Bol. Soc. Paran. Mat.
©SPM – E-ISSN-2175-1188
SPM: www.spm.uem.br/bspm

(3s.) **v. 2026 (44) 6** : 1–13.
ISSN-0037-8712
doi:10.5269/bspm.81059

Partial Prime Exposure Attack on the Cubic Pell RSA Cryptosystem

Mostafa Chaker, Mohammed Rahmani, Mhammed Ziane and Siham Ezzouak

ABSTRACT: A recent contribution by Rahmani and Nitaj (AfricaCrypt 2025) investigates the cryptanalysis of an RSA-inspired scheme derived from the cubic Pell curve $t_1^3+ft_2^3+f^2t_3^3-3ft_1t_2t_3 \equiv 1 \pmod{\mathtt{N}}$, where $\mathtt{N}=\mathtt{pq}$ is a standard RSA modulus and the public–private exponent pair satisfies $ed-1 \equiv 0 \pmod{(\mathtt{p}-1)^2(\mathtt{q}-1)^2}$. In this paper, we revisit their attack showing that when an approximation of one prime factor is known, the scheme becomes significantly more vulnerable. Using a variant of Coppersmith's method, one can factor $\mathtt{N}$ in polynomial time under explicit bounds, which improve previous results.

Keywords: RSA, factoring, Coppersmith's technique, Lattice basis reduction, weak exponents.

Contents

1. Introduction

The RSA scheme [21] stands as one of the most influential public-key cryptosystems, having profoundly shaped modern cryptography. It remains a fundamental tool in asymmetric cryptography, widely applied to ensure secure communications, authenticate users, and safeguard confidential data. The security of RSA relies on the computational difficulty of factoring a large modulus of the form $\mathtt{N}=\mathtt{pq}$, with primes of comparable size. To encrypt a plaintext m, one generates in a random way an integer $e>0$ that is coprime with $\varphi(\mathtt{N})=(\mathtt{p}-1)(\mathtt{q}-1)$ and computes $c \equiv m^e \pmod{\mathtt{N}}$. Decryption reverses the process using the modular inverse d of e modulo $\varphi(\mathtt{N})$ through $m \equiv c^d \pmod{\mathtt{N}}$. The exponents e and d are referred to as the encryption and decryption exponents.

In practical deployments, both encryption and decryption operations may impose significant computational overhead. To mitigate this, a common optimization is to employ a small private exponent to expedite the decryption process. However, Wiener [25] proved in 1990 that RSA loses its security when the decryption exponent is too small, namely when $d < \frac{1}{3}\mathtt{N}^{0.25}$. This limitation was subsequently confirmed by Boneh and Durfee [1], who expanded the applicability of the attack to the broader range $d < \mathtt{N}^{0.292}$. Such vulnerabilities have spurred extensive investigations into reinforcing the security of RSA without sacrificing computational efficiency, resulting in the proposal of numerous alternative constructions. Notable instances include CRT-RSA [18] and related constructions [25,8], which preserve the traditional modulus form $\mathtt{N}=\mathtt{pq}$. In contrast, schemes such as Prime-Power RSA [23] and its subsequent

2020 *Mathematics Subject Classification:* 94A60, 11T71.
Submitted December 28, 2025. Published February 17, 2026

Typeset by $\mathcal{B}^{\mathcal{S}}\mathcal{P}_{\mathcal{M}}$ style.
© Soc. Paran. de Mat.

extensions [24,2] modify the underlying modulus to investigate alternative structural designs. Furthermore, some variants replace the traditional Euler totient function with distinct arithmetic formulations to achieve improved performance or security characteristics.

In later work, Murru and Saettone [13] introduced a novel RSA-inspired scheme arising from the cubic Pell relation

$$t_1^3 + ft_2^3 + f^2t_3^3 - 3ft_1t_2t_3 = 1,$$

where f is an element whose cube is congruent to an integer modulo $\mathtt{N}$. In this setting, the modulus retains the standard form $\mathtt{N} = \mathtt{pq}$, while the exponents e and d are linked through

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

This variant was also cryptanalyzed, as noted in [5,19].

Recently, Nitaj and Seck [16] proposed a novel scheme by combining encoding functions together with the cubic Pell curve:

$$t_1^3 + ft_2^3 + f^2t_3^3 - 3ft_1t_2t_3 \equiv 1 \pmod{\mathtt{N}}.$$

The modulus here is chosen of the form $\mathtt{N} = \mathtt{p}^r\mathtt{q}^s$, and the exponents e and d are constrained by

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

Beyond the well-known attacks of Wiener and their improvement by Boneh and Durfee, several cryptanalytic approaches have been developed against various RSA-type schemes, as discussed in [15,26, 22,5]. In the same study, Nitaj and Seck [16] introduced an attack on the above variant. Their analysis establishes that for moduli $\mathtt{N} = \mathtt{p}^r\mathtt{q}^s$, polynomial-time factorization is achievable whenever the secret exponent d is bounded by $\mathtt{N}^{2-\frac{2(3r+s)}{(r+s)^2}}$.

We note that the Nitaj–Seck attack [16] provides a very weak bound to attack the scheme in the classical RSA setting $\mathtt{N} = \mathtt{pq}$ (i.e., $r = s = 1$), since the former bound tends to be 0. This limitation was later addressed by Rahmani and Nitaj [20], who bridged the gap by developing a Coppersmith-based cryptanalytic approach. Specifically, assuming $\mathtt{N} = \mathtt{pq}$ and $e = \mathtt{N}^\alpha$, they demonstrated that the scheme becomes insecure whenever $\mathtt{N} < e < \mathtt{N}^4$ and $d < \mathtt{N}^{2-\sqrt{\alpha}}$.

