A Novel Partial Key Exposure Attack on Common Prime RSA

Mengce Zheng, Abderrahmane Nitaj

ZWU; UNICAEN, CNRS, LMNO

Africacrypt 2025, Rabat, Morocco

July 22, 2025

Outline

1.1 Common Prime RSA

Common Prime RSA

- Primes p and q share a special structure: $p = 2ga + 1$, $q = 2gb + 1$, where g is a common prime, and a, b are coprime positive integers.
- Modulus $N = pq$, public exponent e, and private exponent d.
- Key generation: $ed \equiv 1 \bmod \lambda(N)$ for $\lambda(N) = \text{lcm}(p-1, q-1) = 2gab$.

The Key Equation

The key generation equation can be written as:

$$ed = 2gabk + 1$$

where k is an unknown positive integer. This is the foundation of attacks.

Partial Key Exposure Attack

Partial Key Exposure Attack (PKEA)

The attacker manages to obtain a fraction of the bits of the private key d.

- **Source**: Side-channel attacks (e.g., power analysis, cold boot attacks).
- **Goal**: Use this partial information to recover the full private key or factor the modulus N in polynomial time.

Existing Research

- PKEA on standard RSA is well studied (see BDF'98, BM'03, TK'19 etc.).
- Research on PKEA for Common Prime RSA is scarce, worthy exploring.
- The first PKEA on Common Prime RSA was presented with limitations.

1.3 Related Work & Our Contributions

Previous Attack (Zheng'24)

- First partial key exposure attack on Common Prime RSA.
- Based on solving two simultaneous modular univariate equations.
- **Main Limitation:** The attack is only effective when $g \simeq N^{\gamma}$ for $\gamma \geq 1/4$.

Summary of Contributions

- **Unified Model:** We propose a generic attack model that handles MSB, LSB, and MSB-LSB leakages uniformly.
- **Extended Range:** Our attack can work for any $\gamma < 1/2$, covering the previously unaddressed case of $\gamma < 1/4$.
- **Improved Bound:** We derive a new, unified, stronger attack condition.

2.1 LATTICES

Lattice Basics

A lattice Λ is a set of points formed by all integer linear combinations of a set of linearly independent basis vectors $\vec{b}_1, \ldots, \vec{b}_\omega$.

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

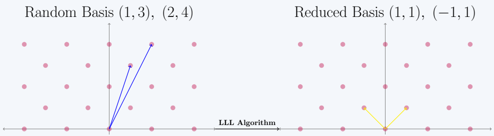
Relevant involved notations are as follows:

- Dimension: $\dim(\Lambda) = \omega$.
- Basis matrix: $B = (b_{ij})_{\omega \times \omega}$.
- Determinant: $\det(\Lambda) = |\det(B)|$.

Coppersmith's Method

Lattice Reduction (LLL Algorithm)

Find an approximately short basis for a given lattice in polynomial-time.



Howgrave-Graham's Lemma

If a polynomial has a small root modulo an integer R, and its coefficient vector is small enough, then this root is also a root over the integers.

$$g(\mathbf{x}^\star) \equiv 0 \bmod R \quad \& \quad \|g(\mathbf{x}\mathbf{X})\| < R/\sqrt{\omega} \quad \Longrightarrow \quad g(\mathbf{x}^\star) = 0$$

2.3 Lattice-Based Attack Strategy

Attack Strategy

1. Transform the attack into finding a small root of a polynomial f.
2. Construct a lattice Λ whose basis is related to shift polynomials.
3. Use the LLL lattice reduction algorithm to find short vectors in Λ.
4. Derive new integer polynomials that share the same small root with f.
5. Solve the system of integer equations to recover the final desired root.

