A refined cryptanalytic attack against a generalized cubic Pell RSA scheme

Brahim Chnioune[a], Mohammed Rahmani[a,*], Abderrahmane Nitaj[b], Mhammed Ziane[a]

[a] *Mohammed I University, Sciences Faculty, Department of Mathematics, ACSA Laboratory, Oujda, 60000, Morocco*
[b] *Normandie Univ, UNICAEN, CNRS, LMNO, Caen, 14000, France*

Abstract

In 2022, Cotan and Teşeleanu proposed an alternative RSA construction in which the modulus takes the form $N = pq$ and the exponents (e, d) are linked through $ed - 1 \equiv 0 \pmod{\psi_n(N)},\ n \geq 2$, where $\psi_n(N) = \frac{(p^n-1)(q^n-1)}{(p-1)(q-1)}$. Their scheme was subsequently examined by Nitaj et al. at Africacrypt 2024, who demonstrated that the system becomes vulnerable when the secret exponent d is less than $N^{0.292(n-1)}$. In the present work, we extend this line of cryptanalysis by developing a lattice-based technique targeting the same key congruence. Our approach succeeds in recovering the private parameters even for secret exponents greater than $N^{0.292(n-1)}$, thereby surpassing the previously known boundary. The factorization of N is achieved in polynomial time, provided that its divisors p and q share a suitably portion of their least significant bits.

Keywords:
RSA, Generalized cubic Pell RSA variant, Integer factorization, Coppersmith's method, LLL reduction algorithm
2020 MSC: 94A60, 11T71

*Corresponding author
Email addresses: brahim.chnioune.d24@ump.ac.ma (Brahim Chnioune), mohammed.rahmani@ump.ac.ma (Mohammed Rahmani), abderrahmane.nitaj@unicaen.fr (Abderrahmane Nitaj), m.ziane@ump.ac.ma (Mhammed Ziane)

1. Introduction

Originally introduced in 1978, the RSA encryption scheme [28] has become a cornerstone in the realm of public-key cryptography, largely due to its extensive practical applications and widespread use. Its security relies on the computational difficulty of factoring large moduli. To set up RSA, one generates two large primes p and q of comparable bit length and defines the modulus $N = pq$. An integer e, referred to as the encryption exponent, is then chosen so that $\gcd(e, (p-1)(q-1)) = 1$. Under this condition, the corresponding secret exponent d is obtained by inverting e modulo $(p-1)(q-1)$.

The encryption process maps a message m to a ciphertext c as $c \equiv m^e \pmod{N}$, while decryption reverses the process by applying $m \equiv c^d \pmod{N}$. The practical performance of both operations depends essentially on the efficiency of modular exponentiation. In an effort to speed up decryption, one might be tempted to select a relatively small private exponent. However, Wiener's landmark result from 1990 [33] demonstrated that RSA becomes insecure when $d \leq \frac{1}{3}N^{1/4}$. This limitation was subsequently strengthened by Boneh and Durfee [2], who extended the vulnerability range up to private exponents of size roughly $N^{0.292}$.

Motivated by the inherent performance and security constraints of the classical RSA protocol, a wide range of alternative constructions has emerged. Certain proposals maintain the conventional modulus $N = pq$, among them CRT-RSA [23], rebalanced RSA [33], and the KMOV scheme [11]. Other designs modify the structure of the modulus altogether, such as Multi-Prime RSA [3], which extends N to a product of several primes, or Prime-Power RSA [32], where the modulus consists of prime powers.

A further development appeared, when Murru and Saettone [15] proposed an RSA-like construction based on the cubic Pell curve

$$x^3 + \nu y^3 + \nu^2 z^3 - 3\nu xyz = 1,$$

where ν is selected as a cubic non-residue modulo N. Their scheme keeps the modulus $N = pq$, but modifies the key generation procedure: the exponents (e, d) are subject to the condition

$$ed - 1 \equiv 0 \pmod{(p^2 + p + 1)(q^2 + q + 1)}.$$

Since its introduction, this variant has been the subject of extensive cryptanalytic studies [34, 29, 7, 25].

In [5], Cotan and Teşeleanu presented an extended construction of the above scheme. Their framework still employs the modulus $N = pq$, but extends the key relation by choosing exponents e and d such that

$$ed - 1 \equiv 0 \pmod{\frac{(p^n - 1)(q^n - 1)}{(p-1)(q-1)}}, \text{ for } n \geq 2.$$

The instance $n = 3$ specializes to the scheme of Murru and Saettone.

Both the RSA cryptosystem and its variants have attracted significant attention in cryptanalysis. Beyond the classical attacks of Wiener and Boneh–Durfee, many other attacks have been developed. In 2004, Steinfeld and Zheng [31] analyzed the security of RSA when the prime factors share a certain number of their least significant bits (LSBs) under partial key exposure attacks. Later, Sun et al. [30] revisited the analysis and gave more explicit bounds.

According to Cotan and Teşeleanu [5, 6], one can mount an attack on the Cotan-Teşeleanu scheme using continued fractions provided that $e = N^{\alpha}$, $d = N^{\delta}$, the constraint $\alpha \leq n - \frac{1}{2}$ holds, and $d < N^{\frac{n}{2} - \frac{\alpha}{2} - \frac{1}{4}}$. In 2024, Nitaj et al. [21] introduced a refined lattice-based cryptanalytic technique for attacking the Cotan–Teşeleanu scheme. In particular, they proved that for all $n \geq 2$, the modulus $N = pq$ can be factored whenever $d < N^{n-1-\sqrt{0.5(n-1)\alpha}}$, which significantly strengthens the earlier bound $d < N^{\frac{n}{2} - \frac{\alpha}{2} - \frac{1}{4}}$, established by Cotan and Teşeleanu.

In 2025, Rahmani et al. [27] extended the cryptanalysis of Nitaj et al. [21] by examining the more general key equation

$$eu - x\psi_n(N) = z,$$

where the integers u and z are assumed to be small. Based on this approach, they proved that the prime factors as well as larger decryption exponents can be recovered in polynomial time whenever

$$|u| < N^{\delta}, \quad |z| < N^{\beta}, \quad |z| < e|u|, \quad |z| < |x||y|^{n-1} < e,$$

and the parameters satisfy

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

In this work, we investigate the relation $ed - k\psi_n(N) = 1$, under the assumption that the prime factors p and q share ℓ LSBs. More precisely,

depending on whether e is odd or even, we transform the former equation into one of the following forms:

$$xG_n(y) + \kappa \equiv 0 \pmod{e},$$

or

$$xH_n(z) - ey + 1 = 0,$$

where $G_n(y)$ and $H_n(z)$ are specific polynomials derived from $\psi_n(N)$.

Under the following setting

$$e = N^{\alpha}, \qquad d < N^{\delta}, \qquad 2^{\ell} = N^{\gamma}, \qquad \gamma < \tfrac{1}{4},$$

our analysis shows that, in each case, solving this type of equation allows us to recover the secret parameters (d, p, q), provided that the pair (α, δ) lies in one of the following two regions

1. $$0 \le \alpha \le \frac{(n-1)(1-4\gamma)}{2} \text{ and } \delta \le \frac{(n-1)(1+4\gamma)}{2}.$$
2. $$\frac{(n-1)(1-4\gamma)}{2} < \alpha < \frac{(n-1)(4\gamma+5)(3-4\gamma)}{8(1-4\gamma)},$$

   and

$$\delta < \frac{\sqrt{n-1}}{6}\left((7-4\gamma)\sqrt{n-1} - 2\sqrt{(1-4\gamma)\left(6\alpha + (n-1)(1-4\gamma)\right)}\right).$$

Notice that the former bound matches that obtained by Rahmani et al. [24] for attacks on schemes based on the key equation $ed - k\psi_n(N) = 1$ with odd public exponents e. Moreover, our attack extends their approach to the case of even public exponents satisfying the same key equation.

It is worth noting that the best known bound on small secret exponents for cryptosystems governed by the key relation $ed - k\psi_n(N) = 1$ was derived by Nitaj et al. [21]. This bound is attained when the public exponent satisfies $e \approx N^{n-1}$, i.e., $\alpha \approx n-1$. In this scenario, the private exponent d is recoverable if

$$d < N^{\left(1-\frac{\sqrt{2}}{2}\right)(n-1)} \approx N^{0.292(n-1)}.$$

In contrast, our implementation achieves new improved bounds as the parameter γ increases within the interval $(0, 1/4)$. For example, in the typical

setting where $\gamma \approx 0.1$ and $e \approx N^{n-1}$, our method enables the recovery of secret exponents even when they lie in the extended range

$$N^{0.292(n-1)} < d < N^{\frac{11-2\sqrt{11}}{10}(n-1)} \approx N^{0.436(n-1)}.$$

Note also that the attack of Rahmani et al. [27] on the RSA variants with the generalized equation $eu - x\psi_n(N) = z$, for suitably small values of z and u, is based on solving the modular equation

$$xH(y) + z \equiv 0 \pmod{e},$$

under the constraint $|z| < |x|\,|y|^{n-1}$. In contrast, our construction considers the case where $z = z_0 = \kappa$ is a fixed constant and relaxes this restriction by allowing larger values satisfying

$$|z_0| > |x|\,|y|^{n-1},$$

while still enabling an efficient resolution of

$$xH(y) + z_0 \equiv 0 \pmod{e},$$

which allows us to target more instances of such variants.

The structure of this paper is outlined as follows. Section 2 reviews the necessary background and summarizes the fundamental tools used throughout. Section 3 describes how Coppersmith's method can be adapted to compromise the proposed RSA variant. Section 4 compares our attack with the existing ones. Section 5 presents two detailed numerical examples validating the attack, and Section 6 concludes our proposed attack.

2. Background

2.1. Useful lemmas

Building on techniques introduced in [16], the lemma below derives concrete bounds for the two primes p and q forming the RSA modulus $N = pq$, assuming a balanced configuration where $q < p < 2q$.

Lemma 1. *For an RSA modulus $N = pq$ with $q < p < 2q$, the two prime factors are forced into the following interval:*

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

The result below demonstrates that, when the primes p and q of an RSA modulus differ by a quantity of the form $p - q = 2^{\ell}w$, where the exponent ℓ is known, one can reconstruct the ℓ LSBs of both primes and, moreover, the 2ℓ LSBs of the prime sum $p + q$ (see [17]).

Lemma 2. *Assume $N = pq$ with prime factors p and q constrained by $q < p < 2q$, and assume that their difference can be written as*

$$p - q = 2^{\ell}w,$$

where the parameter ℓ is known but w is not. Let w_0 denote a solution to

$$x^2 - N \equiv 0 \pmod{2^{\ell}},$$

and define

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

Then there exist three unknowns p_0, q_0, and v such that

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

The generalized cubic totient function [5] for $N = pq$ is defined as

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

With the notation introduced in the previous lemma, the next statement provides a recursive method for computing $\psi_n(N)$ in terms of v (see [21]).