In the presented work, we revisit the Rahmani et Nitaj's work. More precisely, given a modulus $\mathtt{N} = \mathtt{pq}$ and an approximation $\mathtt{p}_0$ of one of its prime factors, we demonstrate that the Nitaj–Seck scheme is more vulnerable when the parameters satisfy $e = \mathtt{N}^\alpha$, $|\mathtt{p} - \mathtt{p}_0| \le \mathtt{N}^\gamma$, and $d < \mathtt{N}^{2-\sqrt{2\alpha\gamma}}$. When $\gamma = \frac{1}{2}$, our bound retrieves the bound of Rahmani and Nitaj [20]. For $\gamma < \frac{1}{2}$, our method yields improved bounds compared to theirs.

The sequel of this article is structured as follows. Section 2 provides the necessary background. Section 3 applies a variant of Coppersmith's method to analyze and attack the Nitaj–Seck scheme. Section 4 provides a detailed numerical example validating the effectiveness of the proposed attack, while Section 5 presents the conclusion of the paper.

2. Preliminaries

2.1. Preliminary lemmas

Under the assumption that prime factors have equal bit-length, the result from [14] establishes concrete bounds on the prime factors $\mathtt{p}$ and $\mathtt{q}$ relative to the modulus $\mathtt{N}$.

Lemma 2.1. *Any pair of prime numbers of equal bit-length forming* $\mathtt{N} = \mathtt{pq}$ *lies within the range*

$$\frac{2^{0.5}}{2}\,\mathtt{N}^{0.5} < \mathtt{q} < \mathtt{N}^{0.5} < \mathtt{p} < 2^{0.5}\,\mathtt{N}^{0.5}.$$

The result below establishes that, from a known approximation of $\mathtt{p}$, both $\mathtt{q}$ and $\mathtt{p} + \mathtt{q}$ can be approximated (see [5]).

Lemma 2.2. *If* $\mathtt{N} = \mathtt{pq}$ *is a modulus with* $\mathtt{q} < \mathtt{p} < 2\mathtt{q}$*, and* $\mathtt{p}_0$ *is an approximation of* $\mathtt{p}$ *with the error* $|\mathtt{p} - \mathtt{p}_0| = \mathtt{N}^{\lambda}$*. Then defining* $\mathtt{q}_0 = \lfloor \mathtt{N}/\mathtt{p}_0 \rfloor$ *provides an approximation of* $\mathtt{q}$ *from which*

$$|\mathtt{q} - \mathtt{q}_0| < \mathtt{N}^{\gamma}, \quad |\mathtt{p} + \mathtt{q} - \mathtt{p}_0 - \mathtt{q}_0| < 2\mathtt{N}^{\gamma}.$$

The result that follows demonstrates that the quantity $(\mathtt{p}-1)^2(\mathtt{q}-1)^2$ can be bounded from below in terms of the modulus $\mathtt{N}$ (see [20]).

Lemma 2.3. *For each pair of primes of equal bit-length forming* $\mathtt{N} = \mathtt{pq}$*, we have*

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

2.2. The scheme of Nitaj and Seck

The cryptographic scheme proposed by Nitaj and Seck [16] is defined over the curve

$$\mathcal{C}_f(\mathtt{N}): \quad t_1^3 + f t_2^3 + f^2 t_3^3 - 3 f t_1 t_2 t_3 \equiv 1 \pmod{\mathtt{N}},$$

where f is a cubic residue modulo $\mathtt{N}$. In both the encryption and decryption procedures, an encoding function $\mathcal{E}$ is employed to map

$$(m_{t_1}, m_{t_2}) \in \mathbb{Z}/\mathtt{N}\mathbb{Z} \times \mathbb{Z}/\mathtt{N}\mathbb{Z}$$

to

$$\mathcal{E}\big((m_{t_1}, m_{t_2}), g, \mathtt{N}\big) = (t_1, t_2, t_3) \in \mathcal{C}_f(\mathtt{N}),$$

where f satisfies $f \equiv g^3 \pmod{\mathtt{N}}$.

Conversely, a decoding function $\mathcal{D}$ is used to invert the mapping from $(t_1, t_2, t_3) \in \mathcal{C}_f(\mathtt{N})$, under the same condition $f \equiv g^3 \pmod{\mathtt{N}}$, via

$$\mathcal{D}\big((t_1, t_2, t_3), g, \mathtt{N}\big) = (m_{t_1}, m_{t_2}) \in \mathbb{Z}/\mathtt{N}\mathbb{Z} \times \mathbb{Z}/\mathtt{N}\mathbb{Z}.$$

The cryptosystem is specified as follows.

Key generation

1. Define three parameters: a security parameter ρ and two small integers r and s.
2. Pick two primes $\mathtt{p}$ and $\mathtt{q}$ randomly, each having ρ bits, with the condition $\mathtt{p} \equiv \mathtt{q} \equiv 1 \pmod 3$.
3. Construct the RSA-like modulus
$$\mathtt{N} = \mathtt{p}^r \mathtt{q}^s$$
and compute the cubic totient
$$\psi(r, s, \mathtt{N}) = \mathtt{p}^{2(r-1)} \mathtt{q}^{2(s-1)} (\mathtt{p}-1)^2 (\mathtt{q}-1)^2.$$
4. Pick an integer g randomly from $\{1, \ldots, \mathtt{N}-1\}$ and set
$$f \equiv g^3 \pmod{\mathtt{N}},$$
with f required to be a nonzero cubic residue modulo both $\mathtt{p}$ and $\mathtt{q}$.
5. Select an integer e satisfying $1 \le e < \mathtt{N}$ and
$$\gcd\big(e, \mathtt{pq}(\mathtt{p}-1)(\mathtt{q}-1)\big) = 1.$$
6. Compute the modular inverse
$$d \equiv e^{-1} \pmod{\psi(r, s, \mathtt{N})}.$$
7. The key pair is then $(\mathtt{N}, g, e)$ for the public key and $(\mathtt{N}, g, d)$ for the private key.

