



Article

An Extended Coppersmith-Based Attack on RSA

Mohammed Rahmani ¹ , Abderrahmane Nitaj ^{2,*} and Mhammed Ziane ¹

¹ ACSA Laboratory, Department of Mathematics, Sciences Faculty, Mohammed First University, Oujda 60000, Morocco; mohammed.rahmani@ump.ac.ma (M.R.); m.ziane@ump.ac.ma (M.Z.)

² Université Caen Normandie, CNRS, Normandie University, LMNO UMR6139, F-14000 Caen, France

* Correspondence: abderrahmane.nitaj@unicaen.fr

Abstract

Lattice-based cryptanalysis has become one of the most powerful tools for evaluating the security of the RSA cryptosystem. Most existing attacks rely on the classical key equation $ed - k\varphi(N) = 1$ and are effective mainly when the decryption exponent is sufficiently small or when significant information about the RSA prime factors is available. However, the dependence on this classical equation restricts the applicability of existing attacks and limits the range of weak exponents that can be targeted. In this paper, we propose a generalized lattice-based technique for solving the extended key equation $er - x\varphi(N) = s$ when an approximation of one of the RSA primes is known and the parameters r , x , and s are suitably small. By transforming this relation into an appropriate modular equation and applying Coppersmith's method, we derive conditions under which the RSA modulus can be factored in polynomial time, even when the corresponding private exponent is large. Our analysis encompasses several well-known attacks as special cases and significantly enlarges the class of vulnerable RSA exponents. Consequently, the proposed framework remains effective in settings where classical lattice-based approaches are no longer applicable.

Keywords: RSA; factoring; Coppersmith's technique; lattice basis reduction; weak exponents

MSC: 94A60

1. Introduction

A central problem in the theory of polynomials is solving polynomial equations, that is, finding the values of variables for which the polynomial evaluates to zero. These solutions, known as roots, are fundamental in various branches of mathematics, ranging from classical algebraic geometry to modern computational number theory. In the context of cryptanalysis, polynomials play a central role in attacking cryptographic systems, especially those based on number-theoretic assumptions. Many public-key cryptosystems, such as RSA and its variants, rely on computationally hard mathematical problems such as integer factorization. These problems can commonly be expressed as finding solutions to polynomial equations modulo a given integer, making polynomial-solving techniques particularly relevant to cryptanalysis. Prior to 1996, solving modular polynomial equations of the form $f(z) \equiv 0 \pmod{N}$ was generally feasible only when the prime factorization of the modulus N was known, typically by exploiting classical properties of modular arithmetic. In a seminal work, Coppersmith [1] introduced two lattice-based techniques, one for solving modular equations $f(z) \equiv 0 \pmod{N}$, even without knowledge of the factorization of N , and one for finding the small roots of the bivariate polynomial equation $g(x, y) = 0$. Since their inception, these methods have been generalized in various ways and used as fundamental



Received: 28 May 2026

Revised: 7 July 2026

Accepted: 9 July 2026

Published: 11 July 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and

conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

tools in cryptanalysis, especially in the analysis of RSA and its variants. In most cases, one of the parameters related to N is the solution to a specific modular equation. Then, finding the modular solution leads to factoring of N .

Over the past four decades, the RSA cryptosystem has been extensively studied from a cryptanalytic perspective [2–5] in order to evaluate its security strength. Most known attacks rely on continued fraction methods, lattice basis reduction techniques, or a combination of both approaches. Among the most notable results, Wiener [6] proved in 1990 that the private exponent d can be efficiently recovered by exploiting the convergents arising from the continued fraction expansion of $\frac{e}{N}$, whenever $d < \frac{1}{3}N^{\frac{1}{4}}$. In 1998, Boneh and Durfee [7] extended Coppersmith's framework to devise a powerful cryptanalytic attack on RSA with small private exponents. They reformulated the RSA key equation $ed - k\phi(N) = 1$ into the modular relation $z_1(-N + z_2) \equiv 1 \pmod{e}$ and employed Coppersmith's lattice-based method to recover the root $(z_1, z_2) = (k, p + q - 1)$. This allowed them to find the RSA primes in a reasonable amount of time. Notably, their approach significantly improved Wiener's attack [6], achieving an attack for $d < N^{0.292}$. This represents the threshold for attacks on small private exponents.

In certain attack models, the adversary is assumed to have access to a portion of the secret parameters, such as a sequence of consecutive bits from the private exponent d or the prime constituents p and q of the RSA modulus $N = pq$. This partial leakage can be leveraged to break the system. In practical scenarios, such information is often extracted through side-channel analysis techniques, as detailed in [8,9]. In 1998, Boneh et al. [10] established that, when the public exponent e is small, the disclosure of a sufficiently large portion of the bits of the private exponent d enables the complete reconstruction of the RSA secret key. Their result was subsequently improved by Blömer and May [11], who extended the applicability of the attack to the case where $e < N^{7/8}$. Later, in 2008, Sarkar et al. [12] showed that exposing a sufficiently large number of the most significant bits (MSBs) of one RSA prime factor is sufficient to break the security of the RSA cryptosystem. More recently, Li et al. [13] proposed an attack on RSA based on combining two main components: a binary search for the MSBs of the prime divisors of N , and the attack method developed by Herrmann and May [14]. They successfully factored large RSA moduli N using small private exponents. In particular, they demonstrated the practical factorization of a 2048-bit RSA modulus $N = pq$ in approximately one month for $d < N^{\delta}$, where $\delta = 0.287$.

In the situation wherein $N = pq$ with a small prime difference $|p - q| < N^{\beta}$ for $\frac{1}{4} < \beta \leq \frac{1}{2}$, de Weger [15] proved that one can solve the equation $ed - k\phi(N) = 1$ whenever $d < N^{1-\sqrt{2\beta-\frac{1}{2}}}$ by using $\tilde{p} = \lfloor \sqrt{N} \rfloor$ as an approximation of p .

Although the aforementioned attacks have significantly advanced the cryptanalysis of RSA, they all rely on the classical key equation $ed - k\phi(N) = 1$ or on specific assumptions regarding the RSA prime factors. Consequently, their applicability is restricted to particular scenarios, such as sufficiently small decryption exponents or strong partial information on the secret parameters. In particular, these approaches do not address more general modular relations involving RSA parameters, thereby limiting the range of weak exponents that can be analyzed. This observation motivates the study of the generalized equation $er - x\phi(N) = s$, which naturally extends the classical RSA key equation and provides a unified framework encompassing several existing attacks. Moreover, such a generalization enables the investigation of a broader class of weak public and private exponents, including situations where the corresponding private exponent may be large.

1.1. Our Contribution

In practical applications, most attacks on RSA have been based on the classical key equation $ed - k\varphi(N) = 1$ and are effective when $d < N^{1-\sqrt{2}/2} \approx N^{0.292}$. However, they fail to reach the maximal theoretical bound, namely, $d \approx N^{0.292}$.

In this paper, instead of studying the key equation $ed - k\varphi(N) = 1$, we study the generalized equation $er - x\varphi(N) = s$. To solve this equation, we assume that an approximation $\tilde{p}$ of p is known.

We start by transforming the generalized equation into a modular trivariate equation of the form

$$z_1 z_2 + b_0 z_1 + z_3 \equiv 0 \pmod{e},$$

and then apply a variant of Coppersmith's method to solve this equation, which leads to a practical RSA break. More specifically, we show that if there exist integers r , x , and s satisfying $er - x\varphi(N) = s$, with $|r| \leq N^\delta$, $|s| \leq N^\gamma$, $e = N^\alpha$, and $|p - \tilde{p}| < N^\varepsilon$, then by defining $\tilde{q} = \left\lfloor \frac{N}{\tilde{p}} \right\rfloor$ and $u = p + q - \tilde{p} - \tilde{q}$, the following parameter constraints

$$|s| < \inf(|er|, |xu|), \quad \varepsilon \leq \alpha \leq 4\varepsilon, \quad \text{and} \quad 1 - \frac{1}{2}\gamma - 2\varepsilon \leq \delta < 1 - \frac{1}{2}\gamma - \sqrt{\alpha\varepsilon},$$

are sufficient to factor N in polynomial time.

This implies the following consequences:

- When $\gamma = 0$, that is, $s = 1$, the equation becomes $ed - k\varphi(N) = 1$, and our derived bound simplifies to $\delta < 1 - \sqrt{\alpha\varepsilon}$. This aligns with the optimal bound concerning partial prime exposure attacks as originally demonstrated by Sarkar et al. [12]. Moreover, in this scenario, the same inequality can be interpreted as an optimal bound for attacks involving small private exponents, particularly when $|p - q| < N^{1/2}$. By setting $\varepsilon = \frac{1}{2}$, we recover the best-known threshold for small private exponent attacks, specifically $\delta < 1 - \sqrt{\frac{\alpha}{2}}$. Additionally, in the setting where $|p - q| < N^\beta$, $\alpha = 1$, and $\varepsilon = 2\beta - \frac{1}{2}$ with $\frac{1}{4} < \beta \leq \frac{1}{2}$, our bound simplifies to $\delta < 1 - \sqrt{2\beta - \frac{1}{2}}$, thereby recovering the bound established by de Weger [15].
- When $\gamma \neq 0$, the number of weak public exponents of the form $e = N^\alpha$ that are susceptible to our approach is on the order of $\mathcal{O}\left(N^{1+\frac{1}{2}\gamma-\sqrt{\alpha\varepsilon}-\nu}\right)$, where ν is a small positive number. This estimate notably exceeds the bounds reported in earlier work: Sarkar et al. provided an upper bound of approximately $\mathcal{O}\left(N^{1-\sqrt{\alpha\varepsilon}-\nu}\right)$, and Boneh and Durfee established a threshold on the order of $\mathcal{O}\left(N^{1-\sqrt{\alpha/2}-\nu}\right)$, while de Weger [15] proved a bound on the order of $\mathcal{O}\left(N^{1-\sqrt{2\beta-\frac{1}{2}}-\nu}\right)$ for exponents susceptible to their respective attacks.
- In addition, from the extended key equation $er - x\varphi(N) = s$, the decryption exponents in our attack take the form

$$d \equiv rs^{-1} \pmod{\varphi(N)},$$

whenever s is invertible modulo $\varphi(N)$. As a consequence of this form, our attack extends to a broader class of public exponents whose corresponding private exponents can be large, even reaching sizes on the order of N , which are much larger than $N^{1-\sqrt{2}/2}$.

To validate our algorithm for solving the equation $er - x\varphi(N) = s$, we present a detailed example and a table where various sizes are tested. We provide an implementation

of our algorithm in SageMath. The source code is available at https://github.com/Med96-hub/RSA_attacks (accessed on 25 June 2026).

1.2. Layout of the Paper

Section 2 reviews essential preliminaries relevant to our attack. Section 3 introduces a Coppersmith-based method for determining small roots of the congruence equation $z_1z_2 + b_0z_1 + z_3 \equiv 0 \pmod{e}$. Section 4 applies our method to attacking RSA. Section 5 compares our attack with previous methods. Section 6 provides comprehensive numerical illustrations to substantiate the efficacy of our attack. Finally, we summarize our findings in Section 7.

2. Background

In this section, we recall the RSA scheme along with useful cryptanalytic tools, such as Coppersmith's method and lattice reduction techniques.

2.1. Notations

For the convenience of the reader, we summarize in Tables 1–4 the principal symbols and parameters used throughout the paper, together with their meanings and their correspondence in the main results.

Table 1. General notation used throughout the paper.

