# Generalized Wiener-Type Attacks on Two RSA-Like Cryptosystems

Abdoulaye Faye[1], Michel Seck[1], Abdoul Aziz Ciss[1], Papa Cheikhou Diop[2], and Oumar Niang[1]

[1] LTISI, CRISIN'2D, Ecole Polytechnique de Thies, Senegal
{faye.abdoulaye,mseck,aaciss,oniang}@ept.edu.sn
[2] Département de Mathématiques, Université Iba Der Thiam de Thiès, Senegal
cheikh.diop@univ-thies.sn

**Abstract.** In AfricaCrypt 2025, Seck *et al.* proposed a new generalized Wiener-type attack on an RSA-like cryptosystem proposed by Cotan and Teşeleanu (NordSec 2023). In their attack, they studied the generalized key equation $eu - (p^4 - 1)(q^4 - 1)v = w$ and showed that a private exponent $d$ which is too large or too small can be recovered in polynomial time. Another RSA variant based on cubic Pell curves with key equation $ed - (p - 1)^2(q - 1)^2k = 1$, was examined by Rahmani and Nitaj in AfricaCrypt 2025. Note that these two attacks are valid for a balanced modulus $N = pq$ $(q < p < 2q)$. In this paper, we extend these two attacks by showing that for a modulus $N = pq$ product of arbitrary primes $p, q$, one can efficiently factor $N$ by studying the two key equations $ex - (p^4 - 1)(q^4 - 1)y = \omega$ and $ex - (p - 1)^2(q - 1)^2y = \omega$ under certain conditions on $x, y$ and $\omega$. Our new attacks are based on Coppersmith method and continued fractions.

**Keywords:** RSA cryptosystem · cryptanalysis · Continued fractions · Coppersmith's method · LLL algorithm · Cubic Pell curves

## 1 Introduction

In 1978, Rivest, Shamir and Adleman published the RSA cryptosystem [RSA78], one of the most widely used public key cryptosystem. RSA is generally used in two contexts : as a public key encryption (PKE) scheme to ensure confidentiality of data or as digital signature scheme to ensure authentification or non-repudiation. As a PKE, the generation of a key pair $(pk, sk)$ begins by selecting two large prime numbers $p$ and $q$ of similar bitsize. From these values, we compute the modulus $N = pq$ and $\varphi(N) = (p - 1)(q - 1)$. Then, a public exponent $e$ is chosen such that $1 < e < \varphi(N)$ and $\gcd(e, \varphi(N)) = 1$. The corresponding private exponent $d$ is determined as the modular inverse of $e$ modular $\varphi(N)$, satisfying $ed \equiv 1 \pmod{\varphi(N)}$. The public key is represented as $pk = (N, e)$, while the private key is $sk = (N, d)$. The encryption of a message $m < N$ is performed by computing the ciphertext $c = m^e \pmod N$ and the decryption by computing $m = c^d \pmod N$. As a digital signature

scheme, the private exponent $d$ is used in the signing process while the public exponent $e$ is used in the verification process. Notice that in real applications, RSA is often combined with padding schemes such as OAEP [FOPS01] for encryption and PSS [BR98] for signatures to enhance security. The security of RSA is based on the supposed hardness of the integer factorization problem i.e. factoring intergers $N = pq$ which are product of two large prime numbers $p$ and $q$. It is demonstrated that RSA is vulnerable if the parameters are not carefully chosen, especially the public exponent $e$, the private exponent $d$, and the primes $p$ and $q$ [MP19,Hås86,May03,Wie90,Bon99,BD99,BNMB22]. Numerous attacks on RSA exploit the algebraic structure of the key equation $ed \equiv 1 \pmod{\varphi(N)}$. Such attacks are generally based on continued fractions [Moo64,HW08] or lattice reduction techniques [LLL82] or combine both techniques. In 1990, Wiener [Wie90] proposed a polynomial time attack that exploits the key equation $ed - k(p-1)(q-1) = 1$ to factor the modulus $N$ when $d < \frac{1}{3}N^{\frac{1}{4}}$. Concretly Wiener has showed that $\frac{k}{d}$ appears among the convergents of the continued fraction expansion of $\frac{e}{N}$ which can be computed in polynomial time in $\log(N)$. This attack has been extended through lattice reduction techniques and Coppersmith's method [May03]. Boneh and Durfee [BD99] refined the Wiener attack using LLL algorithm [LLL82] and improved the bound to $d < N^{0.292}$. They transformed the key equation $ed - k(p-1)(q-1) = 1$ to a modular equation $1 + k(N + 1 - (p+q)) \equiv 0 \pmod{e}$ to solve using Coppersmith's method.

Many RSA variants were published in the last four decades, including the scheme of Elkamchouchi *et al.* [EES02] using the key equation $ed - k(p^2-1)(q^2-1) = 1$, the scheme of Cotan and Teseleanu [CT24b] with the key equation $ed - k(p^n-1)(q^n-1) = 1$ for some positive integer $n$, and the cryptosystem of Nitaj and Seck [NS25,SN25] based on cubic Pell curves and using the key equation $ed - kp^{2(r-1)}q^{2(s-1)}(p-1)^2(q-1)^2 = 1$ for some small positive integers $r$ and $s$. In 2017, Bunder *et al.* [BNST17] studied a generalized attack on variants of RSA cryptosystem related to the generalized key equation $ex - (p^2-1)(q^2-1)y = z$ when $x, y$ and $z$ are suitably small. They showed that if $xy < 2N - 4\sqrt{2}N^{\frac{3}{4}}$ and $|z| < (p-q)N^{\frac{1}{4}}y$, then one can find $p$ and $q$ in polynomial time in $\log(N)$ by combining continued fractions and Coppersmith's method.

In 2023, Cotan and Teşeleanu [CT24b] proposed an RSA variant with key equation $ed - k(p^n-1)(q^n-1) = 1$ and balanced modulus $N = pq$ $(q < p < 2q)$. They showed that one can recover $d$ in polynomial time using continued fractions if $d$ is smaller than the following bound:

$$d < \sqrt{\frac{\sqrt{2}^n N^n \left(\sqrt{N}^n - \delta_n\right)}{e\left(\sqrt{2}^n - 1\right)^2}}, \quad \text{where} \quad \delta_n = \frac{2 \cdot \sqrt{2}^n}{\left(\sqrt{2}^n - 1\right)^2} + \frac{2(2^n+1)}{\sqrt{2}^n}.$$

Later in 2024, Cotan and Teşeleanu [CT24a] generalized their cryptosystem for arbitrary modulus $N = pq$ ($\mu q < p < 2\mu q$) and studied the key equation $ed - k(p^n - 1)(q^n - 1) = 1$. They showed that one can recover the secret exponent $d$ using continued fractions if $d < \sqrt{\dfrac{N^n\left(\sqrt{N}^n - \delta_n^E\right)}{e\Delta_n}}$ where

$$\delta_n^E = \frac{4\sqrt{2\mu}^n}{\mu^n\left(2^n - \sqrt{2}^n\right) - \sqrt{2}^n + 1} + \frac{2\left((2\mu)^n + 1\right)}{\sqrt{2\mu}^n} \text{ and } \Delta_n = \frac{\mu^n\left(2^n - \sqrt{2}^n\right) - \sqrt{2}^n + 1}{\sqrt{2\mu}^n}.$$

In AfricaCrypt 2025, Seck *et al.* [SNS+26] proposed a generalized Wiener attack on an RSA-like cryptosystem proposed by Cotan and Teşeleanu [CT24b]. They studied the generalized key equation $eu - (p^n - 1)(q^n - 1)v = w$ with $n = 4, w \in \mathbb{Z}$ and $u, v \in \mathbb{N}$. Combining continued fractions and Coppersmith's method, they showed that one can recover $u, v$ and the primes $p$ and $q$ in polynomial time in $\log(N)$ if

$$uv < \frac{2N^4 - 49N^2 + 2}{170N^2 + 4N} \quad \text{and} \quad |w| < vN.$$

Furthermore, they showed that for many RSA variant cryptosystems, if the private exponent $d$ is too large or too small, then the modulus $N$ can be factored in polynomial time. Notice that their attack concerns balanced modulus $N = pq$, i.e $q < p < 2p$. Later, Teseleanu [Teş25,Teş26] extended the attack of Seck *et al.* [SNS+26] to the case $n = 3$ and $n = 6$. Rahmani and Nitaj [RN26] published another attack in AfricaCrypt 2025 using lattice reduction techniques on an RSA-like cryptosystem based on cubic Pell curves $\mathcal{C}_b : x^3 + by^3 + b^2z^3 - 3bxyz = 1$ over $\mathbb{Z}/N\mathbb{Z}$. They studied the key equation $ed - k(p-1)^2(q-1)^2 = 1$ for balanced moduli $N = pq$ ($q < p < 2p$). For a public exponent $e = N^\alpha$, they showed that if the corresponding private exponent satisfies $d < N^{2-\sqrt{\alpha}}$ for $1 < \alpha < 4$, then the factors $p$ and $q$ can be recovered in polynomial time.

Recently, Seck and Ciss [SC25] presented an attack against the RSA variant proposed by Cotan and Teşeleanu [CT24b] by studying the key equation $eu - (p^n - 1)(q^n - 1)v = \pm 1$. They showed that if a private exponent $d$ is either too small or too large, one can factor $N$ in polynomial time using lattice reduction techniques. More recently, Rahmani *et al.* [RNZ26a] investigated the key equation $ed - k(p^n - 1)(q^n - 1) = 1$, for $n \geq 1$, and showed that the modulus $N = pq$ can be factored in polynomial time when $d$ is smaller than an explicit bound depending only on $n$ and $N$, using Coppersmith's method and lattice reduction techniques. In a subsequent work, Rahmani *et al.* [RNZ26b] studied the generalized key equation $d \equiv \frac{l_0}{z_0} \mod (p^n - 1)(q^n - 1)$ with a balanced modulus $N = pq$ ($q < p < 2q$). By also using lattice reduction techniques, they showed that the factors $p$ and $q$ can be recovered in polynomial time under certain conditions on $d$, $l_0$, and $z_0$.

In this paper, given an RSA modulus $N = pq$ product of arbitrary primes, i.e. $q < p < \mu q$ for some positive real $\mu > 1$, we propose a new attack on the variants of the RSA cryptosystem with a generalized Euler totient function of the form $\varphi_n(N) = (p^n - 1)(q^n - 1)$ or of the modified form $\psi(N) = (p-1)^2(q-1)^2$. We studied the following generalized two key equations

$$ex - (p^n - 1)(q^n - 1)y = \omega, \tag{1}$$

$$ex - (p-1)^2(q-1)^2 y = \omega, \tag{2}$$

with $x, y > 0$ and $\omega \in \mathbb{Z}$. We summarize our contributions as follows.

- First, we show that for the generalized key equation $ex-(p^n-1)(q^n-1)y = \omega$, the quotient $\frac{y}{x}$ is a convergent of the continued fraction expansion of $\left(2\mu^{\frac{n}{2}}e\right) / \left(2\mu^{\frac{n}{2}}N^n - (\mu^{\frac{n}{2}}+1)^2 N^{\frac{n}{2}} + 2\mu^{\frac{n}{2}}\right)$ if

$$xy < \frac{2\mu^{\frac{n}{2}}N^n - (\mu^{\frac{n}{2}}+1)^2 N^{\frac{n}{2}} + 2\mu^{\frac{n}{2}}}{2(\mu^n - 1)N^{\frac{n}{2}} + 4\mu^{\frac{n}{2}}(\mu^{\frac{n}{2}}+1)N} \text{ and } |\omega| \leq (\mu^{\frac{n}{2}}+1)yN.$$

- Then using this result and some recent results of Seck *et al.* [SNS+26], we demonstrated for the case $n = 4$, if the following conditions hold:

$$xy < \frac{2\mu^2 N^4 - (\mu^2+1)^2 N^2 + 2\mu^2}{2(\mu^4-1)N^2 + 4\mu^2(\mu^2+1)N}$$

and $|\omega| < yN$, then one can find $p$ and $q$ in polynomial time.

