Generalized Cryptanalysis of Cubic Pell RSA*

Hao Kang and Mengce Zheng

Zhejiang Wanli University, Ningbo, China
mengce.zheng@gmail.com

Abstract. The RSA (Rivest-Shamir-Adleman) cryptosystem is a fundamental algorithm of public key cryptography and is widely used across various information domains. For an RSA modulus represented as $N = pq$, with its factorization remaining unknown, security vulnerabilities arise when attackers exploit the key equation $ed-k(p-1)(q-1) = 1$. To enhance the security, Murru and Saettone introduced cubic Pell RSA — a variant of RSA based on the cubic Pell equation, where the key equation becomes $ed-k(p^2+p+1)(q^2+q+1) = 1$. In this paper, we further investigate the security implications surrounding the generalized key equation $eu - (p^2 + p + 1)(q^2 + q + 1)v = w$. We present a novel attack strategy aimed at recovering the prime factors p and q under specific conditions satisfied by u, v, and w. Our generalized attack employs lattice-based Coppersmith's techniques and extends several previous attack scenarios, thus deepening the understanding of mathematical cryptanalysis.

Keywords: Cryptanalysis · Cubic Pell equation · Factorization · Lattice · RSA variant

1 Introduction

Background. The RSA cryptosystem [RSA78], proposed by Rivest, Shamir, and Adleman, stands as a cornerstone in modern cryptography, serving various applications such as data encryption and digital signature. Predicated on the challenge of factoring large integers, RSA's security hinges on the presumed difficulty of this problem. Typically, RSA employs a usual modulus $N = pq$, where p and q are large prime numbers of the same bit length. The public key e (i.e, known as the encryption exponent) is chosen such that $\gcd(e, (p-1)(q-1)) = 1$, while the private key d (i.e, known as the decryption exponent) satisfies $ed \equiv 1 \pmod{(p-1)(q-1)}$, leading to the RSA key equation $ed - k(p-1)(q-1) = 1$. The efficiency of RSA's encryption and decryption operations scales with the bit length of e and d. Hence, to speed up these processes, ones sometimes opt for smaller key sizes, inadvertently rendering RSA susceptible to potential attacks. Consequently, many small key attacks targeting RSA have emerged.

In contrast to the small public key attack, as presented by Coppersmith [Cop97], usually recovering a few plaintexts, the small private key attack poses a severe threat

*This work was supported by the National Natural Science Foundation of China, grant number 62002335, and Ningbo Young Science and Technology Talent Cultivation Program, grant number 2023QL007.

by compromising the entire RSA cryptosystem. Therefore, the investigation into small private key attacks within RSA has garnered more attention. Among these, the seminal Wiener's attack [Wie90] demonstrated that when $d < \frac{1}{3}N^{0.25}$, utilizing the continued fraction-based method leads to the polynomial-time recovery of the complete private key d. Subsequent advancement was given by Boneh and Durfee [BD99], using Coppersmith's techniques based on lattice reduction algorithms to improve the threshold to $d < N^{0.292}$. Building upon both of the continued fraction-based and lattice-based methods, Blömer and May [BM04] proposed an attack targeting the generalized key equation $ex + y = k(p-1)(q-1)$, demonstrating the feasibility of factoring $N = pq$ if $x < \frac{1}{3}N^{\frac{1}{4}}$ and $|y| = O(N^{-\frac{3}{4}}ex)$.

To accommodate distinct application scenarios, the standard RSA scheme has been generalized into several RSA variants. These modifications consist of alterations to the modulus, such as $N = p^r q$ [Tak98] or $N = p_1 p_2 \cdots p_r$ [CHLS98], as well as an enhancement to the decryption process [QC82], aimed at improving practical efficiency. Moreover, some RSA variants adopt specialized arithmetic operations involving elliptic curves [Koy95], quadratic fields [PT00], and cubic fields [MS18] in conjunction with the modulus N and encryption exponent e. These tailored approaches serve to secure RSA against specific attacks, such as chosen ciphertext attack or broadcast attack [Hås85].

Recently, Murru and Saettone [MS18] introduced a novel RSA variant based on the cubic Pell equation $x^3 + ry^3 + r^2z^3 - 3rxyz = 1$. Referred to as the Murru-Saettone cryptosystem or cubic Pell RSA variant, it relies on a key equation $ed \equiv 1 \pmod{(p^2+p+1)(q^2+q+1)}$ with the modulus $N = pq$, the public key e, and the private key d. This equation can be rewritten as

$$ed - k(p^2+p+1)(q^2+q+1) = 1. \tag{1}$$

Additionally, the authors claim that traditional small private key attacks on RSA, such as Wiener's continued fraction-based attack, are ineffective against their scheme.

Extensive security analysis of cubic Pell RSA has been conducted through various studies [ST21, NAAA21, ZKY21, NAA+22, NAB22, FNP24], mainly focusing on small private key attacks under specific circumstances. Denoting $e = N^{\beta}$ and $d = N^{\delta}$, the attack bounds on δ are succinctly summarized in chronological order as follows.

- **ST Attack [ST21].** Susilo and Tonien utilized the continued fraction-based method to establish that for a given RSA modulus $N = pq$ with $q < p < \mu q$, if
$$\delta < \frac{1}{4} - \lambda,$$
where λ is a small positive constant related solely to μ, then the private key d, p, and q can be efficiently recovered.

- **NAAA Attack [NAAA21].** Nitaj et al. employed the continued fraction-based method to demonstrate that if
$$\delta < \frac{5}{4} - \frac{1}{2}\beta \quad \text{for} \quad \frac{3}{2} < \beta < \frac{5}{2},$$

then the RSA modulus $N = pq$ can be efficiently factored. By employing the lattice-based method, the bound can be improved to

$$\delta < \frac{7}{3} - \frac{2}{3}\sqrt{3\beta + 1} \quad \text{for} \quad 1 < \beta < \frac{15}{4}.$$

- **ZKY Attack [ZKY21].** Zheng et al. reformulated the key equation into a modular equation $xh(y) + c \equiv 0 \pmod{e}$, where $h(y)$ is a polynomial of order 2 with integer coefficients. They employed the lattice-based method along with the technique in [Kun12], further refining the bound to

$$\delta < \begin{cases} 2 - \sqrt{\beta}, & 1 \le \beta < \frac{9}{4}, \\ \frac{5}{4} - \frac{\beta}{3}, & \frac{9}{4} \le \beta < \frac{15}{4}. \end{cases}$$

- **NAALC Attack [NAA+22].** Nitaj et al. investigated small decryption exponent attacks under small prime factor difference $|p - q| = N^{\alpha}$ and introduced two distinct attacks. One uses the continued fraction-based method, recovering the private key d and factoring the modulus N if

$$\delta < \frac{7}{4} - \frac{1}{2}\beta - \alpha \quad \text{for} \quad \frac{1}{2} + 2\alpha < \beta < \frac{7}{2} - 2\alpha.$$

Another one uses the lattice-based method, improving the attack bound to

$$\delta < \frac{5}{3} + \frac{4}{3}\alpha - \frac{2}{3}\sqrt{(4\alpha - 1)(3\beta + 4\alpha - 1)} \quad \text{for} \quad \beta > 2\alpha.$$

- **NAB Attack [NAB22].** Nassr et al. explored three types of attacks based on the continued fraction-based method in specific scenarios concerning prime factors p and q. They showed that these attacks are effective if

$$\delta \le \frac{3}{4} - \alpha \quad \text{or} \quad \delta \le \frac{3}{4} - \zeta \quad \text{or} \quad \delta < \frac{1 - \eta}{2},$$

where assuming $|p - q| = N^{\alpha}$, $|2q - p| = N^{\zeta}$, and an approximation p_0 for p such that $|p - p_0| \le N^{\eta}$ with $\eta \le 1/2$.

