Challenges in evaluating costs of known lattice attacks

Daniel J. Bernstein
Tanja Lange

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

Why analysis is important:

- Guide attack optimization.
- Guide attack selection.
- Evaluate crypto parameters.
- Evaluate crypto designs.
- Advise users on security.

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
$aG + e$. 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": $G = -e/a$, 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": $G = -e/a$, and $A = 0$.

Public key for "Ring-LWE": 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": $G = -e/a$, and $A = 0$.

Public key for "Ring-LWE": random G, and $A = aG + e$.

Systematization of naming, recognizing similarity + credits:
"NTRU" $\Rightarrow$ Quotient NTRU.
"Ring-LWE" $\Rightarrow$ Product NTRU.

Encryption for Quotient NTRU:

Input small b, small d.

Ciphertext: $B = 3Gb + d$.

Encryption for Quotient NTRU:

Input small b, small d.

Ciphertext: $B = 3Gb + d$.

Encryption for Product NTRU:

Input encoded message M.

Randomly generate

small b, small d, small c.

Ciphertext: $B = Gb + d$

and $C = Ab + M + c$.

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

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

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

system	parameter set	type	set of multipliers
frodo	640	Product	$(\mathbf{Z}/32768)^{640\times 640}$
frodo	976	Product	$(\mathbf{Z}/65536)^{976\times 976}$
frodo	1344	Product	$(\mathbf{Z}/65536)^{1344\times 1344}$
kyber	512	Product	$((\mathbf{Z}/3329)[x]/(x^{256}+1))^{2\times 2}$
kyber	768	Product	$((\mathbf{Z}/3329)[x]/(x^{256}+1))^{3\times 3}$
kyber	1024	Product	$((\mathbf{Z}/3329)[x]/(x^{256}+1))^{4\times 4}$
lac	128	Product	$(\mathbf{Z}/251)[x]/(x^{512}+1)$
lac	192	Product	$(\mathbf{Z}/251)[x]/(x^{1024}+1)$
lac	256	Product	$(\mathbf{Z}/251)[x]/(x^{1024}+1)$
newhope	512	Product	$(\mathbf{Z}/12289)[x]/(x^{512}+1)$
newhope	1024	Product	$(\mathbf{Z}/12289)[x]/(x^{1024}+1)$
ntru	hps2048509	Quotient	$(\mathbf{Z}/2048)[x]/(x^{509}-1)$
ntru	hps2048677	Quotient	$(\mathbf{Z}/2048)[x]/(x^{677}-1)$
ntru	hps4096821	Quotient	$(\mathbf{Z}/4096)[x]/(x^{821}-1)$
ntru	hrss701	Quotient	$(\mathbf{Z}/8192)[x]/(x^{701}-1)$
ntrulpr	653	Product	$(\mathbf{Z}/4621)[x]/(x^{653}-x-1)$
ntrulpr	761	Product	$(\mathbf{Z}/4591)[x]/(x^{761}-x-1)$
ntrulpr	857	Product	$(\mathbf{Z}/5167)[x]/(x^{857}-x-1)$
round5n1	1	Product	$(\mathbf{Z}/4096)^{636\times 636}$
round5n1	3	Product	$(\mathbf{Z}/32768)^{876\times 876}$
round5n1	5	Product	$(\mathbf{Z}/32768)^{1217\times 1217}$
round5nd	1.0d	Product	$(\mathbf{Z}/8192)[x]/(x^{586}+\ldots+1)$
round5nd	3.0d	Product	$(\mathbf{Z}/4096)[x]/(x^{852}+\ldots+1)$
round5nd	5.0d	Product	$(\mathbf{Z}/8192)[x]/(x^{1170}+\ldots+1)$
round5nd	1.5d	Product	$(\mathbf{Z}/1024)[x]/(x^{509}-1)$
round5nd	3.5d	Product	$(\mathbf{Z}/4096)[x]/(x^{757}-1)$
round5nd	5.5d	Product	$(\mathbf{Z}/2048)[x]/(x^{947}-1)$
saber	light	Product	$((\mathbf{Z}/8192)[x]/(x^{256}+1))^{2\times 2}$
saber	main	Product	$((\mathbf{Z}/8192)[x]/(x^{256}+1))^{3\times 3}$
saber	fire	Product	$((\mathbf{Z}/8192)[x]/(x^{256}+1))^{4\times 4}$
sntrup	653	Quotient	$(\mathbf{Z}/4621)[x]/(x^{653}-x-1)$
sntrup	761	Quotient	$(\mathbf{Z}/4591)[x]/(x^{761}-x-1)$
sntrup	857	Quotient	$(\mathbf{Z}/5167)[x]/(x^{857}-x-1)$
threebears	baby	Product	$(\mathbf{Z}/(2^{3120}-2^{1560}-1))^{2\times 2}$
threebears	mama	Product	$(\mathbf{Z}/(2^{3120}-2^{1560}-1))^{3\times 3}$
threebears	papa	Product	$(\mathbf{Z}/(2^{3120}-2^{1560}-1))^{4\times 4}$

