A Generalized Partial Exposure Lattice Attack Against an RSA variant Based on Cubic Pell Curves

Michel Seck[a,*], Hortense Boudjou Tchapgnouo[b]

[a]*LTISI, CRISIN'2D, Ecole Polytechnique de Thies, Thies, Senegal*
[b]*LaRI Lab, University of Maroua, Maroua, Cameroon*

Abstract

Nitaj and Seck recently published an RSA variant (MJAGA 2024) based on the cubic Pell equation $\mathcal{P}_c(N) : u^3 + cv^3 + c^2w^3 - 3cuvw = 1$ over $\mathbb{Z}/N\mathbb{Z}$ when $N = p^r q^s$. In their cryptosystem, the public exponent e and the private exponent d are related to the key equation $d \equiv e^{-1} \pmod{p^{2(r-1)}q^{2(s-1)}(p-1)^2(q-1)^2}$. In AfricaCrypt 2025, Rahmani and Nitaj published a lattice attack on their scheme in the particular case of $r = s = 1$ by exploiting the key equation $ed - (p-1)^2(q-1)^2k = 1$. In this paper, we present a new generalized partial exposure lattice attack on the scheme of Nitaj and Seck by examining the key equation $eu_0 - (p-1)^2(q-1)^2v_0 = w_0$ when some bits of p or q are known.

Keywords: RSA, Cryptanalysis, Coppersmith's method, LLL algorithm, Lattice attack
2020 MSC: 94A60, 11Y05

1. Introduction

In 1978, Rivest, Shamir and Adleman published one of the famous cryptosystem widely used in the last four decades. The security of RSA relies on the difficulty of factoring large integers $N = pq$ where p and q are two large prime numbers. The RSA cryptosystem is based on the mathematical properties of modular exponentiation and the Euler's totient function

*Corresponding author
Email addresses: mseck@ept.edu.sn (Michel Seck), hortenseboudjou@gmail.com (Hortense Boudjou Tchapgnouo)

$\varphi(N) = (p-1)(q-1)$. The public key is (N, e) where e is a public exponent, and the private key is (N, d) where d is the private exponent such that $ed \equiv 1 \pmod{\varphi(N)}$. If the exponents e and d are not chosen properly, the security of RSA can be compromised by exploiting the key equation $ed - k\varphi(N) = 1$ where k is a positive integer [1, 13, 6]. Wiener [26] was one of the first to show the vulnerability of RSA when the private exponent d is not carefully chosen. More precisely, in 1990, he showed that if $d < N^{0.25}$, then one can factor the modulus N in polynomial time using continued fractions [14]. In 1999, Boneh and Durfee [2] extended Wiener's attack by showing that if $d < N^{1-1/\sqrt{2}} \simeq N^{0.292}$, then the factors p and q can be recovered in polynomial time using lattice reduction techniques. The key idea of Boneh and Durfee's strategy is to transform the RSA key equation $ed-k(p-1)(q-1) = 1$ into a modular polynomial equation $f(x, y) = x(y-N-1)-1 \pmod{e}$, then apply Coppersmith's method [4, 5] to find small roots of $f(x, y)$, and afterwards use the small roots to recover the factors p and q. Several authors have also studied the security of RSA when some bits of the private exponent d or the prime factors p and q are known [8, 21, 17].

For efficiency and security reasons, several variants of RSA have been proposed in the literature. In 1991, Koyama *et al.* [10] introduced a variant called KMOV, which is based on elliptic curves $E_b : y^2 = x^3 + b$ over the ring $\mathbb{Z}/N\mathbb{Z}$ with $N = pq$ and $p, q \equiv 2 \pmod{3}$. In the KMOV scheme, the exponents e and d are related to the key equation

$$ed - k(p+1)(q+1) = 1.$$

Murru and Saettone [15] proposed at NuTMiC 2017 a variant of KMOV based on the cubic Pell equation $\mathcal{P}_c(N) : u^3 + cv^3 + c^2w^3 - 3cuvw = 1$ over $\mathbb{Z}/N\mathbb{Z}$ with $N = pq$. In their scheme, e and d are related to the key equation

$$ed - k(p^2+p+1)(q^2+q+1) = 1.$$

In NuTMiC 2024, Seck and Nitaj [23] proposed a new KMOV variant also based on the cubic Pell equation $\mathcal{P}_c(N)$ over $\mathbb{Z}/N\mathbb{Z}$ when $N = p^r q^s$. The security of their scheme relies on the hardness of factoring composite integers, and on Rabin's trapdoor one-way function [18]. In the cryptosystem of Seck and Nitaj, a ciphertext is a point $C = (c_u, c_v, c_w)$ on the cubic Pell curve $\mathcal{P}_c(N)$. Later, to decrease the size of the ciphertexts of their previous scheme, Nitaj and Seck [16] proposed another variant over the cubic Pell

curves $\mathcal{P}_c(N)$, where the ciphertext is compressed to a pair (c_u, c_v) of integers in $\mathbb{Z}/N\mathbb{Z}$ using encoding functions. In their cryptosystem, the public exponent e and the private exponent d are related to the key equation

$$ed - k\,p^{2(r-1)}q^{2(s-1)}(p-1)^2(q-1)^2 = 1.$$

Nitaj and Seck studied in their paper the security of their scheme against some well-known attacks such as small private exponent attacks based on continued fractions and Coppersmith's method. They showed that their scheme is insecure if

$$d < N^{\delta} \quad \text{with} \quad 0 < \delta < 2 - \frac{2(3r+s)}{(r+s)^2}.$$

In AfricaCrypt 2025, Rahmani and Nitaj [19] published a lattice attack on the scheme of Nitaj and Seck in the particular case of $r = s = 1$ by exploiting the key equation $ed - (p-1)^2(q-1)^2k = 1$.

Our Contributions. In this paper, we present a new generalized partial exposure lattice attack on the scheme of Nitaj and Seck by examining the generalized key equation

$$eu_0 - (p-1)^2(q-1)^2v_0 = w_0$$

when some bits of p or q are known. We summarize our contributions as follows:

- First, we show that when w_0 is a constant, and an approximation p_0 of p is known such that $|p - p_0| < N^{\gamma}$, then one can recover u_0, v_0, and get the prime factors p and q in polynomial time using a result from Kunihiro [11] under certain conditions over u_0, v_0 and w_0. More precisely, if $e = N^{\alpha}, |u_0| < N^{\delta}$ and $\varepsilon = \log(2)/\log(N)$, then the factors p and q can be recovered in polynomial time if

$$\begin{cases} \delta & < 2 - \dfrac{\alpha}{3} - \dfrac{5}{2}\gamma - 6\epsilon \qquad \text{if} \qquad 0 < \gamma < \dfrac{2\alpha}{9} - \epsilon \\ \delta & < 2 - \sqrt{2\alpha(\gamma+\epsilon)} \qquad \text{if} \qquad \dfrac{2\alpha}{9} - \epsilon < \gamma < \dfrac{\alpha}{2} - \epsilon \end{cases}$$

  Using the previous result with a recent result of Seck *et al.* [24] at AfricaCrypt 2025, we show that a private exponent d too large (i.e. $|(p-1)^2(q-1)^2 - d| < N^{\delta}$) or too small (i.e. $d < N^{\delta}$) can be recovered in polynomial time.

