A Generalized Wiener-type Attack Against a Family RSA-like Cryptosystems

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 scheme, 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 $n = 2^i$, where $i > 2$ is an integer. 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

One of the most well-known public-key encryption schemes is RSA, introduced in 1978 by Rivest, Shamir, and Adleman [23]. Its security is closely tied to the computational difficulty of factoring a modulus N, where N is the product of two large prime numbers p and q. To encrypt a message $m \in \mathbb{Z}_N$, the sender uses the recipient's public key (N, e) and computes the ciphertext as $c \equiv m^e \bmod N$. Here, the exponent e is chosen such that $\gcd(e, \varphi(N)) = 1$, where $\varphi(N) = (p-1)(q-1)$. To decrypt the ciphertext, the recipient uses their private key (p, q, d) and computes $m \equiv c^d \bmod N$. For decryption to succeed, the private exponent must satisfy $d \equiv e^{-1} \bmod \varphi(N)$. Throughout this paper, we restrict our attention to balanced primes, *i.e.* primes satisfying $q < p < 2q$.

Numerous cryptanalytic techniques have been developed to recover the private key d from the public key under certain conditions. For example, Wiener [29] showed that if $d < N^{0.25}/3$, then d can be efficiently recovered from the continued fractions expansion of e/N, thereby compromising the security of RSA. This bound was subsequently improved by Boneh and Durfee [4], who employed Coppersmith's method [8] in conjunction with lattice basis reduction algorithms [17] to extend the attack to cases where $d < N^{0.292}$. Later, Herrmann and May [14] obtained the same bound using a simpler approach. For comprehensive surveys of attacks on RSA, we refer the reader to [3, 19, 24].

An extension of RSA to the ring of Gaussian integers modulo N was latter proposed by Elkamchouchi, Elshenawy and Shaban [12]. In this setting, integers

take the form $a + bi$, where $a, b \in \mathbb{Z}_N$ and $i^2 = -1$. The corresponding ring is denoted $\mathbb{Z}_N[i]$, and has cardinality $\phi(N) = (p^2 - 1)(q^2 - 1)$. As in classical RSA, encryption of a message $m \in \mathbb{Z}_N[i]$ is achieved via $c \equiv m^e \bmod N$, where e satisfies $\gcd(e, \phi(N)) = 1$, and decryption is given by $m \equiv c^d \bmod N$ with $d \equiv e^{-1} \bmod \phi(N)$. All computations are performed within the ring $\mathbb{Z}_N[i]$.

Although Elkamchouchi *et al.* claimed enhanced security for their scheme, Bunder *et al.* [5] introduced a continued fraction-based attack similar to Wiener's method, and thus showed that the extension remains vulnerable under this class of attacks. Their attack was later improved to $d < N^{0.585}$ through the application of lattice reduction techniques [22,31]. For further cryptanalytic results targeting this variant, see [10, 24].

From an algebraic perspective, the rings $\mathbb{Z}_p$ and $\mathbb{Z}_p[i]$ can be interpreted respectively as $\mathbb{Z}_p = \mathbb{Z}_p[t]/(t + 1) = GF(p)$ and $\mathbb{Z}_p[i] = \mathbb{Z}_p[t]/(t^2 + 1) = GF(p^2)$, where GF denotes a Galois field. Consequently, the group structure in standard RSA corresponds to $\mathbb{Z}_N = GF(p) \times GF(q)$, while in the Gaussian integer variant it becomes $\mathbb{Z}_N[i] = GF(p^2) \times GF(q^2)$. Leveraging this insight, Cotan and Teşeleanu [10] proposed a further generalization to the product ring $GF(p^n) \times GF(q^n)$ for arbitrary integers $n \geq 1$. The order of the resulting group is given by $\varphi_n(N) = (p^n - 1)(q^n - 1)$, and both the encryption and decryption procedures extend naturally from the prior schemes.

This generalization was primarily motivated by the desire to assess whether Wiener-type attacks remain effective in this broader context. Cotan and Teşeleanu [10] established that for any $n \geq 1$, if $d < N^{0.25n}$, then the continued fraction approach can successfully recover the decryption exponent. This result was later extended to accommodate unbalanced prime moduli in [11]. Although the existence of lattice-based attacks in this generalized setting was initially an open question, it was subsequently addressed in [25], leading to improved bounds. Additional techniques for partial key exposure and factorization based on lattice reduction 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

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

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.

When $n = 3$ the author of [27] obtained that we can factor N if the public exponent e satisfies

$$ae - b\varphi_3(N) = c,$$

where

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

and certain restrictions on p, q and c hold.

The 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.

