

Article

New Cryptanalysis of Two Families of RSA-like Schemes

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

¹ Department of Mathematics, Sciences Faculty, ACSA Laboratory, Mohammed First University, Oujda 60000, Morocco; brahim.chnioune.d24@ump.ac.ma (B.C.); mohammed.rahmani@ump.ac.ma (M.R.); m.ziane@ump.ac.ma (M.Z.)

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

* Correspondence: abderrahmane.nitaj@unicaen.fr

Abstract

In certain variants of the RSA cryptosystem with a modulus $N = pq$, the public exponent e and the private exponent d are related by the equation $ed \equiv 1 \pmod{\varphi_n(N)}$ or $ed \equiv 1 \pmod{\psi_n(N)}$, where $\varphi_n(N) = (p^n - 1)(q^n - 1)$ and $\psi_n(N) = \frac{(p^n - 1)(q^n - 1)}{(p - 1)(q - 1)}$ are defined for a positive integer $n \geq 1$. In this paper, we introduce a new attack against the RSA variants when two public exponents e_1 and e_2 are given, satisfying $e_i d_i \equiv 1 \pmod{\varphi_n(N)}$ or $e_i d_i \equiv 1 \pmod{\psi_n(N)}$ for $i = 1, 2$. Specifically, we show that when the prime factors of N share an amount of their least significant bits, and d_1 and d_2 share an amount of their most significant bits, the factorization of N can be computed in polynomial time. Our method is based on an extension of Coppersmith's technique and lattice basis reduction and achieves improved bounds as the number of shared bits increases. The proposed attacks are heuristic in nature, relying on the standard assumption that the polynomials obtained after lattice reduction are algebraically independent.

Keywords: RSA; RSA-like schemes; Integer factorization; Lattice-based cryptanalysis

MSC: 94A60

1. Introduction

The security of many public key encryption schemes can be regarded as the challenge of solving modular polynomial equations. In particular, the RSA cryptosystem [1] has long attracted extensive cryptanalytic attention. A natural point of departure is the fundamental relation linking the RSA keys, $ed - k\varphi(N) = 1$, which captures the core algebraic structure underlying the system, where $\varphi(N)$ denotes Euler's totient function. This relation can be transformed, in several ways, into modular polynomial equations whose small roots correspond directly to secret information. Consequently, identifying these roots often leads to a full cryptanalytic break. This perspective forms the basis of numerous attacks exploiting lattice reduction, Coppersmith-type methods, and algebraic techniques.

In a landmark contribution, Coppersmith [2] developed two influential lattice-based approaches: one for determining solutions to modular equations of the form $P(x) \equiv 0 \pmod{N}$ without requiring the factorization of N , and another for locating small roots to bivariate polynomial equations $Q(x, y) = 0$. Since then, these techniques have been extended and adapted in numerous directions, and now serve as essential components in modern cryptanalysis, particularly in the study of RSA and its various generalizations. In 1998, Boneh and Durfee [3] broadened Coppersmith's methodology by designing a highly effective attack on RSA instances with small secret exponents. Their idea was to rewrite



Academic Editor: Hashem Bordbar

Received: 7 June 2026

Revised: 16 July 2026

Accepted: 16 July 2026

Published: 19 July 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

the key relation $ed - k\varphi(N) = 1$ as the modular equation $f(x_1, x_2) = -Nx_1 + x_1x_2 - 1 \equiv 0 \pmod{e}$, and then apply Coppersmith's lattice techniques to recover the small solution $(x_1, x_2) = (k, p + q - 1)$. This led to an improvement over Wiener's bound [4], namely $d < 3N^{1/4}$, to the stronger bound $d < N^{0.292}$, which enables efficient factorization of N and contributes to the well-known class of attacks on RSA.

In 2010, Sarkar et al. [5] showed that RSA can be broken when two public keys (N, e_1) and (N, e_2) share the same modulus N and the public exponents are approximately of size N . More precisely, they proved that if the corresponding private exponents $d_1, d_2 < N^\delta$ share a certain number of their most significant bits (MSBs), then RSA can be broken in polynomial time whenever $|d_1 - d_2| < N^\beta$ and $\delta < \frac{5}{8} - \frac{\beta}{2}$. Later, Nitaj et al. [6] improved this bound by showing that if additionally $e_1, e_2 \approx N^\alpha$ and the primes share ℓ of their least significant bits (LSBs) such that $2^\ell = N^\theta$, then the bound can be improved to

$$\delta < \frac{5}{2} - 2\theta - \beta - \frac{1}{4}\sqrt{6(1 - 4\theta)(5 + 4\alpha - 4\theta - 4\beta)}.$$

Other extended RSA-like schemes have also attracted the attention of cryptanalysts. In 2024, Nitaj et al. [7] cryptanalyzed schemes defined by the key equation $ed - k\psi_n(N) = 1$, where $\psi_n(N) = \frac{(p^n - 1)(q^n - 1)}{(p - 1)(q - 1)}$. They presented a small secret exponent attack showing that these schemes are vulnerable when $d < N^{0.292(n-1)}$. In the same year, Teşeleanu [8] showed that schemes defined by the equation $ed - k\varphi_n(N) = 1$ with $\varphi_n(N) = (p^n - 1)(q^n - 1)$ are vulnerable whenever $d < N^{0.292n}$. Further recent attacks on these schemes have been proposed in [9–11], all of which target a single weak public key (N, e) under various constraints.

In this work, we present new lattice-based attacks against RSA-like schemes involving two public keys (N, e_1) and (N, e_2) that share a common modulus N , with corresponding private keys (N, d_1) and (N, d_2) . Our attacks apply to moduli whose prime factors share an amount of their least significant bits, while the associated secret exponents d_1 and d_2 share another amount of their most significant bits.

Starting from the underlying key relations $e_id_i - k_i\psi_n(N) = 1$ or $e_id_i - k_i\varphi_n(N) = 1$, for $i = 1, 2$, we derive a multivariate polynomial $f_n(z_1, z_2, z_3, z_4)$ whose small integer roots are directly related to the secret parameters; by applying Coppersmith's framework for finding small solutions to multivariate polynomial equations, we are able to recover the private exponents and the prime factors of the modulus, namely (d_1, d_2, p, q) . More precisely, we show that when the RSA primes coincide on ℓ least significant bits, with $2^\ell = N^\theta$, and when the secret exponents satisfy $|d_1 - d_2| < N^\beta$ and $d_1, d_2 \leq N^\delta$, while the public exponents satisfy $e_1, e_2 \leq N^\alpha$, the RSA-like schemes defined by either of the equations $ed - k\psi_n(N) = 1$ or $ed - k\varphi_n(N) = 1$ can be efficiently broken.

In particular, we establish that the above schemes are vulnerable whenever the following bounds on δ hold:

$$\beta < \frac{5}{4}n + \alpha - n\theta, \quad \delta < \frac{5}{2}n - 2n\theta - \beta - \frac{1}{4}\sqrt{6n(4n\theta - 4\alpha + 4\beta - 5n)(4\theta - 1)},$$

for schemes based on $ed - k\varphi_n(N) = 1$, and

$$\beta < \frac{5}{4}(n - 1) + \alpha - \theta(n - 1),$$

$$\delta < \left(\frac{5}{2} - 2\theta\right)(n - 1) - \beta - \frac{1}{4}\sqrt{6(n - 1)(4(n - 1)\theta - 4\alpha + 4\beta - 5(n - 1))(4\theta - 1)}.$$

for schemes based on $ed - k\psi_n(N) = 1$, respectively.

As is customary in multivariate Coppersmith-type cryptanalysis, our attacks are heuristic rather than deterministic. In particular, they rely on the standard assumption that the polynomials obtained after the LLL reduction are algebraically independent.

The rest of this paper is organized as follows: In Section 2, we provide the essential background and review the key tools employed throughout the study. Section 3 details the adaptation of Coppersmith's method to the cryptanalysis of the proposed two families of RSA variants. Section 4 illustrates the attack with a comprehensive numerical example, while Section 5 concludes the paper.

2. Foundational Material

In this section, we present auxiliary lemmas that will be instrumental for establishing our main results. We also recall essential concepts, including lattice basis reduction techniques and the extended Coppersmith method. Finally, we describe in detail the two families of cryptographic schemes that are susceptible to our proposed cryptanalysis.

2.1. Technical Lemmas

The following theorem, originally established by Coppersmith [2], is a fundamental tool in the cryptanalysis of RSA and is widely employed for recovering the prime factors of an RSA modulus.

Lemma 1 (Coppersmith). *Let $N = pq$ be an RSA modulus satisfying $q < p < 2q$. If either the most significant half or the least significant half of the bits of one of the prime factors p or q is available, then the factorization of N can be computed in polynomial time.*

The following lemma (see [12]) establishes explicit upper and lower bounds on the prime factors of the RSA modulus $N = pq$, under the standard balanced-prime assumption $q < p < 2q$.

Lemma 2. *When the RSA modulus $N = pq$ is generated from primes of comparable size, namely $q < p < 2q$, the values of p and q are restricted to the interval given below:*

$$(2N)^{0.5} > p > N^{0.5} > q > \left(\frac{N}{2}\right)^{0.5}.$$

Notably, we have $p + q < (1 + \sqrt{2})N^{0.5}$.

When the difference between the primes takes the form $p - q = 2^\ell x$ for some integers x and $\ell > 0$, one can determine the ℓ LSBs of both p and q , and the 2ℓ LSBs of $p + q$. Under the same assumptions, we have the following result. A detailed proof can be found in Appendix B of [6].

