

LATTICE CRYPTANALYSIS

A Review of Lattice Attacks Applied to Two Types of RSA Variants

Ramona Corbeanu · Faculty of Mathematics, University of Bucharest

George Teșeleanu · Simion Stoilow Institute of Mathematics, Romanian Academy

21 September 2026

Outline

1 Motivation

Two families of algebraic RSA generalizations

2 Lattice Preliminaries

Howgrave-Graham and LLL

3 Main Result

A theorem for solving $xP(y) + cz \equiv 0 \pmod{\beta}$

4 Applications to RSA Variants

Four partial-information attack scenarios

5 Conclusions

A unified attack framework

Two Families of RSA-like Variants

Remark

Classical RSA can be viewed as operating over $GF(p) \times GF(q)$, since

$$\mathbb{Z}_p \simeq GF(p)$$

$$\mathbb{Z}_q \simeq GF(q)$$

Type-A · Gaussian-Integer RSA

Encryption over the ring of Gaussian integers modulo N , $\mathbb{Z}_N[i]$ ($\mathbb{Z}_p[i] \simeq GF(p^2)$).

Group order:

$$\varphi(N) = (p^2 - 1)(q^2 - 1)$$

Broken by a Wiener-type attack, later extended by lattice methods to $d < N^{0.585}$.

Type-B · Cubic Pell RSA

Encryption over equivalence classes of polynomials in $GF(p^3) \times GF(q^3)$.

Group order:

$$\psi(N) = (p^2 + p + 1)(q^2 + q + 1)$$

Broken by a Wiener-type attack, later improved to $d < N^{0.585}$.

Type-A Construction

Let p be a prime and $n \geq 1$. Define $\mathbb{A}_n = \mathbb{Z}_p[t]/(t^n - r)$ (where $r \in \mathbb{Z}_p$ is picked so that the polynomial $t^n - r$ is irreducible), which is a cyclic group of order $\varphi_n(\mathbb{Z}_p) = p^n - 1$.

Scheme

Setup

p, q distinct primes, $N = pq$. Choose $r \in \mathbb{Z}_N$ so $t^n - r$ is irreducible over $\mathbb{Z}_p[t], \mathbb{Z}_q[t]$. Then

$$\mathbb{A}_n = \mathbb{Z}_N[t]/(t^n - r) \simeq \mathbb{Z}_p[t]/(t^n - r) \times \mathbb{Z}_q[t]/(t^n - r) = GF(p^n) \times GF(q^n)$$

is a cyclic group of order $\varphi_n(N) = (p^n - 1)(q^n - 1)$. Pick e with $\gcd(e, \varphi_n(N)) = 1$ and d such that $ed \equiv 1 \pmod{\varphi_n(N)}$.

Keys

$$pk = (n, N, r, e) \quad sk = (p, q, d)$$

Encrypt

$$m = (m_0, \dots, m_{n-1}) \mapsto m(t) = m_0 + \dots + m_{n-1}t^{n-1}, \quad c(t) \equiv [m(t)]^e \pmod{N}$$

Decrypt

$$m(t) \equiv [c(t)]^d \pmod{N}, \text{ reassemble } m = (m_0, \dots, m_{n-1})$$

Type-B Construction

Let $\mathbb{B}_n = \mathbb{A}_n^*/\mathbb{Z}_p^*$. An element $[a_0 + \cdots + t^{n-1}] \in \mathbb{B}_n$ is the orbit $\{\gamma a_0 + \cdots + \gamma t^{n-1} \mid \gamma \in \mathbb{Z}_p^*\}$. $\mathbb{B}_n$ is cyclic of order $\psi_n(\mathbb{Z}_p) = (p^n - 1)/(p - 1)$.