The final case found in the literature is $n = 6$ [26]. In this case, we can factor N if the public exponent e satisfies

$$ae - b\varphi_6(N) = c,$$

where

$$ab < \frac{N^6 - 162N^3 + 1}{2N\sqrt{N} + 1100N^3} \quad \text{and } |c| < bN\sqrt{N}.$$

Our Contributions. In this paper, we continue the work started in [1, 6, 20] by developing a generalized Wiener attack for the case $n = 2^i$, where $i > 2$ is an integer. To illustrate the general pattern of the attack, we provide two worked examples for $n = 8$ and $n = 16$. As a special case, our method recovers the results previously established in [20]. To aid us in constructing our attack, we also developed exact formulas for computing φ_n as a polynomial in N and $p+q$, thereby complementing earlier work, which had shown that φ_n is a polynomial with integer coefficients in N and $p+q$, and had provided a recurrence relation for its computation.

Structure of the Paper. Preliminary notions are provided in Section 2. In Section 3 we take a new look at the group's order, while in Section 4 we describe our attack. Some examples are given in Section 4.3 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 $\zeta = [a_0, a_1, a_2, \ldots]$. Note 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 $(y_1, \ldots, y_n)$ when $n \geq 2$, we need the following standard heuristic assumption to hold [4,19].

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.*

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

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 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

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

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 New Look at φ_n

The next two results [25] show that $\varphi_n(N)$ can be expressed as a polynomial in $p + q$ with integer coefficients, and also provide a recurrence relation for $\varphi_n(N)$ in terms of N and $S = p + q$.

Proposition 1. *Let N be a positive integer. Then for any integers $n \geq 1$ the following property holds*

$$\varphi_n(N) = -(p+q)^n + \sum_{k=0}^{n-1} a_k (p+q)^k,$$

where $a_k \in \mathbb{Z}$.

Lemma 1. *Let $N = pq$ and $S = p + q$ be two positive integers. Then for any integers $n \geq 2$ the following property holds*

$$\varphi_n(N) = (N^{n-1} + 1)(N - S + 1) + S\varphi_{n-1}(N) - N\varphi_{n-2}(N),$$

where $\varphi_0(N) = 0$ and $\varphi_1(N) = N - S + 1$.

Compared to the two previous results, in this section, we provide an exact formula for $\varphi_n(N)$ in terms of N and $S = p+q$. When n is even, we also provide a formula in terms of N and $D = p - q$. These formulas will later be used to approximate S and D.

Lemma 2. *Let n be an integer and $k = \lfloor n/2 \rfloor$. For integers p and q the following property holds*

$$p^n + q^n = (p+q)^n + \sum_{i=1}^{k} \frac{n}{i} \cdot \binom{n-i-1}{i-1} \cdot (p+q)^{n-2i} \cdot (-N)^i,$$

where $N = pq$.

Proof. When note that the following relations hold

$$\begin{aligned}
p^1 + q^1 &= p + q \\
p^2 + q^2 &= (p+q)^2 - 2N \\
p^3 + q^3 &= (p+q)^3 - 3N(p+q) \\
p^4 + q^4 &= (p+q)^4 - 4N(p+q)^2 + 2N^2.
\end{aligned}$$

We assume that the relation holds for $n-1$ and $n-2$ and and we prove it for n. First we assume that $n = 2k$. Therefore, we have

$$\begin{aligned}
p^n + q^n &= (p+q)(p^{n-1} + q^{n-1}) - N(p^{n-2} + q^{n-2}) \\
&= (p+q)\left((p+q)^{n-1} + \sum_{i=1}^{k-1} \frac{n-1}{i} \cdot \binom{n-i-2}{i-1} \cdot (p+q)^{n-1-2i} \cdot (-N)^i\right) \\
&- N\left((p+q)^{n-2} + \sum_{i=1}^{k-1} \frac{n-2}{i} \cdot \binom{n-i-3}{i-1} \cdot (p+q)^{n-2-2i} \cdot (-N)^i\right) \\
&= (p+q)^n + \sum_{i=1}^{k-1} \frac{n-1}{i} \cdot \binom{n-i-2}{i-1} \cdot (p+q)^{n-2i} \cdot (-N)^i \\
&- N(p+q)^{n-2} + \sum_{i=2}^{k} \frac{n-2}{i-1} \cdot \binom{n-i-2}{i-2} \cdot (p+q)^{n-2i} \cdot (-N)^i \\
&= (p+q)^n - nN(p+q)^{n-2} + 2 \cdot (-N)^2 \\
&+ \sum_{i=2}^{k-1} \left(\frac{n-1}{i} \cdot \binom{n-i-2}{i-1} + \frac{n-2}{i-1} \cdot \binom{n-i-2}{i-2}\right)(p+q)^{n-2i} \cdot (-N)^i.
\end{aligned}$$