- **FNP Attack [FNP24].** Feng et al. used Kunihiro's technique [Kun12] to solve the modular equation in the form of $xh(y) + 1 \equiv 0 \pmod{e}$. They applied it to the private key attacks under the condition that the most significant bits of p are known, enhancing the bound of Nassr et al.'s third attack [NAB22]. Specifically, if

$$\delta < \begin{cases} 2 - \sqrt{2\beta\xi}, & 2\xi < \beta < \frac{9}{2}\xi, \\ 2 - \frac{1}{3}\beta - \frac{3}{2}\xi, & \frac{9}{2}\xi \le \beta < 6 - \frac{9}{2}\xi, \end{cases}$$

where $|p - p_0| = N^{\xi}$ and p_0 is an approximation of p, then N can be factored in polynomial time.

Our Contribution. We notice that the majority of existing attacks deal with the security issue from the perspective of solving the key equation $ed-k(p^2+p+1)(q^2+q+1)=1$. Additionally, there have been works like [NAA+22, NAB22, FNP24] extending cryptanalysis into specialized scenarios with side channel information. For example, one previous attack [NAA+22] exploited the small difference in prime factors. Their result is identical to that presented in [NAAA21] for $\alpha = 1/2$.

In this paper, from the perspective of mathematical cryptanalysis and theoretical interest like [BNST17, NPT18], we delve deeper into the examination of the security of cubic Pell RSA variant by investigating the generalized key equation

$$eu - (p^2 + p + 1)(q^2 + q + 1)v = w. \tag{2}$$

This equation is reformulated into a modular form as follows:

$$v(p+q)^2 + (N+1)(p+q)v + (N^2 - N + 1)v + w \equiv 0 \pmod{e}.$$

Considering $e = N^\beta$, $u = N^\delta$, and $|w| = N^\gamma$, we demonstrate that if

$$\delta < \frac{7}{3} - \gamma - \frac{2}{3}\sqrt{1 + 3\beta - 3\gamma} - \varepsilon, \tag{3}$$

where ε is a negligible positive real, the lattice-based method can be employed to solve the modular equation efficiently, thereby obtaining the prime factors p and q. Moreover, the original (1) becomes as a special case of (2) when $w = 1$ and hence $\gamma = 0$. The condition (3) then reduces to

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

which is identical to the result given in Nital et al.'s attack [NAAA21].

Organization. The rest of this paper is organized as follows. In Section 2, we provide an overview of the cubic Pell RSA variant, characterized by the key equation $ed - k(p^2 + p + 1)(q^2 + q + 1) = 1$, and revisit basic concepts related to the lattice-based method. Section 3 elaborates on the generalized cryptanalysis of the cubic Pell RSA variant. Section 4 provides a detailed numerical example to validate the correctness and effectiveness of our attack. Finally, Section 5 concludes our findings based on this investigation.

2 Preliminaries

We first introduce the cubic Pell RSA variant that satisfies the key equation $ed - k(p^2 + p + 1)(q^2 + q + 1) = 1$. Then we present some basic concepts related to the lattice-based method, including lattice reduction and Coppersmith's techniques. Moreover, we summarize the specific flow of the lattice-based method and mention an important heuristic assumption.

2.1 Cubic Pell RSA Variant

Let $\mathbb{F}$ be a field with $(t^3 - r)$ being an irreducible polynomial in $\mathbb{F}[t]$. We introduce the quotient field

$$\mathbb{A} = \mathbb{F}[t]/(t^3 - r) = \left\{x + yt + zt^2 : x, y, z \in \mathbb{F}\right\}.$$

Within $\mathbb{A}$, a product $\bullet$ is induced between two triples, denoted as (x_1, y_1, z_1) and $(x_2, y_2, z_2) \in \mathbb{F}^3$. This product, denoted by $(x_1, y_1, z_1) \bullet (x_2, y_2, z_2)$, is computed as

$$(x_1x_2 + (y_2z_1 + y_1z_2)r, x_2y_1 + x_1y_2 + rz_1z_2, y_1y_2 + x_2z_1 + x_1z_2).$$

The norm of an element (x, y, z) is defined as $\mathrm{N}(x, y, z) = x^3 + ry^3 + r^2z^3 - 3rxyz$. By considering the unitary elements, we arrive at the cubic Pell curve

$$\mathcal{C} = \left\{(x, y, z) \in \mathbb{F}^3 : x^3 + ry^3 + r^2z^3 - 3rxyz = 1\right\},$$

where $x^3 + ry^3 + r^2z^3 - 3rxyz = 1$ represents the more natural cubic Pell equation for a non-cubic integer r.

Beginning with $\mathbb{A}$, we examine the quotient group $\mathcal{B} = \mathbb{A}^*/\mathbb{F}^*$ equipped with a non-standard product $\odot$. This group $\mathcal{B}$ can be represented as

$$\mathcal{B} = \left\{[m + nt + t^2] : m, n \in \mathbb{F}\right\} \cup \left\{[m + t] : m \in \mathbb{F}\right\} \cup \left\{[1_{\mathbb{F}^*}]\right\},$$

where $[\cdot]$ denotes the equivalence set. By fixing an element $\theta \notin \mathbb{F}$, the elements of $\mathcal{B}$ can be interpreted as (m, n) with $m, n \in \mathbb{F}$, or (m, θ) with $m \in \mathbb{F}$, or (θ, θ). Consequently, the group $\mathcal{B}$ is expressed as

$$\mathcal{B} = (\mathbb{F} \times \mathbb{F}) \cup (\mathbb{F} \times \{\theta\}) \cup (\{\theta\} \times \{\theta\}).$$

The rules for computing the commutative product $\odot$ in $\mathcal{B}$ are defined as follows, with (θ, θ) representing the identity.

- $(m, \theta) \odot (k, \theta) = (mk, m + k)$;
- $(m, n) \odot (k, \theta) =$
$$\begin{cases} \left(\dfrac{mk + r}{n + k}, \dfrac{m + nk}{n + k}\right), & n + k \neq 0, \\ \left(\dfrac{mk + r}{m - n^2}, \theta\right), & n + k = 0,\ m - n^2 \neq 0, \\ (\theta, \theta), & \text{otherwise;} \end{cases}$$
- $(m, n) \odot (k, l) =$
$$\begin{cases} \left(\dfrac{mk + (n + l)r}{m + k + nl}, \dfrac{nk + ml + r}{m + k + nl}\right), & m + k + nl \neq 0, \\ \left(\dfrac{mk + (n + l)r}{nk + ml + r}, \theta\right), & m + k + nl = 0,\ nk + ml + r \neq 0, \\ (\theta, \theta), & \text{otherwise.} \end{cases}$$

The cubic Pell RSA variant scheme relies on several key principles. By setting $\mathbb{F} = \mathbb{Z}_p$ and fixing $\theta = \infty$, we establish $\mathbb{A} = \mathrm{GF}(p^3)$ in this scenario. Consequently, $\mathcal{B}$ becomes a cyclic group of order $(p^3-1)/(p-1) = p^2+p+1$, with a well-defined product $\odot$. An analog of Fermat's little theorem emerges, expressed as

$$(m,n)^{\odot p^2+p+1} \equiv (\infty,\infty) \pmod{p},$$

for any $m \in \mathbb{Z}_p$ and $n \in \mathbb{Z}_p \cup \{\infty\}$. Furthermore, we can evaluate powers using the $\odot$ product through a generalization of Rédei rational functions. When $N = pq$, with p and q being prime numbers of the same bit length, the power computation yields

$$(m,n)^{\odot (p^2+p+1)(q^2+q+1)} \equiv (\infty,\infty) \pmod{N},$$

which resembles Euler's theorem. The public key cryptosystem proposed in [MS18] utilizing the $\odot$ product is outlined as follows.

