Challenges in evaluating costs of known lattice attacks

Daniel J. Bernstein
Tanja Lange

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

Why analysis is important:

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

Three typical attack problems

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

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

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

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

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

ges in evaluating costs
n lattice attacks

. Bernstein
ange

---

n attack survey from
rnstein–Chuengsatiansup–
an Vredendaal.

---

alysis is important:
attack optimization.
attack selection.
ate crypto parameters.
ate crypto designs.
e users on security.

Three typical attack problems

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

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

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

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

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

Example

Secret k

Public k
and appr

Public k
$G = -e$

uating costs
ttacks

n

urvey from
nuengsatiansup–
daal.

portant:
timization.
ection.
parameters.
designs.
security.

Three typical attack problems

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

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

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

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

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

Examples of target

Secret key: small

Public key reveals
and approximation

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

ts

n

nsup–

.

rs.

Three typical attack problems

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

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

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

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

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

Examples of target cryptosys

Secret key: small a; small e.

Public key reveals multiplier

and approximation $A = aG$ -

Public key for "NTRU": $G = -e/a$, 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 $aG + e$. Small secret $e \in \mathcal{R}$.

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

Examples of target cryptosystems

Secret key: small a; small e.

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

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

Three typical attack problems

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

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

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

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

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

Examples of target cryptosystems

Secret key: small a; small e.

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

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

Public key for "Ring-LWE": 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
$aG + e$. Small secret $e \in \mathcal{R}$.

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

Examples of target cryptosystems

Secret key: small a; small e.

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

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

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

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

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

Examples of target cryptosystems

Secret key: small a; small e.

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

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

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

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

Encrypti
Input sm
Ciphert

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

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

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

$G_2 + e_2$.

$_2 \in \mathcal{R}$.

Examples of target cryptosystems

Secret key: small a; small e.

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

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

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

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

Encryption for Qu

Input small b, sma

Ciphertext: $B = 3$

ns

$-1)$;

$0,1\}$;

$\mathcal{R}$.

q with

$\in \mathcal{R}$.

q and

.

$\mathcal{R}/q$.

Examples of target cryptosystems

Secret key: small a; small e.

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

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

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

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

Encryption for Quotient NT

Input small b, small d.

Ciphertext: $B = 3Gb + d$.

Examples of target cryptosystems

Secret key: small a; small e.

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

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

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

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

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

Examples of target cryptosystems

Secret key: small a; small e.

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

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

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

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

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

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

Examples of target cryptosystems

Secret key: small a; small e.

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

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

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

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

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

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

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

es of target cryptosystems

ey: small a; small e.

ey reveals multiplier G
roximation $A = aG + e$.

ey for "NTRU":
$/a$, and $A = 0$.

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

tization of naming,
ing similarity + credits:
" $\Rightarrow$ Quotient NTRU.
VE" $\Rightarrow$ Product NTRU.

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

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

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

system	parame
frodo	
frodo	
frodo	
kyber	
kyber	
kyber	
lac	
lac	
lac	
newhope	
newhope	
ntru	hps20
ntru	hps20
ntru	hps40
ntru	hr
ntrulpr	
ntrulpr	
ntrulpr	
round5n1	
round5n1	
round5n1	
round5nd	
round5nd	
round5nd	
round5nd	
round5nd	
round5nd	
saber	
saber	
saber	
sntrup	
sntrup	
sntrup	
threebears	
threebears	
threebears	

t cryptosystems

a; small e.

multiplier G

n $A = aG + e$.

TRU":

$= 0$.

ng-LWE":

$= aG + e$.

f naming,

rity + credits:

ient NTRU.

roduct NTRU.

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

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

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

system	parameter set	type
frodo	640	Product
frodo	976	Product
frodo	1344	Product
kyber	512	Product
kyber	768	Product
kyber	1024	Product
lac	128	Product
lac	192	Product
lac	256	Product
newhope	512	Product
newhope	1024	Product
ntru	hps2048509	Quotient
ntru	hps2048677	Quotient
ntru	hps4096821	Quotient
ntru	hrss701	Quotient
ntrulpr	653	Product
ntrulpr	761	Product
ntrulpr	857	Product
round5n1	1	Product
round5n1	3	Product
round5n1	5	Product
round5nd	1.0d	Product
round5nd	3.0d	Product
round5nd	5.0d	Product
round5nd	1.5d	Product
round5nd	3.5d	Product
round5nd	5.5d	Product
saber	light	Product
saber	main	Product
saber	fire	Product
sntrup	653	Quotient
sntrup	761	Quotient
sntrup	857	Quotient
threebears	baby	Product
threebears	mama	Product
threebears	papa	Product

stems

.

G

$+ e$.

.

dits:

U.

TRU.

Encryption for Quotient NTRU:

Input small b, small d.

Ciphertext: $B = 3Gb + d$.

Encryption for Product NTRU:

Input encoded message M.

Randomly generate small b, small d, small c.

Ciphertext: $B = Gb + d$ and $C = Ab + M + c$.

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

system	parameter set	type	set of multipliers
frodo	640	Product	$(\mathbf{Z}/32768)^{640\times 640}$
frodo	976	Product	$(\mathbf{Z}/65536)^{976\times 976}$
frodo	1344	Product	$(\mathbf{Z}/65536)^{1344\times 1344}$
kyber	512	Product	$((\mathbf{Z}/3329)[x]/(x^{256}$
kyber	768	Product	$((\mathbf{Z}/3329)[x]/(x^{256}$
kyber	1024	Product	$((\mathbf{Z}/3329)[x]/(x^{256}$
lac	128	Product	$(\mathbf{Z}/251)[x]/(x^{512}+$
lac	192	Product	$(\mathbf{Z}/251)[x]/(x^{1024}$
lac	256	Product	$(\mathbf{Z}/251)[x]/(x^{1024}$
newhope	512	Product	$(\mathbf{Z}/12289)[x]/(x^{512}$
newhope	1024	Product	$(\mathbf{Z}/12289)[x]/(x^{102}$
ntru	hps2048509	Quotient	$(\mathbf{Z}/2048)[x]/(x^{509}$
ntru	hps2048677	Quotient	$(\mathbf{Z}/2048)[x]/(x^{677}$
ntru	hps4096821	Quotient	$(\mathbf{Z}/4096)[x]/(x^{821}$
ntru	hrss701	Quotient	$(\mathbf{Z}/8192)[x]/(x^{701}$
ntrulpr	653	Product	$(\mathbf{Z}/4621)[x]/(x^{653}$
ntrulpr	761	Product	$(\mathbf{Z}/4591)[x]/(x^{761}$
ntrulpr	857	Product	$(\mathbf{Z}/5167)[x]/(x^{857}$
round5n1	1	Product	$(\mathbf{Z}/4096)^{636\times 636}$
round5n1	3	Product	$(\mathbf{Z}/32768)^{876\times 876}$
round5n1	5	Product	$(\mathbf{Z}/32768)^{1217\times 1217}$
round5nd	1.0d	Product	$(\mathbf{Z}/8192)[x]/(x^{586}$
round5nd	3.0d	Product	$(\mathbf{Z}/4096)[x]/(x^{852}$
round5nd	5.0d	Product	$(\mathbf{Z}/8192)[x]/(x^{1170}$
round5nd	1.5d	Product	$(\mathbf{Z}/1024)[x]/(x^{509}$
round5nd	3.5d	Product	$(\mathbf{Z}/4096)[x]/(x^{757}$
round5nd	5.5d	Product	$(\mathbf{Z}/2048)[x]/(x^{947}$
saber	light	Product	$((\mathbf{Z}/8192)[x]/(x^{256}$
saber	main	Product	$((\mathbf{Z}/8192)[x]/(x^{256}$
saber	fire	Product	$((\mathbf{Z}/8192)[x]/(x^{256}$
sntrup	653	Quotient	$(\mathbf{Z}/4621)[x]/(x^{653}$
sntrup	761	Quotient	$(\mathbf{Z}/4591)[x]/(x^{761}$
sntrup	857	Quotient	$(\mathbf{Z}/5167)[x]/(x^{857}$
threebears	baby	Product	$(\mathbf{Z}/(2^{3120}-2^{1560}$
threebears	mama	Product	$(\mathbf{Z}/(2^{3120}-2^{1560}$
threebears	papa	Product	$(\mathbf{Z}/(2^{3120}-2^{1560}$

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

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

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

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

on for Quotient NTRU:
nall b, small d.
xt: $B = 3Gb + d$.

on for Product NTRU:
coded message M.
ly generate
small d, small c.
xt: $B = Gb + d$
$= Ab + M + c$.

des: survey of G, a, e, c, M
nd variants in NISTPQC
ons. Source: Bernstein,
ring proofs of security
ce-based encryption".