- For the generalized key equation $ex - (p-1)^2(q-1)^2 y = \omega$, we show that using this key equation, one can find $p$ and $q$ in polynomial time if

$$\begin{cases} xy < \dfrac{2\mu N^2 - (\mu-1)^2 N + 2\mu}{2(3\mu^2 + 4\mu^{3/2} + 4\mu + 1)\,N + 8\mu(\sqrt{\mu}+1)N^{3/2} + \left[4(\sqrt{\mu}-1) + 8\mu(\sqrt{\mu}+1)\right] N^{1/2}}, \\ |\omega| < \dfrac{\sqrt{\mu}-1}{\mu} \cdot \dfrac{N+1-(\sqrt{\mu}+1)\sqrt{N}}{N+1+(\sqrt{\mu}+1)\sqrt{N}} \cdot yN^{1/2} < \dfrac{\sqrt{\mu}-1}{\mu}\, yN^{1/2}. \end{cases}$$

- Finally, we provide a proof of concept implementation [3] with SageMath and detailed numerical examples to illustrate step by step our attacks.

**Organization of this paper :** The remainder of this paper is organized as follows. Section 2 presents the necessary background and definitions required for understanding our contributions. We present the RSA variant proposed by Nitaj and Seck [NS25] as well as the cryptosystem introduced by Cotan and Teşeleanu [CT24b]. In Section 3, we introduce our two attacks combining lattice reduction techniques and continued fractions. Our first attack on the RSA variant

[3] https://github.com/Fayeabdoulaye/generalized_wiener_type_attacks

of Cotan and Teşeleanu is based on the key equation $ex-(p^n-1)(q^n-1)y = \omega$ and the second one on the cryptosystem of Nitaj and Seck relies on the key equation $ex - (p-1)^2(q-1)^2y = \omega$. In Section 4, we provide numerical examples to illustrate step by step our attacks. We compare our attacks with former attacks in Section 5. Finally, Section 6 concludes the paper.

## 2 Preliminaries

In this section, we recall the two RSA-like cryptosystems proposed respectively by Nitaj and Seck [NS25], and by Cotan and Teşeleanu [CT24b]. We then provide a brief overview of continued fractions, lattices, and Coppersmith's method. Finally, we present some useful lemmas and theorems that will serve as key ingredients in our attacks.

### 2.1 RSA Variant of Nitaj and Seck

In 2024, Nitaj and Seck [NS25] introduced a new variant of the RSA cryptosystem that leverages the arithmetic of the *cubic Pell curve* defined as:

$$C_b(N): \quad x^3 + by^3 + b^2z^3 - 3bxyz \equiv 1 \pmod{N},$$

where $N = p^r q^s$. In their scheme, the public exponent $e$ and the private exponent $d$ are related to the key equation

$$d \equiv e^{-1} \pmod{p^{2(r-1)}q^{2(s-1)}(p-1)^2(q-1)^2}. \tag{3}$$

In their cryptosystem, Nitaj and Seck [NS25] use an invertible encoding function $\mathcal{E}\mathsf{ncode}$ which takes as input a message $M = (x_m, y_m) \in (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})$, a parameter $f \in \mathbb{Z}/N\mathbb{Z}$ and the modulus $N$ and returns a point $(x, y, z)$ on the cubic Pell curve $\mathcal{C}_b(N)$ where $b = f^3 \pmod{N}$. The decoding function $\mathcal{D}\mathsf{ecode}$ takes as input a point $(x, y, z)$ on the cubic Pell curve $\mathcal{C}_b(N)$, the parameter $f$ and the modulus $N$ and returns the original message $M = (x_m, y_m)$. In the following, we describe key generation, encryption, and decryption algorithms.

1. **Key Generation Algorithm.** This algorithm takes as input a security parameter $\lambda$ and integers $r, s \geq 1$ and outputs a public key $pk = (N, e, f)$ and private key $sk = (N, d, f)$. The different steps are given as follows:
   - Choose randomly two prime numbers $p$ and $q$ of $\lambda$ bits such that $p, q \equiv 1 \pmod 3$.
   - Compute the modulus $N = p^r q^s$.
   - Choose randomly an integer $f \in \mathbb{Z}/N\mathbb{Z}$ such that $f^3 \pmod N$ is a nonzero cubic residue modulo $p$ and modulo $q$.
   - Choose an integer $e \in \mathbb{Z}/N\mathbb{Z}$ with $\gcd(e, pq(p-1)(q-1)) = 1$.
   - Compute

$$d \equiv e^{-1} \pmod{p^{2(r-1)}q^{2(s-1)}(p-1)^2(q-1)^2}.$$

- The public key is $pk = (N, e, f)$ and the private key is $sk = (N, d, f)$.

2. **Encryption Algorithm.** This algorithm takes as input a message $M = (x_m, y_m) \in (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})$ and a public key $pk = (N, e, f)$ and outputs a ciphertext $ctx = (c_x, c_y) \in (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})$. The different steps are given as follows:
   - Compute $b := f^3 \pmod N$.
   - Encode the message $M$ into a point $(x, y, z)$ on the cubic Pell curve $\mathcal{C}_b(N)$ using the function $\mathcal{E}\mathsf{ncode}((x_m, y_m), f, N)$.
   - Compute $uvw = (u, v, w) := e \otimes (x, y, z)$ on the cubic Pell curve $\mathcal{C}_b(N)$.
   - Compress $uvw$ to obtain $(c_x, c_y) := \mathcal{D}\mathsf{ecode}(uvw, f, N)$.
   - The ciphertext $C = (c_x, c_y)$.

3. **Decryption Algorithm.** This algorithm takes as input a ciphertext $C = (c_x, c_y) \in (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})$ and a private key $sk = (N, d, f)$ and outputs a plaintext message $M = (x_m, y_m) \in (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})$. The different steps are given as follows:
   - Compute $b := f^3 \pmod N$.
   - Decompress the ciphertext to obtain $(x_C, y_C, z_C) := \mathcal{E}\mathsf{ncode}(C, b, N)$.
   - Compute $(x, y, z) := d \otimes (x_C, y_C, z_C)$ on the cubic Pell curve $\mathcal{C}_b(N)$.
   - Decode the point $(x, y, z)$ to obtain the plaintext

$$(x_m, y_m) := \mathcal{D}\mathsf{ecode}((x, y, z), b, N).$$

### 2.2 RSA Variant of Cotan and Teşeleanu

At the NordSec 2023 conference, Cotan and Teşeleanu [CT24b] introduced a new RSA-type cryptosystem. Their proposal relies on the following key equation $ed = 1 + k\big(p^n - 1\big)\big(q^n - 1\big)$ where $n$ is a positive integer and $k \in \mathbb{Z}$. Notice that their scheme generalizes some RSA-like cryptosystems. In particular:

- for $n = 1$, the equation coincides with the classical RSA relation[RSA78];
- for $n = 2$, we get the key equation related to the cryptosystem Elkamchouchi, Elshenawy, and Shaban [EES02].

Unlike standard RSA, where computations are performed directly in the ring $\mathbb{Z}_N$, Cotan and Teşeleanu work in an extended structure that incorporates polynomials. More precisely, the arithmetic operations are carried out in $\mathbb{Z}_N[t]/(t^n - r)$ where $t^n - r$ is an irreducible polynomial. Let $p$ be a prime number and $r \in \mathbb{F}_p$ such that the polynomial $t^n - r$ is irreducible over $\mathbb{F}_p[t]$. The quotient

$$A_n(p) = \mathbb{F}_p[t]/(t^n - r)$$

is then a finite field of size $p^n$. Therefore, every element of $A_n(p)$ can be uniquely represented as a polynomial of degree less than $n$, i.e.,

$$A_n(p) = \left\{a(t) = a_0 + a_1 t + \cdots + a_{n-1} t^{n-1}, \quad \text{where } a_0, a_1, \ldots, a_{n-1} \in \mathbb{F}_p\right\}.$$

The multiplication rule within this field is inherited from polynomial multiplication modulo $t^n - r$. For two elements $a(t), b(t) \in A_n(p)$, their product, denoted $a(t) \circ b(t)$, is computed as follows:

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

The set of invertible elements in $A_n(p)$ is denoted by $A_n^*(p)$ and has size $|A_n^*(p)| = p^n - 1$.

When considering two distinct primes $p$ and $q$, the Chinese Remainder Theorem allows us to extend this construction to the ring $A_n(N) = \mathbb{Z}_N[t]/(t^n - r)$ where $N = pq$ and $r$ is an element in $\mathbb{Z}_N$ such that the polynomial $t^n - r$ is irreducible over both $\mathbb{F}_p[t]$ and $\mathbb{F}_q[t]$. Like $A_n^*(p)$, the set of invertible elements in $A_n(N)$ is denoted by $A_n^*(N)$ and has size $|A_n^*(N)| = (p^n - 1)(q^n - 1)$, thanks to the Chinese Remainder Theorem. The cryptosystem proposed by Cotan and Teşeleanu operates within this algebraic structure. By generalizing the classical ring in RSA, their approach offers a more versatile structure that depends on the choice of the parameter $n$. We now describe their scheme by recalling the key generation, encryption, and decryption processes.

1. **Key Generation.** To generate a key pair ($pk$, $sk$), for a given integer $n \geq 1$ and a security parameter $\lambda$, we proceed as follows:
   (a) Randomly select two large distinct primes $p$ and $q$ such that $p, q \geq 2^\lambda$. Then compute the modulus: $N = pq$.
   (b) Choose an element $r \in \mathbb{Z}_N$ such that the polynomial $t^n - r$ is irreducible over both $\mathbb{Z}_p[t]$ and $\mathbb{Z}_q[t]$.
   (c) Define $\varphi_n(N) = (p^n - 1)(q^n - 1)$.
   (d) Select a positive integer $e$ with $e < \varphi_n(N)$ and $\gcd(e, \varphi_n(N)) = 1$.
   (e) Compute $d = e^{-1} \pmod{\varphi_n(N)}$.
   (f) The private key is $sk = (N, d, n, r)$ and the public key is $pk = (N, e, n, r)$.
2. **Encryption Procedure.** Given a plaintext $m = (m_0, m_1, \ldots, m_{n-1}) \in (\mathbb{Z}_N)^n$ and a public key $pk = (N, e, n, r)$, the encryption process is as follows:
   (a) Map the plaintext $m$ to a polynomial $m(t)$ in $A_n^*(N)$:
   $$m(t) = m_0 + m_1 t + \cdots + m_{n-1} t^{n-1} \in A_n^*(N),$$
   (b) Compute the ciphertext $c(t) = [m(t)]^e \pmod{N}$ in $A_n^*(N)$.
3. **Decryption Procedure.** Given a ciphertext $c(t) \in A_n^*(N)$, and a private key $sk = (N, d, n, r)$, the decryption process is as follows:
   (a)
   $$m(t) = [c(t)]^d \pmod{N}.$$
   (b) Extract the coefficients of $m(t)$ to recover the plaintext:
   $$m = (m_0, m_1, \ldots, m_{n-1}).$$

### 2.3 Continued Fractions

**Definition 1.** *A continued fraction[Moo64] is an expression of the form:*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots}}},$$

*where $a_0 \in \mathbb{Z}$ and $a_i, i = 1, 2, \cdots$ are positive integers.*

Notice that

- Every rational number $\eta$ can be expanded into a finite continued fraction:
$$\eta = \frac{\alpha_k}{\beta_k} = [a_0; a_1, a_2, \ldots, a_k]$$
- A continued fraction expansion of $\eta$ is finite if and only if $\eta$ is a rational number.