Encryption

1. Represent the plaintext as $M = (x_M, y_M)$ in $\mathbb{Z}/\mathtt{N}\mathbb{Z} \times \mathbb{Z}/\mathtt{N}\mathbb{Z}$.
2. Compute $f \equiv g^3 \pmod{\mathtt{N}}$.
3. Obtain the triplet (t_1, t_2, t_3) by applying the encoding function $\mathcal{E}$ to (x_M, y_M) with parameters g and $\mathtt{N}$.
4. Compute $C = (x_C, y_C, z_C)$ by exponentiating (t_1, t_2, t_3) to the power e on the curve $\mathcal{C}_f(\mathtt{N})$.
5. Define the ciphertext as
$$(c_{t_1}, c_{t_2}) = \mathcal{D}(C, g, \mathtt{N}).$$

Decryption

Follow these steps to recover the plaintext:

1. Interpret the ciphertext as an ordered pair (c_{t_1}, c_{t_2}) in $\mathbb{Z}/\mathtt{N}\mathbb{Z} \times \mathbb{Z}/\mathtt{N}\mathbb{Z}$.
2. Calculate $f \equiv g^3 \pmod{\mathtt{N}}$.
3. Evaluate the triplet (x_C, y_C, z_C) by applying the encoding function $\mathcal{E}$ to (c_{t_1}, c_{t_2}) with parameters g and $\mathtt{N}$.
4. Compute (t_1, t_2, t_3) by raising (x_C, y_C, z_C) to the exponent d on the curve $\mathcal{C}_f(\mathtt{N})$.
5. Recover the plaintext (x_M, y_M) by applying the function $\mathcal{D}$ to (t_1, t_2, t_3) :
$$(x_M, y_M) = \mathcal{D}\big((t_1, t_2, t_3), g, \mathtt{N}\big).$$

2.3. Euclidean Lattices

We begin by recalling basic definitions related to Euclidean lattices [11]. A Euclidean lattice is a discrete subgroup of $\mathbb{R}^n$. Equivalently, let $n \geq \omega > 0$, and let $\vartheta_1, \ldots, \vartheta_\omega$ be a basis of $\mathbb{R}^\omega$. The lattice spanned by these vectors is given by

$$\mathcal{L} = \sum_{1 \leq l \leq \omega} \mathbb{Z} \cdot \vartheta_l = \left\{ \sum_{1 \leq l \leq \omega} x_l \vartheta_l : x_l \in \mathbb{Z} \text{ for all } l \right\}.$$

In the special case where $\omega = n$, the lattice is referred to as *full*. If the lattice is contained in $\mathbb{Z}^n$, it is called *integer*. A canonical example is the integer lattice $\mathbb{Z}^n$ itself. It is spanned by the standard basis vectors

$$\vartheta_l = (0, \ldots, 0, 1, 0, \ldots, 0)^T, \quad l \in \{1, \ldots, n\},$$

where the entry 1 appears in the l-th position.

The matrix M, whose rows consist of the vectors $\vartheta_1, \vartheta_2, \ldots, \vartheta_\omega$, represents the lattice, and its determinant is given by

$$\det(\mathcal{L}) = \sqrt{\det(MM^T)}.$$

In the full-rank case, this expression simplifies to

$$\det(\mathcal{L}) = |\det(M)|.$$

For lattices of rank $\omega \geq 2$, there exist infinitely many distinct bases. Nevertheless, all bases share the same cardinality and determinant. Constructing a basis of short vectors is an increasingly demanding task as the dimension rises. To overcome the computational difficulty of finding short vectors, the LLL algorithm was proposed by Lenstra, Lenstra, and Lovász [10] in 1982, providing a polynomial-time method to obtain a near-optimal basis. A famous property from [12] in the field of cryptanalysis is the following one.

Theorem 2.1. *Reducing a lattice with an initial basis* $\{\vartheta_1, \ldots, \vartheta_\omega\}$ *produces a newly obtained basis* $\{\vartheta_1^*, \ldots, \vartheta_\omega^*\}$ *which meets the following inequalities:*

$$\|\vartheta_1^*\| \leq \cdots \leq \|\vartheta_i^*\| \leq 2^{\frac{\omega(\omega-1)}{4(\omega+1-l)}} \det(\mathcal{L})^{\frac{1}{\omega+1-l}}, \quad \textit{for } l = 1, \ldots, \omega.$$

2.4. Finding modular roots

Coppersmith [3] proposed in 1996 a powerful lattice-based approach to compute modular roots of equations of the type

$$S(t) \equiv 0 \pmod{A},$$

even if A has unknown factors. The method has since been broadened to address polynomials with the structure

$$S(t_1, t_2, \ldots, t_n) = \sum_{i_1, i_2, \ldots, i_n} n_{i_1, i_2, \ldots, i_n} t_1^{i_1} t_2^{i_2} \cdots t_n^{i_n},$$

with $n_{i_1, i_2, \ldots, i_n} \in \mathbb{Z}$. The norm associated with such polynomials is

$$\|S(t_1, t_2, \ldots, t_n)\| = \sqrt{\sum n_{i_1, i_2, \ldots, i_n}^2}.$$

In 1997, Howgrave-Graham [6] enhanced and simplified the original Coppersmith approach, yielding the following criterion for finding small modular roots.

Theorem 2.2 (Howgrave-Graham). *Let $S(t_1, t_2, \ldots, t_n) \in \mathbb{Z}[t_1, t_2, \ldots, t_n]$ be a polynomial with no more than ω monomial terms, and $A \geq 0$ an integer. Under the following three statements*

1. $S(\chi_1, \chi_2, \ldots, \chi_n) \equiv 0 \pmod{A}$,
2. $\|S(t_1 Y_1, t_2 Y_2, \ldots, t_n Y_n)\| < \frac{A}{\sqrt{\omega}}$,
3. *For* $1 \leq i \leq n$, $|\chi_i| < Y_i$,

one has $S(\chi_1, \chi_2, \ldots, \chi_n) = 0$ in $\mathbb{Z}$.