system	parameter set	type	set of multipliers
frodo	640	Product	$(\mathbf{Z}/32768)^{640\times640}$
frodo	976	Product	$(\mathbf{Z}/65536)^{976\times976}$
frodo	1344	Product	$(\mathbf{Z}/65536)^{1344\times1344}$
kyber	512	Product	$((\mathbf{Z}/3329)[x]/(x^{256}+1))^{2\times2}$
kyber	768	Product	$((\mathbf{Z}/3329)[x]/(x^{256}+1))^{3\times3}$
kyber	1024	Product	$((\mathbf{Z}/3329)[x]/(x^{256}+1))^{4\times4}$
lac	128	Product	$(\mathbf{Z}/251)[x]/(x^{512}+1)$
lac	192	Product	$(\mathbf{Z}/251)[x]/(x^{1024}+1)$
lac	256	Product	$(\mathbf{Z}/251)[x]/(x^{1024}+1)$
newhope	512	Product	$(\mathbf{Z}/12289)[x]/(x^{512}+1)$
newhope	1024	Product	$(\mathbf{Z}/12289)[x]/(x^{1024}+1)$
ntru	hps2048509	Quotient	$(\mathbf{Z}/2048)[x]/(x^{509}-1)$
ntru	hps2048677	Quotient	$(\mathbf{Z}/2048)[x]/(x^{677}-1)$
ntru	hps4096821	Quotient	$(\mathbf{Z}/4096)[x]/(x^{821}-1)$
ntru	hrss701	Quotient	$(\mathbf{Z}/8192)[x]/(x^{701}-1)$
ntrulpr	653	Product	$(\mathbf{Z}/4621)[x]/(x^{653}-x-1)$
ntrulpr	761	Product	$(\mathbf{Z}/4591)[x]/(x^{761}-x-1)$
ntrulpr	857	Product	$(\mathbf{Z}/5167)[x]/(x^{857}-x-1)$
round5n1	1	Product	$(\mathbf{Z}/4096)^{636\times636}$
round5n1	3	Product	$(\mathbf{Z}/32768)^{876\times876}$
round5n1	5	Product	$(\mathbf{Z}/32768)^{1217\times1217}$
round5nd	1.0d	Product	$(\mathbf{Z}/8192)[x]/(x^{586}+\ldots+1)$
round5nd	3.0d	Product	$(\mathbf{Z}/4096)[x]/(x^{852}+\ldots+1)$
round5nd	5.0d	Product	$(\mathbf{Z}/8192)[x]/(x^{1170}+\ldots+1)$
round5nd	1.5d	Product	$(\mathbf{Z}/1024)[x]/(x^{509}-1)$
round5nd	3.5d	Product	$(\mathbf{Z}/4096)[x]/(x^{757}-1)$
round5nd	5.5d	Product	$(\mathbf{Z}/2048)[x]/(x^{947}-1)$
saber	light	Product	$((\mathbf{Z}/8192)[x]/(x^{256}+1))^{2\times2}$
saber	main	Product	$((\mathbf{Z}/8192)[x]/(x^{256}+1))^{3\times3}$
saber	fire	Product	$((\mathbf{Z}/8192)[x]/(x^{256}+1))^{4\times4}$
sntrup	653	Quotient	$(\mathbf{Z}/4621)[x]/(x^{653}-x-1)$
sntrup	761	Quotient	$(\mathbf{Z}/4591)[x]/(x^{761}-x-1)$
sntrup	857	Quotient	$(\mathbf{Z}/5167)[x]/(x^{857}-x-1)$
threebears	baby	Product	$(\mathbf{Z}/(2^{3120}-2^{1560}-1))^{2\times2}$
threebears	mama	Product	$(\mathbf{Z}/(2^{3120}-2^{1560}-1))^{3\times3}$
threebears	papa	Product	$(\mathbf{Z}/(2^{3120}-2^{1560}-1))^{4\times4}$

short element
$\mathbf{Z}^{640\times8}$; $\{-12, \ldots$
$\mathbf{Z}^{976\times8}$; $\{-10, \ldots$
$\mathbf{Z}^{1344\times8}$; $\{-6, \ldots$
$(\mathbf{Z}[x]/(x^{256}+1)$
$(\mathbf{Z}[x]/(x^{256}+1)$
$(\mathbf{Z}[x]/(x^{256}+1)$
$\mathbf{Z}[x]/(x^{512}+1)$;
$\mathbf{Z}[x]/(x^{1024}+1)$
$\mathbf{Z}[x]/(x^{1024}+1)$
$\mathbf{Z}[x]/(x^{512}+1)$;
$\mathbf{Z}[x]/(x^{1024}+1)$
$\mathbf{Z}[x]/(x^{509}-1)$;
$\mathbf{Z}[x]/(x^{677}-1)$;
$\mathbf{Z}[x]/(x^{821}-1)$;
$\mathbf{Z}[x]/(x^{701}-1)$;
$\mathbf{Z}[x]/(x^{653}-x-$
$\mathbf{Z}[x]/(x^{761}-x-$
$\mathbf{Z}[x]/(x^{857}-x-$
$\mathbf{Z}^{636\times8}$; $\{-1, 0,$
$\mathbf{Z}^{876\times8}$; $\{-1, 0,$
$\mathbf{Z}^{1217\times8}$; $\{-1, 0,$
$\mathbf{Z}[x]/(x^{586}+\ldots$
$\mathbf{Z}[x]/(x^{852}+\ldots$
$\mathbf{Z}[x]/(x^{1170}+\ldots$
$\mathbf{Z}[x]/(x^{509}-1)$;
$\mathbf{Z}[x]/(x^{757}-1)$;
$\mathbf{Z}[x]/(x^{947}-1)$;
$(\mathbf{Z}[x]/(x^{256}+1)$
$(\mathbf{Z}[x]/(x^{256}+1)$
$(\mathbf{Z}[x]/(x^{256}+1)$
$\mathbf{Z}[x]/(x^{653}-x-$
$\mathbf{Z}[x]/(x^{761}-x-$
$\mathbf{Z}[x]/(x^{857}-x-$
$\mathbf{Z}^2$; $\sum_{0\le i<312} 2$
$\mathbf{Z}^3$; $\sum_{0\le i<312} 2$
$\mathbf{Z}^4$; $\sum_{0\le i<312} 2$

otient NTRU:
all d.
$3Gb + d$.

oduct NTRU:
ssage M.
e
small c.
$Gb + d$
$+ c$.

y of G, a, e, c, M
ts in NISTPQC
ce: Bernstein,
s of security
ncryption”.

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

short element
$\mathbf{Z}^{640\times 8}$; $\{-12,\ldots,12\}$; Pr 1, 4, 17, .
$\mathbf{Z}^{976\times 8}$; $\{-10,\ldots,10\}$; Pr 1, 6, 29, .
$\mathbf{Z}^{1344\times 8}$; $\{-6,\ldots,6\}$; Pr 2, 40, 364,
$(\mathbf{Z}[x]/(x^{256}+1))^2$; $\sum_{0\le i<4}\{-0.5,$
$(\mathbf{Z}[x]/(x^{256}+1))^3$; $\sum_{0\le i<4}\{-0.5,$
$(\mathbf{Z}[x]/(x^{256}+1))^4$; $\sum_{0\le i<4}\{-0.5,$
$\mathbf{Z}[x]/(x^{512}+1)$; $\{-1,0,1\}$; Pr 1, 2,
$\mathbf{Z}[x]/(x^{1024}+1)$; $\{-1,0,1\}$; Pr 1, 6
$\mathbf{Z}[x]/(x^{1024}+1)$; $\{-1,0,1\}$; Pr 1, 2
$\mathbf{Z}[x]/(x^{512}+1)$; $\sum_{0\le i<16}\{-0.5, 0.5$
$\mathbf{Z}[x]/(x^{1024}+1)$; $\sum_{0\le i<16}\{-0.5, 0.$
$\mathbf{Z}[x]/(x^{509}-1)$; $\{-1,0,1\}$
$\mathbf{Z}[x]/(x^{677}-1)$; $\{-1,0,1\}$
$\mathbf{Z}[x]/(x^{821}-1)$; $\{-1,0,1\}$
$\mathbf{Z}[x]/(x^{701}-1)$; $\{-1,0,1\}$; key corr
$\mathbf{Z}[x]/(x^{653}-x-1)$; $\{-1,0,1\}$; wei
$\mathbf{Z}[x]/(x^{761}-x-1)$; $\{-1,0,1\}$; wei
$\mathbf{Z}[x]/(x^{857}-x-1)$; $\{-1,0,1\}$; wei
$\mathbf{Z}^{636\times 8}$; $\{-1,0,1\}$; weight 57, 57
$\mathbf{Z}^{876\times 8}$; $\{-1,0,1\}$; weight 223, 223
$\mathbf{Z}^{1217\times 8}$; $\{-1,0,1\}$; weight 231, 231
$\mathbf{Z}[x]/(x^{586}+\ldots+1)$; $\{-1,0,1\}$; we
$\mathbf{Z}[x]/(x^{852}+\ldots+1)$; $\{-1,0,1\}$; we
$\mathbf{Z}[x]/(x^{1170}+\ldots+1)$; $\{-1,0,1\}$; w
$\mathbf{Z}[x]/(x^{509}-1)$; $\{-1,0,1\}$; weight 6
$\mathbf{Z}[x]/(x^{757}-1)$; $\{-1,0,1\}$; weight
$\mathbf{Z}[x]/(x^{947}-1)$; $\{-1,0,1\}$; weight
$(\mathbf{Z}[x]/(x^{256}+1))^2$; $\sum_{0\le i<10}\{-0.5,$
$(\mathbf{Z}[x]/(x^{256}+1))^3$; $\sum_{0\le i<8}\{-0.5,$
$(\mathbf{Z}[x]/(x^{256}+1))^4$; $\sum_{0\le i<6}\{-0.5,$
$\mathbf{Z}[x]/(x^{653}-x-1)$; $\{-1,0,1\}$; wei
$\mathbf{Z}[x]/(x^{761}-x-1)$; $\{-1,0,1\}$; wei
$\mathbf{Z}[x]/(x^{857}-x-1)$; $\{-1,0,1\}$; wei
$\mathbf{Z}^2$; $\sum_{0\le i<312} 2^{10i}\{-2,-1,0,1,2\}$;
$\mathbf{Z}^3$; $\sum_{0\le i<312} 2^{10i}\{-1,0,1\}$; Pr 13,
$\mathbf{Z}^4$; $\sum_{0\le i<312} 2^{10i}\{-1,0,1\}$; Pr 5, 2

