Exploring the parameter space in lattice attacks

Daniel J. Bernstein
Tanja Lange

Based on attack survey from 2019 Bernstein–Chuengsatiansup–Lange–van Vredendaal.

Some hard lattice meta-problems:

- Analyze cost of known attacks.
- Optimize attack parameters.
- Compare different attacks.
- Evaluate crypto parameters.
- Evaluate crypto designs.

`sntrup761` evaluations from "NTRU Prime: round 2" Table 2:

Ignoring cost of memory:

368	185	enum, ignoring hybrid
230	169	enum, including hybrid
153	139	sieving, ignoring hybrid
153	139	sieving, including hybrid

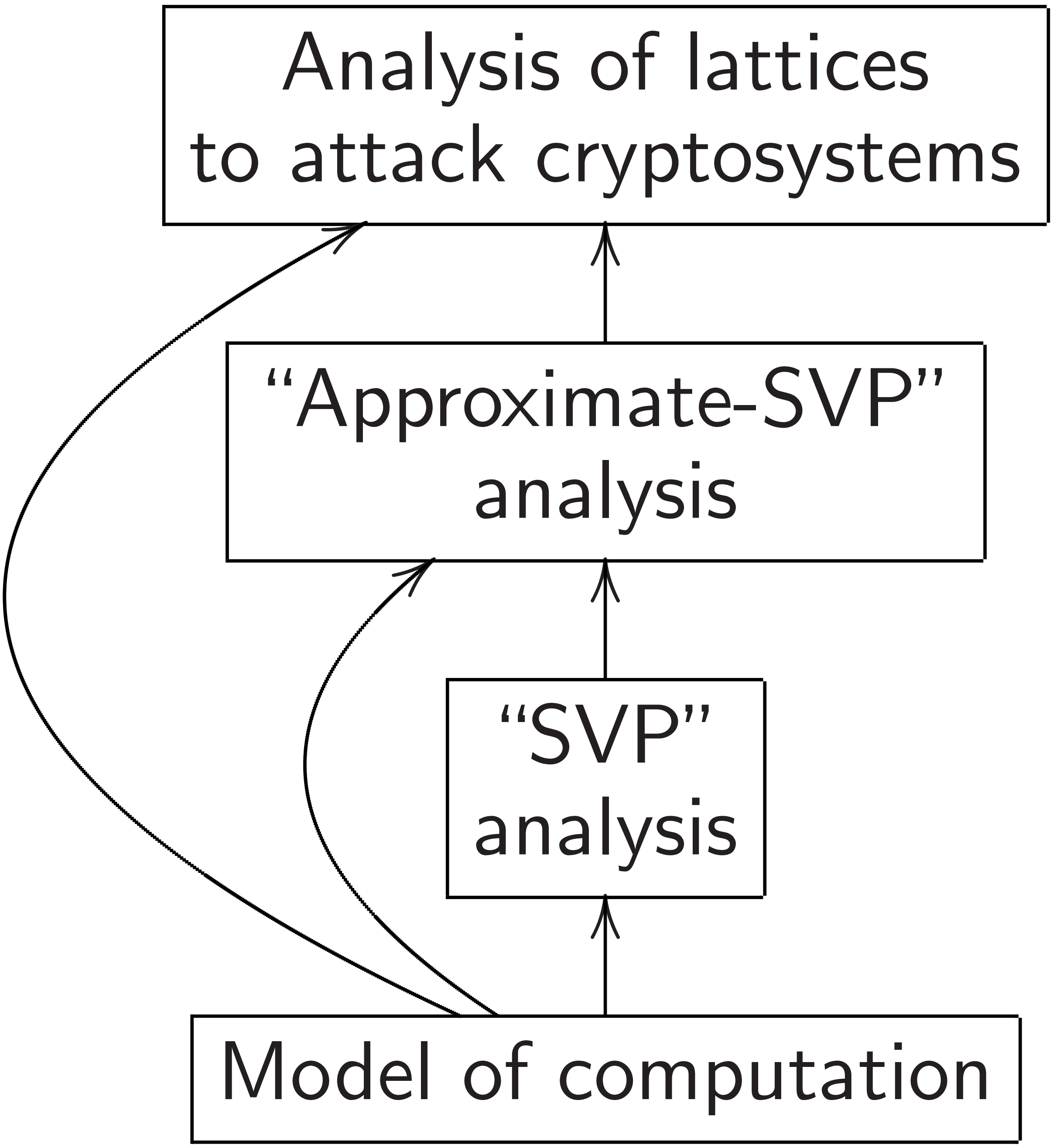
Accounting for cost of memory:

368	185	enum, ignoring hybrid
277	169	enum, including hybrid
208	208	sieving, ignoring hybrid
208	180	sieving, including hybrid

Security levels:

...	pre-quantum	
	...	post-quantum

Analysis of typical lattice attack has complications at four layers, and at interfaces between layers. This talk emphasizes top layer.



