Improved Cryptanalysis of an RSA Variant Based on Cubic Pell Curve

Mohammed Rahmani[1] and Abderrahmane Nitaj[2]

[1] Mohammed First University, Sciences Faculty, Department of Mathematics and Computer Science, ACSA Laboratory, Oujda 60000, Morocco.
mohammed.rahmani@ump.ac.ma

[2] Normandie Univ, UNICAEN, CNRS, LMNO, 14000 Caen, France
abderrahmane.nitaj@unicaen.fr

Abstract. In 2024, based on the cubic Pell curve, Nitaj and Seck proposed a variant of the RSA cryptosystem where the modulus is in the form $N = p^r q^s$, and the public key e and private key d satisfy the equation $ed \equiv 1 \pmod{(p-1)^2(q-1)^2}$. They showed that N can be factored when d is less than a certain bound that depends on r and s in the situation $rs \geq 2$, which is not extendable to $r = s = 1$. In this paper, we propose a cryptanalysis of this scheme in the situation $r = s = 1$, and give an explicit bound for d that makes the scheme insecure. The method is based on Coppersmith's method and lattice reduction.

Keywords: RSA Cryptosystem· Factorization · Coppersmith's method· Lattice reduction · RSA Variant.

1 Introduction

In 1978, the RSA cryptosystem was introduced by Rivest, Shamir, and Adleman [18]. It is still one of the most widely used public-key cryptosystems. Its security is based on the computational challenge of factoring large composite numbers. In this framework, the modulus, denoted by N, is defined as the product of two large primes, p and q, of equal bit-length. A public exponent e is chosen with $e < N$ and $\gcd(e, (p-1)(q-1)) = 1$, guaranteeing the existence of an integer d satisfying the equation $ed \equiv 1 \pmod{(p-1)(q-1)}$. The public key is the pair (N, e), while the private key is the pair (N, d). To encrypt a plaintext message m where $m < N$, the ciphertext c is computed as $c \equiv m^e \pmod{N}$. For decryption, the original message m is recovered by computing $m \equiv c^d \pmod{N}$.

In practical implementations, both encryption and decryption can be computationally costly. A widely adopted strategy to accelerate decryption involves selecting small private exponents. However, Wiener [22] demonstrated in 1990 that RSA becomes insecure when $d < \frac{1}{3}N^{1/4}$. This bound was later refined by Boneh and Durfee [1], who extended the attack to cases where $d < N^{0.292}$. These vulnerabilities have motivated research aimed at strengthening RSA while maintaining efficiency, giving rise to several variants. Noteworthy examples include CRT-RSA [16] and others [22,7], all of which preserve the conventional

modulus structure $N = pq$. Other methods, such as Prime-Power RSA [20] and others [21,2], alter the modulus to investigate different formulations. Additional variants involve the complete substitution of the standard Euler function with alternative expressions.

In 1995, Kuwakado et al. [8] introduced an alternative approach to the RSA cryptosystem based on singular cubic curves described by the equation $y^2 \equiv x^3 + bx^2 \pmod N$, where $N = pq$ represents an RSA modulus and $b \in \mathbb{Z}/N\mathbb{Z}$. Their method involved selecting a public exponent e such that $\gcd(e, \theta(N)) = 1$, with $\theta(N) = (p^2 - 1)(q^2 - 1)$. The secret exponent d was determined through the modular equation $ed \equiv 1 \pmod{(p^2 - 1)(q^2 - 1)}$. Subsequent cryptanalytic efforts on this scheme were presented in [4,17].

In 2018, Murru and Saettone [11] introduced a variant of the RSA cryptosystem that relies on the cubic Pell equation $x_1^3 + \alpha x_2^3 + \alpha^2 x_3^3 - 3\alpha x_1 x_2 x_3 = 1$ in $\mathbb{Z}/N\mathbb{Z}$, where α is a cubic residue modulo N. In this scheme, the modulus is given by $N = pq$, and the exponents e and d are constrained by the modular relation $ed \equiv 1 \pmod{(p^2 + p + 1)(q^2 + q + 1)}$.