Asymptotic Solving Condition

$$2^{\frac{\omega(\omega-1)}{4(\omega+1-i)}} \det(\Lambda)^{\frac{1}{\omega+1-i}} < R/\sqrt{\omega} \quad \Longrightarrow \quad \det(\Lambda) < R^{\omega}$$

The Target Polynomial

1. **Starting Point:** Use the key equation $ed = 2gabk + 1$.
2. Substitute $p = 2ga + 1$ and $q = 2gb + 1$ to get:

$$ed - 1 = (p-1)bk \quad \text{and} \quad ed - 1 = (q-1)ak$$

3. Rearranging gives:

$$ed - 1 + bk = pbk \quad \text{and} \quad ed - 1 + ak = qak$$

4. Multiply the two equations and use $N = pq$:

$$(ed - 1 + bk)(ed - 1 + ak) = pbk \cdot qak = N \cdot ak \cdot bk$$

The Target Polynomial

5. **Partial Key Leakage:** Assume the private key $d(\simeq N^{\delta})$ is partially known, with an unknown part $\bar{d}$:

$$d = d_{\mathrm{M}} M + \bar{d} L + d_{\mathrm{L}}$$

6. **Defining Variables:** Let variables x, y, z denote three unknowns:

$$x \leftarrow \bar{d}, \quad y \leftarrow ak, \quad z \leftarrow bk$$

7. **Final Polynomial:** Substituting the expression for d and the variables, we obtain a trivariate integer polynomial equation $f(x, y, z) = 0$.

Goal

Find the small integer root $(x^{\star}, y^{\star}, z^{\star})$ of the derived polynomial $f(x, y, z)$.

The Target Polynomial

Trivariate Integer Polynomial

$$f(x,y,z) = a_1x^2 + a_2xy + a_3xz + a_4yz + a_5x + a_6y + a_7z + a_0$$

where $a_1 = e^2L^2$, $a_2 = a_3 = eL$, $a_4 = 1 - N$, $a_5 = 2e^2(d_{\mathrm{M}}M + d_{\mathrm{L}})L - 2eL$, $a_6 = a_7 = e(d_{\mathrm{M}}M + d_{\mathrm{L}}) - 1$, $a_0 = (e(d_{\mathrm{M}}M + d_{\mathrm{L}}) - 1)^2$ are all known values.

Bounds on the Unknowns

- $|x^\star| = |\bar{d}| \leq X = N^{\delta - \delta_M - \delta_L}$
- $|y^\star| = |ak| \leq Y = N^{\delta - \gamma + 1/2}$
- $|z^\star| = |bk| \leq Z = N^{\delta - \gamma + 1/2}$
- $U = \|f(xX, yY, zZ)\|_\infty = N^{2\delta - 2\gamma + 2}$

Attack Analysis

Lattice Construction

1. **Shift Polynomials:** Construct a set of shift polynomials $g_{[i,j,k]}(x, y, z)$ that all share the root $(x^\star, y^\star, z^\star)$. These are generated by shifts of $f(x, y, z)$ and multiples of an integer $R = UX^{2m-2+t}Y^{m-1}Z^{m-1}$.
2. **Lattice Construction:** Coefficient vectors of scaled shift polynomials $g_{[i,j,k]}(xX, yY, zZ)$ form the basis of a lattice Λ. The rows of the matrix B are the above scaled coefficient vectors. With a suitable monomial ordering, this matrix B can be made upper triangular.
3. **Lattice Determinant:** Because B is upper triangular, its determinant $\det(\Lambda) = |\det(B)|$ is the product of its diagonal entries. These are derived from the leading terms of scaled shift polynomials.

Attack Analysis

Solving Condition

1. **Lattice Determinant:** Compute the lattice determinant $\det(\Lambda)$. It is composed of X, Y, Z and R, U.
2. **Core Inequality:** Substitute the expressions into the solving condition $\det(\Lambda) < R^\omega$. After simplification, it leads to a core inequality:

$$X^{s_X} Y^{s_Y} Z^{s_Z} < U^{s_\uparrow}$$

   The exponents $s_X, s_Y, s_Z, s_\uparrow$ are sums related to integers m and t.
3. **Exponents Calculation:** Compute the asymptotic exponent sums for $m \to \infty$ and $t = \tau m$:

$$s_\uparrow = (1+\tau)m^3, \quad s_X = (7/3 + 3\tau + \tau^2)m^3, \quad s_Y = s_Z = (5/3 + 3\tau/2)m^3$$

Attack Analysis

Optimizing Inequality

1. **Logarithmic Form:** Plug estimates for X, Y, Z, U into the logarithmic form of the core inequality:

$$(\delta - \delta_{\mathrm{M}} - \delta_{\mathrm{L}}) \cdot s_X + (\delta - \gamma + 1/2) \cdot (s_Y + s_Z) < (2\delta - 2\gamma + 2) \cdot s_{\uparrow}$$