Lemma 3. *The function $\psi_n(N)$ satisfies*

1. $\psi_1(N) = 1$.
2. $\psi_2(N) = N + 1 + 2^{2\ell}v + v_0$.
3. *For each $n \geq 3$, one has*

$$\psi_n(N) = \psi_{n-1}(N)(2^{2\ell}v + v_0) - \psi_{n-2}(N)N + N^{n-1} + 1.$$

For instance, we have

$$\begin{aligned}
\psi_3(N) &= 2^{4\ell}v^2 + (2^{2\ell}N + 2^{2\ell+1}v_0 + 2^{2\ell})v + N^2 + Nv_0 + v_0^2 - N + v_0 + 1,\\
\psi_4(N) &= 2^{6\ell}v^3 + \big(2^{4\ell}(N + 3v_0 + 1)\big)v^2\\
&\quad + \big(2^{2\ell}N^2 + 2^{2\ell+1}Nv_0 + 3\cdot 2^{2\ell}v_0^2 - 2^{2\ell+1}N + 2^{2\ell+1}v_0 + 2^{2\ell}\big)v\\
&\quad + \big(N^3 + N^2v_0 + Nv_0^2 + v_0^3 - N^2 - 2Nv_0 + v_0^2 - N + v_0 + 1\big),\\
\psi_5(N) &= 2^{8\ell}v^4 + \big(2^{6\ell}N + 4\cdot 2^{6\ell}v_0 + 2^{6\ell}\big)v^3\\
&\quad + \big(2^{4\ell}N^2 + 3\cdot 2^{4\ell}Nv_0 + 6\cdot 2^{4\ell}v_0^2 - 3\cdot 2^{4\ell}N + 3\cdot 2^{4\ell}v_0 + 2^{4\ell}\big)v^2\\
&\quad + \big(2^{2\ell}N^3 + 2^{2\ell+1}N^2v_0 + 3\cdot 2^{2\ell}Nv_0^2 + 4\cdot 2^{2\ell}v_0^3 - 2^{2\ell+1}N^2\\
&\quad - 6\cdot 2^{2\ell}Nv_0 + 3\cdot 2^{2\ell}v_0^2 - 2^{2\ell+1}N + 2^{2\ell+1}v_0 + 2^{2\ell}\big)v\\
&\quad + \big(N^4 + N^3v_0 + N^2v_0^2 + Nv_0^3 + v_0^4 - N^3 - 2N^2v_0 - 3Nv_0^2\\
&\quad + v_0^3 + N^2 - 2Nv_0 + v_0^2 - N + v_0 + 1\big).
\end{aligned}$$

A direct consequence of the previous recursive way is that, by employing induction on n, the generalized cubic totient $\psi_n(N)$ admits a polynomial representation in v with integer coefficients. This can be summarized as follows.

Lemma 4. *For any $n \geq 2$, there are integers $c_k \in \mathbb{Z}$, $0 \leq k \leq n-2$, determined by the combination (n, N, ℓ, v_0) for which*

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

Notice that although the coefficients c_k can be computed from (n, N, ℓ, v_0), the attacker still faces the challenge of determining the unknown value v in order to compute $\psi_n(N)$.

2.2. The generalized cubic Pell RSA scheme

Cotan and Teșeleanu [5] put forward a generalized form of the Murru-Saettone cryptosystem [15] in 2022. Before proceeding, it is necessary to introduce some related mathematical objects.

Consider a field $(\mathbb{F}, +, \cdot)$, a positive integer n, and an element $\beta \in \mathbb{F}$ such that the polynomial $x^n - \beta$ is irreducible over $\mathbb{F}[x]$. Let

$$\mathcal{C}_n = \mathbb{F}[x]/(x^n - \beta),$$

denote the corresponding quotient field. Each element of $\mathcal{C}_n$ may be expressed as

$$\beta_0 + \beta_1 x + \cdots + \beta_{n-1} x^{n-1}, \quad \beta_i \in \mathbb{F}.$$

Let $\mathfrak{p} = \sum_{i=0}^{n-1} \gamma_i x^i$ and $\mathfrak{q} = \sum_{i=0}^{n-1} \beta_i x^i$ be elements of $\mathcal{C}_n$. Their product in $\mathcal{C}_n$ is given by

$$\mathfrak{p}\mathfrak{q} = \sum_{a=0}^{n-2} \left(\sum_{b=0}^{a} \gamma_b \beta_{a-b} + \beta \sum_{b=0}^{a+n} \gamma_b \beta_{a-b+n} \right) x^a + \sum_{b=0}^{n-1} \gamma_b \beta_{n-1-b} x^{n-1}.$$

Subsequently, define the quotient group $\mathcal{D}_n = \mathcal{C}_n^*/\mathbb{F}^*$. The elements of this group are equivalence classes of the type

$$\left\{ \alpha\beta_0 + \alpha\beta_1 x + \cdots + \alpha\beta_{n-1} x^{n-1} \,\middle|\, \alpha \in \mathbb{F}^*,\ \beta_i \in \mathbb{F},\ i = 0, \ldots, n-1 \right\}.$$

It can be observed that $\mathcal{D}_n$ can be partitioned in the following manner. For every $\mathfrak{p} \in \mathcal{D}_n$, there exist scalars $\beta_0, \ldots, \beta_{t-1} \in \mathbb{F}$ and a unique integer $t < n$ such that

$$\mathfrak{p} = \beta_0 + \beta_1 x + \cdots + \beta_{t-1} x^{t-1} + x^t.$$

In the context of cryptographic applications, let $\mathbb{F} = \mathbb{F}_p$ be the finite field with p elements, where p is a prime number. Thus, $\mathcal{C}_n$ is a Galois field of order p^n, and $\mathcal{D}_n$ is of order

$$\#\mathcal{D}_n = \frac{p^n - 1}{p - 1}.$$

For any positive integer s and element $\mathfrak{p} \in \mathcal{D}_n$, the notation $\mathfrak{p}^s$ refers to the repeated product of $\mathfrak{p}$ with itself s times. Therefore, an analogue of Fermat's little theorem asserts that

$$\mathfrak{p}^{\#\mathcal{D}_n} \equiv 1 \pmod{p}, \text{ for } \mathfrak{p} \in \mathcal{D}_n.$$

Let $N = pq$, where p and q are prime numbers. The constructions introduced above can be extended to the ring $\mathbb{Z}_N = \mathbb{Z}/N\mathbb{Z}$. In this context, the size of $\mathcal{D}_n$ is given by

$$\psi_n(N) = \#\mathcal{D}_n = \frac{(p^n - 1)(q^n - 1)}{(p - 1)(q - 1)},$$

and for all $\mathfrak{p} \in \mathcal{D}_n$, one has

$$\mathfrak{p}^{\#\mathcal{D}_n} \equiv 1 \pmod{N}.$$

The Cotan–Teşeleanu scheme operates over the group $\mathcal{D}_n$ and can be formally described as follows.

Key generation process

1. Select an integer $n > 1$ and a security parameter $r > 0$.
2. Randomly generate two distinct large prime numbers p and q, each having bit-length r.
3. Compute $N = pq$ and the generalized cubic totient
$$\psi_n(N) = \frac{(p^n - 1)(q^n - 1)}{(p - 1)(q - 1)}.$$
4. Choose an integer β such that the polynomial $x^n - \beta$ is irreducible over the rings $\mathbb{F}_p[x]$, $\mathbb{F}_q[x]$, and $\mathbb{Z}_N[x]$.
5. Select an integer e satisfying $\gcd(e, \psi_n(N)) = 1$, and determine d as the multiplicative inverse of e modulo $\psi_n(N)$.
6. Publish the tuple (N, n, β, e), while keeping (p, q, d) confidential.

Encryption process

To encrypt a message, the plaintext is first encoded as a polynomial in $\mathcal{D}_n$:
$$\mathfrak{m} = \beta_0 + \beta_1 x + \cdots + \beta_{t-1} x^{t-1} + x^t, \quad t < n,$$
where the coefficients $\beta_0, \ldots, \beta_{t-1} \in \mathbb{Z}_N$ represent the message.

The ciphertext is then obtained by exponentiation in $\mathcal{D}_n$ modulo N, replacing any occurrence of x^n with β according to the algebraic structure:
$$\mathfrak{c} \equiv \mathfrak{m}^e \pmod{N}.$$
The resulting encrypted message is the polynomial $\mathfrak{c}$.

Decryption process

To recover the plaintext polynomial $\mathfrak{m}$, compute
$$\mathfrak{m} \equiv \mathfrak{c}^d \pmod{N},$$
replacing any occurrence of x^n with β according to the algebraic structure of $\mathcal{D}_n$.

Remark 1. Using the well-known identity
$$\sum_{i=0}^{n-1} x^i = \frac{x^n - 1}{x - 1},$$

we obtain

$$\psi_n(N) = \left(\sum_{i=0}^{n-1} p^i\right)\left(\sum_{i=0}^{n-1} q^i\right).$$

Since p and q are odd primes, each sum $\sum_{i=0}^{n-1} p^i$ and $\sum_{i=0}^{n-1} q^i$ has the same parity as n. Consequently, we deduce that

$$\begin{aligned} \psi_n(N) \text{ is even} &\iff n \text{ is even}, \\ \psi_n(N) \text{ is odd} &\iff n \text{ is odd}. \end{aligned}$$

Remark 2. From the key generation process, we have $\gcd(e, \psi_n(N)) = 1$. This implies that:

1. If e is even, then $\psi_n(N)$ must be odd, which in turn implies that n is odd.
2. If e is odd, the condition $\gcd(e, \psi_n(N)) = 1$ does not impose any restriction on the parity of $\psi_n(N)$. Consequently, n may be either even or odd.

2.3. LLL reduction

Let $\mathcal{L} \subset \mathbb{R}^d$ be a lattice spanned by $r \leq d$ linearly independent vectors $\mathbf{f}_1, \ldots, \mathbf{f}_r$. In other words, $\mathcal{L} = \mathbb{Z}\mathbf{f}_1 + \cdots + \mathbb{Z}\mathbf{f}_r$. The family $(\mathbf{f}_1, \ldots, \mathbf{f}_r)$ constitutes a basis of $\mathcal{L}$, and we denote by M the associated basis matrix whose rows are the $\mathbf{f}_j$'s. The integer r is the rank of the lattice. The determinant of $\mathcal{L}$, representing the volume of a fundamental parallelepiped generated by the basis vectors, is given by $\det(\mathcal{L}) = \sqrt{\det(MM^\top)}$. In the special case where the lattice has full rank, i.e., $r = d$, this reduces to $\det(\mathcal{L}) = |\det(M)|$.

For any lattice of rank $r \geq 2$, one can form infinitely many different bases; each basis contains the same number of vectors and leads to the same lattice determinant. As the dimension grows, it becomes increasingly challenging to find a basis made of vectors that are both short and nearly orthogonal. The LLL algorithm [12] provides an efficient way to obtain such a basis in polynomial time. More detailed properties and bounds for LLL-reduced bases are discussed in [14].

Theorem 1. *For every lattice $\mathcal{L}$ spanned by a basis $\{\mathbf{f}_1, \ldots, \mathbf{f}_r\}$, the application LLL algorithm outputs a basis $\{\mathbf{e}_1, \ldots, \mathbf{e}_r\}$ for which*

$$\|\mathbf{e}_1\| \leq \|\mathbf{e}_2\| \leq \cdots \leq \|\mathbf{e}_j\| \leq 2^{\frac{r(r-1)}{4(r+1-j)}} \det(\mathcal{L})^{\frac{1}{r+1-j}}, \quad j \in \{1, \ldots, r\}.$$

2.4. Finding small roots to modular equations

Coppersmith's groundbreaking work in 1996 [4] introduced a polynomial-time technique for computing small integer solutions of a univariate polynomial congruence

$$g(x) = \sum_{j=0}^{k} a_j x^j \equiv 0 \pmod{M},\ a_j \in \mathbb{Z},$$

even when the modulus M is given without revealing its factorization. This approach was later extended to the multivariate setting, enabling the treatment of modular polynomial equations of the form

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

with integer coefficients $a_{j_1,\ldots,j_n}$.