RU:

RU:

e, c, M

PQC

tein,

ty

.

system	parameter set	type	set of multipliers	short element
frodo	640	Product	$(\mathbf{Z}/32768)^{640\times640}$	$\mathbf{Z}^{640\times8}$; $\{-12,\ldots,12\}$; Pr 1, 4, 17, ... (spec page 23)
frodo	976	Product	$(\mathbf{Z}/65536)^{976\times976}$	$\mathbf{Z}^{976\times8}$; $\{-10,\ldots,10\}$; Pr 1, 6, 29, ... (spec page 23)
frodo	1344	Product	$(\mathbf{Z}/65536)^{1344\times1344}$	$\mathbf{Z}^{1344\times8}$; $\{-6,\ldots,6\}$; Pr 2, 40, 364, ... (spec page 23)
kyber	512	Product	$((\mathbf{Z}/3329)[x]/(x^{256}+1))^{2\times2}$	$(\mathbf{Z}[x]/(x^{256}+1))^2$; $\sum_{0\le i<4}\{-0.5,0.5\}$
kyber	768	Product	$((\mathbf{Z}/3329)[x]/(x^{256}+1))^{3\times3}$	$(\mathbf{Z}[x]/(x^{256}+1))^3$; $\sum_{0\le i<4}\{-0.5,0.5\}$
kyber	1024	Product	$((\mathbf{Z}/3329)[x]/(x^{256}+1))^{4\times4}$	$(\mathbf{Z}[x]/(x^{256}+1))^4$; $\sum_{0\le i<4}\{-0.5,0.5\}$
lac	128	Product	$(\mathbf{Z}/251)[x]/(x^{512}+1)$	$\mathbf{Z}[x]/(x^{512}+1)$; $\{-1,0,1\}$; Pr 1, 2, 1; weight 128, 128
lac	192	Product	$(\mathbf{Z}/251)[x]/(x^{1024}+1)$	$\mathbf{Z}[x]/(x^{1024}+1)$; $\{-1,0,1\}$; Pr 1, 6, 1; weight 128, 128
lac	256	Product	$(\mathbf{Z}/251)[x]/(x^{1024}+1)$	$\mathbf{Z}[x]/(x^{1024}+1)$; $\{-1,0,1\}$; Pr 1, 2, 1; weight 256, 256
newhope	512	Product	$(\mathbf{Z}/12289)[x]/(x^{512}+1)$	$\mathbf{Z}[x]/(x^{512}+1)$; $\sum_{0\le i<16}\{-0.5,0.5\}$
newhope	1024	Product	$(\mathbf{Z}/12289)[x]/(x^{1024}+1)$	$\mathbf{Z}[x]/(x^{1024}+1)$; $\sum_{0\le i<16}\{-0.5,0.5\}$
ntru	hps2048509	Quotient	$(\mathbf{Z}/2048)[x]/(x^{509}-1)$	$\mathbf{Z}[x]/(x^{509}-1)$; $\{-1,0,1\}$
ntru	hps2048677	Quotient	$(\mathbf{Z}/2048)[x]/(x^{677}-1)$	$\mathbf{Z}[x]/(x^{677}-1)$; $\{-1,0,1\}$
ntru	hps4096821	Quotient	$(\mathbf{Z}/4096)[x]/(x^{821}-1)$	$\mathbf{Z}[x]/(x^{821}-1)$; $\{-1,0,1\}$
ntru	hrss701	Quotient	$(\mathbf{Z}/8192)[x]/(x^{701}-1)$	$\mathbf{Z}[x]/(x^{701}-1)$; $\{-1,0,1\}$; key correlation ≥ 0
ntrulpr	653	Product	$(\mathbf{Z}/4621)[x]/(x^{653}-x-1)$	$\mathbf{Z}[x]/(x^{653}-x-1)$; $\{-1,0,1\}$; weight 252
ntrulpr	761	Product	$(\mathbf{Z}/4591)[x]/(x^{761}-x-1)$	$\mathbf{Z}[x]/(x^{761}-x-1)$; $\{-1,0,1\}$; weight 250
ntrulpr	857	Product	$(\mathbf{Z}/5167)[x]/(x^{857}-x-1)$	$\mathbf{Z}[x]/(x^{857}-x-1)$; $\{-1,0,1\}$; weight 281
round5n1	1	Product	$(\mathbf{Z}/4096)^{636\times636}$	$\mathbf{Z}^{636\times8}$; $\{-1,0,1\}$; weight 57, 57
round5n1	3	Product	$(\mathbf{Z}/32768)^{876\times876}$	$\mathbf{Z}^{876\times8}$; $\{-1,0,1\}$; weight 223, 223
round5n1	5	Product	$(\mathbf{Z}/32768)^{1217\times1217}$	$\mathbf{Z}^{1217\times8}$; $\{-1,0,1\}$; weight 231, 231
round5nd	1.0d	Product	$(\mathbf{Z}/8192)[x]/(x^{586}+\ldots+1)$	$\mathbf{Z}[x]/(x^{586}+\ldots+1)$; $\{-1,0,1\}$; weight 91, 91
round5nd	3.0d	Product	$(\mathbf{Z}/4096)[x]/(x^{852}+\ldots+1)$	$\mathbf{Z}[x]/(x^{852}+\ldots+1)$; $\{-1,0,1\}$; weight 106, 106
round5nd	5.0d	Product	$(\mathbf{Z}/8192)[x]/(x^{1170}+\ldots+1)$	$\mathbf{Z}[x]/(x^{1170}+\ldots+1)$; $\{-1,0,1\}$; weight 111, 111
round5nd	1.5d	Product	$(\mathbf{Z}/1024)[x]/(x^{509}-1)$	$\mathbf{Z}[x]/(x^{509}-1)$; $\{-1,0,1\}$; weight 68, 68; ending 0
round5nd	3.5d	Product	$(\mathbf{Z}/4096)[x]/(x^{757}-1)$	$\mathbf{Z}[x]/(x^{757}-1)$; $\{-1,0,1\}$; weight 121, 121; ending 0
round5nd	5.5d	Product	$(\mathbf{Z}/2048)[x]/(x^{947}-1)$	$\mathbf{Z}[x]/(x^{947}-1)$; $\{-1,0,1\}$; weight 194, 194; ending 0
saber	light	Product	$((\mathbf{Z}/8192)[x]/(x^{256}+1))^{2\times2}$	$(\mathbf{Z}[x]/(x^{256}+1))^2$; $\sum_{0\le i<10}\{-0.5,0.5\}$
saber	main	Product	$((\mathbf{Z}/8192)[x]/(x^{256}+1))^{3\times3}$	$(\mathbf{Z}[x]/(x^{256}+1))^3$; $\sum_{0\le i<8}\{-0.5,0.5\}$
saber	fire	Product	$((\mathbf{Z}/8192)[x]/(x^{256}+1))^{4\times4}$	$(\mathbf{Z}[x]/(x^{256}+1))^4$; $\sum_{0\le i<6}\{-0.5,0.5\}$
sntrup	653	Quotient	$(\mathbf{Z}/4621)[x]/(x^{653}-x-1)$	$\mathbf{Z}[x]/(x^{653}-x-1)$; $\{-1,0,1\}$; weight 288
sntrup	761	Quotient	$(\mathbf{Z}/4591)[x]/(x^{761}-x-1)$	$\mathbf{Z}[x]/(x^{761}-x-1)$; $\{-1,0,1\}$; weight 286
sntrup	857	Quotient	$(\mathbf{Z}/5167)[x]/(x^{857}-x-1)$	$\mathbf{Z}[x]/(x^{857}-x-1)$; $\{-1,0,1\}$; weight 322
threebears	baby	Product	$(\mathbf{Z}/(2^{3120}-2^{1560}-1))^{2\times2}$	$\mathbf{Z}^2$; $\sum_{0\le i<312} 2^{10i}\{-2,-1,0,1,2\}$; Pr 1, 32, 62, 32, 1; *
threebears	mama	Product	$(\mathbf{Z}/(2^{3120}-2^{1560}-1))^{3\times3}$	$\mathbf{Z}^3$; $\sum_{0\le i<312} 2^{10i}\{-1,0,1\}$; Pr 13, 38, 13; *
threebears	papa	Product	$(\mathbf{Z}/(2^{3120}-2^{1560}-1))^{4\times4}$	$\mathbf{Z}^4$; $\sum_{0\le i<312} 2^{10i}\{-1,0,1\}$; Pr 5, 22, 5; *