Lemma 3. *Suppose that $p - q = 2^\ell x$, and let v_0 be a solution to*

$$y^2 - N \equiv 0 \pmod{2^\ell}.$$

Let

$$w_0 \equiv 2v_0 + (N - v_0^2)v_0^{-1} \pmod{2^{2\ell}}.$$

Then, there exist integers p_0, q_0 , and w such that the prime factors and their sum can be expressed as

$$p = 2^\ell p_0 + v_0, \quad q = 2^\ell q_0 + v_0, \quad p + q = 2^{2\ell} w + w_0.$$

Observe that when the prime factors p and q have ℓ identical least significant bits, these bits can be recovered directly by applying Lemma 3, without requiring any side-channel information.

An immediate consequence of Lemma 3 arises when $2^\ell = N^\theta$ with $\theta \geq \frac{1}{4}$. In this case, we have $\ell \geq \frac{1}{4} \log_2(N)$, indicating that at least one-half of the least significant bits of p are determined. By Coppersmith's result (Lemma 1), this amount of information is sufficient to recover the factorization of N in polynomial time. Therefore, throughout the remainder of this paper, we restrict our attention to the case $\theta < \frac{1}{4}$.

In [13,14], the extended totient functions are defined to be

$$\begin{aligned}\varphi_n(N) &= (p^n - 1)(q^n - 1), \quad n \geq 1, \\ \psi_n(N) &= \frac{(p^n - 1)(q^n - 1)}{(p - 1)(q - 1)}, \quad n \geq 2.\end{aligned}$$

The results below furnish estimate bounds for the maximum and minimum values of both $\varphi_n(N)$ and $\psi_n(N)$ [9,12].

Lemma 4. *The values of $\varphi_n(N)$ lie within the following range:*

$$\frac{N^n}{2} < \varphi_n(N) < N^n.$$

Lemma 5. *The function ψ_n takes values in the interval*

$$N^{n-1} < \psi_n(N) < 4N^{n-1}.$$

In connection with Lemma 3, the subsequent results detail recursive approaches for computing $\varphi_n(N)$ and $\psi_n(N)$ as functions in w [7,9].

Lemma 6. *Let $N = pq$ with $p + q = 2^{2\ell}w + w_0$. The function $\varphi_n(N)$ satisfies*

1. $\varphi_1(N) = -2^{2\ell}w - w_0 + N + 1$.
2. $\varphi_2(N) = -2^{4\ell}w^2 - 2^{2\ell+1}w_0w - w_0^2 + (N + 1)^2$.
3. *For any $n \geq 3$, we have*

$$\begin{aligned}\varphi_n(N) &= -\left(N^{n-1} + 1 - \varphi_{n-1}(N)\right)(2^{2\ell}w + w_0) - N\varphi_{n-2}(N) \\ &\quad + (N + 1)\left(N^{n-1} + 1\right).\end{aligned}$$

For example, one has

$$\begin{aligned}\varphi_3(N) &= -2^{6\ell}w^3 - 3 \cdot 2^{4\ell}w_0w^2 - 3 \cdot 2^{2\ell}(w_0^2 - N)w + N^3 - w_0^3 + 3Nw_0 + 1, \\ \varphi_4(N) &= -2^{8\ell}w^4 - 2^{6\ell+2}w_0w^3 - 2^{4\ell+1}(3w_0^2 - 2N)w^2 - 2^{2\ell+2}(w_0^3 - 2Nw_0)w \\ &\quad + N^4 - w_0^4 + 4Nw_0^2 - 2N^2 + 1, \\ \varphi_5(N) &= -2^{10\ell}w^5 - 5 \cdot 2^{8\ell}w_0w^4 - 5 \cdot 2^{6\ell}(2w_0^2 - N)w^3 - 5 \cdot 2^{4\ell}(2w_0^3 - 3Nw_0)w^2 \\ &\quad - 5 \cdot 2^{2\ell}(w_0^4 - 3Nw_0^2 + N^2)w + N^5 - w_0^5 + 5Nw_0^3 - 5N^2w_0 + 1.\end{aligned}$$

Lemma 7. *Let $N = pq$ with $p + q = 2^{2\ell}w + w_0$. The function $\psi_n(N)$ fulfills*

1. $\psi_1(N) = 1$.
2. $\psi_2(N) = 2^{2\ell}w + w_0 + N + 1$.
3. *For any $n \geq 3$, one finds*

$$\psi_n(N) = \psi_{n-1}(N)(2^{2\ell}w + w_0) - \psi_{n-2}(N)N + N^{n-1} + 1.$$

For instance, one finds

$$\begin{aligned}\psi_3(N) &= 2^{4\ell}w^2 + (2^{2\ell}N + 2^{2\ell+1}w_0 + 2^{2\ell})w + N^2 + Nw_0 + w_0^2 - N + w_0 + 1, \\ \psi_4(N) &= 2^{6\ell}w^3 + (2^{4\ell}(N + 3w_0 + 1))w^2 \\ &\quad + (2^{2\ell}N^2 + 2^{2\ell+1}Nw_0 + 3 \cdot 2^{2\ell}w_0^2 - 2^{2\ell+1}N + 2^{2\ell+1}w_0 + 2^{2\ell})w \\ &\quad + (N^3 + N^2w_0 + Nw_0^2 + w_0^3 - N^2 - 2Nw_0 + w_0^2 - N + w_0 + 1), \\ \psi_5(N) &= 2^{8\ell}w^4 + (2^{6\ell}N + 4 \cdot 2^{6\ell}w_0 + 2^{6\ell})w^3 \\ &\quad + (2^{4\ell}N^2 + 3 \cdot 2^{4\ell}Nw_0 + 6 \cdot 2^{4\ell}w_0^2 - 3 \cdot 2^{4\ell}N + 3 \cdot 2^{4\ell}w_0 + 2^{4\ell})w^2 \\ &\quad + (2^{2\ell}N^3 + 2^{2\ell+1}N^2w_0 + 3 \cdot 2^{2\ell}Nw_0^2 + 4 \cdot 2^{2\ell}w_0^3 - 2^{2\ell+1}N^2 \\ &\quad - 6 \cdot 2^{2\ell}Nw_0 + 3 \cdot 2^{2\ell}w_0^2 - 2^{2\ell+1}N + 2^{2\ell+1}w_0 + 2^{2\ell})w \\ &\quad + (N^4 + N^3w_0 + N^2w_0^2 + Nw_0^3 + w_0^4 - N^3 - 2N^2w_0 - 3Nw_0^2 \\ &\quad + w_0^3 + N^2 - 2Nw_0 + w_0^2 - N + w_0 + 1).\end{aligned}$$

From the recursive formulas presented above, it follows by induction on n that $\varphi_n(N)$ and $\psi_n(N)$ are polynomials in w with integer coefficients. This can be summarized as follows: [9,12].

Lemma 8. Let $N = pq$ with $p + q = 2^{2\ell}w + w_0$. For any integer $n \geq 1$, one can compute coefficients $a_k \in \mathbb{Z}$, $0 \leq k \leq n - 1$, using n , N , ℓ , and w_0 , so that

$$\varphi_n(N) = -2^{2\ell n}w^n + \sum_{k=0}^{n-1} a_k w^k.$$

Lemma 9. Let $N = pq$ with $p + q = 2^{2\ell}w + w_0$. For any integer $n \geq 2$, one can compute coefficients $b_k \in \mathbb{Z}$, $0 \leq k \leq n - 2$, using n , N , ℓ , and w_0 , so that

$$\psi_n(N) = 2^{2\ell(n-1)}w^{n-1} + \sum_{k=0}^{n-2} b_k w^k.$$

It is worth emphasizing that knowledge of the coefficients a_k and b_k does not suffice to compute the totients $\varphi_n(N)$ and $\psi_n(N)$. The essential difficulty lies in determining the unknown value w associated with each function.

In what follows, we introduce two families of schemes that are vulnerable to our attacks.

2.2. The First Family of Cryptosystems

We note that for $n = 1$, the function $\varphi_1(N)$ coincides with the standard Euler totient function used in the RSA cryptosystem.

2.2.1. Cryptosystems Related to the Equation $ed - k\varphi_2(N) - 1 = 0$

Castagnos [15] introduced, in 2007, a probabilistic cryptosystem built on quadratic field quotients, where computations are performed using Lucas sequences. The system employs a modulus $N = pq$, and the public and private keys satisfy $ed - k\varphi_2(N) - 1 = 0$. Additional schemes based on the same relation are presented in [16–18].

2.2.2. Cryptosystems Related to the Equation $ed - k\varphi_n(N) - 1 = 0$

In 2023, Cotan and Teşleanu [13] proposed a generalized version of the RSA scheme [1]. The arithmetic operations in this construction are performed over the quotient group $\mathcal{Q}_n = \mathbb{Z}_N[z]/(z^n - a)$ where N is an RSA modulus, and a is chosen such that the polynomial $z^n - a$ is irreducible over $\mathbb{F}[z]$. The function $\varphi_n(N)$ denotes the order of the multiplicative group $\mathcal{Q}_n^*$. For any positive integer i and $\mathfrak{p} \in \mathcal{Q}_n$, we write $\mathfrak{p}^{\odot i}$ to indicate

the repeated product of p with itself i times. An analogue of Fermat's Little Theorem then holds in $\mathcal{Q}_n$:

$$p^{\odot \varphi_n(N)} \equiv 1 \pmod{N}.$$

We note that for an RSA modulus $N = pq$, one has the isomorphism

$$\mathcal{Q}_n \simeq \mathbb{F}_p[z]/(z^n - a) \times \mathbb{F}_q[z]/(z^n - a),$$

and thus $\varphi_n(N) = (p^n - 1)(q^n - 1)$.