- We also show that in the case w_0 is an unknown value but bounded, then using a recent result of Rahmani *et al.* [20], one can recover the factors p and q in polynomial time under certain conditions on u_0 and v_0.
- We demonstrate the effectiveness of our attack through a numerical example and compare our results with existing attacks. We also provide a proof of concept implementation[1] of our attack with SageMath [7].

Organization of this paper. The rest of this paper is structured as follows. In Section 2, we provide the necessary background on lattices and Coppersmith's method for finding small roots of modular polynomials. We also present the Nitaj and Seck cryptosystem, and some useful lemmas and theorems. In Section 3, we present our generalized partial prime exposure lattice attack against the Nitaj and Seck cryptosystem. We also provide a numerical example to illustrate our attack and compare our results with existing attacks. Finally, we conclude this paper in Section 4.

2. Preliminaries

In this section, we first provide the necessary background on lattices and their applications in cryptanalysis of RSA-like schemes. We then present the different algorithms of Nitaj and Seck cryptosystem. Finally, we recall some useful lemmas and theorems that will be helpful in our attack.

2.1. ***Lattices and Coppersmith's method***

Lattices. Let $l \geq 1$ and $k \leq l$. A lattice $\Lambda \subseteq \mathbb{R}^l$ is a discrete additive subgroup and it can be expressed as

$$\Lambda = \text{span}_{\mathbb{Z}}\{u_1, u_2, \ldots, u_k\} = \left\{ \sum_{i=1}^{k} a_i u_i : a_i \in \mathbb{Z} \right\}.$$

where the vectors $u_1, \ldots, u_k \in \mathbb{R}^l$ are linearly independent. Such a family $\{u_1, \ldots, u_k\}$ is called a basis of Λ. If the basis vectors are represented as

[1] https://github.com/mseckept/partial-prime-exposure-attack25.git

columns in an $l \times k$ matrix $A = (u_1 \ \cdots \ u_k)$, then the lattice generated by A is

$$\Lambda(A) = \{Az : z \in \mathbb{Z}^k\}$$

When $k = l$, $\Lambda(A)$ is called a full-rank lattice, and its determinant is given by $\det(\Lambda) = |\det(A)|$. In the general case, the determinant of $\Lambda(A)$ is defined as

$$\det(\Lambda) = \sqrt{\det(A^\top A)}$$

A central computational task in lattices is the Shortest Vector Problem (SVP): find a nonzero vector of minimal Euclidean norm in Λ. A relaxed variant, the γ-Approximate SVP, requires a nonzero $w \in \Lambda$ such that

$$\|w\| \leq \gamma \cdot \lambda_1(\Lambda),$$

where $\lambda_1(\Lambda)$ denotes the length of the shortest nonzero vector. In 1982, Lenstra, Lenstra, and Lovász [12] introduced the well-known LLL algorithm, which takes as input a basis and produces in polynomial time a nearly orthogonal one. More precisely, for any basis obtained by LLL, it holds that

$$\|v_j\| \leq 2^{\frac{k(k-1)}{4(k+1-j)}} \cdot (\det \Lambda)^{1/(k+1-j)}, \quad j = 1, \ldots, k.$$

The LLL algorithm is a powerful tool used in the cryptanalysis of RSA-like schemes, where it serves to get small solutions of modular polynomial equations.

Coppersmith's method. In 1996, Coppersmith [4, 5] introduced a very innovative method that uses the LLL algorithm to find small roots of modular univariate polynomials $f(x) \equiv 0 \pmod{e}$ and modular bivariate polynomials $g(x, y) \equiv 0 \pmod{e}$. Later, his method was extended to the multivariate case and simplified by Howgrave-Graham [9, 13] in 1997 with an essential lemma to determine whether a root of a modular multivariate polynomial $p(y_1, \ldots, y_s) \equiv 0 \pmod{e}$ also corresponds to a root of a polynomial over integers. For a multivariate polynomial $p(y_1, \ldots, y_s) = \sum p_{i_1,i_2,\ldots,i_s} y_1^{i_1} \cdots y_s^{i_s}$, the Euclidean norm $\|p(y_1, \ldots, y_s)\|$ is defined as follows:

$$\|p(y_1, \ldots, y_s)\| := \sqrt{\sum_{i_1,\ldots,i_s} |p_{i_1,\ldots,i_s}|^2}$$

Lemma 1 (Howgrave-Graham). *Let $p(y_1, \ldots, y_s) \in \mathbb{Z}[y_1, \ldots, y_s]$ be a polynomial involving at most t monomials. Fix integers $m > 0$ and e, and bounds $Y_1, \ldots, Y_s > 0$. Assume*

1. *there exist integers $y_1^*, \ldots, y_s^*$ with $|y_i^*| \leq Y_i$ for $i = 1, \ldots, s$ such that*

$$p(y_1^*, \ldots, y_s^*) \equiv 0 \pmod{e^m},$$

2. *and that*

$$\|p(y_1 Y_1, \ldots, y_s Y_s)\| < \frac{e^m}{\sqrt{t}}.$$

Then $p(y_1^*, \ldots, y_s^*) = 0$ holds over $\mathbb{Z}$.

Notice that in the case of one or two variables, one can efficiently find all small roots with Coppersmith's method. In the case of three or more variables, Coppersmith's like methods are heuristic and rely on the following assumption.

Assumption. The reduced polynomials $h(y_1, \ldots, y_s)$ obtained after applying the LLL algorithm are algebraically independent. In other words, the algebraic variety corresponding to the ideal in $\mathbb{Q}[y_1, \ldots, y_s]$ of polynomials $h(y_1, \ldots, y_s)$ recovered after LLL reduction is zero-dimensional.

In this paper, we assume that this assumption holds; and in this case, small roots can be found using techniques like Groebner bases and the resultants method. In the following theorem, we recall an important result due to Kunihiro [11] about the solutions of bivariate modular polynomial equations. Specifically, he has proposed an efficient algorithm based on Coppersmith's method to find a small solution (u_0, v_0) of the modular equation $f(u, v) \equiv 0 \pmod{e}$ with $f(u, v) = uH(v) + c \in \mathbb{Z}[u, v]$ for some constant c, under certain conditions on u_0 and v_0.