Symbol	Meaning
$\mathbb{Z}$	Ring of integers
$\mathbb{R}$	Field of real numbers
$\mathbb{Z}[x_1, \dots, x_n]$	Ring of polynomials in n variables over $\mathbb{Z}$
$\mathcal{L}$	Euclidean lattice
$\det(\mathcal{L})$	Determinant of the lattice $\mathcal{L}$
$\ \mathbf{v}\ $	Euclidean norm of the vector $\mathbf{v}$
$\lfloor x \rfloor$	Floor function of x
$\varphi(N)$	Euler's totient function of N
$\gcd(a, b)$	Greatest common divisor of a and b
$f(x_1, \dots, x_n) \equiv 0 \pmod{N}$	Polynomial congruence modulo N

Table 2. Notation used in Theorem 3.

Symbol	Meaning
N	RSA modulus, $N = pq$
$e = N^\alpha$	Public exponent
α	Exponent associated with e
z_1, z_2, z_3	Unknown roots of the modular equation
z_4	Auxiliary variable defined by $z_4 = z_1z_2 + z_3$
λ	Exponent satisfying $ z_1 \leq N^\lambda$
μ	Exponent satisfying $ z_2 \leq N^\mu$
γ	Exponent satisfying $ z_3 \leq N^\gamma$
Z_1, Z_2, Z_3, Z_4	Bounds on z_1, z_2, z_3, z_4
ν	Lattice parameter controlling the shifts
κ	Optimization parameter in the lattice construction
ρ	Dimension of the lattice

Table 3. Notation used in Theorem 4.

Symbol	Meaning
$N = pq$	RSA modulus
$e = N^\alpha$	Public exponent
α	Exponent associated with e
r	Unknown integer satisfying $er - x\varphi(N) = s$
δ	Exponent satisfying $ r \leq N^\delta$
x	Unknown integer in the key equation
s	Error term in the key equation
γ	Exponent satisfying $ s \leq N^\gamma$
$\tilde{p}$	Known approximation of the prime p
$\tilde{q} = \lfloor N/\tilde{p} \rfloor$	Approximation of q
ε	Exponent satisfying $ p - \tilde{p} < N^\varepsilon$
u	Quantity $u = p + q - \tilde{p} - \tilde{q}$
z_1	Variable corresponding to $-x$
z_2	Variable corresponding to u
z_3	Variable corresponding to s

Table 4. Additional notation used in Corollary 1.

Symbol	Meaning
β	Exponent satisfying $ p - q < N^\beta$
$\lfloor \sqrt{N} \rfloor$	Approximation of both p and q
u	Quantity $u = p + q - 2\lfloor \sqrt{N} \rfloor$
α	Exponent associated with the public exponent e
δ	Exponent satisfying $ r \leq N^\delta$
γ	Exponent satisfying $ s \leq N^\gamma$

2.2. Key Lemmas

The next result yields bounds for the RSA prime factors as well as the sum and the difference of the primes (see [16] for further details).

Lemma 1. For every pair of primes (p, q) satisfying $q < p < 2q$ and $N = pq$, the prime factors are subject to the following inequalities:

$$\begin{aligned}\frac{\sqrt{2}}{2}N^{0.5} &< q < N^{0.5} < p < \sqrt{2}N^{0.5}, \\ 2N^{0.5} &< p + q < \frac{3\sqrt{2}}{2}N^{0.5}, \\ 0 &< p - q < \frac{\sqrt{2}}{2}N^{0.5}.\end{aligned}$$

The following Lemma establishes that, for moduli of the form $N = pq$, if a sufficiently accurate approximation of one of its prime factors is available, it is feasible to estimate the other prime and their sum (see [17]).

Lemma 2. For a modulus $N = pq$ with $q < p < 2q$, assume that an approximation $\tilde{p}$ of p is known, with $|p - \tilde{p}| < N^\varepsilon$. Then, an estimate of q can be obtained using $\tilde{q} = \lfloor \frac{N}{\tilde{p}} \rfloor$, for which the inequalities $|q - \tilde{q}| < N^\varepsilon$ and $|(p + q) - (\tilde{p} + \tilde{q})| < 2N^\varepsilon$ hold.

The subsequent Lemma provides lower and upper bounds for the Euler totient function $\varphi(N)$ in terms of N , assuming that N is sufficiently large.

Lemma 3. For every RSA modulus $N = pq$ with $q < p < 2q$, one has

$$\frac{N}{2} < \varphi(N) < N.$$

Proof. For the upper bound, we use the fact that

$$\varphi(N) = (p-1)(q-1) < pq = N.$$

For the lower bound, according to Lemma 1, we have

$$\varphi(N) = (p-1)(q-1) = N + 1 - (p+q) > N + 1 - \frac{3\sqrt{2}}{2}\sqrt{N}.$$

A sufficient condition for $\varphi(N) > \frac{N}{2}$ is therefore

$$N + 1 - \frac{3\sqrt{2}}{2}\sqrt{N} > \frac{N}{2}.$$

This inequality holds if

$$N - 3\sqrt{2}\sqrt{N} + 2 > 0,$$

which is true for $N > \frac{3\sqrt{2} + \sqrt{10}}{2} \approx 3.7$. This proves the lemma. $\square$

2.3. The RSA Scheme

In 1978, Rivest, Shamir, and Adleman [18] introduced a cryptographic algorithm that laid the foundation for public-key encryption grounded in number-theoretic principles. This protocol, known as RSA, continues to play a crucial role in practical applications such as digital signatures, secure electronic correspondence, and safeguarding of online financial operations. The robustness of RSA is intrinsically linked to the intractability of factoring large moduli into their prime factors. Within this scheme, the modulus N is formed as the product of two large prime numbers, p and q , which are generally selected to be of equal bit size. The Euler totient of N is computed as $\varphi(N) = (p-1)(q-1)$. A public exponent e is chosen such that it satisfies $\gcd(e, \varphi(N)) = 1$, ensuring that a corresponding private exponent d exists, fulfilling the modular inverse relation $ed \equiv 1 \pmod{\varphi(N)}$, or, equivalently, $ed - k\varphi(N) = 1$, for some integer k . This relation is often referred to as the RSA key equation. The public key comprises the pair (N, e) , while the private key is given by (N, d) . Encryption of a message m involves computing the ciphertext c via the congruence $c \equiv m^e \pmod{N}$. Decryption recovers the message m via the congruence $m \equiv c^d \pmod{N}$.

2.4. Lattice Basis Reduction

The central mathematical objects in the geometry of numbers are lattices. They are known as discrete subgroups of $\mathbb{R}^m$. More specifically, a lattice can be defined based on linear algebra as follows [19].

Let $\rho \leq m$ be a positive integer. For a set of ρ linearly independent vectors $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_\rho$ in the Euclidean space $\mathbb{R}^m$, the lattice $\mathcal{L} \subseteq \mathbb{R}^m$ generated by these vectors is defined as the collection of all integer linear combinations of the form

$$\mathcal{L} = \left\{ \sum_{i=1}^{\rho} \alpha_i \mathbf{b}_i \in \mathbb{R}^m : \alpha_1, \dots, \alpha_\rho \in \mathbb{Z} \right\}.$$

The lattice dimension is the positive integer m , and its rank is ρ . The lattice $\mathcal{L}$ can be rigorously characterized through its matrix representation, as follows. Let $\mathcal{M} \in \mathbb{R}^{\rho \times m}$ be

the matrix whose rows are formed by the basis vectors $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_\rho$. A vector $\mathbf{x}$ belongs to the lattice $\mathcal{L}$ precisely when there exists an integral coordinate vector $\mathbf{n} \in \mathbb{Z}^\rho$ such that $\mathbf{x} = \mathbf{n}\mathcal{M}$. The determinant of the lattice, denoted as $\det(\mathcal{L})$, is given by the square root of the determinant of the Gram matrix $\mathcal{M}\mathcal{M}^\top$, i.e., $\det(\mathcal{L}) = \sqrt{\det(\mathcal{M}\mathcal{M}^\top)}$, where $\mathcal{M}^\top$ indicates the transpose of $\mathcal{M}$. When the lattice is full-rank—that is, $\rho = m$ —the determinant then reduces to the form $\det(\mathcal{L}) = |\det(\mathcal{M})|$.

Although any lattice $\mathcal{L}$ of rank $\rho \geq 2$ possesses infinitely many bases, discovering one composed of short vectors is notably difficult, especially when the dimension is sufficiently large. In 1982, Lenstra, Lenstra, and Lovász [19] developed the LLL algorithm, a polynomial time lattice reduction algorithm designed to produce a basis with relatively short vectors. The statement below [5] is frequently used to evaluate the output of the LLL algorithm.

Theorem 1. Suppose $\mathcal{L}$ is a lattice defined by a basis $\{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_\rho\}$. The application of the LLL algorithm to the former basis outputs a lattice basis $\{\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_\rho\}$ such that for every index i with $1 \leq i \leq \rho$, the following inequality holds:

$$\|\mathbf{c}_1\| \leq \dots \leq \|\mathbf{c}_i\| \leq 2^{\frac{\rho(\rho-1)}{4(\rho+1-i)}} \det(\mathcal{L})^{\frac{1}{\rho+1-i}}.$$

2.5. Coppersmith's Method and Its Generalization

Back in 1996, Coppersmith [1] devised a method to efficiently identify small roots of univariate polynomial equations modulo an integer M , specifically those satisfying $f(z) \equiv 0 \pmod{M}$, where the prime factorization of M is unknown. This foundational technique has since been extended to handle multivariate polynomial equations, typically of the form

$$F(z_1, z_2, \dots, z_n) = \sum_{j_1, j_2, \dots, j_n} c_{j_1, j_2, \dots, j_n} z_1^{j_1} z_2^{j_2} \dots z_n^{j_n},$$

where each coefficient $c_{j_1, j_2, \dots, j_n}$ is an integer. The size of such a polynomial is commonly measured by its Euclidean norm, defined as follows:

$$\|F\| = \sqrt{\sum c_{j_1, j_2, \dots, j_n}^2}.$$

Afterward, Howgrave-Graham [20] revisited Coppersmith's ideas and presented the following result for extracting modular roots.

Theorem 2 (Howgrave-Graham). Let $F(z_1, \dots, z_n) \in \mathbb{Z}[z_1, \dots, z_n]$ be a polynomial in n variables with no more than ρ nonzero terms. Let e and v be positive integers. Assume that

1. $F(s_1, \dots, s_n) \equiv 0 \pmod{e^v}$;
2. $\|F(z_1 Z_1, \dots, z_n Z_n)\| < \frac{e^v}{\sqrt{\rho}}$;
3. Each component satisfies the bound $|s_i| < Z_i$ for $1 \leq i \leq n$.

Under these conditions, it follows that $F(s_1, \dots, s_n) = 0$.

Coppersmith-based approaches generally become heuristic in nature when applied to equations involving more than two variables. In this paper, we proceed under the following assumption [7,21,22].

Assumption 1. The polynomials $A_1, A_2, \dots, A_\rho$, obtained through LLL reduction, are assumed to be algebraically independent; that is, there is no multivariate polynomial $P \neq 0$ with integer coefficients such that $P(A_1, A_2, \dots, A_\rho) = 0$.

Our method, as well as nearly all other applications of multivariate Coppersmith methods, depends entirely on a heuristic assumption such as Assumption 1. Here, it is assumed that the LLL algorithm outputs a few algebraically independent polynomials sharing a root that can be found using an algebraic method such as Gröbner bases or resultant computations. We give more details about Assumption 1 at the end of Section 6.

