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

ges in evaluating costs
n lattice attacks

ernstein

---

k algorithm design:
e down algorithm A.
e algorithm costs C.
at, trying to minimize C.

tuation for hard problems:
f of min C for known A.

rse for lattice attacks:
of min C for known A are
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

Commen
that con

```
# XXX UNDER: ma
# XXX OVER: mar
# XXX UNDER/OVE
# XXX UNDER/OVE
# XXX UNDER/OVE
# XXX UNDER/OVE
# XXX UNDER/OVE
# XXX UNDER: as
# XXX UNDER: 'f
# XXX UNDER: ex
# XXX OVER: but
# XXX UNDER: in
# XXX OVER: ass
# XXX OVER: con
# XXX OVER: ass
# XXX OVER: lin
# XXX OVER: lin
# XXX OVER: lin
# XXX OVER/UNDE
# XXX OVER: lin
# XXX OVER: exp
# XXX OVER: ass
# XXX OVER: lin
# XXX OVER: ass
# XXX OVER: lin
# XXX OVER: ass
# XXX OVER: lin
# XXX UNDER/OVE
# XXX UNDER/OVE
# XXX UNDER/OVE
# XXX OVER: lin
# XXX UNDER: ig
# XXX OVER: lin
# XXX UNDER: ig
# XXX OVER: lin
# XXX UNDER: ig
# XXX UNDER: ig
```

uating costs
ttacks

m design:
gorithm A.
n costs C.
to minimize C.

r hard problems:
C for known A.

tice attacks:
or known A are
tified 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 p
that computed the

```
# XXX UNDER: many underestimates
# XXX OVER: many overestimates a
# XXX UNDER/OVER: misuse of asym
# XXX UNDER/OVER: misuse of asym
# XXX UNDER/OVER: misuse of asym
# XXX UNDER/OVER: misuse of asym
# XXX UNDER/OVER: misuse of asym
# XXX UNDER: assumes instant QRA
# XXX UNDER: 'free' options igno
# XXX UNDER: experiments suggest
# XXX OVER: but maybe delta cros
# XXX UNDER: incorrectly treats
# XXX OVER: assumes rotating t t
# XXX OVER: considers only equiv
# XXX OVER: assumes independence
# XXX OVER: limited force search
# XXX OVER: limited m search
# XXX OVER: limited scale search
# XXX OVER/UNDER: assumes averag
# XXX OVER: limited block-size s
# XXX OVER: experiments say smal
# XXX OVER: assumes dual attack
# XXX OVER: limited scale search
# XXX OVER: assumes that forcing
# XXX OVER: limited m search in
# XXX OVER: assumes even split i
# XXX OVER: limited blocksize se
# XXX UNDER/OVER: takes average
# XXX UNDER/OVER: ignores anti-c
# XXX UNDER/OVER: need more expe
# XXX OVER: limited imax search
# XXX UNDER: ignores cost of inn
# XXX OVER: limited imax search
# XXX UNDER: ignores cost of inn
# XXX OVER: limited imax search
# XXX UNDER: ignores cost of inn
# XXX UNDER: ignores collision p
```

ts

ze C.

blems:

n A.

ks:

A are

ses.

`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 s

that computed these numbe

```
# XXX UNDER: many underestimates and potential und
# XXX OVER: many overestimates and potential overe
# 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
# XXX OVER: but maybe delta crosses below this for
# XXX UNDER: incorrectly treats ntru prime as ntru
# XXX OVER: assumes rotating t to \Z is optimal
# XXX OVER: considers only equivalence by rotation
# XXX OVER: assumes independence across equivalenc
# 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 wo
# XXX OVER: assumes dual attack is non-competitive
# XXX OVER: limited scale search
# XXX OVER: assumes that forcing does not help wit
# 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 se
# 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
```

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
```

761 evaluations from
Prime: round 2” Table 2:

hybrid attacks:

5	enum, free memory cost
5	enum, real memory cost
9	sieving, free memory cost
3	sieving, real memory cost

g hybrid attacks:

9	enum, free memory cost
9	enum, real memory cost
9	sieving, free memory cost
0	sieving, real memory cost

levels:
-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 So
choices c
one char
the 35 is

“. . . the
optimiza
attack, v
to Roun
By takin
some pa
Round5
claimed

Goal: pr
2019 So

tions from

und 2" Table 2:

tacks:

ree memory cost
eal memory cost
free memory cost
real memory cost

ttacks:

ree memory cost
eal memory cost
free memory cost
real memory cost

antum

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
choices of Round5
one change inside
the 35 issues listec

"... there is one s
optimization of Al
attack, which was
to Round5 parame
By taking this into
some parameter ch
Round5 cannot en
claimed security le

Goal: pre-quantur
2019 Son says:

n

ble 2:

y cost
y cost
ory cost
ory cost

y cost
y cost
ory cost
ory cost

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 param choices of Round5", illustrat one change inside part of on the 35 issues listed in script:

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

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

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.

nts inside published script
nputed these numbers:

