cryptography

MDPI

Article

A Hybrid Attack on Small Private Exponent RSA via Continued Fractions and Lattices †

Mengce Zheng [1,*], Yansong Feng [2,3], Abderrahmane Nitaj [4] and Yanbin Pan [2,3]

[1] College of Information and Intelligence Engineering, Zhejiang Wanli University, Ningbo 315100, China
[2] State Key Laboratory of Mathematical Sciences, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China
[3] School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing 100190, China
[4] LMNO UMR 6139, French National Centre for Scientific Research (CNRS), Université Caen Normandie, F-14000 Caen, France
* Correspondence: mczheng@zwu.edu.cn
† This paper is an extended version of our paper published in the 30th Australasian Conference on Information Security and Privacy (ACISP 2025, Wollongong, Australia, 14–16 July 2025).

Abstract

In this study, we propose a hybrid cryptanalytic technique targeting the RSA cryptosystem when instantiated with small private exponents. By integrating the continued fraction approach with Coppersmith's lattice-based technique, we formulate a novel vulnerability framework. Utilizing an innovative relationship extracted from continued fraction convergents, we deduce an improved upper bound for the secret key: $d < N^{1-\alpha/3-\gamma/2}$. In this context, $\alpha := \log_N e$ and $\gamma := \log_N |p+q-S|$, where S serves as a known approximation of the prime sum $p+q$. As an extension of our preliminary conference proceedings, this paper supplies comprehensive proofs for all theoretical propositions, performs a comprehensive parameter sensitivity evaluation, and provides bounds for partial prime exposure scenarios. Empirical evaluations confirm the theoretical mechanics of our framework, demonstrating that it offers improved bounds in specific partial leakage scenarios compared to traditional lattice-only baselines.

Keywords: RSA cryptanalysis; continued fractions; lattice-based attacks; Coppersmith's technique; small private exponent; factorization

1. Introduction

Public-key infrastructure has heavily relied on the RSA algorithm [1] since its landmark inception in 1978. While the foundational security of RSA rests upon the integer factorization problem for a large modulus $N = pq$ (where p and q are distinct primes), practical implementations often employ a small private exponent d to accelerate the decryption process. This optimization introduces well-documented vulnerabilities. If e is the public exponent, the fundamental RSA key equation is defined as $ed \equiv 1 \pmod{\phi(N)}$, where $\phi(N) = (p-1)(q-1)$ represents Euler's totient function.

Historically, cryptanalysis targeting a small d has been divided into two primary mathematical domains. The first relies on continued fractions. Wiener [2] originally demonstrated that d can be efficiently recovered if it falls below $\frac{1}{3}N^{1/4}$, a boundary later marginally improved by Susilo et al. [3] to $\frac{1}{\sqrt[4]{18}}N^{1/4}$. Other researchers [4,5] explored exponential-time refinements and exhaustive search techniques to push practical limits. Furthermore, specialized attacks have been developed to exploit specific modulus structures, such as a small prime difference $|p-q|$ [6] or known linear relations involving $\phi(N)$ [7].

Academic Editors: Fuchun Guo, Yudi Zhang, Zhen Zhao and Josef Pieprzyk

Received: 30 April 2026
Revised: 12 June 2026
Accepted: 15 June 2026
Published: 18 June 2026

The second domain leverages lattice basis reduction. Coppersmith's seminal work [8] on finding small roots of polynomial equations paved the way for Boneh and Durfee [9] to establish the widely recognized theoretical threshold of $d < N^{0.292}$, which Herrmann and May [10] subsequently refined. While theoretical improvements have been proposed [11–13], the $N^{0.292}$ threshold remains the benchmark for practical security.

Despite these advancements, practical execution rarely achieves the asymptotic limits predicted by Coppersmith's method due to the computational constraints of reducing high-dimensional lattices. To circumvent this, researchers often assume partial key leakage [14]. Ernst et al. [15] showed that knowing the most significant bits (MSBs) of d extends the attack surface. Similarly, methods guessing the MSBs of $p + q$ or incorporating shared bits between the prime factors have been explored [13,16–18].

For instance, Li et al. [12] recently improved upon Herrmann–May's attack using a binary search for the MSBs of a single prime factor. It is important to note that their attack operates under a fundamentally different threat model specifically requiring precise bit-by-bit searching, whereas our approach focuses on purely algebraic root extraction from a given approximation. Furthermore, recent heuristic approaches, such as the unpublished preprint by Feng et al. [13] (note that this reference currently remains an unpublished manuscript), have also explored exhaustive searches over $p + q$ to approach theoretical limits.

1.1. Our Contribution

This paper is an extended version of research presented at the 30th Australasian Conference on Information Security and Privacy (ACISP 2025) [19]. We present a sophisticated hybrid cryptanalytic framework that synthesizes continued fraction theory with multivariate lattice-based techniques. While standard literature often treats continued fraction methods ($d < N^{0.25}$) and lattice methods ($d < N^{0.292}$) as distinct, our approach demonstrates that their integration can yield improved results.

We begin by revisiting the continued fraction-based approach, thoroughly examining the properties of the convergents of $\frac{e}{N}$ and $\frac{e}{\phi(N)}$ to identify a common convergent $\frac{a}{b}$. Note that in RSA, the exponents e, d and Euler's totient function $\phi(N)$ are related by $ed - k\phi(N) = 1$. This analysis not only clarifies the conditions under which the ratio $\frac{k}{d}$ appears among the convergents of $\frac{e}{N}$ but also shows the optimality of Wiener's attack when solely relying on continued fractions.

Subsequently, we leverage the identified common convergent $\frac{a}{b}$ to enhance small private exponent attacks, particularly in scenarios where partial information like known MSBs of $p + q$ or shared MSBs/LSBs (where LSBs stands for least significant bits) of the primes is available. By expressing the RSA key equation $ed - k\phi(N) = 1$ in terms of parameters derived from the common convergents $\frac{a}{b}$ of $\frac{e}{N}$ and $\frac{e}{\phi(N)}$, we employ a lattice-based strategy to extract the roots of the resulting trivariate modular equations. Compared to Herrmann–May's approach, which approximates $\phi(N)$, our method yields improved results. We also extend our main approach to attack scenarios with known MSBs/LSBs of the prime factors, achieving improved attack performance relative to previous work.

This manuscript significantly extends our previous work presented at ACISP 2025 [19]. Specifically, the new contributions explicitly delineated in this journal version include the following:

- Complete mathematical proofs for all lemmas and theorems regarding common convergents, which were omitted in the conference version.
- The formal introduction and validation of Theorems 7 and 8, extending the hybrid attack to scenarios involving shared MSBs and LSBs of the prime factors.
- A comprehensive empirical sensitivity analysis (see Section 5) demonstrating the impact of lattice parameters on success rates and computation times.

- An expanded experimental baseline directly comparing our empirical bounds and overhead against the Herrmann–May framework.

1.2. Organization

The paper is structured as follows: Section 2 covers essential background on lattice reduction and continued fractions. Section 3 provides a comparative analysis of existing attacks. Our main hybrid attack and its applications to MSB/LSB prime leakage are detailed in Section 4. We present our expanded experimental results in Section 5 and offer concluding remarks in Section 6.

2. Preliminaries

In this section, we outline the mathematical foundations that underpin our proposed hybrid attack. Specifically, we review the properties of continued fraction expansions [20], as well as the lattice reduction mechanisms, most notably the LLL algorithm [21] and Coppersmith's techniques via Howgrave-Graham's lemma [8,22,23].

2.1. Continued Fractions

Let ξ be a nonzero real number. Its continued fraction expansion is given by

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

where $a_0 \in \mathbb{Z}$ and $a_1, a_2, a_3, \ldots$ are positive integers. This expansion is commonly abbreviated as $\xi = [a_0, a_1, a_2, a_3, \ldots]$. The partial quotients a_i are determined by the recurrence

$$x_0 = \xi, \quad a_i = \lfloor x_i \rfloor, \quad x_{i+1} = \frac{1}{x_i - a_i}, \quad i \geq 0, \quad x_i - a_i \neq 0.$$

The nth convergent of ξ is the rational number $\frac{p_n}{q_n} = [a_0, a_1, \ldots, a_n]$. According to the Euler–Wallis theorem, the convergents can be computed recursively:

$$\begin{aligned} &p_0 = a_0, \quad p_1 = a_0 a_1 + 1, \quad p_n = a_n p_{n-1} + p_{n-2}, \quad n \geq 2, \\ &q_0 = 1, \quad q_1 = a_1, \quad q_n = a_n q_{n-1} + q_{n-2}, \quad n \geq 2. \end{aligned}$$

A direct consequence is the identity $p_n q_{n-1} - p_{n-1} q_n = (-1)^{n+1}$, which follows by induction. The convergents satisfy the inequality

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \cdots < \xi < \cdots < \frac{p_3}{q_3} < \frac{p_1}{q_1}. \tag{1}$$

Moreover, for any integers k and d, there exists a unique solution (u, v) to the system

$$\begin{cases} k = u p_r + v p_{r-1}, \\ d = u q_r + v q_{r-1}. \end{cases} \tag{2}$$

This solution is explicitly given by

$$u = \frac{k q_{r-1} - d p_{r-1}}{p_r q_{r-1} - q_r p_{r-1}}, \quad v = \frac{d p_r - k q_r}{p_r q_{r-1} - q_r p_{r-1}},$$

where the denominator equals $(-1)^{r+1}$, ensuring that u and v are integers. It is a crucial observation and will be further utilized in our main attack. A fundamental result due to Legendre [24] that characterizes the convergents of ξ is as follows.