Key Generation. To generate public and private keys, select two prime numbers p and q of the same bit length, and compute the modulus $N = pq$. Randomly choose an integer e such that $\gcd(e,(p^2+p+1)(q^2+q+1)) = 1$, and select a non-cubic integer r from $\mathbb{Z}_p$, $\mathbb{Z}_q$, and $\mathbb{Z}_N$. Compute d satisfying $ed \equiv 1 \pmod{(p^2+p+1)(q^2+q+1)}$. The public key is (N,e,r), while the corresponding private key is (p,q,d).

Encryption. To encrypt plaintexts m_1 and m_2 in $\mathbb{Z}_N$, use the encryption calculation

$$(c_1,c_2) \equiv (m_1,m_2)^{\odot e} \pmod{N}.$$

Decryption. For ciphertexts c_1 and c_2 in $\mathbb{Z}_N$, decrypt them by evaluating

$$(m_1^?,m_2^?) \equiv (c_1,c_2)^{\odot d} \pmod{N}.$$

In summary, this RSA variant scheme, employing cubic Pell equation, uses a novel group with a non-standard product. Its powers are evaluated using generalized Rédei functions.

2.2 Lattice-Based Method

Let n and ω denote two positive integers. Suppose we have ω linearly independent vectors $\vec{b}_1,\ldots,\vec{b}_\omega \in \mathbb{R}^n$. The lattice $\mathcal{L}$, spanned by the above vectors, is a set of all possible integer linear combinations of $\vec{b}_1,\ldots,\vec{b}_\omega$, expressed as

$$\mathcal{L}\left(\vec{b}_1,\ldots,\vec{b}_\omega\right) = \left\{\sum_{i=1}^{\omega} a_i\vec{b}_i \in \mathbb{R}^n : a_i \in \mathbb{Z}\right\}.$$

Furthermore, $\vec{b}_1,\ldots,\vec{b}_\omega$ form a lattice basis for the lattice $\mathcal{L}$. Treating each $\vec{b}_i$ as a row/column vector, they collectively constitute a lattice matrix B. The lattice $\mathcal{L}$ can thus be represented by the lattice matrix B. The lattice determinant is defined as $\det(\mathcal{L}) = \sqrt{\det(BB^{\mathsf{T}})}$, where B^{T} denotes the transpose of B. The dimension and rank of $\mathcal{L}$ are denoted by n and ω, respectively. In the case when the lattice $\mathcal{L}$

attains full rank, i.e., $n = \omega$, the lattice matrix B becomes a square matrix, and hence $\det(\mathcal{L}) = |\det(B)|$.

The LLL lattice reduction algorithm [LLL82], introduced by Lenstra, Lenstra, and Lovász, serves the purpose of discovering a high-quality reduced basis for lattices, finding useful applications in cryptanalysis. Below, we present the result established in [May03].

Lemma 1. *Let $\mathcal{L}$ be a lattice consisting of input basis vectors $(\vec{b}_1, \ldots, \vec{b}_\omega)$. After applying the LLL lattice reduction algorithm, reduced basis vectors $(\vec{v}_1, \ldots, \vec{v}_\omega)$ is obtained, satisfying*

$$\|\vec{v}_i\| \leq 2^{\frac{\omega(\omega-1)}{4(\omega+1-i)}} \det(\mathcal{L})^{\frac{1}{\omega+1-i}},$$

where $i = 1, \ldots, \omega$. The running time is a polynomial related to ω and the maximal norm length of the input lattice basis vectors.

The lattice-based method (also known as Coppersmith's techniques), introduced by Coppersmith [Cop96a, Cop96b], initially addressed solving small roots of univariate modular polynomial equations and bivariate integer polynomial equations efficiently within polynomial time. Since then, the lattice-based method develops heuristic extensions to handle multivariate polynomial equations [May10]. For an n-variate polynomial

$$h(x_1, \ldots, x_n) = \sum_{i_1, \ldots, i_n} a_{i_1, \ldots, i_n} x_1^{i_1} \cdots x_n^{i_n},$$

where $a_{i_1, \ldots, i_n} \in \mathbb{Z}$, the Euclidean norm is defined as

$$\|h(x_1, \ldots, x_n)\| = \sqrt{\sum a_{i_1, \ldots, i_n}^2}.$$

Howgrave-Graham's reformulation [How97] is an improvement of Coppersmith's original approach. The result is described as follows.

Lemma 2. *Let $h(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ be an integer polynomial with at most ω monomials and let e and m be two positive integers. If the following two conditions hold:*

1. *$h(x_1', \ldots, x_n') \equiv 0 \pmod{e^m}$, where $|x_1'| \leq X_1, \ldots, |x_n'| \leq X_n$,*
2. *$\|h(x_1 X_1, \ldots, x_n X_n)\| < e^m/\sqrt{\omega}$.*

Then $(x_1', \ldots, x_n')$ is a solution satisfying $h(x_1', \ldots, x_n') = 0$ over the integers.

Using the lattice-based method, we aim to discover the root (x', y', z') of the target modular polynomial equation $f(x, y, z) = xy^2 + axy + bx + z \equiv 0 \pmod{e}$ according to the above two lemmas. Here, a, b, and e are predetermined integers. First, we build upon $f(x, y, z)$ to derive a set of shift polynomials including $G(x, y, z)$ and $H(x, y, z)$, where the roots of these polynomials modulo e^m correspond to (x', y', z'), with m being a well-chosen positive integer. Subsequently, we construct a lattice $\mathcal{L}$ of dimension ω, with each row vector of the lattice basis matrix representing the coefficient vector of the shift polynomials $G(xX, yY, zZ)$ and

$H(xX, yY, zZ)$. Employing the LLL lattice reduction algorithm on $\mathcal{L}$ yields several reduced basis vectors. These vectors contribute to reproducing newly derived polynomials $h(x, y, z)$ satisfying $h(x, y, z) \equiv 0 \pmod{e^m}$.

Combining Lemma 1 and Lemma 2, we know that if the following inequality is satisfied:

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

then the conditions of the Howgrave-Graham's reformulation are met, enabling the satisfaction of $h(x, y, z)) = 0$ over the integers for the root (x', y', z'). Furthermore, the solution can be recovered through trivial methods such as Gröbner basis computation [BWK93] or resultant elimination.

It is notable that the lattice-based method for multivariate polynomial equations is heuristic, with its effectiveness reliant on the following assumption. The integer equations obtained from the lattice-based method are algebraically independent. Thus, the common root of these derived equations can be efficiently recovered by the Gröbner basis computation or the resultant elimination.

3 Generalized Cryptanalysis

We apply the lattice-based method to analyze the cubic Pell RSA variant with the generalized key equation $eu - (p^2 + p + 1)(q^2 + q + 1)v = w$ with a given modulus $N = pq$ and a given public key e. The generalized cryptanalysis result is stated below.

Proposition 1. *Let $N = pq$ be the product of two unknown prime numbers with $q < p < 2q$. Suppose that $e = N^\beta$ satisfying the generalized key equation $eu - (p^2 + p + 1)(q^2 + q + 1)v = w$, where $u = N^\delta$ and $|w| = N^\gamma$. Then one can factor N in polynomial time if*

$$\delta < \frac{7}{3} - \gamma - \frac{2}{3}\sqrt{1 + 3\beta - 3\gamma} - \varepsilon, \tag{4}$$

provided that $\gamma \leq \beta - 1$.