In 2024, Nitaj and Seck [14] proposed a cryptosystem using encoding functions and the cubic Pell curve defined by the equation

$$x_1^3 + \alpha x_2^3 + \alpha^2 x_3^3 - 3\alpha x_1 x_2 x_3 \equiv 1 \pmod N,$$

with $N = p^r q^s$. In this scheme, the encryption and decryption exponents fulfill the modular equation $ed \equiv 1 \pmod{\psi(r, s, N)}$, where

$$\psi(r, s, N) = p^{2(r-1)} q^{2(s-1)} (p - 1)^2 (q - 1)^2$$

Beyond Wiener's well-known attack and its refinement by Boneh and Durfee, numerous attacks have been devised against alternative RSA variants, as noted in [13,23,19,4]. In the same work by Nitaj and Seck [14], a continued fraction-based attack on the variant with the key equation

$$ed \equiv 1 \pmod{\psi(r, s, N)},$$

is presented. They showed that if $N = p^r q^s$ and $d < N^\delta$ with $\delta < 2 - \frac{2(3r+s)}{(r+s)^2}$, then the factorization of N can be done in polynomial time.

We observe in the former attack that if the modulus takes the classical form $N = pq$, that is $r = s = 1$, the attack of Nitaj and Seck [14] does not work since their condition becomes $\delta < 0$ which is not possible. In this paper, we fill this gap by presenting a Coppersmith-based approach. We show that if $N = pq$, $e = N^\alpha$, and $d < N^\delta$, then we can break the scheme whenever $1 < \alpha < 4$ and $\delta < 2 - \sqrt{\alpha}$.

The rest of the paper is structured as follows. Section 2 covers preliminaries. Section 3 applies a variant of Coppersmith's method for breaking the scheme of Nitaj and Seck. Section 4 offers a detailed numerical experiment to validate the proposed attack. Finally, Section 5 concludes the paper.

2 Preliminaries

2.1 Useful lemmas

The following result from [12] establishes explicit bounds for p and q using the public value N, given that $N = pq$ with $q < p < 2q$.

Lemma 1. *Each pair of primes p and q such that $N = pq$ with $q < p < 2q$ satisfy the following inequalities*

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

The subsequent result yields a lower bound for $(p-1)^2(q-1)^2$.

Lemma 2. *If $N = pq$ and $q < p < 2q$, then*

$$(p-1)^2(q-1)^2 > \frac{N^2}{4}.$$

Proof. We have $(p-1)(q-1) = N - p - q + 1$. According to Lemma 1, we get $p + q < 3\sqrt{N}$, yielding for $N > 6$

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

This implies that

$$(p-1)^2(q-1)^2 > \frac{N^2}{4},$$

which concludes the proof. □

2.2 The scheme of Nitaj and Seck

The scheme of Nitaj and Seck [14] is based on the following cubic Pell curve

$$\mathcal{C}_\alpha(N) \quad : \quad x_1^3 + \alpha x_2^3 + \alpha^2 x_3^3 - 3\alpha x_1 x_2 x_3 \equiv 1 \pmod{N},$$

where α is a cubic residue modulo N. In the encryption and decryption processes, an encoding function $\mathcal{E}$ is used to map $(m_{x_1}, m_{x_2}) \in \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ to

$$\mathcal{E}\left((m_{x_1}, m_{x_2}), \beta, N\right) = (x_1, x_2, x_3) \in \mathcal{C}_\alpha(N),$$

such that $\alpha \equiv \beta^3 \pmod{N}$. Similarly, a decoding function $\mathcal{D}$ is used to reverse $(x_1, x_2, x_3) \in \mathcal{C}_\alpha(N)$ with $\alpha \equiv \beta^3 \pmod{N}$ to

$$\mathcal{D}\left((x_1, x_2, x_3), \beta, N\right) = (m_{x_1}, m_{x_2}) \in \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}.$$

The cryptosystem of Nitaj and Seck can be described as follows.

Key generation

1. Choose a security parameter ρ along with two small positive integers r and s.
2. Randomly choose two prime numbers p and q, both of size ρ, such that $p \equiv q \equiv 1 \pmod 3$.
3. Compute $N = p^r q^s$ and $\psi(r, s, N) = p^{2(r-1)} q^{2(s-1)} (p-1)^2 (q-1)^2$.
4. Randomly select an integer $\beta < N$ and compute $\alpha \equiv \beta^3 \pmod N$, such that α is a nonzero cubic residue modulo p and modulo q.
5. Pick an integer $e < N$ such that $\gcd(e, pq(p-1)(q-1)) = 1$.
6. Compute
$$d \equiv \frac{1}{e} \pmod{\psi(r, s, N)}.$$
7. The public key consists of (N, β, e), while the private key comprises (N, β, d).

Encryption.