**Example 1:** For $\alpha = \frac{128}{37}$, we have

$$\frac{128}{37} = [3; 2, 5, 1, 2] = 3 + \cfrac{1}{2 + \cfrac{1}{5 + \cfrac{1}{1 + \cfrac{1}{2}}}}$$

**Example 2:** Let $\eta = \frac{1+\sqrt{5}}{2}$. This is a solution of the quadratic equation $a^2 - a - 1 = 0$. Notice that $\eta = 1 + \frac{1}{\eta}$. By substituting progressively $\eta$ into the expression $(1 + \frac{1}{\eta})$, we get its continued fraction expansion:

$$\eta = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \ddots}}} = [1; 1, 1, \cdots].$$

**Definition 2 (convergent [Moo64,HW08]).** *A convergent is the rational number which is represented by the part retained if any of the terms of a continued fraction are dropped from the end of this one.*

For instance, let us consider the number $\alpha = [a_0; a_1, a_2, a_3, a_4, a_5]$. The first convergent is $C_1 = a_0$; the second convergent is $C_2 = a_0 + \dfrac{1}{a_1}$, and the third convergent is $C_3 = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2}}$.

**Theorem 1 ([Moo64,HW08]).** *The convergents of a real number $\eta$ with continued fraction expansion $\eta = [a_0; a_1, a_2, a_3, a_4, \ldots]$ are given by $C_n = \frac{\alpha_n}{\beta_n}$, where:*

$$\begin{cases} \alpha_n = a_n \alpha_{n-1} + \alpha_{n-2}, \\ \beta_n = a_n \beta_{n-1} + \beta_{n-2}, \end{cases}$$

*with initial conditions: $\alpha_0 = 1, \beta_0 = 0, \alpha_1 = a_0$ and $\beta_1 = 1$.*

**Theorem 2 (Legendre [Moo64,HW08]).** *Let $\zeta$ be a real number and let $\frac{a}{b}$ be a rational number where $a$ et $b$ are positive integers with $\gcd(a, b) = 1$. If*

$$\left| \zeta - \frac{a}{b} \right| < \frac{1}{2b^2},$$

*then $\frac{a}{b}$ is a convergent of the continued fraction expansion of $\zeta$.*

### 2.4 Lattice Theory and Coppersmith's method

Let $v_1, \ldots, v_n \in \mathbb{Z}^m, m \geq n$ be linearly independent vectors. A lattice $\mathcal{L}$ [May03] spanned by $\{v_1, \ldots, v_n\}$ is the set of all integer linear combinaitions of $v_1, \ldots, v_n$

$$\mathcal{L} = \left\{ \sum_{i=1}^{n} a_i v_i \text{ with } a_i \in \mathbb{Z} \right\}.$$

The set of vectors $B = \{v_1, \ldots, v_n\}$ is called a basis for $\mathcal{L}$ and we say that $\mathcal{L}$ is spanned by the vectors of the basis $B$. The dimension of the lattice is $n$, its rank is $m$ and its determinant is $\det(\mathcal{L}) = \sqrt{\det(B^t B)}$ where $B^t$ is the transpose of $B$. If $m = n$, the lattice is called a full rank lattice and $\det(\mathcal{L}) = |\det(B)|$. A lattice $\mathcal{L}$ can have many bases, and it is hard to find a basis with short vectors when the dimension is large. In 1982, Lenstra, Lenstra and Lovàsz proposed a polynomial time algorithm to find a short basis, called the LLL algorithm. The following theorem is used to estimate the output of the $LLL$ algorithm.

**Theorem 3 (LLL algorithm [May03]).** *Let $\mathcal{L} \subset \mathbb{R}^n$ be a lattice spanned by basis vectors $B = \{b_1, \ldots, b_n\}$. The LLL algorithm outputs a reduced lattice basis $\{v_1, \ldots, v_n\}$ satisfying*

$$\|v_1\| \leq \|v_2\| \leq \cdots \leq \|v_i\| \leq 2^{\frac{n(n-1)}{4(n-i+1)}} \cdot \det(\mathcal{L})^{\frac{1}{n-i+1}} \quad \text{for } i = 1, \ldots, n$$

*in time polynomial in $n$ and in the bit-size of the entries of the basis matrix $B$.*

In 1996, Coppersmith [Cop96] introduced a method for finding small roots of modular polynomial equations using the LLL algorithm. Since then, the method has found many different applications in the area of public key cryptography. Coppersmith's method provides to find small roots of a univariate polynomial

equation $f(x) \equiv 0 \pmod{M}$, for an integer $M$. This method has been generalized to polynomial with more variables of the form

$$h(x_1, x_2, \ldots, x_n) = \sum_{i_1,\ldots,i_n} \lambda_{i_1,i_2,\ldots,i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$$

with $\lambda_{i_1,i_2,\ldots,i_n} \in \mathbb{Z}$. We are now going to formulate Coppersmith's theorem for univariate polynomials.

**Theorem 4 (Coppersmith [May03]).** *Let $N$ be an integer of unknown factorization, which has a divisor $b \geq N^{\beta}$. Furthermore, let $f_b(x)$ be a univariate, monic polynomial of degree $\delta$. Then we can find all solutions $x_0$ for the equation*

$$f_b(x) \equiv 0 \pmod{b}, \quad \textit{with } |x_0| \leq \frac{1}{2} N^{\frac{\beta^2}{\delta} - \varepsilon},$$

*in time polynomial in* $\left(\log N, \delta, \frac{1}{\varepsilon}\right)$.

Coppersmith's method can be used to factor an integer $N$ given an approximation of one of the prime factors. The following theorem states this result.

**Theorem 5 (Coppersmith,[May03]).** *Let $N = pq$ with $p > q$. Assume we are given an approximation $\tilde{p}$ of $p$, such that $|p - \tilde{p}| < N^{1/4}$. Then the factorization of $N$ can be recovered in time polynomial in* $\log(N)$.

In the following, we describe Coppersmith's algorithm for factoring a composite integer $N$ with two unknown primes factors $p$ and $q$ given an approximation of one of them.

### Coppersmith's Algorithm for Factoring $N$

**Input:** the following data:

- A composite integer $N = pq$ ($p$ and $q$ unknown ),
- An approximation $\tilde{p}$ of $p$,
- A positive real $\beta$ such that $p > N^{\beta}$,
- A positive real $\varepsilon$ such that $|\tilde{p} - p| < N^{\frac{1}{2} - \varepsilon}$.

**Output:** a factor $p$ of $N$ or $\perp$.

**Algorithm Steps:**

- Define the polynomial $f_p(x) = x - \tilde{p}$ and choose the smallest integer $m$ such that: $m \geq \max\left\{\frac{\beta^2}{\varepsilon},\ 7\beta\right\}$. Then compute: $t = \left\lfloor m\left(\frac{1}{\beta} - 1\right)\right\rfloor$.
- Compute the shift polynomials

  $g_i(x) = N^i \cdot f_p^{m-i}(x)$ for $0 \leq i \leq m$ and $h_i(x) = x^i \cdot f_p^m(x)$ for $0 \leq i \leq t - 1$.

- Compute the bound $X = \left\lceil N^{\beta^2-\varepsilon} \right\rceil$ and construct the lattice basis $B$ from the coefficient vectors of $g_i(xX)$ and $h_i(xX)$.
- Afterwards, apply the LLL algorithm to the basis $B$. Let $w$ be the shortest vector in the LLL-reduced basis and construct the polynomial $f(x)$ from $w$.
- Find all integer roots $x_0$ of $f(x)$ and for each root $x_0$, check if

$$\gcd(N, f_p(x_0)) \geq N^{\beta}.$$

- If $\tilde{p} + x_0$ divides $N$, return $p = \tilde{p} + x_0$, else return $\perp$.

### 2.5 Useful Lemmas and Theorems

The following lemmas can be obtained easily from [SC25].

**Lemma 1.** *Let $N = pq$ be the product of two unknown prime numbers $p$ and $q$ with $q < p < \mu q$. Then the following bounds hold for $p$ and $q$:*

$$\sqrt{N} < p < \sqrt{\mu N} \text{ and } \sqrt{\frac{N}{\mu}} < q < \sqrt{N}.$$

**Lemma 2.** *Let $N = pq$ be the product of two unknown prime numbers $p$ and $q$ with $q < p < \mu q$. Then the following bounds hold for $p^n + q^n$ and $p^n - q^n$:*

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

$$0 < p^n - q^n < (\mu^{\frac{n}{2}} - \frac{1}{\mu^{\frac{n}{2}}})N^{\frac{n}{2}}.$$

*Remark 1.* From the previous lemma, we can deduce that

$$A = N + 1 - (\sqrt{\mu} + 1)\sqrt{N}$$

is a positive lower bound for $\varphi(N) = (p-1)(q-1) = N - (p+q) + 1$.

*Remark 2.* Let $N = pq$ be the product of two arbitrary prime numbers $p$ and $q$ with $q < p$. There is always a positive rational number $\mu$ with $1 < \mu < p$ such that $q < p < \mu q < N$.

*Remark 3.* Without loss of generality, we assume in the rest of the paper that $p - q > N^{1/4}$. Otherwise, we can factor $N$ in polynomial time using Coppersmith's method or Fermat's factorization method [May03].

The following lemma can be derived from the proof of Lemma 2 in [SNS+26].

**Lemma 3.** *Let $N = pq$ be the product of two unknown prime numbers $p$ and $q$ with $q < p < \mu q$ and $p - q > N^{1/4}$. Let $x, y$ be two positive integers and $\omega \in \mathbb{Z}$ such that $ex - (p^4-1)(q^4-1)y = \omega$. Define the quantities $\tilde{S}_1$ and $\tilde{D}_1$ as follows:*

$$\tilde{S}_1 = \sqrt{2N + \sqrt{(N^2+1)^2 - \frac{ex}{y}}} \text{ and } \tilde{D}_1 = \sqrt{-2N + \sqrt{(N^2+1)^2 - \frac{ex}{y}}}.$$

*If $|\omega| < yN$, then the following bound holds:*

$$|p - p_0| < N^{1/4} \text{ where } p_0 = \frac{1}{2}\left(\tilde{S}_1 + \tilde{D}_1\right).$$

Recently, in AfricaCrypt 2025, Seck et al. [SNS+26] showed an interesting result about the vulnerability of large private exponents in RSA-like cryptosystems. They proved that if a private exponent $d = N^{\delta}$ of an RSA-like cryptosystem is too large, then one can factor the modulus $N$ in polynomial time, under certain conditions on $\delta$.

**Theorem 6 ([SNS+26]).** *Let $N = pq$ be an RSA modulus. Let $\psi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Suppose $\mathcal{A}$ is an algorithm that is able to factor $N$ in polynomial time given $N$ and a public exponent $0 < e < \psi(p, q)$ such that there exist positive integers $x$ and $y$ with $xy < \mathcal{B}_1 \in \mathbb{R}^+$ satisfying*

$$ex - y\psi(p, q) = z \text{ with } |z| \leq \mathcal{B}_2, \ \mathcal{B}_2 \geq 1.$$

*Then, using $\mathcal{A}$, one can factor $N$ in polynomial time given $N$ and a public exponent $0 < e' < \psi(p, q)$ such that the corresponding private exponent $d' = \psi(p, q) - d$ for some $d < \sqrt{\mathcal{B}_1}$.*

## 3 Our contributions

In this section, we present our new attacks on two new variants of RSA with the following two key equations

$$ex - (p^n - 1)(q^n - 1)y = \omega \tag{4}$$
$$ex - (p - 1)^2(q - 1)^2 y = \omega \tag{5}$$

where $n$ is a positive integer, $x, y, \omega \in \mathbb{Z}$ and $N = pq$ is an RSA modulus where $p$ and $q$ are two unknown prime numbers such that $q < p < \mu q$ for some $\mu > 1$.