Theorem 1 ([11, 25]). *Let $H(v) = v^s + \sum_{i=0}^{s-1} a_i v^i \in \mathbb{Z}[v]$ with $s \geq 1$ and e be an integer. Suppose that*

- $u_0 H(v_0) + c \equiv 0 \pmod{e}$ *for some* $|u_0| < U = e^{\eta}$, $|v_0| < V = e^{\beta}$;
- $|c| < UV^s$.

Then the modular equation $uH(v) + c \equiv 0 \pmod{e}$ *can be solved efficiently if the following bounds are satisfied:*

$$\begin{cases} \eta \leq \dfrac{s+2}{2(s+1)} - \dfrac{s+1}{2}\beta, & \text{when } 0 < \beta < \dfrac{s}{(s+1)^2}, \\ \eta \leq 1 - \sqrt{s\beta}, & \text{when } \dfrac{s}{(s+1)^2} \leq \beta \leq \dfrac{1}{s}. \end{cases}$$

Outline of Kunihiro's method. By applying the Howgrave-Graham's Lemma 1, Kunihiro [11, 22] proceeds as follows to find the small solutions (u_0, v_0) of the modular equation

$$uH(v) + c \equiv 0 \pmod{e} \text{ with } H(v) = v^s + \sum_{i=0}^{s-1} a_i v^i$$

where the roots (u_0, v_0) satisfy the following bounds:

$$|u_0| < U = e^{\eta}, |v_0| < V = e^{\beta}$$

1. Introduce a new variable $z = uv^s + c$, which transforms the above modular equation into

$$z + u \cdot h(v) \equiv 0 \pmod{e}, \qquad h(v) = \sum_{i=0}^{s-1} a_i v^i.$$

2. Let m be a positive integer and τ is a parameter such that $0 \leq \tau \leq 1$; and define the shifted polynomials

$$g_{[a,b,k]}(u, v, z) = u^a v^b \left(z + uh(v)\right)^k e^{m-k} \text{ with } [a, b, k] \in \mathcal{G} = \mathcal{E} \cup \mathcal{F}$$

where

$$\mathcal{E} = \left\{[k-a, b, a] : k = 0, \ldots, m;\ a = 0, \ldots, k;\ b = 0, \ldots, s-1\right\},$$

$$\mathcal{F} = \left\{[0, b, k] : k = 0, \ldots, m;\ b = s, \ldots, s + \lfloor \tau k \rfloor - 1\right\}.$$

Notice that all monomials uv^s should be replaced by $z - c$.

3. Apply a scaling $(u, v, z) \mapsto (uU,\ vV,\ zZ)$ with $Z = UV^s + |c|$ and collect the coefficient vectors into a lattice basis $M(m, \tau)$, arranged according to the following ordering in $\mathcal{G}$:

$$g_{[a,b,k]} < g_{[a',b',k']} \Longleftrightarrow \begin{cases} a + k < a' + k' \text{ or} \\ a + k = a' + k' \text{ and } a < a's \text{ or} \\ a = a',\ k = k' \text{ and } b \leq b'. \end{cases}$$

And $u^a v^b z^k$ is ordered in the same way. Note that the orderings of shift polynomials $g_{[a,b,k]}$ and monomials $u^a v^b z^k$ ensure that the lattice basis matrix $M(m, \tau)$ is triangular.

4. Run the LLL algorithm on $M(m, \tau)$ to obtain reduced vectors, corresponding to auxiliary polynomials $f_\ell(u, v, z)$.
5. Solve the system $\{f_\ell(u, v, z) = 0\}$ by algebraic elimination (Groebner bases, resultants).

Applying Howgrave-Graham's Lemma 1 and Coppersmith's method, Rahmani *et al.* [20] recently presented a polynomial-time algorithm to find small roots of modular trivariate polynomials of the form $f(x, y, z) := x(y^2 + ay + b) + z \equiv 0 \pmod{e}$. The following theorem summarizes their result.

Theorem 2 ([20])**.** *Let N and e be positive integers. Let $R(y) := y^2+ay+b \in \mathbb{Z}[y]$ be a monic polynomial of degree 2. Suppose there exist integers v_0, y_0, w_0 such that $v_0 R(y_0) + w_0 \equiv 0 \pmod{e}$ with bounds*

$$|v_0| \leq N^\delta, \quad |y_0| \leq N^\gamma, \quad |w_0| \leq N^\mu.$$

If $e = N^\alpha$, and the following conditions are satisfied:

$$\delta < \alpha - \sqrt{2\alpha\gamma} - \tfrac{1}{2}\mu \text{ and } \alpha \geq 2\gamma$$

then v_0, y_0, w_0 can be recovered in polynomial time.

2.2. ***Nitaj and Seck Cryptosystem***

In 2024, Nitaj and Seck [16] proposed a KMOV-like cryptosystem based on the cubic Pell equation $\mathcal{P}_c(N) : u^3 + cv^3 + c^2w^3 - 3cuvw = 1$ over $\mathbb{Z}/N\mathbb{Z}$ when $N = p^r q^s$ with p and q distinct primes. The public exponent e and the private exponent d are related to the key equation

$$d \equiv e^{-1} \pmod{p^{2(r-1)} q^{2(s-1)} (p-1)^2 (q-1)^2} \tag{1}$$

In their algorithms, they use an encoding function Encode2Curve((u_M, v_M), b, N) to encode a message $(u_M, v_M) \in \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ into a point on the cubic Pell curve $\mathcal{P}_{b^3}(N)$, and a decoding function DecodeFromCurve($(u, v, w), b, N$) to decode a point back into a message. Notice that some of the calculations in their scheme are performed in the group $(\mathcal{P}_c(N), \otimes)$ where the group law $\otimes$ is defined as follows [23, 16]:

$$(u_1, v_1, w_1) \otimes (u_2, v_2, w_2) = (w_1w_2 + c(v_2w_1 + v_1w_2), u_2v_1 + u_1v_2 + cw_1w_2, v_1v_2 + u_2w_1 + u_1w_2)$$

where (u_1, v_1, w_1) and (u_2, v_2, w_2) are two points of the curve $\mathcal{P}_c(N)$. The neutral element of $(\mathcal{P}_c(N), \otimes)$ is the point $(1, 0, 0)$, and the inverse of (u, v, w) is given by $(u^2 - cvw, cw^2 - uv, v^2 - uw)$.

The scheme of Nitaj and Seck. The key generation, encryption, and decryption algorithms are described as follows.