1. Express a plaintext as an ordered pair $M = (x_M, y_M)$ within the set $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$.
2. Compute $\alpha \equiv \beta^3 \pmod N$.
3. Compute the triplet (x_1, x_2, x_3) using the function $\mathcal{E}$ applied to (x_M, y_M), along with β and N.
4. Derive $C = (x_C, y_C, z_C)$ by applying the exponent e to (x_1, x_2, x_3) over the curve $\mathcal{C}_\alpha(N)$.
5. The encrypted output is given by $(c_{x_1}, c_{x_2}) = \mathcal{D}(C, \beta, N)$.

Decryption. To recover the plaintext we follow the steps

1. Consider the ciphertext as an ordered pair (c_{x_1}, c_{x_2}) within the set $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$.
2. Compute $\alpha \equiv \beta^3 \pmod N$.
3. Compute the triplet (x_C, y_C, z_C) using the function $\mathcal{E}$ applied to (c_{x_1}, c_{x_2}), along with β and N.
4. Obtain (x_1, x_2, x_3) by applying the exponent d to (x_C, y_C, z_C) over the curve $\mathcal{C}_\alpha(N)$.
5. The plaintext is retrieved by $(x_M, y_M) = \mathcal{D}((x_1, x_2, x_3), \beta, N)$.

2.3 Lattice theory

A subset $\mathcal{L} \subset \mathbb{R}^n$ is defined as a lattice if it forms a finitely generated free abelian subgroup of $\mathbb{R}^n$, generated by $\omega \leq n$ linearly independent vectors in $\mathbb{R}^n$. In other words, it can be expressed as

$$\mathcal{L} = \mathbb{Z}u_1 + \mathbb{Z}u_2 + \cdots + \mathbb{Z}u_\omega.$$

The lattice $\mathcal{L}$ can be represented by a matrix M, whose rows consist of the basis vectors $u_1, u_2, \ldots, u_\omega$. The lattice dimension is n, its rank is ω, and an associated determinant is given by

$$\det(\mathcal{L}) = \sqrt{\det(M \cdot M^t)},$$

where M^t denotes the transpose of M. In the special case where $\omega = n$, the lattice $\mathcal{L}$ is said to be of full rank, and its determinant becomes $\det(\mathcal{L}) = |\det(M)|$.

A lattice $\mathcal{L}$ possesses an infinite number of possible bases when $\omega \geq 2$. However, every basis of $\mathcal{L}$ consists of the same number of vectors and maintains an identical determinant. Finding a basis consisting of short vectors becomes computationally challenging as the dimension increases. In 1982, Lenstra, Lenstra, and Lovász [9] proposed the LLL algorithm, which efficiently computes an approximate short basis in polynomial time. The following result [10] is frequently used to analyze the output of the basis produced by the LLL algorithm.

Theorem 1. *Consider a lattice $\mathcal{L}$ generated by a basis $\{u_1, u_2, \ldots, u_\omega\}$. The LLL algorithm outputs a reduced basis $\{w_1, w_2, \ldots, w_\omega\}$ that satisfies the following*

$$\|w_1\| \leq \cdots \leq \|w_i\| \leq 2^{\frac{\omega(\omega-1)}{4(\omega+1-i)}} \det(\mathcal{L})^{\frac{1}{\omega+1-i}}, \quad \text{for } i = 1, \ldots, \omega.$$

2.4 Coppersmith's approach

In 1996, Coppersmith [3] introduced an algorithm that operates in polynomial time to find small solutions to a univariate polynomial congruence of the form $p(x) \equiv 0 \pmod{R}$, where R is an integer with an unknown factorization. This method has been extended to handle multivariate polynomials, particularly those of the form

$$p(x_1, x_2, \ldots, x_n) = \sum_{i_1, i_2, \ldots, i_n} n_{i_1, i_2, \ldots, i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n},$$

where the coefficients $n_{i_1, i_2, \ldots, i_n}$ are integers. The Euclidean norm for such polynomials is given by

$$\|p(x_1, x_2, \ldots, x_n)\| = \sqrt{\sum n_{i_1, i_2, \ldots, i_n}^2}.$$

In 1997, Howgrave-Graham [5] refined Coppersmith's technique, simplifying the process of finding small roots, as demonstrated in the following result.