### 3.1 Our Attack With the Equation $ex - (p^n - 1)(q^n - 1)y = \omega$

In AfricaCrypt 2025, Seck et al. [SNS+26] proposed a new attack on the RSA-like cryptosystem of Cotan and Teşeleanu [CT24b] when the private exponent $d$ is too large or too small by studying the particular key equation $ex-(p^4-1)(q^4-1)y = \omega$ for balanced RSA modulus, i.e., $q < p < 2q$. In this section, we generalize their result for arbitrary primes $p, q$. In our attack, the prime factors $p$ and $q$ satisfy the relation $q < p < \mu q$, for $\mu > 1$. Note that Seck *et al.* [SNS+26] studied the particular case where $\mu = 2$.

**Theorem 7.** *Let $N = pq$ be an RSA modulus where $p$ and $q$ verify $q < p < \mu q$. Let $e$ be a public exponent satisfying the key equation $ex - (p^n - 1)(q^n - 1)y = \omega$ where $x$ and $y$ are two positive integers and $\omega \in \mathbb{Z}$. If*

$$xy < \frac{2\mu^{\frac{n}{2}} N^n - (\mu^{\frac{n}{2}} + 1)^2 N^{\frac{n}{2}} + 2\mu^{\frac{n}{2}}}{2(\mu^n - 1)N^{\frac{n}{2}} + 4\mu^{\frac{n}{2}}(\mu^{\frac{n}{2}} + 1)N}, \text{ and } |\omega| \leq (\mu^{n/2} + 1)yN,$$

*then* $\dfrac{y}{x}$ *is a convergent of the continued fraction expansion of*

$$\frac{2\mu^{n/2}e}{2\mu^{n/2}N^n - (\mu^{n/2}+1)^2N^{n/2} + 2\mu^{n/2}}.$$

*Proof.* Suppose that $N = pq$ and $q < p < \mu q$ and $e$ satisfy the equation $ex-(p^n-1)(q^n-1)y = \omega$ with $x, y > 0$ and $\gcd(x, y) = 1$. Set $\varphi_n(N) = (p^n-1)(q^n-1) = N^n + 1 - (p^n + q^n)$, $H_n(N) = \frac{(\mu^{n/2}+1)^2}{2\mu^{n/2}}N^{n/2}$ and

$$\mathcal{E}(n, \mu, N) = \frac{e}{N^n + 1 - H_n(N)} - \frac{y}{x} = \frac{2\mu^{\frac{n}{2}}e}{2\mu^{\frac{n}{2}}N^n - (\mu^{\frac{n}{2}}+1)^2N^{\frac{n}{2}} + 2\mu^{\frac{n}{2}}} - \frac{y}{x}.$$

We have :

$$ex - \varphi_n(N)y = \omega \Longleftrightarrow ex - [N^n + 1 - (p^n + q^n)]\, y = \omega$$

$$\Longleftrightarrow ex - [N^n + 1 - H_n(N)]\, y - [-(p^n + q^n) + H_n(N)]\, y = \omega$$

$$\Longleftrightarrow ex - [N^n + 1 - H_n(N)]\, y = \omega + [-(p^n + q^n) + H_n(N)]\, y$$

$$\Longleftrightarrow \frac{ex}{N^n + 1 - H_n(N)} - y = \frac{\omega + [-(p^n + q^n) + H_n(N)]\, y}{N^n + 1 - H_n(N)}$$

$$\Longleftrightarrow \frac{e}{N^n + 1 - H_n(N)} - \frac{y}{x} = \frac{\omega + [-(p^n + q^n) + H_n(N)]\, y}{N^n + 1 - H_n(N)} \cdot \frac{1}{x}$$

$$\Longrightarrow \left|\frac{e}{N^n + 1 - H_n(N)} - \frac{y}{x}\right| \leq \frac{|\omega| + |-(p^n + q^n) + H_n(N)|\, y}{N^n + 1 - H_n(N)} \cdot \frac{1}{x}$$

By Lemma 2,

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

Then,

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

By substuting $H_n(N)$ by its value, we get:

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

This implies that

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

Then

$$|-(p^n+q^n)+H_n(N)| < \frac{\mu^n-1}{2\mu^{\frac{n}{2}}}N^{\frac{n}{2}}.$$

$$\Longrightarrow |\mathcal{E}(n,\mu,N)| < \frac{|\omega|+\frac{\mu^n-1}{2\mu^{\frac{n}{2}}}\,y\,N^{\frac{n}{2}}}{N^n+1-H_n(N)}\cdot\frac{1}{x}$$

Now, suppose that $|\omega| \leq (\mu^{\frac{n}{2}}+1)yN$, then

$$|\mathcal{E}(n,\mu,N)| < \frac{(\mu^{\frac{n}{2}}+1)N+\frac{\mu^n-1}{2\mu^{\frac{n}{2}}}N^{\frac{n}{2}}}{N^n+1-\frac{(\mu^{\frac{n}{2}}+1)^2}{2\mu^{\frac{n}{2}}}N^{\frac{n}{2}}}\cdot\frac{y}{x} = \frac{2\mu^{\frac{n}{2}}(\mu^{\frac{n}{2}}+1)N+(\mu^n-1)N^{\frac{n}{2}}}{2\mu^{\frac{n}{2}}N^n+2\mu^{\frac{n}{2}}-(\mu^{\frac{n}{2}}+1)^2N^{\frac{n}{2}}}\cdot\frac{y}{x}.$$

Suppose also that

$$xy < \frac{2\mu^{\frac{n}{2}}N^n-(\mu^{\frac{n}{2}}+1)^2N^{\frac{n}{2}}+2\mu^{\frac{n}{2}}}{2(\mu^n-1)N^{\frac{n}{2}}+4\mu^{\frac{n}{2}}(\mu^{\frac{n}{2}}+1)N},$$

then

$$\frac{(\mu^n-1)N^{\frac{n}{2}}+2\mu^{\frac{n}{2}}(\mu^{\frac{n}{2}}+1)N}{2\mu^{\frac{n}{2}}N^n+2\mu^{\frac{n}{2}}-(\mu^{\frac{n}{2}}+1)^2N^{\frac{n}{2}}} < \frac{1}{2xy}.$$

Finally, we get

$$\left|\frac{2\mu^{\frac{n}{2}}e}{2\mu^{\frac{n}{2}}N^n-(\mu^{\frac{n}{2}}+1)^2N^{\frac{n}{2}}+2\mu^{\frac{n}{2}}}-\frac{y}{x}\right| = |\mathcal{E}(n,\mu,N)| < \frac{1}{2xy}\cdot\frac{y}{x} = \frac{1}{2x^2}.$$

By Theorem 2, $\frac{y}{x}$ is a convergent of the continued fraction expansion of

$$\frac{2\mu^{\frac{n}{2}}e}{2\mu^{\frac{n}{2}}N^n-(\mu^{\frac{n}{2}}+1)^2N^{\frac{n}{2}}+2\mu^{\frac{n}{2}}}.$$

This terminates the proof.

□

In the following theorem, we provide the conditions under which one can find the prime factors $p$ and $q$ in polynomial time for a given instance $(N,e)$.

**Theorem 8.** *Let $N=pq$ be an RSA modulus where $p$ and $q$ verify $q<p<\mu q$. Let $e$ be a public exponent satisfying the equation:*

$$ex-(p^4-1)(q^4-1)y=\omega$$

*with $x$ and $y$ two positive integers and $\omega\in\mathbb{Z}$. If*

$$xy < \frac{2\mu^2N^4-(\mu^2+1)^2N^2+2\mu^2}{2(\mu^4-1)N^2+4\mu^2(\mu^2+1)N}$$

*and $|\omega|<yN$, then one can find $p$ and $q$ in polynomial time.*

*Proof.* Suppose that $N = pq$ and $q < p < \mu q$ and $e$ satisfy the equation $ex - (p^4-1)(q^4-1)y = \omega$ with $x, y > 0$ and $\gcd(x, y) = 1$. Suppose also that

$$\begin{cases} xy < \dfrac{2\mu^2 N^4 - (\mu^2+1)^2 N^2 + 2\mu^2}{2(\mu^4-1)N^2 + 4\mu^2(\mu^2+1)N}, \text{and} \\ |\omega| < yN \text{ (this implies } |\omega| < (\mu^2+1)yN). \end{cases}$$

From the previous Theorem 7, we know that $\dfrac{y}{x}$ is a convergent of the continued fraction expansion of

$$\frac{2\mu^2 e}{2\mu^2 N^4 - (\mu^2+1)^2 N^2 + 2\mu^2}. \tag{6}$$

Notice that, without loss of generality, we can assume that $\mu$ is a positive integer, since if $q < p < \mu q$, then $q < p < (\lceil \mu \rceil + 1)q$. The number (6) is rational; therefore, its continued fraction expansion is finite and can be computed in polynomial time using Euclidean divisions [Moo64,HW08]. Once we obtain the continued fraction expansion of (6), we can compute the convergents $\dfrac{\alpha_i}{\beta_i}$ in polynomial time by applying the recurrence relation in Theorem 1. After computing $y/x$ (which is one of the convergents), we can derive an approximation $p_0$ of $p$ such that $|p - p_0| < N^{1/4}$ by Lemma 3 since $|\omega| < yN$. After that, we apply Coppersmith's algorithm (Theorem 5) with input $p_0$ and $N$ to find $p$ and $q$ in polynomial time. This completes the proof.

□

**Corollary 1.** *Let $N = pq$ be an RSA modulus with $q < p < \mu q$. Let $e < (p^4-1)(q^4-1)$ be a public exponent. If the private exponent $d$ satisfies*

$$d < \sqrt{\frac{2\mu^2 N^4 - (\mu^2+1)^2 N^2 + 2\mu^2}{2(\mu^4-1)N^2 + 4\mu^2(\mu^2+1)N}},$$

*then one can find $p$ and $q$ in polynomial time in $\log(N)$.*

*Proof.* Let $N = pq$ such that $q < p < \mu q$. Suppose that the public exponent $e < (p^4-1)(q^4-1)$ and the private exponent verifies the following bound:

$$d < \sqrt{\frac{2\mu^2 N^4 - (\mu^2+1)^2 N^2 + 2\mu^2}{2(\mu^4-1)N^2 + 4\mu^2(\mu^2+1)N}}.$$

We know that $ed - k(p^4-1)(q^4-1) = 1$ for some positive integer $k$. Then by Theorem 8, to show that $N$ can be factored in polynomial time, it suffices to show that

$$kd < \frac{2\mu^2 N^4 - (\mu^2+1)^2 N^2 + 2\mu^2}{2(\mu^4-1)N^2 + 4\mu^2(\mu^2+1)N}.$$

We have: $k = \frac{ed-1}{(p^4-1)(q^4-1)} < \frac{ed}{(p^4-1)(q^4-1)}$. Since $e < (p^4-1)(q^4-1)$, we have $k < d$. Hence,

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

Then, we can conclude that one can find $p$ and $q$ in polynomial time using Theorem 8.

□

**Corollary 2.** *Let $N = pq$ be an RSA modulus with $q < p < \mu q$. Let $e < (p^4-1)(q^4-1)$ be a public exponent. If the private exponent $d$ satisfies*

$$d > (p^4-1)(q^4-1) - \sqrt{\frac{2\mu^2N^4 - (\mu^2+1)^2N^2 + 2\mu^2}{2(\mu^4-1)N^2 + 4\mu^2(\mu^2+1)N}},$$

*then one can find $p$ and $q$ in polynomial time in $\log(N)$.*

*Proof.* It follows from Theorem 6 and Theorem 8.

□

Our attack on the scheme of Cotan and Teseleanu [CT24b] with the equation $ex - (p^4-1)(q^4-1)y = \omega$ is summarized in the following Algorithm 1.