The above algebraic framework naturally supports the design of a cryptosystem analogous to RSA. To initialize the system, two distinct large primes p and q of bit-length r are selected, forming the modulus $N = pq$. Also, the exponents (e, d) are generated such that $ed - 1 \equiv 0 \pmod{\varphi_n(N)}$.

To encrypt a message, the plaintext is first encoded as a polynomial in $\mathcal{Q}_n$:

$$m = \gamma_0 + \gamma_1 z + \cdots + \gamma_{n-1} z^{n-1},$$

where the coefficients $\gamma_0, \dots, \gamma_{n-1} \in \mathbb{Z}_N$ encode the message content.

The ciphertext is then obtained via exponentiation in $\mathcal{Q}_n$ modulo N , replacing any occurrence of z^n with a in accordance with the algebraic structure: $c \equiv m^e \pmod{N}$. The resulting encrypted message is the polynomial c . To decrypt and recover the plaintext polynomial m , one computes $m \equiv c^d \pmod{N}$, again replacing z^n with a according to the structure of $\mathcal{Q}_n$.

Further constructions have been introduced in [19–22], each satisfying $ed - k\varphi_n(N) - 1 = 0$.

2.3. The Second Family of Cryptosystems

2.3.1. Cryptosystems Related to the Equation $ed - k\psi_3(N) - 1 = 0$

In 2018, Murru and Saettone [23] introduced an RSA-like cryptosystem that incorporates a novel operation $\odot$ defined via the cubic Pell equation

$$z_1^3 + az_2^3 + a^2 z_3^3 - 3az_1 z_2 z_3 \equiv 1 \pmod{N}.$$

The modulus is set as $N = pq$, with a chosen to be a cubic non-residue modulo both primes p and q . The encryption exponent e is selected to satisfy $\gcd(e, \psi_3(N)) = 1$ and the corresponding secret exponent d fulfills $ed - k\psi_3(N) - 1 = 0$. Within this framework, encryption raises a plaintext pair (a_1, a_2) to the power of e using the $\odot$ operation, producing the ciphertext

$$(b_1, b_2) = (a_1, a_2)^{\odot e} \pmod{N}.$$

Decryption is performed by exponentiating the ciphertext with d under the same operation, recovering the original plaintext:

$$(a_1, a_2) = (b_1, b_2)^{\odot d} \pmod{N}.$$

2.3.2. Cryptosystems Related to the Equation $ed - k\psi_n(N) - 1 = 0$

Cotan and Teşeleanu [14] introduced in 2022 a generalized Murru–Saettone cryptosystem [23], operating over the quotient group

$$\mathcal{E}_n = \mathcal{F}_n^* / \mathbb{F}^*, \quad \mathcal{F}_n = \mathbb{Z}_N[x] / (z^n - a),$$

where N is an RSA modulus and a ensures that $x^n - a$ is irreducible over $\mathbb{F}$. The order of the unit group $\mathcal{E}_n^*$ is denoted $\psi_n(N)$ and is computed by

$$\psi_n(N) = \frac{(p^n - 1)(q^n - 1)}{(p - 1)(q - 1)}.$$

For any $\mathfrak{p} \in \mathcal{E}_n$ and integer $i > 0$, $\mathfrak{p}^{\odot i}$ indicates repeated multiplication in the group. A Fermat-like property holds:

$$\mathfrak{p}^{\odot \psi_n(N)} \equiv 1 \pmod{N}.$$

The system mirrors RSA in its operation. Two distinct large primes p and q of bit-length r are chosen to form $N = pq$. Similarly, the encryption and decryption exponents are such that $ed - 1 \equiv 0 \pmod{\psi_n(N)}$.

Messages are encoded as polynomials

$$\mathfrak{m} = \gamma_0 + \gamma_1 z + \cdots + \gamma_{t-1} z^{t-1} + z^t, \quad t < n,$$

with coefficients in $\mathbb{Z}_N$. Encryption is performed via

$$\mathfrak{c} \equiv \mathfrak{m}^e \pmod{N},$$

where z^n is replaced by a . Decryption retrieves the plaintext using

$$\mathfrak{m} \equiv \mathfrak{c}^d \pmod{N}.$$

2.4. LLL Algorithm

In geometry of numbers, a lattice $\mathcal{L} \subseteq \mathbb{R}^m$ of rank r can be generated by a finite set of linearly independent vectors. Specifically, there exists a basis $(\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_r)$ of $\mathbb{R}^r$ such that

$$\mathcal{L} = \left\{ \sum_{i=1}^r a_i \mathbf{v}_i \mid a_i \in \mathbb{Z} \right\}.$$

When the number of basis vectors equals the ambient dimension, $r = m$, the lattice is referred to as full-rank.

For practical computations, it is often convenient to encode the lattice in matrix form. Let B be the matrix whose rows are the basis vectors $\mathbf{v}_1, \dots, \mathbf{v}_r$; then the lattice can be described as $\mathcal{L} = \{\mathbf{z}B \mid \mathbf{z} \in \mathbb{Z}^r\}$. The lattice $\mathcal{L}$ has an associated volume, defined by $\det(\mathcal{L}) = \sqrt{\det(B^\top B)}$, where $B^\top$ is the transpose of B . For full-rank lattices, this simplifies to $\det(\mathcal{L}) = |\det(B)|$.

It is noteworthy that any lattice of rank at least two admits infinitely many generating bases, each consisting of the same number of vectors and producing the same lattice volume. Nevertheless, identifying a basis made of short, nearly mutually orthogonal vectors is a challenging problem, especially in higher dimensions. To overcome this difficulty, Lenstra, Lenstra, and Lovász developed the LLL algorithm [24] in 1982. This algorithm efficiently computes a basis in which the vectors are relatively short and nearly orthogonal, providing a practical tool for applications in relatively smaller dimensions.

As stated in [25], the theorem below details the behavior of the LLL algorithm's output and constitutes a key component in the cryptanalysis of RSA and similar cryptographic constructions.

Theorem 1. Let $(\mathbf{v}_1, \dots, \mathbf{v}_r)$ be a basis of a lattice. Applied to $(\mathbf{v}_1, \dots, \mathbf{v}_r)$, the LLL algorithm produces a new basis $(\mathbf{w}_1, \dots, \mathbf{w}_r)$ such that

$$\|\mathbf{w}_1\| \leq \|\mathbf{w}_2\| \leq \dots \leq \|\mathbf{w}_j\| \leq 2^{\frac{r(r-1)}{4(r+1-j)}} \det(\mathcal{L})^{\frac{1}{r+1-j}}, \quad j = 1, \dots, r.$$

2.5. Determining Small Solutions in Modular Congruences

In 1996, Coppersmith [2] presented a polynomial-time algorithm for finding small integer solutions to univariate polynomial congruences $g(x) \equiv 0 \pmod{M}$, assuming that the modulus M is known but its prime decomposition remains hidden. This technique was subsequently generalized to multivariate polynomials, addressing polynomials of the form

$$G(x_1, \dots, x_n) = \sum_{j_1, \dots, j_n} a_{j_1, \dots, j_n} x_1^{j_1} \cdots x_n^{j_n},$$

with integer coefficients $a_{j_1, \dots, j_n}$. The Euclidean norm associated with the polynomial G is introduced as follows:

$$\|G(x_1, x_2, \dots, x_n)\| = \sqrt{\sum_{j_1, j_2, \dots, j_n} a_{j_1, j_2, \dots, j_n}^2}.$$

In 1997, Howgrave-Graham [26] developed a variant of Coppersmith's method that provides a sufficient condition under which small modular roots of a multivariate polynomial correspond precisely to integer solutions. The formal statement is restated as follows:

Theorem 2 (Howgrave-Graham). Let $G(x_1, \dots, x_n)$ be a multivariate polynomial with integer coefficients, containing at most r nonzero monomials. Let $R > 0$ be an integer. Suppose there exist integers $u_1, \dots, u_n$ and positive bounds $U_1, \dots, U_n$ such that

1. $G(u_1, \dots, u_n) \equiv 0 \pmod{R}$,
2. $\|G(x_1 U_1, \dots, x_n U_n)\| < \frac{R}{\sqrt{r}}$.
3. $|u_i| < U_i$ for each $i = 1, \dots, n$.

Then $G(u_1, \dots, u_n) = 0$.

In the case of multivariate polynomials with three or more variables, Coppersmith-type algorithms are usually heuristic. Accordingly, the subsequent assumption [3,27–29] is frequently invoked.

Assumption 1. Let $G_1, G_2, \dots, G_r$ denote the polynomials whose coefficients are given by the components of the reduced vectors obtained from applying the LLL algorithm to the lattice basis. We assume that these polynomials are algebraically independent, that is, for any polynomial $P \in \mathbb{Z}[x_1, \dots, x_r]$, the relation $P(G_1, G_2, \dots, G_r) = 0$ implies that P is identically zero.

Given the preceding conditions, one can determine the shared solution $(u_1, \dots, u_n)$ of the equations

$$G_i(x_1, \dots, x_n) = 0, \quad i = 1, \dots, r,$$

by employing computational techniques such as Gröbner bases or resultants.

Notice that, in practice, multivariate Coppersmith-type attacks have been observed to succeed with high probability in numerous cryptanalytic applications. Nevertheless, no general theoretical guarantee is known when more than two variables are involved. The attack may fail if the polynomials produced after the LLL reduction are not algebraically independent or if the resulting polynomial system is degenerate, preventing Gröbner basis or resultant computations from recovering the desired roots.