short element

$\mathbf{Z}^{640\times 8}$; $\{-12,\ldots,12\}$; Pr $1,4,17,\ldots$ (spec page 23)
$\mathbf{Z}^{976\times 8}$; $\{-10,\ldots,10\}$; Pr $1,6,29,\ldots$ (spec page 23)
$\mathbf{Z}^{1344\times 8}$; $\{-6,\ldots,6\}$; Pr $2,40,364,\ldots$ (spec page 23)
$(\mathbf{Z}[x]/(x^{256}+1))^2$; $\sum_{0\le i<4}\{-0.5,0.5\}$
$(\mathbf{Z}[x]/(x^{256}+1))^3$; $\sum_{0\le i<4}\{-0.5,0.5\}$
$(\mathbf{Z}[x]/(x^{256}+1))^4$; $\sum_{0\le i<4}\{-0.5,0.5\}$
$\mathbf{Z}[x]/(x^{512}+1)$; $\{-1,0,1\}$; Pr $1,2,1$; weight $128,128$
$\mathbf{Z}[x]/(x^{1024}+1)$; $\{-1,0,1\}$; Pr $1,6,1$; weight $128,128$
$\mathbf{Z}[x]/(x^{1024}+1)$; $\{-1,0,1\}$; Pr $1,2,1$; weight $256,256$
$\mathbf{Z}[x]/(x^{512}+1)$; $\sum_{0\le i<16}\{-0.5,0.5\}$
$\mathbf{Z}[x]/(x^{1024}+1)$; $\sum_{0\le i<16}\{-0.5,0.5\}$
$\mathbf{Z}[x]/(x^{509}-1)$; $\{-1,0,1\}$
$\mathbf{Z}[x]/(x^{677}-1)$; $\{-1,0,1\}$
$\mathbf{Z}[x]/(x^{821}-1)$; $\{-1,0,1\}$
$\mathbf{Z}[x]/(x^{701}-1)$; $\{-1,0,1\}$; key correlation ≥ 0
$\mathbf{Z}[x]/(x^{653}-x-1)$; $\{-1,0,1\}$; weight 252
$\mathbf{Z}[x]/(x^{761}-x-1)$; $\{-1,0,1\}$; weight 250
$\mathbf{Z}[x]/(x^{857}-x-1)$; $\{-1,0,1\}$; weight 281
$\mathbf{Z}^{636\times 8}$; $\{-1,0,1\}$; weight $57,57$
$\mathbf{Z}^{876\times 8}$; $\{-1,0,1\}$; weight $223,223$
$\mathbf{Z}^{1217\times 8}$; $\{-1,0,1\}$; weight $231,231$
$\mathbf{Z}[x]/(x^{586}+\ldots+1)$; $\{-1,0,1\}$; weight $91,91$
$\mathbf{Z}[x]/(x^{852}+\ldots+1)$; $\{-1,0,1\}$; weight $106,106$
$\mathbf{Z}[x]/(x^{1170}+\ldots+1)$; $\{-1,0,1\}$; weight $111,111$
$\mathbf{Z}[x]/(x^{509}-1)$; $\{-1,0,1\}$; weight $68,68$; ending 0
$\mathbf{Z}[x]/(x^{757}-1)$; $\{-1,0,1\}$; weight $121,121$; ending 0
$\mathbf{Z}[x]/(x^{947}-1)$; $\{-1,0,1\}$; weight $194,194$; ending 0
$(\mathbf{Z}[x]/(x^{256}+1))^2$; $\sum_{0\le i<10}\{-0.5,0.5\}$
$(\mathbf{Z}[x]/(x^{256}+1))^3$; $\sum_{0\le i<8}\{-0.5,0.5\}$
$(\mathbf{Z}[x]/(x^{256}+1))^4$; $\sum_{0\le i<6}\{-0.5,0.5\}$
$\mathbf{Z}[x]/(x^{653}-x-1)$; $\{-1,0,1\}$; weight 288
$\mathbf{Z}[x]/(x^{761}-x-1)$; $\{-1,0,1\}$; weight 286
$\mathbf{Z}[x]/(x^{857}-x-1)$; $\{-1,0,1\}$; weight 322
$\mathbf{Z}^2$; $\sum_{0\le i<312} 2^{10i}\{-2,-1,0,1,2\}$; Pr $1,32,62,32,1$; *
$\mathbf{Z}^3$; $\sum_{0\le i<312} 2^{10i}\{-1,0,1\}$; Pr $13,38,13$; *
$\mathbf{Z}^4$; $\sum_{0\le i<312} 2^{10i}\{-1,0,1\}$; Pr $5,22,5$; *

