SoK: A Generalized Attack on RSA and Its Variants

Mengce Zheng[1], Abderrahmane Nitaj[2], Maher Boudabra[3], Michel Seck[4], Oumar Niang[4], and Djiby Sow[5]

[1] Zhejiang Wanli University, Ningbo, China
mczheng@zwu.edu.cn, mengce.zheng@gmail.com
[2] Université Caen Normandie, CNRS, Normandie Univ, LMNO UMR6139, F-14000 CAEN, FRANCE
abderrahmane.nitaj@unicaen.fr
[3] King Fahd University of Petroleum and Minerals, Saudi Arabia
[4] LTISI, CRISIN'2D, Ecole Polytechnique de Thies, Senegal
[5] Dept. Mathematics and Computer Science, FST, UCAD, Senegal

Abstract. This paper introduces a generalized cryptanalytic framework for RSA and its variants, systematizing existing attacks while revealing a wide class of structural weaknesses independent of the private exponent's size. While traditional analyses exploit the key equation $ed \equiv 1 \pmod{(p-1)(q-1)}$ or its extensions like $ed \equiv 1 \pmod{(p^n-1)(q^n-1)}$ for a given RSA modulus $N = pq$ and its public exponent e, we unify these approaches by investigating the more general algebraic property defined by the congruence $eu \equiv 1 \pmod{(p^n-a)(q^n-b)}$, where a, b, and u are unknown small integer parameters. Using Coppersmith's method with unravelled linearization, we demonstrate that the modulus N can be factored in polynomial time if such a relation exists for parameters within a new, rigorously derived bound. Our framework not only unifies and generalizes several well-known attacks (retrieving their bounds as special cases when $a = b = 1$) but also significantly expands the set of weak keys. We show that an RSA instance secure against all previous small private exponent attacks may still be broken if its public key possesses this hidden algebraic structure. This work serves as a comprehensive security analysis, highlighting a new family of weak keys that future cryptographic designs should avoid.

Keywords: Coppersmith's method · Factorization · Lattice · RSA · Weak key

1 Introduction

In 1978, Rivest, Shamir, and Adleman [22] proposed the RSA cryptosystem, which remains popular and widely used in various applications. The core arithmetic of RSA consists of modular exponentiation, modulo a public integer $N = pq$, where p and q are private large prime numbers of the same bit-size, typically satisfying $q < p < 2q$. The public exponent is an integer e satisfying

$\gcd(e, \phi(N)) = 1$, where $\phi(N) = (p-1)(q-1)$ is Euler's totient function. The private exponent is an integer d satisfying the key equation $ed \equiv 1 \pmod{\phi(N)}$. In RSA, to encrypt a plaintext message $m < N$, one uses the public key (N, e) and computes the ciphertext $c \equiv m^e \pmod{N}$. To decrypt, one uses the private key (N, d) and computes $m \equiv c^d \pmod{N}$. The security of RSA primarily relies on the presumed difficulty of the integer factorization problem and the key equation problem. Specifically, these are: the problem of factoring the modulus $N = pq$; and the problem of solving the key equation $ed \equiv 1 \pmod{\phi(N)}$ to find the private exponent d where $\phi(N)$ is also unknown.

These problems are considered computationally infeasible for classical computers. Nevertheless, RSA has been intensively cryptanalyzed by exploiting vulnerabilities related to the key equation [1,10,17,27]. In 1990, Wiener [26] proposed an attack based on the continued fraction method, proving that the key equation can be solved, and thus the modulus N can be factored if $d < \frac{1}{3}N^{1/4}$. In 1999, Boneh and Durfee [2] improved this bound, demonstrating that N can be factored if $d < N^{0.292}$. The Boneh-Durfee method is based on Coppersmith's technique [6] and lattice basis reduction. Subsequently, in 2010, Herrmann and May [9] simplified the Boneh-Durfee method and achieved the same bound using the unravelled linearization technique.

Over the last three decades, several variants of RSA have been proposed, often based on different moduli or different arithmetic operations. The primary motivation behind these variants is to enhance security or improve efficiency. Some of these variants retain the modulus $N = pq$ but employ different algebraic structures, such as elliptic curves [13,14], Edwards curves [3], Gaussian integers [8], number fields [5,19,24,29], cubic Pell curves [18,23], and high-dimension curves [7].

For instance, in the RSA variants proposed in [5,8,14], while the modulus remains $N = pq$, Euler's totient function $\phi(N) = (p-1)(q-1)$ is replaced by $\psi_2(N) = \left(p^2-1\right)\left(q^2-1\right)$. This modification leads to a variant key equation $ed \equiv 1 \pmod{\psi_2(N)}$. These schemes have been subject to intensive cryptanalysis in [4,21,28]. To be concrete, Peng et al. [21] and Zheng et al. [28] demonstrated that if $e = N^\alpha$ and $d < N^\delta$, such key equation $ed \equiv 1 \pmod{\psi_2(N)}$ can be solved, and consequently N can be factored, if $\delta < 2 - \sqrt{\alpha}$.

In other variants, such as those described in [7,19,24,29], the key equation takes the form $ed \equiv 1 \pmod{\psi_n(N)}$, where $\psi_n(N) = (p^n-1)(q^n-1)$ for a fixed integer $n \geq 2$. The cryptanalysis of this variant key equation, presented in [25], yielded an attack threshold where $d < N^\delta$ with $\delta < n - \sqrt{\alpha n/2}$ assuming $e = N^\alpha$ and $n/2 \leq \alpha \leq (n+1)^2/(2n)$. This result generalizes previous findings, specifically for $n = 1$ (effectively $\phi(N)$ if $a = b = 1$ were used in a ψ_1 context, leading to $\delta < 1 - \sqrt{\alpha/2}$, which recovers the Boneh-Durfee bound [2] for $\alpha \approx 1$) and for $n = 2$ (leading to $\delta < 2 - \sqrt{\alpha}$ given in [21,28]).

The aforementioned attacks primarily exploit the arithmetic relationships involving e, $N = pq$, and specific functions like $\phi(N) = (p-1)(q-1)$ or its generalization $\psi_n(N) = (p^n-1)(q^n-1)$ for $n \geq 2$. However, these approaches are based on the assumption that a vulnerability, if one exists, must be tied to a

small private exponent d. A fundamental question is whether other, more subtle algebraic structures could render a public key insecure. Could an RSA public key (N, e) be weak even if the corresponding private exponent d is large and safe from all known attacks? This paper answers that question in the affirmative.

We move beyond the paradigm of small private exponents and introduce a new vulnerability model based on a generalized algebraic property of the public key. This paper investigates a more generalized relationship involving e, N, and a novel function $\psi_n(N, a, b)$, defined as

$$\psi_n(N, a, b) = (p^n - a)\,(q^n - b)\,,$$

where a and b are positive integers. Hence, the standard Euler's totient function $\phi(N)$ (corresponding to $\psi_1(N, 1, 1)$) and the generalized function $\psi_n(N)$ (corresponding to $\psi_n(N, 1, 1)$) are special instances of $\psi_n(N, a, b)$.

We analyze a new modified key equation

$$eu \equiv 1 \pmod{\psi_n(N, a, b)},$$

where u (a parameter may be related to the private exponent), a, and b are unknown but sufficiently small. Employing Coppersmith's method [6] in conjunction with the Herrmann-May linearization technique [9], we demonstrate that N can be factored if u, a, and b are suitably small. Specifically, assuming $e = N^{\alpha}$, $u < N^{\delta}$, and $a, b \leq N^{\beta}$ (with $|aq^n - bp^n| < 2N^{n/2}$), we establish that the modified equation $eu \equiv 1 \pmod{\psi_n(N, a, b)}$ can be solved. leading to the factorization of N, provided the following conditions hold

$$\alpha > \frac{n}{2} + \beta, \quad \beta < \frac{n}{6}, \quad \text{and} \quad \delta < n - \sqrt{\frac{\alpha(2\beta + n)}{2}}.$$

We argue that the existence of such a relation for any small (u, a, b) constitutes a new type of weak key, independent of the size of the standard private exponent d. While no current system intentionally uses this structure, our work serves as a crucial security analysis for both existing and future RSA-like schemes, identifying a potential weakness that could arise from faulty key generation, hardware errors, or unforeseen design choices.

We develop a complete cryptanalytic attack using Coppersmith's method to solve for the unknowns and factor the modulus N. We rigorously derive the conditions for our attack's success, establishing the above new bound. Our technical novelty lies in identifying this congruence as an attack surface and developing the algebraic method (see Lemma 1) to recover the necessary parameters from Coppersmith's method. Furthermore, our proposed attacks offer several advantages over the known methods. In terms of concreteness, the following facts are derived.

