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

g the parameter space
e attacks

. Bernstein
ange

n attack survey from
rnstein–Chuengsatiansup–
an Vredendaal.

ard lattice meta-problems:
ze cost of known attacks.
ize attack parameters.
are different attacks.
ate crypto parameters.
ate 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

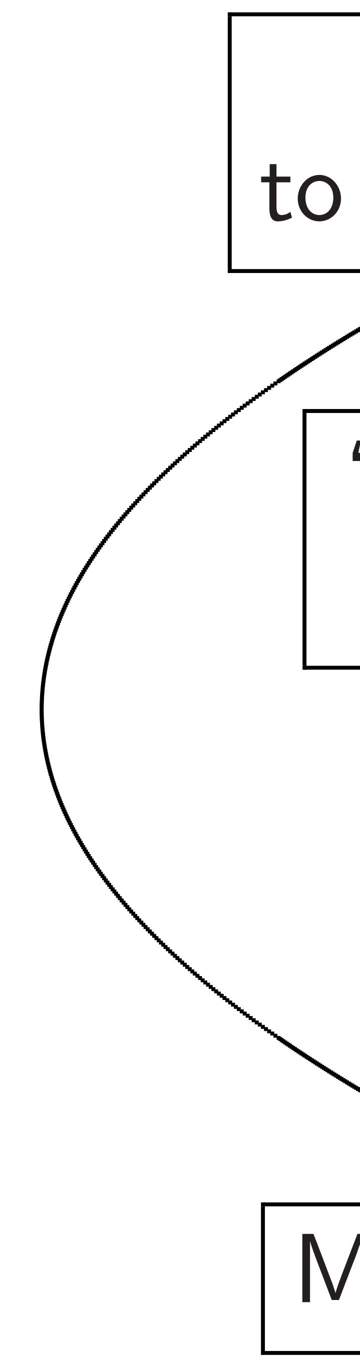
Accounting for cost of memory:

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
has com
and at i
This talk



meter space

n

urvey from

nuengsatiansup–

daal.

meta-problems:

known attacks.

parameters.

nt attacks.

parameters.

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

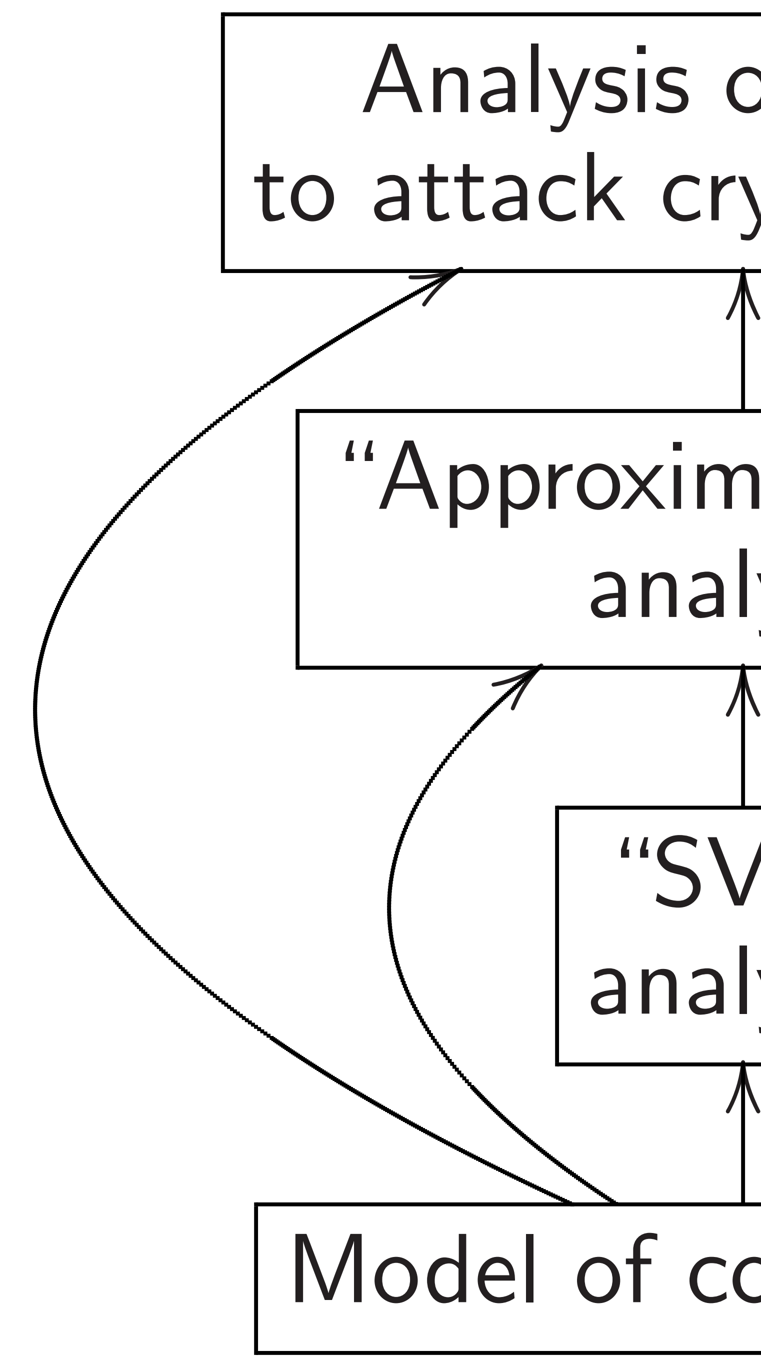
| . . . | post-quantum

Analysis of typical

has complications

and at interfaces b

This talk emphasiz



ce

n
nsup–

blems:
acks.
rs.
-
rs.