key offset (numerator or noise or rounding method)

$\mathbf{Z}^{640\times 8}$; $\{-12,\ldots,12\}$; Pr $1,4,17,\ldots$ (spec page 23)
$\mathbf{Z}^{976\times 8}$; $\{-10,\ldots,10\}$; Pr $1,6,29,\ldots$ (spec page 23)
$\mathbf{Z}^{1344\times 8}$; $\{-6,\ldots,6\}$; Pr $2,40,364,\ldots$ (spec page 23)
$(\mathbf{Z}[x]/(x^{256}+1))^2$; $\sum_{0\le i<4}\{-0.5,0.5\}$
$(\mathbf{Z}[x]/(x^{256}+1))^3$; $\sum_{0\le i<4}\{-0.5,0.5\}$
$(\mathbf{Z}[x]/(x^{256}+1))^4$; $\sum_{0\le i<4}\{-0.5,0.5\}$
$\mathbf{Z}[x]/(x^{512}+1)$; $\{-1,0,1\}$; Pr $1,2,1$; weight $128,128$
$\mathbf{Z}[x]/(x^{1024}+1)$; $\{-1,0,1\}$; Pr $1,6,1$; weight $128,128$
$\mathbf{Z}[x]/(x^{1024}+1)$; $\{-1,0,1\}$; Pr $1,2,1$; weight $256,256$
$\mathbf{Z}[x]/(x^{512}+1)$; $\sum_{0\le i<16}\{-0.5,0.5\}$
$\mathbf{Z}[x]/(x^{1024}+1)$; $\sum_{0\le i<16}\{-0.5,0.5\}$
$\mathbf{Z}[x]/(x^{509}-1)$; $\{-1,0,1\}$; weight $127,127$
$\mathbf{Z}[x]/(x^{677}-1)$; $\{-1,0,1\}$; weight $127,127$
$\mathbf{Z}[x]/(x^{821}-1)$; $\{-1,0,1\}$; weight $255,255$
$\mathbf{Z}[x]/(x^{701}-1)$; $\{-1,0,1\}$; key correlation ≥ 0; $\cdot(x-1)$
round $\{-2310,\ldots,2310\}$ to $3\mathbf{Z}$
round $\{-2295,\ldots,2295\}$ to $3\mathbf{Z}$
round $\{-2583,\ldots,2583\}$ to $3\mathbf{Z}$
round $\mathbf{Z}/4096$ to $8\mathbf{Z}$
round $\mathbf{Z}/32768$ to $16\mathbf{Z}$
round $\mathbf{Z}/32768$ to $8\mathbf{Z}$
round $\mathbf{Z}/8192$ to $16\mathbf{Z}$
round $\mathbf{Z}/4096$ to $8\mathbf{Z}$
round $\mathbf{Z}/8192$ to $16\mathbf{Z}$
reduce mod $x^{508}+\ldots+1$; round $\mathbf{Z}/1024$ to $8\mathbf{Z}$
reduce mod $x^{756}+\ldots+1$; round $\mathbf{Z}/4096$ to $16\mathbf{Z}$
reduce mod $x^{946}+\ldots+1$; round $\mathbf{Z}/2048$ to $8\mathbf{Z}$
round $\mathbf{Z}/8192$ to $8\mathbf{Z}$
round $\mathbf{Z}/8192$ to $8\mathbf{Z}$
round $\mathbf{Z}/8192$ to $8\mathbf{Z}$
$\mathbf{Z}[x]/(x^{653}-x-1)$; $\{-1,0,1\}$; invertible mod 3
$\mathbf{Z}[x]/(x^{761}-x-1)$; $\{-1,0,1\}$; invertible mod 3
$\mathbf{Z}[x]/(x^{857}-x-1)$; $\{-1,0,1\}$; invertible mod 3
$\mathbf{Z}^2$; $\sum_{0\le i<312} 2^{10i}\{-2,-1,0,1,2\}$; Pr $1,32,62,32,1$; *
$\mathbf{Z}^3$; $\sum_{0\le i<312} 2^{10i}\{-1,0,1\}$; Pr $13,38,13$; *
$\mathbf{Z}^4$; $\sum_{0\le i<312} 2^{10i}\{-1,0,1\}$; Pr $5,22,5$; *