Theorem 2 (Howgrave-Graham). *If $p(x_1, x_2, \ldots, x_n) \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$ is a multivariate polynomial containing at most ω monomials, and R is a positive integer with the two statements*

1. *$p(y_1, y_2, \ldots, y_n) \equiv 0 \pmod{R}$.*
2. *$\|p(x_1 Y_1, x_2 Y_2, \ldots, x_n Y_n)\| < \frac{R}{\sqrt{\omega}}$, with $|y_i| < Y_i$ for $i = 1, \ldots, n$,*

then, it follows that $p(y_1, y_2, \ldots, y_n) = 0$ holds true in $\mathbb{Z}$.

When more than two variables are considered, approaches based on Coppersmith's method are heuristic in nature. In this study, we rely on the following assumption [1,6,15,23].

Assumption 1. *The polynomials $h_1, h_2, \ldots, h_\omega$ reduced by the LLL algorithm are algebraically independent.*

Under this assumption, the shared solution $(y_1, y_2, \ldots, y_n)$ to the system of polynomial equations $h_i(y_1, y_2, \ldots, y_n) = 0$ for $i = 1, \ldots, \omega$ can be obtained using approaches like the Gröbner basis technique or resultants.

3 Attacking the scheme of Nitaj and Seck

In this section, we propose a new attack on the scheme of Nitaj and Seck when the modulus takes the standard form $N = pq$.

3.1 The new method

Theorem 3. *Let N be an RSA modulus such that $N = pq$, where $q < p < 2q$. Let $e = N^\alpha$ and $d < N^\delta$ represent the public and private exponents, respectively, such that $ed \equiv 1 \pmod{\Lambda(N)}$, where $\Lambda(N) = (p-1)^2(q-1)^2$. Assume that both α and δ satisfy*

$$1 < \alpha < 4 \quad \text{and} \quad \delta < 2 - \sqrt{\alpha},$$

then the recovery of the RSA primes can be done in polynomial time.

Proof. The first point is to reformulate the modular equation $ed \equiv 1 \pmod{\Lambda(N)}$ into $ed - k\Lambda(N) = 1$ for some integer k. By expressing $\Lambda(N)$ as

$$\Lambda(N) = (p+q)^2 - 2(N+1)(p+q) + (N+1)^2,$$

the former equation can be rewritten as a modular one of the form

$$h(x_1, x_2) \equiv 0 \pmod{e},$$

with $h(x_1, x_2) = x_1(x_2^2 + a_1x_2 + a_0) + 1$ for $x_1 = k$, $x_2 = p+q$, $a_1 = -2(N+1)$, and $a_0 = (N+1)^2$. In order to solve this modular equation, one can use Coppersmith's approach. To this end, we define $x_3 = x_1x_2^2 + 1$. So $h(x_1, x_2) = H(x_1, x_2, x_3)$ where

$$H(x_1, x_2, x_3) = x_3 + x_1(a_1x_2 + a_0).$$

Consider a positive parameter $t > 0$ to be optimized. Let μ be a positive integer and w an integer such that $0 \le w \le \mu$. Define the following set of polynomials

$$A_{w,a,b}(x_1, x_2, x_3) = x_1^a x_2^b H(x_1, x_2, x_3)^w e^{\mu - w}, \quad (w, a, b) \in \mathcal{E} \cup \mathcal{F},$$

where

$$\mathcal{E} = \{(w, a, b) \mid b = 0, 1,\ w = 0, \ldots, \mu,\ a = 1, \ldots, \mu - w\},$$
$$\mathcal{F} = \left\{(w, a, b) \mid b = 0, \ldots, \lfloor t \rfloor,\ w = \left\lfloor \frac{\mu}{t} \right\rfloor b, \ldots, \mu,\ a = 0\right\},$$

and during each computation, replace the term $x_1x_2^2$ with $x_3 - 1$.

As the pair (x_1, x_2) satisfies the equation $h(x_1, x_2) \equiv 0 \pmod{e}$, then also the tuple (x_1, x_2, x_3) fulfills the equation $H(x_1, x_2, x_3) \equiv 0 \pmod{e}$, implying

$$A_{w,a,b}(x_1, x_2, x_3) \equiv 0 \pmod{e^{\mu}},$$

for all $(w, a, b) \in \mathcal{E} \cup \mathcal{F}$. In accordance to Coppersmith's technique, we must try to find bounds X_1, X_2 and X_3 so that

$$|x_1| \leq X_1, \quad |x_2| \leq X_2, \quad |x_3| \leq X_3.$$

By Lemma 2, we get $\Lambda(N) > \frac{N^2}{4}$. This implies that

$$|x_1| = \left|\frac{ed-1}{\Lambda(N)}\right| < 4edN^{-2} \leq 4N^{\alpha+\delta-2}.$$