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

Ignoring cost of memory:

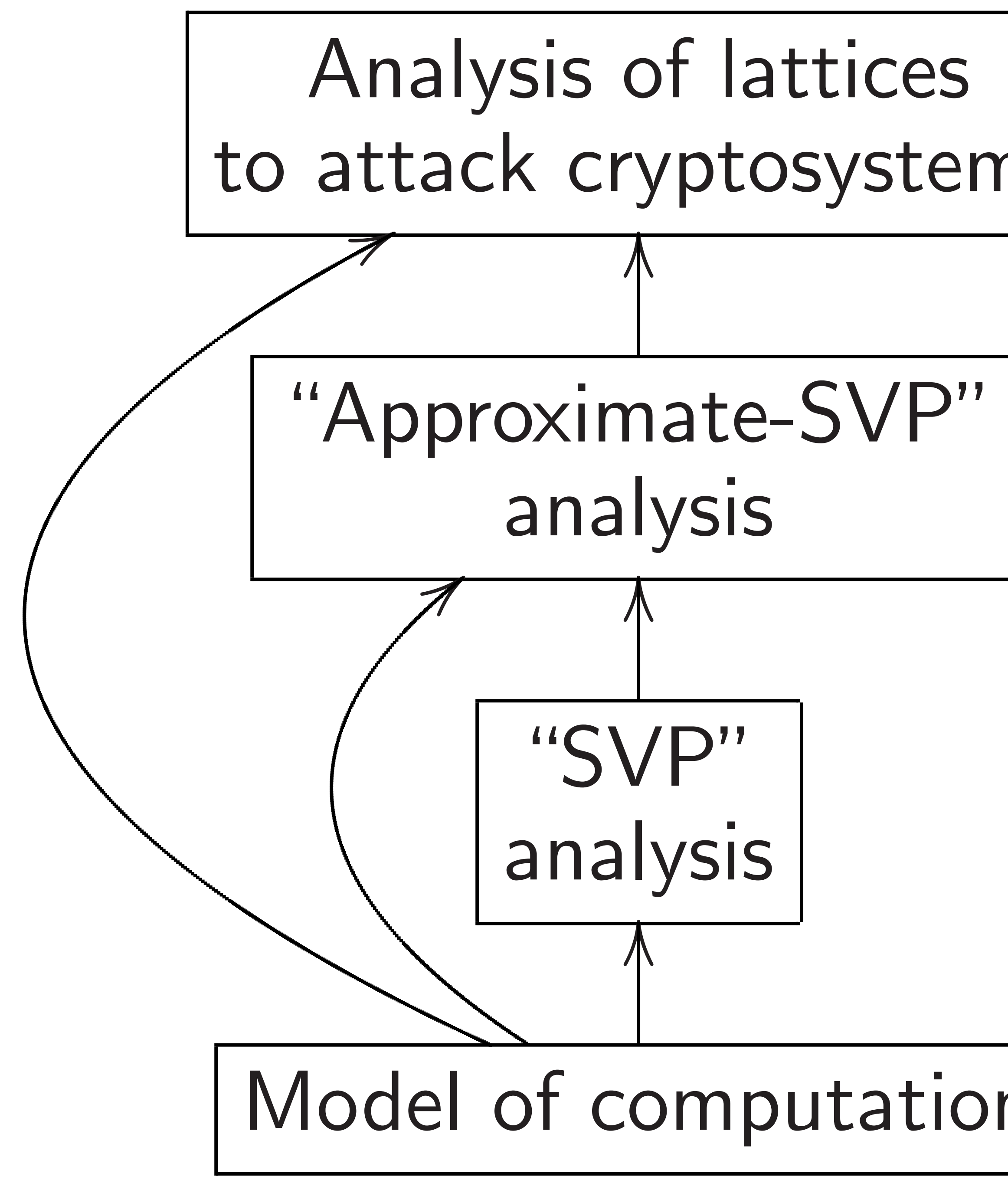
368	185	enum, ignoring hybrid
230	169	enum, including hybrid
153	139	sieving, ignoring hybrid
153	139	sieving, including hybrid

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 at
has complications at four lay
and at interfaces between la
This talk emphasizes top lay



`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:

