Improving RSA Cryptanalysis: Combining Continued Fractions and Coppersmith's Techniques

Mengce Zheng, Yansong Feng, Abderrahmane Nitaj, Yanbin Pan

ZWU; SKLMS, AMSS, CAS; UCAS; UNICAEN, CNRS, LMNO

ACISP 2025, Wollongong, Australia

July 14, 2025

Outline

1.1 RSA & Small Private Exponent

RSA Basics

- Public Key: (N, e), where $N = pq$ for large primes p, q.
- Private Key: d that satisfies the following key equation.
- Key Equation: $ed \equiv 1 \pmod{\phi(N)}$, where $\phi(N) = (p-1)(q-1)$.
- Equivalent Key Equation: $ed = k\phi(N) + 1$ for a positive integer k.

Why small private exponent?

- Using a small d can significantly speed up the decryption process.
- **Question:** How small is too small?

RSA & Small Private Exponent

A Brief Recall of Classic Attacks

- **Wiener's Attack (1990):** Uses Continued Fractions (CF).
  - Effective when $d < \frac{1}{3}N^{\frac{1}{4}} \approx N^{0.25}$.
- **Boneh-Durfee's Attack (1999):** Uses Lattices (Coppersmith's method).
  - Effective when $d < N^{1-\frac{\sqrt{2}}{2}} \approx N^{0.292}$.
  - This is the state-of-the-art bound.

The Research Problem

- Two main lines of attack: Continued Fractions vs. Lattices.
- **Question:** Build a stronger hybrid attack by integrating both methods?

1.3 Our Contribution

Summary of Contributions

- We propose an attack combining the CF method and Coppersmith's technique in a novel way.
- We use a crucial relation from the convergents of $\frac{e}{N}$ to build a more efficient lattice-based attack.
- We improve the attack bound for small private exponents, especially when some partial information is known.
- We establish an improved attack bound $d < N^{1-\frac{\alpha}{3}-\frac{\gamma}{2}}$, where α and γ are related to e and an approximation of $p+q$, respectively.

2.1 Continued Fractions (CF)

Convergents

Any rational number can be expressed as a continued fraction. Convergents are its best rational approximations.

- **Legendre's Theorem:** If $\left|\xi - \frac{a}{b}\right| < \frac{1}{2b^2}$, then $\frac{a}{b}$ is a convergent of ξ.
- Wiener's attack is based on this theorem, applied to $\frac{e}{N}$ with $\left|\frac{e}{N} - \frac{k}{d}\right|$.

A Crucial Observation

Let $\frac{p_{r-1}}{q_{r-1}}$ and $\frac{p_r}{q_r}$ be two consecutive convergents. Any integer solution (k, d) to $ed - k\phi(N) = 1$ can be expressed as:

$$k = u \cdot p_r + v \cdot p_{r-1}, \quad d = u \cdot q_r + v \cdot q_{r-1}$$

Lattice-Based Cryptanalysis

The General Problem

Find small integer roots of a polynomial equation modulo an integer M:

$$f(x_1, \ldots, x_\ell) \equiv 0 \pmod{M}$$

We want to find a small solution $(x_1^\star, \ldots, x_\ell^\star)$ where $|x_i^\star|$ are bounded.

High Level Perspective

Transform an algebraic problem into a geometric one: finding short vectors in a specially constructed lattice.

2.3 Lattice-Based Solving Strategy

How to find small modular roots using lattice reduction?

1. Construct shift polynomials sharing common root modulo R
2. Transform scaled coefficient vectors into 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

$$\det(\mathcal{L}) < R^{\omega} \quad \Longrightarrow \quad |\det(B)| < R^{\omega}$$

3.1 Our New Attack

Main Idea

1. **Start with the key equation:** Focus on $ed - k\phi(N) - 1 = 0$.
2. **Introduce partial information:** Assume we have an approximation S of $p+q$: $\phi(N) = N + 1 - (p+q) = N + 1 - (S + w)$, where $w = p + q - S$ is a small unknown value.
3. **Substitute the CF relation:** Replace k and d with crucial observation: $k = u \cdot p_r + v \cdot p_{r-1}$, and $d = u \cdot q_r + v \cdot q_{r-1}$, where u, v are small unknown integers.
4. **Goal:** Derive a modular equation with three small unknowns: w, u, v and recover them using Jochemsz-May lattice-based strategy.

3.2 Polynomial and Unknowns

The Modular Polynomial

We obtain $f(w,u,v) \equiv 0 \pmod{eq_r}$, where (w,u,v) is the small root we are looking for. The polynomial is of the form:

$$f(x,y,z) = xy + a_1xz + a_2y + a_3z + a_4$$

with $x^\star = w, y^\star = u, z^\star = v$. Here the coefficients a_i are known.