Also, according to Lemma 1, we can set $|x_2| = p + q < 3\sqrt{N}$, so we can apply the following bounds

$$X_1 = 4N^{\alpha+\delta-2}, \quad X_2 = 3N^{0.5}, \quad X_3 = X_1X_2^2.$$

Afterwards, we generate the basis matrix of the lattice $\mathcal{L}$ by taking the coefficient vectors from the polynomials $A_{w,a,b}(X_1x_1, X_2x_2, X_3x_3)$. The rows of this matrix are arranged following the rule

$$A_{w,a,b}(X_1x_1, X_2x_2, X_3x_3) \prec A_{w',a',b'}(X_1x_1, X_2x_2, X_3x_3),$$

if $w < w'$, or if $w = w'$ and $a < a'$, or if $w = w'$, $a = a'$, and $b < b'$. For the monomials, we establish the ordering as

$$x_1^a x_2^b x_3^w \prec x_1^{a'} x_2^{b'} x_3^{w'},$$

based on the same criteria. An example of the lattice basis matrix for $\mu = 2$, $t = 2$, and the polynomial

$$h(x_1, x_2) = x_1(x_2^2 + a_1x_2 + a_0) + 1,$$

with $x_1x_2^2 = x_3 - 1$, is shown in Table 1. Non-zero entries are denoted by $\star$.

The lattice is constructed in such a way that the resulting basis matrix is left triangular, with each diagonal element having the form $X_1^a X_2^b X_3^w e^{\mu-w}$ for a combination (w, a, b) in $\mathcal{E} \cup \mathcal{F}$. As a result, the determinant of the lattice takes the form

$$\det(\mathcal{L}) = X_1^{\lambda_{X_1}} X_2^{\lambda_{X_2}} X_3^{\lambda_{X_3}} e^{\lambda_e}, \tag{1}$$

with $\lambda_{X_1} = \mathcal{B}(a)$, $\lambda_{X_2} = \mathcal{B}(b)$, $\lambda_{X_3} = \mathcal{B}(w)$, $\lambda_e = \mathcal{B}(\mu - w)$, and

$$\mathcal{B}(u) = \sum_{b=0}^{1} \sum_{w=0}^{\mu} \sum_{a=1}^{\mu-w} u + \sum_{b=0}^{\lfloor t \rfloor} \sum_{w=\lfloor \frac{\mu}{t} \rfloor b}^{\mu} \sum_{a=0}^{0} u.$$

$A_{w,a,b}$	1	x_1	x_1x_2	x_1^2	$x_1^2x_2$	x_3	x_2x_3	x_1x_3	$x_1x_2x_3$	x_3^2	$x_2x_3^2$	$x_2^2x_3^2$
$A_{0,0,0}$	e^2	0	0	0	0	0	0	0	0	0	0	0
$A_{0,1,0}$	0	e^2X_1	0	0	0	0	0	0	0	0	0	0
$A_{0,1,1}$	0	0	$e^2X_1X_2$	0	0	0	0	0	0	0	0	0
$A_{0,2,0}$	0	0	0	$e^2X_1^2$	0	0	0	0	0	0	0	0
$A_{0,2,1}$	0	0	0	0	$e^2X_1^2X_2$	0	0	0	0	0	0	0
$A_{1,0,0}$	0	$\star$	$\star$	0	0	eX_3	0	0	0	0	0	0
$A_{1,0,1}$	$\star$	0	$\star$	0	0	$\star$	eX_2X_3	0	0	0	0	0
$A_{1,1,0}$	0	0	0	$\star$	$\star$	0	0	eX_1X_3	0	0	0	0
$A_{1,1,1}$	0	$\star$	0	0	$\star$	0	0	$\star$	$eX_1X_2X_3$	0	0	0
$A_{2,0,0}$	0	$\star$	0	$\star$	$\star$	0	0	$\star$	$\star$	X_3^2	0	0
$A_{2,0,1}$	0	$\star$	$\star$	0	$\star$	$\star$	0	$\star$	$\star$	$\star$	$X_2X_3^2$	0
$A_{2,0,2}$	$\star$	$\star$	$\star$	0	0	$\star$	$\star$	$\star$	$\star$	$\star$	$\star$	$X_2^2X_3^2$

Table 1. The lattice basis matrix for $\mu = 2$ and $t = 2$.