```
any underestimates and potential underestimates
ny overestimates and potential overestimates
ER: misuse of asymptotics
ER: misuse of asymptotics
ER: misuse of asymptotics
ER: misuse of asymptotics
ER: misuse of asymptotics
ssumes instant QRAM
free' options ignore cost of RAM
xperiments suggest delta is actually larger
t maybe delta crosses below this for large b
ncorrectly treats ntru prime as ntru classic
sumes rotating t to \Z is optimal
nsiders only equivalence by rotations
sumes independence across equivalence class
nited force search
nited m search
nited scale search
ER: assumes average g weight
nited block-size search
periments say smaller sizes often work
sumes dual attack is non-competitive
nited scale search
sumes that forcing does not help with hybrid
nited m search in hybrid context
sumes even split is optimal
nited blocksize search
ER: takes average weights
ER: ignores anti-correlation with searched weight
ER: need more experimental evidence
nited imax search
gnores cost of inner loop
nited imax search
gnores cost of inner loop
nited imax search
gnores cost of inner loop
gnores 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 mai

Define $\mathcal{R}$
"small"
$w = 28$
Attacker
small we

published script

ese numbers:

```
 and potential underestimates
nd potential overestimates
ptotics
ptotics
ptotics
ptotics
ptotics
M
re cost of RAM
 delta is actually larger
ses below this for large b
ntru prime as ntru classic
o \Z is optimal
alence by rotations
 across equivalence class



e g weight
earch
ler sizes often work
is non-competitive

 does not help with hybrid
hybrid context
s optimal
arch
weights
orrelation with searched weight
rimental evidence

er loop

er loop

er loop
robability
```


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 p

Define $\mathcal{R} = \mathbf{Z}[x]/$

"small" = all coef

$w = 286$; $q = 459$

Attacker wants to

small weight-w se

script

rs:

derestimates
estimates

larger
large b
classic

ns
ce class

rk
e

th hybrid

earched weight

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 $\mathcal{R} = \mathbf{Z}[x]/(x^{761} - x$

"small" = all coeffs in $\{-1,$

$w = 286$; $q = 4591$.

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

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 $s \in \mathcal{R}$.

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 $s \in \mathcal{R}$.

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

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 $s \in \mathcal{R}$.

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 $e \in \mathcal{R}$.

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 $s \in \mathcal{R}$.

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

n "A note on parameter
of Round5", illustrating
nge inside part of one of
ssues listed in script:

ere is one significant
ntion of Albrecht's dual
which was not reflected
d5 parameter choices.
ng this into consideration,
rameter choices of
cannot enjoy the
security level."

re-quantum 128, 192, 256.
n 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 $s \in \mathcal{R}$.

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
short no
of homo

Problem
with As

on parameter
", illustrating
part of one of
d in script:

significant
brecht's dual
not reflected
eter choices.
o consideration,
hoices of
joy the
evel."

m 128, 192, 256.
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 $s \in \mathcal{R}$.

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 prob
short nonzero solu
of homogeneous $\mathcal{R}$

Problem 1: Find (
with $As + e = 0$, g

neter
ting
ne of
;

ual
ted
es.
ation,

2, 256.
3, 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 $s \in \mathcal{R}$.

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 fin
short nonzero solution to sy
of homogeneous $\mathcal{R}/q$ equat

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

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

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

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

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

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 $A_1, b_1, A_2, b_2 \in \mathcal{R}/q$.

n 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 $s \in \mathcal{R}$.

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

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

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

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

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 $A_1, b_1, A_2, b_2 \in \mathcal{R}/q$.

Recogni
as a full-

Problem
of the m
from $\mathcal{R}^2$

problems

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

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

1.

find

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

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

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

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

ret $e \in \mathcal{R}$.

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

$_2 s + e_2$.

$_2 \in \mathcal{R}$.

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

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 so

as a full-rank latti

Problem 1: Find (

of the map (s, r)

from $\mathcal{R}^2$ to $\mathcal{R}^2$.