The Euclidean norm associated with the polynomial G is defined to be

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

In 1997, Howgrave–Graham [8] proposed a refined variant of Coppersmith's technique. He formulated a sufficient criterion ensuring that the small roots of a multivariate polynomial modulo an integer correspond exactly to its integer solutions. This result is presented in the following statement:

Theorem 2 (Howgrave–Graham)**.** *Let $G(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ with at most r nonzero monomials, and let $E > 0$ be an integer. Assume there exist integers $u_1, \ldots, u_n$ and positive bounds $U_1, \ldots, U_n$ such that:*

1. $G(u_1, \ldots, u_n) \equiv 0 \pmod{E}$.
2. $\|G(x_1U_1, \ldots, x_nU_n)\| < \frac{E}{\sqrt{r}}$.
3. $|u_i| < U_i$ *for each* $i \in \{1, \ldots, n\}$.

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

For polynomials in three or more variables, algorithms inspired by Coppersmith's approach are typically heuristic. In these settings, the following assumption is frequently adopted [2, 9, 22, 34].

Assumption 1. *The polynomials $G_1, G_2, \ldots, G_r$ generated by the LLL reduction form an algebraically independent collection, that is, for every polynomial $P \in \mathbb{Z}[x_1, \ldots, x_r]$, if $P(G_1, G_2, \ldots, G_r) = 0$, then $P = 0$.*

Assuming the above, the common root $(u_1, \ldots, u_n)$ of the equations

$$G_i(x_1, \ldots, x_n) = 0, \quad i \in \{1, \ldots, r\},$$

may be obtained using tools such as Gröbner bases or resultants.

3. Our cryptanalytic result

In this section, we develop a cryptanalytic method aimed at the scheme of Cotan and Teşeleanu [5], assuming that the underlying RSA primes share a specified number of LSBs.

Theorem 3. *Let $n \geq 2$ be an integer, and consider an RSA modulus $N = pq$ with primes satisfying $q < p < 2q$. Let $e = N^\alpha$ be a public encryption exponent. Assume there exist integers d and t such that*

$$ed - t\,\psi_n(N) = 1,\ d < N^\delta,\ \text{where } \psi_n(N) = \frac{(p^n-1)(q^n-1)}{(p-1)(q-1)}.$$

Assume also that the primes p and q share their ℓ LSBs, with $2^\ell = N^\gamma$ for some $\gamma \in [0, \frac{1}{4})$. Under these assumptions, the modulus N can be factored in polynomial time if one of the following situations occurs:

1. $$0 \leq \alpha \leq \frac{(n-1)(1-4\gamma)}{2} \text{ and } \delta \leq \frac{(n-1)(1+4\gamma)}{2}.$$
2. $$\frac{(n-1)(1-4\gamma)}{2} < \alpha < \frac{(n-1)(4\gamma+5)(3-4\gamma)}{8(1-4\gamma)},$$

   and

   $$\delta < \frac{\sqrt{n-1}}{6}\left((7-4\gamma)\sqrt{n-1} - 2\sqrt{(1-4\gamma)\left(6\alpha + (n-1)(1-4\gamma)\right)}\right).$$

Proof. We consider two cases following the parity of e.
Case 1: Assume that e is odd. Then we perform a similar analysis to that presented in [26] where the equation is $ed - k\,(p^n-1)\,(q^n-1) = 1$. Assume

then that the RSA primes p and q share ℓ LSBs, then their prime difference fulfills $p - q = 2^{\ell}w$, for some $w \in \mathbb{Z}$. Let w_0 be an integer such that

$$w_0^2 - N \equiv 0 \pmod{2^{\ell}},$$

and define

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

Then, by Lemma 2, we find that $p + q = 2^{2\ell}v + v_0$ for some unknown integer v. Moreover, Lemma 4 allows us to expand $\psi_n(N)$ as

$$\psi_n(N) = 2^{2(n-1)\ell}v^{n-1} + \sum_{0 \le i \le n-2} c_i v^i. \tag{1}$$

Since $\gcd(e, 2) = 1$, we may define

$$\kappa \equiv 2^{-2(n-1)\ell} \pmod{e}.$$

Inserting this expression for $\psi_n(N)$ into the fundamental key equation

$$ed - t\psi_n(N) = 1,$$

yields the congruence

$$t\left(2^{2(n-1)\ell}v^{n-1} + \sum_{0 \le i \le n-2} c_i v^i\right) + 1 \equiv 0 \pmod{e},$$

which can be reformulated equivalently as

$$tv^{n-1} + \sum_{0 \le i \le n-2} \kappa c_i t v^i + \kappa \equiv 0 \pmod{e}.$$

With this setup, we can focus on identifying small solutions to the corresponding bivariate modular equation

$$R_n(t, v) \equiv 0 \pmod{e},$$

where

$$R_n(x, y) = xy^{n-1} + \sum_{0 \le i \le n-2} \kappa c_i x y^i + \kappa.$$

In order to recover the modular root (t, v) of the preceding congruence, we utilize Coppersmith's technique. For this, an auxiliary positive parameter

$\xi > 0$ is introduced and will be optimized in due course. Two integers ν and k, with $0 \le k \le \nu$, are chosen to define a family of bivariate polynomials

$$R_{k,r,s}^{(n)}(x,y) = x^r y^s R_n(x,y)^k e^{\nu-k}, \quad (k,r,s) \in \mathcal{M} \cup \mathcal{N},$$

where $\mathcal{M}$ and $\mathcal{N}$ are defined as follows

$$\mathcal{M} = \left\{(k,r,s) \in \mathbb{Z}^3 \mid 0 \le k \le \nu,\ 1 \le r \le \nu - k,\ 0 \le s \le n-2\right\},$$
$$\mathcal{N} = \left\{(k,r,s) \in \mathbb{Z}^3 \mid 0 \le k \le \nu,\ r = 0,\ 0 \le s \le \lfloor \nu\xi \rfloor\right\}.$$

Since

$$R_n(t,v) \equiv 0 \pmod{e},$$

it follows that

$$R_{k,r,s}^{(n)}(t,v) \equiv 0 \pmod{e^\nu},$$

for all $(k,r,s) \in \mathcal{M} \cup \mathcal{N}$.

Within the framework of Coppersmith's method, it is crucial to establish suitable upper bounds X and Y so that

$$|t| \le X, \qquad |v| \le Y.$$

Since p and q are large, we can approximate $p-1 \approx p$ and $q-1 \approx q$. Therefore, we obtain the approximation

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

Given that $e = N^\alpha$, $d < N^\delta$ and $ed > 1$, it follows that

$$t = \frac{ed-1}{\psi_n(N)} < 2N^{\alpha+\delta+1-n}.$$

From the relations $p + q = 2^{2\ell}v + v_0$, $2^\ell = N^\gamma$, and the bound $p + q < 3\sqrt{N}$ in Lemma 1, it immediately follows that

$$v = \frac{p+q-v_0}{2^{2\ell}} < 3\,N^{\frac{1}{2}-2\gamma}.$$

If $\gamma \ge \frac{1}{4}$, then v is constrained to take values in $\{1,2\}$, and the relation

$$p + q = 2^{2\ell}v + v_0,$$

immediately provides a factorization of N.

Therefore, we can restrict our attention to $\gamma < \frac{1}{4}$, which allows us to set

$$X = 2N^{\alpha+\delta+1-n}, \qquad Y = 3N^{\frac{1}{2}-2\gamma}. \tag{2}$$

We proceed by generating the lattice $\mathcal{L}$ from the matrix of coefficient vectors corresponding to $R^{(n)}_{k,r,s}(xX, yY)$. To ease the computation of the lattice determinant, the matrix is preferably transformed into a lower or upper triangular form, which is accomplished via an appropriate ordering of rows and columns. In our analysis, we follow the procedure in [9] to make the matrix of the lattice lower triangular. To achieve this, each row of the lattice basis corresponds to a polynomial of the form

$$R^{(n)}_{k,r,s}(xX, yY),$$

where the rows are arranged according to the lexicographical order of the indices (k, r, s). Similarly, the columns, which correspond to the monomials $x^{r+k}y^{s+k(n-1)}$, are ordered based on the same lexicographical ordering of (k, r, s). As an illustration, Table 1 displays the structure of the matrix generating the lattice for $\nu = 2$, $\xi = 1$, and $n = 4$ where the symbol $\star$ indicates the positions of the nonzero entries.

Owing to the triangular form of the matrix, each diagonal entry can be represented as

$$X^{r+k}Y^{s+(n-1)k}e^{\nu-k},$$

for some tuple $(k, r, s) \in \mathcal{M} \cup \mathcal{N}$. Thus, the determinant of $\mathcal{L}$ admits the following expression

$$\det(\mathcal{L}) = X^{\theta_X}Y^{\theta_Y}e^{\theta_e}, \tag{3}$$

with $\theta_X = f(r + k)$, $\theta_Y = f(s + (n - 1)k)$, $\theta_e = f(\nu - k)$, and the function f is given by

$$f(a) = \sum_{k=0}^{\nu}\sum_{r=1}^{\nu-k}\sum_{s=0}^{n-2} a + \sum_{k=0}^{\nu}\sum_{r=0}^{0}\sum_{s=0}^{\lfloor\nu\xi\rfloor} a,$$

where the summation ranges over the index set $\mathcal{M} \cup \mathcal{N}$.

In order to simplify the analysis, we take $\lfloor\nu\xi\rfloor \approx \nu\xi$. Consequently, the exponents θ_X, θ_Y, and θ_e, as well as the lattice dimension $\mathscr{D} = f(1)$, satisfy the asymptotic relations presented below for sufficiently large ν

$R^{(4)}_{k,r,s}$	1	y	y^2	x	xy	xy^2	x^2	x^2y	x^2y^2	xy^3	xy^4	xy^5	x^2y^3	x^2y^4	x^2y^5	x^2y^6	x^2y^7	x^2y^8
$R^{(4)}_{0,0,0}$	e^2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$R^{(4)}_{0,0,1}$	0	e^2Y	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$R^{(4)}_{0,0,2}$	0	0	e^2Y^2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$R^{(4)}_{0,1,0}$	0	0	0	e^2X	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$R^{(4)}_{0,1,1}$	0	0	0	0	e^2XY	0	0	0	0	0	0	0	0	0	0	0	0	0
$R^{(4)}_{0,1,2}$	0	0	0	0	0	e^2XY^2	0	0	0	0	0	0	0	0	0	0	0	0
$R^{(4)}_{0,2,0}$	0	0	0	0	0	0	e^2X^2	0	0	0	0	0	0	0	0	0	0	0
$R^{(4)}_{0,2,1}$	0	0	0	0	0	0	0	e^2X^2Y	0	0	0	0	0	0	0	0	0	0
$R^{(4)}_{0,2,2}$	0	0	0	0	0	0	0	0	$e^2X^2Y^2$	0	0	0	0	0	0	0	0	0
$R^{(4)}_{1,0,0}$	$\star$	0	0	$\star$	$\star$	$\star$	0	0	0	eXY^3	0	0	0	0	0	0	0	0
$R^{(4)}_{1,0,1}$	0	$\star$	0	0	$\star$	$\star$	0	0	0	$\star$	eXY^4	0	0	0	0	0	0	0
$R^{(4)}_{1,0,2}$	0	0	$\star$	0	0	$\star$	0	0	0	$\star$	$\star$	eXY^5	0	0	0	0	0	0
$R^{(4)}_{1,1,0}$	0	0	0	$\star$	0	0	$\star$	$\star$	$\star$	0	0	0	eX^2Y^3	0	0	0	0	0
$R^{(4)}_{1,1,1}$	0	0	0	0	$\star$	0	0	$\star$	$\star$	0	0	0	$\star$	eX^2Y^4	0	0	0	0
$R^{(4)}_{1,1,2}$	0	0	0	0	0	$\star$	0	0	$\star$	0	0	0	$\star$	$\star$	eX^2Y^5	0	0	0
$R^{(4)}_{2,0,0}$	$\star$	0	0	$\star$	$\star$	$\star$	$\star$	$\star$	$\star$	$\star$	0	0	$\star$	$\star$	$\star$	X^2Y^6	0	0
$R^{(4)}_{2,0,1}$	0	$\star$	0	0	$\star$	$\star$	0	$\star$	$\star$	$\star$	$\star$	0	$\star$	$\star$	$\star$	$\star$	X^2Y^7	0
$R^{(4)}_{2,0,2}$	0	0	$\star$	0	0	$\star$	0	0	$\star$	$\star$	$\star$	$\star$	$\star$	$\star$	$\star$	$\star$	$\star$	X^2Y^8