Proof. Assume that the public key $e = N^\beta$ satisfies $eu-(p^2+p+1)(q^2+q+1)v = w$ with $u = N^\delta$ and $|w| = N^\gamma$. We have

$$v = \frac{eu - w}{(p^2 + p + 1)(q^2 + q + 1)} < \frac{eu + |w|}{(p^2 + p + 1)(q^2 + q + 1)} < 2N^{\beta+\delta-2}$$

since $(p^2+p+1)(q^2+q+1) > N^2$ and assuming $|w| < eu$. Therefore, the bounds on the solution (u, v, w) of the generalized key equation $eu-(p^2+p+1)(q^2+q+1)v = w$ are

$$u = N^\delta,\ v < 2N^{\beta+\delta-2},\ |w| = N^\gamma.$$

Moreover, the generalized key equation $eu - (p^2 + p + 1)(q^2 + q + 1)v = w$ can be transformed into the modular form

$$v((p + q)^2 + (N + 1)(p + q) + N^2 - N + 1) + w \equiv 0 \pmod{e}.$$

It can be rewritten as

$$v(p+q)^2 + (N+1)(p+q)v + (N^2 - N + 1)v + w \equiv 0 \pmod{e}.$$

Consider the following trivariate polynomial

$$f(x, y, z) = xy^2 + axy + bx + z, \tag{5}$$

where known parameters are $a = N + 1$ and $b = N^2 - N + 1$. Thus, $(x', y', z') = (v, p + q, w)$ is the root of the modular polynomial equation $f(x, y, z) \equiv 0 \pmod{e}$. In order to recover its small solution, we further use Jochemsz-May's extension strategy [JM06]. Because p and q are of the same bit length, we have $p + q < 3N^{\frac{1}{2}}$. Therefore, we set the upper bounds on (x', y', z') to be

$$X = 2N^{\beta+\delta-2},\ Y = 3N^{\frac{1}{2}},\ Z = N^{\gamma}.$$

Generating Shift Polynomials. Let m be a positive integer and t be a non-negative integer to be optimized later. For $0 \le k \le m$, we define the following monomial set

$$M_k = \bigcup_{0 \le j \le 2+t} \Big\{ x^{i_1} y^{i_2+j} z^{i_3} : x^{i_1} y^{i_2} z^{i_3} \text{ is a monomial of } f(x, y, z)^m \text{ and } \frac{x^{i_1} y^{i_2} z^{i_3}}{(xy^2)^k} \text{ is a monomial of } f(x, y, z)^{m-k} \Big\}.$$

We calculate $f(x, y, z)^m = (xy^2 + axy + bx + z)^m$ as

$$\sum_{i_1=0}^{m} \sum_{j_1=0}^{i_1} \sum_{j_2=0}^{i_1-j_1} \binom{m}{i_1} \binom{i_1}{j_1} \binom{i_1 - j_1}{j_2} x^{i_1} y^{2j_1} (ay)^{j_2} b^{i_1-j_1-j_2} z^{m-i_1},$$

which further leads to

$$\sum_{i_1=0}^{m} \sum_{j_1=0}^{i_1} \sum_{j_2=0}^{i_1-j_1} \binom{m}{i_1} \binom{i_1}{j_1} \binom{i_1 - j_1}{j_2} a^{j_2} b^{i_1-j_1-j_2} x^{i_1} y^{2j_1+j_2} z^{m-i_1}.$$

So, we observe that $x^{i_1} y^{i_2} z^{i_3}$ is a monomial of $f(x, y, z)^m$ if

$$i_1 = 0, \ldots, m,\ i_2 = 0, \ldots, 2i_1,\ i_3 = m - i_1.$$

Similarly, $x^{i_1} y^{i_2} z^{i_3}$ is a monomial of $f(x, y, z)^{m-k}$ if

$$i_1 = 0, \ldots, m - k,\ i_2 = 0, \ldots, 2i_1,\ i_3 = m - k - i_1.$$

For $0 \le k \le m$, if $x^{i_1} y^{i_2} z^{i_3}$ is a monomial of $f(x, y, z)^m$, then $x^{i_1} y^{i_2} z^{i_3}/(xy^2)^k$ is a monomial of $f(x, y, z)^{m-k}$ if

$$i_1 = k, \ldots, m,\ i_2 = 2k, \ldots, 2i_1,\ i_3 = m - i_1.$$

Therefore, we obtain an accurate description of i_1, i_2, i_3 for each $x^{i_1} y^{i_2} z^{i_3} \in M_k$, that is

$$i_1 = k, \ldots, m,\ i_2 = 2k, \ldots, 2i_1 + 2 + t,\ i_3 = m - i_1.$$

Similarly, we have $x^{i_1}y^{i_2}z^{i_3} \in M_{k+1}$ if

$$i_1 = k+1,\ \ldots, m, i_2 = 2k+2, \ldots, 2i_1+2+t,\ i_3 = m-i_1.$$

Thus, we define the following shift polynomials for $x^{i_1}y^{i_2}z^{i_3} \in M_k \setminus M_{k+1}$:

$$g_{k,i_1,i_2,i_3}(x,y,z) = \frac{x^{i_1}y^{i_2}z^{i_3}}{(xy^2)^k} f(x,y,z)^k e^{m-k}.$$

Analyzing it in depth for $t \geq 0$, we can see that $x^{i_1}y^{i_2}z^{i_3} \in M_k \setminus M_{k+1}$ implies either

$$i_1 = k, \ldots, m,\ i_2 = 2k, 2k+1,\ i_3 = m-i_1,$$

or

$$i_1 = k,\ i_2 = 2k+2, \ldots, 2i_1+2+t,\ i_3 = m-i_1.$$

Therefore, the shift polynomials $g_{k,i_1,i_2,i_3}(x,y,z)$ can be further divided into two polynomial sets:

$$\begin{aligned} G_{k,i_1,i_2,i_3}(x,y,z) &= x^{i_1-k}y^{i_2-2k}z^{i_3} f(x,y,z)^k e^{m-k}, \\ &\quad k = 0, \ldots m,\ i_1 = k, \ldots, m,\ i_2 = 2k, 2k+1,\ i_3 = m-i_1, \\ H_{k,i_1,i_2,i_3}(x,y,z) &= y^{i_2-2k}z^{i_3} f(x,y,z)^k e^{m-k}, \\ &\quad k = 0, \ldots m,\ i_1 = k,\ i_2 = 2k+2, \ldots, 2i_1+2+t,\ i_3 = m-i_1. \end{aligned}$$

Since $f(x,y,z) \equiv 0 \pmod{e}$, the constructed shift polynomials satisfy

$$G_{k,i_1,i_2,i_3}(x,y,z) \equiv H_{k,i_1,i_2,i_3}(x,y,z) \equiv 0 \pmod{e^m}.$$

Generating Integer Lattice. Let $\mathcal{L}$ represent a lattice, where the row vectors of its lattice basis matrix correspond to the coefficient vectors of shift polynomials $G_{k,i_1,i_2,i_3}(xX, yY, zZ)$ and $H_{k,i_1,i_2,i_3}(xX, yY, zZ)$, with X, Y, and Z denoting the upper bounds on the root (x', y', z'). In terms of row order, precedence is given to any $G_{k,i_1,i_2,i_3}(xX, yY, zZ)$ over any $H_{k,i_1,i_2,i_3}(xX, yY, zZ)$. Moreover, the polynomial order $\prec_{\mathrm{p}}$ is established as $(k, i_1, i_2, i_3) \prec_{\mathrm{p}} (k', i_1', i_2', i_3')$ if

- $k < k'$; or
- $k = k'$ and $i_1 < i_1'$; or
- $k = k',\ i_1 = i_1'$ and $i_2 < i_2'$; or
- $k = k',\ i_1 = i_1',\ i_2 = i_2'$ and $i_3 < i_3'$.