Three typical attack problems

Define $\mathcal{R} = \mathbf{Z}[x]/(x^{761} - x - 1)$;
"small" $=$ all coeffs in $\{-1, 0, 1\}$;
$w = 286$; $q = 4591$.

Attacker wants to find
small weight-w secret $a \in \mathcal{R}$.

Problem 1: Public $G \in \mathcal{R}/q$ with
$aG + e = 0$. Small secret $e \in \mathcal{R}$.

Problem 2: Public $G \in \mathcal{R}/q$ and
$aG + e = A$. Small secret $e \in \mathcal{R}$.

Problem 3: Public $G_1, G_2 \in \mathcal{R}/q$.
Public $aG_1 + e_1, aG_2 + e_2$.
Small secrets $e_1, e_2 \in \mathcal{R}$.

Examples of target cryptosystems

Secret key: small a; small e.

Public key reveals multiplier G and approximation $A = aG + e$.

Public key for “NTRU” (1996 Hoffstein–Pipher–Silverman): $G = -e/a$, and $A = 0$.

Examples of target cryptosystems

Secret key: small a; small e.

Public key reveals multiplier G and approximation $A = aG + e$.

Public key for "NTRU" (1996 Hoffstein–Pipher–Silverman): $G = -e/a$, and $A = 0$.

Public key for "Ring-LWE" (2010 Lyubashevsky–Peikert–Regev): random G, and $A = aG + e$.

Examples of target cryptosystems

Secret key: small a; small e.

Public key reveals multiplier G and approximation $A = aG + e$.

Public key for "NTRU" (1996 Hoffstein–Pipher–Silverman): $G = -e/a$, and $A = 0$.

Public key for "Ring-LWE" (2010 Lyubashevsky–Peikert–Regev): random G, and $A = aG + e$.

Recognize similarity + credits:
"NTRU" $\Rightarrow$ Quotient NTRU.
"Ring-LWE" $\Rightarrow$ Product NTRU.

Encryption for Quotient NTRU:

Input small b, small d.

Ciphertext: $B = 3bG + d$.

Encryption for Quotient NTRU:
Input small b, small d.
Ciphertext: $B = 3bG + d$.

Encryption for Product NTRU:
Input encoded message M.
Randomly generate
small b, small d, small c.
Ciphertext: $B = bG + d$
and $C = bA + M + c$.

Encryption for Quotient NTRU:
Input small b, small d.
Ciphertext: $B = 3bG + d$.

Encryption for Product NTRU:
Input encoded message M.
Randomly generate
small b, small d, small c.
Ciphertext: $B = bG + d$
and $C = bA + M + c$.

2019 Bernstein "Comparing proofs of security for lattice-based encryption" includes survey of G, a, e, c, M details and variants in NISTPQC submissions.

Lattices

Rewrite each problem as finding **short** nonzero solution to system of homogeneous $\mathcal{R}/q$ equations.

Problem 1: Find $(a, e) \in \mathcal{R}^2$ with $aG + e = 0$, given $G \in \mathcal{R}/q$.

Lattices

Rewrite each problem as finding **short** nonzero solution to system of homogeneous $\mathcal{R}/q$ equations.

Problem 1: Find $(a, e) \in \mathcal{R}^2$ with $aG + e = 0$, given $G \in \mathcal{R}/q$.

Problem 2: Find $(a, t, e) \in \mathcal{R}^3$ with $aG + e = At$, given $G, A \in \mathcal{R}/q$.

Lattices

Rewrite each problem as finding **short** nonzero solution to system of homogeneous $\mathcal{R}/q$ equations.

Problem 1: Find $(a, e) \in \mathcal{R}^2$ with $aG + e = 0$, given $G \in \mathcal{R}/q$.