Rewriting the term for $(p+q)^{n-2i} \cdot (-N)^i$ we obtain

$$\begin{aligned}
&\frac{n-1}{i} \cdot \binom{n-i-2}{i-1} + \frac{n-2}{i-1} \cdot \binom{n-i-2}{i-2} \\
&= \frac{n-1}{i} \cdot \frac{(n-i-2)!}{(i-1)!(n-2i-1)!} + \frac{n-2}{i-1} \cdot \frac{(n-i-2)!}{(i-2)!(n-2i)!} \\
&= \frac{(n-i-2)!}{(i-1)!(n-2i-1)!} \cdot \left(\frac{n-1}{i} + \frac{n-2}{n-2i}\right) \\
&= \frac{(n-i-2)!}{i!(n-2i)!} \cdot (n^2 - 2in - n + 2i + in - 2i) \\
&= \frac{n}{i} \cdot \frac{(n-i-1)!}{(i-1)!(n-2i)!} = \frac{n}{i} \cdot \binom{n-i-1}{i-1}, \qquad (1)
\end{aligned}$$

just as desired.

Now we assume that $n = 2k+1$. Therefore, we have

$$p^n + q^n = (p+q)\left((p+q)^{n-1} + \sum_{i=1}^{k} \frac{n-1}{i} \cdot \binom{n-i-2}{i-1} \cdot (p+q)^{n-1-2i} \cdot (-N)^i\right)$$

$$
\begin{aligned}
&- N\left((p+q)^{n-2} + \sum_{i=1}^{k-1} \frac{n-2}{i} \cdot \binom{n-i-3}{i-1} \cdot (p+q)^{n-2-2i} \cdot (-N)^i\right) \\
&= (p+q)^n + \sum_{i=1}^{k} \frac{n-1}{i} \cdot \binom{n-i-2}{i-1} \cdot (p+q)^{n-2i} \cdot (-N)^i \\
&- N(p+q)^{n-2} + \sum_{i=2}^{k} \frac{n-2}{i-1} \cdot \binom{n-i-2}{i-2} \cdot (p+q)^{n-2i} \cdot (-N)^i \\
&= (p+q)^n - nN(p+q)^{n-2} \\
&+ \sum_{i=2}^{k} \left(\frac{n-1}{i} \cdot \binom{n-i-2}{i-1} + \frac{n-2}{i-1} \cdot \binom{n-i-2}{i-2}\right) (p+q)^{n-2i} \cdot (-N)^i.
\end{aligned}
$$

Using Equation (1) we obtain our desired result. □

Using the definition of φ_n and Lemma 2 we obtain the following value for φ_n as a polynomial in N and $p+q$.

Corollary 1. *Let $N = pq$ and $S = p + q$ be two positive integers. Then the following property holds*

$$\varphi_n(N) = N^n + 1 - S^n - \sum_{i=1}^{k} \frac{n}{i} \cdot \binom{n-i-1}{i-1} \cdot S^{n-2i} \cdot (-N)^i.$$

When n is even we can rewrite φ_n as

$$\varphi_n(N) = (N^k - (-1)^k)^2 - S^n - \sum_{i=1}^{k-1} \frac{n}{i} \cdot \binom{n-i-1}{i-1} \cdot S^{n-2i} \cdot (-N)^i.$$

If we change q with $-q$ in Lemma 2 we obtain the following corollary.

Corollary 2. *Let $n = 2k$. For integers p and q the following property holds*

$$p^n + q^n = (p-q)^n + \sum_{i=1}^{k} \frac{n}{i} \cdot \binom{n-i-1}{i-1} \cdot (p-q)^{n-2i} \cdot N^i,$$

where $N = pq$.

When n is even, using the definition of φ_n and Corollary 2 we obtain the following value for φ_n as a polynomial in N and $p-q$.

Corollary 3. *Let $N = pq$ and $D = p - q$ be two positive integers. Then the following property holds*

$$\varphi_n(N) = (N^k - 1)^2 - D^n - \sum_{i=1}^{k-1} \frac{n}{i} \cdot \binom{n-i-1}{i-1} \cdot D^{n-2i} \cdot N^i.$$

4 A Generalized Wiener-type Attack

In this section, we study the generalized equation $ae - b\varphi_{2^i}(N) = c$, 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.

4.1 Application of Lattices

The main hurdle in developing our attack is to find a good approximation for $p \pm q$. Therefore, we start with the case $i = 3, 4$ and show how to find one for $p+q$. Once our intuition is formed, we provide a general approximation for $p+q$ when $i > 2$. Based on this, we further give a good approximation for $p-q$. Once we have these two results, we can derive an approximation of p that allows us to use Coppersmith's result.

4.1.1 Case $i = 3$

Let $S = p + q$. Using the value for φ_8 proved in Corollary 1, namely

$$\varphi_8 = N^8 - S^8 + 8NS^6 - 20N^2S^4 + 16N^3S^2 - 2N^4 + 1,$$

we further derive approximations for $p + q$.