Let N be an integer to be factored and $F(z_1, \dots, z_n)$ a multivariate polynomial satisfying $F(s_1, \dots, s_n) \equiv 0 \pmod{M}$ where one of the components of $(s_1, \dots, s_n)$ is related to N and permits its factorization. Moreover, let $Z_i, i = 1, \dots, n$, be the bounds satisfying $|s_i| < Z_i$. The goal of Coppersmith's method is to find the solution $(s_1, \dots, s_n)$ efficiently and to use one or more components to factor N . The strategy starts by deriving ρ polynomials $F_k(z_1, \dots, z_n) \in \mathbb{Z}[z_1, \dots, z_n]$ satisfying $F_k(s_1, \dots, s_n) \equiv 0 \pmod{M^\nu}$ for each k with $k = 1, \dots, \rho$. In most cases, the polynomial $F_k(z_1, \dots, z_n)$ is created using

$$F_k(z_1, \dots, z_n) = z_1^{e_1} z_2^{e_2} \dots z_n^{e_n} F^k M^{\nu-f_k},$$

where $e_1, e_2, \dots, e_n, f_k$ are non-negative integers. The coefficients of the monomials of the polynomials $F_k(Z_1 z_1, \dots, Z_n z_n)$ are used as the rows of a matrix $\mathcal{M}$, which is used as the basis of a lattice $\mathcal{L}$. By choosing a suitable ordering for the rows and the columns, the matrix can be lower or upper-triangular. The LLL algorithm is then applied to reduce the basis $\mathcal{M}$ into a reduced basis $\mathcal{N}$, from which ρ polynomials $G_k(z_1, \dots, z_n)$ are derived, satisfying

$$G_k(s_1, \dots, s_n) \equiv 0 \pmod{M^\nu}.$$

Under the condition of Theorem 2, one has $G_k(s_1, \dots, s_n) = 0$ over the integers. Finally, under Assumption 1, the solution $(s_1, \dots, s_n)$ is extracted by using the Gröbner basis technique or resultant computation. Using one of the components of $(s_1, \dots, s_n)$, one prime factor of N can be found.

3. Resolution of the Equation $z_1 z_2 + b_0 z_1 + z_3 \equiv 0 \pmod{e}$

In this section, we develop an efficient method with which to find modular roots of the equation

$$z_1 z_2 + b_0 z_1 + z_3 \equiv 0 \pmod{e},$$

under the assumption that the unknowns z_1, z_2 , and z_3 are sufficiently small. To facilitate the analysis, we first introduce a fundamental Lemma that will be instrumental throughout this section.

Lemma 4. For any integer $v \geq 1$, any integer b_0 , any real parameter $\kappa \in [0, 1]$, and any integer c with $0 \leq c \leq v$, consider the polynomials

$$Q(c, a, b, z_1, z_2, z_3, z_4) = z_1^{a-c} z_2^{b-c} z_3^{v-a} (b_0 z_1 + z_4)^c,$$

where the indices (a, b) lie in one of the disjoint sets

$$E(c) = \left\{ (a, b) \in \mathbb{Z}^2 : a = c, b = c, \dots, c + 1 + \lfloor \kappa c \rfloor \right\},$$

$$F(c) = \left\{ (a, b) \in \mathbb{Z}^2 : a = c + 1, \dots, v, b = c \right\}.$$

Under the constraint $z_1 z_2 = z_4 - z_3$ and with respect to the lexicographic ordering of (c, a, b) , the matrix formed by the coefficient vectors of $Q(c, a, b, z_1, z_2, z_3, z_4)$ is lower-triangular.

Proof. The detailed proof of Lemma 4 is presented in Appendix A. $\square$

The next Theorem concerns the resolution of the modular polynomial equation $z_1 z_2 + b_0 z_1 + z_3 \equiv 0 \pmod{e}$, where b_0 is an integer and the unknowns z_1 , z_2 , and z_3 are appropriately small.

Theorem 3. Let N be an RSA modulus and e a positive integer such that $e = N^\alpha$. Let b_0 be an integer. Suppose there exist three integers z_1 , z_2 , and z_3 satisfying $z_1 z_2 + b_0 z_1 + z_3 \equiv 0 \pmod{e}$, under the constraints $|z_1| \leq N^\lambda$, $|z_2| \leq N^\mu$, $|z_3| \leq N^\gamma$, $|z_3| < |z_1 z_2|$, $\mu \leq \alpha \leq 4\mu$, and

$$\alpha - \frac{1}{2}\gamma - 2\mu \leq \lambda < \alpha - \frac{1}{2}\gamma - \sqrt{\alpha\mu}.$$

Then, under Assumption 1, the computation of z_1 , z_2 , and z_3 can be efficiently achieved in polynomial time.

Proof. Our methodology is rooted in an adaptation of Coppersmith's framework. We begin by introducing the polynomial

$$T(z_1, z_2, z_3) = z_1 z_2 + b_0 z_1 + z_3,$$

which satisfies the congruence relation

$$T(z_1, z_2, z_3) \equiv 0 \pmod{e}.$$

By defining a new variable $z_4 = z_1 z_2 + z_3$, we can reformulate this expression as follows:

$$\theta(z_1, z_4) = z_4 + b_0 z_1 \equiv 0 \pmod{e}.$$

To extract the root (z_1, z_2, z_3, z_4) , we proceed along the lines of Coppersmith's method. Let ν be a positive integer and $\kappa \in [0, 1]$ be a parameter to be optimized in the analysis. For an integer c with $0 \leq c \leq \nu$, and for two integers a, b such that (a, b) lies in one of the disjoint sets

$$\begin{aligned} E(c) &= \{(a, b) \in \mathbb{Z}^2 : a = c, b = c, \dots, c + 1 + \lfloor \kappa c \rfloor\}, \\ F(c) &= \{(a, b) \in \mathbb{Z}^2 : a = c + 1, \dots, \nu, b = c\}, \end{aligned}$$

we examine the following family of polynomials:

$$S(c, a, b, z_1, z_2, z_3, z_4) = z_1^{a-c} z_2^{b-c} z_3^{\nu-a} \theta(z_1, z_4)^c e^{\nu-c},$$

where we substitute the expression $z_1 z_2$ with $z_4 - z_3$ in line with our new variable definition. Given that $T(z_1, z_2, z_3) \equiv \theta(z_1, z_4) \equiv 0 \pmod{e}$, it follows that each polynomial $S(c, a, b, z_1, z_2, z_3, z_4)$ satisfies

$$S(c, a, b, z_1, z_2, z_3, z_4) \equiv 0 \pmod{e^\nu},$$

for all valid integer triples (c, a, b) .

Following the framework of Coppersmith's method, the construction of the lattice begins with defining appropriate bounds for the variables z_1 , z_2 , z_3 , and z_4 . We set $Z_1 = N^\lambda$, $Z_2 = N^\mu$, and $Z_3 = N^\gamma$ as bounds for z_1 , z_2 , and z_3 , respectively. To determine a bound for $z_4 = z_1 z_2 + z_3$, we assume $|z_3| < |z_1 z_2|$, which yields $|z_4| < 2|z_1 z_2|$. Hence, we choose $Z_4 = 2N^{\lambda+\mu}$ as a valid upper bound for z_4 . We then construct the lattice $\mathcal{L}$ spanned by the matrix $\mathcal{M}$ whose rows are formed by the coefficients of the monomials in the polynomials $S(c, a, b, Z_1 z_1, Z_2 z_2, Z_3 z_3, Z_4 z_4)$. The rows of $\mathcal{M}$ correspond to the polynomials

$S(c, a, b, Z_1 z_1, Z_2 z_2, Z_3 z_3, Z_4 z_4)$ and are ordered using the lexicographic ordering of (c, a, b) . Similarly, within each expanded polynomial $S(c, a, b, Z_1 z_1, Z_2 z_2, Z_3 z_3, Z_4 z_4)$, the monomials of the form $z_1^{a-c} z_2^{b-c} z_3^{\nu-a} z_4^c$ correspond to the columns of $\mathcal{M}$ and are arranged in accordance with the lexicographic ordering of (c, a, b) . A representative example is provided in Table 5, where positions marked by $\star$ correspond to nonzero integer coefficients.

Table 5. The corresponding matrix when $\nu = 2$ and $\kappa = 1$.

$S_{(c,a,b)}$	z_3^2	$z_2 z_3^2$	$z_1 z_3$	z_1^2	$z_3 z_4$	$z_2 z_3 z_4$	$z_2^2 z_3 z_4$	$z_1 z_4$	z_4^2	$z_2 z_4^2$	$z_2^2 z_4^2$	$z_2^3 z_4^2$
$S_{(0,0,0)}$	$e^2 Z_3^2$	0	0	0	0	0	0	0	0	0	0	0
$S_{(0,0,1)}$	0	$e^2 Z_2 Z_3^2$	0	0	0	0	0	0	0	0	0	0
$S_{(0,1,0)}$	0	0	$e^2 Z_1 Z_3$	0	0	0	0	0	0	0	0	0
$S_{(0,2,0)}$	0	0	0	$e^2 Z_1^2$	0	0	0	0	0	0	0	0
$S_{(1,1,1)}$	0	0	$\star$	0	$e Z_3 Z_4$	0	0	0	0	0	0	0
$S_{(1,1,2)}$	$\star$	0	0	0	$\star$	$e Z_2 Z_3 Z_4$	0	0	0	0	0	0
$S_{(1,1,3)}$	0	$\star$	0	0	0	$\star$	$e Z_2^2 Z_3 Z_4$	0	0	0	0	0
$S_{(1,2,1)}$	0	0	0	$\star$	0	0	0	$e Z_1 Z_4$	0	0	0	0
$S_{(2,2,2)}$	0	0	0	$\star$	0	0	0	$\star$	Z_4^2	0	0	0
$S_{(2,2,3)}$	0	0	$\star$	0	$\star$	0	0	$\star$	$\star$	$Z_2 Z_4^2$	0	0
$S_{(2,2,4)}$	$\star$	0	0	0	$\star$	$\star$	0	0	$\star$	$\star$	$Z_2^2 Z_4^2$	0
$S_{(2,2,5)}$	0	$\star$	0	0	0	$\star$	$\star$	0	0	$\star$	$\star$	$Z_2^3 Z_4^2$

From Lemma 4, the matrix is identified as lower-triangular, with diagonal elements given by expressions of the form $Z_1^{a-c} Z_2^{b-c} Z_3^{\nu-a} Z_4^c e^{\nu-c}$, where c runs from 0 to ν and the pair (a, b) lies in $E(c) \cup F(c)$. Therefore, the determinant equals the product of these diagonal entries, implying that the determinant of the associated lattice has the structure

$$\det(\mathcal{L}) = Z_1^{n_{Z_1}} Z_2^{n_{Z_2}} Z_3^{n_{Z_3}} Z_4^{n_{Z_4}} e^{n_e}, \quad (1)$$

with $n_{Z_1} = C(a - c)$, $n_{Z_2} = C(b - c)$, $n_{Z_3} = C(\nu - a)$, $n_{Z_4} = C(c)$, and $n_e = C(\nu - c)$, where the function C is defined by summing up over the sets $E(c)$ and $F(c)$ —specifically,

$$C(x_{c,a,b}) = \sum_{c=0}^{\nu} \sum_{a=c}^c \sum_{b=c}^{c+1+\lfloor \kappa c \rfloor} x_{c,a,b} + \sum_{c=0}^{\nu} \sum_{a=c+1}^{\nu} \sum_{b=c}^c x_{c,a,b}.$$

Additionally, the dimension of the lattice is denoted by ρ and is given by $\rho = C(1)$. To simplify the computation, we use the approximation $\lfloor \kappa c \rfloor \approx \kappa c$ and get

$$\begin{aligned} n_{Z_1} &= \frac{1}{6} \nu (\nu + 2) (\nu + 1), \\ n_{Z_2} &= \frac{1}{12} (\nu + 1) (2 \kappa^2 \nu^2 + \kappa^2 \nu + 9 \kappa \nu + 12), \\ n_{Z_3} &= \frac{1}{6} \nu (\nu + 1) (\kappa \nu - \kappa + \nu + 5), \\ n_{Z_4} &= \frac{1}{6} \nu (\nu + 1) (2 \kappa \nu + \kappa + \nu + 5), \\ n_e &= \frac{1}{6} \nu (\nu + 1) (\kappa \nu - \kappa + 2 \nu + 7), \\ \rho &= \frac{1}{2} (\nu + 1) (\kappa \nu + \nu + 4). \end{aligned} \quad (2)$$