For simplicity in the calculations, we approximate $\lfloor t \rfloor \approx t$ and $\left\lfloor \frac{\mu}{t} \right\rfloor \approx \frac{\mu}{t}$. Set $t = \mu\tau$ for some $\tau \geq 0$, then, the main components of the exponents λ_{X_1}, λ_{X_2}, λ_{X_3}, λ_e, and the lattice dimension $\omega = \mathcal{A}(1)$ satisfy

$$\begin{aligned} \lambda_{X_1} &= \frac{1}{3}\mu^3 + o(\mu^3) \\ \lambda_{X_2} &= \frac{1}{6}\tau^2\mu^3 + o(\mu^3) \\ \lambda_{X_3} &= \frac{1}{3}(\tau+1)\mu^3 + o(\mu^3) \\ \lambda_e &= \frac{1}{6}(\tau+4)\mu^3 + o(\mu^3) \\ \omega &= \frac{1}{2}(\tau+2)\mu^2 + o(\mu^2). \end{aligned} \tag{2}$$

The matrix M undergoes reduction via the LLL algorithm, resulting in a new matrix M' that retains the same determinant. From this reduced matrix, we derive ω polynomials $g_i(x_1, x_2, x_3)$, for $i = 1, \ldots, \omega$, each of which satisfies the congruence

$$g_i(x_1, x_2, x_3) \equiv 0 \pmod{e^\mu}.$$

To obtain the root, we connect Theorem 2 with Theorem 1, specifically considering the case where $j = 3$. As a result, we fix

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

By combining with (1), this simplifies to

$$e^{\lambda_e - \mu(\omega-2)} X^{\lambda_X} Y^{\lambda_Y} Z^{\lambda_Z} < \frac{1}{2^{\frac{\omega(\omega-1)}{4}} (\sqrt{\omega})^{\omega-2}} < 1. \tag{3}$$

Along with the dominant parts (2) and the corresponding bounds

$$X_1 = 4N^{\alpha+\delta-2}, \quad X_2 = 3N^{0.5}, \quad X_3 = 36N^{\alpha+\delta-1}, \quad e = N^{\alpha},$$

and by disregarding some smaller values, we obtain that

$$\tau^2 + 4(\delta - 1)\tau + 4\alpha + 8\delta - 12 < 0, \tag{4}$$

for which the optimal value of τ is determined by $\tau_0 = -2\delta + 2$. To guarantee that $\tau_0 > 0$, the parameter δ must meet

$$\delta < 1. \tag{5}$$

Plugging τ_0 into (4), we get

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

By solving the previous inequality for δ, we obtain

$$\delta < 2 - \sqrt{\alpha}.$$

Together with $\alpha > 1$ and (5), we obtain

$$\delta < \min\left(2 - \sqrt{\alpha}, 1\right) = 2 - \sqrt{\alpha}.$$

Furthermore, since $\delta \geq 0$, the inequality

$$2 - \sqrt{\alpha} > 0,$$

is satisfied if $\alpha < 4$.

In addition to the given conditions, we select three reduced and algebraically independent polynomials $g_i(x_1, x_2, x_3)$ where $1 \leq i \leq 3$. From these, we can extract $(x_1, x_2) = (k, p + q)$ by solving the system of equations $g_i(x_1, x_2, x_3) = 0$ for $i = 1, 2, 3$ over the integers, either using the Gröbner basis method or resultant computations.

Finally, combining $N = pq$ with $x_2 = p + q$ leads to the recovery of the prime factors p and q. This completes the proof.

4 A numerical example

This section provides a detailed numerical example demonstrating that our approach can break a specific RSA variant where an earlier method proves ineffective. The computations were carried out using SageMath 10.4 on a PC running Ubuntu 22.04.3 LTS, equipped with an Intel(R) Core(TM) i5-4460 CPU @ 3.20GHz × 4 and 8.00 GB of RAM.

Let the public key $(N, e) \approx (2^{401}, 2^{799})$ be given by

$$\begin{aligned}
N =&45357598713395153140321457888124008348263841758599262405430897 6\backslash\\
&97340490963264684299656262868801953206221746258363955328 11,\\
e =&23777498869049164992891587741589638456139076772868283639206491 3\backslash\\
&36039741937830380140665037768456888567444366961074922450046677 7\backslash\\
&33571176547374191298900694486972402492997080844069280375450338 1\backslash\\
&01988217377135633662596006092159462203515340980683 81.
\end{aligned}$$

This gives that $e = N^{\alpha}$ with $\alpha \approx 1.9922$.

