Challenges in evaluating costs of known lattice attacks

D. J. Bernstein

Textbook algorithm design:

1. Write down algorithm A.
2. Prove algorithm costs C.
3. Repeat, trying to minimize C.

Usual situation for hard problems: No proof of min C for known A.

Even worse for lattice attacks: Claims of min C for known A are piles of poorly justified guesses.

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

Ignoring hybrid attacks:

368	185	enum, free memory cost
368	185	enum, real memory cost
153	139	sieving, free memory cost
208	208	sieving, real memory cost

Including hybrid attacks:

230	169	enum, free memory cost
277	169	enum, real memory cost
153	139	sieving, free memory cost
208	180	sieving, real memory cost

Security levels:

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

Comments inside published script that computed these numbers:

```
# XXX UNDER: many underestimates and potential underestimates
# XXX OVER: many overestimates and potential overestimates
# XXX UNDER/OVER: misuse of asymptotics
# XXX UNDER/OVER: misuse of asymptotics
# XXX UNDER/OVER: misuse of asymptotics
# XXX UNDER/OVER: misuse of asymptotics
# XXX UNDER/OVER: misuse of asymptotics
# XXX UNDER: assumes instant QRAM
# XXX UNDER: 'free' options ignore cost of RAM
# XXX UNDER: experiments suggest delta is actually larger
# XXX OVER: but maybe delta crosses below this for large b
# XXX UNDER: incorrectly treats ntru prime as ntru classic
# XXX OVER: assumes rotating t to \Z is optimal
# XXX OVER: considers only equivalence by rotations
# XXX OVER: assumes independence across equivalence class
# XXX OVER: limited force search
# XXX OVER: limited m search
# XXX OVER: limited scale search
# XXX OVER/UNDER: assumes average g weight
# XXX OVER: limited block-size search
# XXX OVER: experiments say smaller sizes often work
# XXX OVER: assumes dual attack is non-competitive
# XXX OVER: limited scale search
# XXX OVER: assumes that forcing does not help with hybrid
# XXX OVER: limited m search in hybrid context
# XXX OVER: assumes even split is optimal
# XXX OVER: limited blocksize search
# XXX UNDER/OVER: takes average weights
# XXX UNDER/OVER: ignores anti-correlation with searched weight
# XXX UNDER/OVER: need more experimental evidence
# XXX OVER: limited imax search
# XXX UNDER: ignores cost of inner loop
# XXX OVER: limited imax search
# XXX UNDER: ignores cost of inner loop
# XXX OVER: limited imax search
# XXX UNDER: ignores cost of inner loop
# XXX UNDER: ignores collision probability
```

2019 Son "A note on parameter choices of Round5", illustrating one change inside part of one of the 35 issues listed in script:

". . . there is one significant optimization of Albrecht's dual attack, which was not reflected to Round5 parameter choices. By taking this into consideration, some parameter choices of Round5 cannot enjoy the claimed security level."

Goal: pre-quantum 128, 192, 256.
2019 Son says: 123, 183, 243.

The main 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 $s \in \mathcal{R}$.

The main 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 $s \in \mathcal{R}$.

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

The main 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 $s \in \mathcal{R}$.

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

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

The main 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 $s \in \mathcal{R}$.

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

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

Problem 3: Public $A_1, A_2 \in \mathcal{R}/q$.
Public $A_1 s + e_1, A_2 s + e_2$.
Small secrets $e_1, e_2 \in \mathcal{R}$.

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

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

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

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

Problem 2: Find $(s, t, e) \in \mathcal{R}^3$ with $As + e = bt$, given $A, b \in \mathcal{R}/q$.

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

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

Problem 2: Find $(s, t, e) \in \mathcal{R}^3$ with $As + e = bt$, given $A, b \in \mathcal{R}/q$.

Problem 3: Find $(s, t_1, t_2, e_1, e_2) \in \mathcal{R}^5$ with $A_1 s + e_1 = b_1 t_1$, $A_2 s + e_2 = b_2 t_2$, given $A_1, b_1, A_2, b_2 \in \mathcal{R}/q$.