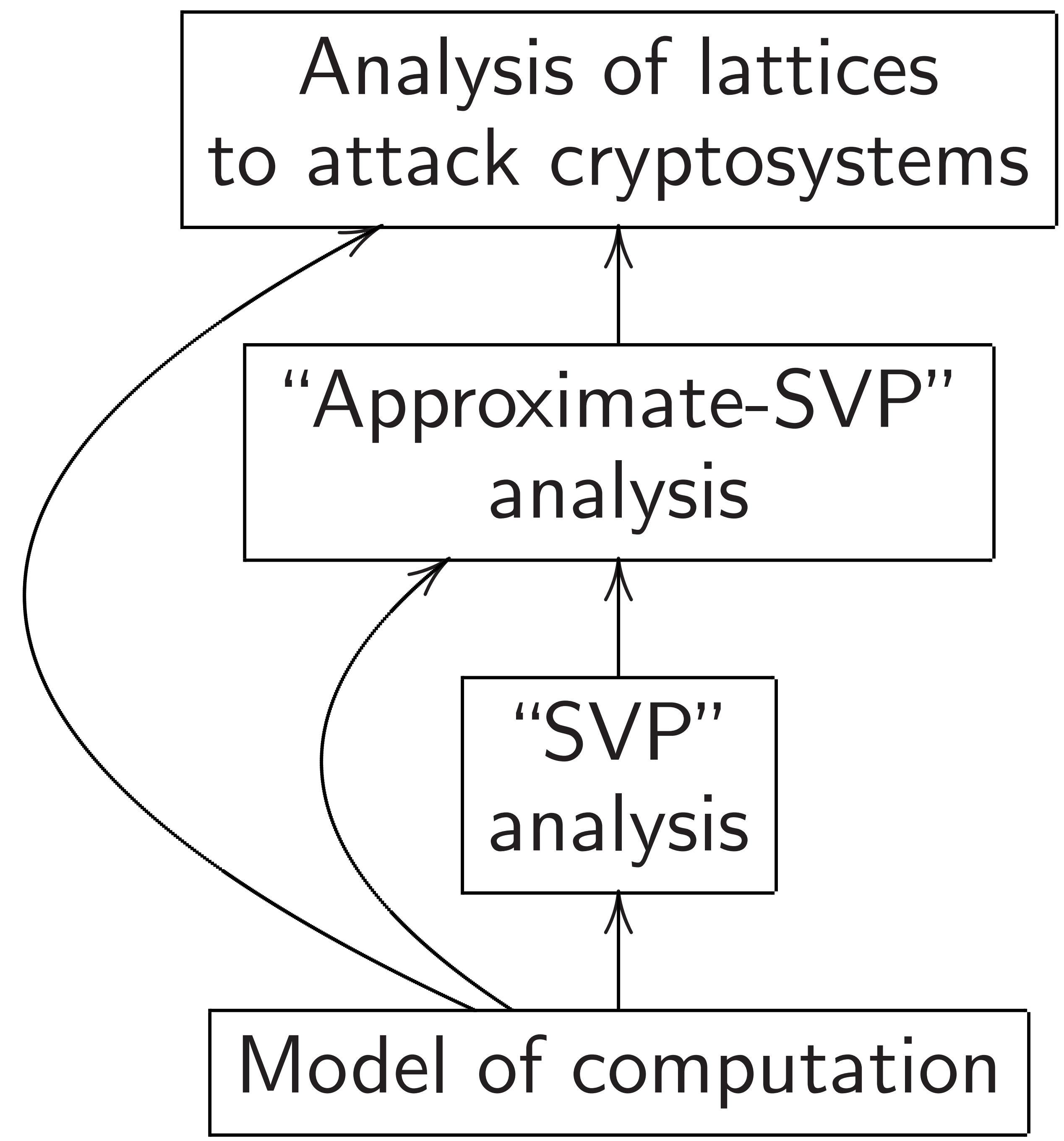
368	185	enum, ignoring hybrid
277	169	enum, including hybrid
208	208	sieving, ignoring hybrid
208	180	sieving, including hybrid

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.



761 evaluations from
Prime: round 2" Table 2:

cost of memory:

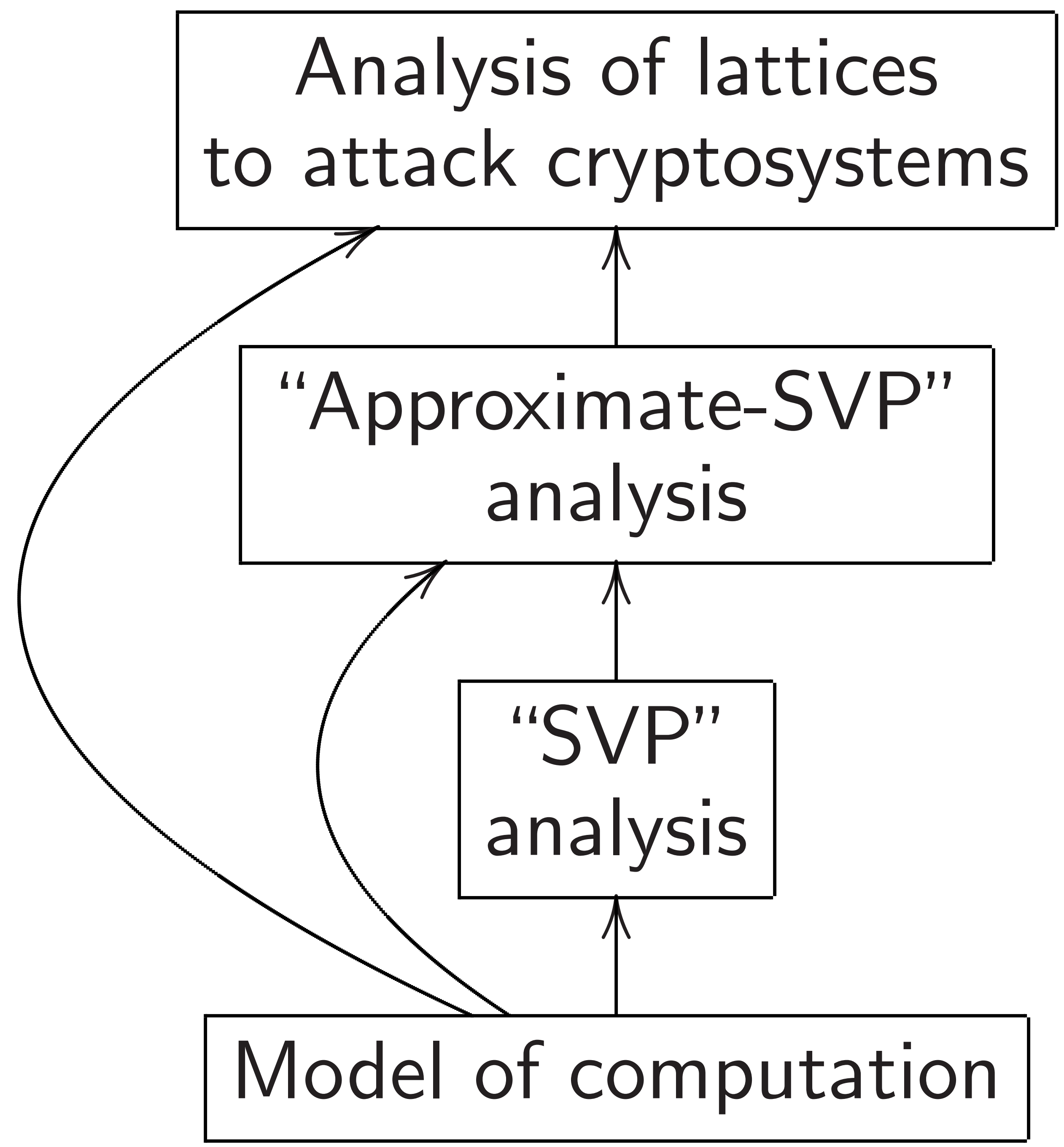
5	enum, ignoring hybrid
9	enum, including hybrid
9	sieving, ignoring hybrid
9	sieving, including hybrid