Table 1: The matrix generating the lattice for $(n, \nu, \xi) = (4, 2, 1)$.

$$
\begin{aligned}
\theta_X &= \frac{1}{6}(2n + 3\xi - 2)\nu^3 + o(\nu^3), \\
\theta_Y &= \frac{1}{6}(n^2 + 3n\xi + 3\xi^2 - 2n - 3\xi + 1)\nu^3 + o(\nu^3), \\
\theta_e &= \frac{1}{6}(2n + 3\xi - 2)\nu^3 + o(\nu^3), \\
\mathscr{D} &= \frac{1}{2}(n + 2\xi - 1)\nu^2 + o(\nu^2).
\end{aligned} \tag{4}
$$

LLL reduction is applied to the lattice basis matrix $\mathcal{B}$, generating a reduced basis $\mathcal{B}'$ that preserves the determinant. Subsequently, $\mathscr{D}$ polynomials are obtained from this reduced basis satisfying

$$
G_i(x, y) \equiv 0 \pmod{e^\nu}, \quad 1 \le i \le \mathscr{D}.
$$

To extract the target solution, we connect Theorem 2 with Theorem 1, specifically examining the scenario $j = 2$. Under this formulation, we require that

the inequality below be satisfied:

$$2^{\frac{\mathscr{D}}{4}} \det(\mathcal{L})^{\frac{1}{\mathscr{D}-1}} < \frac{e^{\nu}}{\sqrt{\mathscr{D}}}.$$

Taking this inequality together with (3) leads to

$$e^{\theta_e} X^{\theta_X} Y^{\theta_Y} < \frac{1}{2^{\frac{\mathscr{D}(\mathscr{D}-1)}{4}} (\sqrt{\mathscr{D}})^{\mathscr{D}-1}} e^{\nu(\mathscr{D}-1)} < e^{\nu(\mathscr{D}-1)}. \tag{5}$$

Incorporating the dominant terms from (4) together with (2), while discarding negligible contributions, yields the following inequality

$$N^{\alpha\frac{1}{6}(2n+3\xi-2)\nu^3} N^{\frac{1}{6}(2n+3\xi-2)(\alpha+\delta+1-n)\nu^3} N^{(\frac{1}{2}-2\gamma)\frac{1}{6}(n^2+3n\xi+3\xi^2-2n-3\xi+1)\nu^3} < N^{\alpha\frac{1}{2}(n+2\xi-1)\nu^3}.$$

Applying logarithms followed by division by ν^3 and $\log(N)$ results in the simplified form

$$\begin{aligned} &-3(4\gamma-1)\xi^2 - 3(4n\gamma - 2\delta + n - 4\gamma - 1)\xi - 4n^2\gamma + 2\alpha n + 4\delta n - 3n^2 \\ &+ 8n\gamma - 2\alpha - 4\delta + 6n - 4\gamma - 3 < 0, \end{aligned} \tag{6}$$

in which the value of ξ that achieves the optimum of the expression is expressed as

$$\xi_0 = \frac{(n-1)(1+4\gamma) - 2\delta}{2(1-4\gamma)}.$$

For ξ_0 to be positive, the parameters should comply with the following restriction

$$\delta < \frac{(n-1)(1+4\gamma)}{2}. \tag{7}$$

Upon substituting ξ_0 into inequality (6), the following expression is obtained:

$$\begin{aligned} &-3\delta^2 - (4n\gamma - 7n - 4\gamma + 7)\delta - 8\alpha n\gamma + 2n^2\gamma + 4(n^2 - 2n + 1)\gamma^2 + 2\alpha n \\ &- \frac{15}{4}n^2 + 8\alpha\gamma - 4n\gamma - 2\alpha + \frac{15}{2}n + 2\gamma - \frac{15}{4} < 0. \end{aligned}$$

Upon solving this quadratic inequality for δ, a valid range is given by

$$\delta < \frac{\sqrt{n-1}}{6}\left((7-4\gamma)\sqrt{n-1} - 2\sqrt{(1-4\gamma)\left(6\alpha + (n-1)(1-4\gamma)\right)}\right).$$

Considering the condition (7), we infer that

$$\delta < \min\Big(\frac{(n-1)(1+4\gamma)}{2}, \\ \frac{\sqrt{n-1}}{6}\Big((7-4\gamma)\sqrt{n-1} - 2\sqrt{(1-4\gamma)\left(6\alpha+(n-1)(1-4\gamma)\right)}\Big)\Big). \quad (8)$$

Case 1.1: If

$$\frac{(n-1)(1+4\gamma)}{2} \\ > \frac{\sqrt{n-1}}{6}\Big((7-4\gamma)\sqrt{n-1} - 2\sqrt{(1-4\gamma)\left(6\alpha+(n-1)(1-4\gamma)\right)}\Big), \quad (9)$$

then (8) gives

$$\delta < \frac{\sqrt{n-1}}{6}\Big((7-4\gamma)\sqrt{n-1} - 2\sqrt{(1-4\gamma)\left(6\alpha+(n-1)(1-4\gamma)\right)}\Big), \quad (10)$$

and (9) is equivalent to

$$\alpha > \frac{(n-1)(1-4\gamma)}{2}.$$

To ensure that the bound on δ remains non-negative, relation (10) imposes

$$(7-4\gamma)\sqrt{n-1} > 2\sqrt{(1-4\gamma)\left(6\alpha+(n-1)(1-4\gamma)\right)},$$

which leads to

$$\alpha < \frac{(n-1)(4\gamma+5)(3-4\gamma)}{8(1-4\gamma)}.$$

Case 1.2: If

$$\frac{(n-1)(1+4\gamma)}{2} \\ \leq \frac{\sqrt{n-1}}{6}\Big((7-4\gamma)\sqrt{n-1} - 2\sqrt{(1-4\gamma)\left(6\alpha+(n-1)(1-4\gamma)\right)}\Big),$$

then proceeding along the same lines, we derive the following constraints

$$0 \leq \alpha \leq \frac{(n-1)(1-4\gamma)}{2}, \qquad \delta \leq \frac{(n-1)(1+4\gamma)}{2}.$$

Under both cases and Assumption 1, let $G_1(x, y)$ and $G_2(x, y)$ be two reduced, algebraically independent polynomials. Solving the system

$$G_1(x, y) = 0, \quad G_2(x, y) = 0,$$

through Gröbner basis or resultant-based methods enables recovery of (t, v). Using the value of v, the relations $p+q = 2^{2\ell}v + v_0$ and $N = pq$ immediately allow us to factor N.

Case 2: Assume that e is even. Then we cannot compute the inverse of $2^{2(n-1)\ell}$ modulo e, and therefore, we use the formula (1) to express $\psi_n(N)$ as

$$\psi_n(N) = 2^{2(n-1)\ell}v^{n-1} + \sum_{0\le k\le n-2} c_k v^k,$$

and then reformulate the key equation $ed - t\psi_n(N) - 1 = 0$ as

$$t\left(2^{2(n-1)\ell}v^{n-1} + \sum_{0\le k\le n-2} c_k v^k\right) - ed + 1 = 0.$$

This shows that the tuple $(x_0, y_0, z_0) = (t, d, v)$ is a particular root to the following trivariate polynomial equation

$$F_n(x, y, z) = x\left(2^{2(n-1)\ell}z^{n-1} + \sum_{0\le k\le n-2} c_k z^k\right) - ey + 1 = 0.$$

The computation of small roots for the above equation is carried out using an adapted version of Coppersmith's method, following the approach proposed by Jochemsz and May [9]. The core idea is to work over two particular sets of monomials derived from the polynomial $F_n(x, y, z)$. More precisely, we fix two positive integers u and ρ, where ρ will later be chosen optimally, and consider the first set

$$\mathscr{S}_1 = \bigcup_{0\le r\le \rho} \left\{x^{i_1}y^{i_2}z^{i_3+r} : x^{i_1}y^{i_2}z^{i_3} \text{ is a monomial of } F_n^{u-1}(x, y, z)\right\},$$

and define the other set $\mathscr{S}_0$ as the collection of monomials obtained by multiplying each monomial of $F_n(x, y, z)$ with those belonging to $\mathscr{S}_1$. The multinomial expansion of the polynomial $F_n^{u-1}(x, y, z)$ demonstrates that monomials

$x^{i_1}y^{i_2}z^{i_3}$ appearing in $F_n^{u-1}(x,y,z)$ can be represented by exponent tuples (i_1,i_2,i_3) satisfying

$$\begin{cases} 0 \leq i_1 \leq u-1, \\ 0 \leq i_2 \leq u-1-i_1, \\ 0 \leq i_3 \leq (n-1)i_1. \end{cases}$$

Hence, the monomials of $\mathscr{S}_1$ are given by

$$\begin{cases} 0 \leq i_1 \leq u-1, \\ 0 \leq i_2 \leq u-1-i_1, \\ 0 \leq i_3 \leq (n-1)i_1 + \rho. \end{cases}$$

By an analogous construction, the monomials belonging to $\mathscr{S}_0$ arise from

$$\begin{cases} 0 \leq i_1 \leq u, \\ 0 \leq i_2 \leq u-i_1, \\ 0 \leq i_3 \leq (n-1)i_1 + \rho. \end{cases}$$

For the continuation of the analysis, it remains to characterize the monomials belonging to $\mathscr{S}_0 \setminus \mathscr{S}_1$. One readily verifies that this collection admits a decomposition into two subsets given by $\mathscr{P}_1 \cup \mathscr{P}_2$. To be more precise, $\mathscr{P}_1$ is the set of monomials characterized by exponent tuples that satisfy

$$\begin{cases} i_1 = u, \\ i_2 = 0, \\ 0 \leq i_3 \leq (n-1)i_1 + \rho. \end{cases}$$

Likewise, $\mathscr{P}_2$ consists of monomials with exponents satisfying

$$\begin{cases} 0 \leq i_1 \leq u-1, \\ i_2 = u-i_1, \\ 0 \leq i_3 \leq (n-1)i_1 + \rho. \end{cases}$$