$-1)$;
$0, 1\}$;

$\mathcal{R}$.

q with
$\in \mathcal{R}$.

q and
.

$\mathcal{R}/q$.

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 spa
as a full-rank lattice:

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

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 $\mathcal{R}^2$.

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 $\mathcal{R}^2$.

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

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 $\mathcal{R}^2$.

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

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

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

3: Find
$, e_1, e_2) \in \mathcal{R}^5$ with
$_1 = b_1 t_1$, $A_2 s + e_2 = b_2 t_2$,
$_1, b_1, A_2, b_2 \in \mathcal{R}/q$.

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 $\mathcal{R}^2$.

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
module,
many in

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

$s, e) \in \mathcal{R}^2$
given $A \in \mathcal{R}/q$.

$s, t, e) \in \mathcal{R}^3$

$\mathcal{R}^5$ with
$A_2 s + e_2 = b_2 t_2$,
$_2 \in \mathcal{R}/q$.

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 $\mathcal{R}^2$.

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 latti
module, and thus
many independent

ding
stem
ions.
^{2}
$\mathcal{R}/q$.
$\mathcal{R}^3$
$= b_2 t_2$,

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 $(s, t, r) \mapsto (s, t, bt + qr - As)$.

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
module, and thus has, gener
many independent short vec

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.

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.

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

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.

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".

ze each solution space
-rank lattice:

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

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

3: Find
$, e_1, e_2)$ in image
ap $(s, t_1, t_2, r_1, r_2) \mapsto$
$, b_1 t_1 + qr_1 - A_1 s,$
$r_2 - A_2 s)$.

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.

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

2001 Ma
1: Force
s to be
rank, sp
despite

lution space
ce:

$s, e)$ in image
$\to (s, qr - As)$

$s, t, e)$
ap $(s, t, r) \mapsto$
$s)$.

image
$t_2, r_1, r_2) \mapsto$
$r_1 - A_1 s,$
.

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–Silverm
1: Force a few coe
s to be 0. This re
rank, speeding up
despite lower succ

ce

age

– As)

$\mapsto$

$\mapsto$

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 Pr

1: Force a few coefficients o

s to be 0. This reduces latti

rank, speeding up various at

despite lower success chance

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.

⇒ 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.

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.

(Always a speedup? Seems to be a slowdown if q is very large.)

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.

(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?)

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

e from 2017 Kirchner–
"there exist many short
in Problem 1 lattices
in Problem 2/3 lattices.

ense in NISTIR 8240:
1 "produces a lattice
somewhat more
e . . . due to having
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.

(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

Lattice

Uniform
secret s

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

17 Kirchner–
ist many short
m 1 lattices
n 2/3 lattices.

STIR 8240:
ces a lattice
t more
to having
cted 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.

(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 o

Lattice has rank 2

Uniform random s
secret s has length

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

er–
short
es
ices.

0:
ce

rs".

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

Lattice has rank $2 \cdot 761 = 1$

Uniform random small weigh
secret s has length $\sqrt{286} \approx$

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 $\sqrt{286} \approx 17$.

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 $\sqrt{286} \approx 17$.

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?)

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 $\sqrt{286} \approx 17$.

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.

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

ay–Silverman, for Problem
a few coefficients of
0. This reduces lattice
eeding up various attacks,
ower success chance.

a speedup? Seems to be
own if q is very large.)

eedup for Problem 2:
any coefficients of (s, t)
Bai–Galbraith special
rce $t = 1$, and force
efficients of s to be 0.

wdown 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 $\sqrt{286} \approx 17$.

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 is in sublattice] $\approx 0.2\%$.

Attacker
another

an, for Problem
efficients of
duces lattice
various attacks,
ess chance.

? Seems to be
very large.)

Problem 2:
cients of (s, t)
raith special
and force
of s to be 0.

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 $\sqrt{286} \approx 17$.

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 is in sublattice] $\approx 0.2\%$.

Attacker is just as
another solution s

oblem
of
ice
tacks,
e.

to be
e.)

2:
s, t)
ial
e
0.

large?)

Standard attack on Problem 1

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

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

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 is in sublattice] $\approx 0.2\%$.

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

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).

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).

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

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 is in sublattice] $\approx 0.2\%$.

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

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 is in sublattice] $\approx 0.2\%$.

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.)

d attack on Problem 1

has rank $2 \cdot 761 = 1522$.

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

random small secret
ngth usually close to
$\overline{3} \approx 23$. (What if it's
What if it's larger?)

parameter: $k = 13$.