Recognize each solution space as a full-rank lattice:

Problem 1: Find (s, e) in image of the map $(s, r) \mapsto (s, qr - As)$ from $\mathcal{R}^2$ to $\mathcal{R}^2$.

Recognize each solution space as a full-rank lattice:

Problem 1: Find (s, e) in image of the map $(s, r) \mapsto (s, qr - As)$ from $\mathcal{R}^2$ to $\mathcal{R}^2$.

Problem 2: Find (s, t, e) in image of the map $(s, t, r) \mapsto (s, t, bt + qr - As)$.

Recognize each solution space as a full-rank lattice:

Problem 1: Find (s, e) in image of the map $(s, r) \mapsto (s, qr - As)$ from $\mathcal{R}^2$ to $\mathcal{R}^2$.

Problem 2: Find (s, t, e) in image of the map $(s, t, r) \mapsto (s, t, bt + qr - As)$.

Problem 3: Find (s, t_1, t_2, e_1, e_2) in image of the map $(s, t_1, t_2, r_1, r_2) \mapsto (s, t_1, t_2, b_1 t_1 + qr_1 - A_1 s, b_2 t_2 + qr_2 - A_2 s)$.

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

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

Nonsense from 2017 Kirchner–Fouque: "there exist many short vectors" in Problem 1 lattices but not in Problem 2/3 lattices.

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

Nonsense from 2017 Kirchner–Fouque: "there exist many short vectors" in Problem 1 lattices but not in Problem 2/3 lattices.

$\Rightarrow$ Nonsense in NISTIR 8240: Problem 1 "produces a lattice that has somewhat more structure . . . due to having shorter than expected vectors".

2001 May–Silverman, for Problem 1: Force a few coefficients of s to be 0. This reduces lattice rank, speeding up various attacks, despite lower success chance.

2001 May–Silverman, for Problem 1: Force a few coefficients of s 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.)

2001 May–Silverman, for Problem 1: Force a few coefficients of s 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.)

Same speedup for Problem 2: Force many coefficients of (s, t) to be 0. Bai–Galbraith special case: Force $t = 1$, and force a few coefficients of s to be 0.

(Also slowdown if q is very large?)

Standard attack on Problem 1

Lattice has rank $2 \cdot 761 = 1522$.

Uniform random small weight-w secret s has length $\sqrt{286} \approx 17$.

Standard attack on Problem 1

Lattice has rank $2 \cdot 761 = 1522$.

Uniform random small weight-w secret s has length $\sqrt{286} \approx 17$.

Uniform random small secret e has length usually close to $\sqrt{1522/3} \approx 23$. (What if it's smaller? What if it's larger?)

Standard attack on Problem 1

Lattice has rank $2 \cdot 761 = 1522$.

Uniform random small weight-w secret s has length $\sqrt{286} \approx 17$.

Uniform random small secret e has length usually close to $\sqrt{1522/3} \approx 23$. (What if it's smaller? What if it's larger?)

Attack parameter: $k = 13$.

Force k positions in s to be 0: restrict to sublattice of rank 1509.

$\Pr[s \text{ is in sublattice}] \approx 0.2\%$.

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

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

Standard analysis for, e.g., $\mathbf{Z}[x]/(x^{761} - 1)$: Each $(x^j s, x^j e)$ has chance ≈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.)

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

Standard analysis for, e.g., $\mathbf{Z}[x]/(x^{761} - 1)$: Each $(x^j s, x^j e)$ has chance ≈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.)

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

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

Standard analysis for, e.g., $\mathbf{Z}[x]/(x^{761} - 1)$: Each $(x^j s, x^j e)$ has chance ≈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.)

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

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

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

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

Attack parameter: $m = 600$.

Ignore $761 - m = 161$ equations:
i.e., project e onto 600 positions.