Lemma 3 (Approximation of $p + q$). *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Also, let e be a public exponent satisfying $ae - b\varphi_8(N) = c$ such that $|c| < bN^2$. We define $S = p + q$ and*

$$\hat{S} = \sqrt{2N + \sqrt{2N^2 + \sqrt{(N^4+1)^2 - \frac{ae}{b}}}}.$$

Then the following holds

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

Proof. We first start by noticing that we can rewrite φ_8 as follows

$$\begin{aligned}
\varphi_8 &= N^8 - 2N^4 + 16N^3S^2 - 20N^2S^4 + 8NS^6 - S^8 + 1 \\
&= -(S^8 - 8NS^6 + 16N^2S^4) + 4N^2(-S^4 + 4NS^2) + (N^4 - 1)^2 \\
&= -(S^4 - 4NS^2)^2 - 4N^2(S^4 - 4NS^2) + (N^4 - 1)^2 \\
&= -t^2 - 4N^2t + (N^4 - 1)^2,
\end{aligned}$$

where $t = S^4 - 4NS^2$.

On the other hand, we have that $\varphi_8(N) = (ae - c)/b$. Therefore, we have that

$$-t^2 - 4N^2t + (N^4 - 1)^2 - \frac{ae - c}{b} = 0.$$

We compute the discriminant

$$\Delta = 16N^4 + 4\left((N^4 - 1)^2 - \frac{ae - c}{b}\right) = 4\left((N^4 + 1)^2 - \frac{ae - c}{b}\right) \geq 0$$

and we obtain that

$$t = -2N^2 + \sqrt{(N^4 + 1)^2 - \frac{ae - c}{b}}.$$

Therefore, S satisfies the equation

$$-S^4 + 4NS^2 - 2N^2 + \sqrt{(N^4 + 1)^2 - \frac{ae - c}{b}} = 0.$$

We again compute the discriminant

$$\begin{aligned}\Delta' &= 16N^2 + 4\left(-2N^2 + \sqrt{(N^4 + 1)^2 - \frac{ae - c}{b}}\right) \\ &= 4\left(2N^2 + \sqrt{(N^4 + 1)^2 - \frac{ae - c}{b}}\right) \geq 0\end{aligned}$$

and we obtain that

$$S^2 = 2N + \sqrt{2N^2 + \sqrt{(N^4 + 1)^2 - \frac{ae - c}{b}}}.$$

Therefore, we have

$$S = \sqrt{2N + \sqrt{2N^2 + \sqrt{(N^4 + 1)^2 - \frac{ae - c}{b}}}}.$$

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

$$|S - \hat{S}| < \left(\frac{|c|}{b}\right)^{1/8} < N^{1/4},$$

just as desired. □

4.1.2 Case $i = 4$

Now we look at the case $n = 16$, where according to Corollary 1 we have

$$\begin{aligned}\varphi_{16} = N^{16} &- 2N^8 + 64N^7S^2 - 336N^6S^4 + 672N^5S^6 - 660N^4S^8 \\ &+ 352N^3S^{10} - 104N^2S^{12} + 16NS^{14} - S^{16} + 1.\end{aligned}$$

Lemma 4 (Approximation of $p + q$). *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Also, let e be a public exponent satisfying $ae - b\varphi_{16}(N) = c$ such that $|c| < bN^4$. We define $S = p + q$ and*

$$\hat{S} = \sqrt{2N + \sqrt{2N^2 + \sqrt{2N^4 + \sqrt{(N^8+1)^2 - \frac{ae}{b}}}}}.$$

Then the following holds

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

Proof. We first start by noticing that we can rewrite φ_8 as follows

$$\begin{aligned}\varphi_{16} &= N^{16} - 2N^8 + 64N^7S^2 - 336N^6S^4 + 672N^5S^6 - 660N^4S^8 \\ &\quad + 352N^3S^{10} - 104N^2S^{12} + 16NS^{14} - S^{16} + 1 \\ &= -(S^4 - 4NS^2 + 2N^2)^4 + 4N^4(S^4 - 4NS^2 + 2N^2)^2 + (N^8 - 1)^2 \\ &= -t^2 + 4N^4t + (N^8 - 1)^2,\end{aligned}$$

where $t = (S^4 - 4NS^2 + 2N^2)^2$.