- Setting $n = 1$ and $\beta = 0$ (corresponding to $a = b = 1$), our bound becomes $\delta < 1 - \sqrt{\alpha/2}$. This retrieves the Boneh-Durfee bound $d < N^{0.292}$ when the public exponent e is full-size (i.e., $\alpha \approx 1$, resulting in $\delta < 1 - \sqrt{2}/2 \approx 0.292$).

- Setting $n = 2$ and $\beta = 0$ (corresponding to $a = b = 1$), our bound $\delta < 2 - \sqrt{\alpha}$ matches the one reported in [21,28].
- For any positive integer n and $\beta = 0$ (corresponding to $a = b = 1$), our bound is $\delta < n - \sqrt{\alpha n/2}$, which is consistent with the bound from [25].
- Our approach leads to the factorization of N even if the private exponent d (satisfying the standard key equation $ed \equiv 1 \pmod{\phi(N)}$ or $ed \equiv 1 \pmod{\psi_n(N)}$ with $a = b = 1$) is larger than the attack thresholds of previous methods. This is because our attack targets a different parameter u related to the generalized congruence $eu \equiv 1 \pmod{\psi_n(N, a, b)}$ for appropriately small a, b (potentially different from 1).

We demonstrate that our framework is a true generalization. By setting $a = b = 1$, our attack bound precisely reduces to the bounds of several existing attacks.

Moreover, the collection of public exponents e that are vulnerable to our proposed attacks is potentially much larger than those susceptible to attacks on standard RSA and its variants. In the standard attacks with $a = b = 1$, the number of weak public exponents e of full-size (i.e., $e \approx N^n$, implying $\alpha \approx n$) is related to the number of private exponents d such that

$$d < N^{(1-\frac{\sqrt{2}}{2})n} \quad \text{and} \quad \gcd\left(d, (p^n - 1)\,(q^n - 1)\right) = 1.$$

With our approach, for each pair of positive integers (a, b) with $a, b \leq N^\beta$ and $\beta < n/6$, a full-size public exponent e with $\alpha \approx n$ is vulnerable if there exists small u such that

$$u < N^{n - \sqrt{\frac{n(2\beta+n)}{2}}} \quad \text{and} \quad \gcd\left(u, (p^n - a)\,(q^n - b)\right) = 1.$$

Therefore, the existence of many such pairs (a, b) significantly increases the vulnerable scenarios under which an exponent e might be found weak.

This work systematizes the security landscape of RSA and its variants by introducing a generalized cryptanalytic framework. Our contributions are threefold:

1. **Unification of Existing Attacks:** We show that the standard RSA key equation and its known variants are all special instances of a single generalized congruence $eu \equiv 1 \pmod{\psi_n(N, a, b)}$. This provides a unified algebraic explanation for why previous attacks succeed.
2. **Expansion of the Weak Key Space:** By relaxing the structural parameters a and b beyond unity, we define a continuous *Security Polytope*. We demonstrate that an RSA instance secure against all previous small private exponent attacks may still be vulnerable if its public key possesses this hidden generalized structure.
3. **A New Generalized Bound:** We rigorously derive a new attack bound that subsumes previous results. Specifically, we prove that for parameters within the derived bound, the modulus N can be factored in polynomial time using Coppersmith's method.

To facilitate reproducibility, the open-source `SageMath` implementation of the proposed attack is available at https://github.com/MengceZheng/RSA_GAF.

The remainder of this paper is organized as follows. In Section 2, we introduce the main tools and useful lemmas used in our proposed attack. In Section 3, we detail the new generalized attack strategy. In Section 4, we provide a comprehensive comparison of our proposed attack with previous ones and show a numerical example. We conclude this paper in Section 5.

2 Preliminaries

In this section, we review the fundamental concepts and tools that support our attack, primarily focusing on lattice basis reduction and Coppersmith's method. Additionally, we introduce several new or specifically adapted lemmas crucial for our attack.

2.1 Lattice Basis Reduction

Let ω be a positive integer, and let $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_\omega$ be ω linearly independent vectors in $\mathbb{R}^k$, where $k \geq \omega$. A lattice $\mathcal{L}$, spanned by the basis vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_\omega$, is the discrete subgroup defined by

$$\mathcal{L} = \left\{ \sum_{i=1}^{\omega} \lambda_i \boldsymbol{b}_i \;\; | \;\; \lambda_i \in \mathbb{Z} \right\}.$$

The integer ω is the rank of the lattice $\mathcal{L}$, and k is the dimension of the ambient space $\mathbb{R}^k$. If $\omega = k$, then $\mathcal{L}$ is a full-rank lattice. An important invariant of the lattice is its determinant (also known as its volume). It is defined by $\det(\mathcal{L}) = \sqrt{\det(BB^\mathsf{T})}$, where B is the matrix whose rows are the basis vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_\omega$ and B^T denotes its matrix transpose. If $\omega = k$, this simplifies to $|\det(B)|$.

A lattice possesses infinitely many bases. Among them, certain bases consisting of relatively short and nearly orthogonal vectors, are particularly useful for solving various Diophantine problems arising in cryptanalysis. In general, finding such a good basis (e.g., one containing the shortest possible non-zero vector) is a computationally hard problem, known as the lattice reduction problem. In 1982, Lenstra, Lenstra, and Lovász [15] introduced the LLL algorithm, which provides an efficient polynomial-time solution for finding a reduced basis. This reduced basis contains vectors that are short in a well-defined sense. The following theorem provides upper bounds on the output vectors of the LLL algorithm, as often used in practice (e.g., see [16]).

Theorem 1 (LLL). *Let $\mathcal{L}$ be a lattice with a basis $(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_\omega)$. The LLL algorithm, applied to $(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_\omega)$, outputs a reduced basis $(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_\omega)$ such that, for $i = 1, \ldots, \omega$,*

$$\|\boldsymbol{u}_1\| \leq \ldots \leq \|\boldsymbol{u}_i\| \leq 2^{\frac{\omega(\omega-1)}{4(\omega+1-i)}} \det(\mathcal{L})^{\frac{1}{\omega+1-i}},$$

where $\|\boldsymbol{u}_i\|$ denotes the Euclidean norm of a vector $\boldsymbol{u}_i$.

2.2 Coppersmith's Method

In 1997, Coppersmith [6] presented a method to find small integer solutions of modular polynomial equations of the form $f_1(x) \equiv 0 \pmod{R}$, where $f_1(x)$ is a univariate polynomial with integer coefficients and R is an integer modulus. He also presented a method to find small integer roots of bivariate polynomial equations $f_2(x, y) = 0$. Since its introduction, Coppersmith's method has become a cornerstone technique for solving various types of Diophantine equations encountered in cryptanalysis. It has also been generalized to find small roots of multivariate polynomial equations [12]. Coppersmith's method and its variants fundamentally rely on lattice reduction techniques. Another key concept is the Euclidean norm of a polynomial, used in Howgrave-Graham's reformulation of Coppersmith's original method.

The Euclidean norm of a polynomial $g(x_1, \ldots, x_k) = \sum a_{i_1,\ldots,i_k} x_1^{i_1} \cdots x_k^{i_k}$ is defined by

$$\|g(x_1, \ldots, x_k)\| = \sqrt{\sum a_{i_1,\ldots,i_k}^2}.$$

In 1997, Howgrave-Graham [11] presented an elegant reformulation of Coppersmith's method for finding small roots of modular polynomial equations. It is later reformulated as the following theorem (see [16]).

Theorem 2 (Howgrave-Graham). *Let e and m be two positive integers. Let $g(x_1, \ldots, x_k) \in \mathbb{Z}[x_1, \ldots, x_k]$ be a multivariate polynomial with at most ω monomials ($\omega \geq k$). If the conditions*

$$g(z_1, \ldots, z_k) \equiv 0 \pmod{e^m} \quad \text{and} \quad \|g(x_1X_1, \ldots, x_kX_k)\| < \frac{e^m}{\sqrt{\omega}}$$

are satisfied for integers $(z_1, \ldots, z_k)$ with $|z_i| < X_i$ and known upper bounds X_i, then $g(z_1, \ldots, z_k) = 0$ holds over the integers.

To solve a given modular polynomial equation $f(x_1, \ldots, x_k) \equiv 0 \pmod{e}$, Coppersmith's method typically starts by constructing a set of ω polynomials $f_1, \ldots, f_\omega$ related to f. These polynomials f_j are constructed such that they share the desired roots $(z_1, \ldots, z_k)$ modulo e^m for some optimized integer m. Using the coefficient vectors of these ω polynomials (scaled appropriately with the bounds X_i), one constructs a basis B for a lattice $\mathcal{L}$ of dimension ω. Applying the LLL algorithm via Theorem 1 to this basis yields a reduced basis, corresponding to ω new polynomials $g_1, \ldots, g_\omega$. These polynomials are integer linear combinations of the coefficient vectors of the f_j's and thus also have the desired roots $(z_1, \ldots, z_k)$ modulo e^m. One or more of these g_i polynomials (particularly those corresponding to first short vectors in the reduced basis) are then tested using Howgrave-Graham's theorem. If Theorem 2 applies, these selected g_i polynomials vanish over the integers for the roots $(z_1, \ldots, z_k)$.