As the number of variables increases, Coppersmith-based methods generally rely on heuristic reasoning. We adopt the heuristic assumption [1,7,17,26] stated below.

Assumption 1. The polynomials $\Gamma_1, \ldots, \Gamma_\omega$ generated by the LLL algorithm form an algebraically independent set. That is, any polynomial Q with integer coefficients satisfying $Q(\Gamma_1, \ldots, \Gamma_\omega) = 0$ must be identically zero.

Given this assumption, the root $(\chi_1, \chi_2, \ldots, \chi_n)$ of the equations

$$\Gamma_i(\chi_1, \chi_2, \ldots, \chi_n) = 0, \quad i = 1, \ldots, \omega,$$

can be extracted employing Gröbner basis computations or resultants.

3. The main results

A cryptanalytic approach for the Nitaj–Seck scheme is proposed in this section, exploiting the availability of an approximation to one RSA prime factor.

Theorem 3.1. *Let $\mathtt{N}$ denote an RSA modulus composed of two primes $\mathtt{p}$ and $\mathtt{q}$ having identical bit-lengths, and let $e = \mathtt{N}^\alpha$ be an encryption exponent. Suppose that we known an approximation $\mathtt{p}_0$ of $\mathtt{p}$ with error $|\mathtt{p} - \mathtt{p}_0| \leq \mathtt{N}^\gamma$, and the decryption exponent d is such that $ed - k\Psi(\mathtt{N}) = 1$ with $k \in \mathbb{Z}$, where $\Psi(\mathtt{N}) = (\mathtt{p}-1)^2(\mathtt{q}-1)^2$. Then, under the following constraints*

$$0 \leq \gamma \leq \frac{1}{2}, \quad 2\gamma < \alpha < \frac{2}{\gamma}, \quad \text{and} \quad \delta < 2 - \sqrt{2\alpha\gamma},$$

the factor pair $(\mathtt{p}, \mathtt{q})$ can be efficiently obtained in polynomial time.

Proof:

The identity $ed - k\Psi(\mathtt{N}) = 1$ can be reformulated as

$$f_e(t_1, t_2) = t_1 t_2^2 - 2b t_1 t_2 + b^2 t_1 + 1 \equiv 0 \pmod{e},$$

for $\Psi(\mathtt{N}) = t_2^2 - 2bt_2 + b^2$, $t_1 = k$, $t_2 = \mathtt{p} + \mathtt{q} - \mathtt{p}_0 - \mathtt{q}_0$, and

$$b = \mathtt{N} - \mathtt{p}_0 - \mathtt{q}_0 + 1.$$

To identify small modular roots of $f_e(t_1, t_2) \equiv 0 \pmod{e}$, we rely on Coppersmith's method. For this purpose, we introduce an auxiliary variable $t_3 = t_1 t_2^2 + 1$, which allows us to rewrite the polynomial as $f_e(t_1, t_2) = F_e(t_1, t_2, t_3)$, where

$$F_e(t_1, t_2, t_3) = t_3 - 2bt_1t_2 + b^2 t_1.$$

Next, for a parameter $t > 0$ to be optimized later, we consider an integer $\kappa \geq 0$ and the following list of trivariate polynomial equations:

$$F^{(e)}_{\epsilon_1,\epsilon_2,\epsilon_3}(t_1, t_2, t_3) = t_1^{\epsilon_2} t_2^{\epsilon_3} F_e(t_1, t_2, t_3)^{\epsilon_1} e^{\kappa - \epsilon_1}, \quad (\epsilon_1, \epsilon_2, \epsilon_3) \in \mathcal{I} \cup \mathcal{J},$$

with

$$\mathcal{I} = \{(\epsilon_1, \epsilon_2, \epsilon_3) \mid \epsilon_3 = 0, 1,\ \epsilon_1 = 0, \ldots, \kappa,\ \epsilon_2 = 1, \ldots, \kappa - \epsilon_1\},$$
$$\mathcal{J} = \left\{(\epsilon_1, \epsilon_2, \epsilon_3) \;\middle|\; \epsilon_3 = 0, \ldots, \lfloor t \rfloor,\ \epsilon_1 = \left\lfloor \frac{\kappa}{t} \right\rfloor \epsilon_3, \ldots, \kappa,\ \epsilon_2 = 0\right\},$$

together with the replacement of $t_1 t_2^2$ by $t_3 - 1$.

Since (t_1, t_2) is a solution of $f_e(t_1, t_2) \equiv 0 \pmod{e}$, the triple (t_1, t_2, t_3) also satisfies $F_e(t_1, t_2, t_3) \equiv 0 \pmod{e}$, and therefore

$$F^{(e)}_{\epsilon_1,\epsilon_2,\epsilon_3}(t_1, t_2, t_3) \equiv 0 \pmod{e^\kappa},$$

for every $(\epsilon_1, \epsilon_2, \epsilon_3)$ in $\mathcal{I} \cup \mathcal{J}$.

Following Coppersmith's technique, we search suitable bounds T_1, T_2 and T_3 such that

$$|t_1| \leq T_1, \quad |t_2| \leq T_2, \quad |t_3| \leq T_3.$$

From Lemma 2.3, we get $\Psi(\mathtt{N}) > \frac{\mathtt{N}^2}{4}$. This implies that

$$|t_1| = \left|\frac{ed - 1}{\Psi(\mathtt{N})}\right| < 4ed\mathtt{N}^{-2} \leq 4\mathtt{N}^{\alpha + \delta - 2} = T_1.$$

On the other hand, according to Lemma 2.2, we get

$$|t_2| = |\mathtt{p} + \mathtt{q} - \mathtt{p}_0 - \mathtt{q}_0| < 2\mathtt{N}^\gamma = T_2.$$

So a bound for $t_3 = t_1 t_2^2 + 1$ can be set as $T_1 T_2^2$.