Key Generation Algorithm. To generate a key pair (pk, sk), one proceed as follows:

1. Choose randomly two prime numbers p and q of λ bits such that $p \equiv 1 \pmod 3$ and $q \equiv 1 \pmod 3$.
2. Compute $N = p^r q^s$.
3. Choose randomly an integer $b \in \mathbb{Z}/N\mathbb{Z}$ such that $c = b^3 \pmod N$ is a nonzero cubic residue modulo p and modulo q.
4. Choose an integer $e \in \mathbb{Z}/N\mathbb{Z}$ with $\gcd(e, pq(p-1)(q-1)) = 1$.
5. Compute
$$d \equiv e^{-1} \pmod{p^{2(r-1)} q^{2(s-1)} (p-1)^2 (q-1)^2}$$
6. The public key is $pk = (N, b, e)$ and the private key is $sk = (N, b, d)$.

Encryption Algorithm. To encrypt a message $M = (u_M, v_M) \in (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})$, one proceed as follows:

1. Compute $c := b^3 \pmod N$.
2. Encode the message M into a point (x, y, z) on the cubic Pell curve $\mathcal{P}_c(N)$ using the function Encode2Curve$((u_M, v_M), b, N)$.
3. Compute $P = (u_P, v_P, w_P) := e \otimes (u, v, w)$ on the cubic Pell curve $\mathcal{P}_c(N)$.
4. Compress P to obtain
$$(c_u, c_v) := \text{DecodeFromCurve}(P, b, N)$$
.
5. The ciphertext is $C = (c_u, c_v)$.

Decryption Algorithm. To decrypt a ciphertext $C = (c_u, c_v)$, one proceed as follows:

1. Compute $c := b^3 \pmod{N}$.
2. Decompress the ciphertext to obtain
$$(u_P, v_P, w_P) := \text{Encode2Curve}((c_u, c_v), b, N)$$
3. Compute $(u, v, w) := d \otimes (u_P, v_P, w_P)$ on the cubic Pell curve $\mathcal{P}_c(N)$.
4. Decode the point (u, v, w) to obtain the plaintext
$$(u_m, v_m) := \text{DecodeFromCurve}((u, v, w), b, N)$$

2.3. ***Useful Lemmas and Theorems***

Seck *et al.* [24] showed, in AfricaCrypt 2025, that private exponents $d = N^\delta$ of RSA-type schemes which are too large can be efficiently recovered, and the modulus N can be factored in polynomial time, under certain conditions on δ.

Theorem 3 ([24])**.** *Let $N = p_1 p_2$ be an RSA modulus. Let $\psi_N : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Suppose $\mathcal{B}$ is an algorithm that is able to factor N in polynomial time given N and a public exponent $0 < e < \psi_N(p_1, p_2)$ such that there exist positive integers u_0 and v_0 with $u_0 < \mathcal{A}_1 \in \mathbb{R}^+$ satisfying*
$$eu_0 - v_0\psi_N(p_1, p_2) = w_0 \text{ with } |w_0| \leq \mathcal{A}_2,\ \mathcal{A}_2 \geq 1.$$
Then, using $\mathcal{B}$, one can factor N in polynomial time given N and a public exponent $0 < e' < \psi_N(p_1, p_2)$ such that the corresponding private exponent $d' = \psi(p_1, p_2) - d$ for some $d < \mathcal{A}_1$.

For a balanced RSA modulus $N = pq$, both p and the sum $p + q$ can be bounded as stated in Lemma 2, and these bounds can be derived from [3, 22].

Lemma 2. *Given an RSA modulus $N = p_1 p_2$ with $p_2 < p_1 < 2p_2$, the following bounds are satisfied:*
$$2\sqrt{N} < p_1 + p_2 < 3\sqrt{N} \text{ and } \sqrt{N} < p_1 < \sqrt{2}\sqrt{N}$$

Lemma 3 ([20])**.** *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Suppose $\widehat{p}$ is an approximation of p such that $|p - \widehat{p}| = N^\gamma$. Then, the quantity $\widehat{q} = \left\lfloor \frac{N}{\widehat{p}} \right\rfloor$ is an approximation of q, and the following inequalities hold:*
$$|q - \widehat{q}| < N^\gamma, \quad \text{and} \quad |p + q - (\widehat{p} + \widehat{q})'| < 2N^\gamma \tag{2}$$

In this paper, we suppose that $|p - \widehat{p}| > N^{1/4}$, otherwise the modulus N can be efficiently factored in polynomial time using Coppersmith's algorithm [13]. We also set $q_0 = 0$ whenever $p_0 = 0$; and in this case; the inequalities in 2 still hold.

3. Our Contribution

In this section, we present a new generalized partial exposure lattice attack on the scheme of Nitaj and Seck [16]. The attack is based on the key equation

$$eu_0 - (p-1)^2(q-1)^2 v_0 = w_0$$

and uses lattice-based cryptanalysis techniques to find small roots when (i) w_0 is a constant or (ii) w_0 is a bounded unknown value.

3.1. ***The New Partial Exposure Lattice Attack when*** w_0 ***is a constant***

We suppose that $w_0 = c_0$ is a constant. Let $N = pq$ be an RSA modulus and let p_0 be an approximation of p such that $|p - p_0| = N^\gamma$ for some $\gamma > \frac{1}{4}$. We will show that the modulus N in the scheme of Nitaj and Seck can be factored in polynomial time by studying the generalized key equation $eu_0 - (p-1)^2(q-1)^2 v_0 = c_0$ under certain conditions on γ, u_0, v_0 and c_0. Our attack is based on Coppersmith's method.

Theorem 4. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Suppose that an approximation p_0 of p is known such that $|p - p_0| < N^\gamma$ for some $\gamma \geq \frac{1}{4}$. Let $e = N^\alpha$ be a public exponent, c_0 a constant, and $\epsilon = \log(2)/\log(N)$. Let u_0 and v_0 be integers satisfying the generalized key equation $eu_0 - (p-1)^2(q-1)^2 v_0 = c_0$ with $|c_0| < e|u_0|$. If the following inequalities hold*

$$\begin{cases} \delta & < 2 - \dfrac{\alpha}{3} - \dfrac{5}{2}\gamma - 6\epsilon \qquad \text{if} \qquad 0 < \gamma < \dfrac{2\alpha}{9} - \epsilon \\ \delta & < 2 - \sqrt{2\alpha(\gamma + \epsilon)} \qquad \text{if} \qquad \dfrac{2\alpha}{9} - \epsilon < \gamma < \dfrac{\alpha}{2} - \epsilon \end{cases}$$

then the modulus N can be factored in polynomial time.

