Generalized Cryptanalysis of Cubic Pell RSA

Mengce Zheng

Zhejiang Wanli University

joint work with Hao Kang

Inscrypt 2024, Kunming, China

December 15, 2024

Outline

1.1.1 BACKGROUND

Cubic Pell RSA

- A new RSA variant introduced by Murru and Saettone
- Based on cubic Pell equation $x^3 + ry^3 + r^2z^3 - 3rxyz = 1$
- Use a novel group with a non-standard product $\odot$ on tuple $(\star, \star)$

Key Information

- Public/private keys are $(N,\ e,\ r)$/$(d,\ p,\ q)$ with $N = pq$
- Ensure $ed \equiv 1 \pmod{\phi(N)}$ for $\phi(N) = (p^2 + p + 1)(q^2 + q + 1)$
- Key equation is $ed - k(p^2 + p + 1)(q^2 + q + 1) = 1$ for an unknown k

1.1.2 PUBLIC KEY CRYPTOSYSTEM

Key Generation

Select two prime numbers p, q and compute the modulus $N = pq$. Choose an integer e ($\approx N^{\beta}$) such that $\gcd(e, (p^2+p+1)(q^2+q+1)) = 1$ and compute d ($\approx N^{\delta}$) satisfying $ed \equiv 1 \pmod{(p^2+p+1)(q^2+q+1)}$.

Encryption

To encrypt two given plaintexts m_1 and m_2 in $\mathbb{Z}_N$, one uses the following encryption:

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

Decryption

To decrypt two given ciphertexts c_1 and c_2 in $\mathbb{Z}_N$, one uses the following decryption:

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

Previous Attacks

ST Attack

Susilo and Tonien[a] utilized the continued fraction-based method to show that for a given RSA modulus $N = pq$ with $q < p < \mu q$, if

$$\delta < \frac{1}{4} - \varepsilon,$$

where ε is a small positive constant related solely to μ, then the private key can be efficiently recovered.

[a] Susilo, W., Tonien, J.: A Wiener-type attack on an RSA-like cryptosystem constructed from cubic Pell equations. Theor. Comput. Sci. 885, 125–130 (2021).

1.1.4 Previous Attacks

NAAA Attack

Nitaj et al.[a] employed the continued fraction-based method to show 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

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

[a] Nitaj, A., Ariffin, M.R.B.K., Adenan, N.N.H., Abu, N.A.: Classical attacks on a variant of the RSA cryptosystem. LATINCRYPT 2021 - LNCS, vol. 12912, pp. 151–167. Springer (2021).

1.1.5 PREVIOUS ATTACKS

ZKY Attack

Zheng et al.[a] 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 Kunihiro's technique, further refining the bound to

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

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

1.1.6 Previous Attacks

NAALC Attack

Nitaj et al.[a] investigated attacks under small prime difference $|p - q| = N^{\alpha}$ and introduced two distinct attacks. One uses the continued fraction-based method, factoring the modulus $N = pq$ 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

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

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

1.1.7 PREVIOUS ATTACKS

NAB Attack

Nassr et al.[a] proposed three new 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

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

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

[a] Nassr, D.I., Anwar, M., Bahig, H.M.: Improving small private exponent attack on the Murru-Saettone cryptosystem. Theor. Comput. Sci. 923, 222–234 (2022).

1.1.8 Previous Attacks

FNP Attack

Feng et al.[a] used Kunihiro's technique to solve the modular equation. They proposed attacks under the condition that the most significant bits of p are known. Specifically, if

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

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

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

1.2.1 RESEARCH PROBLEM

Generalized Key Equation

From perspective of mathematical cryptanalysis and theoretical interest, we further examine the security by investigating the generalized key equation

$$eu - (p^2 + p + 1)(q^2 + q + 1)v = w.$$

This equation can be rewritten into a modular form:

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

Suppose $e = N^\beta$, $u = N^\delta$, and $|w| = N^\gamma$, we aim to derive a solving condition with $\beta,\ \delta,\ \gamma$ for factorization of $N = pq$.