We next associate a lattice $\mathcal{L}$ with a basis matrix $\mathcal{B}$, whose rows are formed from the coefficient vectors of the scaled polynomial $F^{(e)}_{\epsilon_1,\epsilon_2,\epsilon_3}(T_1t_1, T_2t_2, T_3t_3)$. The rows are arranged lexicographically, that is

$$F^{(e)}_{\epsilon_1,\epsilon_2,\epsilon_3}(T_1t_1, T_2t_2, T_3t_3) \prec F^{(e)}_{\epsilon_1',\epsilon_2',\epsilon_3'}(T_1t_1, T_2t_2, T_3t_3),$$

if $\epsilon_1 < \epsilon_1'$, or if $\epsilon_1 = \epsilon_1'$ and $\epsilon_2 < \epsilon_2'$, or if $\epsilon_1 = \epsilon_1'$, $\epsilon_2 = \epsilon_2'$, and $\epsilon_3 < \epsilon_3'$. Similarly for the columns represented by $t_1^{\epsilon_2} t_2^{\epsilon_3} t_3^{\epsilon_1}$, we have

$$t_1^{\epsilon_2} t_2^{\epsilon_3} t_3^{\epsilon_1} \prec t_1^{\epsilon_2'} t_2^{\epsilon_3'} t_3^{\epsilon_1'},$$

if $\epsilon_1 < \epsilon_1'$, or if $\epsilon_1 = \epsilon_1'$ and $\epsilon_2 < \epsilon_2'$, or if $\epsilon_1 = \epsilon_1'$, $\epsilon_2 = \epsilon_2'$, and $\epsilon_3 < \epsilon_3'$.

For instance, the matrix $\mathcal{B}$ for $\kappa = 2$, $t = 1$ can be illustrated in Table 1, for which $\star$ represents non-zero entries.

In Coppermith's framework, the lattice is designed so that its basis matrix becomes lower triangular, where each diagonal entry is expressed as $T_1^{\epsilon_2} T_2^{\epsilon_3} T_3^{\epsilon_1} e^{\kappa - \epsilon_1}$ for some triplet $(\epsilon_1, \epsilon_2, \epsilon_3)$ belonging to $\mathcal{I} \cup \mathcal{J}$. Consequently, the determinant of the constructed lattice can be written as

$$\det(\mathcal{L}) = T_1^{\theta_{T_1}} T_2^{\theta_{T_2}} T_3^{\theta_{T_3}} e^{\theta_e}, \tag{3.1}$$

$F^{(e)}_{\epsilon_1,\epsilon_2,\epsilon_3}$	1	t_1	t_1t_2	t_1^2	$t_1^2t_2$	t_3	t_1t_3	$t_1t_2t_3$	t_3^2	$t_2t_3^2$
$F^{(e)}_{0,0,0}$	e^2	0	0	0	0	0	0	0	0	0
$F^{(e)}_{0,1,0}$	0	e^2T_1	0	0	0	0	0	0	0	0
$F^{(e)}_{0,1,1}$	0	0	$e^2T_1t_2$	0	0	0	0	0	0	0
$F^{(e)}_{0,2,0}$	0	0	0	$e^2T_1^2$	0	0	0	0	0	0
$F^{(e)}_{0,2,1}$	0	0	0	0	$e^2T_1^2T_2$	0	0	0	0	0
$F^{(e)}_{1,0,0}$	0	$\star$	$\star$	0	0	eT_3	0	0	0	0
$F^{(e)}_{1,1,0}$	0	0	0	$\star$	$\star$	0	eT_1T_3	0	0	0
$F^{(e)}_{1,1,1}$	0	$\star$	0	0	$\star$	0	$\star$	$eT_1T_2T_3$	0	0
$F^{(e)}_{2,0,0}$	0	$\star$	0	$\star$	$\star$	0	$\star$	$\star$	T_3^2	0
$F^{(e)}_{2,0,1}$	0	$\star$	$\star$	0	$\star$	$\star$	$\star$	$\star$	$\star$	$T_2T_3^2$

Table 1: The lattice basis matrix associated with $\kappa = 2$ and $t = 1$.

with $\theta_{T_1} = \mathcal{C}(\epsilon_2)$, $\theta_{T_2} = \mathcal{C}(\epsilon_3)$, $\theta_{T_3} = \mathcal{C}(\epsilon_1)$, $\theta_e = \mathcal{C}(\kappa - \epsilon_1)$, and

$$\mathcal{C}(u) = \sum_{\epsilon_3=0}^{1} \sum_{\epsilon_1=0}^{\kappa} \sum_{\epsilon_2=1}^{\kappa-\epsilon_1} u + \sum_{\epsilon_3=0}^{\lfloor t \rfloor} \sum_{\epsilon_1=\left\lfloor \frac{\kappa}{t} \right\rfloor \epsilon_3}^{\kappa} \sum_{\epsilon_2=0}^{0} u.$$

To simplify the forthcoming analysis, we take the approximations $\lfloor t \rfloor \approx t$ and $\left\lfloor \frac{\kappa}{t} \right\rfloor \approx \frac{\kappa}{t}$. Letting $t = \kappa\tau$ for some $\tau \geq 0$, the dominant terms of the exponents θ_{T_1}, θ_{T_2}, θ_{T_3}, θ_e, together with the dimension $D = \mathcal{C}(1)$, satisfy

$$\begin{aligned} \theta_{T_1} &= \frac{1}{3}\kappa^3 + o(\kappa^3) \\ \theta_{T_2} &= \frac{1}{6}\tau^2\kappa^3 + o(\kappa^3) \\ \theta_{T_3} &= \frac{1}{3}(\tau+1)\kappa^3 + o(\kappa^3) \\ \theta_e &= \frac{1}{6}(\tau+4)\kappa^3 + o(\kappa^3) \\ D &= \frac{1}{2}(\tau+2)\kappa^2 + o(\kappa^2). \end{aligned} \tag{3.2}$$