Theorem 1 ([24]). *Let $\xi \in \mathbb{R}$ and let $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1$. If*

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

then $\frac{a}{b}$ is a convergent of ξ.

2.2. Coppersmith's Lattice-Based Techniques

We review the lattice concepts essential to our attack. A lattice Λ is defined as the set of all integer linear combinations of linearly independent vectors $\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_\omega \in \mathbb{R}^n$:

$$\Lambda = \left\{ \sum_{i=1}^{\omega} z_i \vec{b}_i : z_i \in \mathbb{Z} \right\}.$$

Its determinant, denoted $\det(\Lambda)$ is computed as $\sqrt{\det(BB^{\mathsf{T}})}$, where the vectors $\vec{b}_i$ are the rows of the basis matrix B, and B^{T} is its transpose. For a full-rank lattice ($\omega = n$), this simplifies to $\det(\Lambda) = |\det(B)|$.

The LLL algorithm [21] is a pivotal tool for lattice reduction. It produces a reduced basis $(\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_\omega)$ satisfying good property.

Lemma 1 ([21,23]). *For an ω-dimensional lattice Λ, the LLL algorithm computes a reduced basis $(\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_\omega)$ such that*

$$\|\vec{v}_1\| \leq \cdots \leq \|\vec{v}_i\| \leq 2^{\frac{\omega(\omega-1)}{4(\omega+1-i)}} \det(\Lambda)^{\frac{1}{\omega+1-i}}, \quad i = 1, 2, \ldots, \omega.$$

The algorithm runs in time polynomial in ω and the logarithm of the maximal input coefficient.

Howgrave–Graham [22] provided a criterion to lift a modular root to an integer root. For an integer polynomial $g(x_1, \ldots, x_n) = \sum c_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n}$, its norm is defined as $\|g(x_1, \ldots, x_n)\| = \sqrt{\sum |c_{i_1,\ldots,i_n}|^2}$.

Lemma 2 ([22]). *Let $g(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ be a polynomial consisting of at most ω monomials. Given positive integers $R, X_1, \ldots, X_n$, suppose that*

$$g(x_1^\star, \ldots, x_n^\star) \equiv 0 \pmod{R} \quad \text{and} \quad \|g(X_1 x_1, \ldots, X_n x_n)\| < \frac{R}{\sqrt{\omega}},$$

where $|x_i^\star| \leq X_i$ for $i = 1, \ldots, n$. Then $g(x_1^\star, \ldots, x_n^\star) = 0$ over the integers.

By combining the LLL algorithm with Howgrave–Graham's lemma, one can effectively solve modular (and subsequently integer) polynomial equations. Suppose we obtain the first ℓ reduced vectors $(\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_\ell)$ from the lattice. Success is ensured if this crucial condition is solved $2^{\frac{\omega(\omega-1)}{4(\omega+1-\ell)}} \det(\Lambda)^{\frac{1}{\omega+1-\ell}} < \frac{R}{\sqrt{\omega}}$ holds.

The lattice-based solving strategy has the following steps: First, construct a set of shift polynomials from the given polynomial $f(x_1, \ldots, x_n)$ using the estimated bounds $X_1, \ldots, X_n$, ensuring they share a common root modulo R. Second, convert the coefficient vectors of the scaled shift polynomials $g_i(X_1 x_1, \ldots, X_n x_n)$ into the rows of a lattice basis matrix. Third, apply the LLL algorithm to obtain a reduced basis, from which one derives integer polynomials $h_i(x_1, \ldots, x_n)$. Finally, provided the polynomials $h_i(x_1, \ldots, x_n)$ are

algebraically independent, solve the system (e.g., via resultants or Gröbner basis computation) to recover the common root $(x_1^\star, \ldots, x_n^\star)$.

Although the construction of an optimal lattice basis has been extensively studied [25,26], solving the system ultimately relies on extracting independent polynomials. We adopt the standard heuristic assumption utilized throughout lattice-based cryptanalysis:

Assumption 1. *The integer polynomials derived from the LLL-reduced basis are algebraically independent, allowing their common root to be efficiently extracted.*

While Assumption 1 is a standard heuristic, algebraic dependencies can occasionally occur. In practical implementations, if the specific structure of the RSA key equation causes the LLL-reduced polynomials to fail to form a zero-dimensional ideal (preventing root extraction via Gröbner bases), our established fallback strategy is twofold. First, we marginally perturb the theoretical bounds X, Y, or Z. If independence is still not achieved, we iteratively increase the lattice dimension parameter m to generate a larger pool of candidate polynomials, which empirically resolves the dependency and forces independence in the vast majority of failing test cases.

3. Revisiting Previous Attacks

We begin by reviewing several approximations concerning $\phi(N)$ that have been instrumental in previous attacks (see, e.g., [27]).

Lemma 3 ([27])**.** *Let $N = pq$ be an RSA modulus with $q < p < 2q$, and $\phi(N) = (p-1)(q-1) = N + 1 - (p+q)$ Euler's totient function. Then $2\sqrt{N} < p + q < \frac{3\sqrt{2}}{2}\sqrt{N}$, and*

$$N - \frac{3\sqrt{2}}{2}\sqrt{N} + 1 < \phi(N) < N - 2\sqrt{N} + 1.$$

We also recall approximations in scenarios where the primes p and q share either their most or least significant bits.

Lemma 4 ([6])**.** *Let $N = pq$ be an RSA modulus, then*

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

Lemma 5 ([27])**.** *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Suppose that p and q share their least significant bits and $p - q = 2^n g$, where n is known and g is unknown. Let g_0 be a root of $x^2 \equiv N \pmod{2^n}$, and define $r_0 \equiv 2g_0 + (N - g_0^2)g_0^{-1} \pmod{2^{2n}}$. Then there exist positive integers p_0, q_0, and r_1 such that*

$$p = 2^n p_0 + g_0,\ q = 2^n q_0 + g_0,\ p + q = 2^{2n} r_1 + r_0.$$

3.1. Continued Fraction-Based Attacks

We present several results concerning the convergents derived from the continued fraction expansions involved with RSA parameters.

Lemma 6. *Let $N = pq$ be an RSA modulus with $\phi(N) = (p-1)(q-1)$. Let e be a public exponent and let d satisfy $ed \equiv 1 \pmod{\phi(N)}$. Then, there exists a positive integer k such that $ed - k\phi(N) = 1$, and*

- *if $d < \frac{1}{2}\phi(N)$, then $\frac{k}{d}$ is a convergent of $\frac{e}{\phi(N)}$.*
- *if $\frac{1}{2}\phi(N) < d < \phi(N)$, then $\frac{e-k}{\phi(N)-d}$ is a convergent of $\frac{e}{\phi(N)}$.*

Proof. Assume that $ed - k\phi(N) = 1$. If $d < \frac{1}{2}\phi(N)$, then

$$\left|\frac{e}{\phi(N)} - \frac{k}{d}\right| = \frac{1}{d\phi(N)} < \frac{1}{2d^2},$$

and, by Theorem 1, $\frac{k}{d}$ is a convergent of $\frac{e}{\phi(N)}$. If $\frac{1}{2}\phi(N) < d < \phi(N)$, then $\phi(N) - d < \frac{1}{2}\phi(N)$ and consequently, $\frac{1}{\phi(N)} < \frac{1}{2(\phi(N)-d)}$. Thus,

$$\left|\frac{e}{\phi(N)} - \frac{e-k}{\phi(N)-d}\right| = \frac{1}{\phi(N)(\phi(N)-d)} < \frac{1}{2(\phi(N)-d)^2}.$$

Since $e(\phi(N) - d) - \phi(N)(e - k) = -1$, we have $\gcd(e - k, \phi(N) - d) = 1$. Hence, by Theorem 1, $\frac{e-k}{\phi(N)-d}$ is a convergent of $\frac{e}{\phi(N)}$. □

Theorem 2. *Let $N = pq$ with $q < p < 2q$. Let e be a public exponent satisfying $\lfloor \frac{e}{N} \rfloor = \lfloor \frac{e}{\phi(N)} \rfloor = a_0$. If $\frac{a}{b}$ is a common convergent of both $\frac{e}{N}$ and $\frac{e}{\phi(N)}$, then*

$$a < \frac{e - a_0\left(N - \frac{3\sqrt{2}}{2}\sqrt{N} + 1\right)}{\sqrt{e}\,N^{1/4}} \quad \text{and} \quad b < \frac{N^{3/4}}{\sqrt{e}}.$$