Problem 2: Find $(a, t, e) \in \mathcal{R}^3$ with $aG + e = At$, given $G, A \in \mathcal{R}/q$.

Problem 3: Find $(a, t_1, t_2, e_1, e_2) \in \mathcal{R}^5$ with $aG_1 + e_1 = A_1 t_1$, $aG_2 + e_2 = A_2 t_2$, given $G_1, A_1, G_2, A_2 \in \mathcal{R}/q$.

Recognize each solution space as a full-rank lattice:

Problem 1: Lattice is image of the map $(\overline{a}, \overline{r}) \mapsto (\overline{a}, q\overline{r} - \overline{a}G)$ from $\mathcal{R}^2$ to $\mathcal{R}^2$.

Recognize each solution space as a full-rank lattice:

Problem 1: Lattice is image of the map $(\overline{a}, \overline{r}) \mapsto (\overline{a}, q\overline{r} - \overline{a}G)$ from $\mathcal{R}^2$ to $\mathcal{R}^2$.

Problem 2: Lattice is image of the map $(\overline{a}, \overline{t}, \overline{r}) \mapsto (\overline{a}, \overline{t}, A\overline{t} + q\overline{r} - \overline{a}G)$.

Recognize each solution space as a full-rank lattice:

Problem 1: Lattice is image of the map $(\overline{a}, \overline{r}) \mapsto (\overline{a}, q\overline{r} - \overline{a}G)$ from $\mathcal{R}^2$ to $\mathcal{R}^2$.

Problem 2: Lattice is image of the map $(\overline{a}, \overline{t}, \overline{r}) \mapsto (\overline{a}, \overline{t}, A\overline{t} + q\overline{r} - \overline{a}G)$.

Problem 3: Lattice is image of the map $(\overline{a}, \overline{t_1}, \overline{t_2}, \overline{r_1}, \overline{r_2}) \mapsto (\overline{a}, \overline{t_1}, \overline{t_2}, A_1\overline{t_1} + q\overline{r_1} - \overline{a}G_1, A_2\overline{t_2} + q\overline{r_2} - \overline{a}G_2)$.

Module structure

Each of these lattices is an $\mathcal{R}$-module, and thus has, generically, many independent short vectors.

Module structure

Each of these lattices is an $\mathcal{R}$-module, and thus has, generically, many independent short vectors.

e.g. in Problem 2:
Lattice has short (a, t, e).
Lattice has short (xa, xt, xe).
Lattice has short (x^2a, x^2t, x^2e).
etc.

Module structure

Each of these lattices is an $\mathcal{R}$-module, and thus has, generically, many independent short vectors.

e.g. in Problem 2:
Lattice has short (a, t, e).
Lattice has short (xa, xt, xe).
Lattice has short (x^2a, x^2t, x^2e).
etc.

Many more lattice vectors are fairly short combinations of independent vectors:
e.g., $((x+1)a, (x+1)t, (x+1)e)$.

1999 May, for Problem 1: Force a stretch of coefficients of a to be 0. This reduces lattice rank, speeding up various attacks, despite lower success chance.

1999 May, for Problem 1: Force a stretch of coefficients of a to be 0. This reduces lattice rank, speeding up various attacks, despite lower success chance.

(Always a speedup? Seems to be a slowdown if q is very large: see 2016 Kirchner–Fouque.)

1999 May, for Problem 1: Force a stretch of coefficients of a to be 0. This reduces lattice rank, speeding up various attacks, despite lower success chance.

(Always a speedup? Seems to be a slowdown if q is very large: see 2016 Kirchner–Fouque.)

Other problems: same speedup. e.g. "Bai–Galbraith embedding" for Problem 2: Force $t \in \mathbf{Z}$; force a few coefficients of a to be 0.

(Slowdown if q is very large? Literature misses module option!)

Standard analysis for Problem 1

Uniform random small weight-w secret a has length $\sqrt{w} \approx 17$.

Standard analysis for Problem 1

Uniform random small weight-w secret a has length $\sqrt{w} \approx 17$.

Uniform random small secret e has length usually close to $\sqrt{1522/3} \approx 23$. (Impact of variations? Partial answer: 2020 Dachman-Soled–Ducas–Gong–Rossi. Is fixed weight safer?)