Similarly, the monomial order $\prec_{\mathrm{m}}$ is defined as $x^{i_1}y^{i_2}z^{i_3} \prec_{\mathrm{m}} x^{i_1'}y^{i_2'}z^{i_3'}$ if

- $i_1 < i_1'$; or
- $i_1 = i_1'$ and $i_2 < i_2'$; or
- $i_1 = i_1',\ i_2 = i_2'$ and $i_3 < i_3'$.

We know that each polynomial in $G_{k,i_1,i_2,i_3}(x,y,z)$ introduces a monomial $x^{i_1}y^{i_2}z^{i_3}e^{m-k}$ for $k=0,\dots m,\ i_1=k,\dots,m,\ i_2=2k,2k+1,\ i_3=m-i_1$, and each polynomial in $H_{k,i_1,i_2,i_3}(x,y,z)$ introduces a monomial $x^{i_1}y^{i_2}z^{i_3}e^{m-k}$ for $k=0,\dots m,\ i_1=k,\ i_2=2k+2,\dots,2i_1+2+t,\ i_3=m-i_1$. The above polynomial and monomial orders shall lead to the construction of a lower triangular basis matrix. In Table 1, we provide a toy example of the lattice basis matrix for $m=2$ and $t=0$, where the symbol '–' denotes a non-zero off-diagonal element.

Considering that a lower triangular matrix only requires multiplication of the diagonal terms for computing the determinant, we derive the lattice determinant in relation to e, X, Y, and Z as

$$\det(\mathcal{L}) = e^{n_e}X^{n_X}Y^{n_Y}Z^{n_Z}. \tag{6}$$

According to the introduced monomials $x^{i_1}y^{i_2}z^{i_3}e^{m-k}$ in $G_{k,i_1,i_2,i_3}(x,y,z)$ and $H_{k,i_1,i_2,i_3}(x,y,z)$, the exponents $n_e,\ n_X,\ n_Y,\ n_Z$ and the lattice dimension ω are calculated as follows.

$$\begin{aligned}
n_e &= \sum_{k=0}^{m}\sum_{i_1=k}^{m}\sum_{i_2=2k}^{2k+1}\sum_{i_3=m-i_1}^{m-i_1}(m-k) + \sum_{k=0}^{m}\sum_{i_1=k}^{k}\sum_{i_2=2k+2}^{2i_1+2+t}\sum_{i_3=m-i_1}^{m-i_1}(m-k)\\
&= \sum_{k=0}^{m}\sum_{i_1=k}^{m}2(m-k) + \sum_{k=0}^{m}\sum_{i_2=2k+2}^{2i_1+2+t}(m-k)\\
&= \frac{1}{6}m(m+1)(4m+3t+11),\\
n_X &= \sum_{k=0}^{m}\sum_{i_1=k}^{m}\sum_{i_2=2k}^{2k+1}\sum_{i_3=m-i_1}^{m-i_1} i_1 + \sum_{k=0}^{m}\sum_{i_1=k}^{k}\sum_{i_2=2k+2}^{2i_1+2+t}\sum_{i_3=m-i_1}^{m-i_1} i_1\\
&= \sum_{k=0}^{m}\sum_{i_1=k}^{m}2i_1 + \sum_{k=0}^{m}\sum_{i_2=2k+2}^{2i_1+2+t}k\\
&= \frac{1}{6}m(m+1)(4m+3t+11),\\
n_Y &= \sum_{k=0}^{m}\sum_{i_1=k}^{m}\sum_{i_2=2k}^{2k+1}\sum_{i_3=m-i_1}^{m-i_1} i_2 + \sum_{k=0}^{m}\sum_{i_1=k}^{k}\sum_{i_2=2k+2}^{2i_1+2+t}\sum_{i_3=m-i_1}^{m-i_1} i_2\\
&= \sum_{k=0}^{m}\sum_{i_1=k}^{m}(4k+1) + \sum_{k=0}^{m}\sum_{i_2=2k+2}^{2i_1+2+t} i_2\\
&= \frac{1}{6}(m+1)\left(4m^2+6mt+3t^2+17m+15t+18\right),\\
n_Z &= \sum_{k=0}^{m}\sum_{i_1=k}^{m}\sum_{i_2=2k}^{2k+1}\sum_{i_3=m-i_1}^{m-i_1} i_3 + \sum_{k=0}^{m}\sum_{i_1=k}^{k}\sum_{i_2=2k+2}^{2i_1+2+t}\sum_{i_3=m-i_1}^{m-i_1} i_3\\
&= \sum_{k=0}^{m}\sum_{i_1=k}^{m}2(m-i_1) + \sum_{k=0}^{m}\sum_{i_2=2k+2}^{2i_1+2+t}(m-k)\\
&= \frac{1}{6}m(m+1)(2m+3t+7),
\end{aligned}$$

Table 1: A toy example of the lattice basis matrix for $m = 2$ and $t = 0$.

	z^2	yz^2	xz	xyz	x^2	x^2y	xy^2z	xy^3z	x^2y^2	x^2y^3	x^2y^4	x^2y^5	y^2z^2	xy^4z	x^2y^6
$G_{[0,0,0,2]}$	Z^2e^2														
$G_{[0,0,1,2]}$		YZ^2e^2													
$G_{[0,1,0,1]}$			XZe^2												
$G_{[0,1,1,1]}$				$XYZe^2$											
$G_{[0,2,0,0]}$					X^2e^2										
$G_{[0,2,1,0]}$						X^2Ye^2									
$G_{[1,1,2,1]}$	–		–	–			XY^2Ze								
$G_{[1,1,3,1]}$		–		–			–	XY^3Ze							
$G_{[1,2,2,0]}$			–		–	–			X^2Y^2e						
$G_{[1,2,3,0]}$				–		–			–	X^2Y^3e					
$G_{[2,2,4,0]}$	–		–	–	–	–	–		–	–	X^2Y^4				
$G_{[2,2,5,0]}$		–		–		–	–	–	–	–	–	X^2Y^5			
$H_{[0,0,2,2]}$													$Y^2Z^2e^2$		
$H_{[1,1,4,1]}$							–	–					–	XY^4Ze	
$H_{[2,2,6,0]}$							–	–	–	–	–	–	–	–	X^2Y^6

$$\begin{aligned}\omega &= \sum_{k=0}^{m}\sum_{i_1=k}^{m}\sum_{i_2=2k}^{2k+1}\sum_{i_3=m-i_1}^{m-i_1} 1 + \sum_{k=0}^{m}\sum_{i_1=k}^{k}\sum_{i_2=2k+2}^{2i_1+2+t}\sum_{i_3=m-i_1}^{m-i_1} 1\\ &= \sum_{k=0}^{m}\sum_{i_1=k}^{m} 2 + \sum_{k=0}^{m}\sum_{i_2=2k+2}^{2i_1+2+t} 1\\ &= (m+1)(m+t+3).\end{aligned}$$

Letting $t = \tau m$ with a real $\tau \geq 0$ for simplicity, we obtain the following results by calculating the main term concerning m^3 of $n_e,\ n_X,\ n_Y,\ n_Z$ and m^2 of ω, respectively.

$$\begin{aligned} n_e &= \frac{1}{6}(3\tau+4)m^3 + o(m^3),\\ n_X &= \frac{1}{6}(3\tau+4)m^3 + o(m^3),\\ n_Y &= \frac{1}{6}\left(3\tau^2+6\tau+4\right)m^3 + o(m^3),\\ n_Z &= \frac{1}{6}(3\tau+2)m^3 + o(m^3),\\ \omega &= (\tau+1)m^2 + o(m^2).\end{aligned} \tag{7}$$

Generating Reduced Vectors. After applying the lattice-based method, we derive reduced basis vectors $\vec{v_i}$ associated with $h_i(x,y,z)$ for $i \leq 3$ satisfying

$$\|h_i(Xx, Yy, Zz)\| \leq 2^{\frac{\omega(\omega-1)}{4(\omega-2)}} \det(\mathcal{L})^{\frac{1}{\omega-2}}.$$