ing for cost of memory:

5	enum, ignoring hybrid
9	enum, including hybrid
8	sieving, ignoring hybrid
0	sieving, including hybrid

levels:
-quantum
post-quantum

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



Three ty

Define $\mathcal{R}$
"small"
$w = 286$

Attacker
small we

Problem
$aG + e =$

Problem
$aG + e =$

Problem
Public a
Small se

tions from
und 2" Table 2:

emory:

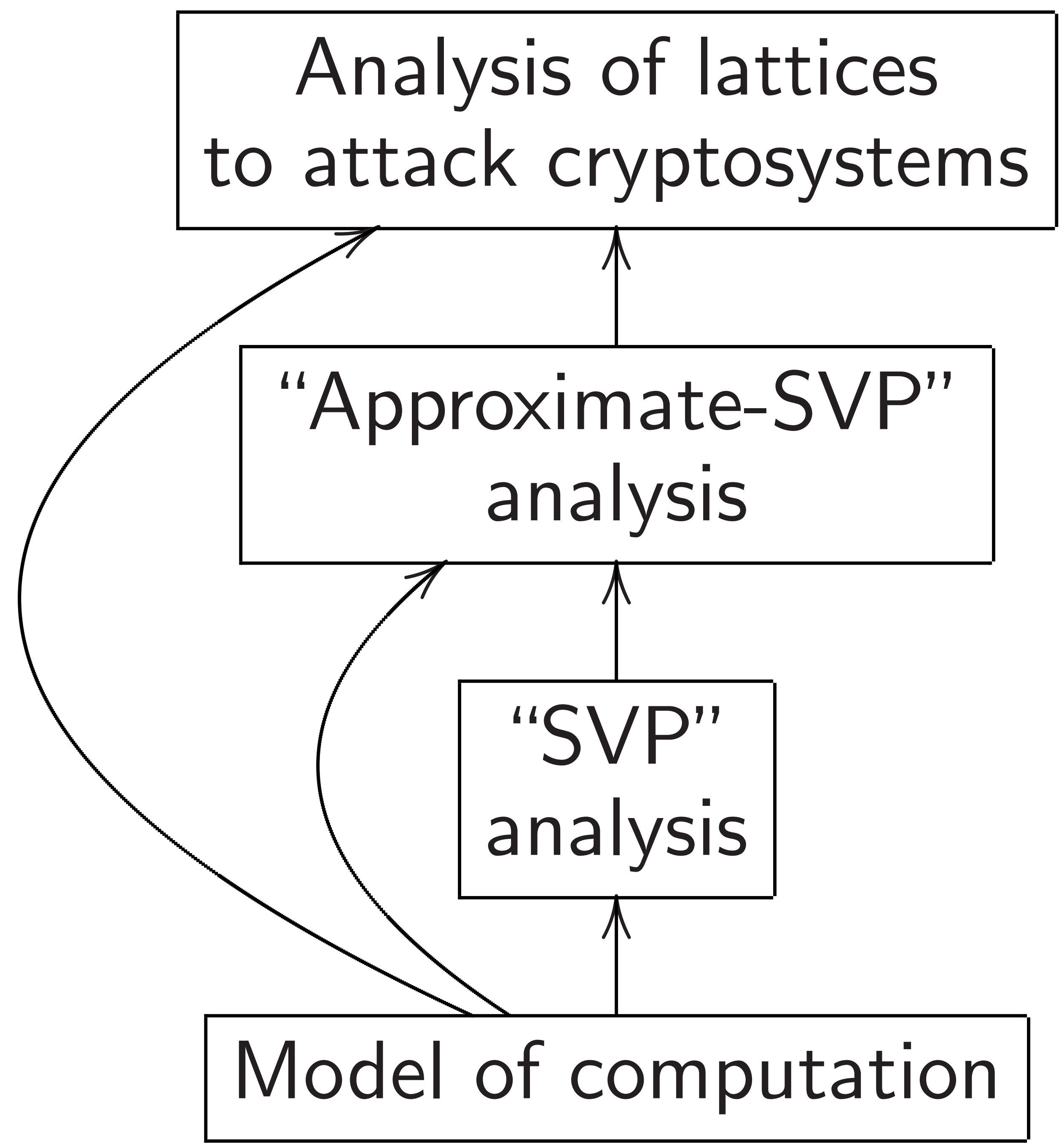
gnoring hybrid
ncluding hybrid
ignoring hybrid
including hybrid