As in **Case 1**, we take the bounds $X = 2N^{\alpha+\delta+1-n}$, $Y = N^{\delta}$, and $Z = 3N^{1/2-2\gamma}$ so that

$$x < X, \quad y < Y, \quad z < Z.$$

By $\mathscr{W}_n$, we mean the maximal absolute value of the coefficients of $F_n(xX, yY, zZ)$, that is to say

$$\mathscr{W}_n = \|F_n(xX, yY, zZ)\|_\infty.$$

In particular, we have $|c_0 X| \leq \mathscr{W}_n$. For sufficiently large N, it follows by induction on n, together with Lemma 3, that $c_0 \approx N^{n-1}$. Therefore,

$$|c_0 X| \approx 2N^{n-1} N^{\alpha+\delta+1-n}.$$

As a result, we obtain

$$N^{\alpha+\delta} \leq \mathscr{W}_n. \tag{11}$$

Let

$$\mathscr{R}_n = \mathscr{W}_n (XY)^{u-1} Z^{(n-1)(u-1)+\rho}.$$

Following the approach of [9], we introduce two families of polynomials derived from the monomial sets $\mathscr{S}_1$ and $\mathscr{S}_0 \setminus \mathscr{S}_1$. For monomials $x^{i_1} y^{i_2} z^{i_3} \in \mathscr{S}_1$, we define

$$G^{(n)}_{i_1,i_2,i_3} = x^{i_1} y^{i_2} z^{i_3} F_n X^{u-1-i_1} Y^{u-1-i_2} Z^{(n-1)(u-1)-i_3+\rho},$$

while for $x^{i_1} y^{i_2} z^{i_3} \in \mathscr{S}_0 \setminus \mathscr{S}_1$, we set

$$H^{(n)}_{i_1,i_2,i_3} = x^{i_1} y^{i_2} z^{i_3} \mathscr{R}_n.$$

By evaluating these polynomials at (xX, yY, zZ), we obtain coefficient vectors that span a Euclidean lattice $\mathcal{L}$. Its dimension $\mathscr{D}$ is determined by counting the cardinality of the set $\mathscr{S}_0$. A straightforward computation yields

$$\begin{aligned}\mathscr{D} &= \sum_{i_1=0}^{u} \sum_{i_2=0}^{u-i_1} \sum_{i_3=0}^{(n-1)i_1+\rho} 1, \\ &= \frac{n-1}{6} u^3 + \frac{n+\rho}{2} u^2 + \frac{2n+9\rho+7}{6} u + \rho + 1.\end{aligned}$$

To make the determinant computation more tractable, we arrange the lattice basis matrix so that it exhibits a triangular form. Following [9], this is achieved by ordering both rows and columns in a consistent way. The rows, corresponding to the polynomials $G^{(n)}_{i_1,i_2,i_3}$ and $H^{(n)}_{i_1,i_2,i_3}$, are sorted lexicographically according to (i_1, i_2, i_3). The columns, associated with the monomials $x^{i_1} y^{i_2} z^{i_3}$, follow the same ordering. This results in an upper triangular matrix. A simple illustration is given in Table 2, where $\star$ denotes nonzero terms.

Polynomials \ Monomials	1	y	y^2	x	xz	xz^2	xy	xyz	xyz^2	x^2	x^2z	x^2z^2	x^2z^3	x^2z^4
$G^{(3)}_{0,0,0}$	XYZ^2	$\star$	0	$\star$	$\star$	$\star$	0	0	0	0	0	0	0	0
$G^{(3)}_{0,1,0}$	0	XYZ^2	$\star$	0	0	0	$\star$	$\star$	$\star$	0	0	0	0	0
$H^{(3)}_{0,2,0}$	0	0	$Y^2\mathscr{R}_3$	0	0	0	0	0	0	0	0	0	0	0
$G^{(3)}_{1,0,0}$	0	0	0	XYZ^2	0	0	$\star$	0	0	$\star$	$\star$	$\star$	0	0
$G^{(3)}_{1,0,1}$	0	0	0	0	XYZ^2	0	0	$\star$	0	0	$\star$	$\star$	$\star$	0
$G^{(3)}_{1,0,2}$	0	0	0	0	0	XYZ^2	0	0	$\star$	0	0	$\star$	$\star$	$\star$
$H^{(3)}_{1,1,0}$	0	0	0	0	0	0	$XY\mathscr{R}_3$	0	0	0	0	0	0	0
$H^{(3)}_{1,1,1}$	0	0	0	0	0	0	0	$XYZ\mathscr{R}_3$	0	0	0	0	0	0
$H^{(3)}_{1,1,2}$	0	0	0	0	0	0	0	0	$XYZ^2\mathscr{R}_3$	0	0	0	0	0
$H^{(3)}_{2,0,0}$	0	0	0	0	0	0	0	0	0	$X^2\mathscr{R}_3$	0	0	0	0
$H^{(3)}_{2,0,1}$	0	0	0	0	0	0	0	0	0	0	$X^2Z\mathscr{R}_3$	0	0	0
$H^{(3)}_{2,0,2}$	0	0	0	0	0	0	0	0	0	0	0	$X^2Z^2\mathscr{R}_3$	0	0
$H^{(3)}_{2,0,3}$	0	0	0	0	0	0	0	0	0	0	0	0	$X^2Z^3\mathscr{R}_3$	0
$H^{(3)}_{2,0,4}$	0	0	0	0	0	0	0	0	0	0	0	0	0	$X^2Z^4\mathscr{R}_3$

Table 2: The lattice matrix for $n = 3$, $u = 2$, and $\rho = 0$.

Additionally, the diagonal contributions corresponding to the polynomials $G^{(n)}_{i_1,i_2,i_3}$ are of the form $(XY)^{u-1}Z^{(n-1)(u-1)+\rho}$. On the other hand, those arising from $H^{(n)}_{i_1,i_2,i_3}$ are given by $\mathscr{W}_n X^{u-1+i_1}Y^{u-1+i_2}Z^{(n-1)(u-1)+\rho+i_3}$. For each integer $k \in \{1,2,3\}$, we define

$$\tau_k = \sum_{x^{i_1}y^{i_2}z^{i_3} \in \mathscr{S}_0 \setminus \mathscr{S}_1} i_k. \tag{12}$$

Then, the determinant of the lattice is given by

$$\begin{aligned}\det(\mathcal{L}) &= X^{(u-1)\#\mathscr{S}_1+(u-1)\#(\mathscr{S}_0\setminus\mathscr{S}_1)+\tau_1} \times Y^{(u-1)\#\mathscr{S}_1+(u-1)\#(\mathscr{S}_0\setminus\mathscr{S}_1)+\tau_2} \\ &\times \mathscr{W}_n^{\#(\mathscr{S}_0\setminus\mathscr{S}_1)} Z^{\left((n-1)(u-1)+\rho\right)\#\mathscr{S}_1+\left((n-1)(u-1)+\rho\right)\#(\mathscr{S}_0\setminus\mathscr{S}_1)+\tau_3} \\ &= \mathscr{W}_n^{\#(\mathscr{S}_0\setminus\mathscr{S}_1)} X^{(u-1)\mathscr{D}+\tau_1}Y^{(u-1)\mathscr{D}+\tau_2}Z^{\left((n-1)(u-1)+\rho\right)\mathscr{D}+\tau_3}.\end{aligned} \tag{13}$$

An LLL reduction is performed on the lattice basis $\mathscr{B}$, resulting in a reduced basis $\mathscr{C}$ that preserves the determinant. The resulting basis vectors induce a set of polynomial relations that fulfill

$$U_i(x,y,z) \equiv 0 \pmod{\mathscr{R}_n}, \qquad 1 \le i \le \mathscr{D}.$$

The desired solution is extracted by combining Theorem 2 with the properties of the LLL-reduced basis established in Theorem 1. In particular, restricting to the case $j = 3$ ensures the solution, provided that the following condition holds

$$2^{\frac{\mathscr{D}(\mathscr{D}-1)}{4(\mathscr{D}-2)}} (\det \mathcal{L})^{\frac{1}{\mathscr{D}-2}} < \frac{\mathscr{R}_n}{\sqrt{\mathscr{D}}},$$

which can be transformed to

$$\det(\mathcal{L}) < \frac{1}{\mathscr{D}^{\frac{\mathscr{D}-2}{2}} 2^{\frac{\mathscr{D}(\mathscr{D}-1)}{4}}} \mathscr{R}_n^{\mathscr{D}-2}.$$

This implies that

$$\det(\mathcal{L}) < \mathscr{R}_n^{\mathscr{D}}.$$

Combining with (13), we derive

$$\mathscr{W}_n^{\#(\mathscr{S}_0\setminus\mathscr{S}_1)} X^{(u-1)\mathscr{D}+\tau_1}Y^{(u-1)\mathscr{D}+\tau_2}Z^{\left((n-1)(u-1)+\rho\right)\mathscr{D}+\tau_3} < \left(\mathscr{W}_n (XY)^{u-1}Z^{u-1+\rho}\right)^{\mathscr{D}}.$$

By observing that $\#\mathscr{S}_0 = \mathscr{D} = \#(\mathscr{S}_0 \setminus \mathscr{S}_1) + \#\mathscr{S}_1$, the former relation reduces to

$$X^{\tau_1}Y^{\tau_2}Z^{\tau_3} < \mathscr{W}_n^{\#\mathscr{S}_1}. \tag{14}$$

To simplify the computation of the quantities τ_k, we use the partition

$$\mathscr{S}_0 \setminus \mathscr{S}_1 = \mathscr{P}_1 \cup \mathscr{P}_2,$$

and define the function

$$g(a) = \sum_{i_1=u}^{u} \sum_{i_2=0}^{0} \sum_{i_3=0}^{(n-1)u+\rho} a + \sum_{i_1=0}^{u-1} \sum_{i_2=u-i_1}^{u-i_1} \sum_{i_3=0}^{(n-1)i_1+\rho} a,$$

so that

$$\tau_k = g(i_k), \qquad k \in \{1, 2, 3\}.$$

Moreover, one has

$$\#\mathscr{S}_1 = \sum_{i_1=0}^{u-1} \sum_{i_2=0}^{u-1-i_1} \sum_{i_3=0}^{(n-1)i_1+\rho} 1.$$

For the purpose of optimizing the bound, we set $\rho = u\kappa$. An elementary computation yields that, in the regime of sufficiently large u, the parameters τ_k and $\#\mathscr{S}_1$ satisfy

$$\begin{aligned}
\tau_1 &= \frac{1}{6}(2n + 3\kappa - 2)u^3 + o(u^3),\\
\tau_2 &= \frac{1}{6}(n + 3\kappa - 1)u^3 + o(u^3),\\
\tau_3 &= \frac{1}{6}(n^2 + 3n\kappa + 3\kappa^2 - 2n - 3\kappa + 1)u^3 + o(u^3),\\
\#\mathscr{S}_1 &= \frac{1}{6}(n + 3\kappa - 1)u^3 + o(u^3).
\end{aligned}$$

Keeping only the dominant terms and substituting X, Y, and Z by their expressions in terms of N, while neglecting lower-order coefficients, relation (14) reduces, by virtue of (11), to

$$\begin{aligned}
&N^{(\alpha+\delta+1-n)(\frac{1}{6}(2n+3\kappa-2)u^3)} N^{\delta(\frac{1}{6}(n+3\kappa-1)u^3)} N^{(1/2-2\gamma)(\frac{1}{6}(n^2+3n\kappa+3\kappa^2-2n-3\kappa+1)u^3)}\\
&< N^{(\alpha+\delta)(\frac{1}{6}(n+3\kappa-1)u^3)}.
\end{aligned}$$