Standard analysis for Problem 1

Uniform random small weight-w secret a has length $\sqrt{w} \approx 17$.

Uniform random small secret e has length usually close to $\sqrt{1522/3} \approx 23$. (Impact of variations? Partial answer: 2020 Dachman-Soled–Ducas–Gong–Rossi. Is fixed weight safer?)

Lattice has rank $2 \cdot 761 = 1522$.
Attack parameter: $k = 13$.
Force k positions in a to be 0: restrict to sublattice of rank 1509.
Pr[a is in sublattice] $\approx 0.2\%$.

Attacker is just as happy to find another solution such as (xa, xe).

Attacker is just as happy to find another solution such as (xa, xe).

Standard analysis for, e.g., $\mathbf{Z}[x]/(x^{761} - 1)$: Each $(x^j a, x^j e)$ has chance $\approx$0.2% of being in sublattice. These 761 chances are independent. (No, they aren't; also, total Pr depends on attacker's choice of positions. See 2001 May–Silverman.)

Attacker is just as happy to find another solution such as (xa, xe).

Standard analysis for, e.g., $\mathbf{Z}[x]/(x^{761} - 1)$: Each $(x^j a, x^j e)$ has chance $\approx$0.2% of being in sublattice. These 761 chances are independent. (No, they aren't; also, total Pr depends on attacker's choice of positions. See 2001 May–Silverman.)

Ignore bigger solutions $(\alpha a, \alpha e)$. (How hard are these to find?)

Attacker is just as happy to find another solution such as (xa, xe).

Standard analysis for, e.g., $\mathbf{Z}[x]/(x^{761} - 1)$: Each $(x^j a, x^j e)$ has chance $\approx$0.2% of being in sublattice. These 761 chances are independent. (No, they aren't; also, total Pr depends on attacker's choice of positions. See 2001 May–Silverman.)

Ignore bigger solutions $(\alpha a, \alpha e)$. (How hard are these to find?)

Pretend this analysis applies to $\mathbf{Z}[x]/(x^{761} - x - 1)$. (It doesn't.)

Write equation $e = qr - aG$
as 761 equations on coefficients.

Write equation $e = qr - aG$
as 761 equations on coefficients.

Attack parameter: $m = 600$.

Ignore $761 - m = 161$ equations:
i.e., project e onto 600 positions.
(1999 May.) Sublattice rank
$d = 1509 - 161 = 1348$; det q^{600}.

Write equation $e = qr - aG$
as 761 equations on coefficients.

Attack parameter: $m = 600$.

Ignore $761 - m = 161$ equations:
i.e., project e onto 600 positions.
(1999 May.) Sublattice rank
$d = 1509 - 161 = 1348$; det q^{600}.

Attack parameter: $\lambda = 1.331876$.
Rescaling (1997 Coppersmith–Shamir): Assign weight λ to positions in a. Increases length of a to $\lambda\sqrt{w} \approx 23$; increases det to $\lambda^{748}q^{600}$. (Is this λ optimal? Interaction with e size variation?)

Cost-analysis challenges

Huge space of attack lattices.
For each of these lattices, try to figure out cost of (e.g.) BKZ-β and chance it finds short vector.

Cost-analysis challenges

Huge space of attack lattices.
For each of these lattices, try to figure out cost of (e.g.) BKZ-β and chance it finds short vector.

Accurate experiments are slow.
Need accurate fast estimates!

Cost-analysis challenges

Huge space of attack lattices.
For each of these lattices, try to figure out cost of (e.g.) BKZ-β and chance it finds short vector.

Accurate experiments are slow.
Need accurate fast estimates!
Efforts to simplify are error-prone; e.g. "conservative lower bound" $(3/2)^{\beta/2}$ on (pre-q) cost is broken for all sufficiently large sizes.

Cost-analysis challenges

Huge space of attack lattices.
For each of these lattices, try to figure out cost of (e.g.) BKZ-β and chance it finds short vector.

Accurate experiments are slow.
Need accurate fast estimates!
Efforts to simplify are error-prone; e.g. "conservative lower bound" $(3/2)^{\beta/2}$ on (pre-q) cost is broken for all sufficiently large sizes.

Hybrid attacks (2008 Howgrave-Graham, . . . , 2018 Wunderer): often faster; different analysis.