st of memory:

gnoring hybrid
ncluding hybrid
ignoring hybrid
including hybrid

antum

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



Three typical atta

Define $\mathcal{R} = \mathbf{Z}[x]/$
"small" = all coef
$w = 286$; $q = 459$

Attacker wants to
small weight-w se

Problem 1: Public
$aG + e = 0$. Smal

Problem 2: Public
$aG + e = A$. Sma

Problem 3: Public
Public $aG_1 + e_1$, a
Small secrets e_1, e

n

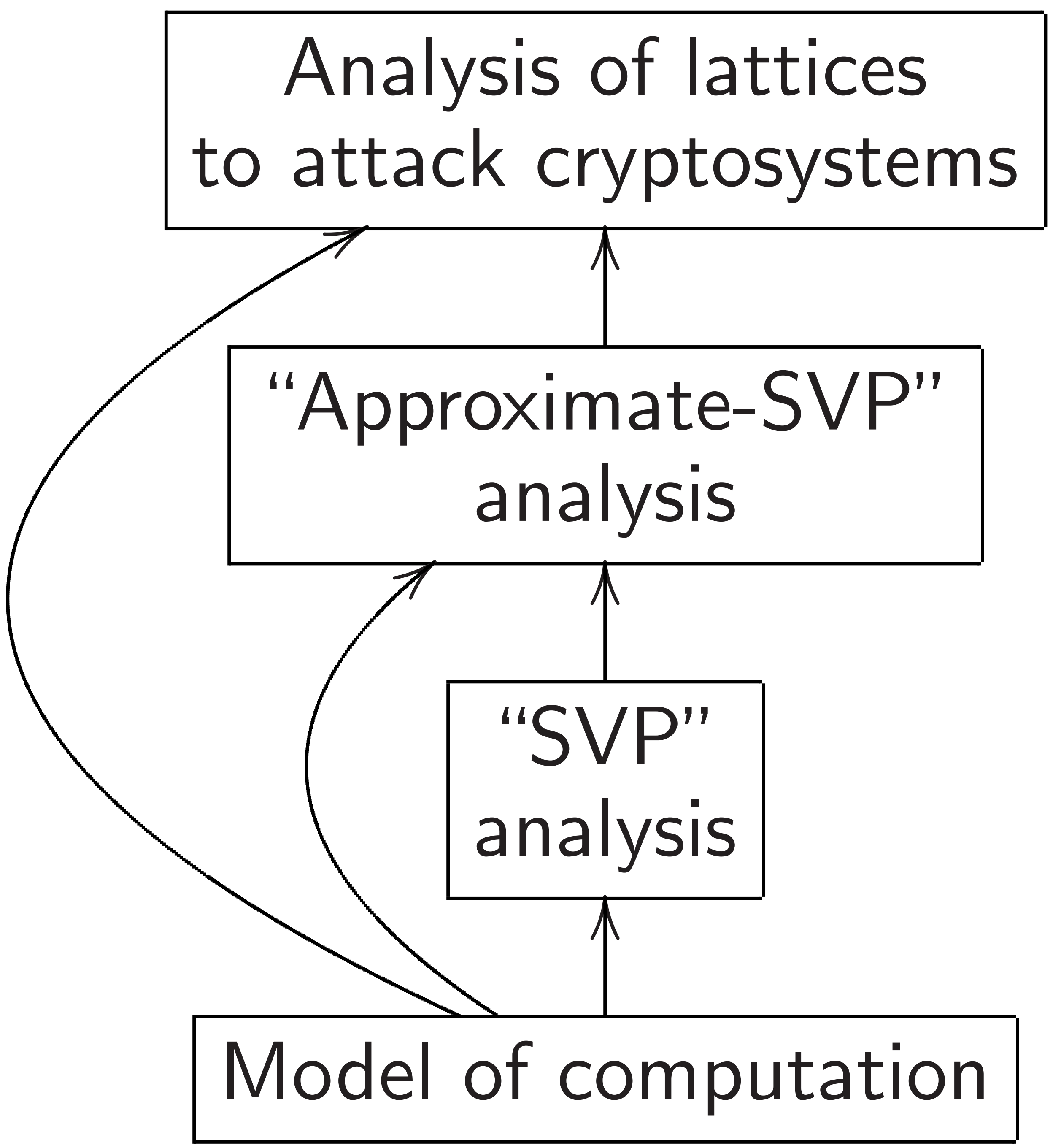
ble 2:

brid
ybrid
ybrid
hybrid

ory:

brid
ybrid
ybrid
hybrid

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



Three typical attack problem

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

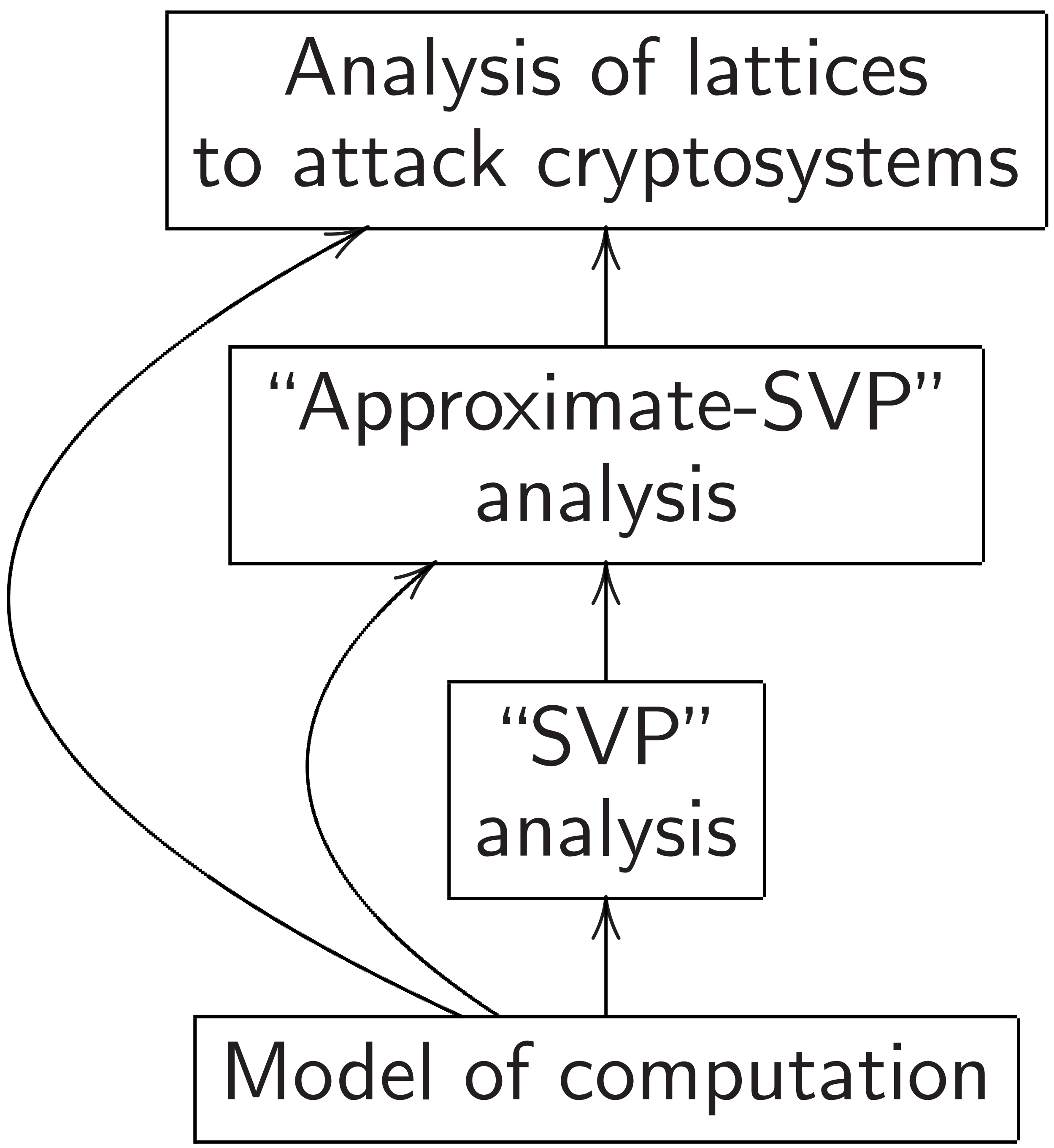
Attacker wants to find small weight-w secret $a \in \mathcal{R}$

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

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

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

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 $\{-1, 0, 1\}$;
$w = 286$; $q = 4591$.

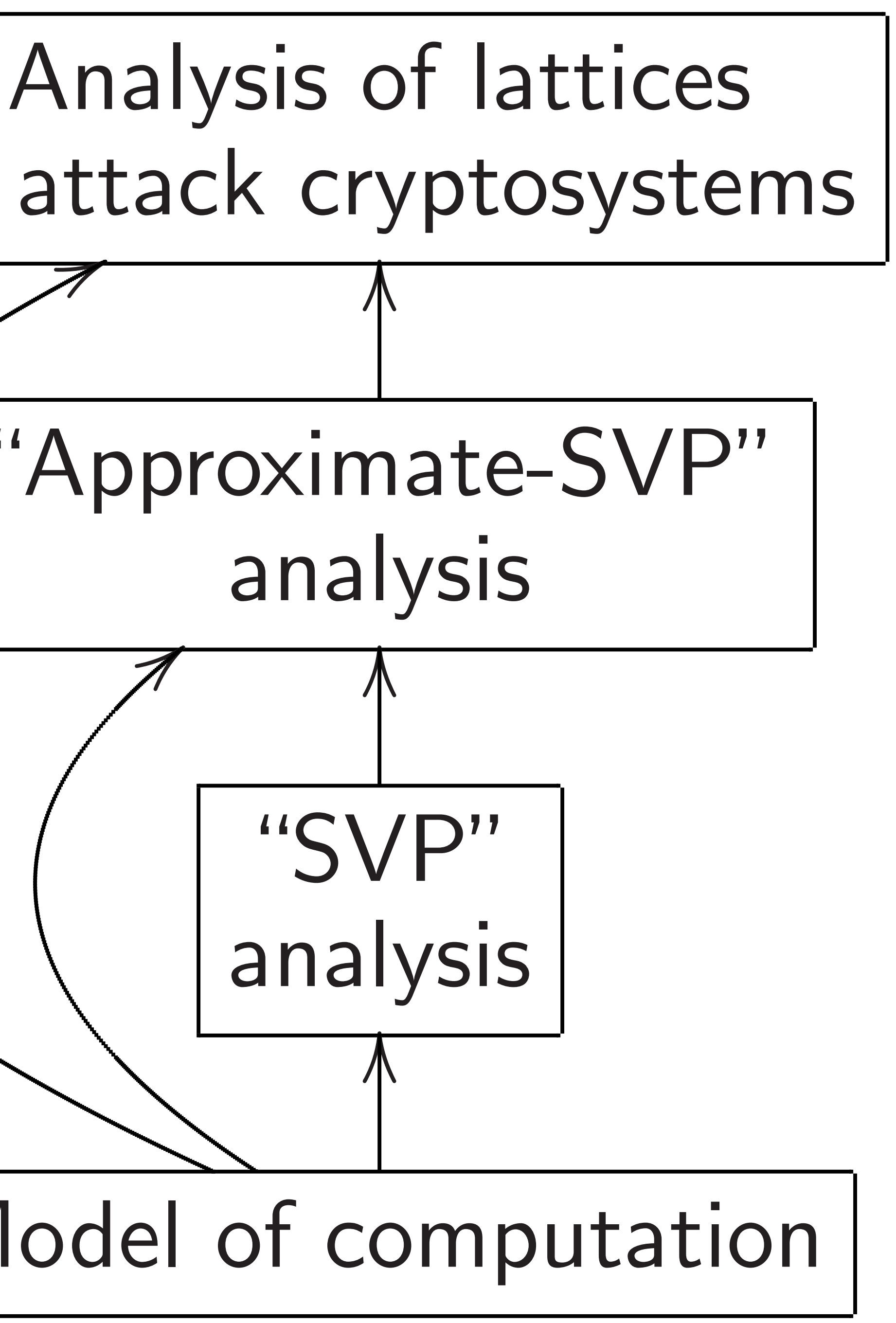
Attacker wants to find small weight-w secret $a \in \mathcal{R}$.