Proof. First, note that if $\phi(N) < e < N$, then $\frac{e}{N} < 1$ while $\frac{e}{\phi(N)} > 1$. Hence, they cannot share a common convergent. Then, suppose that either $e < \phi(N)$ or $e > N$ so that the two fractions have at least one common convergent. Write $\frac{e}{N} = [a_0, a_1, a_2, \dots]$ and $\frac{e}{\phi(N)} = [a_0, a_1', a_2', \dots]$, with $\lfloor \frac{e}{N} \rfloor = \lfloor \frac{e}{\phi(N)} \rfloor = a_0$. By Lemma 3, we have

$$\left|\frac{e}{\phi(N)} - \frac{e}{N}\right| = \frac{e(N - \phi(N))}{N\phi(N)} > \frac{2e\sqrt{N}}{N\left(N - \frac{3\sqrt{2}}{2}\sqrt{N}\right)} = \frac{2e}{N\left(\sqrt{N} - \frac{3\sqrt{2}}{2}\right)}.$$

If $\frac{a}{b}$ is a nonzero common convergent, then

$$\frac{2e}{N\left(\sqrt{N} - \frac{3\sqrt{2}}{2}\right)} \le \left|\frac{e}{\phi(N)} - \frac{a}{b}\right| + \left|\frac{a}{b} - \frac{e}{N}\right| < \frac{2}{b^2},$$

which implies

$$b < \frac{\sqrt{N\left(\sqrt{N} - \frac{3\sqrt{2}}{2}\right)}}{\sqrt{e}} < \frac{N^{3/4}}{\sqrt{e}}.$$

Furthermore, note that the reciprocal $\frac{b}{a}$ is a convergent of both $\frac{N}{e - a_0 N}$ and $\frac{\phi(N)}{e - a_0\phi(N)}$. Applying Lemma 3 again, we obtain

$$\frac{N}{e - a_0 N} - \frac{\phi(N)}{e - a_0\phi(N)} = \frac{e(N - \phi(N))}{(e - a_0 N)(e - a_0\phi(N))} > \frac{2e\sqrt{N}}{(e - a_0 N)(e - a_0\phi(N))}.$$

Thus,

$$\frac{2e\sqrt{N}}{(e - a_0 N)(e - a_0\phi(N))} < \left|\frac{N}{e - a_0 N} - \frac{b}{a}\right| + \left|\frac{b}{a} - \frac{\phi(N)}{e - a_0\phi(N)}\right| < \frac{2}{a^2}.$$

Since $e - a_0 N < e - a_0\phi(N) < e - a_0\left(N - \frac{3\sqrt{2}}{2}\sqrt{N} + 1\right)$, it follows that

$$a < \frac{\sqrt{(e - a_0 N)(e - a_0\phi(N))}}{\sqrt{e}\,N^{1/4}} < \frac{e - a_0\left(N - \frac{3\sqrt{2}}{2}\sqrt{N} + 1\right)}{\sqrt{e}\,N^{1/4}}.$$

https://doi.org/10.3390/cryptography10030040

This terminates the proof. □

Corollary 1. *Let a_0 be a positive integer. If $e \in (1, \sqrt{N}) \cup (a_0\phi(N), a_0N) \cup (N^{3/2}, +\infty)$, then $\frac{e}{\phi(N)}$ and $\frac{e}{N}$ have no nontrivial common convergents.*

Proof. We consider the following three cases:

1. If $e \in (1, \sqrt{N})$, then $a_0 = \lfloor e/N \rfloor = 0$, and Theorem 2 implies any nontrivial common convergent $\frac{a}{b}$ would satisfy $a < \frac{\sqrt{e}}{N^{1/4}} < 1$, which is impossible.
2. If a_0 is a positive integer, and $e \in (a_0\phi(N), a_0N)$, then, since $a_0 < \frac{e}{\phi(N)}$, then $a_0 \leq \lfloor \frac{e}{\phi(N)} \rfloor$. Hence, the inequalities (1) imply that all the convergents of $\frac{e}{\phi(N)}$ are greater than a_0. On the other hand, since $\frac{e}{N} < a_0$, then $\lfloor \frac{e}{N} \rfloor \leq a_0 - 1$. Hence, all the convergents of $\frac{e}{N}$ are less than a_0 and the convergents of $\frac{e}{N}$ and $\frac{e}{\phi(N)}$ lie on opposite sides of a_0, precluding any nontrivial common convergent.
3. If $e > N^{3/2}$, then Theorem 2 implies that any common nontrivial convergent $\frac{a}{b}$ must satisfy $b < \frac{N^{3/4}}{\sqrt{e}} < 1$, which is impossible.

□

Therefore, Corollary 1 implies that $\frac{e}{N}$ and $\frac{e}{\phi(N)}$ may share a nontrivial common convergent for various intervals of e. The following result identifies conditions under which the convergents of $\frac{e}{N}$ cannot be used to attack RSA.

Theorem 3. *Let $N = pq$ be an RSA modulus with $q < p < 2q$ and $\phi(N) = (p-1)(q-1)$. Suppose that e is a public exponent with $a_0 = \lfloor \frac{e}{N} \rfloor$. Let d satisfy $ed \equiv 1 \pmod{\phi(N)}$ with $ed - k\phi(N) = 1$. Then $\frac{k}{d}$ is not among the convergents of $\frac{e}{N}$ if either*

1. $\frac{N^{3/4}}{\sqrt{e}} < d < \frac{1}{2}\phi(N)$ *or* $k > \frac{e - a_0\left(N - \frac{3\sqrt{2}}{2}\sqrt{N} + 1\right)}{\sqrt{e}\,N^{1/4}}$, *or*
2. $\frac{1}{2}\phi(N) < d < \phi(N) - \frac{N^{3/4}}{\sqrt{e}}$ *or* $k < e - \frac{e - a_0\left(N - \frac{3\sqrt{2}}{2}\sqrt{N} + 1\right)}{\sqrt{e}\,N^{1/4}}$.

Proof. Assume $ed - k\phi(N) = 1$ with $d < \phi(N)$. By Lemma 6, if $d < \frac{1}{2}\phi(N)$, then $\frac{k}{d}$ is a convergent of $\frac{e}{\phi(N)}$, whereas if $\frac{1}{2}\phi(N) < d < \phi(N)$, then $\frac{e-k}{\phi(N)-d}$ is a convergent of $\frac{e}{\phi(N)}$. In both cases, take $a_0 = \lfloor \frac{e}{N} \rfloor$.

If $d < \frac{1}{2}\phi(N)$, Theorem 2 implies that $\frac{k}{d}$ is not a convergent of $\frac{e}{N}$ provided that

$$k > \frac{e - a_0\left(N - \frac{3\sqrt{2}}{2}\sqrt{N} + 1\right)}{\sqrt{e}\,N^{1/4}} \quad \text{or} \quad d > \frac{N^{3/4}}{\sqrt{e}}.$$

Similarly, if $\frac{1}{2}\phi(N) < d < \phi(N)$, then $\frac{e-k}{\phi(N)-d}$ is not a convergent of $\frac{e}{N}$ if

$$e - k > \frac{e - a_0\left(N - \frac{3\sqrt{2}}{2}\sqrt{N} + 1\right)}{\sqrt{e}\,N^{1/4}} \quad \text{or} \quad \phi(N) - d > \frac{N^{3/4}}{\sqrt{e}}.$$

Equivalently, these conditions can be expressed as

$$k < e - \frac{e - a_0\left(N - \frac{3\sqrt{2}}{2}\sqrt{N} + 1\right)}{\sqrt{e}\,N^{1/4}} \quad \text{or} \quad d < \phi(N) - \frac{N^{3/4}}{\sqrt{e}}.$$

This completes the proof. □

The following result addresses the case when the public exponent e is of full size and demonstrates that Wiener's attack is nearly optimal.

Theorem 4. *Let $N = pq$ be an RSA modulus with $q < p < 2q$, and let $e < \phi(N)$ be a public exponent satisfying $e \approx N$. If d satisfies $ed \equiv 1 \pmod{\phi(N)}$, then the convergents of $\frac{e}{N}$ fail to recover d if $N^{1/4} < d < \phi(N) - N^{1/4}$.*

Proof. Because $e < \phi(N)$ and $e \approx N$, we have $a_0 = \lfloor e/N \rfloor = 0$. Then the first condition in Theorem 3 becomes $\frac{N^{3/4}}{\sqrt{e}} < d < \frac{1}{2}\phi(N)$, which implies $N^{1/4} < d < \frac{1}{2}\phi(N)$. The second condition in Theorem 3 yields $k > \frac{e}{\sqrt{e}\,N^{1/4}} \approx N^{1/4}$. Hence, we have

$$d = \frac{k\phi(N)+1}{e} > \frac{k\phi(N)}{e} > k > N^{1/4}.$$

Similarly, the third condition requires $\frac{1}{2}\phi(N) < d < \phi(N) - \frac{N^{3/4}}{\sqrt{e}}$, i.e., $\frac{1}{2}\phi(N) < d < \phi(N) - N^{1/4}$. Finally, the fourth condition gives $k < e - \frac{e}{\sqrt{e}\,N^{1/4}} \approx e - N^{1/4}$, so that

$$d = \frac{k\phi(N)+1}{e} < \frac{(e-N^{1/4})\phi(N)}{e} < e - N^{1/4} < \phi(N) - N^{1/4}.$$

Thus, the convergents of $\frac{e}{N}$ cannot yield d when $N^{1/4} < d < \phi(N) - N^{1/4}$. □

3.2. Lattice-Based Attacks

We revisit Herrmann–May's attack [10] for solving the RSA key equation $ed - k(p-1)(q-1) = 1$, under the assumption that an approximation S of $p+q$ is known, with $|p+q-S| < N^{\gamma}$ for $1/4 < \gamma \leq 1/2$.