Scheme

Setup

p, q distinct primes, $N = pq$. Choose $r \in \mathbb{Z}_N$ so $t^n - r$ is irreducible over $\mathbb{Z}_p[t], \mathbb{Z}_q[t]$. Pick e with $\gcd(e, \psi_n(N)) = 1$ and d such that $ed \equiv 1 \pmod{\psi_n(N)}$, where $\psi_n(N) = (p^n - 1)(q^n - 1)/(p - 1)(q - 1)$

Keys

$pk = (n, N, r, e) \quad sk = (p, q, d)$

Encrypt

$m = (m_0, \dots, m_{n-2}) \mapsto m(t) = m_0 + \cdots + m_{n-2}t^{n-2} + t^{n-1}$,
 $c(t) \equiv [m(t)]^e \pmod{N}$

Decrypt

$m(t) \equiv [c(t)]^d \pmod{N}$, reassemble $m = (m_0, \dots, m_{n-2})$

Our Contributions

A polynomial-time lattice method for solving the equation

1

$$xP(y) + cz \equiv 0 \pmod{\beta},$$

where $P(y) \in \mathbb{Z}[y]$ is a monic polynomial, knowing that a solution (x_0, y_0, z_0) exists.

2

Applied uniformly to factor N for both Type-A and Type-B variants under **four** realistic attack scenarios: public key only, known approximation of p , shared LSBs of p, q , known LSBs of d .

3

Systematic comparison with previously published bounds.

Finding Small Roots: Howgrave-Graham

Theorem (Howgrave-Graham)

Let $f(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$ have at most ω monomials, $\alpha \in \mathbb{Z}$. If

- $f(y_1, \dots, y_n) \equiv 0 \pmod{\alpha}$ for some $|y_i| \leq X_i$,
- $\|f(y_1 X_1, \dots, y_n X_n)\| < \alpha / \sqrt{\omega}$,

then $f(y_1, \dots, y_n) = 0$ holds **over the integers**.

LLL Reduction

Theorem (LLL)

Let L be a lattice of dimension ω . In polynomial time, LLL outputs a reduced basis $(b_1, \dots, b_\omega)$ with

$$\|b_1\| \leq \dots \leq \|b_i\| \leq 2^{\frac{\omega(\omega-1)}{4(\omega+1-i)}} \det(L)^{\frac{1}{\omega+1-i}}.$$

Strategy

Build a lattice L whose short vectors correspond to polynomials vanishing modulo a power of β ; run LLL to find them.

Combined with Howgrave-Graham: $\det(L) \leq \varepsilon \alpha^{\omega+1-i}$

Main Theorem

Let $P(y) \in \mathbb{Z}[y]$ be monic of degree $r \geq 1$ and β an integer. Suppose $x_0 P(y_0) + cz_0 \equiv 0 \pmod{\beta}$ for some $|x_0| \leq X = \beta^\delta$, $|y_0| \leq Y = \beta^\gamma$, $|z_0| \leq Z = \beta^\lambda$, $|c| \leq C = \beta^\varepsilon$. Then one can solve $xP(y) + cz \equiv 0 \pmod{\beta}$ if:

Case 1: $CZ \leq XY^r$

$$0.5\lambda + \sqrt{r\gamma} < 1$$

$$\delta \leq 1 - 0.5\lambda - \sqrt{r\gamma}$$

Case 2: $CZ > XY^r$

$$2\lambda + \varepsilon < 1$$

$$\delta \leq 1 - 2\lambda - \varepsilon + \frac{(1 - 1.5\lambda - \varepsilon)^2}{r\gamma}$$

Improving Known Bounds

For $\lambda = 0$, we recover and strictly improve prior work:

Corollary

If $x_0 P(y_0) + c \equiv 0 \pmod{\beta}$ with $|x_0| < X = \beta^\delta$, $|y_0| < Y = \beta^\gamma$, $|c| \leq C < XY^r$, then one can solve $xP(y) + c \equiv 0 \pmod{\beta}$ when $\delta \leq 1 - \sqrt{r\gamma}$, $r\gamma \leq 1$.

vs. Kunihiro (ISC 2012)

Kunihiro's bound needed a piecewise split at $\gamma = r/(r+1)^2$:

$$\delta \leq \frac{r+2}{2(r+1)} - \frac{r+1}{2}\gamma.$$

Our bound strictly dominates it across the whole range.