Proof. Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let p_0 be an approximation of p such that $|p - p_0| < N^\gamma$. By Lemma 3, if $p_0 \neq 0$ (resp. $p_0 = 0$), then $q_0 = \left\lfloor \frac{N}{p_0} \right\rfloor$ (resp. $q_0 = 0$) is an approximation of q such that $|q - q_0| < N^\gamma$ and $|p + q - (p_0 + q_0)| < 2N^\gamma$. The public exponent $e = N^\alpha$ satisfies the generalized key equation $eu_0 - (p-1)^2(q-1)^2 v_0 = c_0$ with

$|u_0| < N^\delta$ and $|c_0| < e|u_0|$. We have

$$\begin{aligned}\psi(N) &= (p-1)^2(q-1)^2 \\ &= (p+q)^2 - 2(N+1)(p+q) + (N+1)^2 \\ &= (p+q-p_0-q_0)^2 + (2(p_0+q_0) - 2(N+1))(p+q-p_0-q_0) \\ &\quad + (p_0+q_0)^2 - 2(N+1)(p_0+q_0) + (N+1)^2 \\ &= (p+q-p_0-q_0)^2 + A(p+q-p_0-q_0) + B\end{aligned}$$

with

$$A = 2(p_0+q_0) - 2(N+1), \quad B = (p_0+q_0)^2 - 2(N+1)(p_0+q_0) + (N+1)^2$$

We have $eu_0 - \psi(N)v_0 = c_0 \Rightarrow v_0\psi(N) + c_0 \equiv 0 \pmod{e}$. This implies that

$$v_0\left((p+q-p_0-q_0)^2 + A(p+q-p_0-q_0) + B\right) + c_0 \equiv 0 \pmod{e} \quad (3)$$

Let us consider the modular bivariate polynomial

$$f(v,y) := v(y^2 + Ay + B) + c_0 \equiv 0 \pmod{e}$$

Notice that solving the previous modular Equation 3 is equivalent to finding the roots $(v_0, y_0 := p+q-p_0-q_0)$ of $f(v,y)$. We have the following bounds

$$\begin{aligned} e &= N^\alpha \\ |u_0| &< N^\delta \\ |y_0| = |p+q-p_0-q_0| &< 2N^\gamma = N^{\gamma+\epsilon} = e^{\frac{\gamma+\epsilon}{\alpha}} \text{ with } \epsilon = \log(2)/\log(N) \\ |v_0| = \left|\frac{eu_0 - c_0}{\psi(N)}\right| &< \left|\frac{2e|u_0|}{\psi(N)}\right| < \left|\frac{2e|u_0|}{\frac{N^2}{4}}\right| = N^{\alpha+\delta+3\epsilon-2} = e^{\frac{\alpha+\delta+3\epsilon-2}{\alpha}}\end{aligned}$$

According to Theorem 1, we can find small roots of the modular polynomial $f(v,y)$ in polynomial time if the following conditions are satisfied:

$$\begin{cases} \dfrac{\alpha+\delta+3\epsilon-2}{\alpha} & < \dfrac{2}{3} - \dfrac{3}{2}\cdot\dfrac{\gamma+\epsilon}{\alpha} \quad \text{if} \quad 0 < \dfrac{\gamma+\epsilon}{\alpha} < \dfrac{2}{9} \\ \dfrac{\alpha+\delta+3\epsilon-2}{\alpha} & < 1 - \sqrt{\dfrac{2(\gamma+\epsilon)}{\alpha}} \quad \text{if} \quad \dfrac{2}{9} < \dfrac{\gamma+\epsilon}{\alpha} < \dfrac{1}{2} \end{cases}$$

$$\iff \begin{cases} \alpha+\delta+3\epsilon-2 & < \dfrac{2\alpha}{3}-\dfrac{3}{2}(\gamma+\epsilon) & \text{if} \quad 0<\gamma+\epsilon<\dfrac{2\alpha}{9} \\ \alpha+\delta+3\epsilon-2 & < \alpha-\sqrt{2\alpha(\gamma+\epsilon)} & \text{if} \quad \dfrac{2\alpha}{9}<\gamma+\epsilon<\dfrac{\alpha}{2} \end{cases}$$

$$\iff \begin{cases} \delta & < 2-\dfrac{\alpha}{3}-\dfrac{5}{2}\gamma-6\epsilon & \text{if} \quad 0<\gamma<\dfrac{2\alpha}{9}-\epsilon \\ \delta & < 2-\sqrt{2\alpha(\gamma+\epsilon)} & \text{if} \quad \dfrac{2\alpha}{9}-\epsilon<\gamma<\dfrac{\alpha}{2}-\epsilon \end{cases} \tag{4}$$

Once we get a solution $(v^{(0)}, y^{(0)})$ of the modular equation $f(v,y) \equiv 0 \pmod{e}$, we can recover the factors p and q in polynomial time by solving the following system of equations:

$$\begin{cases} p+q & = p_0+q_0+y^{(0)} \\ pq & = N \end{cases}$$

Thus, the modulus N can be factored in polynomial if the inequalities in 4 holds.

□

Combining a recent result of Seck *et al.* [24] (see Theorem 3) showing that a private exponent d which is too large or too small can be recovered in polynomial time, and Theorem 4, we can derive the following corollary.

Corollary 1. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Suppose that an approximation p_0 of p is known such that $|p - p_0| < N^\gamma$ for some $\gamma \geq \frac{1}{4}$. Let $e = N^\alpha$ be a public exponent and $\epsilon = \log(2)/\log(N)$. If the private exponent $d = N^\delta$ satisfies the following bounds*

$$d < N^\delta \text{ or } |\psi(N) - d| < N^\delta$$

then one can factor the modulus N in polynomial time if the following inequalities hold:

$$\begin{cases} \delta & < 2-\dfrac{\alpha}{3}-\dfrac{5}{2}\gamma-6\epsilon & \text{if} \quad 0<\gamma<\dfrac{2\alpha}{9}-\epsilon \\ \delta & < 2-\sqrt{2\alpha(\gamma+\epsilon)} & \text{if} \quad \dfrac{2\alpha}{9}-\epsilon<\gamma<\dfrac{\alpha}{2}-\epsilon \end{cases} \tag{5}$$

If we suppose that we do not know any bit of p or q, we derive the following conditions for factoring the modulus N in polynomial time.

Theorem 5. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let $e = N^{\alpha}$ be a public exponent, c_0 a constant, and $\epsilon = \log(2)/\log(N)$. Let u_0 and v_0 be integers satisfying the generalized key equation $eu_0 - (p-1)^2(q-1)^2 v_0 = c_0$ with $|c_0| < e|u_0|$. If the following inequalities hold*

$$\delta < 2 - \sqrt{\alpha(1+3\epsilon)} \qquad \text{and} \qquad \alpha > 1 + 3\epsilon$$

then the modulus N can be factored in polynomial time.