A direct simplification then leads to the following expression

$$\begin{aligned}
&-3(4\gamma-1)\kappa^2 - 3(4n\gamma - 2\delta + n - 4\gamma - 1)\kappa\\
&+ \big(-4n^2\gamma + 2\alpha n + 4\delta n - 3n^2 + 8n\gamma - 2\alpha - 4\delta + 6n - 4\gamma - 3\big) < 0,
\end{aligned}$$

which attains its optimum at

$$\kappa_0 = \frac{(n-1)(1+4\gamma) - 2\delta}{2(1-4\gamma)}.$$

Substituting κ_0 into the preceding inequality yields

$$\begin{aligned}
&-3\delta^2 + (-4n\gamma + 7n + 4\gamma - 7)\delta \\
&+ \big(-8\alpha n\gamma + 2n^2\gamma + 4(n^2 - 2n + 1)\gamma^2 + 2\alpha n - \frac{15}{4}n^2 + 8\alpha\gamma - 4n\gamma \\
&- 2\alpha + \frac{15}{2}n + 2\gamma - \frac{15}{4}\big) < 0.
\end{aligned}$$

The solution of this quadratic inequality provides an admissible range for δ

$$\delta < \frac{\sqrt{n-1}}{6}\left((7-4\gamma)\sqrt{n-1} - 2\sqrt{(1-4\gamma)\left(6\alpha + (n-1)(1-4\gamma)\right)}\right).$$

The remainder of the proof follows similarly to that of **Case 1** to derive the required bounds. This completes the proof. □

Remark 3. In Theorem 3, the case $\gamma \approx 0$ corresponds to prime factors sharing only a negligible number of LSBs. In this case, the bound of Theorem 3 reduces to

$$\delta < \frac{7}{6}(n-1) - \frac{1}{3}\sqrt{(n-1)(6\alpha + n - 1)}.$$

In the scenario where $e \approx N^{n-1}$, i.e., $\alpha = n - 1$, our bound becomes

$$\delta < \left(\frac{7 - 2\sqrt{7}}{6}\right)(n-1) \approx 0.284(n-1),$$

which is weaker than the bound $0.292(n-1)$ established by Nitaj [21].

Remark 4. For $n = 2$, $0.5 < \alpha \leq 1$, and $\gamma = 0$, the bound of Theorem 3 reduces to

$$\delta < \frac{7}{6} - \frac{1}{3}\sqrt{1 + 6\alpha}\,.$$

This coincides with the weaker bound originally obtained by Boneh and Durfee for breaking RSA.

Remark 5. For $n = 3$, the corresponding cryptosystem is the *Cubic Pell RSA* introduced by Murru and Saettone [15]. Applying Theorem 3 for $n = 3$, we can break this scheme whenever

$$\delta < \frac{7}{3} - \frac{4}{3}\gamma - \frac{2}{3}\sqrt{(1-4\gamma)\big(3\alpha+1-4\gamma\big)}.$$

This recovers the result proved by Adenan et al. [1]. In particular, when $\gamma = 0$, the bound becomes

$$\delta < \frac{7}{3} - \frac{2}{3}\sqrt{3\alpha+1}\,,$$

which matches the bound established by Nitaj et al. [20].

Remark 6. Our method for attacking the RSA variants, as described in the proof of Theorem 3, is based on two main algorithms: the LLL algorithm for reducing the lattice basis, and the Gröbner basis method for extracting the roots of the polynomials obtained after the LLL reduction. The complexity of the LLL algorithm is polynomial in terms of the dimension of the lattice and the size of the largest entry in the basis matrix [13]. On the other hand, the complexity of the Gröbner basis method depends on the degree of the polynomials and the number of variables. In our attack, the number of variables is two or three, and the degree of the polynomials is small. This makes the Gröbner basis method efficient for small values of ν.

4. Comparison with existing works

4.1. Comparison with Nitaj et al.'s method

In 2024, Nitaj et al. [21] proposed a small private exponent attack on schemes satisfying the relation $ed - k\psi_n(N) = 1$. Their analysis shows that the prime factors of N can be recovered in polynomial time whenever $e = N^\alpha$ with

$$\frac{n-1}{2} < \alpha < 2(n-1),$$

and the secret exponent satisfies $d < N^\delta$, where

$$\delta < (n-1) - \sqrt{0.5(n-1)\alpha}.$$

Our findings reveal that our bound increases beyond the existing ones as the amount of shared LSBs of the primes grows. To illustrate this in terms of our parameters, let

$$B = (n-1) - \frac{\sqrt{2}}{2}\sqrt{(n-1)\alpha},$$

be the maximal bound established by Nitaj et al. [21], and let A denote the maximal bound of δ, given by

$$A = \frac{\sqrt{n-1}}{6}\Big((7-4\gamma)\sqrt{n-1} - 2\sqrt{(1-4\gamma)\big(6\alpha + (n-1)(1-4\gamma)\big)}\Big). \quad (15)$$

For illustration, we view our estimate as a function of γ for fixed values of α and n. In most scenarios, the public exponent e has the same magnitude as N^{n-1}, that is, $\alpha = n-1$. Figure 1 illustrates the comparison and demonstrates that our bound A becomes substantially larger than B as γ increases within the interval $[0, \frac{1}{4}]$. More precisely, for $\alpha = n-1$, we have

$$A = \frac{n-1}{6}\left((7-4\gamma) - 2\sqrt{(1-4\gamma)(7-4\gamma)}\right),$$
$$B = (n-1)\left(1 - \frac{\sqrt{2}}{2}\right).$$

Let $X = 1 - 4\gamma$. Then, a straightforward computation shows that $A > B$ whenever

$$X + 3\sqrt{2} > 2\sqrt{X^2 + 6X},$$

or equivalently

$$3X^2 + (24 - 6\sqrt{2})X - 18 < 0.$$

This is satisfied if

$$X < \sqrt{2} + \frac{1}{2}\sqrt{-32\sqrt{2} + 96} - 4,$$

that is, if

$$\gamma > \frac{1}{4}\left(5 - \sqrt{2} - 2\sqrt{6 - 2\sqrt{2}}\right) \approx 0.006.$$

Using $2^\ell = N^\gamma$, our method is more suitable when $\ell \geq 0.006\,k$ for a k-bit RSA modulus N. More precisely, for the commonly used parameter sizes,

we obtain improved bounds in the settings

$$\begin{aligned}
\ell &\geq 1 \quad \text{for } k = 128,\\
\ell &\geq 2 \quad \text{for } k = 256,\\
\ell &\geq 4 \quad \text{for } k = 512,\\
\ell &\geq 7 \quad \text{for } k = 1024,\\
\ell &\geq 13 \quad \text{for } k = 2048,\\
\ell &\geq 25 \quad \text{for } k = 4096.
\end{aligned}$$

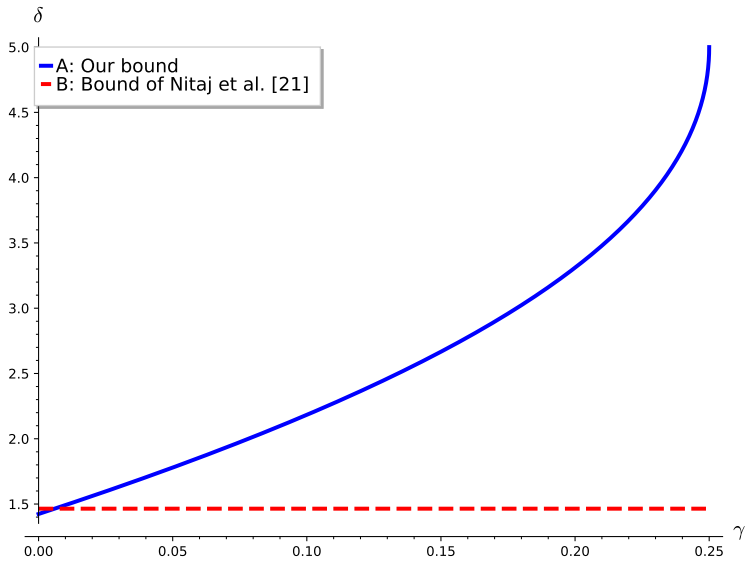

Figure 1: Comparison with our bound and the bound in [21] for $n = 6$

4.2. Comparison with Cotan and Teşeleanu's method

In the construction proposed by Cotan and Teşeleanu [6], the fundamental relation between the public and private keys is $ed - k\psi_n(N) = 1$, where $d < N^{\delta}$, $e = N^{\alpha}$. Their cryptanalysis relies on the continued–fraction technique. The authors show that the secret exponent d can be recovered whenever

$$\log_2(d) < \tfrac{1}{2}\left(n - \alpha - \tfrac{1}{2}\right)\log_2(N),$$

which is equivalent to the condition $d < N^{\frac{2n-1}{4} - \frac{\alpha}{2}}$.

As displayed in Figure 2, the value of our bound A in (15) becomes markedly larger than the bound C with

$$C = \frac{2n-1}{4} - \frac{\alpha}{2},$$

when γ varies over $[0, \frac{1}{4}]$. More specifically, one can easily show that $A > C$ for all $\gamma \geq 0$.

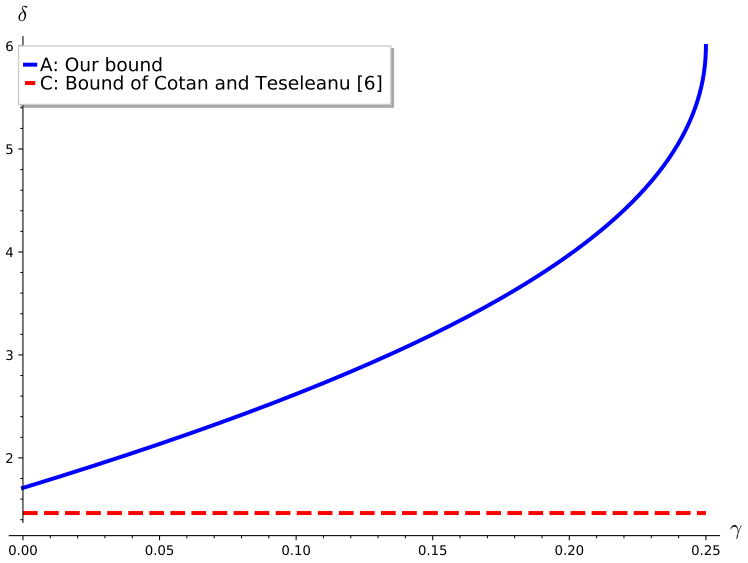

Figure 2: Comparison with our bound and the bound in [6] for $n = 7$

4.3. Comparison with Rahmani et al.'s attack

Rahmani *et al.* [24] introduced an attack on schemes satisfying the key equation $ed - k\psi_n(N) = 1$. They established that if the primes share ℓ LSBs such that $2^\ell = N^\gamma$, with an odd public exponent $e = N^\alpha$, then the scheme can be broken whenever $d < N^\delta$ with

$$\delta < \left(\frac{7}{6} - \frac{2}{3}\gamma\right)(n-1) - \frac{2}{3}\sqrt{3(n-1)\alpha\left(\frac{1}{2} - 2\gamma\right) + (n-1)^2\left(\frac{1}{2} - 2\gamma\right)^2}.$$

Note that this result matches the bound of Theorem 3 for

$$\frac{(n-1)(1-4\gamma)}{2} < \alpha < \frac{(n-1)(4\gamma+5)(3-4\gamma)}{8(1-4\gamma)}.$$

Moreover, we extend their attack to even public exponents.