Write

$$\Lambda(N) = (p-1)^2(q-1)^2 = x_2^2 + a_1 x_2 + a_0,$$

with

$$\begin{aligned}
x_2 &= p + q,\\
a_1 &= -2(N+1),\\
a_0 &= (N+1)^2.
\end{aligned}$$

Specifically, we have

$$\begin{aligned}
a_1 =& -907151974267903062806429157762480166965276835171985248 1086\backslash\\
&17953946809819265293685993125257376039064124434925167279 1065\backslash\\
&624,\\
a_0 =&20573117610453856515069210794296203478710698458587976110 328\backslash\\
&60684444441553160289942374306769429498275161531449932827 664\backslash\\
&39402290424183880869819767073929975427507216457164089014 610\backslash\\
&69349283798785968352496803479524798716459337520078307869 368\backslash\\
&627344.
\end{aligned}$$

Our aim is to find a small solution of the equation

$$x_1(x_2^2 + a_1 x_2 + a_0) + 1 \equiv 0 \pmod{e},$$

To implement the method outlined in Theorem 3, the attacker, who does not know d, p, and q can experiment with different values of δ. Let $\delta = 0.4$. With

these parameters, the inequalities specified by Theorem 3 are satisfied, namely $1 < \alpha < 4$ and $\delta < 2 - \sqrt{\alpha} \approx 0.58854$. Setting then the bounds

$$\begin{aligned}
X_1 =& \lfloor 4N^{\alpha+\delta-2} \rfloor = 84593556141243703579182074721876237528949243904,\\
X_2 =& \lfloor 3N^{1/2} \rfloor = 6389197042043361322138375200782704203704726102304835914929866,\\
X_3 =& X_1 X_2^2 = 34532645158742364585383709283904252396613241012368145624120071897255100245523084047348927768868448893619713884826617771376908934878829058672996296095928566635098982580224.
\end{aligned}$$

To build the lattice $\mathcal{L}$, we select $\mu = t = 3$ and utilize the coefficient vectors of the polynomials $A_{w,a,b}(X_1x_1, X_2x_2, X_3x_3)$, where

$$A_{w,a,b}(x_1, x_2, x_3) = x_1^a x_2^b H(x_1, x_2, x_3)^w e^{\mu - w}, \quad (w, a, b) \in \mathcal{E} \cup \mathcal{F},$$

$$\begin{aligned}
\mathcal{E} &= \{(w, a, b) \mid b = 0, 1,\ w = 0, \ldots, \mu,\ a = 1, \ldots, \mu - w\},\\
\mathcal{F} &= \left\{(w, a, b) \mid b = 0, \ldots, \lfloor t \rfloor,\ w = \left\lfloor \frac{\mu}{t} \right\rfloor b, \ldots, \mu,\ a = 0\right\},
\end{aligned}$$

and the expression $x_1x_2^2$ is substituted with $x_3 - 1$.

The lattice $\mathcal{L}$ has dimension $\omega = 22$. Upon performing lattice reduction through the LLL algorithm, 22 polynomials are generated. Using the Gröbner basis technique, we select three of these polynomials and solve them in the integer domain, yielding

$$\begin{aligned}
x_1 =& 836698386135476817812222872518406307186211 77,\\
x_2 =& 437293191770646679094872037555876887367870158173323560987242 0,\\
x_3 =& 159997929658763465927664834829127211154110714073052286166700893928944004387447490658162717809050679598364098132358986952729411524946976144854470465126493254592582801.
\end{aligned}$$

Using the values of both $x_2 = p + q$ and $N = pq$ gives

$$\begin{aligned}
p =& 268131292295877784572949142081739353395899189826095608468272 7,\\
q =& 169161899474768894521922895474137533971970968347227952518969 3.
\end{aligned}$$

Notice that the LLL algorithm and the Gröbner basis calculations were finished in under 1 second.

The private exponent d can be calculated via the rule

$$d \equiv \frac{1}{e} \pmod{\left((p-1)^2(q-1)^2\right)}.$$

This implies that

$$d = 723940495055544374240447202369395218697349109,$$

and $d = N^{\delta_0}$ for $\delta_0 \approx 0.3718$.