3. The New Attacks

In this section, we present two lattice-based cryptanalytic attacks against the family introduced in Section 2.2 and the second family outlined in Section 2.3.

3.1. Cryptanalysis of the First Family

We analyze the first family in the presence of shared least significant bits among the prime factors and shared most significant bits among two secret exponents.

Theorem 3. Let $n \geq 1$ be an integer, and $N = pq$ be an RSA modulus, where p and q are two primes of equal bit-length sharing ℓ LSBs with $2^\ell = N^\theta$ and $0 \leq \theta < \frac{1}{4}$. Suppose that there exist two pairs of encryption and decryption exponents (e_i, d_i) , $i \in \{1, 2\}$, satisfying the key equations $e_i d_i - k_i \varphi_n(N) = 1$, with $e_1, e_2 \leq N^\alpha$, $|d_1 - d_2| < N^\beta$, and $d_1, d_2 \leq N^\delta$. Then, under Assumption 1, the pair (p, q) can be computed in polynomial time whenever

$$\beta < \frac{5}{4}n + \alpha - n\theta, \quad \delta < \frac{5}{2}n - 2n\theta - \beta - \frac{1}{4}\sqrt{6n(4n\theta - 4\alpha + 4\beta - 5n)(4\theta - 1)}.$$

Proof. On the one hand, by Lemma 8, we have

$$\varphi_n(N) = \sum_{k=0}^n a_k w^k,$$

where $a_n = -2^{2\ell n}$, $a_k \in \mathbb{Z}$ for $0 \leq k \leq n-1$, and w is defined by the relation $p + q = 2^{2\ell}w + w_0$, as stated in Lemma 3. On the other hand, by scaling the first key relation by e_2 and the second by e_1 , and subsequently taking their difference, the resulting expression becomes

$$e_2 e_1 (d_1 - d_2) - e_2 k_1 \varphi_n(N) + e_1 k_2 \varphi_n(N) = e_2 - e_1. \quad (1)$$

This shows that the tuple $(z_1, z_2, z_3, z_4) = (d_1 - d_2, k_1, k_2, w)$ is a root of the polynomial equation

$$f_n(z_1, z_2, z_3, z_4) = 0,$$

where

$$f_n(z_1, z_2, z_3, z_4) = e_1 e_2 z_1 - (e_2 z_2 - e_1 z_3) \left(\sum_{k=0}^n a_k z_4^k \right) + e_1 - e_2. \quad (2)$$

In order to compute small roots of the above equation, we employ a variant of Copper-Smith's method derived from the strategy introduced by Jochemsz and May [27]. This approach consists in constructing two specific sets of monomials associated with the polynomial $f_n(z_1, z_2, z_3, z_4)$. More precisely, we fix two positive integers v and t , where t will be optimized at a later stage. Moreover, let

$$\mathcal{M}_1 = \bigcup_{0 \leq l \leq t} \{z_1^{a_1} z_2^{a_2} z_3^{a_3} z_4^{a_4+l} : z_1^{a_1} z_2^{a_2} z_3^{a_3} z_4^{a_4} \text{ is a monomial of } f_n^{v-1}(z_1, z_2, z_3, z_4)\}.$$

We denote by $\mathcal{M}_0$ the set of monomials obtained by multiplying the monomials of $f_n(z_1, z_2, z_3, z_4)$ by those of $\mathcal{M}_1$. Based on the binomial expansion, the monomials of $f_n^{v-1}(z_1, z_2, z_3, z_4)$ are described by tuples (a_1, a_2, a_3, a_4) satisfying

$$\begin{cases} 0 \leq a_1 \leq v-1, \\ 0 \leq a_2 \leq v-1-a_1, \\ 0 \leq a_3 \leq v-1-a_1-a_2, \\ 0 \leq a_4 \leq na_2+na_3. \end{cases}$$

Then, the monomials of $\mathcal{M}_1$ are identified by

$$\begin{cases} 0 \leq a_1 \leq v-1, \\ 0 \leq a_2 \leq v-1-a_1, \\ 0 \leq a_3 \leq v-1-a_1-a_2, \\ 0 \leq a_4 \leq na_2+na_3+t. \end{cases}$$

In a similar manner, the monomials of $\mathcal{M}_0$ are those composed from

$$\begin{cases} 0 \leq a_1 \leq v, \\ 0 \leq a_2 \leq v-a_1, \\ 0 \leq a_3 \leq v-a_1-a_2, \\ 0 \leq a_4 \leq na_2+na_3+t. \end{cases}$$

In the rest of the analysis, we also need to identify the monomials of $\mathcal{M}_0 \setminus \mathcal{M}_1$. A simple observation shows that the monomials under consideration can be partitioned as $\mathcal{D}_1 \cup \mathcal{D}_2 \cup \mathcal{D}_3$. More precisely, the set $\mathcal{D}_1$ consists of monomials whose exponents satisfy

$$\begin{cases} a_1 = v, \\ 0 \leq a_2 \leq v-a_1, \\ 0 \leq a_3 \leq v-a_1-a_2, \\ 0 \leq a_4 \leq na_2+na_3+t. \end{cases}$$

Similarly, the set $\mathcal{D}_2$ consists of monomials with exponents satisfying

$$\begin{cases} 0 \leq a_1 \leq v-1, \\ a_2 = v-a_1, \\ 0 \leq a_3 \leq v-a_1-a_2, \\ 0 \leq a_4 \leq na_2+na_3+t. \end{cases}$$

Finally, the set $\mathcal{D}_3$ consists of monomials whose exponents fulfill

$$\begin{cases} 0 \leq a_1 \leq v-1, \\ 0 \leq a_2 \leq v-1-a_1, \\ a_3 = v-a_1-a_2, \\ 0 \leq a_4 \leq na_2+na_3+t. \end{cases}$$

A central step in Coppersmith's method is the determination of suitable bounds for the unknown roots. For z_1 , we set $Z_1 = N^\beta$ which stands for $|d_1 - d_2| < N^\beta$. To determine bounds of both z_2 and z_3 , observe that for $i \in \{1, 2\}$,

$$k_i = \frac{ed_i - 1}{\varphi_n(N)},$$

with $e = N^\alpha$, and $d_i < N^\delta$. By Lemma 4, we have $\frac{N^n}{2} \leq \varphi_n(N)$. This implies $k_i < 2N^{\alpha+\delta-n}$. Consequently, we may take

$$Z_2 = Z_3 = 2N^{\alpha+\delta-n}.$$

For z_4 , we use the relations $2^\ell = N^\theta$ and $p + q = 2^{2\ell}w + w_0$, together with the bound $p + q < (1 + \sqrt{2})N^{1/2}$ stated in Lemma 2. This gives

$$w = \frac{p + q - w_0}{2^{2\ell}} < (1 + \sqrt{2})N^{1/2-2\theta}.$$

As $\frac{1}{2} - 2\theta > 0$, a valid bound of z_4 , is Z_4 with

$$Z_4 = (1 + \sqrt{2})N^{1/2-2\theta}.$$

Next, let W_n denote the maximum absolute value of the coefficients of $f_n(z_1Z_1, z_2Z_2, z_3Z_3, z_4Z_4)$, that is, $W_n := \|f_n(z_1Z_1, z_2Z_2, z_3Z_3, z_4Z_4)\|_\infty$. Then, from (2), W_n satisfies the lower bound $e_2Z_2a_0 \leq W_n$. For sufficiently large values of N , Lemma 6 implies that the dominant term of a_0 is N^n . Hence, asymptotically, we have $a_0 \approx N^n$, and therefore

$$2N^\alpha N^{\alpha+\delta-n} N^n = 2N^{2\alpha+\delta} \leq W_n. \quad (3)$$

Define

$$R_n = W_n \left(\prod_{i=1}^3 Z_i \right)^{v-1} Z_4^{n(v-1)+t}.$$

We require that

$$\gcd(R_n, e_1 - e_2) = 1.$$

Since

$$R_n = W_n \left(\prod_{i=1}^3 Z_i \right)^{v-1} Z_4^{n(v-1)+t},$$

it suffices to ensure that

$$\gcd(Z_i, e_1 - e_2) = 1, \quad i = 1, \dots, 4,$$

and

$$\gcd(W_n, e_1 - e_2) = 1.$$

The quantities Z_i are merely upper bounds on the unique solution (z_1, z_2, z_3, z_4) . Therefore, replacing them by larger values preserves the validity of the attack. Since $e_1 - e_2$ is a fixed public integer, it possesses only finitely many prime divisors. Consequently, for each bound Z_i (resp. W_n), there always exists an integer $Z'_i \geq Z_i$ (resp. $W'_n \geq W_n$) such that

$$\gcd(Z'_i, e_1 - e_2) = 1 \quad \text{and} \quad \gcd(W'_n, e_1 - e_2) = 1.$$

Replacing Z_i and W_n by these enlarged bounds does not affect the asymptotic analysis. Hence, without loss of generality, we may assume that

$$\gcd(R_n, e_1 - e_2) = 1.$$

This allows us to compute the inverse of $e_1 - e_2$ modulo R_n , which we denote by c_0 , and to consider the following polynomial:

$$F_n(z_1, z_2, z_3, z_4) = c_0 f_n(z_1, z_2, z_3, z_4) \mod R_n,$$

whose constant term is equal to 1.