The common integer solution $(z_1, \ldots, z_k)$ can then often be found by computing a Gröbner basis or using resultant computations. A common heuristic condition for the success of Coppersmith's method, ensuring that at least k short

vectors from LLL algorithm will likely satisfy the Howgrave-Graham bound, is related to the determinant of the lattice.

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

Analyzing this inequality allows one to determine the maximum size of the roots (i.e., the X_i bounds) that can be found for a given polynomial and its modulus. For multivariate cases ($k \geq 2$), Coppersmith's method relies on heuristic arguments, including the following common assumption.

Assumption 1. *The first k polynomials $g_1, \ldots, g_k$ (or a suitable subset of k polynomials) obtained from the reduced basis that satisfy Theorems 1 and 2 are algebraically independent.*

2.3 Useful Lemmas

If $N = pq$ is an RSA modulus with $q < p < 2q$, then one has the following inequalities (see [20]),

$$\frac{\sqrt{2}}{2} N^{\frac{1}{2}} < q < N^{\frac{1}{2}} < p < \sqrt{2} N^{\frac{1}{2}}. \tag{1}$$

Next, we present an important lemma that will be instrumental in our proposed attack.

Lemma 1. *Let $N = pq$ be an RSA modulus with $q < p < 2q$, and let M be an integer such that $M = aq^n + bp^n - ab$, where a and b are two unknown positive integers. If $a, b < N^{n/6}/2$ and $|aq^n - bp^n| < 2N^{n/2}$, then*

$$aq^n + bp^n = M + \left\lfloor \frac{M^2}{4N^n} \right\rfloor,$$

and

$$|aq^n - bp^n| = \sqrt{\left(M + \left\lfloor \frac{M^2}{4N^n} \right\rfloor\right)^2 - 4N^n \left\lfloor \frac{M^2}{4N^n} \right\rfloor}.$$

Proof. Suppose that $M = aq^n + bp^n - ab$, $|aq^n - bp^n| < 2N^{n/2}$, and $a, b < N^{n/6}/2$. Since $a, b \geq 1$, we have $ab \geq 1$. Then

$$(aq^n + bp^n)^2 = (aq^n - bp^n)^2 + 4abN^n < \left(2N^{\frac{n}{2}}\right)^2 + 4abN^n = 4N^n + 4abN^n.$$

Since $1 \leq ab$, we have $4N^n \leq 4abN^n$. Thus, $4N^n + 4abN^n \leq 8abN^n$. Given $ab < \left(N^{n/6}/2\right)^2 = N^{n/3}/4$, it follows that

$$(aq^n + bp^n)^2 < 8 \cdot \frac{1}{4} N^{\frac{n}{3}} \cdot N^n = 2N^{\frac{4n}{3}}.$$

Hence, $aq^n + bp^n < 2^{1/2}N^{2n/3}$. On the other hand, we have[§]

$$4abN^n < (aq^n + bp^n)^2 = (M + ab)^2 = (aq^n - bp^n)^2 + 4abN^n < 4N^n + 4abN^n.$$

Then

$$ab < \frac{(M + ab)^2}{4N^n} < 1 + ab,$$

and

$$ab = \left\lfloor \frac{(M + ab)^2}{4N^n} \right\rfloor = \left\lfloor \frac{M^2 + 2abM + (ab)^2}{4N^n} \right\rfloor.$$

The term $2abM + (ab)^2$ satisfies

$$2abM + (ab)^2 = 2ab\,(aq^n + bp^n) - (ab)^2 < \frac{1}{2}N^{\frac{n}{3}} \cdot 2^{\frac{1}{2}}N^{\frac{2n}{3}} = 2^{-\frac{1}{2}}N^n.$$

This implies that

$$\frac{M^2 + 2abM + (ab)^2}{4N^n} < \frac{M^2}{4N^n} + 2^{-\frac{5}{2}},$$

and hence

$$ab = \left\lfloor \frac{M^2 + 2abM + (ab)^2}{4N^n} \right\rfloor = \left\lfloor \frac{M^2}{4N^n} \right\rfloor.$$

From this, we deduce

$$aq^n + bp^n = M + ab = M + \left\lfloor \frac{M^2}{4N^n} \right\rfloor,$$

and

$$|aq^n - bp^n| = \sqrt{(aq^n + bp^n)^2 - 4abN^n} = \sqrt{\left(M + \left\lfloor \frac{M^2}{4N^n} \right\rfloor\right)^2 - 4N^n \left\lfloor \frac{M^2}{4N^n} \right\rfloor}.$$

This terminates the proof. □

The following simple result guarantees that, for any given b, the inequality $|aq^n - bp^n| < 2N^{n/2}$ (a condition in Lemma 1) always holds for a certain choice of integer a.

Lemma 2. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let b be a positive integer, and let $a = [bp^n/q^n]$, where $[\zeta]$ denotes the nearest integer to ζ. Then*

$$|aq^n - bp^n| < 2N^{\frac{n}{2}}.$$

[§] This inequality is strict since the equality $aq^n = bp^n$ never occurs for distinct random large primes $p, q \approx N^{1/2}$ and small integers $a, b < N^{n/6}/2 \approx p^{n/3}$ (or $\approx q^{n/3}$).

Proof. Suppose $a = [bp^n/q^n]$. By definition of the nearest integer, we have

$$\left| a - \frac{bp^n}{q^n} \right| \leq \frac{1}{2}.$$

Multiplying by q^n (which is positive), we get

$$|aq^n - bp^n| \leq \frac{1}{2} q^n.$$

Using the inequality $q < N^{1/2}$ from (1), we have $q^n < (N^{1/2})^n = N^{n/2}$. Therefore,

$$|aq^n - bp^n| \leq \frac{1}{2} q^n < \frac{1}{2} N^{\frac{n}{2}} < N^{\frac{n}{2}}.$$

Since it is obvious that $N^{n/2} < 2N^{n/2}$, this terminates the proof. □

3 The Generalized Attack

In this section, we present a new generalized attack on RSA and its variants applicable when there exist two positive integers a and b such that the public exponent e satisfies the congruence $eu \equiv 1 \pmod{(p^n - a)(q^n - b)}$ for a small integer u.¶

Theorem 3. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let a, b be two unknown positive integers such that $a, b \leq N^\beta$ for some $\beta < n/6 - \log_N 2$, and let them also satisfy $|aq^n - bp^n| < 2N^{n/2}$. Let $e = N^\alpha$ be a public exponent satisfying the equation $eu \equiv 1 \pmod{(p^n - a)(q^n - b)}$ with an unknown $u < N^\delta$. If $\alpha > n/2 + \beta$, and*

$$\delta < n - \sqrt{\frac{\alpha(2\beta + n)}{2}}, \tag{2}$$

then N can be factored in polynomial time.

Proof. The equation $eu \equiv 1 \pmod{(p^n - a)(q^n - b)}$ implies the existence of an integer v such that

$$eu - v(p^n - a)(q^n - b) = 1.$$

Expanding the product term gives $(p^n - a)(q^n - b) = N^n - (aq^n + bp^n - ab)$. Let y_0 denote $-(aq^n + bp^n - ab)$. Then the equation becomes $eu - v(N^n + y_0) = 1$, which leads to the congruence $v(N^n + y_0) + 1 \equiv 0 \pmod{e}$.

We can therefore define a polynomial

$$f(x, y) = x(A + y) + 1 \quad \text{with} \quad A = N^n,$$

¶ In this generalized framework, the parameter u acts as a "generalized private exponent." Unlike the standard private exponent d, u is the modular inverse of e with respect to the hidden structure $\psi_n(N, a, b)$.

which has a small integer root $(x_0, y_0) = (v, -(aq^n + bp^n - ab))$ modulo e. To find this root, we apply the linearization method of Herrmann and May [9]. The relation $f(x, y) \equiv 0 \pmod{e}$ can be expressed as $Ax + xy + 1 \equiv 0 \pmod{e}$. Let $z = xy + 1$. This introduces a new variable z and a new polynomial relation

$$g(x, z) = Ax + z \equiv 0 \pmod{e}.$$

The goal is to find the small integer roots (x_0, y_0) by finding the roots of a system of polynomials in variables x, y and z.