Furthermore, we should ensure $\|h_i(Xx, Yy, Zz)\| < e^m/\sqrt{\omega}$ to employ Howgrave-Graham's reformulation. Therefore, we get

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

which can be reduced to

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

Combining it with (6), we deduce that

$$e^{n_e - m\omega} X^{n_X} Y^{n_Y} Z^{n_Z} < 2^{-\frac{\omega(\omega-1)}{4}} \omega^{-\frac{\omega-2}{2}} e^{-2m}.$$

Substituting $e = N^\beta, X = 2N^{\beta+\delta-2}, Y = 3N^{\frac{1}{2}}, Z = N^\gamma$ results in

$$N^{\beta(n_e - m\omega)+(\beta+\delta-2)n_X+\frac{1}{2}n_Y+\gamma n_Z} < 2^{-\frac{\omega(\omega-1)}{4}-n_X} 3^{-n_Y} \omega^{-\frac{\omega-2}{2}} e^{-2m}.$$

We put $n_e, n_X, n_Y, n_Z, \omega$ from (7) and derive the following inequality when dealing with the exponents over N and omitting negligible terms:

$$\begin{aligned}\beta \cdot \left(\frac{1}{2}\tau + \frac{2}{3} - \tau - 1\right) + (\beta+\delta-2)\cdot\left(\frac{1}{2}\tau+\frac{2}{3}\right)\\ + \frac{1}{2}\cdot\left(\frac{1}{2}\tau^2+\tau+\frac{2}{3}\right) + \gamma\cdot\left(\frac{1}{2}\tau+\frac{1}{3}\right) < -\varepsilon_0,\end{aligned} \tag{8}$$

where ε_0 is a negligible positive real. Then, we simplify this inequality (8) and obtain

$$\left(\frac{1}{2}\tau + \frac{2}{3}\right)\delta + \frac{1}{4}\tau^2 + \left(\frac{1}{2}\gamma - \frac{1}{2}\right)\tau + \frac{1}{3}\beta + \frac{1}{3}\gamma - 1 < -\varepsilon_0.$$

We further have

$$\delta < \frac{-3\tau^2 + (6 - 6\gamma)\tau + 12 - 4\beta - 4\gamma}{6\tau + 8} - \varepsilon, \tag{9}$$

where ε is a negligible positive real. By setting $\tau_0 = (2\sqrt{1 + 3\beta - 3\gamma} - 4)/3$, the right side of inequality (9) can be maximized to

$$\delta < \frac{7}{3} - \gamma - \frac{2}{3}\sqrt{1 + 3\beta - 3\gamma} - \varepsilon.$$

Note that we need $\tau_0 \geq 0$, which implies $2\sqrt{1 + 3\beta - 3\gamma} - 4 \geq 0$ and hence $\gamma \leq \beta - 1$. Moreover, we should ensure $1 + 3\beta - 3\gamma \geq 0$ and fortunately $\gamma \leq \beta - 1$ is sufficient for this constraint.

On the other hand, we should set $\tau_0 = 0$ if $\gamma > \beta - 1$. Then the inequality (9) turns to

$$\delta < \frac{3}{2} - \frac{1}{2}\beta - \frac{1}{2}\gamma - \varepsilon.$$

However, we let $X = 2N^{\beta+\delta-2}$ and hence we have $\beta + \delta \geq 2$. Combining together (and omitting negligible ε) leads to

$$2 - \beta \leq \delta < \frac{3}{2} - \frac{1}{2}\beta - \frac{1}{2}\gamma.$$

This reduces to $\gamma < \beta - 1$ that is contradictory to the prerequisite $\gamma > \beta - 1$. Thus, we conclude that the proposed generalized attack is available for $\gamma \leq \beta - 1$ if

$$\delta < \frac{7}{3} - \gamma - \frac{2}{3}\sqrt{1 + 3\beta - 3\gamma} - \varepsilon. \tag{10}$$

Under the attack condition (10), we apply the proposed attack strategy and finally obtain three integer polynomials $h_1(x, y, z), h_2(x, y, z), h_3(x, y, z)$. These polynomials share the common root $(x', y', z') = (v, p + q, w)$. Therefore, $y' = p + q$ can be extracted by using the Gröbner basis computation or the resultant elimination methods. Combining $p + q$ with given modulus $N = pq$, N can be factored in polynomial time, thus terminating the proof. □

Comparison and Discussion. The detailed comparison of our generalized attack with existing ones against the cubic Pell RSA variant with $N = pq$, $e = N^\beta$, $d = N^\delta$, and $\varphi(N) = (p^2 + p + 1)(q^2 + q + 1)$ is given in Table 2.

Our generalized attack is a natural extension of previous small private key attack for $w = 1$ with $\gamma = 0$. We show more comparative results for $w = 1$. In this case, our bound (4) in Proposition 1 results in

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

Table 2: The comparison of known attacks against the cubic Pell RSA variant.

Attack	Key Equation	Insecure Bound	†Method
ST [ST21]	$ed - k\varphi(N) = 1$	$^{\star}\delta < \frac{1}{4} - \lambda$	CF
NAAA [NAAA21]	$ed - k\varphi(N) = 1$	$\delta < \frac{5}{4} - \frac{1}{2}\beta$	CF
		$\delta < \frac{7}{3} - \frac{2}{3}\sqrt{3\beta + 1}$	LM
ZKY [ZKY21]	$ed - k\varphi(N) = 1$	$\delta < \begin{cases} 2 - \sqrt{\beta}, & 1 \le \beta < \frac{9}{4} \\ \frac{5}{4} - \frac{\beta}{3}, & \frac{9}{4} \le \beta < \frac{15}{4} \end{cases}$	LM
NAALC [NAA+22]	$ed - k\varphi(N) = 1$	$\delta < \frac{7}{4} - \frac{1}{2}\beta - \alpha$	CF
		$\delta < \frac{5}{3} + \frac{4}{3}\alpha - \frac{2}{3}\sqrt{(4\alpha - 1)(3\beta + 4\alpha - 1)}$	LM
NAB [NAB22]	$ed - k\varphi(N) = 1$	$^{*}\delta \le \max\left\{\frac{3}{4} - \alpha,\ \frac{3}{4} - \zeta,\ \frac{1-\eta}{2}\right\}$	CF
FNP [FNP24]	$ed - k\varphi(N) = 1$	$^{\diamond}\delta < \begin{cases} 2 - \sqrt{2\beta\xi}, & 2\xi < \beta < \frac{9}{2}\xi \\ 2 - \frac{1}{3}\beta - \frac{3}{2}\xi, & \frac{9}{2}\xi \le \beta < 6 - \frac{9}{2}\xi \end{cases}$	LM
Ours	$^{\ddagger}eu - v\varphi(N) = w$	$\delta < \frac{7}{3} - \gamma - \frac{2}{3}\sqrt{1 + 3\beta - 3\gamma}$	LM

† Abbreviations CF and LM stand for the continued fraction-based and lattice-based methods respectively.
⋆ λ is a small positive constant related to μ for $q < p < \mu q$.
* α, ζ denote the prime differences in $|p - q| = N^{\alpha}$ and $|2q - p| = N^{\zeta}$, and η comes from $|p - p_0| \le N^{\eta}$ with a known approximation p_0.
◇ ξ denotes the prime leakage in $|p - p_0| = N^{\xi}$ with a known approximation p_0.
‡ δ, γ denote the upper bounds on u and w with $u = N^{\delta}$ and $|w| = N^{\gamma}$.