Following [27], we build two family of polynomials

$$\begin{aligned} g_{a_1, a_2, a_3, a_4}^{(n)} &= z_1^{a_1} z_2^{a_2} z_3^{a_3} z_4^{a_4} F_n Z_1^{v-1-a_1} Z_2^{v-1-a_2} Z_3^{v-1-a_3} Z_4^{n(v-1)+t-a_4} \\ &\text{for } z_1^{a_1} z_2^{a_2} z_3^{a_3} z_4^{a_4} \in \mathcal{M}_1, \\ h_{a_1, a_2, a_3, a_4}^{(n)} &= z_1^{a_1} z_2^{a_2} z_3^{a_3} z_4^{a_4} R_n \\ &\text{for } z_1^{a_1} z_2^{a_2} z_3^{a_3} z_4^{a_4} \in \mathcal{M}_0 \setminus \mathcal{M}_1. \end{aligned} \quad (4)$$

Subsequently, the coefficient vectors of the polynomials

$$g_{a_1, a_2, a_3, a_4}^{(n)}(z_1 Z_1, z_2 Z_2, z_3 Z_3, z_4 Z_4) \quad \text{and} \quad h_{a_1, a_2, a_3, a_4}^{(n)}(z_1 Z_1, z_2 Z_2, z_3 Z_3, z_4 Z_4)$$

form a Euclidean lattice $\mathcal{L}(n, v, t)$ whose dimension is given by the number of elements in $\mathcal{M}_1$ and $\mathcal{M}_0 \setminus \mathcal{M}_1$, that is

$$r(n, t, v) = \frac{1}{12} v^4 (n + 2t) + \frac{1}{6} v^3 (3n + 6t + 1) + \frac{1}{12} v^2 (11n + 22t + 12) + \frac{1}{6} v (3n + 6t + 11) + 1.$$

For the purpose of simplifying the determinant computation, it is customary to impose a suitable ordering on the rows and columns of the lattice basis matrix so that it assumes a left or right triangular form. Following the approach of [27], the matrix can be arranged in a right triangular form as follows: The rows corresponding to the polynomials $g_{a_1, a_2, a_3, a_4}^{(n)}$ and $h_{a_1, a_2, a_3, a_4}^{(n)}$ are ordered according to the lexicographic order on the index tuple (a_1, a_2, a_3, a_4) . Likewise, the columns, which correspond to the monomials $z_1^{a_1} z_2^{a_2} z_3^{a_3} z_4^{a_4}$, are arranged according to the same lexicographic order on (a_1, a_2, a_3, a_4) . A toy example is presented in Table 1 where the symbol $\odot$ represents non-zero entries.

Table 1. The lattice matrix when $(v, t, n) = (1, 1, 2)$.

Polynomials \ Monomials	1	z_4	z_3	$z_3 z_4$	$z_3 z_4^2$	$z_3 z_4^3$	z_2	$z_2 z_4$	$z_2 z_4^2$	$z_2 z_4^3$	z_1	$z_1 z_4$
$g_{0,0,0,0}^{(2)}$	Z_4	0	$\odot$	$\odot$	$\odot$	0	$\odot$	$\odot$	$\odot$	0	$\odot$	0
$g_{0,0,0,1}^{(2)}$	0	Z_4	0	$\odot$	$\odot$	$\odot$	0	$\odot$	$\odot$	$\odot$	0	$\odot$
$h_{0,0,1,0}^{(2)}$	0	0	$Z_3 R_2$	0	0	0	0	0	0	0	0	0
$h_{0,0,1,1}^{(2)}$	0	0	0	$Z_3 Z_4 R_2$	0	0	0	0	0	0	0	0
$h_{0,0,1,2}^{(2)}$	0	0	0	0	$Z_3 Z_4^2 R_2$	0	0	0	0	0	0	0
$h_{0,0,1,3}^{(2)}$	0	0	0	0	0	$Z_3 Z_4^3 R_2$	0	0	0	0	0	0
$h_{0,1,0,0}^{(2)}$	0	0	0	0	0	0	$Z_2 R_2$	0	0	0	0	0
$h_{0,1,0,1}^{(2)}$	0	0	0	0	0	0	0	$Z_2 Z_4 R_2$	0	0	0	0
$h_{0,1,0,2}^{(2)}$	0	0	0	0	0	0	0	0	$Z_2 Z_4^2 R_2$	0	0	0
$h_{0,1,0,3}^{(2)}$	0	0	0	0	0	0	0	0	0	$Z_2 Z_4^3 R_2$	0	0
$h_{1,0,0,0}^{(2)}$	0	0	0	0	0	0	0	0	0	0	$Z_1 R_2$	0
$h_{1,0,0,1}^{(2)}$	0	0	0	0	0	0	0	0	0	0	0	$Z_1 Z_4 R_2$

In addition, the diagonal terms corresponding to the polynomials $g_{a_1, a_2, a_3, a_4}^{(n)}$ are of the form $(Z_1 Z_2 Z_3)^{v-1} Z_4^{n(v-1)+t}$, while those associated with $h_{a_1, a_2, a_3, a_4}^{(n)}$ take the form $W_n Z_1^{v-1+a_1} Z_2^{v-1+a_2} Z_3^{v-1+a_3} Z_4^{n(v-1)+t+a_4}$. For $1 \leq k \leq 4$, define

$$\sigma_k = \sum_{z_1^{a_1} z_2^{a_2} z_3^{a_3} z_4^{a_4} \in \mathcal{M}_0 \setminus \mathcal{M}_1} a_k. \quad (5)$$

It follows that the lattice determinant can be written as

$$\begin{aligned}\det(\mathcal{L}) &= \prod_{j=1}^3 Z_j^{(v-1)\#\mathcal{M}_1 + (v-1)\#(\mathcal{M}_0 \setminus \mathcal{M}_1) + \sigma_j} \\ &\times W_n^{\#(\mathcal{M}_0 \setminus \mathcal{M}_1)} Z_4^{(n(v-1)+t)\#\mathcal{M}_1 + (n(v-1)+t)\#(\mathcal{M}_0 \setminus \mathcal{M}_1) + \sigma_4} \\ &= \prod_{j=1}^3 Z_j^{(v-1)\#\mathcal{M}_0 + \sigma_j} \times W_n^{\#(\mathcal{M}_0 \setminus \mathcal{M}_1)} Z_4^{(n(v-1)+t)\#\mathcal{M}_0 + \sigma_4}.\end{aligned}\quad (6)$$

We perform an LLL reduction on the lattice basis matrix $\mathcal{B}(n, t, v)$, producing a reduced basis $\mathcal{B}'(n, t, v)$ that preserves the determinant. The vectors of this reduced basis generate a set of polynomial relations

$$G_i(z_1, z_2, z_3, z_4) \equiv 0 \pmod{R_n}, \quad i = 1, \dots, r(n, t, v).$$

The extraction of the desired solution is achieved by combining Theorem 2 with the properties of the LLL-reduced basis from Theorem 1. By focusing on the case $j = 4$, the solution can be guaranteed by imposing the condition below

$$2^{\frac{r(n,t,v)(r(n,t,v)-1)}{4(r(n,t,v)-3)}} \left(\det \mathcal{L}(n, t, v) \right)^{\frac{1}{r(n,t,v)-3}} < \frac{R_n}{\sqrt{r(n, t, v)}},$$

or equivalently

$$\det(\mathcal{L}(n, t, v)) < \frac{1}{r(n, t, v)^{\frac{r(n,t,v)-3}{2}} 2^{\frac{r(n,t,v)(r(n,t,v)-1)}{4}}} R_n^{r(n,t,v)-3}.$$

This leads to

$$\det(\mathcal{L}(n, t, v)) < R_n^{r(n,t,v)}.$$

In addition to (6), we get

$$\begin{aligned}W_n^{\#(\mathcal{M}_0 \setminus \mathcal{M}_1)} \times \left(\prod_{j=1}^3 Z_j^{(v-1)\#\mathcal{M}_0 + \sigma_j} \right) \times Z_4^{(n(v-1)+t)\#\mathcal{M}_0 + \sigma_4} \\ < \left(W_n Z_4^{n(v-1)+t} \prod_{j=1}^3 Z_j^{(v-1)} \right)^{r(n,t,v)}.\end{aligned}$$

Combining with $\#\mathcal{M}_0 = r(n, t, v)$, we find that

$$\prod_{j=1}^4 Z_j^{\sigma_j} < W_n^{\#\mathcal{M}_1}.\quad (7)$$

To obtain an optimal bound, we replace t by vt . Using (5) and summing over the indices corresponding to the monomials in $\mathcal{M}_0 \setminus \mathcal{M}_1$, we obtain

$$\begin{aligned}\sigma_1 &= \frac{1}{12}(n+2t)v^4 + \frac{1}{6}(n+3t+1)v^3 - \frac{1}{12}(n-4t-6)v^2 - \frac{1}{6}(n-2)v, \\ \sigma_2 &= \frac{1}{24}(3n+4t)v^4 + \frac{1}{12}(5n+6t+2)v^3 + \frac{1}{24}(9n+8t+12)v^2 + \frac{1}{12}(n+4)v, \\ \sigma_3 &= \frac{1}{24}(3n+4t)v^4 + \frac{1}{12}(5n+6t+2)v^3 + \frac{1}{24}(9n+8t+12)v^2 + \frac{1}{12}(n+4)v, \\ \sigma_4 &= \frac{1}{24}(3n^2+8nt+6t^2)v^4 + \frac{1}{12}(5n^2+12nt+9t^2+2n+3t)v^3 \\ &\quad + \frac{1}{24}(9n^2+16nt+12t^2+12n+18t)v^2 + \frac{1}{12}(n^2+4n+6t)v.\end{aligned}$$