Let m and t be two positive integer parameters to be optimized later. We define two sets of indices (k, i, j) as follows.

$$\begin{aligned}\mathcal{I} &= \{(k,i,j) \mid j = 0,\ k = 0, \ldots, m,\ i = 0, \ldots, m-k\},\\ \mathcal{J} &= \{(k,i,j) \mid j = 1, \ldots, t,\ k = \lfloor m/t \rfloor j, \ldots, m,\ i = 0\}.\end{aligned}$$

From the relationship

$$v = \frac{eu - 1}{(p^n - a)(q^n - b)} \approx \frac{eu}{N^n},$$

and given the sizes $e = N^\alpha$ and $u < N^\delta$, we can establish bounds for the roots. For the solution $(x_0, y_0) = (v, -(aq^n + bp^n - ab))$, we have

- $|x_0| = |v| < N^{\alpha+\delta-n}$ and we set the bound $X = N^{\alpha+\delta-n}$.
- $|y_0| = |aq^n + bp^n - ab| < (a + b)p^n < 2N^\beta(2^{1/2}N^{1/2})^n = 2^{1+n/2}N^{\beta+n/2}$ and we set the bound $Y = 2^{1+n/2}N^{\beta+n/2}$.
- $|z_0| = |x_0y_0 + 1| < XY + 1$ and we set the bound $Z = 2^{1+n/2}N^{\alpha+\beta+\delta-n/2}$.

Since $N \gg 2$ for standard RSA and its variants, we omit constant factors for simplicity in the asymptotic analysis. These bounds can be formally written as

$$X = N^{\alpha+\delta-n},\ Y = N^{\beta+\frac{n}{2}},\ Z = N^{\alpha+\beta+\delta-\frac{n}{2}}. \tag{3}$$

Remark 1. In the above bounds for $|x_0|, |y_0|, |z_0|$, we omit small constant factors to simplify the asymptotic analysis, which is also a common treatment used in Coppersmith's method. In a finite-dimensional implementation, these constants imply a negligible reduction in the bound δ, which does not affect the polynomial-time solvability.

To apply Coppersmith's method, we construct a lattice $\mathcal{L}$ from the following set of polynomials, which all have the root (x_0, y_0, z_0) modulo e^m.

$$G_{k,i,j}(x, y, z) = x^i y^j g(x, z)^k e^{m-k} \quad \text{for} \quad (k, i, j) \in \mathcal{I} \cup \mathcal{J},$$

where $g(x, z) = Ax + z$ and the relation $xy = z - 1$ is used. The lattice is built by constructing a basis matrix where the rows are the coefficients of the polynomials $G_{k,i,j}(xX, yY, zZ)$, ordered following the lexical order of $(k, i, j) \in \mathcal{I} \cup \mathcal{J}$, and

Table 1. A toy example of lattice basis matrix for $m = 3$ and $t = 1$.

$G_{k,i,j}$	1	x	x^2	x^3	z	xz	x^2z	z^2	xz^2	z^3	yz^3
$G_{0,0,0}$	e^3	0	0	0	0	0	0	0	0	0	0
$G_{0,1,0}$	0	Xe^3	0	0	0	0	0	0	0	0	0
$G_{0,2,0}$	0	0	X^2e^3	0	0	0	0	0	0	0	0
$G_{0,3,0}$	0	0	0	X^3e^3	0	0	0	0	0	0	0
$G_{1,0,0}$	0	AXe^2	0	0	Ze^2	0	0	0	0	0	0
$G_{1,1,0}$	0	0	AX^2e^2	0	0	XZe^2	0	0	0	0	0
$G_{1,2,0}$	0	0	0	AX^3e^2	0	0	X^2Ze^2	0	0	0	0
$G_{2,0,0}$	0	0	A^2X^2e	0	0	$2AXZe$	0	Z^2e	0	0	0
$G_{2,1,0}$	0	0	0	A^2X^3e	0	0	$2AX^2Ze$	0	XZ^2e	0	0
$G_{3,0,0}$	0	0	0	A^3X^3	0	0	$3A^2X^2Z$	0	$3AXZ^2$	Z^3	0
$G_{3,0,1}$	0	0	$-A^3X^2$	0	0	$-3A^2XZ$	A^3X^2Z	$-3AZ^2$	$3A^2XZ^2$	$3AZ^3$	YZ^3

the columns are the coefficients of the monomials $x^iy^jz^k$, ordered in the same way. A toy example of the resulting lattice basis matrix for $m = 3$ and $t = 1$ is shown in Table 1.

By construction, the matrix of the lattice is upper triangular, and its determinant is the product of its diagonal entries, that is

$$\det(\mathcal{L}) = X^{n_X} Y^{n_Y} Z^{n_Z} e^{n_e}, \tag{4}$$

where the exponents n_X, n_Y, n_Z, n_e and the lattice dimension ω are sums over the index set $I \cup J$. More precisely,[‖]

$$\begin{aligned} n_X &= \sum_{k=0}^{m} \sum_{i=0}^{m-k} i + \sum_{j=1}^{t} \sum_{k=\lfloor m/t \rfloor j}^{m} 0 \\ &= \frac{1}{6} m(m+1)(m+2), \\ n_Y &= \sum_{k=0}^{m} \sum_{i=0}^{m-k} 0 + \sum_{j=1}^{t} \sum_{k=\lfloor m/t \rfloor j}^{m} j \\ &= \frac{1}{6} (t+1)(mt - m + 3t), \end{aligned}$$

[‖] For asymptotic simplicity, we assume m is a multiple of t and then omit the floor function $\lfloor m/t \rfloor$.

$$
\begin{aligned}
n_Z &= \sum_{k=0}^{m}\sum_{i=0}^{m-k} k + \sum_{j=1}^{t}\sum_{k=\lfloor m/t\rfloor j}^{m} k \\
&= \frac{1}{6}m(m+1)(m+2) + \frac{m}{12t}(4mt^2 - 3mt - m + 9t^2 + 3t), \\
n_e &= \sum_{k=0}^{m}\sum_{i=0}^{m-k} (m-k) + \sum_{j=1}^{t}\sum_{k=\lfloor m/t\rfloor j}^{m} (m-k) \\
&= \frac{1}{3}m(m+1)(m+2) + \frac{m}{12t}(t-1)(2mt - m + 3t), \\
\omega &= \sum_{k=0}^{m}\sum_{i=0}^{m-k} 1 + \sum_{j=1}^{t}\sum_{k=\lfloor m/t\rfloor j}^{m} 1 \\
&= \frac{1}{2}(m+1)(m+2) + \frac{1}{2}m(t-1) + t.
\end{aligned}
$$

Setting $t = \tau m$ for $\tau > 0$ and considering the dominant terms for sufficiently large m, the above quantities can be approximated by

$$
n_X = \frac{1}{6}m^3,\ n_Y = \frac{\tau^2}{6}m^3,\ n_Z = \frac{2\tau+1}{6}m^3,\ n_e = \frac{\tau+2}{6}m^3,\ \omega = \frac{\tau+1}{2}m^2. \quad (5)
$$

For the attack to succeed, we need to find at least three algebraically independent polynomials that are short enough to satisfy the conditions in Theorem 2. Using the LLL bound for the third vector ($i = 3$ in Theorem 1), the resulting condition is

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

which can be transformed into

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

Asymptotically, for large ω, this simplifies to $\det(\mathcal{L}) < e^{m\omega}$. Combining this with (4) yields the inequality

$$
X^{n_X} Y^{n_Y} Z^{n_Z} e^{n_e} < e^{m\omega}.
$$

Using the derived exponents (5), and neglecting the lower-order terms, we have

$$
X^{\frac{1}{6}m^3} Y^{\frac{\tau^2}{6}m^3} Z^{\frac{2\tau+1}{6}m^3} e^{\frac{\tau+2}{6}m^3} < e^{\frac{\tau+1}{2}m^3}.
$$

Then, substituting the bounds from (3), we obtain

$$
N^{\frac{1}{6}m^3\cdot(\alpha+\delta-n)} N^{\frac{\tau^2}{6}m^3\cdot(\beta+\frac{n}{2})} N^{\frac{2\tau+1}{6}m^3\cdot(\alpha+\beta+\delta-\frac{n}{2})} N^{\frac{\tau+2}{6}m^3\cdot\alpha} < N^{\frac{\tau+1}{2}m^3\cdot\alpha}.
$$

Taking the logarithm and simplifying, we get

$$
\alpha + \delta - n + \tau^2\left(\beta + \frac{n}{2}\right) + (2\tau+1)\left(\alpha + \beta + \delta - \frac{n}{2}\right) + (\tau+2)\alpha < 3(\tau+1)\alpha,
$$

which leads to

$$(2\beta + n)\tau^2 + (4\beta + 4\delta - 2n)\tau + 2\alpha + 2\beta + 4\delta - 3n < 0.$$