On the other hand, we have that $\varphi_{16}(N) = (ae - c)/b$. Therefore, we have that

$$-t^2 + 4N^4t + (N^8 - 1)^2 - \frac{ae - c}{b} = 0.$$

We compute the discriminant

$$\Delta = 16N^8 + 4\left((N^8 - 1)^2 - \frac{ae - c}{b}\right) = 4\left((N^8 + 1)^2 - \frac{ae - c}{b}\right) \geq 0$$

and we obtain that

$$t = 2N^4 + \sqrt{(N^8 + 1)^2 - \frac{ae - c}{b}}.$$

Therefore, S satisfies the equation

$$S^4 - 4NS^2 + 2N^2 - \sqrt{2N^4 + \sqrt{(N^8 + 1)^2 - \frac{ae - c}{b}}} = 0.$$

We again compute the discriminant

$$\Delta' = 16N^2 + 4\left(-2N^2 + \sqrt{2N^4 + \sqrt{(N^8+1)^2 - \frac{ae-c}{b}}}\right)$$
$$= 4\left(2N^2 + \sqrt{2N^4 + \sqrt{(N^8+1)^2 - \frac{ae-c}{b}}}\right) \geq 0$$

and we obtain that

$$S^2 = 2N + \sqrt{2N^2 + \sqrt{2N^4 + \sqrt{(N^8+1)^2 - \frac{ae-c}{b}}}}.$$

Therefore, we have

$$S = \sqrt{2N + \sqrt{2N^2 + \sqrt{2N^4 + \sqrt{(N^8+1)^2 - \frac{ae-c}{b}}}}}.$$

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

$$|S - \hat{S}| < \left(\frac{|c|}{b}\right)^{1/16} < N^{1/4},$$

just as desired. □

4.1.3 General Case

Taking a closer look at the results presented in [20] and Sections 4.1.1 and 4.1.2 we start to see a pattern for $\widehat{p+q}$. We sum up all known results in Table 1.

	$\widehat{p+q}$	$\lvert c\rvert$
$n=4$	$\sqrt{2N + \sqrt{(N^2+1)^2 - \frac{ae}{b}}}$	$\lvert c\rvert < bN$
$n=8$	$\sqrt{2N + \sqrt{2N^2 + \sqrt{(N^4+1)^2 - \frac{ae}{b}}}}$	$\lvert c\rvert < bN^2$
$n=16$	$\sqrt{2N + \sqrt{2N^2 + \sqrt{2N^4 + \sqrt{(N^8+1)^2 - \frac{ae}{b}}}}}$	$\lvert c\rvert < bN^4$

Table 1. Summary on approximations.

We formally provide a good approximation for $p \pm q$ in the following theorems. In the proofs, we make use of the fact that φ_n can be written as a polynomial in pq and $p+q$ (Corollary 1), and, when n is even, as a polynomial in pq and $p-q$ (Corollary 3).

Theorem 7. *Let $N = pq$ and $S = p+q$ be the product and sum of two unknown primes with $q < p < 2q$. Also, let e be a public exponent satisfying $ae - b\varphi_{2^i}(N) = c$. Then*

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

Proof. We already know that when $i = 2, 3, 4$ (see Table 1) S has the needed form. We further assume that the relation holds for i and we prove it for $i+1$. We denote by $S_{2^i}(N)$ and $S_{2^{i+1}}(N)$ the corresponding sums. In order to do that, we first observe that

$$\begin{aligned}
\varphi_{2^{i+1}}(p,q) &= N^{2^{i+1}} - p^{2^{i+1}} - q^{2^{i+1}} + 1 \\
&= (N^2)^{2^i} - (p^2)^{2^i} - (q^2)^{2^i} + 1 \\
&= \varphi_{2^i}(p^2, q^2).
\end{aligned}$$

Since φ is a polynomial in pq and $p+q$ we get that

$$\begin{aligned}
\varphi_{2^{i+1}}(N, S_{2^{i+1}}(N)) &= \varphi_{2^{i+1}}(pq, p+q) \\
&= \varphi_{2^{i+1}}(p,q) \\
&= \varphi_{2^i}(p^2, q^2) \\
&= \varphi_{2^i}((pq)^2, p^2+q^2) \\
&= \varphi_{2^i}((pq)^2, (p+q)^2 - 2pq) \\
&= \varphi_{2^i}(N^2, (S_{2^{i+1}}(N))^2 - 2N).
\end{aligned}$$

Since $S_{2^i}(N^2)$ and $S_{2^{i+1}}(N)$ are obtained as x solutions of $\varphi_{2^i}(N^2, x) = (ae-c)/b$ and $\varphi_{2^{i+1}}(N, x) = \varphi_{2^i}(N^2, x^2 - 2N) = (ae-c)/b$, we obtain that $S_{2^i}(N^2) = (S_{2^{i+1}}(N))^2 - 2N$. This leads to

$$\begin{aligned}
S_{2^{i+1}}(N) &= \sqrt{2N + S_{2^i}(N^2)} \\
&= \sqrt{2N + \sqrt{2N^2 + \sqrt{\ldots \sqrt{2N^{2^{i-1}} + \sqrt{(N^{2^i} + 1)^2 - \frac{ae-c}{b}}}}}},
\end{aligned}$$

where for the second equality we used the induction step. This concludes our proof. □