Similarly, we have

$$\#\mathcal{M}_1 = \frac{1}{12}(n+2t)v^4 + \frac{1}{6}(n+3t+1)v^3 - \frac{1}{12}(n-4t-6)v^2 - \frac{1}{6}(n-2)v.$$

Then, an elementary computation shows that, for sufficiently large v , the parameters σ_k and $\#\mathcal{M}_1$ satisfy the following asymptotic behavior:

$$\begin{aligned}\sigma_1 &= \frac{n+2t}{12}v^4 + o(v^4), \\ \sigma_2 &= \frac{3n+4t}{24}v^4 + o(v^4), \\ \sigma_3 &= \frac{3n+4t}{24}v^4 + o(v^4), \\ \sigma_4 &= \frac{1}{24}(3n^2+8nt+6t^2)v^4 + o(v^4), \\ \#\mathcal{M}_1 &= \frac{1}{12}(n+2t)v^4 + o(v^4).\end{aligned}$$

Retaining only the dominant parts, substituting the bounds Z_1, Z_2, Z_3, Z_4 , and neglecting smaller coefficients, relation (7) reduces, in view of (3), to

$$N^{\beta \frac{n+2t}{12} v^4} N^{(\alpha+\delta-n) \frac{3n+4t}{24} v^4} N^{(\alpha+\delta-n) \frac{3n+4t}{24} v^4} N^{\left(\frac{1}{2}-2\theta\right) \frac{1}{24} (3n^2+8nt+6t^2) v^4} < N^{(2\alpha+\delta) \frac{1}{12} (n+2t) v^4}.$$

After taking logarithms and dividing both sides by v^4 , we obtain the following inequality

$$\begin{aligned}\beta \frac{n+2t}{12} + (\alpha+\delta-n) \frac{3n+4t}{24} + (\alpha+\delta-n) \frac{3n+4t}{24} + \left(\frac{1}{2}-2\theta\right) \frac{1}{24} (3n^2+8nt+6t^2) \\ < (2\alpha+\delta) \frac{1}{12} (n+2t),\end{aligned}$$

or equivalently

$$-6(4\theta-1)t^2 - 8(4n\theta - \beta - \delta + n)t - 12n^2\theta + 4\alpha n + 4\beta n + 8\delta n - 9n^2 < 0,$$

which is optimized at

$$t_0 = \frac{2}{3} \left(\frac{4n\theta - \beta - \delta + n}{1-4\theta} \right).$$

Plugging t_0 in the preceding inequality yields

$$-8\delta^2 - 8(4n\theta + 2\beta - 5n)\delta + 16n^2\theta^2 - 48\alpha n\theta + 16\beta n\theta + 8n^2\theta - 8\beta^2 + 12\alpha n + 28\beta n - 35n^2 < 0.$$

After solving this quadratic inequation, a valid range of δ is

$$\delta < \frac{5}{2}n - 2n\theta - \beta - \frac{1}{4}\sqrt{6n(4n\theta - 4\alpha + 4\beta - 5n)(4\theta - 1)}.$$

It is worth noting that, since $\theta < \frac{1}{4}$, then the above bound is well defined if

$$4n\theta - 4\alpha + 4\beta - 5n < 0$$

or equivalently

$$\beta < \frac{5}{4}n + \alpha - n\theta.$$

Under this bound, together with Assumption 1, we consider four polynomials, namely $g_1^{(n)}, g_2^{(n)}, g_3^{(n)}$, and $g_4^{(n)}$. By solving the system

$$g_i^{(n)}(z_1, z_2, z_3, z_4) = 0, \quad i \in \{1, 2, 3, 4\},$$

using Gröbner basis techniques or resultant computations, we derive the value of $z_4 = w$. Combining the relations $N = pq$ and $p + q = 2^{2\ell}w + w_0$, we could then efficiently recover the prime factors (p, q) . This completes the proof. $\square$

Remark 1. When $n = 1$, the bound obtained in [6] coincides exactly with the bound derived in Theorem 3 as a special case. As a consequence, our attack applies to the same cryptographic setting as that considered in [6]. However, the proof presented here follows a different approach, relying on a new lattice construction and on the heuristic Assumption 1 concerning the algebraic independence of the polynomials produced after the LLL reduction.

Theorem 3 leads to two distinct consequences, depending on whether the secret exponents share a significant number of their most significant bits or share none at all.

Corollary 1. Let $n \geq 1$ be an integer, and $N = pq$ be an RSA modulus, where p and q are two primes of equal bit-length sharing ℓ LSBs with $2^\ell = N^\theta$ and $0 \leq \theta < \frac{1}{4}$. Suppose that there exist two pairs of encryption and decryption exponents (e_i, d_i) , $i \in \{1, 2\}$, satisfying the key equations $e_i d_i - k_i \varphi(N) = 1$, with $e_1, e_2 \leq N^\alpha$, and $d_1 \approx d_2 \approx N^\delta$. Then, under Assumption 1, the pair (p, q) can be computed in polynomial time whenever

$$0 < \frac{5}{4}n + \alpha - n\theta, \quad \delta < \frac{5}{2}n - 2n\theta - \frac{1}{4}\sqrt{6n(4n\theta - 4\alpha - 5n)(4\theta - 1)}.$$

Proof. When the secret exponents share a large portion of their most significant bits, Theorem 3 implies that $d_1 \approx d_2$, that is, $\beta \approx 0$. This satisfies the required bound. $\square$

Remark 2. In connection with Corollary 1, the bound for breaking RSA of Sarkar et al. [5] is

$$\delta < \frac{5}{8} - \frac{\beta}{2}.$$

To compare the resulting bounds, we take $\theta = 0$, $\alpha = 1$, $\beta = 0$, and $n = 1$. Then, the bound from Corollary 1 reduces to

$$\delta < \frac{5}{2} - \frac{3}{4}\sqrt{6} \approx 0.662,$$

which improves upon the bound $\delta < \frac{5}{8} \approx 0.625$ of [5].

Corollary 2. Let $n \geq 1$ be an integer, and let $N = pq$ be an RSA modulus, where p and q are two primes of equal bit-length sharing ℓ LSBs with $2^\ell = N^\theta$ and $0 \leq \theta < \frac{1}{4}$. Suppose that there exist two pairs of encryption and decryption exponents (e_i, d_i) , $i \in \{1, 2\}$, satisfying the key equations $e_i d_i - k_i \varphi_n(N) = 1$, with $e_1, e_2 \leq N^\alpha$, and $d_1, d_2 \leq N^\delta$. Then, under Assumption 1, the pair (p, q) can be computed in polynomial time whenever

$$\delta < \min\left(\frac{5}{4}n + \alpha - n\theta, \frac{17}{16}n - \frac{1}{4}n\theta - \frac{1}{16}\sqrt{3n(4\theta - 1)(12n\theta - 3n - 32\alpha)}\right).$$

Proof. If the secret exponents do not share any portion of their most significant bits, a natural bound for $|d_1 - d_2|$ is $\max(d_1, d_2) < N^\delta$. In this case, Theorem 3 applies with $\delta = \beta$, and solving the inequation with unknown δ provides the required bound. $\square$

Remark 3. In connection with Corollary 2, Sarkar et al. [5] (Corollary 1) showed that the maximal bound for breaking RSA is $\delta < 0.416$.

To compare the resulting bounds, we take $n = 1$, $\theta = 0$, and $\alpha = 1$ in Corollary 2. Then, our bound becomes $\delta < \delta_2$, where

$$\delta_2 = \frac{17}{16} - \frac{1}{16}\sqrt{105} \approx 0.422,$$

which is slightly improves the former bound of Sarkar et al. [5].

Remark 4. The optimal bound of [7] for small secret exponent attacks targeting a single secret exponent in schemes defined by $ed - k\varphi_n(N) = 1$ with $d < N^\delta$ is $\delta < 0.292n$. Figure 1 highlights that attacks exploiting two encryption exponents provide better bounds than those focusing on a single exponent. The comparison further shows that our bound A grows significantly beyond $B = 0.292n$ as θ varies over the interval $[0, \frac{1}{4}]$.

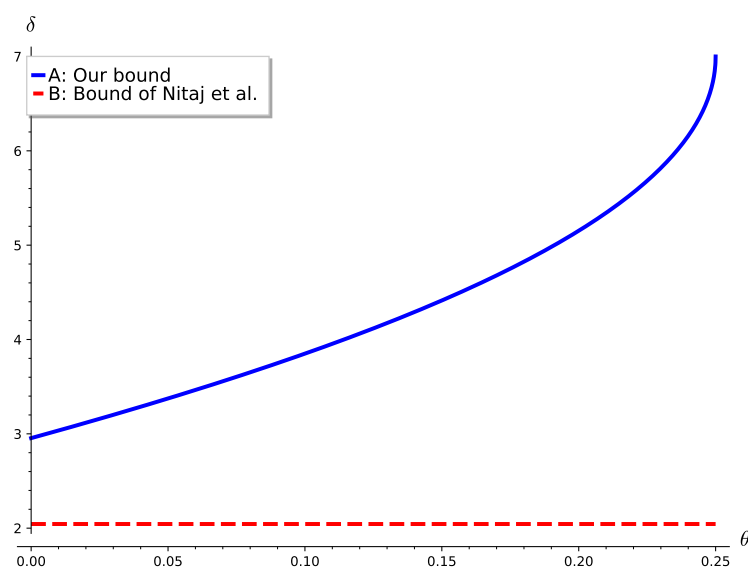


Figure 1. Comparison of our bound with the bound presented by Nitaj et al. in [7] for $n = 7$.