ciphertext offset (noise or rounding method)

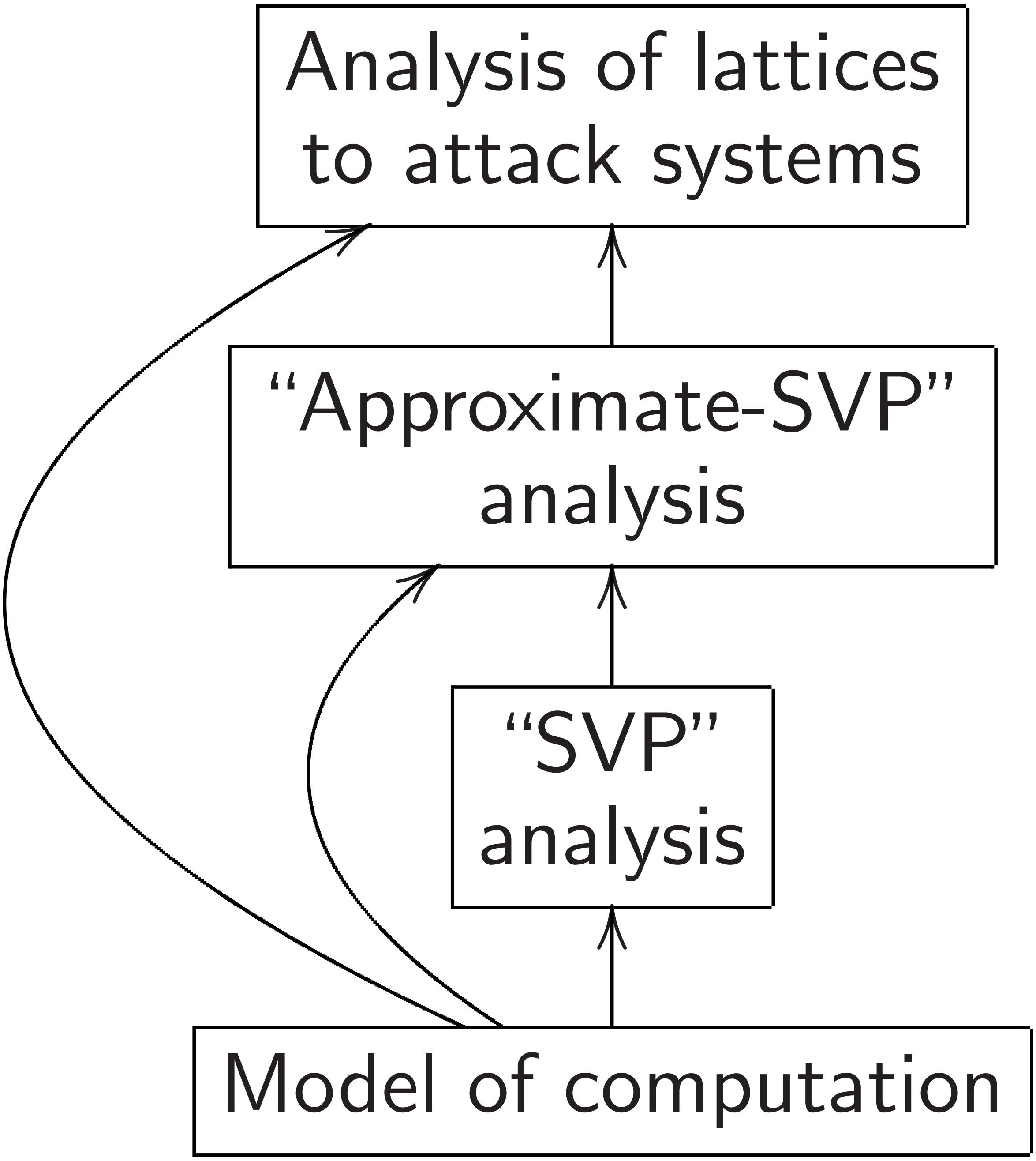
$\mathbf{Z}^{8\times 8}$; $\{-12,\dots,12\}$; Pr $1, 4, 17, \dots$ (spec page 23)
$\mathbf{Z}^{8\times 8}$; $\{-10,\dots,10\}$; Pr $1, 6, 29, \dots$ (spec page 23)
$\mathbf{Z}^{8\times 8}$; $\{-6,\dots,6\}$; Pr $2, 40, 364, \dots$ (spec page 23)
$\mathbf{Z}[x]/(x^{256}+1)$; $\sum_{0\le i<4}\{-0.5, 0.5\}$
$\mathbf{Z}[x]/(x^{256}+1)$; $\sum_{0\le i<4}\{-0.5, 0.5\}$
$\mathbf{Z}[x]/(x^{256}+1)$; $\sum_{0\le i<4}\{-0.5, 0.5\}$
$\mathbf{Z}[x]/(x^{512}+1)$; $\{-1, 0, 1\}$; Pr $1, 2, 1$
$\mathbf{Z}[x]/(x^{1024}+1)$; $\{-1, 0, 1\}$; Pr $1, 6, 1$
$\mathbf{Z}[x]/(x^{1024}+1)$; $\{-1, 0, 1\}$; Pr $1, 2, 1$
$\mathbf{Z}[x]/(x^{512}+1)$; $\sum_{0\le i<16}\{-0.5, 0.5\}$
$\mathbf{Z}[x]/(x^{1024}+1)$; $\sum_{0\le i<16}\{-0.5, 0.5\}$
not applicable
not applicable
not applicable
not applicable
bottom 256 coeffs; $z \mapsto \lfloor (114(z+2156)+16384)/32768 \rfloor$
bottom 256 coeffs; $z \mapsto \lfloor (113(z+2175)+16384)/32768 \rfloor$