Theorem 8. *Let $N = pq$ and $D = p - q$ be the product and difference of two unknown primes with $q < p < 2q$. Also, let e be a public exponent satisfying $ae - b\varphi_{2^i}(N) = c$. Then*

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

Proof. For a given i we denote by $D_{2^i}(N)$ and $S_{2^i}(N)$ the corresponding difference and sum. We first observe that

$$\varphi_{2^i}(N, D_{2^i}(N)) = \varphi_{2^i}(p, q) = \varphi_{2^i}(p, -q) = \varphi_{2^i}(-N, S_{2^i}(-N)).$$

Since $D_{2^i}(N)$ and $S_{2^i}(-N)$ are obtained as x solutions of $\varphi_{2^i}(N, x) = (ae - c)/b$ and $\varphi_{2^i}(-N, x) = (ae - c)/b$, we obtain that

$$D_{2^i}(N) = S_{2^i}(-N) = \sqrt{-2N + \sqrt{2N^2 + \sqrt{\dots \sqrt{2N^{2^{i-2}} + \sqrt{(N^{2^{i-1}} + 1)^2 - \frac{ae - c}{b}}}}}},$$

just as desired. □

Using Theorems 7 and 8 we can derive good approximations for S and D. We only provide the proof for $\hat{S}$, since the one for $\hat{D}$ is similar.

Corollary 4 (Approximation of $p + q$). *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Also, let e be a public exponent satisfying $ae - b\varphi_{2^i}(N) = c$ such that $|c| < bN^{2^{i-2}}$. We define $S = p + q$ and*

$$\hat{S} = \sqrt{2N + \sqrt{2N^2 + \sqrt{\dots \sqrt{2N^{2^{i-2}} + \sqrt{(N^{2^{i-1}} + 1)^2 - \frac{ae}{b}}}}}}.$$

Then the following holds

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

Proof. Using Theorem 7 and the fact that for positive integers u and v we have $\sqrt{u} - \sqrt{v} < \sqrt{u \pm v} < \sqrt{u} + \sqrt{v}$, we obtain the following

$$|S - \hat{S}| < \left(\frac{|c|}{b}\right)^{1/2^i} < N^{1/4},$$

just as desired. □

Corollary 5 (Approximation of $p-q$). *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Also, let e be a public exponent satisfying $ae - b\varphi_{2^i}(N) = c$ such that $|c| < bN^{2^{i-2}}$. We define $D = p - q$ and*

$$\hat{D} = \sqrt{-2N + \sqrt{2N^2 + \sqrt{\dots \sqrt{2N^{2^{i-2}} + \sqrt{(N^{2^{i-1}}+1)^2 - \frac{ae}{b}}}}}}.$$

Then the following holds

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

Once we know that $\hat{S}$ and $\hat{D}$ are good approximations, we can derive the following result.

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

Proof. Using the approximation derived in Corollaries 4 and 5 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, $\hat{p} = 0.5(\hat{S} + \hat{D})$ is a good approximation of p. Now according to Theorem 5, we can factor N in polynomial time. □

4.2 Application of Continued Fractions

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

Lemma 5. *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 a useful bound for the continued fraction part of our attack.

Lemma 6. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Let $n = 2^i$ and*

$$L = -3^n + \sum_{\substack{j=1 \\ j=j+2}}^{2^{i-1}-1} \frac{n}{j} \cdot \binom{n-j-1}{j-1} \cdot 2^{n-2j} - \sum_{\substack{j=2 \\ j=j+2}}^{2^{i-1}-2} \frac{n}{j} \cdot \binom{n-j-1}{j-1} \cdot 3^{n-2j},$$

$$U = -2^n + \sum_{\substack{j=1 \\ j=j+2}}^{2^{i-1}-1} \frac{n}{j} \cdot \binom{n-j-1}{j-1} \cdot 3^{n-2j} - \sum_{\substack{j=2 \\ j=j+2}}^{2^{i-1}-2} \frac{n}{j} \cdot \binom{n-j-1}{j-1} \cdot 2^{n-2j},$$

where $j = j + 2$ denotes incrementing the index j by 2. Then the following property holds

$$\left| \varphi_{2^i}(N) - (N^{2^{i-1}} - 1)^2 - \frac{L+U}{2} N^{2^{i-1}} \right| < \frac{U-L}{2} N^{2^{i-1}}$$

where $S = p + q$.