This quadratic expression in τ on the left side can be minimized at

$$\tau_0 = \frac{n - 2\beta - 2\delta}{2\beta + n}.$$

Substituting this value into the inequality yields

$$-2\delta^2 + 4n\delta + 2\alpha\beta + n\alpha - 2n^2 < 0.$$

This is a quadratic inequality in δ, which holds if δ is less than the smallest root, leading to the condition

$$\delta < n - \sqrt{\frac{\alpha(2\beta + n)}{2}}.$$

Furthermore, the optimization requires $\tau_0 > 0$, which implies $n - 2\beta - 2\delta > 0$, or $\delta < n/2 - \beta$. The condition $\alpha > n/2 + \beta$ given in the theorem ensures that

$$\delta < \min\left\{ n - \sqrt{\frac{\alpha(2\beta + n)}{2}},\ \frac{n}{2} - \beta \right\} = n - \sqrt{\frac{\alpha(2\beta + n)}{2}}.$$

Under this condition on δ, the LLL algorithm will produce sufficiently short vectors corresponding to at least three algebraically independent polynomials that hold over the integers. Using resultants or Gröbner basis computations, one can solve for the integer root $(x_0, y_0) = (v, -(aq^n + bp^n - ab))$. Let $M = -y_0 = aq^n + bp^n - ab$. Using Lemma 1 with $a, b < N^{n/6}/2$, one computes

$$S = M + \left\lfloor \frac{M^2}{4N^n} \right\rfloor = aq^n + bp^n$$

and

$$D = \sqrt{S^2 - 4N^n \left\lfloor \frac{M^2}{4N^n} \right\rfloor} = |aq^n - bp^n|.$$

This allows one to recover $S = aq^n + bp^n$ and $D = |aq^n - bp^n|$. From these two values, one can determine $2aq^n$ and $2bp^n$ and compute prime factors using greatest common divisors with N through $\gcd(N, S + D)$ and $\gcd(N, S - D)$. This finally reveals the prime factors

$$p = \max\left\{\gcd(N, S + D),\ \gcd(N, S - D)\right\},$$

and

$$q = \min\left\{\gcd(N, S + D),\ \gcd(N, S - D)\right\},$$

thus factoring $N = pq$. This completes the proof. □

Algorithm 1 Factoring Algorithm Based on the Generalized Attack

Input: An RSA modulus N, a public exponent e, an integer n, and reals α, β, δ.
Output: The factorization of $N = pq$ with its prime factors p and q.

1: Define a modular polynomial $f(x, y)$ with unknown variables x, y:

$$f(x, y) = x(N^n + y) + 1 \pmod{e}.$$

2: Let $z = xy + 1$ and define a linear polynomial $g(x, z)$ with unknown variables x, z:

$$g(x, z) = N^n x + z \pmod{e}.$$

3: Set the estimated bounds X, Y, Z on unknown variables x, y, z:

$$X = \left\lfloor N^{\alpha+\delta-n} \right\rfloor, \ Y = \left\lfloor 2^{1+\frac{n}{2}} N^{\beta+\frac{n}{2}} \right\rfloor, \ Z = XY + 1.$$

4: Choose a suitable integer m and compute the relevant optimized integer t:

$$t = \left\lceil \frac{n - 2\beta - 2\delta}{2\beta + n} \cdot m \right\rceil$$

5: Extract root $y_0 = -(aq^n + bp^n - ab)$ using Coppersmith's method via Theorem 3.
6: Let $M = -y_0$ and compute S (i.e., $aq^n + bp^n$) and D (i.e., $|aq^n - bp^n|$):

$$S = M + \left\lfloor \frac{M^2}{4N^n} \right\rfloor, \ D = \sqrt{S^2 - 4N^n \left\lfloor \frac{M^2}{4N^n} \right\rfloor}$$

7: Compute $\gcd(N, S + D)$, $\gcd(N, S - D)$ and return the factorization of $N = pq$:

$$\{p, \ q\} = \{\gcd(N, S + D), \ \gcd(N, S - D)\}$$

For completeness, we present the following algorithm that outputs the prime factors of a given RSA modulus satisfying Theorem 3.

We briefly describe the post-factorization parameter recovery of u, a, b. Once the modulus N is factored into p and q, the parameters a and b can be efficiently recovered to run the decryption algorithm. Recall that $S = aq^n + bp^n$ and $D = |aq^n - bp^n|$ are recovered using Algorithm 1. Then, aq^n and bp^n can be easily determined. Since p, q are known, we compute p^n and q^n. With aq^n and bp^n known, we can efficiently derive values for a, b using divisions. Finally, we can recover $u = e^{-1} \bmod (p^n - a)(q^n - b)$.

4 Comparison and Discussion

In this section, we compare the generalized attack with several existing methods that target the standard RSA key equation or its variants (see Table 2). We demonstrate that our result covers previous bounds as special cases. Furthermore, we visualize the attack bounds and provide a detailed numerical example to illustrate the practical application of the generalized attack.

Table 2. Comparison of attacks on RSA and its variants with $e = N^\alpha$, $a, b \leq N^\beta$.

Attack	Target Equation	Attack Condition	Parameters (n, α, β)
Wiener [26]	$ed \equiv 1 \pmod{\phi(N)}$	$d < \frac{1}{3}N^{0.25}$	$(1, 1, 0)$
Boneh-Durfee [2]	$ed \equiv 1 \pmod{\phi(N)}$	$d < N^{0.292}$	$(1, 1, 0)$
Peng et al. [21] Zheng et al. [28]	$ed \equiv 1 \pmod{\psi_2(N)}$	$d < N^{2-\sqrt{\alpha}}$	$(2, \alpha, 0)$
Teleşeanu [25]	$ed \equiv 1 \pmod{\psi_n(N)}$	$d < N^{n-\sqrt{\alpha n/2}}$	$(n, \alpha, 0)$
This Work	$eu \equiv 1 \pmod{\psi_n(N, a, b)}$	$u < N^{n-\sqrt{\alpha(2\beta+n)/2}}$	(n, α, β)

4.1 Comparison with Existing Attacks

Comparison with Boneh-Durfee Attack. A landmark attack on RSA with small private exponents is the one by Boneh and Durfee [2]. It exploits the key equation $ed \equiv 1 \pmod{(p-1)(q-1)}$, where $d < N^{\delta_0}$ is the private exponent. For a public exponent of full-size $e \approx N$ (i.e., $\alpha = 1$), the attack is effective for $\delta_0 < 1 - \sqrt{2}/2 \approx 0.292$.

This bound can be retrieved as a special case of our result in Theorem 3. By setting the parameters to match standard RSA (i.e., $n = 1$, $a = b = 1$, which implies $\beta = 0$) and assuming a full-size public exponent (i.e., $\alpha = 1$), the bound

from (2) becomes

$$\delta < n - \sqrt{\frac{\alpha(2\beta + n)}{2}} = 1 - \sqrt{\frac{1}{2}} = 1 - \frac{\sqrt{2}}{2}.$$

This exactly matches the Boneh-Durfee bound.

Discussion on Standard RSA with Implicit Perturbation ($n = 1, \beta > 0$). Our framework extends to standard RSA where the prime factors satisfy a perturbed relation $eu \equiv 1 \pmod{(p-a)(q-b)}$ with $a, b \approx N^{\beta} > 1$. This corresponds to RSA with shifted primes. Our bound becomes $\delta < 1 - \sqrt{\alpha/2 + \alpha\beta}$. As the perturbation size β increases, the attack range for d decreases continuously.

Comparison with Attacks on RSA Variants ($n = 2$). In [21,28], Peng et al. and Zheng et al. proposed methods to attack RSA variants where the key equation is $ed \equiv 1 \pmod{\left(p^2 - 1\right)\left(q^2 - 1\right)}$. Both works showed that their attacks can factor the modulus $N = pq$ if $e = N^{\alpha}$ and the private key $d < N^{\delta_0}$ satisfies $\delta_0 < 2 - \sqrt{\alpha}$.

Our generalized result also covers this bound. By setting $n = 2$ and $a = b = 1$ (implying $\beta = 0$), the bound from Theorem 3 becomes

$$\delta < n - \sqrt{\frac{\alpha(2\beta + n)}{2}} = 2 - \sqrt{\frac{2\alpha}{2}} = 2 - \sqrt{\alpha}.$$

This exactly matches the bound reported in [21,28].

Comparison with Teleşeanu's Attack. Recently, Teleşeanu [25] presented an attack on RSA-like schemes with a key equation of the form

$$ed \equiv 1 \pmod{\left(p^n - 1\right)\left(q^n - 1\right)}$$

for $n \geq 2$. The attack succeeds if $d < N^{\delta_0}$ with $\delta_0 < n - \sqrt{\alpha n/2}$, for a public exponent $e = N^{\alpha}$ in a certain range.

Once again, our generalized attack retrieves this bound. Setting $a = b = 1$ (which means $\beta = 0$), the condition from Theorem 3 gives

$$\delta < n - \sqrt{\frac{\alpha(2\beta + n)}{2}} = n - \sqrt{\frac{\alpha n}{2}}.$$

matching the bound from [25].