system	parameter set	type	set of multipliers	short element
frodo	640	Product	$(\mathbf{Z}/32768)^{640\times640}$	$\mathbf{Z}^{640\times8}$; $\{-12,\ldots,12\}$; Pr 1, 4, 17, ... (spec page 23)
frodo	976	Product	$(\mathbf{Z}/65536)^{976\times976}$	$\mathbf{Z}^{976\times8}$; $\{-10,\ldots,10\}$; Pr 1, 6, 29, ... (spec page 23)
frodo	1344	Product	$(\mathbf{Z}/65536)^{1344\times1344}$	$\mathbf{Z}^{1344\times8}$; $\{-6,\ldots,6\}$; Pr 2, 40, 364, ... (spec page 23)
kyber	512	Product	$((\mathbf{Z}/3329)[x]/(x^{256}+1))^{2\times2}$	$(\mathbf{Z}[x]/(x^{256}+1))^2$; $\sum_{0\le i<4}\{-0.5,0.5\}$
kyber	768	Product	$((\mathbf{Z}/3329)[x]/(x^{256}+1))^{3\times3}$	$(\mathbf{Z}[x]/(x^{256}+1))^3$; $\sum_{0\le i<4}\{-0.5,0.5\}$
kyber	1024	Product	$((\mathbf{Z}/3329)[x]/(x^{256}+1))^{4\times4}$	$(\mathbf{Z}[x]/(x^{256}+1))^4$; $\sum_{0\le i<4}\{-0.5,0.5\}$
lac	128	Product	$(\mathbf{Z}/251)[x]/(x^{512}+1)$	$\mathbf{Z}[x]/(x^{512}+1)$; $\{-1,0,1\}$; Pr 1, 2, 1; weight 128, 128
lac	192	Product	$(\mathbf{Z}/251)[x]/(x^{1024}+1)$	$\mathbf{Z}[x]/(x^{1024}+1)$; $\{-1,0,1\}$; Pr 1, 6, 1; weight 128, 128
lac	256	Product	$(\mathbf{Z}/251)[x]/(x^{1024}+1)$	$\mathbf{Z}[x]/(x^{1024}+1)$; $\{-1,0,1\}$; Pr 1, 2, 1; weight 256, 256
newhope	512	Product	$(\mathbf{Z}/12289)[x]/(x^{512}+1)$	$\mathbf{Z}[x]/(x^{512}+1)$; $\sum_{0\le i<16}\{-0.5,0.5\}$
newhope	1024	Product	$(\mathbf{Z}/12289)[x]/(x^{1024}+1)$	$\mathbf{Z}[x]/(x^{1024}+1)$; $\sum_{0\le i<16}\{-0.5,0.5\}$
ntru	hps2048509	Quotient	$(\mathbf{Z}/2048)[x]/(x^{509}-1)$	$\mathbf{Z}[x]/(x^{509}-1)$; $\{-1,0,1\}$
ntru	hps2048677	Quotient	$(\mathbf{Z}/2048)[x]/(x^{677}-1)$	$\mathbf{Z}[x]/(x^{677}-1)$; $\{-1,0,1\}$
ntru	hps4096821	Quotient	$(\mathbf{Z}/4096)[x]/(x^{821}-1)$	$\mathbf{Z}[x]/(x^{821}-1)$; $\{-1,0,1\}$
ntru	hrss701	Quotient	$(\mathbf{Z}/8192)[x]/(x^{701}-1)$	$\mathbf{Z}[x]/(x^{701}-1)$; $\{-1,0,1\}$; key correlation ≥ 0
ntrulpr	653	Product	$(\mathbf{Z}/4621)[x]/(x^{653}-x-1)$	$\mathbf{Z}[x]/(x^{653}-x-1)$; $\{-1,0,1\}$; weight 252
ntrulpr	761	Product	$(\mathbf{Z}/4591)[x]/(x^{761}-x-1)$	$\mathbf{Z}[x]/(x^{761}-x-1)$; $\{-1,0,1\}$; weight 250
ntrulpr	857	Product	$(\mathbf{Z}/5167)[x]/(x^{857}-x-1)$	$\mathbf{Z}[x]/(x^{857}-x-1)$; $\{-1,0,1\}$; weight 281
round5n1	1	Product	$(\mathbf{Z}/4096)^{636\times636}$	$\mathbf{Z}^{636\times8}$; $\{-1,0,1\}$; weight 57, 57
round5n1	3	Product	$(\mathbf{Z}/32768)^{876\times876}$	$\mathbf{Z}^{876\times8}$; $\{-1,0,1\}$; weight 223, 223
round5n1	5	Product	$(\mathbf{Z}/32768)^{1217\times1217}$	$\mathbf{Z}^{1217\times8}$; $\{-1,0,1\}$; weight 231, 231
round5nd	1.0d	Product	$(\mathbf{Z}/8192)[x]/(x^{586}+\ldots+1)$	$\mathbf{Z}[x]/(x^{586}+\ldots+1)$; $\{-1,0,1\}$; weight 91, 91
round5nd	3.0d	Product	$(\mathbf{Z}/4096)[x]/(x^{852}+\ldots+1)$	$\mathbf{Z}[x]/(x^{852}+\ldots+1)$; $\{-1,0,1\}$; weight 106, 106
round5nd	5.0d	Product	$(\mathbf{Z}/8192)[x]/(x^{1170}+\ldots+1)$	$\mathbf{Z}[x]/(x^{1170}+\ldots+1)$; $\{-1,0,1\}$; weight 111, 111
round5nd	1.5d	Product	$(\mathbf{Z}/1024)[x]/(x^{509}-1)$	$\mathbf{Z}[x]/(x^{509}-1)$; $\{-1,0,1\}$; weight 68, 68; ending 0
round5nd	3.5d	Product	$(\mathbf{Z}/4096)[x]/(x^{757}-1)$	$\mathbf{Z}[x]/(x^{757}-1)$; $\{-1,0,1\}$; weight 121, 121; ending 0
round5nd	5.5d	Product	$(\mathbf{Z}/2048)[x]/(x^{947}-1)$	$\mathbf{Z}[x]/(x^{947}-1)$; $\{-1,0,1\}$; weight 194, 194; ending 0
saber	light	Product	$((\mathbf{Z}/8192)[x]/(x^{256}+1))^{2\times2}$	$(\mathbf{Z}[x]/(x^{256}+1))^2$; $\sum_{0\le i<10}\{-0.5,0.5\}$
saber	main	Product	$((\mathbf{Z}/8192)[x]/(x^{256}+1))^{3\times3}$	$(\mathbf{Z}[x]/(x^{256}+1))^3$; $\sum_{0\le i<8}\{-0.5,0.5\}$
saber	fire	Product	$((\mathbf{Z}/8192)[x]/(x^{256}+1))^{4\times4}$	$(\mathbf{Z}[x]/(x^{256}+1))^4$; $\sum_{0\le i<6}\{-0.5,0.5\}$
sntrup	653	Quotient	$(\mathbf{Z}/4621)[x]/(x^{653}-x-1)$	$\mathbf{Z}[x]/(x^{653}-x-1)$; $\{-1,0,1\}$; weight 288
sntrup	761	Quotient	$(\mathbf{Z}/4591)[x]/(x^{761}-x-1)$	$\mathbf{Z}[x]/(x^{761}-x-1)$; $\{-1,0,1\}$; weight 286
sntrup	857	Quotient	$(\mathbf{Z}/5167)[x]/(x^{857}-x-1)$	$\mathbf{Z}[x]/(x^{857}-x-1)$; $\{-1,0,1\}$; weight 322
threebears	baby	Product	$(\mathbf{Z}/(2^{3120}-2^{1560}-1))^{2\times2}$	$\mathbf{Z}^2$; $\sum_{0\le i<312}2^{10i}\{-2,-1,0,1,2\}$; Pr 1, 32, 62, 32, 1; *
threebears	mama	Product	$(\mathbf{Z}/(2^{3120}-2^{1560}-1))^{3\times3}$	$\mathbf{Z}^3$; $\sum_{0\le i<312}2^{10i}\{-1,0,1\}$; Pr 13, 38, 13; *
threebears	papa	Product	$(\mathbf{Z}/(2^{3120}-2^{1560}-1))^{4\times4}$	$\mathbf{Z}^4$; $\sum_{0\le i<312}2^{10i}\{-1,0,1\}$; Pr 5, 22, 5; *