Theorem 5. *Let $N = pq$ be an RSA modulus with $q < p < 2q$ and let $e = N^{\alpha}$ be a public exponent satisfying $ed - k(p-1)(q-1) = 1$ with $d < N^{\delta_0}$. Assume that an approximation S of $p+q$ is known such that $|p+q-S| < N^{\gamma}$ for $1/4 < \gamma \leq 1/2$. Then N can be factored in polynomial time provided that*

$$\delta_0 < 1 - \sqrt{\alpha\gamma}.$$

Proof. Let x denote the unknown k and set $y = p+q-S$. The key equation $ed - k(p-1)(q-1) = 1$ can be rewritten as $x(S-N-1+y) - 1 \equiv 0 \pmod{e}$. Define the polynomial

$$f(x,y) = x(A+y) - 1, \quad \text{with} \quad A = S - N - 1.$$

Then $(x_0, y_0) = (k,\ p+q-S)$ is a small solution to $f(x,y) \equiv 0 \pmod{e}$. To apply the lattice-based strategy in [10], we introduce an auxiliary variable $u = xy - 1$.

Let N^{δ_0} be a bound for d and N^{γ} a bound for $|p+q-S|$. Noting that $k < \frac{ed}{(p-1)(q-1)} \approx N^{\alpha+\delta_0-1}$, we set

$$X = N^{\alpha+\delta_0-1}, \quad Y = N^{\gamma}, \quad \text{and} \quad U \approx XY = N^{\alpha+\delta_0+\gamma-1}.$$

Let m and t be two positive integers. Construct a lattice $\mathcal{L}$ using the shift polynomials

$$g_{k,i,j}(x,y,u) = x^i y^j f(x,y)^k e^{m-k},$$

where each occurrence of $xy - 1$ is replaced by u, and $(k,i,j) \in I \cup J$ with

$$I = \{(k,i,j) : j = 0,\ k = 0,\ldots,m,\ i = 0,\ldots,m-k\}$$

and

$$J = \{(k,i,j) : i = 0,\ j = 1,\ldots,t,\ k = \lfloor m/t \rfloor j,\ldots,m\}.$$

The lattice basis is formed by the coefficient vectors of the shift polynomials $g_{k,i,j}(Xx, Yy, Uu)$ (ordered lexicographically by (k, i, j)). The monomials $x^i y^j u^k$ are ordered similarly. This construction yields a triangular lattice matrix whose determinant has the form

$$\det(\mathcal{L}) = X^{n_X} Y^{n_Y} U^{n_U} e^{n_e}.$$

The exponents are $n_X = S(i)$, $n_Y = S(j)$, $n_U = S(k)$, $n_e = S(m-k)$ determined by the sums of the respective degrees, and lattice dimension is $\omega = S(1)$ for

$$S(\sigma) = \sum_{k=0}^{m} \sum_{i=0}^{m-k} \sigma + \sum_{j=1}^{t} \sum_{k=\lfloor m/t \rfloor j}^{m} \sigma.$$

For simplicity, we set $t = m\tau$ with $\tau > 0$ and approximate $\lfloor m/t \rfloor j \approx j/\tau$. Then, omitting lower-order terms, we obtain $\omega \approx \frac{1}{2}(\tau+1)m^2$ and

$$n_X \approx \frac{1}{6}m^3, \quad n_Y \approx \frac{1}{6}\tau^2 m^3, \quad n_U \approx \frac{1}{6}(2\tau+1)^2 m^3, \quad n_e \approx \frac{1}{6}(\tau+2)m^3.$$

By applying the LLL algorithm (Lemma 1) with $i = 3$ and then invoking Howgrave–Graham's lemma (Lemma 2), one deduces that

$$2^{\frac{\omega(\omega-1)}{4(\omega-2)}} \det(\mathcal{L})^{\frac{1}{\omega-2}} < \frac{e^m}{\sqrt{\omega}}.$$

After simplification, this condition reduces to

$$\gamma\tau^2 + 2(\delta_0 + \gamma - 1)\tau + \gamma + \alpha + 2\delta_0 - 2 < 0.$$

The left term is optimized by setting τ to be $\frac{1-\delta_0-\gamma}{\gamma}$, leading to

$$-\delta_0^2 + 2\delta_0 + \alpha\gamma - 1 < 0,$$

which in turn implies

$$\delta_0 < 1 - \sqrt{\alpha\gamma}.$$

□

4. Hybrid Attack via Continued Fractions and Lattices

In this section, we integrate the relation (2) obtained from continued fractions into lattice-based attacks on small private exponents. In particular, we present new attacks that exploit both the information from (2) and the partial leakage of prime factors.

4.1. The Main Attack

Theorem 6. *Let $N = pq$ be an RSA modulus with $q < p < 2q$, and let $e = N^\alpha$ be a public exponent satisfying $ed - k(p-1)(q-1) = 1$. Let $\frac{p_{r-1}}{q_{r-1}}$ and $\frac{p_r}{q_r}$ be two consecutive convergents of $\frac{e}{N}$ with the largest denominators subject to $q_{r-1} < q_r < \frac{N^{3/4}}{\sqrt{e}}$ and $\gcd(p_r, e) = 1$. Assume that there exist integers u and v with $|u|, |v| < N^\delta$, such that $d = u\,q_r + v\,q_{r-1}$ and $k = u\,p_r + v\,p_{r-1}$. Further, let S be an approximation of $p+q$ satisfying $|p+q-S| < N^\gamma$ for $1/4 < \gamma \leq 1/2$. Then, N can be factored in polynomial time provided that*

$$\delta < \frac{1}{6}\alpha - \frac{1}{2}\gamma + \frac{1}{4}.$$

Proof. Let $\frac{p_{r-1}}{q_{r-1}}$ and $\frac{p_r}{q_r}$ be two consecutive convergents of $\frac{e}{N}$ satisfying $q_{r-1} < q_r < \frac{N^{3/4}}{\sqrt{e}}$ and $\gcd(e, p_r) = 1$. Assume that $ed - k(p-1)(q-1) = 1$ with $d = u\,q_r + v\,q_{r-1}$ and $k = u\,p_r + v\,p_{r-1}$ and that $p + q = S + w$, where S is known and w is unknown. Then the key equation can be rewritten as

$$e(uq_r + vq_{r-1}) - (up_r + vp_{r-1})(N + 1 - S - w) = 1.$$

Rearranging terms, we obtain

$$p_r wu + p_{r-1}wv - (N+1-S)p_r u - \Big((N+1-S)p_{r-1} - eq_{r-1}\Big)v - 1 \equiv 0 \pmod{eq_r}.$$

Multiplying by the inverse $p_r^{-1} \pmod{eq_r}$, we deduce

$$wu + a_1 wv + a_2 u + a_3 v + a_4 \equiv 0 \pmod{eq_r},$$

where

$$\begin{aligned}
a_1 &\equiv p_{r-1}p_r^{-1} \pmod{eq_r},\\
a_2 &\equiv -(N+1-S) \pmod{eq_r},\\
a_3 &\equiv -\Big((N+1-S)p_{r-1} - eq_{r-1}\Big)p_r^{-1} \pmod{eq_r},\\
a_4 &\equiv -p_r^{-1} \pmod{eq_r}.
\end{aligned}$$

We define the polynomial

$$f(x, y, z) = xy + a_1 xz + a_2 y + a_3 z + a_4.$$

Then the triple $(x_0, y_0, z_0) = (w, u, v)$ is a solution of the congruence $f(x, y, z) \equiv 0 \pmod{eq_r}$. We apply the lattice-based strategy of Jochemsz–May [25]. Let m and t be two positive integers. Consider the monomial set for $0 \le k \le m$:

$$M_k = \bigcup_{0 \le h \le t} \Big\{ x^i y^j z^{l+h} : x^i y^j z^l \text{ is a monomial in } f^m(x, y, z), \text{ and } \frac{x^i y^j z^l}{(xy)^k} \text{ is a monomial in } f^{m-k}(x, y, z) \Big\}.$$

An analysis shows that the monomials in $f^m(x, y, z)$ are of the form

$$x^i y^j z^l : \quad i = 0, \ldots, m, \quad j = 0, \ldots, m, \quad l = \max(i - j, 0), \ldots, m - j,$$

while those in $f^{m-k}(x, y, z)$ satisfy

$$i = 0, \ldots, m - k, \quad j = 0, \ldots, m - k, \quad l = \max(i - j, 0), \ldots, m - k - j.$$