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 $e_1, e_2 \in \mathcal{R}$.

of typical lattice attack
plications at four layers,
nterfaces between layers.
k 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 $e_1, e_2 \in \mathcal{R}$.

Example

Secret k

Public k

and app

Public k

Hoffstei

$G = -e$

lattice attack
at four layers,
between layers.
zes top layer.

of lattices
yptosystems

ate-SVP"
ysis

VP"
ysis

omputation

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 targe

Secret key: small

Public key reveals
and approximation

Public key for "N
Hoffstein–Pipher–
$G = -e/a$, and A

tack
yers,
yers.
ver.

ns

n

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 cryptosy

Secret key: small a; small e.

Public key reveals multiplier
and approximation $A = aG$ -

Public key for "NTRU" (199
Hoffstein–Pipher–Silverman)
$G = -e/a$, and $A = 0$.

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 $A = 0$.

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 $A = 0$.

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

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 $A = 0$.

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.

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 $e_1, e_2 \in \mathcal{R}$.

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

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 $e_1, e_2 \in \mathcal{R}$.

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 $C = bA + M + c$.

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 $e_1, e_2 \in \mathcal{R}$.

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.

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 $e_1, e_2 \in \mathcal{R}$.

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 $G \in \mathcal{R}/q$.

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 $e_1, e_2 \in \mathcal{R}$.

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 $G, A \in \mathcal{R}/q$.

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 $e_1, e_2 \in \mathcal{R}$.

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 $G_1, A_1, G_2, A_2 \in \mathcal{R}/q$.

ypical attack problems

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

r wants to find
eight-w secret $a \in \mathcal{R}$.

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

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

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

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 $G_1, A_1, G_2, A_2 \in \mathcal{R}/q$.

Recogniz
as a full-

Problem
the map
from $\mathcal{R}^2$

ck problems

$(x^{761} - x - 1)$;

fs in $\{-1, 0, 1\}$;

1.

find

cret $a \in \mathcal{R}$.

: $G \in \mathcal{R}/q$ with

l secret $e \in \mathcal{R}$.

: $G \in \mathcal{R}/q$ and

ll secret $e \in \mathcal{R}$.

: $G_1, G_2 \in \mathcal{R}/q$.

$G_2 + e_2$.

$_2 \in \mathcal{R}$.

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 so
as a full-rank lattic

Problem 1: Lattic
the map $(\bar{a}, \bar{r}) \mapsto$
from $\mathcal{R}^2$ to $\mathcal{R}^2$.

ns

$- 1)$;

$0, 1\}$;

$\mathcal{R}$.

q with

$\in \mathcal{R}$.

q and

$\in \mathcal{R}$.

$\mathcal{R}/q$.

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 spa
as a full-rank lattice:

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

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 $(\bar{a}, \bar{r}) \mapsto (\bar{a}, q\bar{r} - \bar{a}G)$ from $\mathcal{R}^2$ to $\mathcal{R}^2$.

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 $\mathcal{R}^2$.

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

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 $\mathcal{R}^2$.

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 $(\overline{a}, \overline{t_1}, \overline{t_2}, \overline{r_1}, \overline{r_2}) \mapsto (\overline{a}, \overline{t_1}, \overline{t_2}, A_1\overline{t_1} + q\overline{r_1} - \overline{a}G_1, A_2\overline{t_2} + q\overline{r_2} - \overline{a}G_2)$.

each problem as finding
onzero solution to system
geneous $\mathcal{R}/q$ equations.

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

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

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

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 $\mathcal{R}^2$.

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

Each of
module,
many in

lem as finding
ution to system
$\mathcal{R}/q$ equations.

$(a, e) \in \mathcal{R}^2$
given $G \in \mathcal{R}/q$.