Proof. Using Lemma 5 we obtain that

$$2^j N^{j/2} < S^j < 3^j N^{j/2}.$$

Plugging this into Corollary 1 we obtain that

$$LN^{2^{i-1}} < \varphi_n(N) - (N^{2^{i-1}} - 1)^2 < UN^{2^{i-1}},$$

which is equivalent to

$$-\frac{U-L}{2} N^{2^{i-1}} = \left(L - \frac{L+U}{2} \right) N^{2^{i-1}} < \varphi_{2^i}(N) - (N^{2^{i-1}} - 1)^2 - \frac{L+U}{2} N^{2^{i-1}}$$

and

$$\varphi_{2^i}(N) - (N^{2^{i-1}} - 1)^2 - \frac{L+U}{2} N^{2^{i-1}} < \left(U - \frac{L+U}{2} \right) N^{2^{i-1}} = \frac{U-L}{2} N^{2^{i-1}},$$

just as desired. □

Once we have a bound on $\varphi_n(N) - (N^n - 1)^2$ we derive the continued fraction part of our attack.

Theorem 10. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Also, let e be a public exponent satisfying $ae - b\varphi_{2^i}(N) = c$ such that $|c| < bN^{2^{i-2}}$. Given e, N we can factor N in polynomial time if*

$$ab < \frac{2N^{2^i} + (L+U-4)N^{2^{i-1}} + 2}{2(U-L)N^{2^{i-1}} + 4N^{2^{i-2}}}.$$

Proof. We denote by

$$C = \varphi_{2^i}(N) - (N^{2^{i-1}} - 1)^2 - \frac{L+U}{2} N^{2^{i-1}}$$

We know that

$$ae - b\left(N^{2^i} - 2N^{2^{i-1}} + C + \frac{L+U}{2} N^{2^{i-1}} + 1\right) = c$$

which is equivalent to

$$ae - b\left(N^{2^i} + \frac{L+U-4}{2} N^{2^{i-1}} + 1\right) = c + bC.$$

Dividing everything by $a(N^{2^i} + (L+U-4)N^{2^{i-1}}/2 + 1)$ we obtain

$$\begin{aligned}
\left| \frac{2e}{2N^{2^i} + (L+U-4)N^{2^{i-1}} + 2} - \frac{b}{a} \right| &\leq \frac{2(|c| + |bC|)}{a(2N^{2^i} + (L+U-4)N^{2^{i-1}} + 2)} \\
&\leq \frac{2N^{2^{i-2}} + |C|}{2N^{2^i} + (L+U-4)N^{2^{i-1}} + 2} \cdot \frac{b}{a} \\
&\leq \frac{2N^{2^{i-2}} + (U-L)N^{2^{i-1}}}{2N^{2^i} + (L+U-4)N^{2^{i-1}} + 2} \cdot \frac{b}{a} \\
&< \frac{1}{2ab} \cdot \frac{b}{a} = \frac{1}{2a^2}.
\end{aligned}$$

where for the third inequality we used Lemma 6 and for the last inequality we used our hypothesis. Since

$$\left| \frac{2e}{2N^{2^i} + (L+U-4)N^{2^{i-1}} + 2} - \frac{b}{a} \right| < \frac{1}{2a^2}.$$

then according to Theorem 1 b/a appears among the convergents of $2e/(2N^{2^i} + (L+U-4)N^{2^{i-1}} + 2)$. Once we obtain a and b we apply Theorem 9, and thus we conclude our proof. □

To conclude, we further apply our generic result to the RSA-like cryptosystem with $n = 2^i$, for $i > 2$.

Corollary 6. *Let $N = pq$ be the product of two unknown primes with $q < p < 2q$. Also, let $e < \varphi_{2^i}(N)$ be a public exponent satisfying $ed - k\varphi_{2^i}(N) = 1$. Given e, N we can factor N in polynomial time if*

$$d < \sqrt{\frac{2N^{2^i} + (L + U - 4)N^{2^{i-1}} + 2}{2(U - L)N^{2^{i-1}} + 4N^{2^{i-2}}}}$$

or

$$d > \varphi_{2^i}(N) - \sqrt{\frac{2N^{2^i} + (L + U - 4)N^{2^{i-1}} + 2}{2(U - L)N^{2^{i-1}} + 4N^{2^{i-2}}}}.$$

Proof. We notice that

$$k = \frac{ed - 1}{\varphi_{2^i}(N)} < \frac{ed}{\varphi_{2^i}(N)} < d$$

and

$$kd < d^2 < \frac{2N^{2^i} + (L + U - 4)N^{2^{i-1}} + 2}{2(U - L)N^{2^{i-1}} + 4N^{2^{i-2}}}.$$

Therefore, according to Theorem 10 we can factor N in polynomial time. The second part of the corollary is a direct consequence of Theorem 6. □

To conclude we provide in Table 2 a summary for the first values of i. Thus, if $d < \delta$ or $d > \varphi_{2^i}(N) - \delta$ then we can factor N.