eter set	type	set of multipliers
640	Product	$(\mathbf{Z}/32768)^{640\times 640}$
976	Product	$(\mathbf{Z}/65536)^{976\times 976}$
1344	Product	$(\mathbf{Z}/65536)^{1344\times 1344}$
512	Product	$((\mathbf{Z}/3329)[x]/(x^{256}+1))^{2\times 2}$
768	Product	$((\mathbf{Z}/3329)[x]/(x^{256}+1))^{3\times 3}$
1024	Product	$((\mathbf{Z}/3329)[x]/(x^{256}+1))^{4\times 4}$
128	Product	$(\mathbf{Z}/251)[x]/(x^{512}+1)$
192	Product	$(\mathbf{Z}/251)[x]/(x^{1024}+1)$
256	Product	$(\mathbf{Z}/251)[x]/(x^{1024}+1)$
512	Product	$(\mathbf{Z}/12289)[x]/(x^{512}+1)$
1024	Product	$(\mathbf{Z}/12289)[x]/(x^{1024}+1)$
048509	Quotient	$(\mathbf{Z}/2048)[x]/(x^{509}-1)$
048677	Quotient	$(\mathbf{Z}/2048)[x]/(x^{677}-1)$
096821	Quotient	$(\mathbf{Z}/4096)[x]/(x^{821}-1)$
rss701	Quotient	$(\mathbf{Z}/8192)[x]/(x^{701}-1)$
653	Product	$(\mathbf{Z}/4621)[x]/(x^{653}-x-1)$
761	Product	$(\mathbf{Z}/4591)[x]/(x^{761}-x-1)$
857	Product	$(\mathbf{Z}/5167)[x]/(x^{857}-x-1)$
1	Product	$(\mathbf{Z}/4096)^{636\times 636}$
3	Product	$(\mathbf{Z}/32768)^{876\times 876}$
5	Product	$(\mathbf{Z}/32768)^{1217\times 1217}$
1.0d	Product	$(\mathbf{Z}/8192)[x]/(x^{586}+\ldots+1)$
3.0d	Product	$(\mathbf{Z}/4096)[x]/(x^{852}+\ldots+1)$
5.0d	Product	$(\mathbf{Z}/8192)[x]/(x^{1170}+\ldots+1)$
1.5d	Product	$(\mathbf{Z}/1024)[x]/(x^{509}-1)$
3.5d	Product	$(\mathbf{Z}/4096)[x]/(x^{757}-1)$
5.5d	Product	$(\mathbf{Z}/2048)[x]/(x^{947}-1)$
light	Product	$((\mathbf{Z}/8192)[x]/(x^{256}+1))^{2\times 2}$
main	Product	$((\mathbf{Z}/8192)[x]/(x^{256}+1))^{3\times 3}$
fire	Product	$((\mathbf{Z}/8192)[x]/(x^{256}+1))^{4\times 4}$
653	Quotient	$(\mathbf{Z}/4621)[x]/(x^{653}-x-1)$
761	Quotient	$(\mathbf{Z}/4591)[x]/(x^{761}-x-1)$
857	Quotient	$(\mathbf{Z}/5167)[x]/(x^{857}-x-1)$
baby	Product	$(\mathbf{Z}/(2^{3120}-2^{1560}-1))^{2\times 2}$
mama	Product	$(\mathbf{Z}/(2^{3120}-2^{1560}-1))^{3\times 3}$
papa	Product	$(\mathbf{Z}/(2^{3120}-2^{1560}-1))^{4\times 4}$

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

key offset (nume
$\mathbf{Z}^{640\times 8}$; $\{-12,\ldots$
$\mathbf{Z}^{976\times 8}$; $\{-10,\ldots$
$\mathbf{Z}^{1344\times 8}$; $\{-6,\ldots$
$(\mathbf{Z}[x]/(x^{256}+1$
$(\mathbf{Z}[x]/(x^{256}+1$
$(\mathbf{Z}[x]/(x^{256}+1$
$\mathbf{Z}[x]/(x^{512}+1)$;
$\mathbf{Z}[x]/(x^{1024}+1$
$\mathbf{Z}[x]/(x^{1024}+1$
$\mathbf{Z}[x]/(x^{512}+1)$;
$\mathbf{Z}[x]/(x^{1024}+1$
$\mathbf{Z}[x]/(x^{509}-1)$;
$\mathbf{Z}[x]/(x^{677}-1)$;
$\mathbf{Z}[x]/(x^{821}-1)$;
$\mathbf{Z}[x]/(x^{701}-1)$;
round $\{-2310,\ldots$
round $\{-2295,\ldots$
round $\{-2583,\ldots$
round $\mathbf{Z}/4096$ to
round $\mathbf{Z}/32768$ t
round $\mathbf{Z}/32768$ t
round $\mathbf{Z}/8192$ to
round $\mathbf{Z}/4096$ to
round $\mathbf{Z}/8192$ to
reduce mod x^{508}
reduce mod x^{756}
reduce mod x^{946}
round $\mathbf{Z}/8192$ to
round $\mathbf{Z}/8192$ to
round $\mathbf{Z}/8192$ to
$\mathbf{Z}[x]/(x^{653}-x$
$\mathbf{Z}[x]/(x^{761}-x$
$\mathbf{Z}[x]/(x^{857}-x$
$\mathbf{Z}^2$; $\sum_{0\le i<312}2$
$\mathbf{Z}^3$; $\sum_{0\le i<312}2$
$\mathbf{Z}^4$; $\sum_{0\le i<312}2$

set of multipliers

$(\mathbf{Z}/32768)^{640\times 640}$
$(\mathbf{Z}/65536)^{976\times 976}$
$(\mathbf{Z}/65536)^{1344\times 1344}$
$((\mathbf{Z}/3329)[x]/(x^{256}+1))^{2\times 2}$
$((\mathbf{Z}/3329)[x]/(x^{256}+1))^{3\times 3}$
$((\mathbf{Z}/3329)[x]/(x^{256}+1))^{4\times 4}$
$(\mathbf{Z}/251)[x]/(x^{512}+1)$
$(\mathbf{Z}/251)[x]/(x^{1024}+1)$
$(\mathbf{Z}/251)[x]/(x^{1024}+1)$
$(\mathbf{Z}/12289)[x]/(x^{512}+1)$
$(\mathbf{Z}/12289)[x]/(x^{1024}+1)$
$(\mathbf{Z}/2048)[x]/(x^{509}-1)$
$(\mathbf{Z}/2048)[x]/(x^{677}-1)$
$(\mathbf{Z}/4096)[x]/(x^{821}-1)$
$(\mathbf{Z}/8192)[x]/(x^{701}-1)$
$(\mathbf{Z}/4621)[x]/(x^{653}-x-1)$
$(\mathbf{Z}/4591)[x]/(x^{761}-x-1)$
$(\mathbf{Z}/5167)[x]/(x^{857}-x-1)$
$(\mathbf{Z}/4096)^{636\times 636}$
$(\mathbf{Z}/32768)^{876\times 876}$
$(\mathbf{Z}/32768)^{1217\times 1217}$
$(\mathbf{Z}/8192)[x]/(x^{586}+\ldots+1)$
$(\mathbf{Z}/4096)[x]/(x^{852}+\ldots+1)$
$(\mathbf{Z}/8192)[x]/(x^{1170}+\ldots+1)$
$(\mathbf{Z}/1024)[x]/(x^{509}-1)$
$(\mathbf{Z}/4096)[x]/(x^{757}-1)$
$(\mathbf{Z}/2048)[x]/(x^{947}-1)$
$((\mathbf{Z}/8192)[x]/(x^{256}+1))^{2\times 2}$
$((\mathbf{Z}/8192)[x]/(x^{256}+1))^{3\times 3}$
$((\mathbf{Z}/8192)[x]/(x^{256}+1))^{4\times 4}$
$(\mathbf{Z}/4621)[x]/(x^{653}-x-1)$
$(\mathbf{Z}/4591)[x]/(x^{761}-x-1)$
$(\mathbf{Z}/5167)[x]/(x^{857}-x-1)$
$(\mathbf{Z}/(2^{3120}-2^{1560}-1))^{2\times 2}$
$(\mathbf{Z}/(2^{3120}-2^{1560}-1))^{3\times 3}$
$(\mathbf{Z}/(2^{3120}-2^{1560}-1))^{4\times 4}$

short element

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

key offset (numerator or noise or rou

$\mathbf{Z}^{640\times 8}$; $\{-12,\ldots,12\}$; Pr $1,4,17,$.
$\mathbf{Z}^{976\times 8}$; $\{-10,\ldots,10\}$; Pr $1,6,29,$.
$\mathbf{Z}^{1344\times 8}$; $\{-6,\ldots,6\}$; Pr $2,40,364,$
$(\mathbf{Z}[x]/(x^{256}+1))^2$; $\sum_{0\le i<4}\{-0.5,$
$(\mathbf{Z}[x]/(x^{256}+1))^3$; $\sum_{0\le i<4}\{-0.5,$
$(\mathbf{Z}[x]/(x^{256}+1))^4$; $\sum_{0\le i<4}\{-0.5,$
$\mathbf{Z}[x]/(x^{512}+1)$; $\{-1,0,1\}$; Pr $1,2,$
$\mathbf{Z}[x]/(x^{1024}+1)$; $\{-1,0,1\}$; Pr 1, 6
$\mathbf{Z}[x]/(x^{1024}+1)$; $\{-1,0,1\}$; Pr 1, 2
$\mathbf{Z}[x]/(x^{512}+1)$; $\sum_{0\le i<16}\{-0.5,0.5$
$\mathbf{Z}[x]/(x^{1024}+1)$; $\sum_{0\le i<16}\{-0.5,0.$
$\mathbf{Z}[x]/(x^{509}-1)$; $\{-1,0,1\}$; weight
$\mathbf{Z}[x]/(x^{677}-1)$; $\{-1,0,1\}$; weight
$\mathbf{Z}[x]/(x^{821}-1)$; $\{-1,0,1\}$; weight
$\mathbf{Z}[x]/(x^{701}-1)$; $\{-1,0,1\}$; key corr
round $\{-2310,\ldots,2310\}$ to $3\mathbf{Z}$
round $\{-2295,\ldots,2295\}$ to $3\mathbf{Z}$
round $\{-2583,\ldots,2583\}$ to $3\mathbf{Z}$
round $\mathbf{Z}/4096$ to $8\mathbf{Z}$
round $\mathbf{Z}/32768$ to $16\mathbf{Z}$
round $\mathbf{Z}/32768$ to $8\mathbf{Z}$
round $\mathbf{Z}/8192$ to $16\mathbf{Z}$
round $\mathbf{Z}/4096$ to $8\mathbf{Z}$
round $\mathbf{Z}/8192$ to $16\mathbf{Z}$
reduce mod $x^{508}+\ldots+1$; round $\mathbf{Z}$
reduce mod $x^{756}+\ldots+1$; round $\mathbf{Z}$
reduce mod $x^{946}+\ldots+1$; round $\mathbf{Z}$
round $\mathbf{Z}/8192$ to $8\mathbf{Z}$
round $\mathbf{Z}/8192$ to $8\mathbf{Z}$
round $\mathbf{Z}/8192$ to $8\mathbf{Z}$
$\mathbf{Z}[x]/(x^{653}-x-1)$; $\{-1,0,1\}$; inve
$\mathbf{Z}[x]/(x^{761}-x-1)$; $\{-1,0,1\}$; inve
$\mathbf{Z}[x]/(x^{857}-x-1)$; $\{-1,0,1\}$; inve
$\mathbf{Z}^2$; $\sum_{0\le i<312}2^{10i}\{-2,-1,0,1,2\}$;
$\mathbf{Z}^3$; $\sum_{0\le i<312}2^{10i}\{-1,0,1\}$; Pr 13,
$\mathbf{Z}^4$; $\sum_{0\le i<312}2^{10i}\{-1,0,1\}$; Pr 5, 2