which outperforms the bounds given in [ST21, NAB22]. For $|p-q| = N^{\frac{1}{2}}$, implying that p differs from q concerning the most significant bits. Our bound (4) in Proposition 1 is identical to the ones in [NAAA21, NAA+22]. Besides, Zheng et al. [ZKY21] proposed an improved bound with $\delta < 2 - \sqrt{\beta}$ for $1 < \beta < 9/4$, and $\delta < 5/4 - \beta/3$ for $9/4 \leq \beta < 15/4$. More concretely, for $1 < \beta < 9/4$, we have

$$\begin{aligned}\delta_1 &= 2 - \sqrt{\beta} - \left(\frac{7}{3} - \frac{2}{3}\sqrt{1+3\beta}\right) = \frac{2(\sqrt{1+3\beta}) - (3\sqrt{\beta}+1)}{3} \\ &= \frac{(\sqrt{\beta}-1)^2}{2\sqrt{1+3\beta}+3\sqrt{\beta}+1} > 0.\end{aligned}$$

For $9/4 \leq \beta < 15/4$, we have

$$\begin{aligned}\delta_2 &= \frac{5}{4} - \frac{\beta}{3} - \left(\frac{7}{3} - \frac{2}{3}\sqrt{1+3\beta}\right) = \frac{8\sqrt{1+3\beta} - (4\beta+13)}{12} \\ &= \frac{-(4\beta-7)(4\beta-15)}{12\left(8\sqrt{1+3\beta}+4\beta+13\right)} > 0.\end{aligned}$$

Therefore, our generalized attack is weaker than Zheng et al.'s attack (and Feng et al.'s attack [FNP24] as well). Differences between their lattice constructions and ours may lead to an additional advantage of their attacks. Nevertheless, our advantage is that the target attack scenario is more general and not limited to $w = 1$.

4 A Numerical Example

We verify the correctness and effectiveness of our generalized attack on the cubic Pell RSA variant through several numerical experiments. The attack experiments run on `SageMath` [The23] under Windows 11 equipped with AMD R55600H. An open source implementation of the proposed attack is provided and the source code is available at https://github.com/MengceZheng/GCPRSA.

Let us now consider a cubic Pell RSA instance with the following public parameters:

$$\begin{aligned}N = {} & 55036620946398325422485189815192043868757214175712155228727025727043796796595708168357793703727607350605192450111339626017017 1, \\ e = {} & 10578003884146132696993930345795908212610088212443443116131322083334835220854572592930841652745184949911092016662030067520314560450321716128630634340225226095506928925611547638614849887118730348691487416121904790439636647883772 09.\end{aligned}$$

Therefore, we have $\beta \approx 1.813$ for $e = N^{\beta}$. For the generalized key equation $eu - (p^2+p+1)(q^2+q+1)v = w$, there exist infinitely many solutions (u, v, w) with positive integers u, v and a non-zero integer w. Our purpose is to extract one root by solving the modular equation $xy^2 + axy + bx + z \equiv 0 \pmod{e}$, where $a = N+1$ and $b = N^2 - N + 1$. To be concrete, we want to find the solution $(x', y', z') = (v, p+q, w)$ satisfying Proposition 1 through our generalized attack.

For $|w| = N^{\gamma}$ with an unknown γ, we may try to reasonably select γ in a certain range, such as $\gamma = 0.1, 0.2, \ldots$ and so on. In this numerical example, we set $\gamma = 0.5$, the attack bound then becomes $\delta < \frac{7}{3} - \gamma - \frac{2}{3}\sqrt{1 + 3\beta - 3\gamma} \approx 0.352$. Using $\delta = 0.352$, we set

$$\begin{aligned}
X &= 2N^{\beta+\delta-2} = 2\left\lfloor N^{0.165} \right\rfloor = 1253639937596726444032,\\
Y &= 3N^{\frac{1}{2}} = 3\left\lfloor N^{0.5} \right\rfloor\\
&= 22256001179852254406157203206163382029610351089090704027701739 52,\\
Z &= N^{\gamma} = \left\lfloor N^{0.5} \right\rfloor\\
&= 74186670599507517731985755126592353023044571789225304375531929 6.
\end{aligned}$$

Next, we choose $m = 4$ and $t = 1$ to construct a lattice $\mathcal{L}$ with dimension $\omega = 40$. The LLL lattice reduction algorithm is executed to output a newly reduced basis and we obtain three integer polynomials. Through the Gröbner basis computation, we obtain the root[1]

$$\begin{aligned}
x' &= 1148264901826,\\
y' &= 153635499145574170774247824596425218872605389729280303848778 2580,\\
z' &= 640938456769247372267247687491800648303566489807825552592834 254.
\end{aligned}$$

After that, using $p + q = y'$ and $pq = N$, we extract

$$\begin{aligned}
p &= 967502495361032247552444598347042412041475154993790090306919213,\\
q &= 568852496094709460190033647617209776684578742299012948180863367.
\end{aligned}$$

Additionally, we can check why our proposed attack applies to this numerical example. We calculate u using $v = x', w = z'$ as follows.

$$\begin{aligned}
u &= \frac{\left(p^2 + p + 1\right)\left(q^2 + q + 1\right)v + w}{e}\\
&= 3288076338659375076524797803216713 40.
\end{aligned}$$

We compute $\delta \approx 0.282$ for $u = N^{\delta}$ and $\gamma \approx 0.499$ for $w = N^{\gamma}$. hence δ, β, γ satisfy the attack condition (4) of Proposition 1. Finally, we compute d as

$$\begin{aligned}
d &= e^{-1} \pmod{(p^2 + p + 1)(q^2 + q + 1)}\\
&= 291299318111792954743124699306973300942774595686767508222770981\\
&\quad 035449126643240795725693062666535871022576676383598809755517829\\
&\quad 339073489412206120878267982273702937142406526252935267790785313\\
&\quad 588516464756006431937128237268745477048505085271366967838413040.
\end{aligned}$$

Note that $\rho \approx 1.999$ for $d = N^{\rho}$, which cannot be achieved by all the existing attacks on the cubic Pell RSA variant. Therefore, when (N, e) satisfies the certain condition, our generalized attack works even if the private key d is extremely large.

[1]We always first recover y' and then x' and z' in our validating experiments.

5 Concluding Remarks

In this paper, we propose a generalized lattice-based attack on the cubic Pell RSA variant, which bases on the key equation $ed - k(p^2 + p + 1)(q^2 + q + 1) = 1$ with $N = pq$. We further extend the key equation to its generalized form $eu - v(p^2 + p + 1)(q^2 + q + 1) = w$. We demonstrate that when

$$\delta < \frac{7}{3} - \gamma - \frac{2}{3}\sqrt{1 + 3\beta - 3\gamma} - \varepsilon,$$

N can be efficiently factored and hence this RSA variant is insecure. Moreover, we achieve superior attack effect even if the private key d is much larger, our generalized attack is still possible to successfully extract the prime factors of N.

The major limitation of our proposed attack on the cubic Pell RSA variant is that it does not reach the best existing attack results [ZKY21, FNP24]. Thus, future research should be undertaken to explore how to incorporate a similar technique used in [ZKY21, FNP24] into our generalized lattice-based attack.

References

[BD99] Dan Boneh and Glenn Durfee. Cryptanalysis of RSA with private key d less than $N^{0.292}$. In Jacques Stern, editor, *Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2-6, 1999, Proceeding*, volume 1592 of *Lecture Notes in Computer Science*, pages 1–11. Springer, 1999.

[BM04] Johannes Blömer and Alexander May. A generalized Wiener attack on RSA. In Feng Bao, Robert H. Deng, and Jianying Zhou, editors, *Public Key Cryptography - PKC 2004, 7th International Workshop on Theory and Practice in Public Key Cryptography, Singapore, March 1-4, 2004*, volume 2947 of *Lecture Notes in Computer Science*, pages 1–13. Springer, 2004.