bottom 256 coeffs; $z \mapsto \lfloor (101(z+2433)+16384)/32768 \rfloor$
round $\mathbf{Z}/4096$ to $64\mathbf{Z}$
round $\mathbf{Z}/32768$ to $512\mathbf{Z}$
round $\mathbf{Z}/32768$ to $64\mathbf{Z}$
bottom 128 coeffs; round $\mathbf{Z}/8192$ to $512\mathbf{Z}$
bottom 192 coeffs; round $\mathbf{Z}/4096$ to $128\mathbf{Z}$
bottom 256 coeffs; round $\mathbf{Z}/8192$ to $256\mathbf{Z}$
bottom 318 coeffs; round $\mathbf{Z}/1024$ to $64\mathbf{Z}$
bottom 410 coeffs; round $\mathbf{Z}/4096$ to $512\mathbf{Z}$
bottom 490 coeffs; round $\mathbf{Z}/2048$ to $64\mathbf{Z}$
round $\mathbf{Z}/8192$ to $1024\mathbf{Z}$
round $\mathbf{Z}/8192$ to $512\mathbf{Z}$
round $\mathbf{Z}/8192$ to $128\mathbf{Z}$
not applicable
not applicable
not applicable
$\mathbf{Z}$; $\sum_{0\le i<312} 2^{10i}\{-2, -1, 0, 1, 2\}$; Pr $1, 32, 62, 32, 1$; *
$\mathbf{Z}$; $\sum_{0\le i<312} 2^{10i}\{-1, 0, 1\}$; Pr $13, 38, 13$; *
$\mathbf{Z}$; $\sum_{0\le i<312} 2^{10i}\{-1, 0, 1\}$; Pr $5, 22, 5$; *