3.2. Cryptanalysis of the Second Family

We analyze the second family in the presence of shared least significant bits among the prime factors and shared most significant bits among two secret exponents.

Theorem 4. Let $n \geq 1$ be an integer, and let $N = pq$ be an RSA modulus, where p and q are two primes of equal bit-length sharing ℓ LSBs with $2^\ell = N^\theta$ and $0 \leq \theta < \frac{1}{4}$. Suppose that there exist two pairs of encryption and decryption exponents (e_i, d_i) , $i \in \{1, 2\}$, satisfying the key equations $e_i d_i - k_i \psi_n(N) = 1$, with $e_1, e_2 \leq N^\alpha$, $|d_1 - d_2| < N^\beta$, and $d_1, d_2 \leq N^\delta$. Then, under Assumption 1, the pair (p, q) can be computed in polynomial time whenever

$$\beta < \frac{5}{4}(n-1) + \alpha - \theta(n-1),$$

and

$$\delta < \left(\frac{5}{2} - 2\theta\right)(n-1) - \beta - \frac{1}{4}\sqrt{6(n-1)(4(n-1)\theta - 4\alpha + 4\beta - 5(n-1))(4\theta - 1)}.$$

Proof. Analogously to Theorem 3, we apply Lemma 9 to write

$$\psi_n(N) = \sum_{k=0}^{n-1} b_k w^k, \quad \text{with } b_{n-1} = 2^{2\ell(n-1)},$$

and

$$e_2 e_1 (d_1 - d_2) - e_2 k_1 \psi_n(N) + e_1 k_2 \psi_n(N) = e_2 - e_1. \quad (8)$$

This shows that the tuple $(z_1, z_2, z_3, z_4) = (d_1 - d_2, k_1, k_2, w)$ is a root of the polynomial equation $f_n(z_1, z_2, z_3, z_4) = 0$, where

$$f_n(z_1, z_2, z_3, z_4) = e_1 e_2 z_1 - (e_2 z_2 - e_1 z_3) \left(\sum_{k=0}^{n-1} b_k z_4^k \right) + e_1 - e_2.$$

The remainder of the analysis follows as in Theorem 3 by noting that the polynomial representing $\varphi_n(N)$ has degree n , whereas that representing $\psi_n(N)$ has degree $n-1$. Consequently, it suffices to replicate the analysis of Theorem 3, replacing n with $n-1$. This yields the required bound of δ and completes the proof. $\square$

Remark 5. Analogous results to Corollaries 1 and 2 also hold for the schemes satisfying $ed - k\psi_n(N) - 1 = 0$, upon replacing n with $n-1$.

4. A Detailed Numerical Experiment

In this section, we explain how the approach of Theorem 3 can be applied to carry out the attack in the present setting. Similar arguments can be simulated to implement Theorem 4.

All experiments were conducted using SageMath 10.4 on a system running Ubuntu 22.04.3 LTS, with an Intel® Core™ i5-4460 processor (3.20 GHz, 4 cores) and 8 GB of RAM.

For reproducibility purposes, the SageMath implementation used in our experiments, including the construction of the lattice and the computation of its dimension, has been made publicly available at https://github.com/algre96-hue/Attacking_RSA_Variants (accessed on 5 July 2026).

As a straightforward example to solve the equations

$$e_1 d_1 - k_1 \varphi_n(N) = e_2 d_2 - k_2 \varphi_n(N) = 1,$$

with unknowns $(d_1, d_2, k_1, k_2, \varphi_n(N))$, we fix $n = 3$, and use the public keys (N, e_1) and (N, e_2) given by

$$\begin{aligned} N &= 806245068963983742968693740528808594508793710387341582779982776 \backslash \\ &\quad 108779113, \\ e_1 &= 231691282929459044923108178276104618307528831372890503810101486 \backslash \\ &\quad 734951858438308718179865880413093925253316607860087206264898127 \backslash \\ &\quad 500677294931977139734051853846423113495173217473039304044159127 \backslash \\ &\quad 943164434958361854295459709, \\ e_2 &= 354338496806918522318046730914011367732246940549869784461102758 \backslash \\ &\quad 703145195910947658646243151957949682027354673165753581691230678 \backslash \\ &\quad 829996717301436163472036677513178388725597399984508751887100181 \backslash \\ &\quad 779436382627610885045199557. \end{aligned}$$

Under this setting, we obtain $(e_1, e_2) = (N^{\alpha_1}, N^{\alpha_2})$, where $\alpha_1 \approx 2.9951$ and $\alpha_2 \approx 2.9976$. We therefore set $\alpha = \max(\alpha_1, \alpha_2) = 2.9976$.

Suppose that the prime factors p and q of the RSA modulus $N = pq$ coincide on their ℓ least significant bits. Since the parameter ℓ is typically unknown, it can be determined by testing successive values $\ell = 1, 2, \dots$. In our experiments, we fix $\ell = 41$, which implies $2^\ell = N^\theta$ with $\theta \approx 0.172$. In relation to Lemma 3, we solve the equation $y^2 \equiv N \pmod{2^\ell}$. We obtain

$$v_0 \in \{127069610899, 972442016877, 1226581238675, 2071953644653\}.$$

In the present experiment, we choose $v_0 = 1226581238675$ and then compute

$$w_0 \equiv 2v_0 + (N - v_0^2)v_0^{-1} \pmod{2^{2\ell}},$$

yielding

$$w_0 = 3341263838569273827051302.$$

According to Lemma 6, the quantity $\varphi_3(N)$ can be expanded as

$$\varphi_3(N) = -2^{6\ell}w^3 + a_2w^2 + a_1w + a_0,$$

for

$$\begin{aligned} a_2 &= -3 \cdot 2^{4\ell} w_0, \\ a_1 &= -3 \cdot 2^{2\ell} (w_0^2 - N), \\ a_0 &= N^3 - w_0^3 + 3Nw_0 + 1. \end{aligned}$$

We thus seek to solve the equation

$$f_n(z_1, z_2, z_3, z_4) = e_1 e_2 z_1 - (e_2 z_2 - e_1 z_3) \left(-2^{6\ell} z_4^3 + a_2 z_4^2 + a_1 z_4 + a_0 \right) + e_1 - e_2 = 0,$$

which admits the particular root $(z_1, z_2, z_3, z_4) = (d_1 - d_2, k_1, k_2, w)$.

Following the framework of Theorem 3, we assume that d_1 and d_2 share 60 of their most significant bits. Since both d_1 and d_2 are unknown, the attacker may test several values of (δ, β) . We therefore assume that $d_1, d_2 < N^\delta$ and $|d_1 - d_2| < N^\beta$ with $\delta = \beta = 1.01$. Under these assumptions, all conditions of Theorem 3 are satisfied; in particular

$$\beta < \frac{5}{4}n + \alpha - n\theta \approx 6.2345,$$

and

$$\delta < \frac{5}{2}n - 2n\theta - \beta - \frac{1}{4}\sqrt{6n(4n\theta - 4\alpha + 4\beta - 5n)(4\theta - 1)} \approx 2.7499.$$

Next, we compute the corresponding bounds $Z_1 = N^\beta$, $Z_2 = Z_3 = 2N^{\alpha+\delta-n}$, and $Z_4 = (1 + \sqrt{2})N^{\frac{1}{2}-2\theta}$, as well as the quantity

$$R_n = W_n \left(\prod_{i=1}^3 Z_i \right)^{v-1} Z_4^{n(v-1)+t},$$

with $(v, t) = (2, 2)$ and

$$W_n := \|f_n(z_1 Z_1, z_2 Z_2, z_3 Z_3, z_4 Z_4)\|_\infty.$$

The computations show that $\gcd(e_1 - e_2, R_n) = 4$. We then increase the values of Z_i and W_n iteratively until we find $\gcd(Z_i, e_1 - e_2) = \gcd(W_n, e_1 - e_2) = 1$. The resulting updated values are

$$Z_1 = \lfloor N^\beta \rfloor \approx 422213137107693002779033747929516689837287923966529404308847711 \setminus 5052457985,$$

$$Z_2 = Z_3 = \lfloor 2N^{\alpha+\delta-n} \rfloor \approx 56752659365596464032000432082389163100210066153940897 \setminus 01791984314065354753,$$

$$Z_4 = (1 + \sqrt{2})N^{\frac{1}{2}-2\theta} = 494914431531$$

$$W_n = 1857032707364209387680402928084975626239658859824439493240028346627255 \setminus 7167887525559998260297204877002954821057384249002971375276303927846166 \setminus 1916786302078646232463676528546729532090629250584340525741135674076736 \setminus 3825772105684273718709619280306807780580944369937253700928658995136780 \setminus 3479977164414815842293669704635722150024956370326264909939449641204279 \setminus 1130587271083117994582227296721374354885116943278010289795584672095199 \setminus 317720089077,$$

which ensures that $\gcd(e_1 - e_2, R_n) = 1$, as required in the proof of Theorem 3.