$+1))^{2\times 2}$
$+1))^{3\times 3}$
$+1))^{4\times 4}$
$1)$
$+1)$
$+1)$
$+1)$
$^4+1)$
$-1)$
$-1)$
$-1)$
$-1)$
$-x-1)$
$-x-1)$
$-x-1)$
$+\ldots+1)$
$+\ldots+1)$
$+\ldots+1)$
$-1)$
$-1)$
$-1)$
$+1))^{2\times 2}$
$+1))^{3\times 3}$
$+1))^{4\times 4}$
$-x-1)$
$-x-1)$
$-x-1)$
$-1))^{2\times 2}$
$-1))^{3\times 3}$
$-1))^{4\times 4}$

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

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

short element

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

key offset (numerator or noise or rounding method)

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

$\ldots, 12\}$; Pr $1, 4, 17, \ldots$ (spec page 23)
$\ldots, 10\}$; Pr $1, 6, 29, \ldots$ (spec page 23)
$\ldots, 6\}$; Pr $2, 40, 364, \ldots$ (spec page 23)
$))^2$; $\sum_{0\le i<4}\{-0.5, 0.5\}$
$))^3$; $\sum_{0\le i<4}\{-0.5, 0.5\}$
$))^4$; $\sum_{0\le i<4}\{-0.5, 0.5\}$
$\{-1, 0, 1\}$; Pr $1, 2, 1$; weight $128, 128$
$)$; $\{-1, 0, 1\}$; Pr $1, 6, 1$; weight $128, 128$
$)$; $\{-1, 0, 1\}$; Pr $1, 2, 1$; weight $256, 256$
$\sum_{0\le i<16}\{-0.5, 0.5\}$
$)$; $\sum_{0\le i<16}\{-0.5, 0.5\}$
$\{-1, 0, 1\}$
$\{-1, 0, 1\}$
$\{-1, 0, 1\}$
$\{-1, 0, 1\}$; key correlation ≥ 0
$-1)$; $\{-1, 0, 1\}$; weight 252
$-1)$; $\{-1, 0, 1\}$; weight 250
$-1)$; $\{-1, 0, 1\}$; weight 281
$1\}$; weight $57, 57$
$1\}$; weight $223, 223$
$1\}$; weight $231, 231$
$+1)$; $\{-1, 0, 1\}$; weight $91, 91$
$+1)$; $\{-1, 0, 1\}$; weight $106, 106$
$.+1)$; $\{-1, 0, 1\}$; weight $111, 111$
$\{-1, 0, 1\}$; weight $68, 68$; ending 0
$\{-1, 0, 1\}$; weight $121, 121$; ending 0
$\{-1, 0, 1\}$; weight $194, 194$; ending 0
$))^2$; $\sum_{0\le i<10}\{-0.5, 0.5\}$
$))^3$; $\sum_{0\le i<8}\{-0.5, 0.5\}$
$))^4$; $\sum_{0\le i<6}\{-0.5, 0.5\}$
$-1)$; $\{-1, 0, 1\}$; weight 288
$-1)$; $\{-1, 0, 1\}$; weight 286
$-1)$; $\{-1, 0, 1\}$; weight 322
${}^{0i}\{-2, -1, 0, 1, 2\}$; Pr $1, 32, 62, 32, 1$; *
${}^{0i}\{-1, 0, 1\}$; Pr $13, 38, 13$; *
${}^{0i}\{-1, 0, 1\}$; Pr $5, 22, 5$; *

key offset (numerator or noise or rounding method)

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

ciphertext offset

$\mathbf{Z}^{8\times 8}$; $\{-12, \ldots$
$\mathbf{Z}^{8\times 8}$; $\{-10, \ldots$
$\mathbf{Z}^{8\times 8}$; $\{-6, \ldots,$
$\mathbf{Z}[x]/(x^{256}+1)$;
$\mathbf{Z}[x]/(x^{256}+1)$;
$\mathbf{Z}[x]/(x^{256}+1)$;
$\mathbf{Z}[x]/(x^{512}+1)$;
$\mathbf{Z}[x]/(x^{1024}+1$
$\mathbf{Z}[x]/(x^{1024}+1$
$\mathbf{Z}[x]/(x^{512}+1)$;
$\mathbf{Z}[x]/(x^{1024}+1$
not applicable
not applicable
not applicable
not applicable
bottom 256 coef
bottom 256 coef
bottom 256 coef
round $\mathbf{Z}/4096$ to
round $\mathbf{Z}/32768$ t
round $\mathbf{Z}/32768$ t
bottom 128 coef
bottom 192 coef
bottom 256 coef
bottom 318 coef
bottom 410 coef
bottom 490 coef
round $\mathbf{Z}/8192$ to
round $\mathbf{Z}/8192$ to
round $\mathbf{Z}/8192$ to
not applicable
not applicable
not applicable
$\mathbf{Z}$; $\sum_{0\le i<312} 2^{10}$
$\mathbf{Z}$; $\sum_{0\le i<312} 2^{10}$
$\mathbf{Z}$; $\sum_{0\le i<312} 2^{10}$

. . (spec page 23)
. . (spec page 23)
. . . (spec page 23)
$0.5\}$
$0.5\}$
$0.5\}$
1; weight 128, 128
, 1; weight 128, 128
, 1; weight 256, 256
$5\}$
$.5\}$

relation ≥ 0
ght 252
ght 250
ght 281

eight 91, 91
eight 106, 106
veight 111, 111
68, 68; ending 0
121, 121; ending 0
194, 194; ending 0
$0.5\}$
$0.5\}$
$0.5\}$
ght 288
ght 286
ght 322
Pr 1, 32, 62, 32, 1; *
38, 13; *
22, 5; *

key offset (numerator or noise or rounding method)

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

ciphertext offset (noise or rounding r

$\mathbf{Z}^{8\times 8}$; $\{-12,\ldots,12\}$; Pr $1,4,17,\ldots$
$\mathbf{Z}^{8\times 8}$; $\{-10,\ldots,10\}$; Pr $1,6,29,\ldots$
$\mathbf{Z}^{8\times 8}$; $\{-6,\ldots,6\}$; Pr $2,40,364,\ldots$
$\mathbf{Z}[x]/(x^{256}+1)$; $\sum_{0\leq i<4}\{-0.5,0.5$
$\mathbf{Z}[x]/(x^{256}+1)$; $\sum_{0\leq i<4}\{-0.5,0.5$
$\mathbf{Z}[x]/(x^{256}+1)$; $\sum_{0\leq i<4}\{-0.5,0.5$
$\mathbf{Z}[x]/(x^{512}+1)$; $\{-1,0,1\}$; Pr 1, 2,
$\mathbf{Z}[x]/(x^{1024}+1)$; $\{-1,0,1\}$; Pr 1, 6
$\mathbf{Z}[x]/(x^{1024}+1)$; $\{-1,0,1\}$; Pr 1, 2
$\mathbf{Z}[x]/(x^{512}+1)$; $\sum_{0\leq i<16}\{-0.5,0.5$
$\mathbf{Z}[x]/(x^{1024}+1)$; $\sum_{0\leq i<16}\{-0.5,0.$
not applicable
not applicable
not applicable
not applicable
bottom 256 coeffs; $z\mapsto\lfloor(114(z+2$
bottom 256 coeffs; $z\mapsto\lfloor(113(z+2$
bottom 256 coeffs; $z\mapsto\lfloor(101(z+2$
round $\mathbf{Z}/4096$ to $64\mathbf{Z}$
round $\mathbf{Z}/32768$ to $512\mathbf{Z}$
round $\mathbf{Z}/32768$ to $64\mathbf{Z}$
bottom 128 coeffs; round $\mathbf{Z}/8192$ to
bottom 192 coeffs; round $\mathbf{Z}/4096$ to
bottom 256 coeffs; round $\mathbf{Z}/8192$ to
bottom 318 coeffs; round $\mathbf{Z}/1024$ to
bottom 410 coeffs; round $\mathbf{Z}/4096$ to
bottom 490 coeffs; round $\mathbf{Z}/2048$ to
round $\mathbf{Z}/8192$ to $1024\mathbf{Z}$
round $\mathbf{Z}/8192$ to $512\mathbf{Z}$
round $\mathbf{Z}/8192$ to $128\mathbf{Z}$
not applicable
not applicable
not applicable
$\mathbf{Z}$; $\sum_{0\leq i<312} 2^{10i}\{-2,-1,0,1,2\}$; P
$\mathbf{Z}$; $\sum_{0\leq i<312} 2^{10i}\{-1,0,1\}$; Pr 13, 3
$\mathbf{Z}$; $\sum_{0\leq i<312} 2^{10i}\{-1,0,1\}$; Pr 5, 22

key offset (numerator or noise or rounding method)