Hence, the monomials in M_k can be written as

$$x^{i-k} y^{j-k} z^l : \quad i = k, \ldots, m, \quad j = k, \ldots, m, \quad l = \max(i - j, 0), \ldots, m - j + t.$$

Similarly, the monomials in M_{k+1} are those with

$$i = k + 1, \ldots, m, \quad j = k + 1, \ldots, m, \quad l = \max(i - j, 0), \ldots, m - j + t.$$

https://doi.org/10.3390/cryptography10030040

The Jochemsz–May strategy employs the set difference $M_k \setminus M_{k+1}$, which consists of monomials of the form $x^{i-k}y^{j-k}z^l$ for indices (i,j,l) in the sets

$$I_k = \{(i,j,l) : i = k,\ j = k,\dots,m,\ l = \max(i-j,0),\dots,m-j+t\},$$
$$J_k = \{(i,j,l) : i = k+1,\dots,m,\ j = k,\ l = \max(i-j,0),\dots,m-j+t\}.$$

For each $(i,j,l) \in I_k \cup J_k$, define the shift polynomial

$$g_{k,i,j,l}(x,y,z) = x^{i-k}y^{j-k}z^l\, f^k(x,y,z)(eq_r)^{m-k}.$$

Then for every $0 \le k \le m$ and every $(i,j,l) \in I_k \cup J_k$, we have

$$g_{k,i,j,l}(x_0,y_0,z_0) \equiv 0 \pmod{eq_r}.$$

Let X, Y, and Z be bounds for $x_0 = w$, $y_0 = u$, and $z_0 = v$, respectively. We set

$$|x_0| < X = N^\gamma, \quad |y_0| < Y = N^\delta, \quad |z_0| < Z = N^\delta.$$

Using the coefficient vectors of the scaled polynomials $g_{k,i,j,l}(Xx,Yy,Zz)$, we construct a lattice $\mathcal{L}$. We order the rows of the lattice matrix lexicographically by (k,i,j,l) and the columns corresponding to the monomials $x^iy^jz^l$ similarly. With this ordering, the lattice matrix is triangular, and its determinant takes the form

$$\det(\mathcal{L}) = X^{n_X}Y^{n_Y}Z^{n_Z}(eq_r)^{n_e}.$$

The exponents $n_X = S(i)$, $n_Y = S(j)$, $n_Z = S(l)$, $n_e = S(m-k)$ and the lattice dimension $\omega = S(1)$ are defined via appropriate summations $S(\sigma)$ with

$$S(\sigma) = \sum_{k=0}^{m}\sum_{i=k}^{k}\sum_{j=k}^{m}\sum_{l=0}^{m-j+t}\sigma + \sum_{k=0}^{m}\sum_{i=k+1}^{m}\sum_{j=k}^{k}\sum_{l=i-j}^{m-j+t}\sigma.$$

Note that in the initial double sum of $S(\sigma)$, the inner index ranges from $i = k$ to k. This is a degenerate sum intentionally formalized to denote that i is fixed exactly at k for that specific subset of shifted monomials, preventing index overlap with the subsequent J_k subset.

In particular, setting $t = m\tau$ with $\tau > 0$ for simplicity, we obtain

$$\begin{aligned} n_X &= \frac{1}{8}(4\tau+1)m^4 + o(m^4),\\ n_Y &= \frac{1}{8}(4\tau+1)m^4 + o(m^4),\\ n_Z &= \frac{1}{8}(2\tau+1)^2m^4 + o(m^4),\\ n_e &= \frac{1}{12}(8\tau+3)m^4 + o(m^4),\\ \omega &= \frac{1}{3}(3\tau+1)m^3 + o(m^3). \end{aligned} \tag{3}$$

Using $e = N^\alpha$ and $q_r < \frac{N^{3/4}}{\sqrt{e}}$, we get $eq_r < \frac{eN^{3/4}}{\sqrt{e}} = N^{\frac{\alpha}{2}+\frac{3}{4}}$. To mix Lemma 1 with $i = 3$, and Lemma 2, we set

$$2^{\frac{\omega(\omega-1)}{4(\omega-2)}}\det(\mathcal{L})^{\frac{1}{\omega-2}} < \frac{(eq_r)^m}{\sqrt{\omega}}.$$

Extracting the exponents from the solvable condition

$$X^{n_X} Y^{n_Y} Z^{n_Z} (eq_r)^{n_e} < \frac{1}{2^{\frac{\omega(\omega-1)}{4}} \omega^{\frac{\omega-2}{2}}} (eq_r)^{(\omega-2)m},$$

and substituting the above estimates (3), we deduce after simplification that

$$24\delta\tau^2 + 4(12\delta - 2\alpha + 6\gamma - 3)\tau + 12\delta - 2\alpha + 6\gamma - 3 < 0.$$

The quadratic expression in τ attains its minimum at

$$\frac{2\alpha - 12\delta - 6\gamma + 3}{12\delta}.$$

After further simplification, it yields the condition

$$\delta < \frac{1}{6}\alpha - \frac{1}{2}\gamma + \frac{1}{4}. \tag{4}$$

This completes the proof. □

For comparison, Herrmann–May's attack via Theorem 5 gives the bound $\delta_0 < 1 - \sqrt{\alpha\gamma}$. In our new attack, since $d = q_r u + q_{r-1} v$ with $q_{r-1} < q_r < N^{\frac{3}{4} - \frac{\alpha}{2}}$, and $|u|, |v| < N^{\delta}$ with δ satisfying (4), the overall bound on $d < N^{\delta_0}$ is given by

$$\delta_0 = \delta + \frac{3}{4} - \frac{\alpha}{2} < 1 - \frac{1}{3}\alpha - \frac{1}{2}\gamma.$$

Furthermore, the difference between our bound and that of Theorem 5 is

$$\begin{aligned}\Delta = 1 - \frac{1}{3}\alpha - \frac{1}{2}\gamma - \left(1 - \sqrt{\alpha\gamma}\right) &= \sqrt{\alpha\gamma} - \left(\frac{1}{3}\alpha + \frac{1}{2}\gamma\right) \\ &= -\frac{\gamma}{3}\left(\sqrt{\frac{\alpha}{\gamma}} - \frac{3+\sqrt{3}}{2}\right)\left(\sqrt{\frac{\alpha}{\gamma}} - \frac{3-\sqrt{3}}{2}\right).\end{aligned}$$

Hence $\Delta > 0$ whenever $\frac{6-3\sqrt{3}}{2}\gamma < \alpha < \frac{6+3\sqrt{3}}{2}\gamma$. In most cases, we have $\gamma \approx \frac{1}{2}$, leading to $\frac{6-3\sqrt{3}}{4} < \alpha < \frac{6+3\sqrt{3}}{4}$, namely $0.201 < \alpha < 2.799$ that is the most used interval for e. It follows that, in most choices of e, we have $\Delta > 0$, implying that our improved attack yields a better theoretical bound than that derived by using Herrmann–May's attack.

Remark 1. *It is worth noting that the lattice construction used in the proof of Theorem 6 might be further optimized. For example, by using an additional shift on the variable x, one might obtain an improved bound in certain regions for smaller γ with a fixed α. However, such modifications introduce heavy analytical complexity and tiny resulting improvement in the bound. Both this asymptotic bound and the one presented earlier in our main attack can also be computed using the formulas provided in [28] and their code (https://github.com/fffmath/AsymptoticBounds, accessed on 20 April 2026).*

Remark 2. *We further investigate Assumption 1 regarding the algebraic independence of the LLL-reduced basis. In our experiments, we observed that while the Jochemsz–May strategy typically yields the required number of independent equations, the specific structure of the RSA key equation might lead to dependencies if the bounds X, Y, Z are not well tuned.*

4.2. Applications to Primes Sharing MSBs or LSBs

We present two more applications of the main attack in scenarios where the primes share certain MSBs or LSBs.