$(a, t, e) \in \mathcal{R}^3$
,
.

$\mathcal{R}^5$ with
$aG_2 + e_2 = A_2 t_2$,
$A_2 \in \mathcal{R}/q$.

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 $\mathcal{R}^2$.

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 latti
module, and thus
many independent

ding
stem
ions.
2
$\mathcal{R}/q$.
$\mathcal{R}^3$
$= A_2 t_2$,

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 $(\overline{a}, \overline{t}, \overline{r}) \mapsto (\overline{a}, \overline{t}, A\overline{t} + q\overline{r} - \overline{a}G)$.

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
module, and thus has, gener
many independent short vec

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.

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.

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.

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.

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

ze each solution space
-rank lattice:

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

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

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

Module structure

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

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 Ma
a stretch
be 0. Th
speeding
despite l

lution space
ce:

e is image of
$(\bar{a}, q\bar{r} - \bar{a}G)$

e is
$(\bar{a}, \bar{t}, \bar{r}) \mapsto$
$G)$.

e is image of
$\overline{r_1}, \overline{r_2}) \mapsto$
$\overline{r_1} - \bar{a}G_1,$
$)$.

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 Pro
a stretch of coeffic
be 0. This reduces
speeding up variou
despite lower succ

ce

of

$G)$

of

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: F
a stretch of coefficients of a
be 0. This reduces lattice ra
speeding up various attacks,
despite lower success chance

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.

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.

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

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.

(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!)

structure

these lattices is an $\mathcal{R}$-
and thus has, generically,
dependent short vectors.

roblem 2:
as short (a, t, e).
as short (xa, xt, xe).
as short (x^2a, x^2t, x^2e).

ore lattice vectors
short combinations
endent vectors:
$+1)a, (x+1)t, (x+1)e)$.

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.

(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

Uniform
secret a

ices is an $\mathcal{R}$-
has, generically,
short vectors.

$a, t, e)$.
$xa, xt, xe)$.
$x^2 a, x^2 t, x^2 e)$.

vectors
mbinations
ctors:
$+1)t, (x+1)e)$.

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.

(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

Uniform random s
secret a has length

$\mathcal{R}$-
rically,
tors.

).
$x^2 e$).

s

$+ 1)e$).

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.

(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 Proble

Uniform random small weigh
secret a has length $\sqrt{w} \approx 1$

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 $\sqrt{w} \approx 17$.

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 $\sqrt{w} \approx 17$.

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?)

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 $\sqrt{w} \approx 17$.

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

ay, for Problem 1: Force
n of coefficients of a to
his reduces lattice rank,
g up various attacks,
ower success chance.

a speedup? Seems to be
own if q is very large:
6 Kirchner–Fouque.)

roblems: same speedup.
i–Galbraith embedding"
lem 2: Force $t \in \mathbf{Z}$; force
oefficients of a to be 0.

wn if q is very large?
re misses module option!)

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
another

blem 1: Force
cients of a to
s lattice rank,
us attacks,
ess chance.

? Seems to be
very large:
–Fouque.)

ame speedup.
h embedding"
rce $t \in \mathbf{Z}$; force
of a to be 0.

very large?
module option!)

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
another solution s

orce
to
ank,

e.

to be
e:

dup.
ing"
force
0.

?
tion!)

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

Attacker is just as happy to
another solution such as $(xa$

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).

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

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.)

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

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?)

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

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.)

d analysis for Problem 1

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

random small secret
ngth usually close to
$\overline{3} \approx 23$. (Impact of
ns? Partial answer: 2020
n-Soled–Ducas–Gong–
s fixed weight safer?)

has rank $2 \cdot 761 = 1522$.
parameter: $k = 13$.
positions in a to be 0:
to sublattice of rank 1509.
n sublattice] $\approx 0.2\%$.

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 ec
as 761 e

for Problem 1

mall weight-w

n $\sqrt{w} \approx 17$.

mall secret

ly close to

Impact of

l answer: 2020

Ducas–Gong–

ght safer?)

$\cdot 761 = 1522$.

$k = 13$.

in a to be 0:

ce of rank 1509.

ce] $\approx 0.2\%$.

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 $e =$

as 761 equations o

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 coeffici

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.

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.

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}.

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.

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?)

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

d analysis for, e.g.,
$^{761}-1)$: Each $(x^j a, x^j e)$
nce $\approx$0.2% of being in
ce. These 761 chances
pendent. (No, they
lso, total Pr depends on
's choice of positions.
1 May–Silverman.)

igger solutions $(\alpha a, \alpha e)$.
ard are these to find?)

this analysis applies to
$^{761}-x-1)$. (It doesn't.)

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-ana

Huge sp
For each
figure ou
and char

happy to find
uch as (xa, xe).

for, e.g.,
Each $(x^j a, x^j e)$
% of being in
761 chances
(No, they
Pr depends on
of positions.
verman.)

tions $(\alpha a, \alpha e)$.
se to find?)

sis applies to
1). (It doesn't.)

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?)

<u>Cost-analysis chall</u>

Huge space of att
For each of these
figure out cost of
and chance it find

find
$a, xe)$.

$x^j e)$
in
es

s on
s.

$\alpha e)$.
?)

to
esn't.)

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?)

<u>Cost-analysis challenges</u>

Huge space of attack lattice
For each of these lattices, tr
figure out cost of (e.g.) BKZ
and chance it finds short vec

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.

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.

Accurate experiments are slow.
Need accurate fast estimates!

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.

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.

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.

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.