2. **Further Computation:** Substitute expressions for $s_X, s_Y, s_Z, s_{\uparrow}$ and simplify further, it leads to an inequality for δ in terms of τ:

$$\delta < \delta_{\mathrm{M}} + \delta_{\mathrm{L}} + \frac{8\eta + 2 + (6\eta + 3)\tau}{22 + 24\tau + 6\tau^2}$$

where $\eta = \gamma - \delta_{\mathrm{M}} - \delta_{\mathrm{L}}$.

3.7 Attack Analysis (4)

Attack Bound

1. **Bound Maximizing:** Optimize over the parameter $\tau \geq 0$ to maximize the bound, and obtain the final attack condition.
2. **Attack Implication:** The more bits are leaked ($\delta_{\mathrm{M}} + \delta_{\mathrm{L}}$), the larger the vulnerable private exponent size δ can be.

Main Theorem (Informal)

The attack succeeds in polynomial time if:

$$\begin{cases} \delta < \gamma + 1 - \sqrt{4\eta^2 + 20\eta + 13}/4, & \gamma \leq \delta_{\mathrm{M}} + \delta_{\mathrm{L}} + 3/10 \\ \delta < (4\gamma + 7\delta_{\mathrm{M}} + 7\delta_{\mathrm{L}} + 1)/11, & \gamma > \delta_{\mathrm{M}} + \delta_{\mathrm{L}} + 3/10 \end{cases}$$

4.1 Experimental Validation

Experiment Setup

- Implemented in SageMath on a laptop running Ubuntu 22.04.
- Source code given at `https://github.com/MengceZheng/CPRSA_PKEA`.

ℓ	γ	$\delta_{\mathrm{M}}\ell$	$\delta_{\mathrm{L}}\ell$	δ_t	δ_e	m	t	ω	Time (sec.)
1024	0.25	153	0	0.280	0.209	2	0	27	0.96
2048	0.17	200	0	0.219	0.145	2	0	27	2.39
4096	0.20	491	0	0.244	0.166	2	0	27	7.82
1024	0.30	0	225	0.344	0.272	3	1	80	182.25
2048	0.22	0	250	0.252	0.164	2	0	27	2.17
4096	0.25	0	655	0.287	0.211	2	0	27	7.43
1024	0.40	40	256	0.424	0.333	3	0	64	37.46
2048	0.35	280	150	0.353	0.225	2	0	27	2.15
4096	0.25	327	327	0.287	0.205	2	0	27	7.68

4.2 Experiment Observations

Summary of Observations

- The experimental results confirm our theoretical analysis and its main attack bounds.
- The attack is practical for realistic parameters, running in seconds or minutes even for 2048-bit and 4096-bit RSA moduli.
- The gap between experimental bound δ_e and theoretical bound δ_t is due to using small lattice dimensions for quick verification.
- The attack performance can be improved when increasing the lattice dimension with larger m, t and using faster LLL implementation.

4.3 A Concrete Example

Known Parameters

$\ell = 512,\ \gamma = 0.1,\ 79$-bit $d,\ 20$-bit MSBs, 25-bit LSBs, $m = 3,\ t = 1$

Attack Execution

- Set lattice parameters resulting in an 80-dimensional lattice.
- After about 56 seconds, we recovered the desired root $(x^\star, y^\star, z^\star)$.
- Computed $k = \gcd(y^\star, z^\star)$, a, b, and g leading to the factorization of N.

Result Comparison

Our successful attack for $\gamma = 0.1$ cannot be achieved by previous attacks.

5. Conclusion & Future Work

Conclusion

- More general partial key exposure attack on Common Prime RSA.
- Extend the range of prior work especially for small common primes g.
- Validate the practicality of our attack through numerical experiments.

Future Work

- Further optimize the solving strategy to achieve better attack bounds or more efficient attacks.
- Investigate other attack scenarios where the leaked bits are from the middle of the private exponent d.

Mengce Zheng

Africacrypt 2025, Rabat, Morocco, July 22, 2025

mengce.zheng@gmail.com