4.2 Visualizing the Attack Surface

To highlight the improvement of our method, we further visualize the attack bounds. Figure 1 plots the attack threshold δ as a function of the public exponent size α and a structural parameter β for the case $n = 2$. The solid line represents the bound for previous attacks on the $\psi_2(N)$ variant (i.e., $\delta < 2 - \sqrt{\alpha}$), which

assumes $a = b = 1$ (i.e., $\beta = 0$). The dashed lines represent the bounds on our parameter u for different choices of $\beta > 0$.

While the bound on u becomes stricter as β grows, our attack opens up a new multi-dimensional surface of vulnerability. An adversary is no longer limited to attacking a single line (i.e., $\beta = 0$), but can now search for weaknesses across the entire area under the curves. Any public key (N, e) is vulnerable if it satisfies our generalized relation for *any* combination of small (δ, β) that falls below the corresponding curve.

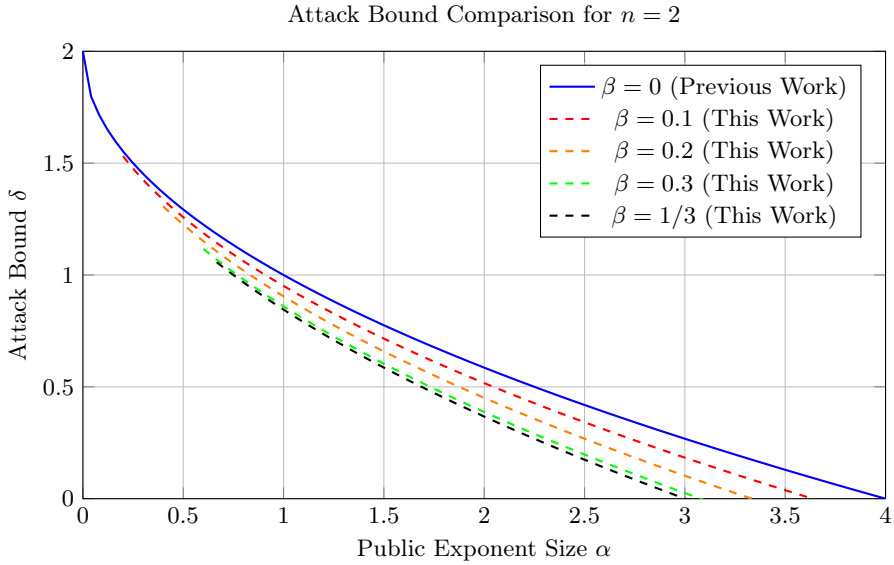


Fig. 1. Comparison of the attack bound δ as a function of α, β for $n = 2$. The curves represent the security threshold for different parameters β. The area *below* each curve indicates the *Insecure Region* corresponding to that β. Note that our framework reveals a multi-dimensional attack surface (parameterized by $\beta > 0$), whereas previous attacks are restricted to the single curve where $\beta = 0$ (i.e., $a = b = 1$).

4.3 A Numerical Example

We show a detailed numerical example below to illustrate the practical application of our generalized attack. Consider an attack scenario with parameters $n = 2$, a 200-bit modulus N, and a 400-bit public exponent e. Suppose we are given the following known values.

$$N = 1223852682569144461759988126766200863829976896432051027669117,$$
$$e = 3215127331379995171260794981442320178984588355909234391254 46\backslash$$

$$209176245589781982713585429478802913290977733402324388498259.$$

Here, $e = N^{\alpha}$ with $\alpha \approx 1.9888$. The standard attacks mentioned above are ineffective, as we will show later. To apply our method as described in Algorithm 1, we take attack parameters $\delta = 0.35$ and $\beta = 0.25$, which satisfy the condition $\delta < n - \sqrt{\alpha(2\beta + n)/2} \approx 0.423$. The estimated bounds for the factoring algorithm are

$$\begin{aligned}
X &= \left\lfloor N^{\alpha+\delta-n} \right\rfloor = 230425029816594033263,\\
Y &= \left\lfloor 2^{1+\frac{n}{2}} N^{\beta+\frac{n}{2}} \right\rfloor\\
&= 514898256753110504766215294701696155526633164678617068924491\backslash\\
&\quad 6943569617861620,\\
Z &= XY + 1\\
&= 118645446164847778103070031409659415386669175332066817546790\backslash\\
&\quad 5809686279902253667309027921211066061.
\end{aligned}$$

We construct the lattice $\mathcal{L}$ as described in Section 3 with parameters $m = 5$ and $t = 1$, resulting in a lattice of dimension $\omega = 22$. After applying the LLL algorithm and extracting the integer root $(x_0, y_0) = (v, -(aq^n - bp^n + ab))$ of the resulting polynomial system, we obtain

$$\begin{aligned}
x_0 &= 5456620570385672808910,\\
y_0 &= -171810640254871482249218003757737130702123357988858634565108\backslash\\
&\quad 06276539393443929.
\end{aligned}$$

Setting $M = -y_0$ and applying Lemma 1, we obtain

$$\begin{aligned}
S &= M + \left\lfloor \frac{M^2}{4N^n} \right\rfloor\\
&= 171810640254871482249218003757737130702123358481557807120603\backslash\\
&\quad 23650505499574146,\\
D &= \sqrt{S^2 - 4N^n \left\lfloor \frac{M^2}{4N^n} \right\rfloor}\\
&= 881198282453531512973346249225950699540463763905045143868792.
\end{aligned}$$

From S and D, we can find the prime factors of N by computing

$$\begin{aligned}
p &= \gcd(N, S - D) = 126737023755379813131313152809849,\\
q &= \gcd(N, S + D) = 96566310798914716590235592093 3.
\end{aligned}$$

The product of p and q correctly yields the original modulus N.

Moreover, u, a, b can be efficiently computed as well. We first obtain aq^n and bp^n using S and D.

$$aq^n = \frac{S + D}{2}$$

$$= 859053201274357455306004141465261302177929253705324012626204\backslash$$
$$3777775321721469,$$
$$bp^n = \frac{S-D}{2}$$
$$= 859053201274357367186175896112110004843304331110254058579827\backslash$$
$$9872730177852677.$$

With p and q known for $n = 2$, we compute

$$a = \frac{aq^2}{q^2} = 9212315021370821, \quad b = \frac{bp^2}{p^2} = 5348266656237077.$$

Finally, u can be computed as

$$u = e^{-1} \bmod (p^2 - a)(q^2 - b) = 25420487022328541540539.$$

With p and q known, we can analyze why previous attacks in [2,21,25,28] would fail. The standard RSA private exponent d_1 under the standard RSA key equation $ed_1 \equiv 1 \pmod{(p-1)(q-1)}$ corresponding to e is

$$d_1 = 247546520703218464660341133806246364106550753212697462817211.$$

Therefore, we know

$$d_1 \approx N^{0.988}, \text{ and } 0.988 \gg 1 - \frac{\sqrt{2}}{2} \approx 0.292.$$

This value is far too large for the Boneh-Durfee attack.

Similarly, for the RSA variant with $n = 2$, the corresponding private exponent d_2 in the equation $ed_2 \equiv 1 \pmod{\left(p^2-1\right)\left(q^2-1\right)}$ is

$$d_2 = 250148675052854853529770371485147567517341585024696444533613\backslash$$
$$023787882623696448783275637234294751010323656907973776011739.$$

Therefore, we know

$$d_2 \approx N^{1.987}, \text{ and } 1.987 \gg 2 - \sqrt{\alpha} \approx 0.589.$$

This value is much larger than the bound required by the attacks in [21,25,28]. This numerical example demonstrates that our generalized attack can succeed even when the private exponents for RSA key equations are large.

4.4 Estimating the Number of Weak Exponents

Our generalized attack significantly increases the set of public exponents that can be considered weak. In standard attacks, a public exponent e is deemed vulnerable only if its corresponding private exponent d is small. In our method,

however, e is vulnerable if there exists a certain set of small parameters (u, a, b) that satisfies the generalized key equation $eu \equiv 1 \pmod{\psi_n(N, a, b)}$.

It is important to distinguish between targeted variants and standard RSA instances. For a cryptosystem explicitly designed with parameters satisfying $\psi_n(N, a, b)$ for specific $a, b > 1$, our attack is deterministic. However, for a standard RSA key generated with random primes, the probability that there exist small a, b satisfying the relation is determined by the density of such algebraic structures. While this probability may be low for random keys, our analysis proves that the class of weak keys is larger than previously understood.