Theorem 7. *Let $N = pq$ be an RSA modulus with $q < p < 2q$, and let $e = N^{\alpha}$ be a public exponent satisfying $ed - k(p-1)(q-1) = 1$. Let $\frac{p_{r-1}}{q_{r-1}}$ and $\frac{p_r}{q_r}$ be two consecutive convergents of $\frac{e}{N}$ with $q_{r-1} < q_r < \frac{N^{3/4}}{\sqrt{e}}$ and $\gcd(e, p_r) = 1$. Suppose there exist integers u and v with $|u|, |v| < N^{\delta}$ such that $d = u\,q_r + v\,q_{r-1}$ and $k = u\,p_r + v\,p_{r-1}$, and assume that p and q share their most significant bits so that $p - q < N^{\beta}$, with $1/4 < \beta \leq 1/2$. Then, N can be factored in polynomial time provided that*

$$\delta < \frac{1}{6}\alpha - \beta + \frac{1}{2}.$$

Proof. Assume that $p - q = N^{\beta}$. Then by Lemma 4 we have

$$p + q - 2\sqrt{N} < \frac{(p-q)^2}{4\sqrt{N}} = \frac{1}{4}N^{2\beta - \frac{1}{2}}.$$

Thus, writing $p + q = S + w$ with $S = \lfloor 2\sqrt{N} \rfloor$ known and $w < \frac{1}{4}N^{2\beta-\frac{1}{2}}$, we set

$$X = \frac{1}{4}N^{2\beta-\frac{1}{2}},$$

so that $\gamma = 2\beta - \frac{1}{2}$. Then the condition (4) becomes

$$\delta < \frac{1}{6}\alpha - \frac{1}{2}\left(2\beta - \frac{1}{2}\right) + \frac{1}{4} = \frac{1}{6}\alpha - \beta + \frac{1}{2}.$$

This completes the proof. □

For comparison, if we set $S = 2\sqrt{N}$ so that $|p + q - S| < N^{\gamma}$ with $\gamma = 2\beta - \frac{1}{2}$, Theorem 5 yields the bound $\delta_0 < 1 - \sqrt{(2\beta - \frac{1}{2})\alpha}$. In our new attack via Theorem 7, we obtain an overall bound on $d < N^{\delta_0}$ with

$$\delta_0 = \delta + \frac{3}{4} - \frac{\alpha}{2} < \frac{5}{4} - \frac{1}{3}\alpha - \beta.$$

Thus, a similar analysis shows that our new bound is superior than the bound in Theorem 5 (i.e., it is similar to the comparison in Section 4.1 using $\gamma = 2\beta - \frac{1}{2}$).

Next, we consider another attack case when p and q share some of their least significant bits.

Theorem 8. *Let $N = pq$ be an RSA modulus with $q < p < 2q$, and let $e = N^{\alpha}$ be a public exponent satisfying $ed - k(p-1)(q-1) = 1$. Let $\frac{p_{r-1}}{q_{r-1}}$ and $\frac{p_r}{q_r}$ be two consecutive convergents of $\frac{e}{N}$ with $q_{r-1} < q_r < \frac{N^{3/4}}{\sqrt{e}}$ and $\gcd(e, p_r) = 1$. Suppose there exist integers u and v with $|u|, |v| < N^{\delta}$ such that $d = u\,q_r + v\,q_{r-1}$ and $k = u\,p_r + v\,p_{r-1}$, and assume that p and q share their least significant bits so that $p - q = 2^n g$ with $2^n = N^{\beta}$, $\beta < \frac{1}{4}$, where n is known and g is unknown. Then, N can be factored in polynomial time provided that*

$$\delta < \frac{1}{6}\alpha + \beta.$$

Proof. Assume that $p - q = 2^n g$ with known n and unknown g. By Lemma 5, let g_0 be a solution of $x^2 \equiv N \pmod{2^n}$, and define $r_0 \equiv 2g_0 + (N - g_0^2)g_0^{-1} \pmod{2^{2n}}$. Then

we may express $p+q = 2^{2n}r_1 + r_0$, for some unknown integer r_1. The key equation $ed - k(p-1)(q-1) = 1$ can be rewritten as

$$e(uq_r + vq_{r-1}) - (up_r + vp_{r-1})(N + 1 - 2^{2n}r_1 - r_0) = 1.$$

Rearranging terms yields

$$2^{2n}p_r r_1 u + 2^{2n}p_{r-1}r_1 v - p_r(N+1-r_0)u \\ - \Big((N+1-r_0)p_{r-1} - eq_{r-1}\Big)v - 1 \equiv 0 \pmod{eq_r}.$$

Assuming $\gcd(2p_r, eq_r) = 1$, we multiply by $2^{-2n}p_r^{-1} \pmod{eq_r}$ to obtain

$$r_1 u + a_1 r_1 v + a_2 u + a_3 v + a_4 \equiv 0 \pmod{eq_r},$$

where

$$\begin{aligned} a_1 &\equiv p_{r-1}p_r^{-1} \pmod{eq_r}, \\ a_2 &\equiv -2^{-2n}(N+1-r_0) \pmod{eq_r}, \\ a_3 &\equiv -2^{-2n}\Big((N+1-r_0)p_{r-1} - eq_{r-1}\Big)p_r^{-1} \pmod{eq_r}, \\ a_4 &\equiv -2^{-2n}p_r^{-1} \pmod{eq_r}. \end{aligned}$$

We define the polynomial

$$f(x,y,z) = xy + a_1 xz + a_2 y + a_3 z + a_4.$$

Then the triple (r_1, u, v) is a solution of $f(x,y,z) \equiv 0 \pmod{eq_r}$. Following the same strategy as in the proof of Theorem 6 (with r_1 in place of w), and setting $2^n = N^\beta$, we have

$$r_1 = \frac{p+q-r_0}{2^{2n}} < \frac{p+q}{N^{2\beta}} < 3N^{\frac{1}{2}-2\beta}.$$

Taking $X = 3N^{\frac{1}{2}-2\beta}$ so that $\gamma = \frac{1}{2} - 2\beta$ in (4), it follows that

$$\delta < \frac{1}{6}\alpha - \frac{1}{2}\gamma + \frac{1}{4} = \frac{1}{6}\alpha + \beta.$$

This completes the proof. □

For comparison, Sun et al. [29] derived, via a weaker Boneh–Durfee's attack, the bound on $d < N^{\delta_0}$:

$$\delta_0 < \frac{2}{3}\eta + \frac{5}{6} - \frac{4}{3}\sqrt{\eta^2 + \Big(\frac{3}{2}\alpha - \frac{1}{2}\Big)\eta - \frac{6\alpha - 1}{16}}.$$

Under our notation with $\eta = \frac{1}{2} - \beta$, this bound becomes

$$\delta_0 < \frac{7}{6} - \frac{2}{3}\beta - \frac{4}{3}\sqrt{\beta^2 - \Big(\frac{3}{2}\alpha + \frac{1}{2}\Big)\beta + \frac{6\alpha + 1}{16}}.$$

In contrast, our new bound is

$$\delta_0 = \delta + \frac{3}{4} - \frac{\alpha}{2} < \beta - \frac{1}{3}\alpha + \frac{3}{4}.$$

After some tedious computation, we find that our bound is demonstrably better for $\beta < \frac{1}{4} + \frac{2\sqrt{10}-7}{9}\alpha$.

Remark 3. *It is interesting to observe that the attack bounds in Theorems 7 and 8 are indeed consistent. In Theorem 7 (with $1/4 < \beta_1 \leq 1/2$), the bound is $\delta < \frac{1}{6}\alpha - \beta_1 + \frac{1}{2}$, whereas in Theorem 8 (with $\beta_2 < 1/4$) the bound is $\delta < \frac{1}{6}\alpha + \beta_2$. Omitting identical parts in two bounds, i.e., $\frac{1}{6}\alpha$, the remaining ranges $\frac{1}{2} - \beta_1$ and β_2 coincide. It implies that Theorems 7 and 8 shall achieve the same best attack performance.*

5. Experimental Results and Discussion

To validate the correctness and effectiveness of our proposed attacks, we conducted a series of numerical experiments based on Theorem 6 (since the other theorems derive from this main result). All experiments were executed on a machine running a 64-bit Windows 11 operating system with Ubuntu 22.04 installed via WSL 2. The implementation was performed in SageMath (Version 10.3) [30], and the parameters for generating experimental instances were chosen at random.

5.1. Implementation Details and Settings

Our root extraction phase was handled using SageMath's default Gröbner basis implementation. To ensure high reliability and properly measure variability, we enforced a strict parameter strategy: for each configuration of m and t, the experiment was repeated across 10 independent random RSA instances. A timeout threshold of 600 s was set for the Gröbner basis computation to prevent infinite stalls in the event of algebraic dependence. The timing metrics recorded in our tables represent the mean execution time alongside the standard deviation ($\pm$ SD).

To generate simulated RSA instances, we first randomly selected two prime numbers p, q of a predetermined size and computed $N = pq$. Next, we generated a private exponent d of a fixed size δ_0 at random and computed its modular inverse e. Subsequently, we determined the most significant bits of $p + q$ to a prescribed ratio γ. Finally, we released the public values N, e, and S, with the known parameters $\log_2 N$, α, δ, γ, and δ_0. The open-source implementation of the proposed attacks is available at https://github.com/MengceZheng/RSA_CFL, accessed on 20 April 2026.

5.2. Experimental Validation of Our Main Result

During the experiments, we selected the parameter m and used an optimized t to control the lattice settings. Table 1 summarizes the outcomes. We successfully extracted the target integer root with 100% reliability at these lattice configurations.

Table 1. Experimental results of our hybrid attack based on Theorem 6.

Input Parameters & Lattice Settings							Attack Outcomes		
$\log_2 N$	α	δ	γ	m	t	ω	δ_0	Success Rate	Avg. Time $\pm$ SD (s)
1024	0.999	0.051	0.426	3	8	158	0.301	100%	37.61 $\pm$ 1.88
1024	1.000	0.061	0.415	3	7	142	0.311	100%	27.46 $\pm$ 1.37
1024	0.999	0.072	0.393	3	6	126	0.321	100%	20.30 $\pm$ 1.04
1024	0.999	0.076	0.380	3	5	110	0.328	100%	13.95 $\pm$ 0.70
1024	0.999	0.101	0.361	4	5	180	0.350	100%	176.19 $\pm$ 8.81

To illustrate our proposed attack, we also present the following numerical example.