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

ciphertext offset (noise or rounding method)

$\mathbf{Z}^{8\times 8}$; $\{-12,\ldots,12\}$; Pr $1,4,17,\ldots$ (spec page 23)
$\mathbf{Z}^{8\times 8}$; $\{-10,\ldots,10\}$; Pr $1,6,29,\ldots$ (spec page 23)
$\mathbf{Z}^{8\times 8}$; $\{-6,\ldots,6\}$; Pr $2,40,364,\ldots$ (spec page 23)
$\mathbf{Z}[x]/(x^{256}+1)$; $\sum_{0\le i<4}\{-0.5,0.5\}$
$\mathbf{Z}[x]/(x^{256}+1)$; $\sum_{0\le i<4}\{-0.5,0.5\}$
$\mathbf{Z}[x]/(x^{256}+1)$; $\sum_{0\le i<4}\{-0.5,0.5\}$
$\mathbf{Z}[x]/(x^{512}+1)$; $\{-1,0,1\}$; Pr $1,2,1$
$\mathbf{Z}[x]/(x^{1024}+1)$; $\{-1,0,1\}$; Pr $1,6,1$
$\mathbf{Z}[x]/(x^{1024}+1)$; $\{-1,0,1\}$; Pr $1,2,1$
$\mathbf{Z}[x]/(x^{512}+1)$; $\sum_{0\le i<16}\{-0.5,0.5\}$
$\mathbf{Z}[x]/(x^{1024}+1)$; $\sum_{0\le i<16}\{-0.5,0.5\}$
not applicable
not applicable
not applicable
not applicable
bottom 256 coeffs; $z\mapsto\lfloor(114(z+2156)+16384)/3276$
bottom 256 coeffs; $z\mapsto\lfloor(113(z+2175)+16384)/3276$
bottom 256 coeffs; $z\mapsto\lfloor(101(z+2433)+16384)/3276$
round $\mathbf{Z}/4096$ to $64\mathbf{Z}$
round $\mathbf{Z}/32768$ to $512\mathbf{Z}$
round $\mathbf{Z}/32768$ to $64\mathbf{Z}$
bottom 128 coeffs; round $\mathbf{Z}/8192$ to $512\mathbf{Z}$
bottom 192 coeffs; round $\mathbf{Z}/4096$ to $128\mathbf{Z}$
bottom 256 coeffs; round $\mathbf{Z}/8192$ to $256\mathbf{Z}$
bottom 318 coeffs; round $\mathbf{Z}/1024$ to $64\mathbf{Z}$
bottom 410 coeffs; round $\mathbf{Z}/4096$ to $512\mathbf{Z}$
bottom 490 coeffs; round $\mathbf{Z}/2048$ to $64\mathbf{Z}$
round $\mathbf{Z}/8192$ to $1024\mathbf{Z}$
round $\mathbf{Z}/8192$ to $512\mathbf{Z}$
round $\mathbf{Z}/8192$ to $128\mathbf{Z}$
not applicable
not applicable
not applicable
$\mathbf{Z}$; $\sum_{0\le i<312}2^{10i}\{-2,-1,0,1,2\}$; Pr $1,32,62,32,1$; *
$\mathbf{Z}$; $\sum_{0\le i<312}2^{10i}\{-1,0,1\}$; Pr $13,38,13$; *
$\mathbf{Z}$; $\sum_{0\le i<312}2^{10i}\{-1,0,1\}$; Pr $5,22,5$; *

key offset (numerator or noise or rounding method)

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

ciphertext offset (noise or rounding method)

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

rator or noise or rounding method)

. . . , 12}; Pr $1, 4, 17, \ldots$ (spec page 23)
. . . , 10}; Pr $1, 6, 29, \ldots$ (spec page 23)
. . , 6}; Pr $2, 40, 364, \ldots$ (spec page 23)
$))^2$; $\sum_{0 \le i < 4}\{-0.5, 0.5\}$
$))^3$; $\sum_{0 \le i < 4}\{-0.5, 0.5\}$
$))^4$; $\sum_{0 \le i < 4}\{-0.5, 0.5\}$
$\{-1, 0, 1\}$; Pr $1, 2, 1$; weight $128, 128$
); $\{-1, 0, 1\}$; Pr $1, 6, 1$; weight $128, 128$
); $\{-1, 0, 1\}$; Pr $1, 2, 1$; weight $256, 256$
$\sum_{0 \le i < 16}\{-0.5, 0.5\}$
); $\sum_{0 \le i < 16}\{-0.5, 0.5\}$
$\{-1, 0, 1\}$; weight $127, 127$
$\{-1, 0, 1\}$; weight $127, 127$
$\{-1, 0, 1\}$; weight $255, 255$
$\{-1, 0, 1\}$; key correlation ≥ 0; $\cdot(x-1)$
. . . , 2310} to $3\mathbf{Z}$
. . . , 2295} to $3\mathbf{Z}$
. . . , 2583} to $3\mathbf{Z}$
o $8\mathbf{Z}$
to $16\mathbf{Z}$
to $8\mathbf{Z}$
o $16\mathbf{Z}$
o $8\mathbf{Z}$
o $16\mathbf{Z}$
$+ \ldots + 1$; round $\mathbf{Z}/1024$ to $8\mathbf{Z}$
$+ \ldots + 1$; round $\mathbf{Z}/4096$ to $16\mathbf{Z}$
$+ \ldots + 1$; round $\mathbf{Z}/2048$ to $8\mathbf{Z}$
o $8\mathbf{Z}$
o $8\mathbf{Z}$
o $8\mathbf{Z}$
$-1)$; $\{-1, 0, 1\}$; invertible mod 3
$-1)$; $\{-1, 0, 1\}$; invertible mod 3
$-1)$; $\{-1, 0, 1\}$; invertible mod 3
$^{10i}\{-2, -1, 0, 1, 2\}$; Pr $1, 32, 62, 32, 1$; *
$^{10i}\{-1, 0, 1\}$; Pr $13, 38, 13$; *
$^{10i}\{-1, 0, 1\}$; Pr $5, 22, 5$; *

ciphertext offset (noise or rounding method)

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

set of encoded m

8×8 matrix ove
8×8 matrix ove
8×8 matrix ove
$\sum_{0 \le i < 256}\{0, 16$
$\sum_{0 \le i < 256}\{0, 16$
$\sum_{0 \le i < 256}\{0, 16$
256-dim subcode
256-dim subcode
256-dim subcode
$\sum_{0 \le i < 256}\{0, 61$
$\sum_{0 \le i < 256}\{0, 61$
not applicable
not applicable
not applicable
not applicable
$\sum_{0 \le i < 256}\{0, 23$
$\sum_{0 \le i < 256}\{0, 22$
$\sum_{0 \le i < 256}\{0, 25$
8×8 matrix ove
8×8 matrix ove
8×8 matrix ove
$\sum_{0 \le i < 128}\{0, 40$
$\sum_{0 \le i < 192}\{0, 20$
$\sum_{0 \le i < 256}\{0, 40$
128-dim subcode
192-dim subcode
256-dim subcode
$\sum_{0 \le i < 256}\{0, 40$
$\sum_{0 \le i < 256}\{0, 40$
$\sum_{0 \le i < 256}\{0, 40$
not applicable
not applicable
not applicable
256-dim subcode
256-dim subcode
256-dim subcode

nding method)
. . (spec page 23)
. . (spec page 23)
. . . (spec page 23)
0.5}
0.5}
0.5}
1; weight 128, 128
, 1; weight 128, 128
, 1; weight 256, 256
5}
.5}
127, 127
127, 127
255, 255
relation ≥ 0; $\cdot(x-1)$
/1024 to 8**Z**
/4096 to 16**Z**
/2048 to 8**Z**
ertible mod 3
ertible mod 3
ertible mod 3
Pr 1, 32, 62, 32, 1; *
38, 13; *
22, 5; *

ciphertext offset (noise or rounding method)