A heuristic estimate can quantify this increase. For a full-size public exponent $e \approx N^n$ (i.e., $\alpha = n$), the number of standard weak exponents is determined by the number of private exponents d that fall below the attack bound [25]. This quantity is on the order of $\mathcal{O}(N^{(1-\sqrt{2}/2)n-\epsilon})$. To formalize this, we analyze such a full-size case when the corresponding private exponent d in the equation $ed \equiv 1 \pmod{(p^n - 1)(q^n - 1)}$ satisfies $d < N^{(1-\sqrt{2}/2)n}$. The number of such weak exponents corresponds to the cardinality of the set

$$\mathcal{D}_n = \left\{ d \;\mid\; d < N^{(1-\frac{\sqrt{2}}{2})n} \text{ and } \gcd\left(d, (p^n - 1)(q^n - 1)\right) = 1 \right\}.$$

Thus, the cardinality of $\mathcal{D}_n$ can be approximated by considering the density of integers that are coprime to $\psi_n(N)$. We have $|\mathcal{D}_n| \approx \rho \cdot N^{(1-\sqrt{2}/2)n}$, where the density ratio $\rho = \varphi(\psi_n(N))/\psi_n(N)$ is a value bounded between two positive constants for sufficiently large N. As a consequence, the number of weak exponents is extremely close to $N^{(1-\sqrt{2}/2)n}$, which can be written as $\mathcal{O}(N^{(1-\sqrt{2}/2)n-\epsilon})$, that is $\mathcal{O}(N^{0.292n-\epsilon})$.

Moreover, our approach introduces new parameters $a, b < N^{n/6}/2$. The availability of approximately $N^{n/6}/2$ choices for parameter a (and b of nearly the same size) can be viewed as expanding the dimensions of vulnerability. This leads to a simplified estimate for the number of weak instances on the order of

$$\mathcal{O}\left(N^{\frac{n}{6}}\right) \cdot \mathcal{O}\left(N^{n-\sqrt{\frac{(2\cdot\frac{n}{6}+n)\cdot n}{2}}-\epsilon}\right) = \mathcal{O}\left(N^{\frac{n}{6}} \cdot N^{(1-\frac{\sqrt{6}}{3})n-\epsilon}\right) = \mathcal{O}\left(N^{(\frac{7}{6}-\frac{\sqrt{6}}{3})n-\epsilon}\right),$$

that is $\mathcal{O}\left(N^{0.350n-\epsilon}\right)$. This leads to a considerable increase $\mathcal{O}(N^{0.350n-0.292n}) \approx \mathcal{O}(N^{0.057n})$ in the number of potentially weak exponents compared to previous attacks.

Remark 2. The attack strategy is not restricted to the integer n and can be mounted for any integer r such that $1 \leq r \leq n$. This means that a public exponent e is vulnerable if a relation of $eu \equiv 1 \pmod{(p^r - a)(q^r - b)}$ exists for *any* such r with small parameters.

A common critique regarding small exponent attacks is the perceived sparsity of weak keys. Indeed, for a randomly chosen modulus N, the probability that the private exponent d falls below the Boneh-Durfee bound is low. However, this observation presents a narrow view, limited of the vulnerability space.

Our generalized framework reveals that such scarcity of weak keys is an artifact of fixing the structural parameters to unity. By introducing the generalized attack along with a unified bound, we define a continuous *Security Polytope* in the parameter space $(n, \alpha, \beta, \delta)$. Within this polytope:

- While standard weak keys may be rare, the universe of RSA variants (characterized by $\beta > 0$) is vast. Our result demonstrates that as the structural complexity of a variant increases with various a, b, the secure region for the private exponent δ shrinks. This implies that many RSA variants proposed in the literature might be inherently more fragile than standard RSA.
- If a protocol designer chooses parameters that satisfy a perturbed key equation (e.g., to enable faster decryption or other properties), they essentially move the cryptosystem along the β-axis of our polytope. Our analysis serves as a rigorous impossibility result: it quantifies exactly how much algebraic structure can be added before the system becomes insecure, regardless of the randomness of d.

4.5 Further Generalization for Intermediate Powers

The attack presented in Theorem 3 can be generalized for any intermediate power r where $1 \leq r \leq n$. This significantly broadens the applicability of the attack, as a single public key must be secure against a family of potential congruences.

Corollary 1. *Let $N = pq$ be an RSA modulus using the variant Euler function $\psi_n(N, 1, 1)$ with $q < p < 2q$. Let $1 \leq r \leq n-1$ be a positive integer. Suppose that a, b are two unknown positive integers such that $a, b \leq N^\beta$ for some $\beta < r/6 - \log_N 2$, and a, b also satisfy $|aq^r - bp^r| < 2N^{r/2}$. Suppose that $e = N^\alpha$ is a public exponent satisfying the equation $eu \equiv 1 \pmod{(p^r - a)(q^r - b)}$ with an unknown $u < N^\delta$. If $\alpha > r/2 + \beta$, and*

$$\delta < r - \sqrt{\frac{\alpha(2\beta + r)}{2}},$$

then N can be factored in polynomial time.

Proof. The proof follows directly from the proof of Theorem 3 by substituting n with r. □

This corollary implies that the total number of weak instances for an RSA variant based on $\psi_n(N, 1, 1)$ is not just the number of vulnerable exponents related to $(p^n - 1)(q^n - 1)$, but the union of vulnerable exponents across all intermediate structures $(p^r - a)(q^r - b)$ defined by $r = 1, 2, \ldots, n-1$ and potential a, b.

Moreover, a direct consequence of this corollary is that one can test for vulnerabilities related to the simpler structure $\psi_r(N, 1, 1) = (p^r - 1)(q^r - 1)$ for $r = 1$ and 2.

Corollary 2. *Let $N = pq$ be an RSA modulus using the variant Euler function $\psi_n(N, 1, 1)$ with $q < p < 2q$. Let $r = 1, 2$ and suppose given a public exponent $e = N^\alpha$ satisfying the equation $eu \equiv 1 \pmod{(p^r - 1)(q^r - 1)}$ with an unknown $u < N^\delta$. If $\alpha > r/2$, and*

$$\delta < r - \sqrt{\frac{\alpha r}{2}},$$

then N can be factored in polynomial time.

Proof. This is a direct application of Corollary 1 with parameters $a = b = 1$, which implies $\beta = 0$. Note that $|aq^r - bp^r| < 2N^{r/2}$, i.e., $p^r - q^r < 2p^{r/2}q^{r/2}$ must be ensured. Therefore, we have

$$\left(\frac{p}{q}\right)^r - 1 < 2\left(\frac{p}{q}\right)^{\frac{r}{2}},$$

which leads to

$$\left(\frac{p}{q}\right)^r - 2\left(\frac{p}{q}\right)^{\frac{r}{2}} - 1 < 0.$$

Focusing on the resulting quadratic inequality with respect to $(p/q)^{r/2}$, we have

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

Note that p and q are positive primes; we shall ensure that

$$0 < \left(\frac{p}{q}\right)^{\frac{r}{2}} < 1 + \sqrt{2}.$$

Since we have $q < p < 2q$, i.e., $1 < p/q < 2$, it follows that $r = 1$ or $r = 2$ will fulfill the required constraint. To be specific, we obtain $1 < (p/q)^{1/2} < \sqrt{2}$ for $r = 1$, which falls within the above interval. For $r = 2$, we obtain $1 < (p/q)^{2/2} < 2$, which still falls within the above interval. The existence of such a relation for $r = 1, 2$ is sufficient for the generalized attack to succeed, which covers the previous attacks [2,21,28]. □

5 Conclusion

We introduced a generalized attack framework on RSA and its variants in this research. The attack is based on the new key equation $eu \equiv 1 \pmod{\psi_n(N, a, b)}$, where $\psi_n(N, a, b) = (p^n - a)(q^n - b)$ for an RSA modulus $N = pq$ and $n \geq 1$ with small unknown integers a and b. We demonstrated that if this equation holds for a sufficiently small parameter u, the modulus N can be efficiently factored (subject to a standard assumption within Coppersmith's method).

This result significantly expands the class of weak exponents beyond those covered by former small private exponent attacks. It also subsumes previous cryptanalytic work as special cases, since our attack bounds reduce to the well-known bounds of earlier methods when setting $a = b = 1$. Our findings suggest that the security of RSA-like cryptosystems relies on more complex algebraic relationships than previously considered.

Acknowledgments. The authors would like to thank the anonymous reviewers for their detailed comments and impressive suggestions, which improved this paper in terms of both technical and editorial quality. Mengce Zheng gratefully acknowledges the financial support for academic visiting provided by the China Scholarship Council (CSC No. 202308330390). This work was partially supported by the National Natural Science Foundation of China (No. 62002335), and Ningbo Young Science and Technology Talent Cultivation Program (No. 2023QL007).

Disclosure of Interests. The authors have no competing interests.