**Algorithm 1** Attack to factor a modulus $N$ on RSA-like cryptosystem with the equation $ex - (p^4-1)(q^4-1)y = \omega$

**Input:** The modulus $N$, the public exponent $e$ and the parameter $\mu$.
**Output:** The factors $(p, q)$ of $N$ or $\perp$.

$\mathcal{R} := \dfrac{2\mu^2 e}{2\mu^2N^4 - (\mu^2+1)^2N^2 + 2\mu^2}$.
**For** each convergent $\frac{y}{x}$ of the continued fraction expansion of $\mathcal{R}$ **do**
  $\tilde{S_1} := \left\lfloor \sqrt{\left| 2N + \sqrt{\left| (N^2+1)^2 - \frac{ex}{y} \right|} \right|} \right\rfloor$.
  $\tilde{D_1} := \left\lfloor \sqrt{\left| -2N + \sqrt{\left| (N^2+1)^2 - \frac{ex}{y} \right|} \right|} \right\rfloor$.
  $\tilde{p} := \left\lfloor \frac{1}{2}\left(\tilde{S_1} + \tilde{D_1}\right) \right\rfloor$.
  $p :=$ Coppersmith(N, p̃) ▷ See Theo. 5
  **If** $p \neq \perp$ **then**
    $q := N/p$.
    Return $(p, q)$ and stop the loop.
  **end If**
**end For**
Return $\perp$.

Notice that similar factoring algorithms for the RSA variant of Cotan and Teseleanu [CT24b], with key equation $ex - (p^n - 1)(q^n - 1)y = \omega$, can be obtained for the cases $n = 3$ and $n = 6$ using our Theorem 7 and recent results by Teseleanu [Teş25,Teş26]. For the cases $n = 2$ and $n = 1$, similar factoring algorithms can also be obtained by combining Theorem 7 with some results of Bunder *et al.* [BNST17] and Blömer and May [BM04] respectively.

### 3.2 Our Attack With the Equation $ex - (p-1)^2(q-1)^2y = \omega$

In this section, we present a new attack on the RSA-like cryptosystem of Nitaj and Seck [NS25] by studying the generalized key equation $ex-(p-1)^2(q-1)^2y = \omega$ for arbitrary primes $p, q$, i.e., $q < p < \mu q$ for some $\mu > 1$. Like our first attack, we combine continued fractions and Coppersmith's method to factor the RSA modulus $N$ in polynomial time for a given instance $(N, e)$.

**Lemma 4.** *Let $N = pq$ be an RSA modulus where the prime factors satisfy $q < p < \mu q$ for some real number $\mu > 1$ such that $\sqrt{N} > 2(\sqrt{\mu} + 1)$. Let $x$ and $y$ be positive integers, $\omega \in \mathbb{Z}$, and let $e$ be a public exponent such that $ex - (p-1)^2(q-1)^2y = \omega$. Define the following quantities:*

$$S = p + q, \quad \tilde{S} = (N + 1) - \sqrt{\frac{ex}{y}}, \quad \text{and} \quad C_\mu = \frac{\sqrt{\mu}(\sqrt{\mu} + 1)}{\sqrt{\mu} - 1}.$$

*If $|\omega| < \frac{\sqrt{\mu}-1}{\mu}\, y\, N^{\frac{3}{4}}$, then the difference between $S$ and $\tilde{S}$ verifies the following inequality:*

$$|S - \tilde{S}| < \frac{N^{\frac{1}{4}}}{C_\mu}.$$

*Proof.* We start with the the following equalities:

$$(p-1)^2(q-1)^2 = (p+q)^2 - 2(N+1)(p+q) + (N+1)^2 = \frac{ex}{y} - \frac{\omega}{y}.$$

Rearranging terms, we obtain

$$(p+q)^2 - 2(N+1)(p+q) + (N+1)^2 - \frac{ex}{y} + \frac{\omega}{y} = 0.$$

This can be written as $\left(p + q - (N+1)\right)^2 - \frac{ex}{y} + \frac{\omega}{y} = 0$, which implies

$$\left|p + q - (N+1) - \sqrt{\tfrac{ex}{y}}\right| \cdot \left|p + q - (N+1) + \sqrt{\tfrac{ex}{y}}\right| = \frac{|\omega|}{y}.$$

We isolate the factor $\left|p + q - (N+1) + \sqrt{\frac{ex}{y}}\right|$ and obtain:

$$\left|p + q - \left[(N+1) - \sqrt{\tfrac{ex}{y}}\right]\right| = \frac{|\omega|}{y \cdot \left|p + q - \left[(N+1) + \sqrt{\frac{ex}{y}}\right]\right|}.$$

We have $(p-1)(q-1) = N+1-(p+q) > 0$; then $N+1 > (p+q)$. This implies that $|N+1+\sqrt{\frac{ex}{y}} - (p+q)| = N+1+\sqrt{\frac{ex}{y}} - (p+q)$. Let's show that this value is greater than $p+q$; that is to say $N+1+\sqrt{\frac{ex}{y}} - 2(p+q) > 0$. By the lemma 2, $p+q < (\sqrt{\mu}+1)\sqrt{N} \Longrightarrow -2(p+q) > -2(\sqrt{\mu}+1)\sqrt{N}$. Then

$$N+1+\sqrt{\frac{ex}{y}} - 2(p+q) > N+1+\sqrt{\frac{ex}{y}} - 2(\sqrt{\mu}+1)\sqrt{N} > N - 2(\sqrt{\mu}+1)\sqrt{N}+1.$$

$$\Longrightarrow N+1+\sqrt{\frac{ex}{y}} - 2(p+q) > N - 2(\sqrt{\mu}+1)\sqrt{N} = \sqrt{N}(\sqrt{N} - 2(\sqrt{\mu}+1)).$$

Since $\sqrt{N} > 2(\sqrt{\mu}+1)$, then we have $\left|p+q-[(N+1)+\sqrt{\frac{ex}{y}}]\right| > p+q$. This implies that

$$\left|p+q-\left[(N+1)-\sqrt{\tfrac{ex}{y}}\right]\right| < \frac{|\omega|}{(p+q)y}.$$

We know that $|\omega| < \frac{\sqrt{\mu}-1}{\mu} y N^{\frac{3}{4}}$, and $p+q > \left(1+\frac{1}{\sqrt{\mu}}\right)\sqrt{N}$ from Lemma 2, therefore

$$\left|p+q-\left[(N+1)-\sqrt{\tfrac{ex}{y}}\right]\right| < \frac{\frac{\sqrt{\mu}-1}{\mu} y N^{\frac{3}{4}}}{\left(1+\frac{1}{\sqrt{\mu}}\right) y\sqrt{N}}.$$

Simplifying,

$$\left|p+q-\left[(N+1)-\sqrt{\tfrac{ex}{y}}\right]\right| < \frac{\sqrt{\mu}-1}{\sqrt{\mu}(\sqrt{\mu}+1)} N^{\frac{1}{4}} = \frac{N^{\frac{1}{4}}}{C_\mu}.$$

Hence

$$|S-\widetilde{S}| = \left|p+q-\left[(N+1)-\sqrt{\tfrac{ex}{y}}\right]\right| < \frac{N^{\frac{1}{4}}}{C_\mu}.$$

This ends the proof.

□

**Lemma 5.** *Let $N = pq$ be an RSA modulus with primes satisfying $q < p < \mu q$, for some real number $\mu > 1$ such that $\sqrt{N} > 2(\sqrt{\mu}+1)$. Let $x, y$ be positive integers, $\omega \in \mathbb{Z}$, and let $e$ be a public exponent such that $ex-(p-1)^2(q-1)^2 y = \omega$ such that $\left(N+1-\sqrt{(ex)/y}\right) - 2\sqrt{N} \geq 0$. Define the quantities*

$$D = p-q, \text{ and } \tilde{D} = \sqrt{\left(N+1-\sqrt{\frac{ex}{y}}\right)^2 - 4N}.$$

*If $|\omega| < \frac{\sqrt{\mu}-1}{\mu} \cdot \frac{A}{B} \cdot y N^{\frac{1}{2}}$, then $|D-\tilde{D}| < N^{\frac{1}{4}}$, where*

$$A = N+1-(\sqrt{\mu}+1)\sqrt{N}, \quad B = N+1+(\sqrt{\mu}+1)\sqrt{N}.$$

*Proof.* We begin with the well-known relation between $p$, $q$, and $N = pq$:

$$(p-q)^2 = (p+q)^2 - 4N,$$

which directly implies that $D = p - q = \sqrt{(p+q)^2 - 4N}$. As in Lemma 4, we set $S = p + q$ and $\widetilde{S} = (N+1) - \sqrt{\frac{ex}{y}}$. Then, we have

$$\widetilde{D} = \sqrt{\widetilde{S}^2 - 4N}.$$

Our goal is to prove that $|D - \widetilde{D}| < N^{\frac{1}{4}}$. For positive real numbers $a$ and $b$, it is known that the identity: $\sqrt{a} - \sqrt{b} = \frac{a-b}{\sqrt{a}+\sqrt{b}}$ holds. Applying this with $a = S^2 - 4N$ and $b = \widetilde{S}^2 - 4N$, we get

$$D - \widetilde{D} = \sqrt{S^2 - 4N} - \sqrt{\widetilde{S}^2 - 4N} = \frac{S^2 - \widetilde{S}^2}{D + \widetilde{D}} = \frac{(S - \widetilde{S})(S + \widetilde{S})}{D + \widetilde{D}}.$$

By taking absolute values, we obtain

$$|D - \widetilde{D}| = \frac{|S - \widetilde{S}|(S + \widetilde{S})}{D + \widetilde{D}} < \frac{|S - \widetilde{S}|(S + \widetilde{S})}{D}.$$

Since $\widetilde{S} = N + 1 - \sqrt{\frac{ex}{y}} < N + 1$ and $S \leq (\sqrt{\mu} + 1)\sqrt{N}$, it follows that

$$|D - \widetilde{D}| < \frac{|S - \widetilde{S}|(N + 1 + (\sqrt{\mu} + 1)\sqrt{N})}{D}. \tag{7}$$

Let us now express $S - \widetilde{S}$ explicitly:

$$S - \widetilde{S} = (N + 1 - \varphi(N)) - \left(N + 1 - \sqrt{\tfrac{ex}{y}}\right) = \sqrt{\frac{ex}{y}} - \varphi(N).$$

Since $\dfrac{ex}{y} = \varphi(N)^2 + \dfrac{\omega}{y}$, we can rewrite the previous difference as

$$S - \widetilde{S} = \sqrt{\varphi(N)^2 + \frac{\omega}{y}} - \varphi(N).$$

Using the identity $\sqrt{u} - \sqrt{v} = \frac{u-v}{\sqrt{u}+\sqrt{v}}$, we get

$$S - \widetilde{S} = \frac{\frac{\omega}{y}}{\sqrt{\varphi(N)^2 + \frac{\omega}{y}} + \varphi(N)}.$$

Taking absolute values,

$$|S - \widetilde{S}| = \frac{|\omega|}{y\left(\sqrt{\varphi(N)^2 + \frac{\omega}{y}} + \varphi(N)\right)} < \frac{|\omega|}{y\varphi(N)} < \frac{|\omega|}{yA}.$$

Substituting this into the previous inequality (7), we have

$$|D - \widetilde{D}| < \frac{|\omega|}{yD} \cdot \frac{B}{A}.$$

By hypothesis, we know that $|\omega| < \frac{\sqrt{\mu}-1}{\mu} \cdot \frac{A}{B}\, y\, N^{\frac{1}{2}}$. So substituting this bound on $|\omega|$, we obtain

$$|D - \widetilde{D}| < \left(\frac{\sqrt{\mu}-1}{\mu} \cdot \frac{A}{B} y N^{\frac{1}{2}}\right)\left(\frac{1}{yD} \cdot \frac{B}{A}\right).$$

Since by Remark 3, we assumed that $D > N^{\frac{1}{4}}$, we have

$$|D - \widetilde{D}| < \frac{\sqrt{\mu}-1}{\mu} N^{\frac{1}{2}} \cdot N^{-\frac{1}{4}} = \frac{\sqrt{\mu}-1}{\mu} N^{\frac{1}{4}}.$$

Finally, since $\mu > 1$, we conclude that

$$|D - \widetilde{D}| < N^{\frac{1}{4}},$$

which completes the proof.