Proof. Since $q < p < 2q$, by Lemma 2, we have $p < \sqrt{2}\sqrt{N} = N^{\frac{1+\epsilon}{2}}$. Then, one can take $\gamma = \frac{1+\epsilon}{2}$. By substituting the value of γ in the inequalities of Theorem 4, we obtain the conditions for factoring the modulus N in polynomial time. □

Corollary 2. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let $e = N^{\alpha}$ be a public exponent and $\epsilon = \log(2)/\log(N)$. If the private exponent $d = N^{\delta}$ satisfies the following bounds*

$$d < N^{\delta} \text{ or } |\psi(N) - d| < N^{\delta}$$

then one can factor the modulus N in polynomial time if the following inequalities hold:

$$\delta < 2 - \sqrt{\alpha(1+3\epsilon)} \qquad \text{and} \qquad \alpha > 1 + 3\epsilon$$

3.2. ***The New Partial Exposure Lattice Attack when w_0 is a variable***

In this section, we present a new partial exposure lattice attack when w_0 is an unknown value but bounded.

Theorem 6. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Suppose that an approximation p_0 of p is known such that $|p - p_0| < N^{\gamma}$ for some $\gamma > \frac{1}{4}$. Let $e = N^{\alpha}$ be a public exponent satisfying the generalized key equation $eu_0 - (p-1)^2(q-1)^2 v_0 = w_0$ with $|u_0| < N^{\delta}$ and $|w_0| \leq N^{\mu}, \mu < \alpha + \delta$. If the following inequalities hold*

$$\begin{cases} \delta & < 2 - \sqrt{2\alpha(\gamma+\epsilon)} - \dfrac{\mu}{2} - 3\epsilon \\ \alpha & \geq 2\,(\gamma+\epsilon) \end{cases}$$

with $\epsilon = \log(2)/\log(N)$, then the modulus N can be factored in polynomial time.

Proof. Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let p_0 be an approximation of p such that $|p - p_0| < N^\gamma$. By Lemma 3, if $p_0 \neq 0$ (resp. $p_0 = 0$), then $q_0 = \left\lfloor \frac{N}{p_0} \right\rfloor$ (resp. $q_0 = 0$) is an approximation of q such that $|q - q_0| < N^\gamma$ and $|p + q - (p_0 + q_0)| < 2N^\gamma$. The public exponent $e = N^\alpha$ satisfies the generalized key equation $eu_0 - (p-1)^2(q-1)^2 v_0 = w_0$ with $|u_0| < N^\delta$ and $|w_0| < N^\mu$. By equation 3, the following holds.

$$\left((p + q - p_0 - q_0)^2 + A(p + q - p_0 - q_0) + B\right) v_0 + w_0 \equiv 0 \pmod{e} \quad (6)$$

Let us consider the modular trivariate polynomial

$$g(v, y, w) := (y^2 + Ay + B)v + w \equiv 0 \pmod{e}$$

Solving the previous modular Equation 6 is equivalent to finding the roots $(v_0, p + q - p_0 - q_0, w_0)$ of $g(v, y, w)$. We have the following bounds

$$\begin{aligned} e &= N^\alpha \\ |u_0| &< N^\delta, \\ |p + q - p_0 - q_0| &< 2N^\gamma = N^{\gamma+\epsilon} \text{ with } \epsilon = \log(2)/\log(N) \\ |w_0| &\leq N^\mu \qquad \text{with } \mu < \alpha + \delta \\ |v_0| &= \left|\frac{eu_0 - w_0}{\psi(N)}\right| < \left|\frac{2e|u_0|}{\psi(N)}\right| < \left|\frac{2e|u_0|}{\frac{N^2}{4}}\right| = N^{\alpha+\delta+3\epsilon-2} \end{aligned}$$

According to Theorem 2, we can find small roots of the modular polynomial $f(v, y, w)$ in polynomial time if the following conditions hold:

$$\begin{aligned} \alpha + \delta + 3\epsilon - 2 &< \alpha - \sqrt{2\alpha(\gamma + \epsilon)} - \frac{\mu}{2} \\ &\iff \delta < 2 - \sqrt{2\alpha(\gamma + \epsilon)} - \frac{\mu}{2} - 3\epsilon \\ \alpha &\geq 2(\gamma + \epsilon) \text{ and } \mu < \alpha + \delta \end{aligned}$$

Once we get a solution $(v^{(0)}, y^{(0)}, w^{(0)})$ of the modular equation $f(v, y, w) \equiv 0 \pmod{e}$, we can recover the factors p and q in polynomial time by solving the following system of equations:

$$\begin{cases} p + q &= p_0 + q_0 + y^{(0)} \\ pq &= N \end{cases}$$

Thus, we can factor the modulus N in polynomial time if

$$\begin{cases} \delta & < 2 - \sqrt{2\alpha(\gamma + \epsilon)} - \dfrac{\mu}{2} - 3\epsilon \\ \alpha & \geq 2\,(\gamma + \epsilon) \end{cases}$$

□

3.3. ***Numerical Example***

Consider the following modulus and the exponent such that $N \simeq 2^{507}$ and $e \simeq 2^{1014}$:

$$\begin{aligned} N =& 212921445995430382062696543311476661688549347768529760422931060401572727548506682067852221486471826024808130124334174082584493733882975283986304952656663 9 \\ e =& 253002689294728454390948153236725234070702385621982920041141260533789745439707798985212619462989679563292330384216160669253725340223232992352120694088859994474232431012886361991803761956066742811108187918794022471513571944463462912623465177423723018838851598336649058480701489194744929343085987065489775045 3 \end{aligned}$$

Suppose that we know the 50 most significant bits of p and get the following approximation of p:

$$\begin{aligned} p_0 =& 417953278947945189153407130871496501733975104 \\ & 500891851824021213578415822602 24 \end{aligned}$$

From p_0, we compute $q_0 = \left\lfloor \frac{N}{p_0} \right\rfloor$ and get the following approximation of q:

$$\begin{aligned} q_0 =& 509438391131629574201871771842878762763420342973328968203333599070671731403 98 \end{aligned}$$

For this instance (N, e), we have $e \simeq N^{1.9983}$ which means that $\alpha \simeq 1.9983$.