Projected sublattice rank $d =$
$1509 - 161 = 1348$; det q^{600}.

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

Attack parameter: $m = 600$.

Ignore $761 - m = 161$ equations: i.e., project e onto 600 positions.

Projected sublattice rank $d = 1509 - 161 = 1348$; det q^{600}.

Attack parameter: $\lambda = 1.331876$.

Rescaling: Assign weight λ to positions in s. Increases length of s to $\lambda\sqrt{286} \approx 23$; increases det to $\lambda^{748} q^{600}$. (Is this λ optimal?)

Attack parameter: $\beta = 525$.

Use BKZ-β algorithm to reduce lattice basis. (What about alternatives to BKZ?)

Attack parameter: $\beta = 525$.

Use BKZ-β algorithm to reduce lattice basis. (What about alternatives to BKZ?)

Standard analysis of BKZ-β:

"Normally" finds nonzero vector of length $\delta^d (\det L)^{1/d}$ where $\delta = (\beta(\pi\beta)^{1/\beta}/(2\pi e))^{1/(2(\beta-1))}$.

Attack parameter: $\beta = 525$.

Use BKZ-β algorithm to reduce lattice basis. (What about alternatives to BKZ?)

Standard analysis of BKZ-β:

"Normally" finds nonzero vector of length $\delta^d (\det L)^{1/d}$ where $\delta = (\beta(\pi\beta)^{1/\beta}/(2\pi e))^{1/(2(\beta-1))}$.

(This δ formula is an *asymptotic* claim without claimed error bounds. Does not match experiments for specific d.)

Standard analysis, continued:

"Geometric-series assumption" holds. (What about deviations identified in 2018 experiments?)

Standard analysis, continued:

"Geometric-series assumption" holds. (What about deviations identified in 2018 experiments?)

BKZ-β finds unique (mod $\pm$) shortest nonzero vector $\Leftrightarrow$ length $\le \delta^{2\beta-d}(\det L)^{1/d}\sqrt{d/\beta}$. (What about deviations identified in 2017 experiments?)

Standard analysis, continued:

"Geometric-series assumption" holds. (What about deviations identified in 2018 experiments?)

BKZ-β finds unique (mod $\pm$) shortest nonzero vector $\Leftrightarrow$ length $\le \delta^{2\beta-d}(\det L)^{1/d}\sqrt{d/\beta}$. (What about deviations identified in 2017 experiments?)

Hence the attack finds (s, e), assuming forcing worked. If it didn't, retry. (Are these tries independent? Should they use new parameters? Grover?)

How long does BKZ-β take?

Standard answer: $2^{0.265\beta} =$
$2^{139.125}$ quantum operations.

How long does BKZ-β take?

Standard answer: $2^{0.265\beta} = 2^{139.125}$ quantum operations.

(Plugging $o(1) = 0$ into the $2^{(0.265+o(1))\beta}$ *asymptotic* does not match experiments. What's the actual performance? And what exactly is an "operation"?)

How long does BKZ-β take?

Standard answer: $2^{0.265\beta} = 2^{139.125}$ quantum operations.

(Plugging $o(1) = 0$ into the $2^{(0.265+o(1))\beta}$ *asymptotic* does not match experiments. What's the actual performance? And what exactly is an "operation"?)

Surprising fact: A reported 400$\times$ experimental speedup from a variant of this algorithm had zero effect on claimed security levels. Large parts of the speedup do *not* match underestimates in claims.

2019 Bernstein–Chuengsatiansup–Lange–van Vredendaal "NTRU Prime: round 2" Section 6: broader and more detailed survey of (1) how known lattice attacks work, including hybrid attacks, and (2) open questions regarding the performance of these attacks.

New lattice-analysis papers: 2019 Son (dual); 2019 Son–Cheon (hybrid); 2019 Albrecht–Curtis–Wunderer (hybrid); 2019 Albrecht–Gheorghiu–Postlethwaite–Schanck (sieving).