The matrix $\mathcal{B}$ is subsequently subjected to LLL reduction, producing a new matrix $\mathcal{C}$ while leaving the determinant unchanged. From the LLL-reduced basis, one derives D polynomials $\Gamma_i(t_1, t_2, t_3)$, for $i = 1, \ldots, D$, each of which satisfies the modular relation

$$\Gamma_i(t_1, t_2, t_3) \equiv 0 \pmod{e^\kappa}.$$

To extract the desired root, we combine the results of Theorem 2.2 and Theorem 2.1, focusing on the particular case where $j = 3$. Consequently, we set

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

By incorporating equation (3.1), the expression simplifies to

$$e^{\theta_e} T_1^{\theta_{T_1}} T_2^{\theta_{T_2}} T_3^{\theta_{T_3}} < \frac{1}{2^{\frac{D(D-1)}{4}} \left(\sqrt{D}\right)^{D-2}} e^{\kappa(D-2)} < e^{\kappa D}. \tag{3.3}$$

Taking the dominant parts given in (3.2) and their associated bounds

$$T_1 = 4\mathtt{N}^{\alpha+\delta-2}, \quad T_2 = 2\mathtt{N}^{\gamma}, \quad T_3 = 16\mathtt{N}^{\alpha+\delta-2+2\gamma}, \quad e = \mathtt{N}^{\alpha},$$

and by neglecting lower-order terms, we deduce that

$$\gamma\tau^2 + 2(\delta + 2\gamma - 2)\tau + 2\alpha + 4\delta + 4\gamma - 8 < 0, \tag{3.4}$$

where the optimal choice of τ is given by

$$\tau_0 = \frac{2 - \delta - 2\gamma}{\gamma}.$$

To ensure that τ_0 remains positive, the parameters must satisfy

$$\delta < 2 - 2\gamma. \tag{3.5}$$

Substituting τ_0 into (3.4) yields

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

Solving the preceding inequality for δ gives

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

Combining this with the condition $\alpha > 2\gamma$ and equation (3.5), we arrive at

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

Moreover, given that $\delta > 0$, the following inequality $2 - \sqrt{2\gamma\alpha} > 0$ is fulfilled if $\alpha < \frac{2}{\gamma}$. Under the specified assumptions along with Assumption 1, three reduced polynomials $\Gamma_1, \Gamma_2, \Gamma_3$ in the variables (t_1, t_2, t_3) are selected such that they form an algebraically independent set. By solving the integer system

$$\Gamma_i(t_1, t_2, t_3) = 0, \quad i = 1, 2, 3,$$

using either Gröbner bases or resultants, we can compute

$$(t_1, t_2) = (k, \mathtt{p} + \mathtt{q} - \mathtt{p}_0 - \mathtt{q}_0).$$

In conclusion, using $\mathtt{N} = \mathtt{pq}$ together with $t_2 + \mathtt{p}_0 + \mathtt{q}_0 = \mathtt{p} + \mathtt{q}$ determines the primes $\mathtt{p}$ and $\mathtt{q}$, thereby completing the proof. □

□

A direct consequence of the preceding theorem is that, when the gap $|p - q|$ is sufficiently small, the prime p can be well approximated by $\sqrt{N}$, as established in Lemma 2.1. In this setting, our attack is applicable to small secret exponents and yields improved theoretical bounds compared to those obtained in [20].

Corollary 3.1. *Let* $\mathtt{N}$ *denote an RSA modulus composed of two primes* $\mathtt{p}$ *and* $\mathtt{q}$ *having identical bit-lengths, and let* $e = \mathtt{N}^{\alpha}$ *be an encryption exponent. Suppose that* $|\mathtt{p} - \mathtt{q}| < N^{\gamma}$ *and the decryption exponent* d *is such that* $ed - k\Psi(\mathtt{N}) = 1$ *with* $k \in \mathbb{Z}$*, where* $\Psi(\mathtt{N}) = (\mathtt{p}-1)^2(\mathtt{q}-1)^2$*. Then, under the following constraints*

$$0 \le \gamma \le \frac{1}{2}, \quad 2\gamma < \alpha < \frac{2}{\gamma}, \quad \text{and} \quad \delta < 2 - \sqrt{2\alpha\gamma},$$

the factor pair (p, q) *can be efficiently obtained in polynomial time.*

Proof:

It suffices to observe that $\mathtt{p}_0 = \lfloor\sqrt{\mathtt{N}}\rfloor$ can be approximated by $\mathtt{N}^{0.5}$ when $\mathtt{N}$ is large enough. In such a case, we use Lemma 2.1, which yields

$$0 < |\mathtt{p} - \mathtt{p}_0| \approx |\mathtt{p} - \mathtt{N}^{0.5}| < |\mathtt{p} - \mathtt{q}| < \mathtt{N}^{\gamma}.$$

Hence, Theorem 3.1 can be applied to $\mathtt{p}_0 = \lfloor\sqrt{\mathtt{N}}\rfloor$ and $\mathtt{q}_0 = \lfloor\frac{\mathtt{N}}{\mathtt{p}_0}\rfloor$ with $|\mathtt{p} - \mathtt{p}_0| < \mathtt{N}^{\gamma}$. This finishes the demonstration. □ □

4. A numerical example

This section provides a detailed numerical example demonstrating that the proposed method successfully breaks a specific RSA variant for which earlier techniques are ineffective. All experiments were carried out in SageMath 10.4 on a machine running Ubuntu 22.04.3 LTS, equipped with an Intel(R) Core(TM) i5-4460 CPU @ 3.20GHz × 4 and 8 GB of RAM.

