as follows

$$\begin{aligned}
\varphi_6 &= N^6 - 2N^3 - 9N^2D^2 - 6ND^4 - D^6 + 1 \\
&= -D^2(D^4 + 6ND^2 + 9N^2) + (N^3 - 1)^2 \\
&= -D^2(D^2 + 3N)^2 + (N^3 - 1)^2 \\
&= -t^2 + (N^3 - 1)^2,
\end{aligned}$$

where $t = D^3 + 3ND$. Similarly to the proof of Lemma 2, we obtain that

$$t = \sqrt{(N^3-1)^2 - \frac{ae-c}{b}}.$$

Therefore, D satisfies the equation

$$D^3 + 3NS - \sqrt{(N^3-1)^2 - \frac{ae-c}{b}} = 0.$$

Using Cardano's formula, we obtain that $D = \alpha + (-\beta)$, where

$$\alpha = \sqrt[3]{\frac{1}{2}\left(\sqrt{(N^3-1)^2 - \frac{ae-c}{b}} + \sqrt{(N^3+1)^2 - \frac{ae-c}{b}}\right)},$$
$$-\beta = \sqrt[3]{\frac{1}{2}\left(\sqrt{(N^3-1)^2 - \frac{ae-c}{b}} - \sqrt{(N^3+1)^2 - \frac{ae-c}{b}}\right)}.$$

Similarly to the proof of Lemma 2 we obtain the following

$$|D - \hat{D}| < N^{1/4},$$

just as desired. □

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

Theorem 8. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Also, let e be a public exponent satisfying $ae - b\varphi_6(N) = c$ such that $|c| < bN\sqrt{N}$. Given e, N, a and b we can factor N in polynomial time.*

Proof. Using the approximation derived in Lemmas 2 and 3 we have that

$$\begin{aligned}\left|p - \frac{1}{2}(\hat{S} + \hat{D})\right| &= \left|\frac{1}{2}(S + D) - \frac{1}{2}(\hat{S} + \hat{D})\right| \\ &\leq \frac{1}{2}|S - \hat{S}| + \frac{1}{2}|D - \hat{D}| \\ &< \frac{1}{2}N^{1/4} + \frac{1}{2}N^{1/4} = N^{1/4}.\end{aligned}$$

Therefore,

$$\hat{p} = 0.5(\hat{S} + \hat{D}) = \sqrt[3]{\frac{1}{2} \cdot \left(\sqrt{(N^3-1)^2 - \frac{ae}{b}} + \sqrt{(N^3+1)^2 - \frac{ae}{b}}\right)}$$

is a good approximation of p. Now according to Theorem 6, we can factor N in polynomial time. □

3.2 Application of Continued Fractions

We start the section with the following lower and upper bounds for $p+q$ (see [6, Lemma 3]).

Lemma 4. *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 5. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Then the following property holds*

$$\left|9N^2S^2 - 6NS^4 + S^6 - 164N^3\right| < 550N^3$$

where $S = p + q$.

Proof. Using Lemma 4 we obtain that

$$2^2N < S^2 < 3^2N \quad 2^4N^2 < S^4 < 3^4N^2 \quad 2^6N^3 < S^6 < 3^6N^3.$$

Let $A = 9N^2S^2 - 6NS^4 + S^6$. Therefore, we have

$$-386N^3 = (9 \cdot 2^2 - 6 \cdot 3^4 + 2^6)N^3 < A < (9 \cdot 3^2 - 6 \cdot 2^4 + 3^6)N^3 = 714N^3.$$

Thus, we obtain

$$-550N^3 = -386N^3 - 164N^3 < A - 164N^3 < 714N^3 - 164N^3 = 550N^3,$$

just as desired. □

Theorem 9. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Also, let e be a public exponent satisfying $ae - b\varphi_6(N) = c$ such that $|c| < bN\sqrt{N}$. Given e, N we can factor N in polynomial time if*

$$ab < \frac{N^6 - 162N^3 + 1}{2N\sqrt{N} + 1100N^3}.$$

Proof. We denote by

$$A = 9N^2S^2 - 6NS^4 + S^6 - 164N^3.$$

We know that

$$ae - b\left(N^6 + 2N^3 - A - 164N^3 + 1\right) = c$$

which is equivalent to

$$ae - b\left(N^6 - 162N^3 + 1\right) = c - bA.$$

Dividing everything by $a(N^6 - 162N^3 + 1)$ we obtain

$$\frac{e}{N^6 - 162N^3 + 1} - \frac{b}{a} = \frac{c - bA}{a(N^6 - 162N^3 + 1)}.$$