set of encoded messages
8×8 matrix over $\{0, 8192, 16384, 24576\}$
8×8 matrix over $\{0, 8192, \ldots, 57344\}$
8×8 matrix over $\{0, 4096, \ldots, 61440\}$
$\sum_{0 \le i < 256} \{0, 1665\} x^i$
$\sum_{0 \le i < 256} \{0, 1665\} x^i$
$\sum_{0 \le i < 256} \{0, 1665\} x^i$
256-dim subcode (see spec) of $\sum_{0 \le i < 512} \{0, 126\} x^i$
256-dim subcode (see spec) of $\sum_{0 \le i < 1024} \{0, 126\} x^i$
256-dim subcode (see spec) of $\sum_{0 \le i < 1024} \{0, 126\} x^i$
$\sum_{0 \le i < 256} \{0, 6145\} x^i (1 + x^{256})$
$\sum_{0 \le i < 256} \{0, 6145\} x^i (1 + x^{256} + x^{512} + x^{768})$
not applicable
not applicable
not applicable
not applicable
$\sum_{0 \le i < 256} \{0, 2310\} x^i$
$\sum_{0 \le i < 256} \{0, 2295\} x^i$
$\sum_{0 \le i < 256} \{0, 2583\} x^i$
8×8 matrix over $\{0, 1024, 2048, 3072\}$
8×8 matrix over $\{0, 4096, \ldots, 28672\}$
8×8 matrix over $\{0, 2048, \ldots, 30720\}$
$\sum_{0 \le i < 128} \{0, 4096\} x^i$
$\sum_{0 \le i < 192} \{0, 2048\} x^i$
$\sum_{0 \le i < 256} \{0, 4096\} x^i$
128-dim subcode (see spec) of $\sum_{0 \le i < 318} \{0, 512\} x^i$
192-dim subcode (see spec) of $\sum_{0 \le i < 410} \{0, 2048\} x^i$
256-dim subcode (see spec) of $\sum_{0 \le i < 490} \{0, 1024\} x^i$
$\sum_{0 \le i < 256} \{0, 4096\} x^i$
$\sum_{0 \le i < 256} \{0, 4096\} x^i$
$\sum_{0 \le i < 256} \{0, 4096\} x^i$
not applicable
not applicable
not applicable
256-dim subcode (see spec) of $\sum_{0 \le i < 274} \{0, 512\} 2^{10i}$
256-dim subcode (see spec) of $\sum_{0 \le i < 274} \{0, 512\} 2^{10i}$
256-dim subcode (see spec) of $\sum_{0 \le i < 274} \{0, 512\} 2^{10i}$

Attacking these problems

Attack strategy with reputation of usually being best: "primal" strategy. Focus of this talk.

Normal layers in analysis:



Models of computation

Multitape Turing machine: e.g., sort N ints, each $N^{o(1)}$ bits, in time $N^{1+o(1)}$, space $N^{1+o(1)}$.

Models of computation

Multitape Turing machine: e.g., sort N ints, each $N^{o(1)}$ bits, in time $N^{1+o(1)}$, space $N^{1+o(1)}$.

Brent–Kung 2D circuit model allows parallelism—e.g., sort in time $N^{0.5+o(1)}$, space $N^{1+o(1)}$.

Models of computation

Multitape Turing machine: e.g., sort N ints, each $N^{o(1)}$ bits, in time $N^{1+o(1)}$, space $N^{1+o(1)}$.