Consider a public key $(\mathtt{N}, e) \approx (2^{512}, 2^{1023})$ defined as follows

$$\begin{aligned}
\mathtt{N} =& 8631765886976097647127189021937992660759124525093764765593844109387793949659127949714 7\backslash \\
& 8741226378151864248684751482164470544812540687440178883341639177 6457, \\
e =& 6819436587258726123926835632759578417038254418086843901834529218018723048787618676746 1\backslash \\
& 5556788896979318182896821882344865671061158697125494586437995085183924207578741302628 4\backslash \\
& 3865327505680043986774794532515334920477147942477718270021916707188634850766179842508 3\backslash \\
& 39435736251298242174937390497869361174457475854101.
\end{aligned}$$

From this, we have $e = \mathtt{N}^{\alpha}$ with $\alpha \approx 1.99975$.

Assume that we have 62 bits of the most significant bits of $\mathtt{p}$. Then, we set $\mathtt{p}_0$ and $\mathtt{q}_0 = \left\lfloor \frac{\mathtt{N}}{\mathtt{p}_0} \right\rfloor$ as

$$\begin{aligned}
\mathtt{p}_0 =& 111910390438478239186936975298304923371579061126458447581470584901530168590335, \\
\mathtt{q}_0 =& 77131049701067173365789658056755204053648229032353055415096289859347725786560,
\end{aligned}$$

and write

$$\Psi(\mathtt{N}) = (\mathtt{p} - 1)^2(\mathtt{q} - 1)^2 = t_2^2 - 2bt_2 + b^2,$$

for

$$\begin{aligned}
t_2 &= \mathtt{p} + \mathtt{q} - \mathtt{p}_0 - \mathtt{q}_0, \\
b &= \mathtt{N} - \mathtt{p}_0 - \mathtt{q}_0 + 1.
\end{aligned}$$

In particular, we obtain

$$\begin{aligned}
b =& 8631765886976097647127189021937992660759124525093764765593844109387793949658938908274\backslash \\
& 64786685122879200913178738739641741528931390387783491407253849739 9563.
\end{aligned}$$

Our goal is to determine a small solution to the trivariate polynomial equation

$$F_e(t_1, t_2, t_3) = t_3 - 2bt_1t_2 + b^2t_1 \equiv 0 \pmod{e}.$$

The procedure of Theorem 3.1 can be executed by an adversary lacking knowledge of d, $\mathtt{p}$, and $\mathtt{q}$ through testing different choices of δ and γ. For instance, setting $(\delta, \gamma) = (0.63, 0.36)$ satisfies the hypotheses of Theorem 3.1, namely $2\gamma = 0.72 < \alpha < \frac{2}{\gamma} \approx 5.55$ and $\delta < 2 - \sqrt{2\gamma\alpha} \approx 0.800075$.

We then consider the following bounds:

$$\begin{aligned} T_1 =& \lfloor 4\mathtt{N}^{\alpha+\delta-2} \rfloor = 349396658849257802787724638763114429112874297090639458727141335448487404389\backslash \\ & 188703371957724124282\,88, \\ T_2 =& \lfloor 2\mathtt{N}^{\gamma} \rfloor = 5224273087596015873536555291683081666913021861448 7515136, \\ T_3 =& T_1 T_2^2 = 953609324512165340185366581486829518219282060777891672419780869812137105244 3603\backslash \\ & 2044525275032040534867279211995290513595878469923651914237412450872313574576 6444850022\backslash \\ & 9372200565847771312289512034267890528865 4848. \end{aligned}$$

For the lattice construction we fix $\kappa = 4$ and $t = 3$ and build $\mathcal{L}$ from the coefficient vectors of the polynomials $F^{(e)}_{\epsilon_1,\epsilon_2,\epsilon_3}(T_1 t_1, T_2 t2, T_3 t_3)$, where

$$F^{(e)}_{\epsilon_1,\epsilon_2,\epsilon_3}(t_1,t_2,t_3) = t_1^{\epsilon_2} t_2^{\epsilon_3} F_e(t_1,t_2,t_3)^{\epsilon_1} e^{\kappa-\epsilon_1}, \quad (\epsilon_1,\epsilon_2,\epsilon_3) \in \mathcal{I} \cup \mathcal{J},$$

with

$$\begin{aligned} \mathcal{I} &= \{(\epsilon_1,\epsilon_2,\epsilon_3) \mid \epsilon_3 = 0,1,\ \epsilon_1 = 0,\dots,\kappa,\ \epsilon_2 = 1,\dots,\kappa-\epsilon_1\}, \\ \mathcal{J} &= \left\{(\epsilon_1,\epsilon_2,\epsilon_3) \mid \epsilon_3 = 0,\dots,\lfloor t \rfloor,\ \epsilon_1 = \left\lfloor \frac{\kappa}{t} \right\rfloor \epsilon_3,\dots,\kappa,\ \epsilon_2 = 0\right\}, \end{aligned}$$

and in every polynomial we substitute the term $t_1 t_2^2$ with the expression $t_3 - 1$

In this case, the dimension of the lattice is $D = 34$. Applying then the LLL algorithm produces 34 polynomials. From these, we choose three using the Gröbner basis method and solve them over the integers, obtaining

$$\begin{aligned} t_1 =& 134886701233279741286817501560698818545757122643288960919304795140235161135431495912390\backslash \\ & 2096594722, \\ t_2 =& -3557091324921755728066668042210992847724893102905143493, \\ t_3 =& 170670776585008984319313354107204488410540182309571397692645704725985646124192509115901\backslash \\ & 163121638323695197759769111026754351007420263526892080291163537823236542381921079275962\backslash \\ & 5594653289110796879633430114 3379. \end{aligned}$$

Using the known values of $t_2 + \mathtt{p}_0 + \mathtt{q}_0 = \mathtt{p} + \mathtt{q}$ together with $\mathtt{N} = \mathtt{pq}$ allows us to determine

$$\begin{aligned} \mathtt{p} =& 11191039043847823918692552955291248354279464356705291944275956325265503177 7413, \\ \mathtt{q} =& 77131049701067173365797546710822722126704579923716372560959586615119957455989. \end{aligned}$$

Remarkably, the LLL reduction and Gröbner basis computations were completed in under four seconds.