Observe that the condition for breaking the scheme of Nitaj and Seck [14] when $N = p^r q^s$ and $d < N^{\delta_0}$ is given by

$$0 < \delta_0 < 2 - \frac{2(3r+s)}{(r+s)^2}.$$

To compare this with our case, consider setting $r = s = 1$. In this scenario, their bound becomes

$$2 - \frac{2 \times 4}{4} = 0.$$

This result indicates that their method fails to break the scheme in this case.

5 Conclusion

In this paper, we introduced a novel approach to compromising the scheme proposed by Nitaj and Seck when an RSA modulus $N = pq$ is employed. We transformed the key equation $ed - k(p-1)^2(q-1)^2 = 1$ into a modular equation and applied Coppersmith's method along with lattice basis reduction techniques to solve it, allowing for the recovery of the prime factors in polynomial time.

References

1. 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 **1592**, pp. 1–11,Springer, Berlin, Heidelberg, (1999).
2. Boudabra, M., Nitaj, A.: A new generalization of the KMOV cryptosystem, Journal of Applied Mathematics and Computing, June 2018, Volume 57, Issue 12, pp 229–245 (2018).
3. Coppersmith, D.: Small solutions to polynomial equations, and low exponent RSA vulnerabilities. Journal of Cryptology,**10**(4), 233–260, (1997).
4. Feng, Y., Nitaj, A., Pan, Y.: Partial prime factor exposure attacks on some RSA variants. Theoretical Computer Science, **999**, pp. 114549, Elsevier (2024).
5. Howgrave-Graham, N.: Finding small roots of univariate modular equations revisited, In: IMA International Conference on Cryptography and Coding, LNCS 1355, pp. 131–142, Springer, Berlin, Heidelberg (1997).
6. Jochemsz, E., May, A.: A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants, In: ASIACRYPT 2006, LNCS 4284, pp. 267–282, Springer-Verlag (2006).
7. 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 (1991).
8. 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 TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, **78**(1), pp. 27–33, The Institute of Electronics, Information and Communication Engineers (1995)

9. Lenstra, A.K., Lenstra, H.W., Lovász, L.: Factoring polynomials with rational coefficients, Mathematische Annalen, **261**, pp. 513–534, (1982).
10. May, A.: New RSA Vulnerabilities Using Lattice Reduction Methods. PhD thesis, University of Paderborn (2003).
11. 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, **10737** pp. 91–103, Springer, Cham, (2018).
12. Nitaj, A.: Another generalization of Wiener's attack on RSA, In: Vaudenay, S. (Ed.) Africacrypt 2008. LNCS, vol. 5023, pp. 174–190. Springer, Heidelberg (2008)
13. Nitaj, A., Arrifin, M.R.K., Adenan, N.N.H., Abu, N.A.: Classical attacks on a variant of the RSA cryptosystem, LatinCrypt 2021, to appear (2021).
14. Nitaj, A., Seck, M.: A New Public Key Encryption Scheme Based on the Cubic Pell Curve Using Encoding Functions, Moroccan Journal of Algebra and Geometry with Applications (2024). `https://ced.fst-usmba.ac.ma/p/mjaga/wp-content/uploads/2024/12/NitajSeck_MJAGA-2.pdf`
15. 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).
16. Quisquater, J. J., Couvreur, C.: Fast decipherment algorithm for RSA public-key cryptosystem. Electronics Letters, **18**(21), pp. 905-907 (1982).
17. Rahmani, M., Nitaj, A., Ziane, M.: Further cryptanalysis of some variants of the RSA cryptosystem. Journal of Applied Mathematics and Computing, 1-31 (2024).
18. Rivest, R., Shamir, A., Adleman, L.: A Method for Obtaining digital signatures and public-key cryptosystems, Communications of the ACM,**21**(2), 120–126 (1978).
19. 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.
20. Takagi, T.: A fast RSA-type public-key primitive modulo $p^k q$ using Hensel lifting, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences **87**(1), 94–101 (2004).
21. T. Collins, D. Hopkins, S. Langford, and M. Sabin. Public key cryptographic apparatus and Method. US Patent #5,848,159, Jan. 1997 (1997).
22. Wiener, M.: Cryptanalysis of short RSA secret exponents, IEEE Transactions on Information Theory,**36**(3), 553–558 (1990)
23. Zheng, M., Kunihiro, N., Yao, Y.: Cryptanalysis of the RSA variant based on cubic Pell equation. Theor. Comput. Sci. 889, pp. 135–144 (2021).