Recovering Known Bounds

For $\varepsilon = 0$, we recover prior work of Rahmani–Nitaj–Ziane:

Corollary

If $x_0 P(y_0) + z_0 \equiv 0 \pmod{\beta}$ with $|x_0| < X = \beta^\delta$, $|y_0| < Y = \beta^\gamma$, $|z_0| < Z = \beta^\lambda < XY^r$, then one can solve $xP(y) + z \equiv 0 \pmod{\beta}$ when

$$\delta \leq 1 - 0.5\lambda - \sqrt{r\gamma}, 0.5\lambda + \sqrt{r\gamma} < 1.$$

For $r=1$ and $P(y)=y+b$, we recover prior work of Rahmani–Nitaj–Ziane:

Corollary

If $x_0 y_0 + b x_0 \equiv c z_0 \pmod{\beta}$ with $|x_0| < X = \beta^\delta$, $|y_0| < Y = \beta^\gamma$, $|z_0| < Z = \beta^\lambda < XY$, then one can solve $xy + bx \equiv cz \pmod{\beta}$ when

$$\delta \leq 1 - 0.5\lambda - \sqrt{\gamma}, 0.5\lambda + \gamma < 1.$$

Attack Scenarios

Applied to both Type-A ($\varphi_n(N)$) and Type-B ($\psi_n(N)$) variants, using

$$\begin{aligned}\varphi_n(N) &= -(p + q - M)^n + \sum_{k=0}^{n-1} a_k (p + q - M)^k \\ \psi_n(N) &= (p + q - M)^{n-1} + \sum_{j=0}^{n-2} b_j (p + q - M)^j\end{aligned}$$

1

No information

$$e \equiv z_0 u_0^{-1} \pmod{\varphi_n(N)}$$

2

Approximate p

$$\text{known } \tilde{p}, |p - \tilde{p}| \leq N^\lambda$$

3

Shared LSBs

p, q share s low bits

4

LSBs of d

$$d = d_1 \cdot 2^S + d_0 \text{ known}$$

Public Key Only

1 Let $e = N^\delta$, $e \equiv z_0 u_0^{-1} \pmod{\varphi_n(N)}$, $|u_0| \leq N^{\gamma_1}$, $|z_0| \leq N^{\gamma_2}$. Then N factors in polynomial time if

$$\begin{cases} \gamma_1 \leq n - 0.5\gamma_2 - \sqrt{0.5n\delta}, & \gamma_2 < \min(\delta + \gamma_1 - 0.5n, 2\delta - \sqrt{2n\delta}) \\ \gamma_1 \leq 0.5(n - \delta), & \delta + \gamma_1 - 0.5n < \gamma_2 < 0.5\delta \end{cases}$$

Direct secret-exponent version: with $|d| \leq N^\gamma$, $\gamma \leq n - \sqrt{0.5n\delta}$ (large δ), or $\gamma \leq 0.5n - \delta$ (small δ).

Recovers the bounds of Rahmani–Nitaj–Ziane and Teşeleanu as special cases. For $n=1, 2$ it recovers the optimal RSA / Gaussian-RSA bounds; for $n=3$ it recovers the Murru–Saettone bound $d < N^{0.585}$.