1.2.2 Our Contribution

Generalized Lattice-Based Attack

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

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

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

2.1.1 Lattice-Based Solving Strategy

Lattice Concepts

The set of all integer linear combinations of linearly independent vectors.

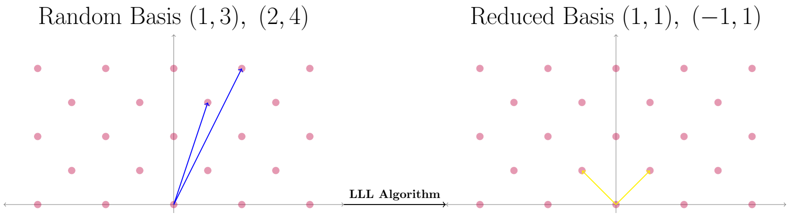
- Dimension: $\dim(\mathcal{L}) = \omega$
- Basis vectors: $\vec{b}_1, \ldots, \vec{b}_\omega$
- Basis matrix: $B = (b_{ij})_{\omega \times \omega}$
- Determinant: $\det(\mathcal{L}) = |\det(B)|$

$$\mathcal{L} = \mathbb{Z}\vec{b}_1 + \cdots + \mathbb{Z}\vec{b}_\omega = \left\{ \sum_{i=1}^{\omega} z_i \vec{b}_i \, : \, z_i \in \mathbb{Z}, \; \vec{b}_i \in \mathbb{R}^\omega \right\}$$

2.1.2 Lattice-Based Solving Strategy

Lattice Reduction

- Lenstra, Lenstra, and Lovász proposed the famous LLL algorithm
- Output approximately shortest reduced vectors in polynomial time
- Lattice-based solving strategy is applied in public key cryptanalysis



2.1.3 Lattice-Based Solving Strategy

Find Small Modular Roots Using Lattice Reduction

1. Construct shift polynomials with common root modulo $E = e^m$
2. Transform their coefficient vectors into a lattice basis matrix B
3. Calculate short reduced vectors from ω-dimensional lattice $\mathcal{L}(B)$
4. Transform output reduced vectors into integer equations system
5. Extract desired root over the integers using some simple methods

Asymptotic Solving Condition (LLL Lemma & HG Lemma)

$$2^{\frac{\omega(\omega-1)}{4(\omega-2)}} \det(\mathcal{L})^{\frac{1}{\omega-2}} < E/\sqrt{\omega} \implies \det(\mathcal{L}) < E^{\omega} \implies |\det(B)| < E^{\omega}$$

2.1.4 Target Equation

Trivariate Modular Equation

Using generalized key equation $eu - (p^2 + p + 1)(q^2 + q + 1)v = w$, we have

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

Consider the following trivariate polynomial

$$f(x, y, z) = xy^2 + axy + bx + z,$$

where $a = N + 1$ and $b = N^2 - N + 1$. Thus, $(x', y', z') = (v, p + q, w)$ is the modular root. We set the upper bounds to be

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

Detailed Attack

Monomial Sets

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

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

We can obtain an accurate description of i_1, i_2, i_3 for each $x^{i_1} y^{i_2} z^{i_3} \in M_k$:

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

Detailed Attack

Shift Polynomials

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

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

Furthermore, shift polynomials can be divided into two polynomial sets:

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

Detailed Attack

Coefficient Vectors

Coefficient vectors of $G_{k,i_1,i_2,i_3}(xX, yY, zZ)$ and $H_{k,i_1,i_2,i_3}(xX, yY, zZ)$, with X, Y, and Z denoting the upper bounds. In terms of row order, precedence is given to any $G_{k,i_1,i_2,i_3}(xX, yY, zZ)$ over any $H_{k,i_1,i_2,i_3}(xX, yY, zZ)$. 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 $i_3 < i'_3$.