Bounds on the Unknowns

- $|w| < X = N^\gamma$ (from partial information S on $p+q$).
- $|u| < Y = N^\delta$ (one new parameter for our attack).
- $|v| < Z = N^\delta$ (another new parameter for our attack).

3.3 Main Result: Improved Bound

Our Main Result (Informal)

Let $e \approx N^{\alpha}$ and $|p+q-S| < N^{\gamma}$. Our attack can factor N if the private exponent $d \approx N^{\delta_0}$ satisfies

$$\delta_0 < 1 - \frac{1}{3}\alpha - \frac{1}{2}\gamma$$

How to read this bound?

The total bound δ_0 on the private key d is composed of two parts:

- The size of the convergents from the CF method: $q_r < N^{\frac{3}{4}-\frac{\alpha}{2}}$.
- The size of the unknowns u, v found by the lattice: $|u|, |v| < N^{\delta}$.

Main Result: Bound Comparison

Previous Bound (HM)

$$\delta_0 < 1 - \sqrt{\alpha\gamma}$$

Our New Bound

$$\delta_0 < 1 - \frac{1}{3}\alpha - \frac{1}{2}\gamma$$

When is our bound better?

- The difference $\Delta := \sqrt{\alpha\gamma} - (\frac{1}{3}\alpha + \frac{1}{2}\gamma) > 0$ when $\frac{6-3\sqrt{3}}{2}\gamma < \alpha < \frac{6+3\sqrt{3}}{2}\gamma$.
- For common attack cases where $\gamma \approx 0.5$, it becomes $0.201 < \alpha < 2.799$.

Numerical Comparison

Consider a numerical case for $\alpha = 1,\ \gamma = 0.4$. Previous bound is $d < N^{0.367}$ and our new one is $d < N^{0.466}$. This shows our theoretical improvement!

Applications: Primes Sharing MSBs

Attack Scenario and Implication

Suppose the most significant bits of p and q are the same, such that their difference is small: $|p - q| < N^{\beta}$. This gives us information about the sum $p + q$. Set $S = \lfloor 2\sqrt{N} \rfloor$ and derive a bound on $w = p + q - S$.

Result (MSBs)

Our attack framework applies and yields an improved bound:

$$\delta_0 < \frac{5}{4} - \frac{1}{3}\alpha - \beta$$

3.6 Applications: Primes Sharing LSBs

Attack Scenario and Implication

Suppose the least significant bits of p and q are the same, such that $p \equiv q \pmod{2^n}$, where $2^n = N^\beta$. This gives us a structured approximation for $p+q$, where we know $p + q \pmod{2^{2n}}$.

Result (LSBs)

Our attack framework again provides a better bound than previous works:

$$\delta_0 < \frac{3}{4} - \frac{1}{3}\alpha + \beta$$

4.1 Experimental Validation

Experiment Setup

- Implemented in SageMath on a standard desktop machine.
- Generated random RSA instances according to attack parameters.
- Source code given at `https://github.com/MengceZheng/RSA_CFL`.

$\log_2 N$	α	δ	γ	$\delta_0 = \log_N d$	ω	Time (sec.)
1024	0.999	0.051	0.426	0.301	158	59.4
1024	1.000	0.061	0.415	0.309	142	40.9
1024	0.998	0.072	0.393	0.319	126	26.9
1024	0.991	0.076	0.379	0.329	110	16.383
1024	0.998	0.101	0.361	0.350	180	236.091

4.2 A Concrete Example

Known Parameters

$$\log_2 N = 512, \quad \alpha \approx 1, \quad \delta \approx 0.07, \quad \gamma \approx 0.4$$

Attack Execution

- Set lattice parameters resulting in a 126-dimensional lattice.
- After about 8 seconds, we recovered the unknowns (w_0, u_0, v_0).
- Computed the sum $p + q = S + w_0$ leading to the factorization of N.

Result Comparison

Our $d \approx N^{0.317}$ is above $N^{0.292}$ and also slightly better than the HM bound.

5. Conclusion

Improvements

- New hybrid attack on RSA combining continued fractions and lattices.
- Improved theoretical bounds on vulnerable d with partial information.

Limitation

- Still a gap between our theoretical bounds and experimental results.

Future Work

- Suggest that the proposed attack might be further optimized.
- Explore the hidden structures could lead to even tighter bounds.

Mengce Zheng

ACISP 2025, Wollongong, Australia, July 14, 2025

mengce.zheng@gmail.com