□

**Lemma 6.** *Let $N = pq$ be an RSA modulus, where the prime factors satisfy $q < p < \mu q$ for some real constant $\mu > 1$ such that $\sqrt{N} > 2(\sqrt{\mu}+1)$. Let $x$ and $y$ be positive integers, and let $e$ be a public exponent such that $ex-(p-1)^2(q-1)^2y = \omega$, where $\omega$ is an integer satisfying the bound*

$$|\omega| < \frac{\sqrt{\mu}-1}{\mu} \cdot \frac{A}{B}\, y\, N^{\frac{1}{2}},$$

*with*

$$A = N + 1 - (\sqrt{\mu}+1)\sqrt{N}, \quad B = N + 1 + (\sqrt{\mu}+1)\sqrt{N}.$$

*Moreover, assume that $\left(N + 1 - \sqrt{(ex)/y}\right) - 2\sqrt{N} \geq 0$. Then, given the values of $e$, $N$, $x$, and $y$, one can compute the prime factors $p$ and $q$ of $N$ in polynomial time.*

*Proof.* Suppose that $e$, $N$, $x$, and $y$ are known integers such that $ex-(p-1)^2(q-1)^2y = \omega$, where $\omega$ satisfies $|\omega| < \frac{\sqrt{\mu}-1}{\mu} \cdot \frac{A}{B}\, y\, N^{\frac{1}{2}}$ with $A = N+1-(\sqrt{\mu}+1)\sqrt{N}$, and $B = N + 1 + (\sqrt{\mu}+1)\sqrt{N}$. Define the following quantities:

$$S = p + q, \text{ and } \tilde{S} = N + 1 - \sqrt{\frac{ex}{y}}$$

and

$$D = p - q, \text{ and } \tilde{D} = \sqrt{\left(N + 1 - \sqrt{\frac{ex}{y}}\right)^2 - 4N}.$$

Since $|\omega| < \frac{\sqrt{\mu}-1}{\mu} \cdot \frac{A}{B}\, y\, N^{\frac{1}{2}} < \frac{\sqrt{\mu}-1}{\mu} \cdot y\, N^{\frac{1}{2}} < \frac{\sqrt{\mu}-1}{\mu} \cdot y\, N^{\frac{3}{4}}$, we can apply Lemma 4. Combining it with Lemma 5, we obtain the following bounds:

$$|S - \widetilde{S}| < \frac{N^{\frac{1}{4}}}{C_\mu} < N^{\frac{1}{4}} \quad \text{and} \quad |D - \widetilde{D}| < N^{\frac{1}{4}},$$

where $C_\mu = \frac{\sqrt{\mu}(\sqrt{\mu}+1)}{\sqrt{\mu}-1} > 1$. We know that from $p+q$ and $p-q$, we can express $p$ as

$$p = \frac{1}{2}\big((p+q) + (p-q)\big) = \frac{1}{2}\big(S + D\big).$$

Replacing $p+q$ and $p-q$ by their approximations, we define

$$\widetilde{p} = \frac{1}{2}\big(\widetilde{S} + \widetilde{D}\big).$$

The error between $p$ and $\widetilde{p}$ is then

$$\big|p - \widetilde{p}\big| = \left|\frac{1}{2}(S + D - \widetilde{S} - \widetilde{D})\right| \leq \frac{1}{2}|S - \widetilde{S}| + \frac{1}{2}|D - \widetilde{D}|.$$

Using the bounds for $|S - \widetilde{S}|$ and $|D - \widetilde{D}|$, we get

$$\big|p - \widetilde{p}\big| < \frac{1}{2}N^{\frac{1}{4}} + \frac{1}{2}N^{\frac{1}{4}} = N^{\frac{1}{4}}.$$

Thus, we have constructed an approximation $\widetilde{p}$ of $p$ with error strictly less than $N^{\frac{1}{4}}$.

Since $|p - \widetilde{p}| < N^{\frac{1}{4}}$, we can apply Coppersmith's method 5 to efficiently recover the exact value of $p$ from its approximation $\widetilde{p}$. Once $p$ is recovered, the other prime factor can be easily computed as $q = \frac{N}{p}$.

We have shown that, given the values of $e$, $N$, $x$, and $y$, one can first approximate $p$ within $N^{\frac{1}{4}}$, then apply Coppersmith's algorithm to determine $p$ exactly, and finally compute $q$. Hence, the RSA modulus $N$ can be factored in polynomial time under the stated conditions.

□

**Theorem 9.** *Let $N = pq$ be an RSA modulus where $q < p < \mu q$ for some real $\mu > 1$ such that $\sqrt{N} > 2(\sqrt{\mu}+1)$. Let $e$ be a public exponent satisfying the key equation: $ex - \psi(N)y = \omega$ with $x, y > 0, \omega \in \mathbb{Z}$ and $\psi(N) = (p-1)^2(q-1)^2$ such that $\left(N + 1 - \sqrt{(ex)/y}\right) - 2\sqrt{N} \geq 0$. If the following two conditions hold:*

$$\begin{cases} xy < \dfrac{2\mu N^2 - (\mu-1)^2 N + 2\mu}{2(3\mu^2 + 4\mu^{3/2} + 4\mu + 1)\, N + 8\mu(\sqrt{\mu}+1)N^{3/2} + \left[4(\sqrt{\mu}-1) + 8\mu(\sqrt{\mu}+1)\right] N^{1/2}}, \\ |\omega| < \dfrac{\sqrt{\mu}-1}{\mu} \cdot \dfrac{N + 1 - (\sqrt{\mu}+1)\sqrt{N}}{N + 1 + (\sqrt{\mu}+1)\sqrt{N}} \cdot y N^{1/2}, \end{cases}$$

*then one can find $p$ and $q$ in polynomial time.*

*Proof.* Suppose that $N = pq$ with $q < p < \mu q$ such that $\sqrt{N} > 2(\sqrt{\mu}+1)$. Let $e$ be a public exponent satisfying $ex - \psi(N)y = \omega$ such that $\left(N + 1 - \sqrt{(ex)/y}\right) - 2\sqrt{N} \geq 0$. We have

$$\psi(N) = (p-1)^2(q-1)^2 = N^2 + 1 + 2N + (p+q)^2 - 2(N+1)(p+q).$$

Substituting this into the relation $ex - \psi(N)y = \omega$, we obtain:

$$ex - \left[N^2 + 2N + 1 + (p+q)^2 - 2(N+1)(p+q)\right] y = \omega.$$

This implies that

$$ex - \left(N^2 + 2N + 1 - \frac{(\mu+1)^2}{2\mu}N\right) y - \left[(p+q)^2 - 2(N+1)(p+q) + \frac{(\mu+1)^2}{2\mu}N\right] y = \omega,$$

$$\iff ex - \left(N^2 - \frac{(\mu-1)^2}{2\mu}N + 1\right) y = \omega + \left[(p+q)^2 - 2(N+1)(p+q) + \frac{(\mu+1)^2}{2\mu}N\right] y.$$

Dividing both sides by $N^2 - \frac{(\mu-1)^2}{2\mu}N + 1$, we obtain

$$\frac{2\mu ex}{2\mu N^2 - (\mu-1)^2 N + 2\mu} - y = \frac{\omega + \left[(p+q)^2 - 2(N+1)(p+q) + \frac{(\mu+1)^2}{2\mu}N\right] y}{N^2 - \frac{(\mu-1)^2}{2\mu}N + 1}$$

$$\implies \frac{2\mu e}{2\mu N^2 - (\mu-1)^2 N + 2\mu} - \frac{y}{x} = \frac{\omega + \left[(p+q)^2 - 2(N+1)(p+q) + \frac{(\mu+1)^2}{2\mu}N\right] y}{\left(N^2 - \frac{(\mu-1)^2}{2\mu}N + 1\right)} \cdot \frac{1}{x}$$

$$\implies \left|\frac{2\mu e}{2\mu N^2 - (\mu-1)^2 N + 2\mu} - \frac{y}{x}\right| \leq \frac{|\omega| + \left|(p+q)^2 - 2(N+1)(p+q) + \frac{(\mu+1)^2}{2\mu}N\right| y}{\left(N^2 - \frac{(\mu-1)^2}{2\mu}N + 1\right)} \cdot \frac{1}{x}$$

$$\implies \left|\frac{2\mu e}{2\mu N^2 - (\mu-1)^2 N + 2\mu} - \frac{y}{x}\right| \leq \frac{|\omega| + (p+q)^2 y + 2(N+1)(p+q)y + \frac{(\mu+1)^2}{2\mu}Ny}{\left(N^2 - \frac{(\mu-1)^2}{2\mu}N + 1\right)} \cdot \frac{1}{x}.$$

By Lemma 2, we know that

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

then,

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

Using the previous upper bound of $p+q$, we get

$$\left|\frac{2\mu e}{2\mu N^2 - (\mu-1)^2 N + 2\mu} - \frac{y}{x}\right| < \frac{|\omega| + (\sqrt{\mu}+1)^2 Ny + 2(N+1)(\sqrt{\mu}+1)\sqrt{N}y + \frac{(\mu+1)^2}{2\mu}Ny}{\left(N^2 - \frac{(\mu-1)^2}{2\mu}N + 1\right)} \cdot \frac{1}{x}.$$

Since

$$|\omega| < \frac{\sqrt{\mu}-1}{\mu} \cdot \frac{N+1-(\sqrt{\mu}+1)\sqrt{N}}{N+1+(\sqrt{\mu}+1)\sqrt{N}} \cdot yN^{1/2} < \frac{\sqrt{\mu}-1}{\mu} yN^{1/2},$$

substituting and expanding $2(N+1)(\sqrt{\mu}+1)\sqrt{N} = 2(\sqrt{\mu}+1)N^{3/2}+2(\sqrt{\mu}+1)N^{1/2}$, we get

$$\left|\frac{2\mu e}{2\mu N^2-(\mu-1)^2N+2\mu} - \frac{y}{x}\right| < \frac{\left[(\sqrt{\mu}+1)^2+\frac{(\mu+1)^2}{2\mu}\right]N + 2(\sqrt{\mu}+1)N^{3/2} + \left[\frac{\sqrt{\mu}-1}{\mu}+2(\sqrt{\mu}+1)\right]N^{1/2}}{N^2-\frac{(\mu-1)^2}{2\mu}N+1} \cdot \frac{y}{x}.$$

Multiplying numerator and denominator by $2\mu$ and setting $\alpha_\mu = 3\mu^2+4\mu^{3/2}+4\mu+1$ and $\beta_\mu = 2(\sqrt{\mu}-1)+4\mu(\sqrt{\mu}+1)$, this becomes

$$\left|\frac{2\mu e}{2\mu N^2-(\mu-1)^2N+2\mu} - \frac{y}{x}\right| < \frac{\alpha_\mu N + 4\mu(\sqrt{\mu}+1)N^{3/2}+\beta_\mu N^{1/2}}{2\mu N^2-(\mu-1)^2N+2\mu} \cdot \frac{y}{x}.$$

Since

$$xy < \frac{2\mu N^2-(\mu-1)^2N+2\mu}{2(3\mu^2+4\mu^{3/2}+4\mu+1)N + 8\mu(\sqrt{\mu}+1)N^{3/2}+\left[4(\sqrt{\mu}-1)+8\mu(\sqrt{\mu}+1)\right]N^{1/2}}.$$

then the following inequality holds:

$$\frac{\alpha_\mu N + 4\mu(\sqrt{\mu}+1)N^{3/2}+\beta_\mu N^{1/2}}{2\mu N^2-(\mu-1)^2N+2\mu} < \frac{1}{2xy}.$$

Hence

$$\left|\frac{2\mu e}{2\mu N^2-(\mu-1)^2N+2\mu} - \frac{y}{x}\right| < \frac{1}{2xy} \cdot \frac{y}{x} = \frac{1}{2x^2}.$$

Therefore $\frac{y}{x}$ is among the convergent of the continued fraction expansion of $(2\mu e)/(2\mu N^2-(\mu-1)^2N+2\mu)$. Once we get $x$ and $y$, by Lemma 6, one can find $p$ and $q$ in polynomial time in $\log(N)$.