The monomial order $\prec_{\mathrm{m}}$ is defined as $x^{i_1} y^{i_2} z^{i_3} \prec_{\mathrm{m}} x^{i'_1} y^{i'_2} z^{i'_3}$ in a similar way.

Detailed Attack

Integer Lattice

Regarding derived coefficient vectors as $\vec{b}_i$ for $i = 1, \ldots, \omega$ and construct

$$\mathcal{L} = \left\{ \sum_{i=1}^{\omega} z_i \vec{b}_i : z_i \in \mathbb{Z} \right\}.$$

The lattice dimension ω is calculated as

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

Detailed Attack

Toy Example

A toy example of the lattice basis matrix for $m = 2$ and $t = 0$ is shown.

	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

Detailed Attack

Lattice Determinant

A lower triangular basis matrix only requires multiplication of the diagonal terms for computing the determinant:

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

Letting $t = \tau m$ with a real $\tau \geq 0$ for simplicity, we obtain $\omega = (\tau + 1)m^2 + o(m^2)$ and

$$n_e = \frac{1}{6}(3\tau + 4)m^3 + o(m^3), \ n_X = \frac{1}{6}(3\tau + 4)m^3 + o(m^3),$$
$$n_Y = \frac{1}{6}\left(3\tau^2 + 6\tau + 4\right)m^3 + o(m^3), \ n_Z = \frac{1}{6}(3\tau + 2)m^3 + o(m^3).$$

Detailed Attack

Attack Bound

The solving condition $\det(\mathcal{L}) < E^{\omega}$ with $E = e^m$ yields

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

Simplify the exponents over N and obtain

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

By setting $\tau_0 = (2\sqrt{1+3\beta-3\gamma} - 4)/3$, it further leads to

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

2.3.1 EXPERIMENTAL RESULTS

Experiment Details

- Performed on a laptop computer running Ubuntu 22.04
- Conducted using `SageMath` mathematics software system
- Chose random parameters for generating a numerical instance
- Provided source code at `https://github.com/MengceZheng/GCPRSA`

```
Input given parameters of GCPRSA attack instance as follows:
Input N: 5503662094639832542248518981519204386875721417571215522872702572704379679659570816835779370372760735060519245011339626
0170171
Input e: 10578003884146132696993930345795908212610088212443443116131322083334835220854572592930841652745184949911092016662030067
52031456045032171612863063434022522609550692892561154763861484988711873034869148741612190479043963664788377209
Input g: 0.5
Input m: 4
Input t: 1
Found primes:
p = 9675024953610322475524445983470424120414751549937900903069192l3
q = 5688524960947094601900336476172097766845787422990129481808633 67
The attack costs 0.832 seconds...
```

2.3.2 Experimental Results

Numerical Example

Try $\gamma = 0.5$ and the attack bound then becomes $\delta < 0.352$. We set

$$
\begin{aligned}
X &= 2N^{\beta+\delta-2} = 2\left\lfloor N^{0.165} \right\rfloor = 125363993759672644 4032, \\
Y &= 3N^{\frac{1}{2}} = 3\left\lfloor N^{0.5} \right\rfloor \\
&= 22256001179852254406157203206163382029610351089090704027701739 52, \\
Z &= N^{\gamma} = \left\lfloor N^{0.5} \right\rfloor \\
&= 74186670599507517731985755126592353023044571789225304375531929 6.
\end{aligned}
$$

Use $m = 4$ and $t = 1$ to construct $\mathcal{L}$ with dimension $\omega = 40$ and recover $y' =$

$$153635499145574170774247824596425218872605389729280303848778258 0.$$

3. Conclusion

Improvements

- Provide new results using generalized key equation of cubic Pell RSA
- Achieve advanced attack effect even if the private key d is much larger

Limitation

- Our proposed attack does not reach the best existing attack results

Future Work

- Explore further improvements using better lattice construction
- Extend generalized attack in cases like key exposure or multiple keys

Mengce Zheng

mengce.zheng@gmail.com

Inscrypt 2024, Kunming, China, December 15, 2024