Brent–Kung 2D circuit model allows parallelism—e.g., sort in time $N^{0.5+o(1)}$, space $N^{1+o(1)}$.

PRAM: multiple inequivalent definitions, untethered to physical explanations. Sort in time $N^{o(1)}$.

Models of computation

Multitape Turing machine: e.g., sort N ints, each $N^{o(1)}$ bits, in time $N^{1+o(1)}$, space $N^{1+o(1)}$.

Brent–Kung 2D circuit model allows parallelism—e.g., sort in time $N^{0.5+o(1)}$, space $N^{1+o(1)}$.

PRAM: multiple inequivalent definitions, untethered to physical explanations. Sort in time $N^{o(1)}$.

Quantum computing:
similar divergence of models.

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., $((x+1)a, (x+1)t, (x+1)e)$.

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

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

Other problems: same speedup. e.g. Problem 2: Force many coefficients of (a, t) to be 0. Bai–Galbraith special case: Force $t = 1$, and force a few coefficients of a to be 0.

(Also slowdown if q is very large?)

Standard analysis for Problem 1

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

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

Standard analysis for Problem 1

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

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

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

Standard analysis for Problem 1

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

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

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

Attack parameter: $k = 13$.
Force k positions in a to be 0: restrict to sublattice of rank 1509.

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

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 ≈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 (xa, xe).

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

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.

Projected 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.

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

Attack parameter: $\lambda = 1.331876$.

Rescaling: 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?)

Lattice-basis reduction

Attack parameter: $\beta = 525$.

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

Lattice-basis reduction

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 $\delta = (\beta(\pi\beta)^{1/\beta}/(2\pi e))^{1/(2(\beta-1))}$.

Lattice-basis reduction

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 (a, 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: $2^{0.292\beta} = 2^{153.3}$ operations by "sieving".

How long does BKZ-β take?

Standard answer: $2^{0.292\beta} = 2^{153.3}$ operations by “sieving”.

(Plugging $o(1) = 0$ into the $2^{(0.292+o(1))\beta}$ *asymptotic* does not match experiments. What’s the actual performance? And what exactly is an “operation”?)

How long does BKZ-β take?

Standard answer: $2^{0.292\beta} = 2^{153.3}$ operations by "sieving".

(Plugging $o(1) = 0$ into the $2^{(0.292+o(1))\beta}$ *asymptotic* does not match experiments. What's the actual performance? And what exactly is an "operation"?)

0.292β (fake) cost for "sieving" is advertised as being below $0.187\beta \log_2 \beta - 1.019\beta + 16.1$ (questionable extrapolation of experiments) for "enumeration".

Note fragility of comparison.

$S \le 43 \Rightarrow E < S$ for
$S = 0.396\beta$, $E =$
$0.187\beta \log_2 \beta - 1.019\beta + 16.1$.

Note fragility of comparison.

$S \le 43 \Rightarrow E < S$ for
$S = 0.396\beta$, $E =$
$0.187\beta \log_2 \beta - 1.019\beta + 16.1$.

$S \le 225 \Rightarrow E < S$ for
$S = 0.369\beta$, $E =$
$(0.187\beta \log_2 \beta - 1.019\beta + 16.1)/2$.

Note fragility of comparison.

$S \le 43 \Rightarrow E < S$ for $S = 0.396\beta$, $E = 0.187\beta\log_2\beta - 1.019\beta + 16.1$.

$S \le 225 \Rightarrow E < S$ for $S = 0.369\beta$, $E = (0.187\beta\log_2\beta - 1.019\beta + 16.1)/2$.

$S \le 86 \Rightarrow E < S$ for $S = 0.265\beta$, $E = (0.125\beta\log_2\beta - 0.545\beta + 10)/2$.

Note fragility of comparison.

$S \le 43 \Rightarrow E < S$ for
$S = 0.396\beta$, $E =$
$0.187\beta \log_2 \beta - 1.019\beta + 16.1$.

$S \le 225 \Rightarrow E < S$ for
$S = 0.369\beta$, $E =$
$(0.187\beta \log_2 \beta - 1.019\beta + 16.1)/2$.