References

1. Boneh, D.: Twenty years of attacks on the RSA cryptosystem. Notices of the AMS **46**(2), 203–213 (1999)
2. Boneh, D., Durfee, G.: Cryptanalysis of RSA with private key d less than $N^{0.292}$. In: Stern, J. (ed.) Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2-6, 1999, Proceeding. Lecture Notes in Computer Science, vol. 1592, pp. 1–11. Springer (1999). https://doi.org/10.1007/3-540-48910-X_1
3. Boudabra, M., Nitaj, A.: A new public key cryptosystem based on Edwards curves. J. Appl. Math. Comput. **61**(1-2), 431–450 (2019). https://doi.org/10.1007/S12190-019-01257-Y
4. Bunder, M.W., Nitaj, A., Susilo, W., Tonien, J.: A new attack on three variants of the RSA cryptosystem. In: Liu, J.K., Steinfeld, R. (eds.) Information Security and Privacy - 21st Australasian Conference, ACISP 2016, Melbourne, VIC, Australia, July 4-6, 2016, Proceedings, Part II. Lecture Notes in Computer Science, vol. 9723, pp. 258–268. Springer (2016). https://doi.org/10.1007/978-3-319-40367-0_16
5. Castagnos, G.: An efficient probabilistic public-key cryptosystem over quadratic fields quotients. Finite Fields Their Appl. **13**(3), 563–576 (2007). https://doi.org/10.1016/J.FFA.2006.05.004
6. Coppersmith, D.: Small solutions to polynomial equations, and low exponent RSA vulnerabilities. J. Cryptol. **10**(4), 233–260 (1997). https://doi.org/10.1007/s001459900030
7. Cotan, P., Teşeleanu, G.: Small private key attack against a family of RSA-like cryptosystems. In: Fritsch, L., Hassan, I., Paintsil, E. (eds.) Secure IT Systems - 28th Nordic Conference, NordSec 2023, Oslo, Norway, November 16-17, 2023, Proceedings. Lecture Notes in Computer Science, vol. 14324, pp. 57–72. Springer (2023). https://doi.org/10.1007/978-3-031-47748-5_4
8. Elkamchouchi, H., Elshenawy, K., Shaban, H.: Extended RSA cryptosystem and digital signature schemes in the domain of Gaussian integers. In: The 8th International Conference on Communication Systems, 2002. ICCS 2002. vol. 1, pp. 91–95. IEEE (2002)
9. Herrmann, M., May, A.: Maximizing small root bounds by linearization and applications to small secret exponent RSA. In: Nguyen, P.Q., Pointcheval, D. (eds.) Public Key Cryptography - PKC 2010, 13th International Conference on Practice and Theory in Public Key Cryptography, Paris, France, May 26-28, 2010. Proceedings. Lecture Notes in Computer Science, vol. 6056, pp. 53–69. Springer (2010). https://doi.org/10.1007/978-3-642-13013-7_4
10. Hinek, M.J.: Cryptanalysis of RSA and its variants. CRC press (2009)

11. Howgrave-Graham, N.: Finding small roots of univariate modular equations revisited. In: Darnell, M. (ed.) Cryptography and Coding, 6th IMA International Conference, Cirencester, UK, December 17-19, 1997, Proceedings. Lecture Notes in Computer Science, vol. 1355, pp. 131–142. Springer (1997). https://doi.org/10.1007/BFb0024458
12. Jochemsz, E., May, A.: A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants. In: Lai, X., Chen, K. (eds.) Advances in Cryptology - ASIACRYPT 2006, 12th International Conference on the Theory and Application of Cryptology and Information Security, Shanghai, China, December 3-7, 2006, Proceedings. Lecture Notes in Computer Science, vol. 4284, pp. 267–282. Springer (2006). https://doi.org/10.1007/11935230_18
13. Koyama, K., Maurer, U.M., Okamoto, T., Vanstone, S.A.: New public-key schemes based on elliptic curves over the ring $\mathbb{Z}_n$. In: Feigenbaum, J. (ed.) Advances in Cryptology - CRYPTO '91, 11th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1991, Proceedings. Lecture Notes in Computer Science, vol. 576, pp. 252–266. Springer (1991). https://doi.org/10.1007/3-540-46766-1_20
14. Kuwakado, H., Koyama, K., Tsuruoka, Y.: New RSA-type scheme based on singular cubic curves $y^2 \equiv x^3 + bx^2 \pmod{n}$. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences **E78-A**(1), 27–33 (1995)
15. Lenstra, A., Lenstra, H., Lovász, L.: Factoring polynomials with rational coefficients. Mathematische Annalen **261**(4), 515–534 (1982)
16. May, A.: New RSA vulnerabilities using lattice reduction methods. Ph.D. thesis, University of Paderborn (2003)
17. May, A.: Using LLL-reduction for solving RSA and factorization problems. In: Nguyen, P.Q., Vallée, B. (eds.) The LLL Algorithm - Survey and Applications, pp. 315–348. Information Security and Cryptography, Springer (2010). https://doi.org/10.1007/978-3-642-02295-1_10
18. Murru, N., Saettone, F.: A novel RSA-like cryptosystem based on a generalization of the Rédei rational functions. In: Kaczorowski, J., Pieprzyk, J., Pomykała, J. (eds.) Number-Theoretic Methods in Cryptology, NuTMiC 2017. Lecture Notes in Computer Science, vol. 10737, pp. 91–103. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-76620-1_6
19. Nasrutdinov, M., Tronin, S.: RSA cryptosystem for rings with commuting ideals. Lobachevskii Journal of Mathematics **43**(12), 3591–3596 (2022)
20. Nitaj, A.: Another generalization of Wiener's attack on RSA. In: Vaudenay, S. (ed.) Progress in Cryptology - AFRICACRYPT 2008, First International Conference on Cryptology in Africa, Casablanca, Morocco, June 11-14, 2008. Proceedings. Lecture Notes in Computer Science, vol. 5023, pp. 174–190. Springer (2008). https://doi.org/10.1007/978-3-540-68164-9_12
21. Peng, L., Hu, L., Lu, Y., Wei, H.: An improved analysis on three variants of the RSA cryptosystem. In: Chen, K., Lin, D., Yung, M. (eds.) Information Security and Cryptology - 12th International Conference, Inscrypt 2016, Beijing, China, November 4-6, 2016, Revised Selected Papers. Lecture Notes in Computer Science, vol. 10143, pp. 140–149. Springer (2016). https://doi.org/10.1007/978-3-319-54705-3_9
22. Rivest, R., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **21**(2), 120–126 (1978). https://doi.org/10.1145/359340.359342

23. Seck, M., Nitaj, A.: A new public key cryptosystem based on the cubic Pell curve. In: Dabrowski, A., Pieprzyk, J., Pomykala, J. (eds.) Number-Theoretic Methods in Cryptology - 4th International Conference, NuTMiC 2024, Szczecin, Poland, June 24-26, 2024, Revised Selected Papers. Lecture Notes in Computer Science, vol. 14966, pp. 239–261. Springer (2024). https://doi.org/10.1007/978-3-031-82380-0_8
24. Takagi, T., Naito, S.: Construction of RSA cryptosystem over the algebraic field using ideal theory and investigation of its security. Electronics and Communications in Japan (Part III: Fundamental Electronic Science) **83**(8), 19–29 (2000)
25. Teşeleanu, G.: A lattice attack against a family of RSA-like cryptosystems. In: Dolev, S., Elhadad, M., Kutylowski, M., Persiano, G. (eds.) Cyber Security, Cryptology, and Machine Learning - 8th International Symposium, CSCML 2024, Be'er Sheva, Israel, December 19-20, 2024, Proceedings. Lecture Notes in Computer Science, vol. 15349, pp. 343–355. Springer (2024). https://doi.org/10.1007/978-3-031-76934-4_25
26. Wiener, M.: Cryptanalysis of short RSA secret exponents. IEEE Trans. Inf. Theory **36**(3), 553–558 (1990). https://doi.org/10.1109/18.54902
27. Zheng, M., Kang, H.: Lattice-based cryptanalysis of RSA-type cryptosystems: a bibliometric analysis. Cybersecur. **7**(1), 74 (2024). https://doi.org/10.1186/s42400-024-00289-7
28. Zheng, M., Kunihiro, N., Hu, H.: Cryptanalysis of RSA variants with modified Euler quotient. In: Joux, A., Nitaj, A., Rachidi, T. (eds.) Progress in Cryptology - AFRICACRYPT 2018 - 10th International Conference on Cryptology in Africa, Marrakesh, Morocco, May 7-9, 2018, Proceedings. Lecture Notes in Computer Science, vol. 10831, pp. 266–281. Springer (2018). https://doi.org/10.1007/978-3-319-89339-6_15
29. Zheng, Z., Liu, F.: On the high dimensional RSA algorithm - A public key cryptosystem based on lattice and algebraic number theory. CoRR **abs/2202.02675** (2022), https://arxiv.org/abs/2202.02675