	Bound (δ)
$n = 4$	$\sqrt{\frac{2N^4 - 49N^2 + 2}{170N^2 + 4N}}$
$n = 8$	$\sqrt{\frac{2N^8 - 2209N^4 + 2}{26010N^4 + 4N^2}}$
$n = 16$	$\sqrt{\frac{2N^{16} - 4870849N^8 + 2}{398291130N^8 + 4N^4}}$
$n = 32$	$\sqrt{\frac{2N^{32} - 23725150497409N^{16} + 2}{80378731866132090N^{16} + 4N^8}}$
$n = 64$	$\sqrt{\frac{2N^{64} - 562882766124611619513723649N^{32} + 2}{3230655365485506408874194001502970N^{32} + 4N^{16}}}$

Table 2. Summary on bounds.

4.3 Experimental Results

In this section we provide two numerical examples for our attack. Note that we based our code on the Coppersmith attack implementation found in [30]. For both examples we used the following modulus

$$N = 348965558859919659799872778156428368196003826103849376373 1.$$

4.4 Case $i = 3$

We used the following public exponent for our experiment

$$\begin{aligned} e = 18555167738862185672576798537349156553445777090051707104002748078900254063105098868053098514293450942701643168926426512659338340822525617334395915967414446775404808903265028907201530180137111652600374377492211908605072830685026424712373040080616654979124842004654114761071811322317797455647551175815185278845497696695351867672469894203440226792634427160819410995139167838110175799491088904923684085672503371765214741337816802692137522415538143236188410184247 31.\end{aligned}$$

Computing the continued fraction expansion of $2e/(2N^8 - 2209N^4 + 2)$, we get the first 25 partial quotients

$$[0, 11, 1, 5, 1, 3, 5, 14, 2, 1, 351, 1, 6, 1, 3, 2, 2, 13, 1, 1, 1, 3, 7, 4, 1, \ldots].$$

Looking at the $79th$ convergent we obtain

$$\begin{aligned} a &= 142724769270595988105828596944949513638274677 1, \\ b &= 120421408647555060026249055715459708471315764, \end{aligned}$$

which satisfy the condition of Theorem 10. Therefore, we obtain the following approximations of S and D

$$\begin{aligned} \hat{S} &= 158666848432062407414462565131 \\ \hat{D} &= 105908198157490520315381810349. \end{aligned} \tag{2}$$

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

$$\hat{p} = 0.5(\hat{S} + \hat{D}) = 132287523294776463864922187740. \tag{3}$$

Using Coppersmith's algorithm we find

$$p = 132287523294776463864922187741,$$

and then we can compute

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

4.5 Case $i = 4$

In this case, we used the following public exponent

$$\begin{aligned}e = {} & 151850300379134641050216509172052891078565405046851565128460318761\\ & 281104864282907216847380393032998644293643403864091825676539185437\\ & 319736928553366703694512118727659329531829182675897677725952497516\\ & 035204340775773744570361971570299107168338864426209287685120750422\\ & 619822111973911693327924576445892433931965591785609084136517364290\\ & 333656074695426211158639556099118106996248401270147846892775841262\\ & 899160111149705010943156677913851634410253210967731423968238785173\\ & 530791290474344938772113541670180810321812821473366700097022943064\\ & 621291899119395630856339800559609228013301960801163610003601003708\\ & 901082261491719482148337513493610835922857939812389232163759729169\\ & 556705753364778493708063058738055885437399659874746137792949103631\\ & 501243098329092234554773896507762575333150974587820638889551764794\\ & 325313473557627343612341833442949770330367903907567238927708886821\\ & 276207587808093132889415939840212530760098604801766795067448731.\end{aligned}$$

Computing the continued fraction expansion of $2e/(2N^{16} - 4870849N^8 + 2)$, we get the first 25 partial quotients

$$[0, 3, 5, 2, 2, 5, 1, 50, 1, 1, 5, 1, 70, 1, 40, 1, 32, 1, 13, 1, 2, 1, 12, 1, 1, \ldots].$$

Looking at the $86th$ convergent we obtain

$$\begin{aligned}a &= 142724769270595988105828596944949513638274677 1,\\ b &= 448119602994560621387851853179442893633766061,\end{aligned}$$

which satisfy the condition of Theorem 10. Computing $\hat{S}$ and $\hat{D}$ we obtain the same approximations of S and D as in Equation (2), and implicitly the one for p stated in Equation (3). Using Coppersmith's algorithm we again find N's factorization

$$\begin{aligned}p &= 132287523294776463864922187741,\\ q &= 263793251372859435495403773 91.\end{aligned}$$

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 $ae - b\varphi_{2^i}(N) = c$, 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 other values of n that are not covered by our work.

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.: 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)
26. Teşeleanu, G.: A Generalized Wiener-type Attack Against an RSA-like Cryptosystem. In: CSCML. Lecture Notes in Computer Science, vol. 16244, pp. 53–67. Springer (2025)
27. Teşeleanu, G.: Attacking an RSA-Like Cryptosystem Using Continued Fractions and Lattices. In: NordSec 2025. Lecture Notes in Computer Science, vol. 16325, pp. 43–56. 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)