Now we have to solve the equation $eu_0 - (p-1)^2(q-1)^2 v_0 = -1$. To do so, we will solve the modular equation

$$v_0\left((p+q-p_0-q_0)^2+A(p+q-p_0-q_0)+B\right)+c_0\equiv 0 \pmod{e}$$

with

$$\begin{aligned}A =&2(p_0+q_0)-2(N+1)\\ =&42584289199086076412539308662295332337709869553705\\ &95208458621208031454550969948163023028514776765464\\ &71561972743378400256219503051365403471719628154233 2036\end{aligned}$$

and

$$\begin{aligned}B =&(p_0+q_0)^2-2(N+1)(p_0+q_0)+(N+1)^2\\ =&45335542164784976682264502730255403902180507362008517702\\ &78832338112997024455107506616364859214336335222799553889\\ &75178844673106935797603177346867473362628895271660121519\\ &88043858660604986898783430125075861947372398029904425316\\ &14486723731895251898889270015681000566848547609345092462\\ &59395361196671006731797 6324\end{aligned}$$

Consider the modular bivariate polynomial

$$f(v,y) := v(y^2+Ay+B)+c_0\equiv 0 \pmod{e}$$

To obtain a small root (v_0, y_0) of the modular equation $f(v, y) \equiv 0 \pmod{e}$, we set $\delta = 0.35, \gamma = 0.5$ and $c_0 = -1$. We obtain the following bounds :

$$\begin{aligned}V=\left\lfloor\frac{8eN^{\delta}}{N^2}\right\rfloor =&\ 20637310724466703896281418298454753918926000420080844 80\\ Y=\lfloor 2N^{\gamma}\rfloor =&\ 92286823760584670381484585904249356172284\\ &\ 68415358368421368546978586153394493 1\\ Z=\left\lfloor VY^2+1\right\rfloor =&\ 17576504163641814188743382248726626285829619270 05\\ &\ 69651119369223964664522166187516924550630778 1\\ &\ 78142845155414100813066891100136982969959442 1\\ &\ 50388285764028701424604296131268870860032269 8\\ &\ 40071925779155735334092 81\end{aligned}$$

Next, to construct the lattice basis $M(m, \tau)$, we set $m = 2$ and $\tau = 1$, obtaining a lattice of dimension $\omega = 15$. Applying the LLL lattice reduction algorithm yields a reduced basis in 0.058 seconds. Using the Groebner basis computation (in 0.978 seconds), we selected two integer polynomials and obtained the following root (v_0, y_0).

$$\begin{aligned} v_0 =& 717360905978040033035688539461656223557654938 4 \\ y_0 =& -209284674313605828806715636615151961995686198 \\ & 9638903296991238 \end{aligned}$$

Finally, to obtain the factors p and q of N, we solve the following system:

$$\begin{cases} pq = N =& 641991165268270258720286669452012076077852153752836 9 \\ & 297376712045939327935894837385543867963940676480098 9 \\ & 585904927690078197719192930307211251658819261472 9 \\ p + q =& y_0 + p_0 + q_0 \\ =& 927391670079574742426811471353792383825 \\ & 831785959024620458734916260054584093 84 \end{cases}$$

Solving the above system of equations, we get following values for p and q.

$$\begin{cases} p =& 509438391131629457660890156426633308057060 1 \\ & 602237690531608597358199872973507 7 \\ q =& 417953278947945284765921314927159075768771 6 \\ & 257352555672978751804400672867430 7 \end{cases}$$

For the private exponent d, the following value is obtained which is too large:

$$\begin{aligned} d =& 453355421647849766822645027302554039021805073620085177 02 \\ & 788323381129970244551075066163648592232485743187066857 98 \\ & 113424979975047356477754931591583686561383539313925193 44 \\ & 201184575963111220969637826744176597780425491695462324 03 \\ & 252127653879216473259497741030839077960492033905473246 80 \\ & 927019215951369960444481245 \end{aligned}$$

3.4. ***Comparison with Previous Work***

In this section, we compare our results with previous work in the field. We highlight the improvements achieved by our new prime partial exposure lattice attack against the scheme of Nitaj and Seck [16].

3.4.1. ***Comparison with the attack of Rahmani and Nitaj.***

Recently, in AfricaCrypt 2025, Rahmani and Nitaj [19] presented a lattice-based attack against the scheme of Nitaj and Seck [16] when $r = s = 1$. In their main theorem, they showed that if the private exponent d is small enough, then the factors p and q can be recovered efficiently by studying the key equation

$$ed - k(p-1)^2(q-1)^2 = 1$$

More precisely, they showed that if $e = N^\alpha$ and

$$d < N^\delta \text{ with } \delta < 2 - \sqrt{\alpha} \text{ and } 1 < \alpha < 4$$

then the modulus N can be factored in polynomial time. In this paper, we have extended their attack to the case where the private exponent d is too large (i.e., $|(p-1)^2(q-1)^2 - d| < N^\delta$). We have also showed in our work how to recover the factors p and q if an approximation p_0 of p is known. In addition, we have studied the generalized key equation $eu_0 - (p-1)^2(q-1)^2 v_0 = w_0$ and showed that if w_0 is a constant or a bounded unknown value, then the modulus N can be factored in polynomial time under certain conditions on u_0, v_0, w_0 and p_0. Furthermore, if we set $p_0 = 0$ (which means that $\gamma \simeq 1/2$) and neglect ϵ (i.e. $\epsilon \simeq 0$) in the Inequal. 5 of our Corollary 1, we recover the same conditions as in the main theorem of Rahmani and Nitaj [19].

3.4.2. ***Comparison with the Attack of Nitaj and Seck.***

In [16], Nitaj and Seck presented a lattice-based attack against their scheme. They showed that if $N = p^r q^s$ and $d < N^\delta$ with $0 < \delta < 2 - \dfrac{2(3r+s)}{(r+s)^2}$, then the factors p and q of N can be recovered in polynomial time. Notice that in the case of $r = s = 1$, their attack requires $\delta < 0$, which is impossible since δ is a non-negative number. Thus, their attack is not applicable in this case.

4. Conclusion

In this paper, we have presented a new prime partial exposure lattice attack against the RSA variant of Nitaj and Seck [16]. We have studied the generalized key equation $eu_0 - (p-1)^2(q-1)^2 v_0 = w_0$ and have shown that if w_0 is a constant or a bounded unknown value, then the modulus N (product

of two unknown primes p and q) can be factored in polynomial time under certain conditions on u_0, v_0, w_0 and p. Our results extend the previous work of Nitaj and Seck [16] and Rahmani and Nitaj [19] by considering cases where the private exponent is too large or when an approximation of p is known.

References

[1] Dan Boneh. Twenty years of attacks on the RSA cryptosystem. *Notices of the AMS*, 46(2):203–213, 1999.