Example 1. *In this example, we consider an attack scenario where* $\alpha \approx 1$, $\delta \approx 0.07$ *and* $\gamma \approx 0.4$. *The RSA modulus* N *is constructed from two 256-bit primes* p *and* q, *resulting in a composite with* $\log_2 N = 512$. *The specific values for this RSA instance are as follows:*

$$\begin{aligned} N &= 667881289802154038823628680614836895352147070157135359517370\backslash \\ &\quad 786146585569663805767598976469948361102331675600617530514952\backslash \\ &\quad 057207848849500018684481139964 1203, \\ e &= 172324352961620028297389245608298028274463258941568240927392\backslash \\ &\quad 475948736506291258628505383961459191164157282917843848198210\backslash \\ &\quad 219650188200994722142336142 9104051, \\ S &= 166371334020806181832789298204468315927873129868852419579261\backslash \\ &\quad 224686653643161600. \end{aligned}$$

In order to execute the proposed attack, we search for the parameters p_r, q_r, p_{r-1}, q_{r-1} *and* a_1, a_2, a_3, a_4 *specified in Theorem 6. Then we set* $m = 3$ *and choose an optimized* $t = 6$, *which results in the construction of a 126-dimensional lattice. After approximately 8 s of computation, we successfully extract the desired root* (x_0, y_0, z_0). *The extracted values are:*

$$\begin{aligned} x_0 &= 120228099916687374966650778411483044027272168213633206581747 6, \\ y_0 &= 24562461685, \\ z_0 &= 8887884439. \end{aligned}$$

Using the recovered value x_0 *along with* S, *we compute* $p + q = x_0 + S$, *which in turn enables the factorization of* $N = pq$ *as follows:*

$$\begin{aligned} p &= 987112039719424516017990219085220105075795285600185553619734\backslash \\ &\quad 35865055813332459, \\ q &= 676601300488637314332712754628200550868013854236643044900094\backslash \\ &\quad 70957929895646617. \end{aligned}$$

One may verify that $N = p\,q$, *confirming the success of our proposed attack. Moreover, upon computing the private exponent* d, *we find that* $d \approx N^{0.317}$. *It is crucial to note that under the exact same lattice settings, this specific instance falls outside the practical recovery range of the standard Herrmann–May framework [10], directly highlighting the improved capability of our hybrid method.*

5.3. Parameter Sensitivity and Failure Analysis

While the asymptotic bounds derived in Theorem 6 suggest that the attack becomes more powerful as the lattice dimension increases, practical implementation is constrained by the computational cost of the LLL algorithm and the quality of the reduced basis. To this end, we provide an in-depth evaluation of how the choice of parameters m and t affects the attack's performance and success rate.

The solvable condition for our trivariate modular equation is directly influenced by the lattice dimension ω. As demonstrated in Table 2, increasing m from 2 to 5 allows the attack to successfully recover larger private exponents, reaching a practical bound of $\delta_0 = 0.366$ when $\omega = 271$.

We observed a 10% failure rate strictly for the $m = 2$ configurations. At these extremely low dimensions, the LLL-reduced basis occasionally violates Assumption 1, yielding algebraically dependent polynomials that stall Gröbner basis extraction. Increasing m

resolves this dependency entirely, leading to 100% success rates for all $\omega \geq 94$ (i.e., $m \geq 3$). The average computation time grows swiftly with the lattice dimension; while dimensions around $\omega = 50$ require less than one second, the high-dimensional case at $\omega = 271$ requires approximately 1500 s.

Table 2. Impact of lattice parameters m, t on our hybrid attack.

Input Parameters & Lattice Settings							Attack Outcomes		
$\log_2 N$	α	δ	γ	m	t	ω	δ_0	Success Rate	Avg. Time $\pm$ SD (s)
1024	0.999	0.059	0.400	2	5	59	0.308	90%	1.10 ± 0.03
1024	1.000	0.065	0.390	2	4	50	0.314	90%	0.78 ± 0.04
1024	1.000	0.065	0.400	3	7	142	0.314	100%	20.76 ± 1.04
1024	1.000	0.100	0.350	3	4	94	0.349	100%	10.42 ± 0.52
1024	0.999	0.100	0.361	4	5	180	0.350	100%	182.05 ± 9.10
1024	1.000	0.105	0.350	4	5	180	0.355	100%	186.43 ± 9.32
1024	1.000	0.116	0.350	5	5	271	0.366	100%	1522.73 ± 76.19

5.4. Experimental Validation of Prime Leakage Scenarios

To further demonstrate the versatility of our framework, we conducted targeted experiments simulating partial exposure scenarios where the prime factors p and q share either their MSBs or LSBs (see Theorems 7 and 8). Table 3 summarizes the empirical outcomes using $\log_2 N = 1024$ and $m = 3$ with an optimized t. The results confirm that as the number of shared bits increases (reflected by β), the solvable condition relaxes, allowing our attack to recover larger private exponents.

Table 3. Experimental results of our hybrid attack based on Theorems 7 and 8.

Input Parameters & Leakage Conditions						Attack Outcomes		
Scenario	Theorem	α	β	δ	ω	δ_0	Success Rate	Avg. Time $\pm$ SD (s)
MSB	Theorem 7	0.999	0.400	0.127	78	0.377	100%	3.76 ± 0.21
MSB	Theorem 7	1.000	0.350	0.191	46	0.441	100%	1.37 ± 0.04
MSB	Theorem 7	0.999	0.300	0.255	46	0.505	100%	1.34 ± 0.05
LSB	Theorem 8	1.000	0.200	0.254	46	0.504	100%	1.45 ± 0.02
LSB	Theorem 8	0.999	0.150	0.190	46	0.440	100%	1.49 ± 0.04
LSB	Theorem 8	1.000	0.100	0.127	78	0.377	100%	4.35 ± 0.36

5.5. Discussion on Theoretical vs. Experimental Gap

While our approach introduces a marginal preprocessing overhead to compute continued fraction convergents and constructs a lattice of slightly larger dimension for the equivalent parameter m, it successfully recovers the private exponent in regions where the baseline method fails. We omit a direct runtime comparison with Li et al. [12], as their attack relies on a fundamentally different threat model rather than the purely algebraic root extraction utilized in our framework.

While the asymptotic bounds derived suggest the attack reaches $\delta < 0.21$, our empirical results reliably succeed around $\delta \approx 0.07$. Upon deeper analysis, this discrepancy is primarily driven by the fact that Assumption 1 occasionally fails to hold strictly for high-dimensional constructions. Furthermore, as m increases, the gap between theoretical and empirical bounds does not close entirely but stabilizes. We conjecture that this stabilization points to the existence of an implicit sub-lattice structure; if characterized mathematically, bounds could be made much tighter. Finally, as matrix dimensions exceed $\omega > 300$, LLL reduction hits a computational ceiling, representing the practical limit of modern hardware rather than a flaw in the theoretical framework.

It is also important to consider these limits in a broader cryptographic context. While our attack model focuses purely on mathematical key recovery from public parameters, real-world systems that are theoretically secure can be vulnerable to implementation flaws. Side-channel leakages such as power consumption, acoustic emanations, or network latency offer orthogonal vectors to recover key bits. Our algebraic framework directly complements side-channel attacks by reducing the number of bits an adversary must physically extract to compromise the RSA cryptosystem.

6. Conclusions

In this work, we have presented a novel approach that combines continued fractions with Coppersmith's lattice-based techniques to attack RSA with small private exponents. Our improved attacks use additional information such as partial leakage of prime factors or approximations of $p + q$ to derive higher bounds on the private exponent d. Specifically, by integrating the relation obtained from continued fraction of $\frac{e}{N}$ into a refined lattice-based attack, we have established improved theoretical bounds, as demonstrated in Theorems 6–8. Numerical experiments further validated the feasibility and effectiveness of our approach. Furthermore, our method successfully factors RSA moduli with a larger private exponent and offers improved bounds in specific partial leakage scenarios compared to existing attacks.

However, our experimental results indicate that there exists a non-negligible gap between the theoretical asymptotic predictions and the empirical limits. This discrepancy is largely driven by the degradation of LLL basis quality at high dimensions and the heuristic nature of polynomial independence. As a concrete direction for future work, we plan to investigate whether an additional independent shift on the variable x yields a measurable improvement for specific (α, γ) regions. Furthermore, we aim to extend this hybrid framework to multi-prime RSA architectures to evaluate if the continued fraction convergents maintain their structural vulnerabilities when the modulus comprises more than two prime factors.

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

Funding: This work was partially supported by the National Natural Science Foundation of China under grant numbers 62002335, 62372445, and Ningbo Young Science and Technology Talent Cultivation Program under grant number 2023QL007.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Acknowledgments: Mengce Zheng gratefully acknowledges the financial support for academic visiting provided by the China Scholarship Council (CSC No. 202308330390).