From the coefficient vectors of the polynomials defined in (4), we construct a lattice $\mathcal{L}$ of dimension $r = 60$. After applying LLL reduction, the reduced basis yields 60 polynomials in one minute and 30 s. Computing a Gröbner basis allows us to extract the first four polynomials, and solving the resulting system over the integers yields the root in one minute and 13 s:

$$z_1 = 158262425115417123302104131002430427126427538464388740390172851092259 \setminus 4988,$$

$$z_2 = 139931758497970038898605235717441206034796833314785345344291469671521 \setminus 9858,$$

$$z_3 = 107002750243339113448222401480215470932254552554636736687358669177995 \setminus 3085,$$

$$z_4 = 371367493936.$$

Once $w = z_4$ is determined, the function $\varphi_3(N)$ is computed via

$$\varphi_3(N) = -2^{6\ell}w^3 + a_2w^2 + a_1w + a_0,$$

which yields

$$\begin{aligned} \varphi_3(N) = & 52408437810134958302844633027857758682441543029734412475676183 \backslash \\ & 40493356840772483135022976102946207086062981503532221720897449 \backslash \\ & 71478978062175468192886676645378920146508465035147003603703407 \backslash \\ & 091305574841771464418254080356. \end{aligned}$$

At the final stage, we solve the system formed by

$$p + q = 2^{2\ell}w + w_0 = 1795823007942579783416907274874046246,$$

and $N = pq$, resulting in

$$\begin{aligned} p &= 897911503971289891708485523274228627, \\ q &= 897911503971289891708421751599817619. \end{aligned}$$

Taking the modular inverses of e_1 and e_2 modulo $\varphi_3(N)$ results in

$$\begin{aligned} d_1 &= 316524850230834246430717185769744795475591926108172907331665413789090 \backslash \\ & 0861, \\ d_2 &= 158262425115417123128613054767314368349164387643784166941492562696830 \backslash \\ & 5873. \end{aligned}$$

Note that the sizes of d_1 and d_2 are on the order of $N^{1.0083}$ and $N^{1.0041}$, respectively, which are much larger than the maximum bound for small secret exponent attacks on a single encryption exponent, namely $N^{0.292n} \approx N^{0.876}$.

5. Conclusions

We presented lattice-based cryptanalytic attacks on two families of RSA-like cryptosystems characterized by one of the below equations:

$$ed - k \frac{(p^n - 1)(q^n - 1)}{(p - 1)(q - 1)} = 1 \quad \text{and} \quad ed - k(p^n - 1)(q^n - 1) = 1.$$

Assuming that two encryption exponents were employed, that the prime factors shared an amount of their least significant bits, and that the corresponding decryption exponents shared an amount of their most significant bits, we combined Coppersmith's method with Euclidean lattice reduction techniques to derive newly bounds on the secret parameters under which these schemes became vulnerable. Our attacks showed that this setting yielded improved bounds compared with the use of a single encryption exponent. In RSA and its variants, the primes are generated randomly. Then, with overwhelming probability, the primes will be of the size of $N^{0.5}$, and could share an amount of their least significant bits. Similarly, when two decryption exponents are generated randomly, then they could share an amount of their most significant bits. To avoid our attacks in the real-world, it is easy to check that the former scenarios do not occur.

Author Contributions: Conceptualization, B.C. and M.R.; methodology, B.C., M.R. and A.N.; software, B.C. and M.R.; validation, M.R., A.N. and M.Z.; formal analysis, M.R. and A.N.; investigation, B.C. and M.R.; resources, B.C. and M.R.; data curation, B.C. and M.R.; writing—original draft preparation, B.C. and M.R.; writing—review and editing, B.C., M.R. and A.N.; visualization, M.R. and

A.N.; supervision, A.N. and M.Z.; project administration, A.N. and M.Z.; funding acquisition, M.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

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

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

Abbreviations

The following abbreviations are used in this manuscript:

RSA	Rivest, Shamir and Adleman
LLL	Lenstra, Lenstra, Lovász
MSBs	most significant bits
LSBs	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.
2. Coppersmith, D. Small solutions to polynomial equations, and low exponent RSA vulnerabilities. *J. Cryptol.* **1997**, *10*, 233–260.
3. Boneh, D.; Durfee, G. Cryptanalysis of RSA with private key d less than $N^{0.292}$. In *Advances in Cryptology-Eurocrypt'99*; Lecture Notes in Computer Science; Springer-Verlag: Berlin, Germany, 1999; Volume 1592, pp. 1–11.
4. Wiener, M. Cryptanalysis of short RSA secret exponents. *IEEE Trans. Inf. Theory* **1990**, *36*, 553–558.
5. Sarkar, S.; Maitra, S. Cryptanalysis of RSA with two decryption exponents. *Inf. Process. Lett.* **2010**, *110*, 178–181.
6. Nitaj, A.; Ariffin, M.R.K.; Nassr, D.I.; Bahig, H.M. New attacks on the RSA cryptosystem. In *International conference on cryptology in Africa*; Springer International Publishing: Cham, Switzerland, 2014; pp. 178–198. Available online: <https://eprint.iacr.org/2014/549> (accessed on 5 July 2026).
7. Nitaj, A.; Adenan, N.N.H.; Ariffin, M.R.K. Cryptanalysis of a New Variant of the RSA Cryptosystem. In *Progress in Cryptology—AFRICACRYPT 2024*; Vaudenay, S., Petit, C., Eds.; AFRICACRYPT 2024, Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2024; Volume 14861.
8. Teşeleanu, G. (2025). A Lattice Attack Against a Family of RSA-Like Cryptosystems. In: *Cyber Security, Cryptology, and Machine Learning. CSCML 2024*. Lecture Notes in Computer Science, Springer, Cham.2024; vol 15349.
9. Rahmani, M.; Nitaj, A.; Ziane, M. Cryptanalysis of some algebraic variants of the RSA cryptosystem. *Finite Fields Their Appl.* **2026**, *110*, 102757.
10. Seck, M.; Ciss, A.A. A New Generalized Lattice Attack Against a Family of RSA-Like Cryptosystems. *Theor. Comput. Sci.* **2025**, *1055*, 115548.
11. Shi, G.; Wang, G.; Gu, D. Further Cryptanalysis of a Type of RSA Variants. In *Information Security*; Susilo, W., Chen, X., Guo, F., Zhang, Y., Intan, R., Eds.; ISC 2022, Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2022; Volume 13640.
12. Rahmani, M.; Nitaj, A.; Ziane, M. Partial exposure attacks on new RSA variant. *Cryptography* **2024**, *8*, 44.
13. Cotan, P.; Teşeleanu, G. Small private key attack against a family of RSA-like cryptosystems. In *Nordic Conference on Secure IT Systems 2023*; Lecture Notes in Computer Science; NordSec: Vilnius, Lithuania, 2023; pp. 57–72.
14. Teşeleanu, G.; Cotan, P. *Continued Fractions Applied to a Family of RSA-like Cryptosystems*; Cryptology ePrint Archive, Paper 2022/1241. 2022. Available online: <https://eprint.iacr.org/2022/1241> (accessed on 5 July 2026)
15. Castagnos, G. An efficient probabilistic public-key cryptosystem over quadratic fields quotients. *Finite Fields Their Appl.* **2007**, *13*, 563–576.
16. Kuwakado, H.; Koyama, K.; Tsuruoka, Y. A New RSA-type scheme based on singular cubic curves with equation $y^2 \equiv x^3 + bx^2 \pmod{N}$. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **1995**, *78*, 27–33.
17. 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*; IEEE: New York, NY, USA, 2002; Volume 1, pp. 91–95.
18. Said, M.R.M.; Loxton, J. A cubic analogue of the RSA cryptosystem. *Bull. Aust. Math. Soc.* **2003**, *68*, 21–38.
19. Petukhova, K.A.; Tronin, S.N. RSA cryptosystem for Dedekind rings. *Lobachevskii J. Math.* **2016**, *37*, 284–287. <https://doi.org/10.1134/S1995080216030197>.

20. Takagi, T.; Naito, S. Construction of RSA cryptosystem over the algebraic field using ideal theory and investigation of its security. *Electron. Commun. Jpn. Part III Fundam. Electron. Sci.* **2015**, *83*, 19–29.
21. Zheng, Z.; Liu, F. On the high dimensional RSA algorithm-A public key cryptosystem based on lattice and algebraic number theory. In *International Forum on Financial Mathematics and Financial Technology*; Springer Nature: Singapore, 2021; pp. 169–189.
22. Nasrutdinov, M.F.; Tronin, S.N. RSA cryptosystem for rings with commuting ideals. *Lobachevskii J. Math.* **2022**, *43*, 3591–3596.
23. Murru N.; Saettone F.M. A Novel RSA-Like Cryptosystem Based on a Generalization of the Rédei Rational Functions. In *Number-Theoretic Methods in Cryptology*; Kaczorowski J., Pieprzyk J., Pomykala J., Eds.; NuTMiC 2017, Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2018; Volume 10737.
24. Lenstra, A.K.; Lenstra, H.W.; Lovász, L. Factoring polynomials with rational coefficients. *Math. Ann.* **1982**, *261*, 513–534.
25. May, A. New RSA Vulnerabilities Using Lattice Reduction Methods. Ph.D. Thesis, University of Paderborn, Paderborn, Germany, 2003.
26. Howgrave-Graham, N. Finding small roots of univariate modular equations revisited. In *Cryptography and Coding*; Lecture Notes in Computer Science; Springer-Verlag: Berlin, Germany, 1997; Volume 1355, pp. 131–142.
27. Jochemsz, E.; May, A. A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants. In *ASIACRYPT 2006*; Lecture Notes in Computer Science; Springer-Verlag: Berlin, Germany, 2006; Volume 4284, pp. 267–282.
28. Zheng, M.; Kunihiro, N.; Yao, Y. Cryptanalysis of the RSA variant based on cubic Pell equation. *Theor. Comput. Sci.* **2021**, *889*, 135–144.
29. Peng, L.; Hu, L.; Lu, Y.; Wei, H. An improved analysis on three variants of the RSA cryptosystem. *Int. Conf. Inf. Secur. Cryptol.* **2016**, *10143*, 140–149.

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