[2] Dan Boneh and Glenn Durfee. Cryptanalysis of RSA with private key d less than $N^{0.292}$. In *Advances in Cryptology—EUROCRYPT'99: International Conference on the Theory and Application of Cryptographic Techniques Prague, Czech Republic, May 2–6, 1999 Proceedings 18*, pages 1–11. Springer, 1999. doi: 10.1007/3-540-48910-X_1.

[3] Martin Bunder, Abderrahmane Nitaj, Willy Susilo, and Joseph Tonien. A generalized attack on RSA type cryptosystems. *Theoretical Computer Science*, 704:74–81, 2017. doi: 10.1016/j.tcs.2017.09.009.

[4] Don Coppersmith. Finding a small root of a univariate modular equation. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 155–165. Springer, 1996.

[5] Don Coppersmith. Finding a small root of a bivariate integer equation; factoring with high bits known. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 178–189. Springer, 1996.

[6] B. de Weger. Cryptanalysis of RSA with small prime difference. *Appl. Algebra Eng. Commun. Comput.*, 13(1):17–28, 2002.

[7] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 10.4)*. SageMath, https://www.sagemath.org, 2025.

[8] Martin Ernst, Eelco Jochemsz, Alexander May, and Benne de Weger. Partial key exposure attacks on rsa up to full size exponents. In Ronald Cramer, editor, *Advances in Cryptology – EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 371–386. Springer, 2005. doi: 10.1007/11426639_22.

[9] Nicholas Howgrave-Graham. Finding small roots of univariate modular equations revisited. In *IMA International Conference on Cryptography and Coding*, pages 131–142. Springer, 1997.

[10] K. Koyama, U. Maurer, T. Okamoto, and S. A. Vanstone. New public-key schemes based on elliptic curves over the ring $\mathbb{Z}_n$. In *Advances in Cryptology – CRYPTO '91*, volume 576 of *Lecture Notes in Computer Science*, pages 252–266, Berlin, Heidelberg, 1992. Springer. doi: 10.1007/3-540-46766-1_20.

[11] Noboru Kunihiro. On optimal bounds of small inverse problems and approximate GCD problems with higher degree. In *International Conference on Information Security*, pages 55–69. Springer, 2012. doi: 10.1007/978-3-642-33383-5_4.

[12] Arjen K Lenstra, Hendrik Willem Lenstra, and László Lovász. Factoring polynomials with rational coefficients. *Mathematische annalen*, 261:515–534, 1982.

[13] Alexander May. *New RSA vulnerabilities using lattice reduction methods. Ph.D. Thesis, University of Paderborn, Paderborn, Germany.* PhD thesis, Citeseer, 2003.

[14] Charles G. Moore. *An Introduction to Continued Fractions.* National Council of Teachers of Mathematics, Washington, D.C., 1964.

[15] N. Murru and F. M. Saettone. A novel RSA-like cryptosystem based on a generalization of the rédei rational functions. In J. Kaczorowski, J. Pieprzyk, and J. Pomykala, editors, *Number-Theoretic Methods in Cryptology (NuTMiC 2017)*, volume 10737 of *Lecture Notes in Computer Science*, pages 91–103, Cham, 2018. Springer. doi: 10.1007/978-3-319-89339-9_7.

[16] Abderrahmane Nitaj and Michel Seck. A new public key encryption scheme based on the cubic pell curve using encoding functions. *Moroccan Journal of Algebra and Geometry with Applications*, 4:89–107, 2025.

[17] Li Peng, Limin Hu, Zhen Huang, and Jian Xu. Partial prime factor exposure attacks on rsa and its takagi's variant. In Javier Lopez and Yung-Chen Wu, editors, *Information Security Practice and Experience*, vol-

ume 9065 of *Lecture Notes in Computer Science*, pages 98–113. Springer, 2015. doi: 10.1007/978-3-319-17533-1_7.

[18] Michael O. Rabin. Digitalized signatures and public key functions as intractable as factorization. Technical Report MIT/LCS/TR-212, MIT Laboratory for Computer Science, Cambridge, MA, USA, 1979. Also appears as a chapter in "Foundations of Secure Computation" (Academic Press, 1978).

[19] Mohammed Rahmani and Abderrahmane Nitaj. Improved cryptanalysis of an RSA variant based on cubic pell curve. In Abderrahmane Nitaj, Svetla Petkova-Nikova, and Vincent Rijmen, editors, *Progress in Cryptology - AFRICACRYPT 2025*, pages 113–125, Cham, 2026. Springer Nature Switzerland. ISBN 978-3-031-97260-7. doi: 10.1007/978-3-031-97260-7_6.

[20] Mohammed Rahmani, Abderrahmane Nitaj, Abdelhamid Tadmori, and Mhammed Ziane. An improved attack on the RSA variant based on cubic pell equation. *Cryptography*, 9(2):40, 2025. doi: 10.3390/cryptography9020040.

[21] Santanu Sarkar, Sourav Sen Gupta, and Subhamoy Maitra. Partial key exposure attack on rsa – improvements for limited lattice dimensions. In Guang Gong and Kishan Chand Gupta, editors, *Progress in Cryptology – INDOCRYPT 2010*, pages 2–16. Springer, 2010. doi: 10.1007/978-3-642-17401-8_2.

[22] Michel Seck and Abdoul Aziz Ciss. A new generalized lattice attack against a family of RSA-like cryptosystems. *Theoretical Computer Science*, page 115548, 2025. ISSN 0304-3975. doi: 10.1016/j.tcs.2025.115548.

[23] Michel Seck and Abderrahmane Nitaj. A new public key cryptosystem based on the cubic pell curve. In Andrzej Dąbrowski, Josef Pieprzyk, and Jacek Pomykała, editors, *Number-Theoretic Methods in Cryptology*, pages 239–261, Cham, 2025. Springer Nature Switzerland. doi: 10.1007/978-3-031-82380-0_8.

[24] Michel Seck, Oumar Niang, Djiby Sow, Abderrahmane Nitaj, Mengce Zheng, and Maher Boudabra. A new generalized attack on RSA-like

cryptosystems. In Abderrahmane Nitaj, Svetla Petkova-Nikova, and Vincent Rijmen, editors, *Progress in Cryptology – AFRICACRYPT 2025*, pages 126–144, Cham, 2026. Springer Nature Switzerland. ISBN 978-3-031-97260-7. doi: 10.1007/978-3-031-97260-7_7.

[25] George Teşeleanu. A lattice attack against a family of RSA-like cryptosystems. In *International Symposium on Cyber Security, Cryptology, and Machine Learning*, pages 343–355. Springer, 2024. doi: 10.1007/978-3-031-76934-4_25.

[26] Michael J Wiener. Cryptanalysis of short RSA secret exponents. *IEEE Transactions on Information theory*, 36(3):553–558, 1990.