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

Abbreviations

The following abbreviations are used in this manuscript:

RSA	Rivest–Shamir–Adleman
LLL	Lenstra–Lenstra–Lovász
MSB	Most Significant Bits
LSB	Least Significant Bits

References

1. Rivest, R.; Shamir, A.; Adleman, L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
2. Wiener, M. Cryptanalysis of short RSA secret exponents. *IEEE Trans. Inf. Theory* **1990**, *36*, 553–558. [CrossRef]
3. Susilo, W.; Tonien, J.; Yang, G. The Wiener Attack on RSA Revisited: A Quest for the Exact Bound. In *Proceedings of the Information Security and Privacy—24th Australasian Conference, ACISP 2019, Christchurch, New Zealand, 3–5 July 2019, Proceedings*; Jang-Jaccard, J., Guo, F., Eds.; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2019; Volume 11547, pp. 381–398. [CrossRef]
4. Verheul, E.; Tilborg, H. Cryptanalysis of 'Less Short' RSA Secret Exponents. *Appl. Algebra Eng. Commun. Comput.* **1997**, *8*, 425–435. [CrossRef]
5. Dujella, A. Continued fractions and RSA with small secret exponent. *arXiv* **2004**, arXiv:cs/0402052.
6. Weger, B. Cryptanalysis of RSA with Small Prime Difference. *Appl. Algebra Eng. Commun. Comput.* **2002**, *13*, 17–28. [CrossRef]
7. Blömer, J.; May, A. A Generalized Wiener Attack on RSA. In *Proceedings of the Public Key Cryptography—PKC 2004, 7th International Workshop on Theory and Practice in Public Key Cryptography, Singapore, 1–4 March 2004*; Bao, F., Deng, R.H., Zhou, J., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2004; Volume 2947, pp. 1–13.
8. Coppersmith, D. Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities. *J. Cryptol.* **1997**, *10*, 233–260. [CrossRef]
9. Boneh, D.; Durfee, G. Cryptanalysis of RSA with Private Key d Less than $N^{0.292}$. In *Proceedings of the Advances in Cryptology—EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, 2–6 May 1999, Proceeding*; Stern, J., Ed.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 1999; Volume 1592, pp. 1–11. [CrossRef] [PubMed]
10. Herrmann, M.; May, A. Maximizing Small Root Bounds by Linearization and Applications to Small Secret Exponent RSA. In *Proceedings of the Public Key Cryptography—PKC 2010, 13th International Conference on Practice and Theory in Public Key Cryptography, Paris, France, 26–28 May 2010, Proceedings*; Nguyen, P.Q., Pointcheval, D., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2010; Volume 6056, pp. 53–69. [CrossRef]
11. Takayasu, A.; Kunihiro, N. How to Generalize RSA Cryptanalyses. In *Proceedings of the Public-Key Cryptography—PKC 2016—19th IACR International Conference on Practice and Theory in Public-Key Cryptography, Taipei, Taiwan, 6–9 March 2016, Proceedings, Part II*; Cheng, C., Chung, K., Persiano, G., Yang, B., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2016; Volume 9615, pp. 67–97. [CrossRef]
12. 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. [CrossRef]
13. Feng, Y.; Liu, Z.; Nitaj, A.; Pan, Y. Practical Small Private Exponent Attacks against RSA. *Cryptol. ePrint Arch.* **2024**, Paper 2024/1331.
14. Boneh, D.; Durfee, G.; Frankel, Y. An Attack on RSA Given a Small Fraction of the Private Key Bits. In *Proceedings of the Advances in Cryptology—ASIACRYPT '98, International Conference on the Theory and Applications of Cryptology and Information Security, Beijing, China, 18–22 October 1998, Proceedings*; Ohta, K., Pei, D., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 1998; Volume 1514, pp. 25–34. [CrossRef] [PubMed]
15. Ernst, M.; Jochemsz, E.; May, A.; Weger, B. Partial Key Exposure Attacks on RSA up to Full Size Exponents. In *Proceedings of the Advances in Cryptology—EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, 22–26 May 2005, Proceedings*; Cramer, R., Ed.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2005; Volume 3494, pp. 371–386. [CrossRef]
16. Sarkar, S.; Maitra, S. Improved Partial Key Exposure Attacks on RSA by Guessing a Few Bits of One of the Prime Factors. In *Proceedings of the Information Security and Cryptology—ICISC 2008, 11th International Conference, Seoul, Republic of Korea, 3–5 December 2008, Revised Selected Papers*; Lee, P.J., Cheon, J.H., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2008; Volume 5461, pp. 37–51. [CrossRef]
17. Peng, L.; Hu, L.; Huang, Z.; Xu, J. Partial Prime Factor Exposure Attacks on RSA and Its Takagi's Variant. In *Proceedings of the Information Security Practice and Experience—11th International Conference, ISPEC 2015, Beijing, China, 5–8 May 2015, Proceedings*; López, J., Wu, Y., Eds.; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2015; Volume 9065, pp. 96–108. [CrossRef]
18. Takayasu, A.; Kunihiro, N. A Tool Kit for Partial Key Exposure Attacks on RSA. In *Proceedings of the Topics in Cryptology—CT-RSA 2017—The Cryptographers' Track at the RSA Conference 2017, San Francisco, CA, USA, 14–17 February 2017, Proceedings*; Handschuh, H., Ed.; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2017; Volume 10159, pp. 58–73. [CrossRef]
19. Zheng, M.; Feng, Y.; Nitaj, A.; Pan, Y. Improving RSA Cryptanalysis: Combining Continued Fractions and Coppersmith's Techniques. In *Proceedings of the Information Security and Privacy—30th Australasian Conference, ACISP 2025, Wollongong, NSW, Australia, 14–16 July 2025, Proceedings, Part III*; Susilo, W., Pieprzyk, J., Eds.; Lecture Notes in Computer Science; Springer: Singapore, 2025; pp. 438–446. [CrossRef]

20. Hardy, G.; Wright, E. *An Introduction to the Theory of Numbers*; Oxford University Press: Oxford, UK, 1995.
21. Lenstra, A.; Lenstra, H.; Lovász, L. Factoring Polynomials with Rational Coefficients. *Math. Ann.* **1982**, *261*, 515–534. [CrossRef]
22. Howgrave-Graham, N. Finding Small Roots of Univariate Modular Equations Revisited. In *Proceedings of the Cryptography and Coding, 6th IMA International Conference, Cirencester, UK, 17–19 December 1997, Proceedings*; Darnell, M., Ed.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 1997; Volume 1355, pp. 131–142. [CrossRef]
23. May, A. New RSA Vulnerabilities Using Lattice Reduction Methods. Ph.D. Thesis, University of Paderborn, Paderborn, Germany, 2003.
24. Legendre, A. *Essai sur la Théorie des Nombres*; Duprat, An VI: Paris, France, 1798.
25. Jochemsz, E.; May, A. A Strategy for Finding Roots of Multivariate Polynomials with New Applications in Attacking RSA Variants. In *Proceedings of the Advances in Cryptology—ASIACRYPT 2006, 12th International Conference on the Theory and Application of Cryptology and Information Security, Shanghai, China, 3–7 December 2006, Proceedings*; Lai, X., Chen, K., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2006; Volume 4284, pp. 267–282. [CrossRef]
26. Lu, Y.; Zhang, R.; Peng, L.; Lin, D. Solving Linear Equations Modulo Unknown Divisors: Revisited. In *Proceedings of the Advances in Cryptology—ASIACRYPT 2015—21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, 29 November–3 December 2015, Proceedings, Part I*; Iwata, T., Cheon, J.H., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2015; Volume 9452, pp. 189–213. [CrossRef]
27. Nitaj, A.; Ariffin, M.; Nassr, D.; Bahig, H. New Attacks on the RSA Cryptosystem. In *Proceedings of the Progress in Cryptology—AFRICACRYPT 2014—7th International Conference on Cryptology in Africa, Marrakesh, Morocco, 28–30 May 2014, Proceedings*; Pointcheval, D., Vergnaud, D., Eds.; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2014; Volume 8469, pp. 178–198. [CrossRef]
28. Feng, Y.; Luo, H.; Chen, Q.; Nitaj, A.; Pan, Y. Computing Asymptotic Bounds for Small Roots in Coppersmith's Method via Sumset Theory. In *Proceedings of the Advances in Cryptology—CRYPTO 2025—45th Annual International Cryptology Conference, Santa Barbara, CA, USA, 17–21 August 2025, Proceedings, Part I*; Kalai, Y.T., Kamara, S.F., Eds.; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2025; pp. 3–32. [CrossRef]
29. Sun, H.; Wu, M.; Steinfeld, R.; Guo, J.; Wang, H. Cryptanalysis of Short Exponent RSA with Primes Sharing Least Significant Bits. In *Proceedings of the Cryptology and Network Security, 7th International Conference, CANS 2008, Hong Kong, China, 2–4 December 2008, Proceedings*; Franklin, M.K., Hui, L.C.K., Wong, D.S., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2008; Volume 5339, pp. 49–63. [CrossRef]
30. The Sage Developers. SageMath, the Sage Mathematics Software System (Version 10.3). 2025. Available online: https://www.sagemath.org (accessed on 20 April 2026).