□

By using a recent result of Seck et al. [SNS+26], we can derive the following corollary which shows the weakness of too small and too large private exponents.

**Corollary 3.** *Let $N = pq$ be an RSA modulus with $q < p < \mu q$ for some real $\mu > 1$ such that $\sqrt{N} > 2(\sqrt{\mu}+1)$. Let $e < (p-1)^2(q-1)^2$ be a public exponent and $d < (p-1)^2(q-1)^2$ be the corresponding private exponent satisfying the key equation $ed - k(p-1)^2(q-1)^2 = 1$ for some integer $k$ such that $\left(N+1-\sqrt{(ed)/k}\right) - 2\sqrt{N} \geq 0$. Define the following bound:*

$$\mathcal{B}_\mu = \frac{2\mu N^2-(\mu-1)^2N+2\mu}{2(3\mu^2+4\mu^{3/2}+4\mu+1)N + 8\mu(\sqrt{\mu}+1)N^{3/2}+\left[4(\sqrt{\mu}-1)+8\mu(\sqrt{\mu}+1)\right]N^{1/2}}.$$

*If $d$ satisfies the following bounds:*

$$d < \sqrt{\mathcal{B}_\mu} \text{ or } \left|(p-1)^2(q-1)^2 - d\right| < \sqrt{\mathcal{B}_\mu},$$

*then one can find $p$ and $q$ in polynomial time in $\log(N)$.*

*Proof.* Suppose that $e < (p-1)^2(q-1)^2$ and $d < \sqrt{\mathcal{B}_\mu}$ such that $ed - k(p-1)^2(q-1)^2 = 1$ and $\left(N + 1 - \sqrt{(ed)/k}\right) - 2\sqrt{N} \geq 0$. This implies that

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

But $e < (p-1)^2(q-1)^2$, then $kd < d^2 < \mathcal{B}_\mu$. By Theorem 9, one can find $p$ and $q$ in polynomial time in $\log(N)$. Now suppose that $\left|(p-1)^2(q-1)^2 - d\right| < \sqrt{\mathcal{B}_\mu}$, then applying Theorem 6 and Theorem 9, we get also that $p$ and $q$ can be found in polynomial time in $\log(N)$.

□

Our attack on the scheme of Nitaj and Seck [NS25] with the equation $ex - (p-1)^2(q-1)^2 y = \omega$ is summarized in the following Algorithm 2.

**Algorithm 2** Attack to factor a modulus $N$ on RSA-like cryptosystem with the equation $ex - (p-1)^2(q-1)^2 y = \omega$

**Input:** The modulus $N$, the public exponent $e$ and the parameter $\mu$.
**Output:** The factors $(p, q)$ of $N$ or $\perp$.

$\mathcal{K} := \dfrac{2\mu e}{2\mu N^2 - (\mu-1)^2 N + 2\mu}$.
**For** each convergent $\dfrac{y}{x}$ of the continued fraction expansion of $\mathcal{K}$ **do**
  $\tilde{S} = \left\lfloor N + 1 - \sqrt{\dfrac{ex}{y}} \right\rfloor$.
  $\tilde{D} = \left\lfloor \sqrt{\left| \left( N + 1 - \sqrt{\dfrac{ex}{y}} \right)^2 - 4N \right|} \right\rfloor$.
  $\tilde{p} := \left\lfloor \frac{1}{2}\left(\tilde{S} + \tilde{D}\right) \right\rfloor$.
  $p :=$ Coppersmith(N, $\tilde{\text{p}}$) ▷ See Theo. 5
  **If** $p \neq \perp$ **then**
    $q := N/p$.
    Return $(p, q)$ and stop the loop.
  **end If**
**end For**
Return $\perp$.

## 4 Numerical Examples

In this section, we give two numerical examples demonstrating the effectiveness of our attacks. The first example, with key equation $ex - (p^4-1)(q^4-1)\, y = \omega$ is a direct application of Algorithm 1, and the second example, with key equation $ex - (p-1)^2(q-1)^2\, y = \omega$ is an application of Algorithm 2. The experiments were performed on a machine with the following specifications: Intel(R) Core(TM) i5-10210U CPU @ 1.60GHz (2.11 GHz) and 16 GB of RAM, running Windows 11.

The total runtime for the first example is approximately 412 ms (7.42 ms for computing the convergents and about 3.29 ms for each Coppersmith step), while the second example takes around 93.5 ms (2.23 ms for computing the convergents and about 4.21 ms for each Coppersmith step).

### 4.1 A Numerical Example for the Equation $ex-(p^4-1)(q^4-1)y=\omega$

Let us present a numerical example to demonstrate the effectiveness of our attack against the cryptosystem of Cotan and Teseleanu [CT24b], with key equation $ex-(p^4-1)(q^4-1)y=\omega$. Consider the following instance $(N,e,\mu)$ where $N$ is a 195-bit modulus.

$$
\begin{aligned}
N &= 267755019081919059468766682566076282527064743865046990470 17\\
e &= 453050078713827481952641242194154220277177895571370108486994 49\\
&\quad 212800560972746423187054123667434674299935198694810635460479 50\\
&\quad 691802080601297771452630781047920754283193563428820345543075 04\\
&\quad 611258078457626617783956800491143320938846608793\\
\mu &= 15.
\end{aligned}
$$

Before applying our attack to the instance $(N,e,\mu)$, we would like to highlight that the attack of Seck *et al.* [SNS+26] fails to recover the factors $p$ and $q$ of $N$ given the public parameters $(N,e)$ when using their implementation. This can be explained by the fact that the condition $q<p<2q$ is not satisfied. We emphasize that both our approach and that of Seck *et al.* [SNS+26] provide only sufficient conditions for the attacks to succeed; consequently, outside these bounds, successful recovery of the factors is not guaranteed.

**Our attack given the instance $(N,e,\mu)$:** Using the instance $(N,e,\mu)$ we get $2\mu^2N^4-(\mu^2+1)^2N^2+2\mu^2$

$$
\begin{aligned}
=&231293269686838772825147596949286534730255264912936193785242 0\\
&135947166074971527082143774724077439160236775851275166904811 1\\
&468474588420989678594582338153338642172000289005941032935203 3\\
&121701951719187146387674135012335593620864062243175936
\end{aligned}
$$

The continued fraction expansion of $\dfrac{2\mu^2e}{2\mu^2N^4-(\mu^2+1)^2N^2+2\mu^2}$ is given as follows.

$$
\begin{aligned}
&[0;1,7,2,3,2,1,9,60,1,29,1,1,1,1,1,2,2,5,3,6,1,2,4,1,1,1,1,1,2,\\
&5,1,2,2,1,2,14,1,1,1,2,1,1,4,1,5,6,2,1,1,1,1,1,5,5,1,1,1,1,1,\\
&6,4,1,5,1,2,1,1,1,2,1,5,7,2,1,1,1,4,1,5,1,3,2,1,1,1,1,1,16,58,\\
&4,1,3,1,63,1,83,3,1,5,2,3,3,3,4,6\ldots].
\end{aligned}
$$

For the $132^{\text{th}}$ convergent $C_{132}$ we have

$$\begin{aligned} x = &\quad 185478571698212416718414381411112925244143304134720783394 3, \\ y = &\quad 163489351547583158392464635508002652684652512306529936906 3. \end{aligned}$$

Notice that the following bound for $xy$ hold:

$$xy < \frac{2\mu^2 N^4 - (\mu^2+1)^2 N^2 + 2\mu^2}{2(\mu^4-1)N^2 + 4\mu^2(\mu^2+1)N}.$$

By Lemma 3, we obtain the following approximations of $p+q$ and $p-q$:

$$\begin{aligned} \tilde{S_1} &= 672640407479450197855897199978, \\ \tilde{D_1} &= 587659008389519353487629115304. \end{aligned}$$

From the approximation $\tilde{S_1}$ of $p+q$ and $\tilde{D_1}$ of $p-q$, we compute the approximation $\tilde{p}$ of $p$ and obtain

$$\tilde{p} = \left\lfloor \frac{\tilde{S_1} + \tilde{D_1}}{2} \right\rfloor = 630149707934484775671763157641.$$

By applying Coppersmith's algorithm, we find

$$p = 630149707934484775671763157641$$

which is a divisor of $N$. Finally, we compute the other factor as

$$q = N/p = 424906995449654224184134042337.$$

One can check that $\omega = ex - (p^4-1)(q^4-1)y = -1$ which means the bound $|\omega| < yN$ is satisfied. The private exponent $d$ is

$$\begin{aligned} d = &\, 513985043748530606278105770998414521622789477584302652856 09 \\ &\, 336354381468332700601825417216090609759116372796695003701 36 \\ &\, 482381861786620522704064923189344486340199492054104489711 12 \\ &\, 429586820607402450617885704240913771707686120208991487657. \end{aligned}$$

Notice that $d$ is large but, as shown by Seck *et al.* [SNS+26], $\varphi_4(N) - d$ is small.

$$\varphi_4(N) - d = 185478571698212416718414381411112925244143304134720783394 3$$

### 4.2 A Numerical Example for the Equation $ex-(p-1)^2(q-1)^2y = \omega$

In this section, we present a detailed numerical example to illustrate the attack developed in Theorem 9. Consider the following public parameters when $N$ is a 200-bit size and $\mu = 2$:

$$N = 265839721739624484719433732023423940832894821073878576476773,$$

$$e = 110880032405182550312827189834993561274916981853311646141448\backslash$$
$$98087286354771002542344519459394576885438741530757179984727.$$

Our goal is to recover the prime factors $p$ and $q$ of $N$ given the public instance $(N, e, \mu)$. The continued fraction expansion of $\frac{4e}{4N^2-N+4}$ is given as follows:

$$[0; 6, 2, 1, 2, 10, 1, 40, 1, 1, 1, 2, 1, 1, 5, 20, 1, 1, 1, 1, 5, 7, 4, 1, 1, 1, 1, 1, 5, 3,$$
$$1, 8, 117, 6, 2, 8, 1, 1, 4, 5, 2, 2, 3, 1, 1, 2, 1, 1, 1, 4, 1, 4, 1, 2, 2, 1, 1, 1, 3, 1, 1,$$
$$2, 2, 2, 2, 9, 2, 12, 26, 6, 18, 1, 1, 4, 1, 2, 1, 1, 1, 7, 33, 2, 1, 1, 1, 4, 1, 369, 4, 2,$$
$$2, 2, 1, 2, 14, 1, 2, 3, 1, 1, 2, 1, 1, 3, 2, 9, 2, 1, 2, 7, 1, 4, 6, 1, 3, 7, 1, 1, 9, 1, 20,$$
$$1, 936, 3, 8, 3, 1, 1, 3, 1, 5, 2, 18, 2, 1, 11, 3, 225, 2, 4, 33, 1, 32, 1, 1, 3, 1, \ldots]$$

Let $(y, x)$ denote the numerator-denominator pair of the selected convergent $C_{31}$:

$$x = 83688527736729 \text{ and } y = 13130447409016.$$

We can check that

$$xy < \frac{2\mu N^2 - (\mu-1)^2 N + 2\mu}{2(3\mu^2 + 4\mu^{3/2} + 4\mu + 1)\, N + 8\mu(\sqrt{\mu}+1)N^{3/2} + \left[4(\sqrt{\mu}-1) + 8\mu(\sqrt{\mu}+1)\right] N^{1/2}}.$$

From $(x, y)$, we derive the approximations $\tilde{S}$ and $\tilde{D}$ of $p+q$ and $p-q$ (respectively).

$$\tilde{S} = 10314840158580062276149807912 06, \qquad \tilde{D} = 24502816410806819107771882812.$$

Consequently, an approximation $\tilde{p}$ of $p$ can be computed as:

$$\tilde{p} = \frac{\tilde{S} + \tilde{D}}{2} = 52799341613440652336137633 7009.$$

We apply Coppersmith's method to the instance $(N, \tilde{p})$ to recover the exact value of $p$:

$$p = 52799341613440652336137633 7009$$

which divides $N$. The cofactor then follows as

$$q = \frac{N}{p} = 50349059972359970425360445 4197.$$

This completes the factorization of $N$.