The application of the LLL reduction to the lattice $\mathcal{L}$ yields ρ polynomials of the form $A_\ell(Z_1 z_1, Z_2 z_2, Z_3 z_3, Z_4 z_4)$ for $\ell = 1, \dots, \rho$ that satisfy the congruence

$$A_\ell(z_1, z_2, z_3, z_4) \equiv 0 \pmod{e^\nu}.$$

Because the determinant is preserved during the reduction, solving the equations $A_\ell(z_1, z_2, z_3, z_4) = 0$ with $\ell \leq \rho$ over the integers involves combining Theorems 1 and 2 for $i = 4$. This can be achieved when the condition

$$2^{\frac{\rho(\rho-1)}{4(\rho-3)}} \det(\mathcal{L})^{\frac{1}{\rho-3}} < \frac{e^\nu}{\sqrt{\rho}},$$

is imposed. Invoking (1), we can simplify the above inequality to

$$Z_1^{n_{Z_1}} Z_2^{n_{Z_2}} Z_3^{n_{Z_3}} Z_4^{n_{Z_4}} e^{n_e} < \frac{1}{\rho^{\frac{\rho-3}{2}} 2^{\frac{\rho(\rho-1)}{4}}} e^{\nu(\rho-3)} < e^{\nu\rho}.$$

To solve the former inequality, we omit the smaller-order terms in the exponents and the dimension and use the dominant parts in (2) such that

$$\begin{aligned} n_{Z_1} &\approx \frac{1}{6}\nu^3, \\ n_{Z_2} &\approx \frac{1}{6}\kappa^2\nu^3, \\ n_{Z_3} &\approx \frac{1}{6}(\kappa+1)\nu^3, \\ n_{Z_4} &\approx \frac{1}{6}(2\kappa+1)\nu^3, \\ n_e &\approx \frac{1}{6}(\kappa+2)\nu^3, \\ \rho &\approx \frac{1}{2}(\kappa+1)\nu^2. \end{aligned} \tag{3}$$

Then, after using the bounds $Z_1 = N^\lambda$, $Z_2 = N^\mu$, $Z_3 = N^\gamma$, and $Z_4 = 2N^{\lambda+\mu}$ $e = N^\alpha$ and the approximations from (3) and omitting some negligible terms, we get

$$N^{\frac{\lambda\nu^3}{6}} N^{\frac{\mu\kappa^2\nu^3}{6}} N^{\frac{\gamma(\kappa+1)\nu^3}{6}} N^{\frac{(\lambda+\mu)(2\kappa+1)\nu^3}{6}} N^{\frac{\alpha(\kappa+2)\nu^3}{6}} < N^{\frac{\alpha(\kappa+1)\nu^3}{2}}.$$

After logarithms are taken and the terms ν^3 and $\log(N)$ are eliminated, the former relation simplifies to

$$\lambda + \mu\kappa^2 + \gamma(\kappa+1) + (\lambda+\mu)(2\kappa+1) + \alpha(\kappa+2) - 3\alpha(\kappa+1) < 0,$$

which can be reformulated as

$$\mu\kappa^2 - (2\alpha - \gamma - 2\lambda - 2\mu)\kappa - \alpha + \gamma + 2\lambda + \mu < 0. \tag{4}$$

Viewing the former relation as a function of κ , we can see that it attains its minimum at

$$\kappa_0 = \frac{2\alpha - \gamma - 2\lambda - 2\mu}{2\mu}.$$

For the condition $0 \leq \kappa_0 \leq 1$ to hold, the parameters are required to satisfy

$$\alpha - \frac{1}{2}\gamma - 2\mu \leq \lambda \leq \alpha - \frac{1}{2}\gamma - \mu. \tag{5}$$

The inequality

$$0 \leq \lambda \leq \alpha - \frac{1}{2}\gamma - \mu,$$

implies that $\alpha \geq \mu$. Then, using the previous conditions and substituting κ_0 into (4) yields

$$-4\lambda^2 + (8\alpha - 4\gamma)\lambda + 4\alpha\gamma - 4\alpha^2 - \gamma^2 + 4\alpha\mu < 0,$$

which can equivalently be expressed as

$$-4\left(\lambda - \alpha + \frac{1}{2}\gamma + \sqrt{\alpha\mu}\right)\left(\lambda - \alpha + \frac{1}{2}\gamma - \sqrt{\alpha\mu}\right) < 0.$$

The preceding inequality holds true if

$$\lambda - \alpha + \frac{1}{2}\gamma + \sqrt{\alpha\mu} < 0,$$

and

$$\lambda - \alpha + \frac{1}{2}\gamma - \sqrt{\alpha\mu} < 0.$$

As a result,

$$\begin{aligned}\lambda &< \min\left(\alpha - \frac{1}{2}\gamma - \sqrt{\alpha\mu}, \alpha - \frac{1}{2}\gamma + \sqrt{\alpha\mu}\right), \\ &= \alpha - \frac{1}{2}\gamma - \sqrt{\alpha\mu}.\end{aligned}$$

By merging this result with (5), it follows that, for $\alpha \geq \mu$,

$$\lambda < \min\left(\alpha - \frac{1}{2}\gamma - \mu, \alpha - \frac{1}{2}\gamma - \sqrt{\alpha\mu}\right) = \alpha - \frac{1}{2}\gamma - \sqrt{\alpha\mu}.$$

Alongside the conditions in (5), the inequality

$$\alpha - \frac{1}{2}\gamma - 2\mu \leq \alpha - \frac{1}{2}\gamma - \sqrt{\alpha\mu},$$

must also be satisfied. This holds under the restriction $\alpha \leq 4\mu$.

Employing the conditions outlined earlier, as well as Assumption 1, we can find that given four reduced and algebraically independent polynomials $A_k(z_1, z_2, z_3, z_4)$ for $1 \leq k \leq 4$, the solution (z_1, z_2, z_3, z_4) can be obtained by solving the system of equations

$$A_k(z_1, z_2, z_3, z_4) = 0, \quad 1 \leq k \leq 4,$$

over the integers, utilizing Gröbner basis computations or resultant-based methods. This concludes the proof. $\square$

Remark 1. It is worth noting that while the final asymptotic upper bound obtained in Theorem 3 coincides with the one established in [23], the underlying lattice configurations are fundamentally distinct. In [23], the optimization parameter is a real positive value ($t \in \mathbb{R}^+$), whereas our formulation optimizes the parameter κ strictly within the interval $[0, 1]$. Furthermore, due to the different algebraic structures of the modular equations, the sets of indices for the shift polynomials are completely different, leading to distinct lattice geometries.

4. Application of the Method to the Cryptanalysis of RSA

In this section, we employ the approach described in Section 3 to compute small solutions to the equation $er - x\varphi(N) = s$, under the assumption that the parameters r , x , and s are sufficiently small and that an integer close to one of the RSA primes is known. By leveraging the resulting roots, we can efficiently find the primes that make up $N = pq$.

Theorem 4. Let p and q be two large prime numbers of equal bit-length, and $N = pq$. Let the public exponent be $e = N^\alpha$. Assume there exist integers r , x , and s such that $er - x\varphi(N) = s$ with bounds $|r| \leq N^\delta$ and $|s| \leq N^\gamma$, and suppose further that an integer $\tilde{p}$ close to p is known, with $|p - \tilde{p}| < N^\varepsilon$. Let $\tilde{q} = \lfloor N/\tilde{p} \rfloor$, and define $u = p + q - \tilde{p} - \tilde{q}$. If the parameters satisfy $|s| < \inf(|er|, |xu|)$, $\varepsilon \leq \alpha \leq 4\varepsilon$, and

$$1 - \frac{1}{2}\gamma - 2\varepsilon \leq \delta < 1 - \frac{1}{2}\gamma - \sqrt{\alpha\varepsilon},$$

then, under Assumption 1, the factorization of N can be efficiently achieved in polynomial time.

Proof. For $N = pq$, the original equation $er - x(p-1)(q-1) = s$ can be reformulated as

$$er - (N + 1 - \tilde{p} - \tilde{q})x + x(p + q - \tilde{p} - \tilde{q}) = s,$$

which implies that

$$-x(p + q - \tilde{p} - \tilde{q}) + (N + 1 - \tilde{p} - \tilde{q})x + s \equiv 0 \pmod{e}.$$

Hence, setting $b_0 = \tilde{p} + \tilde{q} - N - 1$ and $u = p + q - \tilde{p} - \tilde{q}$, we can find that the equation

$$z_1 z_2 + b_0 z_1 + z_3 \equiv 0 \pmod{e}$$

has the particular solution $(z_1, z_2, z_3) = (-x, u, s)$. Our goal is to find a large bound for x . This implies that $|s|$ should be minimized.

Given the conditions $e = N^\alpha$, $|r| \leq N^\delta$, and $|s| \leq N^\gamma$, and assuming that $|s| < |er|$, then, together with the inequality $(p-1)(q-1) > \frac{N}{2}$ as stated in Lemma 3, it follows that

$$|z_1| = \left| \frac{er - s}{(p-1)(q-1)} \right| < \frac{4e|r|}{N} \leq 4N^{\alpha+\delta-1}.$$

From Lemma 2, it holds that $|z_2| < 2N^\varepsilon$. To utilize Theorem 3, it is also necessary to establish a bound for $z_4 = z_1 z_2 + z_3$. If we suppose $|s| < |xu|$, that is, $|z_3| < |z_1 z_2|$, then

$$|z_4| = |z_1 z_2 + z_3| < 2|z_1 z_2| < 16N^{\alpha+\delta+\varepsilon-1}.$$

This allows us to define the bounds of the unknowns in terms of N as

$$|z_1| < Z_1 = 4N^{\alpha+\delta-1}, \quad |z_2| < Z_2 = 2N^\varepsilon, \quad |z_3| \leq Z_3 = N^\gamma,$$

and

$$|z_4| < Z_4 = 2Z_1 Z_2 = 16N^{\alpha+\delta+\varepsilon-1}.$$

Referring to Theorem 3, where the bounds satisfy $|z_1| \leq N^\lambda$ and $|z_2| \leq N^\mu$, we identify $\lambda = \alpha + \delta - 1$ and $\mu = \varepsilon$. The condition $\mu \leq \alpha \leq 4\mu$ translates to

$$\varepsilon \leq \alpha \leq 4\varepsilon,$$

and the condition

$$\alpha - \frac{1}{2}\gamma - 2\mu \leq \lambda < \alpha - \frac{1}{2}\gamma - \sqrt{\alpha\mu},$$

becomes

$$1 - \frac{1}{2}\gamma - 2\varepsilon \leq \delta < 1 - \frac{1}{2}\gamma - \sqrt{\alpha\varepsilon}.$$

These constraints ensure the feasibility of extracting the root (z_1, z_2, z_3, z_4) , where $z_2 = p + q - \tilde{p} - \tilde{q}$. By combining $z_2 + \tilde{p} + \tilde{q} = p + q$ with $N = pq$, we can recover the pair (p, q) , thus enabling the efficient factorization of N under the stated conditions. This completes the proof. $\square$

Remark 2. In Theorem 4, the condition $|s| < \inf(|er|, |xu|)$ is essential for ensuring that $|z_3| < |z_1 z_2|$, which in turn justifies the upper bound for Z_4 . The condition $|z_3| < |z_1 z_2|$ is also needed in two applications. First, in RSA, the key equation is $ed - k\phi(N) = 1$, together with its variants $er - x\phi(N) = s$, where $|s|$ is small. Second, our general equation $z_1 z_2 + b_0 z_1 + z_3 \equiv 0 \pmod{e}$, with $b_0 = \tilde{p} + \tilde{q} - N - 1$ and $(z_1, z_2, z_3) = (-x, p + q - \tilde{p} - \tilde{q}, s)$, is derived from the variant $er - x\phi(N) = s$. Since we aim for x to be as large as possible, we require $|z_3| = |s|$ to be as small as possible. On the other hand, the condition $|s| < |er|$ is effective when s is minimized, allowing us to construct a suitable bound for x . As a consequence, our method works only when the condition $|s| < \inf(|er|, |xu|)$ is satisfied.