$S \le 86 \Rightarrow E < S$ for
$S = 0.265\beta$, $E =$
$(0.125\beta \log_2 \beta - 0.545\beta + 10)/2$.

Need to get analyses right!
First step: include models
that account for memory cost.

`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

Hybrid attacks

Extreme special case:

Search all small weight-w a.

Hybrid attacks

Extreme special case:
Search all small weight-w a.

Grover reduces cost to $\sqrt{\ }$.

Hybrid attacks

Extreme special case:
Search all small weight-w a.

Grover reduces cost to $\sqrt{\ }$.

Can also get "$\sqrt{\ }$" using memory without quantum computation.

Represent a as $a_1 + a_2$. (What is the optimal a_1, a_2 overlap?)
Look for approximate collision between $H_1(a_1)$ and $H_2(a_2)$.

Hybrid attacks

Extreme special case:
Search all small weight-w a.

Grover reduces cost to $\sqrt{}$.

Can also get "$\sqrt{}$" using memory without quantum computation.

Represent a as $a_1 + a_2$. (What is the optimal a_1, a_2 overlap?)
Look for approximate collision between $H_1(a_1)$ and $H_2(a_2)$.

e.g. Problem 1: aG small so $a_1G \approx -a_2G$. (How fast are near-neighbor algorithms?)

Seems worse than basis reduction for typical $\{a\}$.

Seems worse than basis reduction for typical $\{a\}$. But hybrid attack uses basis reduction *and* search; can beat basis reduction alone.

Seems worse than basis reduction for typical $\{a\}$. But hybrid attack uses basis reduction *and* search; can beat basis reduction alone.

Unified lattice description: $\{(u, uM + qr)\}$ given matrix M.

Seems worse than basis reduction for typical $\{a\}$. But hybrid attack uses basis reduction *and* search; can beat basis reduction alone.

Unified lattice description: $\{(u, uM + qr)\}$ given matrix M.

Relabel: $\{(v, w, vK + wL + qr)\}$. Attacker chooses subset of u indices to relabel as v.

Seems worse than basis reduction for typical $\{a\}$. But hybrid attack uses basis reduction *and* search; can beat basis reduction alone.

Unified lattice description: $\{(u, uM + qr)\}$ given matrix M.

Relabel: $\{(v, w, vK + wL + qr)\}$. Attacker chooses subset of u indices to relabel as v.

Use BKZ-β to find short B with $\{(w, wL + qr)\} = \{zB\}$.

Seems worse than basis reduction for typical $\{a\}$. But hybrid attack uses basis reduction *and* search; can beat basis reduction alone.

Unified lattice description: $\{(u, uM + qr)\}$ given matrix M.

Relabel: $\{(v, w, vK + wL + qr)\}$. Attacker chooses subset of u indices to relabel as v.

Use BKZ-β to find short B with $\{(w, wL + qr)\} = \{zB\}$.

Now $\{(v, w, vK + wL + qr)\}$ $= \{(v, v(0, K) + zB)\}$.

Search through many of the most likely choices of v.

Search through many of the most likely choices of v.

For each v: Quickly find z with $zB \approx -v(0, K)$. Check whether $(v, v(0, K) + zB)$ is short enough.

Search through many of the most likely choices of v.

For each v: Quickly find z with $zB \approx -v(0, K)$. Check whether $(v, v(0, K) + zB)$ is short enough.

Can again do quantum search, or approximate collision search.

Search through many of the most likely choices of v.

For each v: Quickly find z with $zB \approx -v(0, K)$. Check whether $(v, v(0, K) + zB)$ is short enough.

Can again do quantum search, or approximate collision search.

Can afford exponentially many z, maybe compensating for lower β.

Search through many of the most likely choices of v.

For each v: Quickly find z with $zB \approx -v(0, K)$. Check whether $(v, v(0, K) + zB)$ is short enough.

Can again do quantum search, or approximate collision search.

Can afford exponentially many z, maybe compensating for lower β.

Common claim: This saves time only for sufficiently narrow $\{a\}$. (Is this true, or a calculation error in existing algorithm analyses?)