The decryption exponent d can be computed as the multiplication inverse of e modulo $(\mathtt{p}-1)^2(\mathtt{q}-1)^2$, resulting in

$$\begin{aligned} d =& 147373685363820111458424596597177069155815715261810642969170789712224271949682645233153\backslash \\ & 2181688893, \end{aligned}$$

and $d = \mathtt{N}^{\delta_0}$ for $\delta_0 \approx 0.62472$.

5. Comparison with Previous Attacks

Against Nitaj and Seck's Method.

For the cryptosystem analyzed by Nitaj and Seck [16], where $\mathtt{N} = \mathtt{p}^r \mathtt{q}^s$ and the private exponent satisfies $d < \mathtt{N}^{\delta_0}$, the condition under which their attack succeeds is

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

In our case, $r = s = 1$, so the bound simplifies to

$$2 - \frac{2 \cdot 4}{4} = 0,$$

demonstrating that their method is ineffective for this particular configuration.

Against Rahmani and Nitaj's Attack.

In 2025, Rahmani and Nitaj [20] extended the previous result of Nitaj and Seck for $r = s = 1$, establishing that if

$$e = N^{\alpha}, \qquad d < \mathtt{N}^{\delta}, \qquad 1 < \alpha < 4, \qquad \delta < 2 - \sqrt{\alpha},$$

then the cryptosystem can be broken in polynomial time.

By applying Theorem 3.1 with $\gamma = 0.5$, we recover these same bounds, indicating that the approach of Rahmani and Nitaj [20] is a special case of our method. Furthermore, by taking $\gamma < 0.5$ in our theorem, the improvement of our bound over theirs can be quantified as

$$\Delta = (2 - \sqrt{2\gamma\alpha}) - (2 - \sqrt{\alpha}) = \sqrt{\alpha}\,(1 - \sqrt{2\gamma}) > 0,$$

clearly showing that our result strictly improves upon theirs.

In the numerical example discussed previously, we obtained $\delta_0 > 2 - \sqrt{\alpha} \approx 0.5858$, demonstrating that their attack would not succeed in this instance.

6. Conclusion

We introduced a cryptanalytic attack on the Nitaj–Seck RSA variant when the modulus $\mathtt{N} = \mathtt{pq}$ and an approximation of one prime factor $\mathtt{p}$ is available. By expressing the relation

$$ed - k(\mathtt{p} - 1)^2(\mathtt{q} - 1)^2 = 1$$

in a polynomial modular equation, we apply a lattice-based strategy rooted in Coppersmith's framework to compute the unknown values. The proposed approach improved upon earlier bounds for breaking the Nitaj–Seck scheme and permits polynomial-time recovery of the prime factors.

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. Elkamchouchi, H., Elshenawy, K., Shaban, H., *Extended RSA cryptosystem and digital signature schemes in the domain of Gaussian integers.* In : The 8th International Conference on Communication Systems, 2002. ICCS 2002. vol. 1, pp. 91–95. IEEE (2002)

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

6. 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).

7. 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).

8. 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).

9. Kuwakado, H., Koyama, K., Tsuruoka, Y., *A New RSA-Type Scheme Based on Singular Cubic Curves with equation $y^2 \equiv x^3 + bx^2 \ (mod\ N)$*. IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, **78**(1), pp. 27–33, The Institute of Electronics, Information and Communication Engineers (1995)

10. Lenstra, A.K., Lenstra, H.W., Lovász, L., *Factoring polynomials with rational coefficients,* Mathematische Annalen, **261**, pp. 513–534, (1982).

11. Ludwig, S. C., Chandrasekharan K., *Lectures on the Geometry of Numbers.* Springer, (1989).

12. May, A., *New RSA Vulnerabilities Using Lattice Reduction Methods.* PhD thesis, University of Paderborn (2003).

13. 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).

14. 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)

15. 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).

16. 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

17. 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).

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

19. Rahmani, M., Nitaj, A., Ziane, M., *Further cryptanalysis of some variants of the RSA cryptosystem.* Journal of Applied Mathematics and Computing, 1-31 (2024).

20. Rahmani, M., Nitaj, A., *Improved Cryptanalysis of an RSA Variant Based on Cubic Pell Curve.* In International Conference on Cryptology in Africa. Cham: Springer Nature Switzerland, pp. 113-125, (2025).

21. 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).

22. Shi, G., Wang, G., Gu, D., *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.

23. 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).

24. T. Collins, D. Hopkins, S. Langford, and M. Sabin., *Public key cryptographic apparatus and Method.* US Patent #5,848,159, Jan. 1997 (1997).

25. Wiener, M., *Cryptanalysis of short RSA secret exponents,* IEEE Transactions on Information Theory,**36**(3), 553–558 (1990)

26. Zheng, M., Kunihiro, N., Yao, Y., *Cryptanalysis of the RSA variant based on cubic Pell equation.* Theor. Comput. Sci. 889, pp. 135–144 (2021).

Mostafa Chaker,
Department of Mathematics, LASMA Laboratory
Faculty of sciences Dhar Al Mahraz, Sidi Mohammed Ben Abdellah University, Fez 30000,
Morocco .
E-mail address: mostafa.chaker@usmba.ac.ma

and

Mohammed Rahmani,
Department of Mathematics, ACSA Laboratory
Faculty of sciences, Mohammed I University, Oujda 60000,
Morocco.
E-mail address: mohammed.rahmani@ump.ac.ma

and

Mhammed Ziane,
Department of Mathematics, ACSA Laboratory
Faculty of sciences, Mohammed I University, Oujda 60000,
Morocco.
E-mail address: m.ziane@ump.ac.ma

and

Siham Ezzouak,
Department of Mathematics, LASMA Laboratory
Faculty of sciences Dhar Al Mahraz, Sidi Mohammed Ben Abdellah University, Fez 30000, Morocco.
E-mail address: siham.ezzouak@usmba.ac.ma