Theorem 4 directly yields the following corollary, which addresses the case where the modulus $N = pq$ is the product of two primes p and q of equal bit-size and a sufficiently small prime difference $|p - q| < N^\beta$. We note that if $\beta \leq \frac{1}{4}$, Fermat's method [15] can find p and q directly from N . The same result is established in [24] using Coppersmith's method. On the other hand, by Lemma 1, we know that $|p - q| < N^{0.5}$. Consequently, in the following, we restrict our attention to parameters β such that $\frac{1}{4} < \beta \leq \frac{1}{2}$. Moreover, when $|p - q|$ is sufficiently small, Lemma 1 implies that an approximation of p is $\tilde{p} = \lfloor \sqrt{N} \rfloor$, and that an approximation of q is $\tilde{q} = \lfloor \sqrt{N} \rfloor$. Hence, $2\lfloor \sqrt{N} \rfloor$ is an approximation of $p + q$. The following result gives a precise approximation of this fact (see [15]).

Lemma 5. Let p and q be two large prime numbers of equal bit-length, and $N = pq$ with $|p - q| < N^\beta$ for $\frac{1}{4} < \beta \leq \frac{1}{2}$. Then,

$$0 < p + q - 2\lfloor \sqrt{N} \rfloor < \frac{1}{4}N^{2\beta - \frac{1}{2}}.$$

Theorem 4 can be applied to the situation where the prime difference $|p - q|$ is sufficiently small.

Corollary 1. Let p and q be two large prime numbers of equal bit-length, and $N = pq$ with $|p - q| < N^\beta$ for $\frac{1}{4} < \beta \leq \frac{1}{2}$. Let the public exponent be $e = N^\alpha$. Assume there exist integers r, x , and s such that $er - x\phi(N) = s$ with $|r| \leq N^\delta$ and $|s| \leq N^\gamma$. Let $u = p + q - 2\lfloor \sqrt{N} \rfloor$. If the parameters satisfy $|s| < \min(|er|, |xu|)$,

$$2\beta - \frac{1}{2} \leq \alpha \leq 8\beta - 2,$$

and

$$2 - \frac{1}{2}\gamma - 4\beta \leq \delta < 1 - \frac{1}{2}\gamma - \sqrt{\alpha\left(2\beta - \frac{1}{2}\right)},$$

then, under Assumption 1, the factorization of N can be computed efficiently in polynomial time.

Proof. Assume that $q < p < 2q$, and that the prime gap satisfies $p - q < N^\beta$. Then, Lemma 5 ensures that $0 < u < \frac{1}{4}N^{2\beta - \frac{1}{2}}$. We can then apply Theorem 4 with $\tilde{p} = \tilde{q} = \lfloor \sqrt{N} \rfloor$, $\tilde{p} + \tilde{q} = 2\lfloor \sqrt{N} \rfloor$, and $\varepsilon = 2\beta - \frac{1}{2}$. Using these substitutions, the condition $\varepsilon \leq \alpha \leq 4\varepsilon$ gives

$$2\beta - \frac{1}{2} \leq \alpha \leq 8\beta - 2,$$

and the condition $1 - \frac{1}{2}\gamma - 2\varepsilon \leq \delta < 1 - \frac{1}{2}\gamma - \sqrt{\alpha\varepsilon}$ becomes

$$2 - \frac{1}{2}\gamma - 4\beta \leq \delta < 1 - \frac{1}{2}\gamma - \sqrt{\alpha\left(2\beta - \frac{1}{2}\right)}.$$

This concludes the proof. $\square$

Remark 3. We observe that Corollary 1 yields a better theoretical bound on δ than Theorem 4 when the difference $|p - q|$ is sufficiently small and $\tilde{p} = \lfloor \sqrt{N} \rfloor$. To compare both results, we set $\varepsilon = \beta \in (\frac{1}{4}, \frac{1}{2})$ in Theorem 4. Let D denote the difference between the bound on δ given by Corollary 1 and that obtained from Theorem 4. Then, a straightforward computation gives

$$\begin{aligned} D &= \left(1 - \frac{\gamma}{2} - \sqrt{\alpha\left(2\beta - \frac{1}{2}\right)}\right) - \left(1 - \frac{\gamma}{2} - \sqrt{\alpha\beta}\right), \\ &= \frac{\sqrt{\alpha}\left(\frac{1}{2} - \beta\right)}{\sqrt{\beta} + \sqrt{2\beta - \frac{1}{2}}}. \end{aligned}$$

This shows that $D > 0$ for all parameters $\alpha > 0$ and $\beta < \frac{1}{2}$.

Remark 4.

1. In the previous related literature [25,26] (the case $n = 1$) wherein no partial information is available, the bound on δ for breaking the scheme defined by

$$er - x\varphi(N) = s, \quad (6)$$

with $|r| < N^\delta$, and $|s| < N^\gamma$ is given by

$$\delta < 1 - \frac{\gamma}{2} - \sqrt{\alpha}.$$

In our method, by applying Corollary 1 with $\beta = 0.5$ (the standard case when $|p - q| < N^{0.5}$), we recover this bound using a different approach.

2. In the case where partial information is available, we recover the same bound as in [25,26] in the particular case of the standard RSA. Moreover, our new implementation performs better when only a few bits of the prime factors are exposed. It is worth noting that, in the classical work of Coppersmith, an attacker must know at least 50% of the bits of the prime factors to successfully mount the attack. In contrast, in the example presented in Section 6.1, our method succeeds even when only 20% of the bits of the prime factors are known.
3. For the setting in which the prime difference is small, that is, when $|p - q| < N^\lambda$, the bound given in Theorem 10 of [26] can be stated as $\delta + \frac{\gamma}{2} < 1 - \sqrt{\alpha\lambda}$. In contrast, our new result yields $\delta + \frac{\gamma}{2} < 1 - \sqrt{\alpha(2\lambda - 0.5)}$. As pointed out in Remark 3, our bound improves upon the previous one. For instance, in the typical scenario where $e \approx N$ and $|p - q| \approx N^{0.4}$ —i.e., $\alpha = 1$ and $\lambda = 0.4$ —the maximal bound obtained in [26] is $1 - \sqrt{\alpha\lambda} \approx 0.3675$, whereas our result gives $1 - \sqrt{\alpha(2\lambda - 0.5)} \approx 0.4523$. Hence, our approach allows larger values of $\delta + \frac{\gamma}{2}$ whenever $0.25 < \lambda < 0.5$ and therefore leads to a stronger cryptanalytic result.

5. Comparative Analysis: Comparison with Optimal Methods

In this section, we present a comparative analysis between our proposed approach and previously established methods addressing the same problem. It is important to note that all these methods exhibit comparable computational complexity and memory requirements, and each relies on Assumption 1. Therefore, our comparison primarily concentrates on the respective bounds achieved by each method.

5.1. Comparison with Boneh and Durfee's RSA Attack

In their seminal work, Boneh and Durfee [7] introduced a notable cryptanalytic approach targeting RSA through the key relation $ed - k\varphi(N) = 1$. They derived a critical threshold for the security of RSA when the private exponent is relatively small, showing that if the public exponent satisfies $e \approx N^\alpha$, and the private exponent scales as $d = N^\delta$ with $\delta < 1 - \sqrt{\alpha/2}$, the cryptosystem is susceptible to compromise. Our analysis reveals that by assigning $(\beta, \gamma) = (\frac{1}{2}, 0)$ in Corollary 1, this classical boundary condition is fully recovered. Consequently, their attack is a special instance of our generalized attack.

5.2. Comparison with Sarkar et al.'s RSA Attack

In 2008, Sarkar et al. [12] proposed an RSA cryptanalytic attack governed by the key equation $ed - k\varphi(N) = 1$, with the private exponent being of the form $d = N^\delta$. Their results established that when a known approximation $\tilde{p}$ of one of the RSA primes p satisfies $|p - \tilde{p}| < N^\epsilon$, and the inequality $\delta < 1 - \sqrt{\alpha\epsilon}$ holds, the system's security is compromised. By specializing the parameters in our Theorem 4 to $\gamma = 0$, this threshold is exactly recovered. This alignment indicates that the attack identified in [12] is encapsulated within the generalized category addressed by our attack.

5.3. Comparison with de Weger's RSA Attack

The attack developed by de Weger [15] concerns the RSA cryptosystem when the modulus $N = pq$ is such that p and q are of the same bit-size and the prime difference $|p - q|$ is sufficiently small. More precisely, using the equation

$$ed - k(p - 1)(q - 1) = 1,$$

where $e \approx N$, and the difference $|p - q| < N^\beta$, de Weger showed that one can factor N under the condition

$$2 - 4\beta \leq \delta < 1 - \sqrt{2\beta - \frac{1}{2}}.$$

This condition can be retrieved by taking $(\alpha, \gamma) = (1, 0)$ in Corollary 1, which shows that de Weger's result is a particular case of our generalized attack.

5.4. Comparing the Number of Weak Exponents

A meaningful metric for evaluating the strength of exponent-based cryptanalytic techniques lies in comparing the number of encryption exponents of the form $e = N^\alpha$ that can be successfully targeted.

In the attack proposed by Boneh and Durfee [7], the key equation is of the form $ed - k\varphi(N) = 1$ or, equivalently, $e \equiv \frac{1}{d} \pmod{\varphi(N)}$, where $d < \varphi(N)$ and $\varphi(N) = (p - 1)(q - 1)$. Their method can solve this equation if $d < N^{1-\sqrt{\alpha/2}}$ and $\gcd(d, \varphi(N)) = 1$. Since

$$\#\{d : 1 \leq d < \varphi(N), \gcd(d, \varphi(N)) = 1\} = \varphi(\varphi(N)),$$

then

$$\#\{d : 1 \leq d < N^{1-\sqrt{\alpha}/2}, \gcd(d, \varphi(N)) = 1\} \approx \frac{\varphi(\varphi(N))}{\varphi(N)} N^{1-\sqrt{\alpha}/2}.$$

Since

$$\frac{\varphi(\varphi(N))}{\varphi(N)} \approx \frac{C}{\log \log(\varphi(N))} = N^{-\nu},$$

for a constant $C > 0$ and a small positive number ν (see Theorem 328 of [27]), the number of weak exponents in Boneh and Durfee's attack can be estimated as follows:

$$\frac{\varphi(\varphi(N))}{\varphi(N)} N^{1-\sqrt{\alpha}/2} \approx N^{1-\sqrt{\alpha}/2-\nu}.$$

In the attack designed by Sarkar et al. [12], the equation is also $ed - k(p-1)(q-1) = 1$ with a known approximation $\tilde{p}$ of p satisfying $|p - \tilde{p}| < N^\varepsilon$. The equation can be solved if $d < N^{1-\sqrt{\alpha\varepsilon}}$. Hence, the number of such exponents d satisfying $\gcd(d, \varphi(N)) = 1$ can be estimated by

$$\frac{\varphi(\varphi(N))}{\varphi(N)} N^{1-\sqrt{\alpha\varepsilon}} \approx N^{1-\sqrt{\alpha\varepsilon}-\nu}.$$