## 5 Comparison with former attacks

In this section, we compare our attacks with previous attacks on two RSA variants studied in this paper: the cryptosystem of Cotan and Teseleanu [CT24b] with key equation $ed-(p^n-1)(q^n-1)k = 1$ for some integer $n > 1$, and the cryptosystem of Nitaj and Seck [NS25] with key equation $ed-(p-1)^2(q-1)^2k = 1$.

- For the RSA variant of Nitaj and Seck [NS25], there is a practical attack proposed by Rahmani and Nitaj [RN26] based on Coppersmith's method and lattice reduction techniques. However, their attack targets only small private exponents and balanced moduli $N = pq$ with $q < p < 2q$. Their attack relies on the key equation $ed - (p-1)^2(q-1)^2k = 1$. In contrast, our attack on the same scheme is based on the generalized key equation $ex - (p-1)^2(q-1)^2y = \omega$ and applies to a wider range of parameters, including larger private exponents and unbalanced moduli with $q < p < \mu q$ for some $\mu > 1$.
- For the RSA variant of Cotan and Teseleanu [CT24b], several attacks have been proposed based either on Coppersmith's method, continued fractions, or both. However, almost all of these attacks target balanced moduli $N = pq$ with $q < p < 2q$ and small private exponents [CT24b,RNZ26a,RNZ26b,CT24a] [SNS+26,RN26], or are related to the key equation $ed-(p^n-1)(q^n-1)k = \pm 1$ [SC25].
  For the specific case $n = 4$, our attack is based on the generalized key equation $ex-(p^4-1)(q^4-1)y = \omega$ and applies to a wider range of parameters, including larger private exponents and unbalanced moduli with $q < p < \mu q$ for some $\mu > 1$. Even in the balanced case ($\mu = 2$), our attack applies to a wider range of parameters than the attack of Seck *et al.* [SNS+26].
  Notice that by studying the generalized equation $ex-(p^4-1)(q^4-1)y = \omega$, Seck *et al.* [SNS+26] showed that one can factor the modulus $N$ in polynomial time if the following conditions hold:

$$xy < \frac{2N^4 - 49N^2 + 2}{170N^2 + 4N} \quad \text{and} \quad |\omega| < yN.$$

  In Theorem 7, we have shown that one can factor $N$ in polynomial time if

$$xy < \frac{2\mu^2N^4 - (\mu^2+1)^2N^2 + 2\mu^2}{2(\mu^4-1)N^2 + 4\mu^2(\mu^2+1)N} \quad \text{and} \quad |\omega| < yN.$$

  Setting $\mu = 2$, the above conditions become

$$xy < \frac{8N^4 - 25N^2 + 8}{30N^2 + 80N} \quad \text{and} \quad |\omega| < yN.$$

  Define the function

$$f(N) = \frac{8N^4 - 25N^2 + 8}{30N^2 + 80N} - \frac{2N^4 - 49N^2 + 2}{170N^2 + 4N}.$$

  Simplifying $f(N)$ gives

$$f(N) = \frac{650N^5 - 64N^4 - 1390N^3 + 1910N^2 + 650N - 64}{10(3N^2 + 8N)(85N + 2)}.$$

  Notice that the numerator of $f(N)$ is positive for all $N > 1$, then $f(N) > 0$ for all $N > 1$. Therefore, the bound on $xy$ in our attack is larger than the bound in the attack of Seck *et al.* [SNS+26] for all $N > 1$. Hence, our attack applies to a wider range of parameters than theirs.

## Acknowledgments

The authors thank the anonymous reviewers for their valuable comments and suggestions, which have greatly improved the quality of this paper.

## 6 Conclusion

In this paper, we have presented novel polynomial-time attacks on two RSA variants with moduli $N = pq$ product of two unknown arbitrary primes $p$ and $q$ where $q < p < \mu q$ for some real number $\mu > 1$. Our attacks extend the work of Seck et al. [SNS+26] and Rahmani and Nitaj [RN26] published in AfricaCrypt 2025 by demonstrating that the generalized key equations $ex - (p^n - 1)(q^n - 1)y = \omega$ and $ex - (p-1)^2(q-1)^2y = \omega$ can be exploited to factor $N$ efficiently under certain conditions on the parameters involved. Our attacks are based on the Coppersmith method which is based on lattice reduction techniques and continued fractions.

## References

BD99. Dan Boneh and Glenn Durfee. Cryptanalysis of RSA with private key d less than $N^{0.292}$. In *Advances in Cryptology – EUROCRYPT'99*, volume 1592 of *Lecture Notes in Computer Science*, pages 1–11, 1999.

BM04. Johannes Blömer and Alexander May. A generalized wiener attack on RSA. In *Public Key Cryptography – PKC 2004*, volume 2947 of *Lecture Notes in Computer Science*, pages 1–13, 2004. doi:10.1007/978-3-540-24632-9_1.

BNMB22. Hatem M. Bahig, Dieaa I. Nassr, Mohammed A. Mahdi, and Hazem M. Bahig. Small private exponent attacks on RSA using continued fractions and multicore systems. *Symmetry*, 14(9):1897, 2022. doi:10.3390/sym14091897.

BNST17. Martin Bunder, Abderrahmane Nitaj, Willy Susilo, and Joseph Tonien. A generalized attack on RSA type cryptosystems. *Theoretical Computer Science*, 704:74–81, 2017. doi:10.1016/j.tcs.2017.09.009.

Bon99. Dan Boneh. Twenty years of attacks on the RSA cryptosystem. *Notices of the AMS*, 46(2):203–213, 1999.

BR98. Mihir Bellare and Phillip Rogaway. PSS: Provably secure encoding method for digital signatures. Technical report, IEEE P1363a, 1998.

Cop96. Don Coppersmith. Finding a small root of a univariate modular equation. In *Advances in Cryptology – EUROCRYPT '96*, volume 1070 of *Lecture Notes in Computer Science*, pages 155–165, 1996. doi:10.1007/3-540-68339-9_14.

CT24a. Paul Cotan and George Teşeleanu. A security analysis of two classes of RSA-like cryptosystems. *Journal of Mathematical Cryptology*, 18(1):20240013, 2024. doi:10.1515/jmc-2024-0013.

CT24b. Paul Cotan and George Teşeleanu. Small private key attack against a family of RSA-like cryptosystems. In *Secure IT Systems*, pages 57–72, 2024. doi:10.1007/978-3-031-47748-5_4.

EES02. H. Elkamchouchi, K. Elshenawy, and H. Shaban. Extended RSA cryptosystem and digital signature schemes in the domain of gaussian integers. In *The 8th International Conference on Communication Systems (ICCS 2002)*, volume 1, pages 91–95, 2002.

FOPS01. Eiichiro Fujisaki, Tatsuaki Okamoto, David Pointcheval, and Jacques Stern. RSA-OAEP is secure under the RSA assumption. In *Annual International Cryptology Conference*, pages 260–274, 2001. doi:10.1007/3-540-44647-8_16.

Hås86. Johan Håstad. On using RSA with low exponent in a public key network. In *Advances in Cryptology – CRYPTO '85*, volume 218 of *Lecture Notes in Computer Science*, pages 403–408, 1986. doi:10.1007/3-540-47721-7_29.

HW08. G. H. Hardy and Edward M. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, 2008.

LLL82. Arjen K. Lenstra, Hendrik W. Lenstra, and László Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261:515–534, 1982. doi:10.1007/BF01457454.

May03. Alexander May. *New RSA Vulnerabilities Using Lattice Reduction Methods*. PhD thesis, University of Paderborn, 2003.

Moo64. C. G. Moore. *An Introduction to Continued Fractions*. National Council of Teachers of Mathematics, 1964.

MP19. Majid Mumtaz and Luo Ping. Forty years of attacks on the RSA cryptosystem: A brief survey. *Journal of Discrete Mathematical Sciences and Cryptography*, 22(1):9–29, 2019. doi:10.1080/09720529.2018.1564201.

NS25. Abderrahmane Nitaj and Michel Seck. A new public key encryption scheme based on the cubic Pell curve using encoding functions. *Moroccan Journal of Algebra and Geometry with Applications*, 4(1):89–107, 2025.

RN26. Mohamed Rahmani and Abderrahmane Nitaj. Improved cryptanalysis of an RSA variant based on cubic Pell curve. In *Progress in Cryptology – AFRICACRYPT 2025*, volume 15651 of *Lecture Notes in Computer Science*, pages 107–125, 2026. doi:10.1007/978-3-031-97260-7_6.

RNZ26a. Mohammed Rahmani, Abderrahmane Nitaj, and Mhammed Ziane. Cryptanalysis of some algebraic variants of the RSA cryptosystem. *Finite Fields and Their Applications*, 110:102757, 2026.

RNZ26b. Mohammed Rahmani, Abderrahmane Nitaj, and Mhammed Ziane. A novel cryptanalytic attack on a family of RSA-like cryptosystems. *Discrete Mathematics*, 349(1):114660, 2026.

RSA78. R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978. doi:10.1145/359340.359342.

SC25. Michel Seck and Abdoul Aziz Ciss. A new generalized lattice attack against a family of RSA-like cryptosystems. *Theoretical Computer Science*, 1055:115548, 2025. doi:10.1016/j.tcs.2025.115548.

SN25. Michel Seck and Abderrahmane Nitaj. A new public key cryptosystem based on the cubic Pell curve. In Andrzej Dąbrowski, Josef Pieprzyk, and Jacek Pomykała, editors, *Number-Theoretic Methods in Cryptology*, pages 239–261, Cham, 2025. Springer Nature Switzerland.

SNS+26. Michel Seck, Oumar Niang, Djiby Sow, Abderrahmane Nitaj, Mengce Zheng, and Maher Boudabra. A new generalized attack on RSA-like cryptosystems. In *Progress in Cryptology – AFRICACRYPT 2025*, pages 126–144, 2026. doi:10.1007/978-3-031-97260-7_7.

Teş25. George Teşeleanu. A generalized Wiener-type attack against an RSA-like cryptosystem. In *Cyber Security, Cryptology, and Machine Learning (CSCML 2025)*, pages 53–67, Be'er Sheva, Israel, 2025. Springer. doi:10.1007/978-3-032-10759-6_4.

Teş26. George Teşeleanu. Attacking an RSA-like cryptosystem using continued fractions and lattices. In Raimundas Matulevičius, Liina Kamm, and Mubashar Iqbal, editors, *Secure IT Systems*, pages 43–56, Cham, 2026. Springer Nature Switzerland. doi:10.1007/978-3-032-14782-0_3.

Wie90. Michael J Wiener. Cryptanalysis of short RSA secret exponents. *IEEE Transactions on Information theory*, 36(3):553–558, 1990. doi:10.1109/18.54902.