4.4. Comparison with Rahmani et al.'s method

In a recent work, Rahmani et al. [27] proposed an attack on schemes satisfying

$$eu - x\psi_n(N) = z.$$

They transformed the earlier equation into a modular equation, expressed as

$$xH(y) + z \equiv 0 \pmod{e},$$

for suitably small z, and they solved it under the conditions

$$|u| < N^{\delta}, \qquad |z| < N^{\beta}, \qquad |z| < e|u|, \qquad |z| < |x|\,|y|^{n-1} < e,$$

with parameters

$$0 < \alpha < 2(n-1), \qquad 0 < \beta < \tfrac{n-1}{2}, \qquad \delta + \tfrac{1}{2}\beta < (n-1) - \sqrt{\tfrac{n-1}{2}\,\alpha}.$$

Their solution yields the factorization of the modulus and applies even to large private exponents, but it crucially depends on the constraint $|z| < |x|\,|y|^{n-1}$. In contrast, our method considers the case where $z = z_0 = \kappa$ is a fixed constant, and it relaxes this restriction, allowing larger values $|z_0| > |x|\,|y|^{n-1}$ while still efficiently solving

$$xH(y) + z_0 \equiv 0 \pmod{e},$$

which again leads to factoring the modulus.

5. Numerical experiments

In this section, we offer an experimental validation of the attack described in Theorem 3.

All experiments were carried out in SageMath 10.4 on a machine running Ubuntu 22.04.3 LTS, equipped with an Intel® Core™ i5–4460 CPU (3.20 GHz, 4 cores) and 8 GB of RAM.

5.1. A detailed numerical example in the case where e is odd

As a simple example of solving the equation $ed - t\psi_n(N) = 1$ of unknowns $(d, t, \psi_n(N))$, we take $n = 4$, and consider the public key (N, e) given by the following parameters

$$\begin{aligned}
N =& 162198906210172407435799313346834376938039634103664153865743965\backslash \\
& 26715906842397778398200232393, \\
e =& 103740828914636247276570126554137285143980513135941078585487624\backslash \\
& 63412108635790141422356936337098687446591677775641283995317017 5\backslash \\
& 32062753060587531293197614439499955305782695466181115517735373 5\backslash \\
& 77748585145868770187280237831103865604047218398903823209171282 3\backslash \\
& 45158439718857840851533 43.
\end{aligned}$$

This corresponds to $e = N^{\alpha}$ with $\alpha \approx 2.9933$.

Assume that the primes p and q of the modulus $N = pq$ have the same ℓ LSBs. Since ℓ is generally unknown, one can test successive values $\ell = 1, 2, \ldots$. Here, we fix $\ell = 30$, yielding $2^{\ell} = N^{\gamma}$ with $\gamma \approx 0.098$.

Denote by w_0 a root of the modular equation

$$x^2 \equiv N \pmod{2^{\ell}}.$$

Upon solving, we obtain the set of admissible values

$$w_0 \in \{104732317, 432138595, 641603229, 969009507\}.$$

In the present instance, setting $w_0 = 641603229$, we compute

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

leading to

$$v_0 = 1130441424798231866.$$

From Lemma 3, the expansion of $\psi_4(N)$ can be set as

$$\psi_4(N) = 2^{6\ell}v^3 + a_2v^2 + a_1v + a_0,$$

for the coefficients

$$\begin{aligned}
a_2 &= 2^{4\ell}(N + 3v_0 + 1), \\
a_1 &= 2^{2\ell}(N^2 + 2Nv_0 + 3v_0^2 - 2N + 2v_0 + 1), \\
a_0 &= N^3 + N^2v_0 + Nv_0^2 + v_0^3 - N^2 - 2Nv_0 + v_0^2 - N + v_0 + 1.
\end{aligned}$$

Setting

$$\kappa \equiv 2^{-6\ell} \pmod{e}.$$

Then, our objective is to solve the modular equation

$$t(2^{6\ell}v^3 + a_2v^2 + a_1v + a_0) + 1 \equiv 0 \pmod{e},$$

which is able to be equivalently written as

$$t(v^3 + b_2v^2 + b_1v + b_0) + \kappa \equiv 0 \pmod{e},$$

where

$$\begin{aligned} b_2 &\equiv \kappa a_2 \pmod{e}, \\ b_1 &\equiv \kappa a_1 \pmod{e}, \\ b_0 &\equiv \kappa a_0 \pmod{e}. \end{aligned}$$

From this, we compute

$$\begin{aligned} \kappa =& 44676530100923008385241958102812144354663180389382825234463\backslash \\ & 3857577070258858135850062182213113127304389628752112035767908\backslash \\ & 3477094790455431114070214209300951048271798534205747108557888\backslash \\ & 8392146778377343596569644386917722045709388255839141586301666\backslash \\ & 5066402333499671914790012578886128 75, \\ b_2 =& 80333272727358895167431214123650376292440501297482270325789 4\backslash \\ & 5909506824840420778305749720478821461727045458555571995283 16\backslash \\ & 4112933918658617689244840387834452245638888771080939427277 44\backslash \\ & 2970656729655625638683581133504289609303471992337628957542 15\backslash \\ & 8561909992117204195224056916327922 43. \end{aligned}$$

and

$$\begin{aligned}
b_1 =&972288020157897513304869432339178181701386528842266777673583\backslash\\
&830436499910388518225375727682469164598194460054729016235688\backslash\\
&107228109117836628297032030667577061458521915442737498825640\backslash\\
&804711170476711275499594177143145013174402059537741724430811\backslash\\
&401990208479280056832484342338653878,\\
b_0 =&724307556439856747749852572645345559421697939459939522165580\backslash\\
&641285323458278126131500744183576838668326235966763086342422\backslash\\
&597461903960499433065861214539674902214976024448107678651013\backslash\\
&465795486314523989265985774444937615335755503575283286928742\backslash\\
&997492404843836556037315895294883214.
\end{aligned}$$

Adopting the setting of Theorem 3, let $d < N^{\delta}$ with $\delta = 0.962$. This ensures that all hypotheses of Theorem 3 hold, specifically

$$\begin{cases}
\dfrac{(n-1)(1-4\gamma)}{2} \approx 0.912 < \alpha < \dfrac{(n-1)(4\gamma+5)(3-4\gamma)}{8(1-4\gamma)} \approx 8.67331, \\
\delta < \dfrac{\sqrt{n-1}}{6}\left((7-4\gamma)\sqrt{n-1} - 2\sqrt{(1-4\gamma)\left(6\alpha + (n-1)(1-4\gamma)\right)}\right) \approx 1.3016.
\end{cases}$$

We subsequently compute the following bounds

$$\begin{aligned}
X &= \lfloor 2N^{\alpha+\delta+1-n} \rfloor \approx 24506922354465584806137892206114552407047760\backslash\\
&\quad 4\backslash\\
&\quad 024553844323228318872326551656468664203345 92,\\
Y &= \lfloor 3N^{\frac{1}{2}-2\gamma} \rfloor \approx 32283143960251949202335072256.
\end{aligned}$$

With the selections $\nu = \xi = 3$, and upon defining the polynomials

$$R_{k,r,s}^{(n)}(x,y) = x^r y^s R_n(x,y)^k e^{\nu-k}, \quad (k,r,s) \in \mathcal{M} \cup \mathcal{N},$$

with

$$R_n(x,y) = x(y^3 + b_2 y^2 + b_1 y + b_0) + \kappa,$$

and with the index sets $\mathcal{M}$ and $\mathcal{N}$ given by

$$\begin{aligned}
\mathcal{M} &= \left\{(k,r,s) \in \mathbb{Z}^3 \mid 0 \le k \le \nu,\ 1 \le r \le \nu - k,\ 0 \le s \le n-2\right\},\\
\mathcal{N} &= \left\{(k,r,s) \in \mathbb{Z}^3 \mid 0 \le k \le \nu,\ r = 0,\ 0 \le s \le \lfloor \nu\xi \rfloor\right\},
\end{aligned}$$

we produce a lattice $\mathcal{L}$ of dimension $\mathscr{D} = 58$, generated by the coefficient vectors of $R_{k,r,s}(xX, yY)$. Following LLL reduction, 58 polynomials arise from the reduced basis. By computing a Gröbner basis, the first two polynomials can be extracted, and solving the resulting integer system leads to

$$\begin{aligned}
t = {} & 1148475727879351106177058963500432303962822907175403040291505\backslash \\
& 5689429110447505660734188017, \\
v = {} & 220929757791159944578079903 25.
\end{aligned}$$

Afterwards, using the known value v, we can compute the generalized cubic totient $\psi_4(N)$ through

$$\psi_4(N) = 2^{6\ell}v^3 + a_2v^2 + a_1v + a_0,$$

leading to

$$\begin{aligned}
\psi_4(N) = {} & 426720751955745206291308301002927715296145303152505601325735 25\backslash \\
& 199850280732306082897146067643321242597337964030210823840486 08\backslash \\
& 162683849098023083719366903717386850076143866114186203548158 87\backslash \\
& 819184385384773496422690178780669630600971728635382290700950 38\backslash \\
& 421818841839369304865666692 00.
\end{aligned}$$

At the final stage, we solve

$$p + q = 2^{2\ell}v + v_0 = 25471466876501039663149437939800428742161739066,$$

in conjunction with $N = pq$, resulting in

$$\begin{aligned}
p = {} & 12735733438250519831574718969900214372691482269, \\
q = {} & 12735733438250519831574718969900214369470256797.
\end{aligned}$$

It is worth noting that the LLL reduction took 15 seconds, and the Gröbner basis computation took 10 seconds.

Evaluating the modular inverse of e modulo $\psi_4(N)$ results in

$$\begin{aligned}
d = {} & 472406506995295396534784418099066580206429765704629508378414 40\backslash \\
& 3520081719761999755269210 07.
\end{aligned}$$

In the attack proposed by Nitaj et al. [21], the prime factors p and q can be recovered only when the secret exponent d satisfies

$$d < N^{\,n-1-\frac{\sqrt{2}}{2}\sqrt{\alpha(n-1)}}.$$

In our instance, however, we obtain

$$d \approx 2.708149 \times 10^{7}\, N^{\,n-1-\frac{\sqrt{2}}{2}\sqrt{\alpha(n-1)}},$$

which clearly exceeds the admissible range. Consequently, their attack does not apply in this setting.

Likewise, the method introduced by Cotan and Teşeleanu [5] succeeds in factoring N under the condition that the secret exponent d remains below the bound

$$d < N^{\frac{2n-1}{4}-\frac{\alpha}{2}}.$$

For our specific parameters, however, we find

$$d \approx 2.05541 \times 10^{65}\, N^{\frac{2n-1}{4}-\frac{\alpha}{2}},$$

which lies far beyond the permissible threshold. Hence, their approach cannot be employed to compromise this instance.

We further observe that the method of Rahmani et al. [27], developed for schemes satisfying the key relation

$$ed - k\psi(N) = 1,$$

relies on solving the modular equation

$$x\big(y^3 + b_2y^2 + b_1y + b_0\big) + \kappa \equiv 0 \pmod{e},$$

under the crucial requirement

$$|\kappa| < |xy^3|.$$

In our case, the pair $(x, y) = (t, v)$ is a root of this equation, but we have

$$\kappa \approx 1.381 \times 10^{190}\, |xy^3|,$$

meaning that $|\kappa|$ is enormously larger than $|xy^3|$. Hence, their technique is not sufficient to solve this equation which leads to factoring N in this instance.

5.2. A detailed numerical example in the case where e is even

Here, we consider the scenario where the public exponent is even, so that the methods presented in [1, 24] do not apply. To this end, we fix $n = 3$ and consider the public key (N, e) defined by

$$\begin{aligned} N =& 156171464429814459345276193284160970830808318422041658267174945\backslash \\ & 2934988201833605441857, \\ e =& 105167062965343463074021383065654861076956188812894226726875222\backslash \\ & 5104446940634186864226934851500964959853542796157664354700598 90\backslash \\ & 7373447461543426566950869271638600774921602. \end{aligned}$$

This corresponds to $e = N^{\alpha}$ with $\alpha \approx 1.9957$.