In the attack designed by de Weger [15], the equation is again $ed - k(p-1)(q-1) = 1$ with $|p - q| < N^\beta$. The equation can be solved if $d < N^{1-\sqrt{2\beta-\frac{1}{2}}}$. Hence, the number of such exponents d satisfying $\gcd(d, \varphi(N)) = 1$ can be estimated using

$$\frac{\varphi(\varphi(N))}{\varphi(N)} N^{1-\sqrt{2\beta-\frac{1}{2}}} \approx N^{1-\sqrt{2\beta-\frac{1}{2}}-\nu}.$$

In our attack (as presented in Theorem 4), the equation to be solved is

$$er - x\varphi(N) = s,$$

with the bounds $|r| \leq N^\delta$, $|s| \leq N^\gamma$, under the conditions that an approximation $\tilde{p}$ of p is known with $|p - \tilde{p}| < N^\varepsilon$ and $\delta < 1 - \frac{1}{2}\gamma - \sqrt{\alpha\varepsilon}$. The preceding generalized equation can be rewritten as

$$e \equiv \frac{s}{r} \pmod{\varphi(N)},$$

whenever $\gcd(r, \varphi(N)) = 1$. The number of such exponents under the former conditions can then be estimated as follows:

$$2N^\gamma \times 2 \frac{\varphi(\varphi(N))}{\varphi(N)} N^{1-\frac{1}{2}\gamma-\sqrt{\alpha\varepsilon}} \approx 4N^{1+\frac{1}{2}\gamma-\sqrt{\alpha\varepsilon}-\nu},$$

where the factor 4 is used to count both positive and negatives values of r and s . In particular, for $\alpha = 1$ and $\varepsilon = 2\beta - \frac{1}{2}$ with $\frac{1}{4} < \beta \leq \frac{1}{2}$, the former estimation can be reduced to

$$4N^{1+\frac{1}{2}\gamma-\sqrt{2\beta-\frac{1}{2}}-\nu}.$$

As we can see, the number of weak exponents in our method is significantly larger by a factor $4N^{\frac{1}{2}\gamma}$ than the number of weak exponents in the previously mentioned methods.

To facilitate the comparison between the considered attacks, Table 6 summarizes their main characteristics, including the underlying equations, assumptions, bounds on the private exponent, estimated numbers of weak exponents, and applicability to large private exponents.

Table 6. Summary comparison between existing attacks and our attack.

Method	Equation	Assumptions	Bound on δ	Weak Exponent Count	Supports Large d
Boneh–Durfee [7]	$ed - k\varphi(N) = 1$	d small	$\delta < 1 - \sqrt{\alpha}/2$	$N^{1-\sqrt{\alpha}/2-\nu}$	No
Sarkar et al. [12]	$ed - k\varphi(N) = 1$	$ \tilde{p} - p < N^\epsilon$	$\delta < 1 - \sqrt{\alpha\epsilon}$	$N^{1-\sqrt{\alpha\epsilon}-\nu}$	No
de Weger [15]	$ed - k\varphi(N) = 1$	$ p - q < N^\beta$	$\delta < 1 - \sqrt{2\beta - \frac{1}{2}}$	$N^{1-\sqrt{2\beta-\frac{1}{2}}-\nu}$	No
Proposed attack	$er - x\varphi(N) = s$	$ \tilde{p} - p < N^\epsilon, s \leq N^\gamma$	$\delta < 1 - \frac{\gamma}{2} - \sqrt{\alpha\epsilon}$	$4N^{1+\frac{\gamma}{2}-\sqrt{\alpha\epsilon}-\nu}$	Yes

6. Illustrative Numerical Examples

In this section, we report the results of numerical experiments performed to evaluate the effectiveness of our attack strategy. The results demonstrate that our method can recover private exponents that lie significantly above the previously established bounds.

The parameter choices used in our numerical experiments are intended to reflect realistic RSA scenarios encountered in practice. In particular, the modulus size $N \approx 2^{2048}$ is consistent with modern cryptographic standards, where RSA moduli of 2048 bits or larger are commonly employed. Moreover, the choice $\alpha \approx 1$ corresponds to the practical setting in which the public exponent is of the same order of magnitude as the modulus. The parameters δ , ϵ , and γ were selected to satisfy the theoretical conditions established in Theorem 4 while remaining close to the corresponding security boundaries. Consequently, the proposed experiments assess the effectiveness of our attack under realistic conditions rather than in artificially favorable instances.

All computations were carried out using SageMath 10.4 on a PC running Ubuntu 22.04.3 LTS, equipped with an Intel(R) Core(TM) i5-4460 CPU @ 3.20GHz $\times$ 4 and 8 GB of RAM.

6.1. A Detailed Example for When an Approximation of One of the Prime Factors Is Known

This numerical example illustrates how an attacker can use an integer $\tilde{p}$, which is sufficiently close to one of the RSA prime factors, to break the RSA scheme as outlined in Theorem 4.

Assume that we know a portion of 150 bits of the prime p , and consider a modulus $N = pq \approx 2^{1500}$ and an encryption exponent $e \approx 2^{1500}$, along with the values

```

N = 2023015071662036435333942788700653635301518610767103980467\
6350922407405235094661783619338916505341043622377759526683\
8744324250249468515155578640947037344042491146241559909407\
4663256470481322762214095248970901334655324650989195510452\
3614013426336483300126789464075902294131497536475583486370\
7619240344426356726975139739270818648313965877667498271949\
8015370791981563098703581593857157358054058680535908587751\
7418262255139391335244682522425944011148032041,

```

$e = 2007962699496609299179362737112599707525361599726387680760 \backslash$
 $3031827811678854974475728778197203099001444566864526624794 \backslash$
 $9304758266938375747792210297027028557659782351260948550040 \backslash$
 $6077928451514428857097901648786276107846683592056664578769 \backslash$
 $5885912899886179895753814759063998583758368032721140341311 \backslash$
 $0886023270595435795112910722794303618945406150831418147010 \backslash$
 $7229902502586963163297561507069993875226956665585696579830 \backslash$
 $6000164700860095783699060395192670232171453145.$

It follows that the public exponent takes the form $e = N^\alpha$, where $\alpha \approx 0.99999$.

Let $\tilde{p}$ be an approximation of p and $\tilde{q} = \lfloor \frac{N}{\tilde{p}} \rfloor$. Building upon the methodologies presented in Theorems 3 and 4, our objective is to determine a small-integer solution (z_1, z_2, z_3) to the equation

$$z_1 z_2 + b_0 z_1 + z_3 \equiv 0 \pmod{e},$$

where $z_2 = p + q - \tilde{p} - \tilde{q}$, $b_0 = \tilde{p} + \tilde{q} - N - 1$. In this instance, we take

$\tilde{p} = 5748807539017702360253319010999088144012726969566017705645 \backslash$
 $8346933266062730545478426359479113510309777904054882975766 \backslash$
 $8307781488466938982448077805001056799625657882165054014905 \backslash$
 $9342808787762752774995538991348130034509503050809343,$
 $\tilde{q} = 3519016870771270648543366986935010687561815856310481283443 \backslash$
 $1407162140204255071761310977984330946061305415106548958220 \backslash$
 $1501580729206485058038236872536685491794541580393504213871 \backslash$
 $4379565672752841074668577627305834076271968355360528,$
 $b_0 = -2023015071662036435333942788700653635301518610767103980 \backslash$
 $4676350922407405235094661783619338916505341043622377759526 \backslash$
 $6838744324250249468515155578640947037344042491146241559909 \backslash$
 $4074663256470481322762214095248970901334655324650989194583 \backslash$
 $6699204224453327686614128855365244327751305621037486494510 \backslash$
 $9612212973358809116989637676294814447564994804445733511291 \backslash$
 $0135797697367941076784026043851565737158591500122307131215 \backslash$
 $5142957746661289727218626028558315162539741862171.$

Given that the values of r , x , u , and s in Theorem 4 are unknown to the adversary, one may instead define suitable bounds by selecting parameters δ , γ , and ε , from which the quantities Z_1 , Z_2 , Z_3 , and Z_4 are derived. In particular, we assume that $|r| \leq N^\delta$ with $\delta = 0.244$, $|p - \tilde{p}| < N^\varepsilon$ for $\varepsilon = 0.4$, and $|s| \leq N^\gamma$ for $\gamma = 0.24$. It is straightforward to verify that the assumptions of Theorem 4 are satisfied, namely, that $\varepsilon \leq \alpha \leq 4\varepsilon = 1.6$ and

$$1 - \frac{1}{2}\gamma - 2\varepsilon = 0.08 \leq \delta < 1 - \frac{1}{2}\gamma - \sqrt{\alpha\varepsilon} \approx 0.2475.$$

Accordingly, we proceed by choosing the following parameter bounds

$$\begin{aligned} Z_1 &\approx \lfloor 4N^{\alpha+\delta-1} \rfloor = 5202483556457181140754379698061164199681474302309380 \backslash \\ &\quad 88037602992955319262858283630440421612069778885153623375872, \\ Z_2 &\approx \lfloor 2N^\epsilon \rfloor = 665931629638695293669927928878682200723898098091064778420 \backslash \\ &\quad 68186678540119877217584057245080035008761116509194152165861296467877 \backslash \\ &\quad 25382903076751993171494287643817312256419079672970608640, \\ Z_3 &\approx \lfloor N^\gamma \rfloor = 2057973548493501610086935933430960036516879940583622771473 \backslash \\ &\quad 279406703284535556180203986975728784860098982838272, \\ \\ Z_4 &\approx \lfloor 16N^{\alpha+\delta+\epsilon-1} \rfloor = 69289967058392926336831129862009716397313604164230 \backslash \\ &\quad 71328359476900524715784130895244511075562851536725882288052538781090 \backslash \\ &\quad 10849031972738007273560901539668097998562900149037795843870958733186 \backslash \\ &\quad 74350295152877383857093735907481388694174220682309216979450652283985 \backslash \\ &\quad 96170227540304924641838390496871841792. \end{aligned}$$

To construct the lattice $\mathcal{L}$, we select the parameters $\nu = 6$ and $\kappa = 1$ and then build its matrix $\mathcal{M}$, whose rows consist of the coefficient vectors of the polynomials $S(c, a, b, Z_1z_1, Z_2z_2, Z_3z_3, Z_4z_4)$ with

$$S(c, a, b, z_1, z_2, z_3, z_4) = z_1^{a-c} z_2^{b-c} z_3^{\nu-a} \theta(z_1, z_4)^c e^{\nu-c},$$

where $\theta(z_1, z_4) = z_4 + b_0z_1$, and the auxiliary variable z_4 is derived from the relation $z_1z_2 = z_4 - z_3$. The triplets (c, a, b) are selected from the union of index sets $E \cup F$, where

$$\begin{aligned} E &= \left\{ (c, a, b) \in \mathbb{Z}^3 : c = 0, \dots, \nu, a = c, b = c, \dots, c + 1 + \lfloor \kappa c \rfloor \right\}, \\ F &= \left\{ (c, a, b) \in \mathbb{Z}^3 : c = 0, \dots, \nu, a = c + 1, \dots, \nu, b = c \right\}. \end{aligned}$$

The lattice $\mathcal{L}$ constructed for the attack has dimension $\rho = 56$. Upon applying the LLL algorithm to the matrix $\mathcal{M}$, we obtain a reduced matrix $\mathcal{N}$, from which a total of 56 polynomial relations are extracted. A selected subset, specifically the initial four of these polynomials, is then processed using Gröbner basis techniques. Solving the resulting system over the integers enables the recovery of the targeted root:

$$\begin{aligned} z_1 &= -66152449106614773236331136060056002230720676415724791856306319 \backslash \\ &\quad 304304253413102945889356830615697312412919902902, \\ z_2 &= -66482192815293331198104035588695550344166760368709178262130829 \backslash \\ &\quad 42019642555744441239148839529184264566485221158490539129380730619 \backslash \\ &\quad 43625325345669808333707773207578142177831409544160741, \\ z_3 &= 19573879840518761645356985839063650438428636095846768704137026831 \backslash \\ &\quad 33840359463826244243075276509507478919826621, \end{aligned}$$

$$z_4 = 43979598767098424233792277008770130106327477306656289527848328225 \backslash \\ 38423606345032991668098925779817875265913916792641389532503026860 \backslash \\ 34299755074550010565386135831724912691281758991637582457819134260 \backslash \\ 53732202900550243035700024024611123866929471695786543705981933041 \backslash \\ 274612715252038348733720197003.$$

The combined runtime for performing the LLL lattice reduction and computing the Gröbner basis amounts to under two minutes.