Taking the absolute value we obtain

$$\begin{aligned}\left|\frac{e}{N^6-162N^3+1}-\frac{b}{a}\right| &\leq \frac{|c|+|bA|}{a(N^6-162N^3+1)}\\ &\leq \frac{N\sqrt{N}+|A|}{N^6-162N^3+1}\cdot\frac{b}{a}\\ &\leq \frac{N\sqrt{N}+550N^3}{N^6-162N^3+1}\cdot\frac{b}{a}\\ &< \frac{1}{2ab}\cdot\frac{b}{a}=\frac{1}{2a^2}.\end{aligned}$$

where for the third inequality we used Lemma 5 and for the last inequality we used our hypothesis. Since

$$\left|\frac{e}{N^6-162N^3+1}-\frac{b}{a}\right|<\frac{1}{2a^2}.$$

then according to Theorem 1 b/a appears among the convergents of $e/(N^6-162N^3+1)$. Once we obtain a and b we apply Theorem 8, and thus we conclude our proof. □

To conclude, we further apply our generic result to the RSA-like cryptosystem with $n=6$. Note that for the second corollary we use Theorem 7.

Corollary 1. *Let $N=pq$ be the product of two unknown primes with $q<p<2q$. Also, let $e<\varphi_6(N)$ be a public exponent satisfying $ed-k\varphi_6(N)=1$. Given e, N we can factor N in polynomial time if*

$$d<\sqrt{\frac{N^6-162N^3+1}{2N\sqrt{N}+1100N^3}}.$$

Proof. We notice that

$$k=\frac{ed-1}{\varphi_6(N)}<\frac{ed}{\varphi_6(N)}<d$$

and

$$kd<d^2<\frac{N^6-162N^3+1}{2N\sqrt{N}+1100N^3}$$

According to Theorem 9 we can factor N in polynomial time. □

Corollary 2. *Let $N=pq$ be the product of two unknown primes with $q<p<2q$. Also, let $e<\varphi_6(N)$ be a public exponent satisfying $ed-k\varphi_6(N)=1$. Given e, N we can factor N in polynomial time if*

$$d>\varphi_6(N)-\sqrt{\frac{N^6-162N^3+1}{2N\sqrt{N}+1100N^3}}.$$

4 Experimental Results

To check the validity of our result, we ran the code for our attack [26] on a workstation using Ubuntu 20.04.1, with the following specifications: Intel(R) Core(TM) i7-1165G7 CPU 2.80GHz with 8 cores and 16 Gigabytes of RAM. The programming language we used for implementing our attack was SageMath 10.3. We based our code on the Coppersmith attack implementation found in [30].

We used the following parameters

$$
\begin{aligned}
N = {} & 34896555885991965979987277815642836819600382610384937637 31,\\
e = {} & 64887895311260797429337117325274093239555004850028011671287555160 6\\
& 46758056488111885840989403372618071232564916245022855580340245150 9\\
& 64243048689414213285611982982901144618110895707754416430711150763 1\\
& 78550595361948248638494393457612477786440539836133785922870877845 8\\
& 36196719794863532512659286006619894864080811569114018915410751083 5\\
& 437673068035277.
\end{aligned}
$$

Computing the continued fraction expansion of $e/(N^6 - 162N^3 + 1)$, we get the first 25 partial quotients

$$[0, 2, 1, 3, 1, 1, 1, 1, 3, 10, 7, 1, 3, 2, 12, 1, 11, 1, 9, 1, 2, 2, 2, 5, 2, \ldots].$$

Looking at the $87th$ convergent we obtain

$$
\begin{aligned}
a &= 11150372599265311570767859136324180752990213\\
b &= 40064310154513261257270992156604492130226 40,
\end{aligned}
$$

which satisfy the condition of Theorem 9. Therefore, we obtain the following approximation of p

$$\hat{p} = 13228752329477646386492218774 0.$$

Using Coppersmith's algorithm we find

$$p = 13228752329477646386492218774 1,$$

and then we can compute

$$q = N/p = 26379325137285943549540377391.$$

5 Conclusions

In this paper, we presented a generalized Wiener-type attack against RSA-like cryptosystems. To mount our attack, we first study the general equation $ae - b\varphi_6(N) = c$, after which we apply a result proven by Coppersmith [2, 8]. As a result, we show that if d is either small or very large, one can factor N in polynomial time.

Future work. It would be interesting to develop a generic method that works for $\varphi_i(N)$ for any i, not just particular cases (*i.e.* for $n = 1, 2, 4, 6$).

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. Tao, Y.: Polynomials I - The Cubic Formula. https://circles.math.ucla.edu/circles/lib/data/Handout-3357-2927.pdf
26. 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
27. 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)
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)