As in the explanation provided in the previous example, we choose the parameter $\ell = 52$, which yields $2^{\ell} = N^{\gamma}$ with $\gamma \approx 0.18592$, and

$$\begin{aligned} w_0 &= 616515777667745, \\ v_0 &= 17415232201953992313252764861762. \end{aligned}$$

From Lemma 3, we can write

$$\psi_3(N) = av^2 + bv + c,$$

for the coefficients

$$\begin{aligned} a &= 2^{4\ell}, \\ b &= 2^{2\ell}N + 2^{2\ell+1}v_0 + 2^{2\ell}, \\ c &= N^2 + Nv_0 + v_0^2 - N + v_0 + 1. \end{aligned}$$

Our goal is therefore to solve the trivariate equation

$$F_3(x, y, z) = x(az^2 + bz + c) - ey + 1 = 0.$$

Following the proof of Theorem 3, assume that $d < N^{\delta}$ with $\delta = 0.608$. This ensures that all hypotheses of Theorem 3 hold, specifically

$$\begin{cases} \dfrac{(n-1)(1-4\gamma)}{2} \approx 0.2563 < \alpha < \dfrac{(n-1)(4\gamma+5)(3-4\gamma)}{8(1-4\gamma)} \approx 12.64, \\ \delta < \dfrac{\sqrt{n-1}}{6}\left((7-4\gamma)\sqrt{n-1} - 2\sqrt{(1-4\gamma)\left(6\alpha + (n-1)(1-4\gamma)\right)}\right) \approx 1.242. \end{cases}$$

Next, we compute the bounds

$$X = \lfloor 2N^{\alpha+\delta+1-n} \rfloor \approx 1344953692277598540546964399757024463354819822747648,$$
$$Y = \lfloor N^{\delta} \rfloor = 154778211187241402253430183472052442596029841276928 0,$$
$$Z = \lfloor 3N^{\frac{1}{2}-2\gamma} \rfloor \approx 185085862191.$$

After selecting the lattice parameters $\rho = u = 3$ and using the polynomials $G^{(n)}_{i_1,i_2,i_3}(x, y, z)$ and $H^{(n)}_{i_1,i_2,i_3}(x, y, z)$ introduced in the proof of Theorem 3, we construct a lattice $\mathcal{L}$ of dimension $\mathscr{D} = 60$, generated by the coefficient vectors of the polynomials $G^{(n)}_{i_1,i_2,i_3}(xX, yY, zZ)$ and $H^{(n)}_{i_1,i_2,i_3}(xX, yY, zZ)$. After applying LLL reduction, we obtain 60 polynomials from the reduced basis in 55 seconds. Computing a Gröbner basis allows us to extract the first three polynomials in 7 seconds. Solving the resulting system of integer equations then yields

$$t = 628188207561388561691827644905178747010028924367557,$$
$$d = 145684517367092693735944386619687280306658605817787 9,$$
$$v = 123228535726.$$

Finally, combining

$$p + q = 2^{2\ell}v + v_0 = 249937163647037060109891541335157486506937 8,$$

with $N = pq$, we recover

$$p = 124968581823518530054945777197798202940688 1,$$
$$q = 124968581823518530054945764137359283566249 7.$$

In the attack proposed by Zheng et al. [34] for schemes with the key equation $ed - k\psi_3(N) = 1$, the prime factors p and q can be recovered only when the secret exponent d satisfies

$$d < N^{2-\sqrt{\alpha}} \approx N^{0.5873}.$$

In our instance, however, we have

$$d \approx N^{0.6076},$$

which indicates that their attack does not apply to this instance.

6. Conclusion

We proposed an improved cryptanalytic strategy against the generalized Cubic Pell RSA scheme for a modulus $N = pq$ with the key equation

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

Assuming that the primes p and q shared a fraction of their least significant bits, our method combined Coppersmith's technique with lattice reduction to obtain improved bounds on the secret exponent d than those reported in previous studies.

References

[1] Adenan, N. N. H., Nitaj, A., Ariffin, M. R. K., Abu, N. A.: Cryptanalysis of a cubic Pell variant of RSA with primes sharing least significant bits. Journal of Information and Optimization Sciences, **45**(5), 1263-1280 (2024).

[2] Boneh, D., Durfee, G.: Cryptanalysis of RSA with private key d less than $N^{0.292}$, Advances in Cryptology-Eurocrypt'99, Lecture Notes in Computer Science Vol. 1592, Springer-Verlag, pp. 1–11 (1999)

[3] T. Collins, D. Hopkins, S. Langford, and M. Sabin. Public key cryptographic apparatus and Method. US Patent #5,848,159, Jan. 1997.

[4] Coppersmith, D.: Small solutions to polynomial equations, and low exponent RSA vulnerabilities. Journal of Cryptology, 10(4), pp. 233–260 (1997)

[5] Teseleanu, G., Cotan, P.: Continued Fractions Applied to a Family of RSA-like Cryptosystems, Cryptology ePrint Archive, Paper 2022/1241, 2022, `https://eprint.iacr.org/2022/1241`

[6] Cotan, P., Teşeleanu, G.: A security analysis of two classes of RSA-like cryptosystems. Journal of Mathematical Cryptology, **18**(1), pp. 20240013 (2024).

[7] Feng, Y., Nitaj, A., Pan, Y.: Partial prime factor exposure attacks on some RSA variants. Theoretical Computer Science, **999**, pp. 114549, Elsevier (2024).

[8] Howgrave-Graham, N.: Finding small roots of univariate modular equations revisited, In Cryptography and Coding, LNCS 1355, pp. 131–142, Springer-Verlag (1997)

[9] Jochemsz, E., May, A.: A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants, in: ASIACRYPT 2006, LNCS 4284, 2006, pp. 267–282, Springer-Verlag (2006)

[10] Koyama, K.: Fast RSA type scheme based on singular cubic curve $y^2 + axy = x^3 \pmod{n}$. Proc. Eurocrypt'95, Lecture Notes in Computer Science, **921**, Springer-Verlag, 329–339 (1995)

[11] 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: Proceedings of CRYPTO 1991, Lecture Notes in Computer Science 576, 1991, pp. 252–266.

[12] Lenstra, A.K., Lenstra, H.W., Lovász, L.: Factoring polynomials with rational coefficients, Mathematische Annalen, Vol. 261, pp. 513–534, (1982)

[13] Nguyen, P. Q., Stehlé, D.: An LLL Algorithm with Quadratic Complexity, SIAM Journal on Computing, (39), pp. 874-903 (2009)

[14] May, A.: New RSA Vulnerabilities Using Lattice Reduction Methods. PhD thesis, University of Paderborn (2003).

[15] Murru N., Saettone F.M.: A Novel RSA-Like Cryptosystem Based on a Generalization of the Rédei Rational Functions. In: Kaczorowski J., Pieprzyk J., Pomykala J. (eds) Number-Theoretic Methods in Cryptology. NuTMiC 2017. Lecture Notes in Computer Science, vol 10737. Springer, Cham (2018)

[16] Nitaj, A.: Another generalization of Wiener's attack on RSA, In: Vaudenay, S. (Ed.) Africacrypt 2008. LNCS, vol. 5023, 1740. Springer, Heidelberg (2008)

[17] Nitaj, A., Ariffin, M.R.K., D.I. Nassr, Bahig, H.M.: New attacks on the RSA cryptosystem, in D. Pointcheval and D. Vergnaud (Eds.): AFRICACRYPT 2014, LNCS 8469, pp. 178198, 2014. Springer (2014)

[18] Nitaj, A., Ariffin, M.R.B.K., Adenan, N.N.H., Abu, N.A.: Classical Attacks on a Variant of the RSA Cryptosystem. In: LATINCRYPT 2021. Lecture Notes in Computer Science, vol. 12912, pp. 151–167 Springer (2021)

[19] Nitaj, A., Ariffin, M. R. B. K., Adenan, N. N. H., Lau, T. S. C., Chen, J.: Security issues of novel RSA variant. IEEE Access, 10, 53788-53796 (2022).

[20] Nitaj, A., Ariffin, M.R.B.K., Adenan, N.N.H., Lau, T.S.C., Chen, J.: Security Issues of Novel RSA Variant. IEEE Access 10, pp. 53788–53796 (2022)

[21] Nitaj, A., Adenan, N.N.H., Ariffin, M.R.K. (2024). Cryptanalysis of a New Variant of the RSA Cryptosystem. In: Vaudenay, S., Petit, C. (eds) Progress in Cryptology - AFRICACRYPT 2024. AFRICACRYPT 2024. Lecture Notes in Computer Science, vol 14861. Springer, Cham.

[22] Peng, Liqiang and Hu, Lei and Lu, Yao and Wei, Hongyun.: An improved analysis on three variants of the RSA cryptosystem. International Conference on Information Security and Cryptology, **10143**, pp. 140–149, Springer (2016).

[23] Quisquater, J. J., Couvreur, C.: Fast decipherment algorithm for RSA public-key cryptosystem. Electronics Letters, 18(21), pp. 905–907 (1982)

[24] Rahmani, M., Nitaj, A., Ziane, M. Partial exposure attacks on new RSA variant. Cryptography 2024, 8, 44, 2024.

[25] Rahmani, M., Nitaj, A., Ziane, M.: Further cryptanalysis of some variants of the RSA cryptosystem. Journal of Applied Mathematics and Computing, **71**(2), pp. 1911-1941, (2025).

[26] Rahmani, M., Nitaj, A., Ziane, M.: Cryptanalysis of some algebraic variants of the RSA cryptosystem. Finite Fields and Their Applications, **110**, pp. 102757, (2026).

[27] Rahmani, M., Nitaj, A., Ziane, M: A generalized attack on a new variant of the RSA cryptosystem. Computational and Applied Mathematics, **45**(1), pp. 11, (2026).

[28] Rivest, R., Shamir, A., Adleman, L.: A Method for Obtaining digital signatures and public-key cryptosystems, Communications of the ACM, Vol. 21 (2), pp. 120–126 (1978)

[29] Shi, G., Wang, G., Gu, D. (2022). Further Cryptanalysis of a Type of RSA Variants. In: Susilo, W., Chen, X., Guo, F., Zhang, Y., Intan, R. (eds) Information Security. ISC 2022. Lecture Notes in Computer Science, vol 13640. Springer, Cham.

[30] Sun, H. M., Wu, M. E., Steinfeld, R., Guo, J., Wang, H. .: Cryptanalysis of short exponent RSA with primes sharing least significant bits. In International Conference on Cryptology and Network Security . Berlin, Heidelberg: Springer Berlin Heidelberg (pp. 49-63) (2008)

[31] Steinfeld, R., Zheng, Y.: On the Security of RSA with Primes Sharing Least-Significant Bits. Appl. Algebra Eng. Commun. Comput. 15(3-4), 179200 (2004)

[32] Takagi, T.: A fast RSA-type public-key primitive modulo $p^k q$ using Hensel lifting, IEICE Transactions 2004, 87-A, 94–101.

[33] Wiener, M.: Cryptanalysis of short RSA secret exponents, IEEE Transactions on Information Theory, Vol. 36, 553–558 (1990)

[34] Zheng, M., Kunihiro, N., Yao, Y: Cryptanalysis of the RSA variant based on cubic Pell equation, Theoretical Computer Science 889, pp. 135–144 (2021)