Thereafter, we need to find the value of r . To this end, one can compute it by the formula

$$r = -\frac{z_4 + b_0 z_1}{e} = 6664835039196079860240789649351761707985139598650609 \backslash \\ 3699268036723928579696998993737014907386100496261948392581.$$

This ensures that the condition $|s| < \inf(|er|, |xu|)$ with $(x, u, s) = (-z_1, z_2, z_3)$ is fulfilled as described in Theorem 4.

By employing both the values of the modulus $N = pq$ and the prime sum $p + q = z_2 + \tilde{p} + \tilde{q}$, one finds that

$$p = 574880753901770236025331901099908814401272696785198536750014631826 \backslash \\ 795707453492516010319411694523507455487558614539235819168445397032 \backslash \\ 592893195966784021996446474840127748170441579048789353257815307632 \backslash \\ 3436880582050234300403800137, \\ q = 351901687077127064854336698693501068756181585735969169343589577929 \backslash \\ 162926813984331018888462381331025115573226284604208432749359884903 \backslash \\ 052301276065088868083388819231137002752141430656122131320736288001 \backslash \\ 9974195239882715761458208993.$$

Subsequently, the private exponent

$$d \equiv rs^{-1} \pmod{(p-1)(q-1)},$$

can be computed. The resulting value is given by

$$d = 293003937781728628119336073116210013442955838020194830016043074607 \backslash \\ 194869415575968702453991311708648684100812330351919964447442213473 \backslash \\ 157914726577120419920759234423217388445883901675660004647454734417 \backslash \\ 686360131275397139988386067892703203856667838713185046787569451959 \backslash \\ 478712858942061938805095978217073724294867295557591223834053234231 \backslash \\ 095805061878065535381813504758821222991752454313895365896497302977 \backslash \\ 4198239648202770237184901255482252665619264496227793257,$$

which shows that $d = N^{\delta_0}$ with $\delta_0 \approx 1$.

Observe that, in this instance, we have $|p - p_0| \approx N^{\varepsilon_0}$ with $\varepsilon_0 \approx 0.399361$ and that the maximal bound provided by Sarkar et al. [12] for private exponents d rendering RSA insecure is $N^{1-\sqrt{\alpha\varepsilon_0}} \approx N^{0.36805}$. This means that our method could retrieve d , despite being significantly above the prior bound.

Notice also that in the method designed by Boneh and Durfee [7] as well as in the method developed by Li et al. [13], the private exponent d required to break RSA satisfies the inequality $d \leq N^{0.292}$. This is very far from our result, which is quite natural since we employed extra information.

6.2. Further Experiments for Large Values of N and e

In this subsection, we apply the results of Corollary 1 using the methods outlined in Theorems 3 and 4 to larger values of (N, e) . We show that, when an attacker has no additional information about one of the primes, Corollary 1 can still be used to break RSA for large values of d . In this situation, we take $\tilde{p} = \tilde{q} = \lfloor \sqrt{N} \rfloor$. A sequence of computational experiments was then conducted; at each iteration, we solved the corresponding modular equation

$$z_1 z_2 + b_0 z_1 + z_3 \equiv 0 \pmod{e},$$

for

$$b_0 = 2 \lfloor \sqrt{N} \rfloor - N - 1,$$

using the same methodologies described in Sections 3 and 4.

Notice that our method can retrieve the private exponent d satisfying

$$ed - k(p-1)(q-1) = 1,$$

despite it being significantly above the prior bounds $N^{0.292}$ and $N^{1-\sqrt{2\beta-\frac{1}{2}}}$ established by Boneh and Durfee [7] and de Weger [15], respectively.

Table 7 summarizes the experimental data, where the key equation is expressed as $er - x\varphi(N) = s$, with parameter definitions detailed subsequently

- $\text{bs}(a)$ represents the bit-size of the integer a .
- α satisfies $e = N^\alpha$ with $\alpha \approx 1$.
- δ_0 fulfills $d = N^{\delta_0}$ with $\delta_0 \approx 1$.
- δ is an exponent such that $|r| \approx N^\delta$.
- γ ensures $|s| \approx N^\gamma$.
- β is an exponent satisfying $|p - q| \approx N^\beta$.
- ν and κ are two parameters used to build the lattice $\mathcal{L}$.
- ρ is the dimension of the lattice.
- T_{LLL} and T_{GB} refer to the runtime of the LLL reduction and Gröbner basis computation, respectively.

For each size, we experimented with 10 random examples. In all cases, Assumption 1 was true, and our method was successful. The worst times of execution for each size are reported in the last two columns.

Assumption 1 is well supported by our experiments for suitable parameters. Nevertheless, it does not hold for the following cases:

- One of the bounds Z_1, Z_2, Z_3 , or Z_4 is too large.
- The conditions of Theorem 4 are not satisfied.
- The number of exposed bits of one of the prime factors is less than 17% in Theorem 4.
- The conditions of Corollary 1 are not satisfied.
- The lattice dimension becomes prohibitively large, particularly when ν is large.
- The parameter ν satisfies $\nu \leq 2$.
- The parameter r is smaller than s in both Theorem 4 and Corollary 1.

An open-source implementation of our method is available at https://github.com/Med96-hub/RSA_attacks (accessed on 25 June 2026).

Table 7. Experiments with primes satisfying $|p - q| \approx N^\beta$.

$bs(N)$	$bs(e)$	δ	γ	β	ν	κ	ρ	T_{LLL}	T_{GB}
1000	997	0.19006	0.18517	0.49822	8	1	90	26.23 s	2.6 s
2000	1999	0.14466	0.13479	0.49861	8	1	90	1.25 min	17.03 s
3000	2999	0.19673	0.19335	0.49948	8	1	90	2.51 min	9.07 s
4000	3996	0.18742	0.18621	0.49935	7	1	72	1.53 min	10.57 s
5000	4999	0.18987	0.18889	0.49965	4	1	30	3.31 s	0.51 s
6000	5998	0.19168	0.19086	0.49957	4	1	30	4.72 s	0.53 s
7000	6999	0.17425	0.17356	0.49956	4	1	30	6.46 s	0.58 s
8000	7997	0.17746	0.17684	0.49990	4	1	30	7.18 s	0.59 s
9000	9000	0.17894	0.17790	0.49949	4	1	30	9.80 s	0.63 s
100,00	9998	0.18112	0.18011	0.49982	4	1	30	10.72 s	0.63 s

7. Conclusions

In this work, we presented an extended cryptanalytic approach targeting the RSA cryptosystem. Specifically, we devised a technique for determining small-integer solutions to the modular equation $z_1 z_2 + b_0 z_1 + z_3 \equiv 0 \pmod{e}$ by leveraging Coppersmith's method in conjunction with lattice basis reduction strategies. We then applied this framework to solve instances of the equation $er - x\varphi(N) = s$, ultimately enabling the factorization of the RSA modulus $N = pq$ and compromising the underlying security of the RSA system. We also implemented our method to validate its effectiveness in cases where an integer close to one of the RSA primes is known, especially when the gap $|p - q|$ is sufficiently small. Furthermore, our approach not only encompasses several existing attacks as special cases for smaller private exponents but also enhances them through a more unified and effective methodology targeting larger ones. Nevertheless, our analysis relies on Assumption 1 concerning the algebraic independence of the generated polynomials, which remains heuristic in nature. In addition, the effectiveness of the proposed attack depends on the availability of sufficiently accurate information about the RSA prime factors. Future research directions include establishing rigorous conditions guaranteeing the validity of Assumption 1, improving the theoretical bounds derived in this work, and extending the proposed framework to other public-key cryptosystems and RSA variants.

Author Contributions: Conceptualization, M.R.; methodology, M.R. and A.N.; software, M.R.; validation, A.N. and M.Z.; formal analysis, A.N. and M.Z.; investigation, M.R. and A.N.; resources, M.R.; data curation, M.R.; writing—original draft preparation, M.R.; writing—review and editing, M.R. and A.N.; visualization, M.R. and A.N.; supervision, A.N. and M.Z.; project administration, M.R. and A.N. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A. Proof of Lemma 4

Proof. We aim to establish that each monomial appearing in the polynomial $Q(c, a, b, z_1, z_2, z_3, z_4)$, for indices (c, a, b) satisfying $0 \leq c \leq \nu$ and $(a, b) \in E(c) \cup F(c)$, and under the constraint $z_1 z_2 = z_4 - z_3$, can be written as a linear combination of elements from the collection

$$\left\{ z_1^{a-c} z_2^{b-c} z_3^{\nu-a} z_4^c \right\} \cup \bigcup_{\substack{(a', b') \in E(c') \cup F(c') \\ (c', a', b') \prec (c, a, b)}} \left\{ z_1^{a'-c'} z_2^{b'-c'} z_3^{\nu-a'} z_4^{c'} \right\},$$

where

$$E(c') = \left\{ (a', b') \in \mathbb{Z}^2 : a' = c', b' = c', \dots, c' + 1 + \lfloor \kappa c' \rfloor \right\},$$

$$F(c') = \left\{ (a', b') \in \mathbb{Z}^2 : a' = c' + 1, \dots, \nu, b' = c' \right\}.$$

Monomials that do not appear explicitly in the expansion of $Q(c, a, b, z_1, z_2, z_3, z_4)$ are understood to have vanishing coefficients.

By expanding the polynomial $(z_4 + b_0 z_1)^c$, we get

$$Q(c, a, b, z_1, z_2, z_3, z_4) = z_1^{a-c} z_2^{b-c} z_3^{\nu-a} z_4^c + \sum_{i_1=0}^{c-1} \binom{c}{i_1} b_0^{c-i_1} z_1^{a-i_1} z_2^{b-c} z_3^{\nu-a} z_4^{i_1}.$$

Case A1. For $(a, b) \in F(c)$, we have $c + 1 \leq a \leq \nu$ and $b = c$. Then,

$$z_1^{a-c} z_2^{b-c} z_3^{\nu-a} z_4^c = z_1^{a-c} z_3^{\nu-a} z_4^c,$$

and the remaining monomials satisfy

$$\begin{aligned} z_1^{a-i_1} z_2^{b-c} z_3^{\nu-a} z_4^{i_1} &= z_1^{a-i_1} z_3^{\nu-a} z_4^{i_1} \\ &= z_1^{a'-c'} z_2^{b'-c'} z_3^{\nu-a'} z_4^{c'}, \end{aligned}$$

where

$$a' = a, \quad b' = c', \quad c' = i_1.$$

Since $c + 1 \leq a \leq \nu$ and $c > i_1$, we obtain

$$c' + 1 < a' \leq \nu, \quad 0 \leq c' < c \leq \nu,$$

which together ensure that $(a', b') \in F(c')$ and $(c', a', b') \prec (c, a, b)$.