[BNST17] Martin W. Bunder, Abderrahmane Nitaj, Willy Susilo, and Joseph Tonien. A generalized attack on RSA type cryptosystems. *Theor. Comput. Sci.*, 704:74–81, 2017.

[BWK93] Thomas Becker, Volker Weispfenning, and Heinz Kredel. *Gröbner bases - a computational approach to commutative algebra*, volume 141 of *Graduate texts in mathematics*. Springer, 1993.

[CHLS98] Thomas Collins, Dale Hopkins, Susan Langford, and Michael Sabin. Public key cryptographic apparatus and method, dec 1998. U.S. Patent 5848159.

[Cop96a] Don Coppersmith. Finding a small root of a bivariate integer equation; factoring with high bits known. In Ueli M. Maurer, editor, *Advances in Cryptology - EUROCRYPT '96, International Conference on the Theory*

and Application of Cryptographic Techniques, Saragossa, Spain, May 12-16, 1996, Proceeding, volume 1070 of *Lecture Notes in Computer Science*, pages 178–189. Springer, 1996.

[Cop96b] Don Coppersmith. Finding a small root of a univariate modular equation. In Ueli M. Maurer, editor, *Advances in Cryptology - EUROCRYPT '96, International Conference on the Theory and Application of Cryptographic Techniques, Saragossa, Spain, May 12-16, 1996, Proceeding*, volume 1070 of *Lecture Notes in Computer Science*, pages 155–165. Springer, 1996.

[Cop97] Don Coppersmith. Small solutions to polynomial equations, and low exponent RSA vulnerabilities. *J. Cryptol.*, 10(4):233–260, 1997.

[FNP24] Yansong Feng, Abderrahmane Nitaj, and Yanbin Pan. Partial prime factor exposure attacks on some RSA variants. *Theoretical Computer Science*, 999:114549, 2024.

[Hås85] Johan Håstad. On using RSA with low exponent in a public key network. In Hugh C. Williams, editor, *Advances in Cryptology - CRYPTO '85, Santa Barbara, California, USA, August 18-22, 1985, Proceedings*, volume 218 of *Lecture Notes in Computer Science*, pages 403–408. Springer, 1985.

[How97] Nick Howgrave-Graham. Finding small roots of univariate modular equations revisited. In Michael Darnell, editor, *Cryptography and Coding, 6th IMA International Conference, Cirencester, UK, December 17-19, 1997, Proceedings*, volume 1355 of *Lecture Notes in Computer Science*, pages 131–142. Springer, 1997.

[JM06] Ellen Jochemsz and Alexander May. A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants. In Xuejia Lai and Kefei Chen, editors, *Advances in Cryptology - ASIACRYPT 2006, 12th International Conference on the Theory and Application of Cryptology and Information Security, Shanghai, China, December 3-7, 2006, Proceedings*, volume 4284 of *Lecture Notes in Computer Science*, pages 267–282. Springer, 2006.

[Koy95] Kenji Koyama. Fast RSA-type schemes based on singular cubic curves $y^2 + axy = m^3 \pmod{n}$. In Louis C. Guillou and Jean-Jacques Quisquater, editors, *Advances in Cryptology - EUROCRYPT '95, International Conference on the Theory and Application of Cryptographic Techniques, Saint-Malo, France, May 21-25, 1995, Proceeding*, volume 921 of *Lecture Notes in Computer Science*, pages 329–340. Springer, 1995.

[Kun12] Noboru Kunihiro. On optimal bounds of small inverse problems and approximate GCD problems with higher degree. In Dieter Gollmann and Felix C. Freiling, editors, *Information Security - 15th International*

Conference, ISC 2012, Passau, Germany, September 19-21, 2012. Proceedings, volume 7483 of *Lecture Notes in Computer Science*, pages 55–69. Springer, 2012.

[LLL82] Arjen Klaas Lenstra, Hendrik Willem Lenstra, and László Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4):515–534, 1982.

[May03] Alexander May. *New RSA vulnerabilities using lattice reduction methods.* PhD thesis, University of Paderborn, 2003.

[May10] Alexander May. Using LLL-reduction for solving RSA and factorization problems. In Phong Q. Nguyen and Brigitte Vallée, editors, *The LLL Algorithm - Survey and Applications*, Information Security and Cryptography, pages 315–348. Springer, 2010.

[MS18] Nadir Murru and Francesco M. Saettone. A novel RSA-like cryptosystem based on a generalization of the Rédei rational functions. In Jerzy Kaczorowski, Josef Pieprzyk, and Jacek Pomykała, editors, *Number-Theoretic Methods in Cryptology, NuTMiC 2017*, volume 10737 of *Lecture Notes in Computer Science*, pages 91–103, Cham, 2018. Springer.

[NAA+22] Abderrahmane Nitaj, Muhammad Rezal Bin Kamel Ariffin, Nurul Nur Hanisah Adenan, Terry Shue Chien Lau, and Jiahui Chen. Security issues of novel RSA variant. *IEEE Access*, 10:53788–53796, 2022.

[NAAA21] Abderrahmane Nitaj, Muhammad Rezal Bin Kamel Ariffin, Nurul Nur Hanisah Adenan, and Nur Azman Abu. Classical attacks on a variant of the RSA cryptosystem. In Patrick Longa and Carla Ràfols, editors, *Progress in Cryptology - LATINCRYPT 2021 - 7th International Conference on Cryptology and Information Security in Latin America, Bogotá, Colombia, October 6-8, 2021, Proceedings*, volume 12912 of *Lecture Notes in Computer Science*, pages 151–167. Springer, 2021.

[NAB22] Dieaa I. Nassr, M. Anwar, and Hatem M. Bahig. Improving small private exponent attack on the Murru-Saettone cryptosystem. *Theor. Comput. Sci.*, 923:222–234, 2022.

[NPT18] Abderrahmane Nitaj, Yanbin Pan, and Joseph Tonien. A generalized attack on some variants of the RSA cryptosystem. In Carlos Cid and Michael J. Jacobson Jr., editors, *Selected Areas in Cryptography - SAC 2018 - 25th International Conference, Calgary, AB, Canada, August 15-17, 2018, Revised Selected Papers*, volume 11349 of *Lecture Notes in Computer Science*, pages 421–433. Springer, 2018.

[PT00] Sachar Paulus and Tsuyoshi Takagi. A new public-key cryptosystem over a quadratic order with quadratic decryption time. *J. Cryptol.*, 13(2):263–272, 2000.

[QC82] J.-J. Quisquater and C. Couvreur. Fast decipherment algorithm for RSA public-key cryptosystem. *Electronics Letters*, 18(21):905–907, 1982.

[RSA78] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, 1978.

[ST21] Willy Susilo and Joseph Tonien. A Wiener-type attack on an RSA-like cryptosystem constructed from cubic pell equations. *Theor. Comput. Sci.*, 885:125–130, 2021.

[Tak98] Tsuyoshi Takagi. Fast RSA-type cryptosystem modulo $p^k q$. In Hugo Krawczyk, editor, *Advances in Cryptology - CRYPTO '98, 18th Annual International Cryptology Conference, Santa Barbara, California, USA, August 23-27, 1998, Proceedings*, volume 1462 of *Lecture Notes in Computer Science*, pages 318–326. Springer, 1998.

[The23] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.3)*, 2023. `https://www.sagemath.org`.

[Wie90] Michael J. Wiener. Cryptanalysis of short RSA secret exponents. *IEEE Trans. Inf. Theory*, 36(3):553–558, 1990.

[ZKY21] Mengce Zheng, Noboru Kunihiro, and Yuanzhi Yao. Cryptanalysis of the RSA variant based on cubic Pell equation. *Theor. Comput. Sci.*, 889:135–144, 2021.