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

n sublattice] $\approx 0.2\%$.

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

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

Write ec
as 761 e

n Problem 1

$\cdot\ 761 = 1522$.

mall weight-w
n $\sqrt{286} \approx 17$.

mall secret
ly close to
What if it's
t's larger?)

$k = 13$.

in s to be 0:
ce of rank 1509.

e] $\approx 0.2\%$.

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

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

Write equation e =
as 761 equations o

<u>1</u>

522.

nt-w

17.

t

’s

)

0:

1509.

.

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 coeffici

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.

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.

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}.

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 $\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 $(\alpha s, \alpha e)$. (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.

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?)

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

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

igger solutions $(\alpha s, \alpha e)$.
rd are these to find?)

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

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 p

Use BKZ
lattice b
alternati

happy to find
uch as (xs, xe).

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

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

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

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:

Use BKZ-β algorit
lattice basis. (Wh
alternatives to BK

find
$s, xe)$.

$x^j e)$
in
es

s on
s.)

$\alpha e)$.
?)

to
esn't.)

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 red
lattice basis. (What about
alternatives to BKZ?)

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?)

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?)

Standard analysis of BKZ-β:

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

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?)

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.)

quation $e = qr - As$

quations on coefficients.

parameter: $m = 600$.

$61 - m = 161$ equations:

ect e onto 600 positions.

d sublattice rank d =

$161 = 1348$; det q^{600}.

parameter: $\lambda = 1.331876$.

g: Assign weight λ to

s in s. Increases length of

$\overline{286} \approx 23$; increases det to

. (Is this λ optimal?)

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

“Geome

holds. (

identifie

$= qr - As$

on coefficients.

$m = 600$.

161 equations:

600 positions.

ce rank d =

8; det q^{600}.

$\lambda = 1.331876$.

weight λ to

reases length of

increases det to

λ optimal?)

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,

"Geometric-series

holds. (What abo

identified in 2018

ents.

.

tions:

tions.

=

0.

1876.

to

gth of

det to

?)

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 assumptio

holds. (What about deviatio

identified in 2018 experimen

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?)

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?)

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?)

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?)

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?)

parameter: $\beta = 525$.

Z-β algorithm to reduce
asis. (What about
ves to BKZ?)

d analysis of BKZ-β:

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

formula is an *asymptotic*
thout claimed error
Does not match
ents for specific d.)

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 $\leq \delta^{2\beta-d} (\det L)^{1/d} \sqrt{d/\beta}$. (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 lon

Standar
$2^{139.125}$

$\beta = 525$.

thm to reduce
at about
Z?)

of BKZ-β:

nonzero vector
$)^{1/d}$ where
$\pi e))^{1/(2(\beta-1))}$.

an *asymptotic*
med error
match
ecific d.)

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 BK

Standard answer:
$2^{139.125}$ quantum

luce

:

ector
e
3−1)).

totic

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

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.

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.

(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"?)

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.

(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.

d analysis, continued:

tric-series assumption”
What about deviations
d in 2018 experiments?)

finds unique (mod $\pm$)
nonzero vector $\Leftrightarrow$
$\le \delta^{2\beta-d}(\det L)^{1/d}\sqrt{d/\beta}$.
bout deviations identified
experiments?)

ne attack finds (s, e),
g forcing worked. If it
etry. (Are these tries
dent? Should they use
ameters? Grover?)

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 Be
Lange–v
Prime: r
broader
of (1) ho
work, inc
and (2)
the perfo

New latt
2019 So
Cheon (
Curtis–W
2019 Alb
Postleth

continued:

assumption"
ut deviations
experiments?)

ue (mod $\pm$)
ector $\Leftrightarrow$
et $L)^{1/d}\sqrt{d/\beta}$.
ations identified
ts?)

finds (s, e),
worked. If it
these tries
uld they use
Grover?)

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–Ch
Lange–van Vreden
Prime: round 2" S
broader and more
of (1) how known
work, including hy
and (2) open ques
the performance o

New lattice-analys
2019 Son (dual); 2
Cheon (hybrid); 20
Curtis–Wunderer (
2019 Albrecht–Gh
Postlethwaite–Sch

d:

on”

ons

ts?)

±)

$\overline{d/\beta}$.

ntified

),

it

s

use

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× 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–Chuengsatia
Lange–van Vredendaal “NTI
Prime: round 2” Section 6:
broader and more detailed s
of (1) how known lattice att
work, including hybrid attac
and (2) open questions rega
the performance of these att

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

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).