Case A2. For $(a, b) \in E(c)$, we have $a = c$ and $c \leq b \leq c + 1 + \kappa c$. Hence,

$$z_1^{a-c} z_2^{b-c} z_3^{\nu-a} z_4^c = z_2^{b-c} z_3^{\nu-c} z_4^c,$$

and

$$z_1^{a-i_1} z_2^{b-c} z_3^{\nu-a} z_4^{i_1} = z_1^{c-i_1} z_2^{b-c} z_3^{\nu-c} z_4^{i_1}.$$

In order to replace $z_1 z_2$ with $z_4 - z_3$ in the computations, we distinguish between two other cases.

Case A3. If $2c > i_1 + b$, then

$$\begin{aligned}
 z_1^{a-i_1} z_2^{b-c} z_3^{\nu-a} z_4^{i_1} &= z_1^{c-i_1} z_2^{b-c} z_3^{\nu-c} z_4^{i_1} \\
 &= z_1^{2c-i_1-b} (z_1 z_2)^{b-c} z_3^{\nu-c} z_4^{i_1} \\
 &= z_1^{2c-i_1-b} (z_4 - z_3)^{b-c} z_3^{\nu-c} z_4^{i_1} \\
 &= \sum_{k_1=0}^{b-c} \binom{b-c}{k_1} (-1)^{k_1} z_1^{2c-i_1-b} z_3^{\nu-c+k_1} z_4^{b-c-k_1+i_1} \\
 &= \sum_{k_1=0}^{b-c} \binom{b-c}{k_1} (-1)^{k_1} z_1^{a'-c'} z_2^{b'-c'} z_3^{\nu-a'} z_4^{c'},
 \end{aligned}$$

with

$$a' = c - k_1, \quad b' = c', \quad c' = b - c - k_1 + i_1.$$

Moreover, since $c \leq \nu$, $0 \leq k_1 \leq b - c$, and $2c > i_1 + b$, we deduce the following

$$a' \leq c \leq \nu, \quad a' - (c' + 1) = (2c - i_1 - b) - 1 \geq 0, \quad c' - c = (i_1 + b - 2c) - k_1 < 0,$$

and

$$c' = (b - c) - k_1 + i_1 \geq i_1 \geq 0.$$

This leads to

$$c' + 1 \leq a' \leq \nu, \quad b' = c', \quad 0 \leq c' < c \leq \nu,$$

which implies that $(a', b') \in F(c')$ and $(c', a', b') \prec (c, a, b)$.

Case A4. If $2c \leq i_1 + b$, then

$$\begin{aligned}
 z_1^{a-i_1} z_2^{b-c} z_3^{\nu-a} z_4^{i_1} &= z_1^{c-i_1} z_2^{b-c} z_3^{\nu-c} z_4^{i_1} \\
 &= z_2^{i_1+b-2c} (z_1 z_2)^{c-i_1} z_3^{\nu-c} z_4^{i_1} \\
 &= z_2^{i_1+b-2c} (z_4 - z_3)^{c-i_1} z_3^{\nu-c} z_4^{i_1} \\
 &= \sum_{k_1=0}^{c-i_1} \binom{c-i_1}{k_1} (-1)^{k_1} z_2^{i_1+b-2c} z_3^{\nu-c+k_1} z_4^{c-k_1} \\
 &= \sum_{k_1=0}^{c-i_1} \binom{c-i_1}{k_1} (-1)^{k_1} z_1^{a'-c'} z_2^{b'-c'} z_3^{\nu-a'} z_4^{c'},
 \end{aligned}$$

with

$$a' = c', \quad b' = i_1 + b - c - k_1, \quad c' = c - k_1.$$

Here, we want to show that $(a', b') \in E(c')$. It is enough to show $0 \leq c' \leq \nu$ and $c' \leq b' \leq c' + 1 + \lfloor \kappa c' \rfloor$. Since $0 \leq k_1 \leq c - i_1$ and $c \leq \nu$, we find that

$$0 \leq i_1 \leq c - k_1 = c' \leq c \leq \nu.$$

As $i_1 + b - 2c \geq 0$, we deduce that $b' - c' \geq 0$ —that is, $c' \leq b'$. On the other hand, using $b \leq c + 1 + \kappa c$, $k_1 \leq c - i_1$, and $\kappa \leq 1$, we get

$$\begin{aligned}
 b' - (c' + 1 + \kappa c') &= (b - c - 1 - \kappa c) + (i_1 + \kappa k_1 - c) \\
 &\leq (b - c - 1 - \kappa c) + (k_1 - c + i_1) \leq 0.
 \end{aligned}$$

It follows that

$$b' \leq c' + 1 + \kappa c',$$

which, after applying the floor function to both sides, implies that

$$b' \leq c' + 1 + \lfloor \kappa c' \rfloor.$$

We have $c' \leq c$. If $c' < c$, then $(c', a', b') \prec (c, a, b)$.

If $c' = c$, then $a' = a = c$ and $k_1 = 0$. Therefore

$$b' - b = i_1 - c < 0,$$

that is $(c', a', b') \prec (c, a, b)$.

In all instances, the polynomial $Q(c, a, b, z_1, z_2, z_3, z_4)$ admits the representation

$$Q(c, a, b, z_1, z_2, z_3, z_4) = z_1^{a-c} z_2^{b-c} z_3^{v-a} z_4^c + \sum_{\substack{(a', b') \in E(c') \cup F(c') \\ (c', a', b') \prec (c, a, b)}} \beta_{c', a', b'} z_1^{a'-c'} z_2^{b'-c'} z_3^{v-a'} z_4^{c'},$$

where $\beta_{c', a', b'} \in \mathbb{Z}$ and the leading term $z_1^{a-c} z_2^{b-c} z_3^{v-a} z_4^c$ dominates with respect to the predefined monomial order. By listing the monomials $z_1^{a'-c'} z_2^{b'-c'} z_3^{v-a'} z_4^{c'}$ for c varying from 0 to v and for $(a, b) \in E(c) \cup F(c)$ in lexicographic order, and assembling the corresponding coefficients from all such polynomials $Q(c, a, b, z_1, z_2, z_3, z_4)$, the resulting matrix of coefficients exhibits a lower triangular form. This concludes the proof.

□

References

1. Coppersmith, D. Small solutions to polynomial equations, and low exponent RSA vulnerabilities. *J. Cryptol.* **1997**, *10*, 233–260.
2. Bahig, H.M.; Nassr, D.I.; Mahdi, M.A.; Bahig, H.M. Small private exponent attacks on RSA using continued fractions and multicore systems. *Symmetry* **2022**, *14*, 1897.
3. Blömer, J.; May, A. A generalized Wiener attack on RSA. In *Public Key Cryptography—PKC 2004*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2004; Volume 2947, pp. 1–13.
4. Hastad, J. N using RSA with low exponent in a public key network. In *Conference on the Theory and Application of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 1985; pp. 403–408.
5. May, A. New RSA Vulnerabilities Using Lattice Reduction Methods. Ph.D. Thesis, University of Paderborn, Paderborn, Germany, 2003.
6. Wiener, M. Cryptanalysis of short RSA secret exponents. *IEEE Trans. Inf. Theory* **1990**, *36*, 553–558.
7. Boneh, D.; Durfee, G. Cryptanalysis of RSA with private key d less than $N^{0.292}$. In *Advances in Cryptology—Eurocrypt'99*; Lecture Notes in Computer Science 1592; Springer: Berlin/Heidelberg, Germany, 1999; pp. 1–11.
8. Kocher, P.C. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In *Advances in Cryptology "CRYPTO'96: 16th Annual International Cryptology Conference, Santa Barbara, CA, USA, 18–22 August 1996*; Springer: Berlin/Heidelberg, Germany, 1996; pp. 104–113.
9. Kocher, P.; Jaffe, J.; Jun, B. Differential power analysis. In *Advances in Cryptology "CRYPTO'99: 19th Annual International Cryptology Conference, Santa Barbara, CA, USA, 15–19 August 1999*; Springer: Berlin/Heidelberg, Germany, 1999; pp. 388–397.
10. Boneh, D.; Durfee, G.; Frankel, Y. An attack on RSA given a small fraction of the private key bits. In *Advances in Cryptology—ASIACRYPT'98: International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, 18–22 October 1998 Proceedings*; Springer: Berlin/Heidelberg, Germany, 1998; pp. 25–34.
11. Blomer, J.; May, A. New partial key exposure attacks on RSA. In *Annual International Cryptology Conference*; Springer: Berlin/Heidelberg, Germany, 2003; pp. 27–43.
12. Sarkar, S.; Maitra, S.; Sarkar, S. RSA cryptanalysis with increased bounds on the secret exponent using less lattice dimension. *Cryptol. ePrint Arch.* **2008**. Available online: <https://eprint.iacr.org/2008/315> (accessed on 25 June 2026).
13. Li, Q.; Zheng, Q.; Qi, W. Practical attacks on small private exponent RSA: New records and new insights. *Des. Codes Cryptogr.* **2023**, *91*, 4107–4142.

14. Herrmann, M.; May, A. Maximizing small root bounds by linearization and applications to small secret exponent RSA. In *Public Key Cryptography-PKC 2010: 13th International Conference on Practice and Theory in Public Key Cryptography, Paris, France, 26–28 May 2010*; Proceedings 13; Springer: Berlin/Heidelberg, Germany, 2010; pp. 53–69.
15. de Weger, B. Cryptanalysis of RSA with small prime difference. In *Applicable Algebra in Engineering, Communication and Computing*; Springer-Verlag: Berlin/Heidelberg, Germany, 2002; Volume 13, pp. 17–28.
16. Nitaj, A. Another generalization of Wiener’s attack on RSA, In *Africacrypt 2008*; Vaudenay, S., Ed.; LNCS; Springer: Heidelberg, Germany, 2008; Volume 5023, pp. 174–190.
17. Feng, Y.; Nitaj, A.; Pan, Y. Partial prime factor exposure attacks on some RSA variants. In *Theoretical Computer Science*; Elsevier: Amsterdam, The Netherlands, 2024; Volume 999, p. 114549.
18. Rivest, R.; Shamir, A.; Adleman, L. A Method for Obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **1978**, *21*, 120–126.
19. Lenstra, A.K.; Lenstra, H.W.; Lovász, L. Factoring polynomials with rational coefficients. *Math. Ann.* **1982**, *261*, 513–534.
20. Howgrave-Graham, N. Finding small roots of univariate modular equations revisited. In *IMA International Conference on Cryptography and Coding*; LNCS 1355; Springer: Berlin/Heidelberg, Germany, 1997; pp. 131–142.
21. Jochemsz, E.; May, A. A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants. In *ASIACRYPT 2006*; LNCS 4284; Springer: Berlin/Heidelberg, Germany, 2006; pp. 267–282.
22. Peng, L.; Hu, L.; Lu, Y.; Wei, H. An improved analysis on three variants of the RSA cryptosystem. In *International Conference on Information Security and Cryptology*; Springer: Berlin/Heidelberg, Germany, 2016; Volume 10143, pp. 140–149.
23. Rahmani, M.; Nitaj, A.; Ziane, M. A novel cryptanalytic attack on a family of RSA-like cryptosystems. *Discret. Math.* **2026**, *349*, 114660.
24. Bunder, M.; Nitaj, A.; Susilo, W.; Tonien, J. A generalized attack on RSA type cryptosystems. *Theor. Comput. Sci.* **2017**, *704*, 74–81.
25. Rahmani, M.; Nitaj, A.; Ziane, M. A generalized attack on a new variant of the RSA cryptosystem. *Comput. Appl. Math.* **2026**, *45*, 11.
26. Corbeanu, R.; Teseleanu, G. A Review of Lattice Attacks Applied to Two Types of RSA Variants. Eprint. Available online: <https://eprint.iacr.org/2026/1137.pdf> (accessed on 25 June 2026).
27. Hardy, G.H.; Wright, E.M. *An Introduction to the Theory of Numbers*; Oxford University Press: London, UK, 1965.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.