Known Approximation of p

2 Suppose $|p - \tilde{p}| \leq N^\lambda$, where $\tilde{p}$ is an approximation of p . Then $\tilde{q} = \lfloor N/\tilde{p} \rfloor$ approximates q , and $\varphi_n(N)$ becomes monic in $y = p + q - \tilde{p} - \tilde{q}$. Assuming that $e \equiv z_0 u_0^{-1} \bmod \varphi_n(N)$, where $|u_0| \leq N^{\gamma_1}$, $|z_0| \leq N^{\gamma_2}$ with $\gamma_2 \leq \delta + \gamma_1$, we obtain the bounds:

$$\begin{cases} \gamma_1 \leq n - 0.5\gamma_2 - \sqrt{n\lambda\delta} \\ \gamma_1 \leq n(1 - \lambda) - 0.5\delta \end{cases}$$

For $e \equiv d^{-1} \bmod \varphi_n(N)$: $\gamma \leq n - \sqrt{n\delta\lambda}$ or $\gamma \leq n(1 - \lambda) - \delta$

Comparison with related work: Simplifies and improves a bound of Teşeleanu (2025) via Kunihiro's technique, and improves bounds of Rahmani–Nitaj–Ziane.

Primes Sharing Least Significant Bits

3 Assume $p - q = 2^s t$ (share s LSBs), $2^s = N^\alpha$, $\alpha \in [0, 1/4)$. Then $p + q = v_1 \cdot 2^{2s} + v_0$ with v_0 computable and v_1 small: $|v_1| < 3N^{0.5-2\alpha}$.

$$\gamma_1 \leq n - 0.5\gamma_2 - \sqrt{\delta n(0.5 - 2\alpha)}$$

For $e \equiv d^{-1} \pmod{\varphi_n(N)}$: $\gamma \leq n - \sqrt{n\delta(0.5 - 2\alpha)}$

Comparison with related work: Recovers and simplifies a bound of Teşeleanu (2025); improves the bounds of Rahmani–Nitaj–Ziane for both φ_n and ψ_n .

Known LSBs of the Secret Exponent

- 4 Suppose $d = d_1 \cdot 2^s + d_0$ with s and $d_0 \geq 1$ known, $2^s = N^\alpha$, $E = e \cdot 2^s = N^{\delta+\alpha}$.

$$\gamma \leq \frac{7n}{6} + \alpha - \frac{1}{3}\sqrt{n^2 + 6n(\delta + \alpha)}$$

A CORRECTION TO PRIOR LITERATURE

G. Teşeleanu (2025) claimed a bound for this scenario via Kunihiro's method. We show its stated validity range is *never satisfiable* as it leads to a contradiction in both cases.

How the Attacks Fit Together

Scenario	Key equation	Tool
Public key only	$z_0 u_0^{-1} \equiv e \pmod{\varphi_n(N)}$	$c=1$
Approx. of p	same, shifted at $\tilde{p} + \tilde{q}$	$c=1$
Shared LSBs of p, q	same, shifted at v_0	$c = 2^{-2sn}$
Known LSBs of d	$-k\varphi_n(N) + ed_0 - 1 \equiv 0 \pmod{E}$	$z=0$

In every case: reduce to a monic polynomial equation in $y \approx p + q$ (or a shift thereof). Type-B proofs are structurally identical, replacing $\varphi_n(N)$ by $\psi_n(N)$ (degree $n-1$ instead of n).

Summary of Improvements

- 1 Unified framework: a single equation $xP(y)+cz \equiv 0 \pmod{\beta}$ and one theorem subsume previously separate lattice constructions.
- 2 Tighter or equal bounds in every comparable case.
- 3 Corrects a bound in the known-LSBs-of- d scenario from prior work.

Conclusions

1

Introduced a polynomial-time lattice algorithm for $xP(y)+cz \equiv 0 \pmod{\beta}$, generalizing prior small-root techniques.

2

Applied it uniformly to factor the modulus of Type-A and Type-B RSA-like cryptosystems under four realistic attack models.

3

Obtained bounds on the secret exponent d that match or improve every comparable result, and corrected one bound.

4

The approach is generic in n : instantiating $n=1,2,3$ recovers RSA, Elkamchouchi et al., and Murru–Saettone automatically.

Thank You!

Questions?

Ramona Corbeanu · George Teșeleanu