$\mathbf{Z}^{8\times8}$; $\{-12,\ldots,12\}$; Pr $1,4,17,\ldots$ (spec page 23)
$\mathbf{Z}^{8\times8}$; $\{-10,\ldots,10\}$; Pr $1,6,29,\ldots$ (spec page 23)
$\mathbf{Z}^{8\times8}$; $\{-6,\ldots,6\}$; Pr $2,40,364,\ldots$ (spec page 23)
$\mathbf{Z}[x]/(x^{256}+1)$; $\sum_{0\leq i<4}\{-0.5,0.5\}$
$\mathbf{Z}[x]/(x^{256}+1)$; $\sum_{0\leq i<4}\{-0.5,0.5\}$
$\mathbf{Z}[x]/(x^{256}+1)$; $\sum_{0\leq i<4}\{-0.5,0.5\}$
$\mathbf{Z}[x]/(x^{512}+1)$; $\{-1,0,1\}$; Pr 1, 2, 1
$\mathbf{Z}[x]/(x^{1024}+1)$; $\{-1,0,1\}$; Pr 1, 6, 1
$\mathbf{Z}[x]/(x^{1024}+1)$; $\{-1,0,1\}$; Pr 1, 2, 1
$\mathbf{Z}[x]/(x^{512}+1)$; $\sum_{0\leq i<16}\{-0.5,0.5\}$
$\mathbf{Z}[x]/(x^{1024}+1)$; $\sum_{0\leq i<16}\{-0.5,0.5\}$
not applicable
not applicable
not applicable
not applicable
bottom 256 coeffs; $z\mapsto\lfloor(114(z+2156)+16384)/32768\rfloor$
bottom 256 coeffs; $z\mapsto\lfloor(113(z+2175)+16384)/32768\rfloor$
bottom 256 coeffs; $z\mapsto\lfloor(101(z+2433)+16384)/32768\rfloor$
round $\mathbf{Z}/4096$ to $64\mathbf{Z}$
round $\mathbf{Z}/32768$ to $512\mathbf{Z}$
round $\mathbf{Z}/32768$ to $64\mathbf{Z}$
bottom 128 coeffs; round $\mathbf{Z}/8192$ to $512\mathbf{Z}$
bottom 192 coeffs; round $\mathbf{Z}/4096$ to $128\mathbf{Z}$
bottom 256 coeffs; round $\mathbf{Z}/8192$ to $256\mathbf{Z}$
bottom 318 coeffs; round $\mathbf{Z}/1024$ to $64\mathbf{Z}$
bottom 410 coeffs; round $\mathbf{Z}/4096$ to $512\mathbf{Z}$
bottom 490 coeffs; round $\mathbf{Z}/2048$ to $64\mathbf{Z}$
round $\mathbf{Z}/8192$ to $1024\mathbf{Z}$
round $\mathbf{Z}/8192$ to $512\mathbf{Z}$
round $\mathbf{Z}/8192$ to $128\mathbf{Z}$
not applicable
not applicable
not applicable
$\mathbf{Z}$; $\sum_{0\leq i<312}2^{10i}\{-2,-1,0,1,2\}$; Pr 1, 32, 62, 32, 1; *
$\mathbf{Z}$; $\sum_{0\leq i<312}2^{10i}\{-1,0,1\}$; Pr 13, 38, 13; *
$\mathbf{Z}$; $\sum_{0\leq i<312}2^{10i}\{-1,0,1\}$; Pr 5, 22, 5; *

set of encoded messages

8×8 matrix over $\{0,8192,16384,24$
8×8 matrix over $\{0,8192,\ldots,5734$
8×8 matrix over $\{0,4096,\ldots,6144$
$\sum_{0\leq i<256}\{0,1665\}x^i$
$\sum_{0\leq i<256}\{0,1665\}x^i$
$\sum_{0\leq i<256}\{0,1665\}x^i$
256-dim subcode (see spec) of $\sum_{0\leq}$
256-dim subcode (see spec) of $\sum_{0\leq}$
256-dim subcode (see spec) of $\sum_{0\leq}$
$\sum_{0\leq i<256}\{0,6145\}x^i(1+x^{256})$
$\sum_{0\leq i<256}\{0,6145\}x^i(1+x^{256}+x^5$
not applicable
not applicable
not applicable
not applicable
$\sum_{0\leq i<256}\{0,2310\}x^i$
$\sum_{0\leq i<256}\{0,2295\}x^i$
$\sum_{0\leq i<256}\{0,2583\}x^i$
8×8 matrix over $\{0,1024,2048,307$
8×8 matrix over $\{0,4096,\ldots,2867$
8×8 matrix over $\{0,2048,\ldots,3072$
$\sum_{0\leq i<128}\{0,4096\}x^i$
$\sum_{0\leq i<192}\{0,2048\}x^i$
$\sum_{0\leq i<256}\{0,4096\}x^i$
128-dim subcode (see spec) of $\sum_{0\leq}$
192-dim subcode (see spec) of $\sum_{0\leq}$
256-dim subcode (see spec) of $\sum_{0\leq}$
$\sum_{0\leq i<256}\{0,4096\}x^i$
$\sum_{0\leq i<256}\{0,4096\}x^i$
$\sum_{0\leq i<256}\{0,4096\}x^i$
not applicable
not applicable
not applicable
256-dim subcode (see spec) of $\sum_{0\leq}$
256-dim subcode (see spec) of $\sum_{0\leq}$
256-dim subcode (see spec) of $\sum_{0\leq}$

7	8
ciphertext offset (noise or rounding method)	set of encoded messages
$\mathbf{Z}^{8\times 8}$; $\{-12,\dots,12\}$; Pr $1,4,17,\dots$ (spec page 23)	8×8 matrix over $\{0,8192,16384,24576\}$
$\mathbf{Z}^{8\times 8}$; $\{-10,\dots,10\}$; Pr $1,6,29,\dots$ (spec page 23)	8×8 matrix over $\{0,8192,\dots,57344\}$
$\mathbf{Z}^{8\times 8}$; $\{-6,\dots,6\}$; Pr $2,40,364,\dots$ (spec page 23)	8×8 matrix over $\{0,4096,\dots,61440\}$
$\mathbf{Z}[x]/(x^{256}+1)$; $\sum_{0\le i<4}\{-0.5,0.5\}$	$\sum_{0\le i<256}\{0,1665\}x^i$
$\mathbf{Z}[x]/(x^{256}+1)$; $\sum_{0\le i<4}\{-0.5,0.5\}$	$\sum_{0\le i<256}\{0,1665\}x^i$
$\mathbf{Z}[x]/(x^{256}+1)$; $\sum_{0\le i<4}\{-0.5,0.5\}$	$\sum_{0\le i<256}\{0,1665\}x^i$
$\mathbf{Z}[x]/(x^{512}+1)$; $\{-1,0,1\}$; Pr $1,2,1$	256-dim subcode (see spec) of $\sum_{0\le i<512}\{0,126\}x^i$
$\mathbf{Z}[x]/(x^{1024}+1)$; $\{-1,0,1\}$; Pr $1,6,1$	256-dim subcode (see spec) of $\sum_{0\le i<1024}\{0,126\}x^i$
$\mathbf{Z}[x]/(x^{1024}+1)$; $\{-1,0,1\}$; Pr $1,2,1$	256-dim subcode (see spec) of $\sum_{0\le i<1024}\{0,126\}x^i$
$\mathbf{Z}[x]/(x^{512}+1)$; $\sum_{0\le i<16}\{-0.5,0.5\}$	$\sum_{0\le i<256}\{0,6145\}x^i(1+x^{256})$
$\mathbf{Z}[x]/(x^{1024}+1)$; $\sum_{0\le i<16}\{-0.5,0.5\}$	$\sum_{0\le i<256}\{0,6145\}x^i(1+x^{256}+x^{512}+x^{768})$
not applicable	not applicable
not applicable	not applicable
not applicable	not applicable
not applicable	not applicable
bottom 256 coeffs; $z\mapsto\lfloor(114(z+2156)+16384)/32768\rfloor$	$\sum_{0\le i<256}\{0,2310\}x^i$
bottom 256 coeffs; $z\mapsto\lfloor(113(z+2175)+16384)/32768\rfloor$	$\sum_{0\le i<256}\{0,2295\}x^i$
bottom 256 coeffs; $z\mapsto\lfloor(101(z+2433)+16384)/32768\rfloor$	$\sum_{0\le i<256}\{0,2583\}x^i$
round $\mathbf{Z}/4096$ to $64\mathbf{Z}$	8×8 matrix over $\{0,1024,2048,3072\}$
round $\mathbf{Z}/32768$ to $512\mathbf{Z}$	8×8 matrix over $\{0,4096,\dots,28672\}$
round $\mathbf{Z}/32768$ to $64\mathbf{Z}$	8×8 matrix over $\{0,2048,\dots,30720\}$
bottom 128 coeffs; round $\mathbf{Z}/8192$ to $512\mathbf{Z}$	$\sum_{0\le i<128}\{0,4096\}x^i$
bottom 192 coeffs; round $\mathbf{Z}/4096$ to $128\mathbf{Z}$	$\sum_{0\le i<192}\{0,2048\}x^i$
bottom 256 coeffs; round $\mathbf{Z}/8192$ to $256\mathbf{Z}$	$\sum_{0\le i<256}\{0,4096\}x^i$
bottom 318 coeffs; round $\mathbf{Z}/1024$ to $64\mathbf{Z}$	128-dim subcode (see spec) of $\sum_{0\le i<318}\{0,512\}x^i$
bottom 410 coeffs; round $\mathbf{Z}/4096$ to $512\mathbf{Z}$	192-dim subcode (see spec) of $\sum_{0\le i<410}\{0,2048\}x^i$
bottom 490 coeffs; round $\mathbf{Z}/2048$ to $64\mathbf{Z}$	256-dim subcode (see spec) of $\sum_{0\le i<490}\{0,1024\}x^i$
round $\mathbf{Z}/8192$ to $1024\mathbf{Z}$	$\sum_{0\le i<256}\{0,4096\}x^i$
round $\mathbf{Z}/8192$ to $512\mathbf{Z}$	$\sum_{0\le i<256}\{0,4096\}x^i$
round $\mathbf{Z}/8192$ to $128\mathbf{Z}$	$\sum_{0\le i<256}\{0,4096\}x^i$
not applicable	not applicable
not applicable	not applicable
not applicable	not applicable
$\mathbf{Z}$; $\sum_{0\le i<312}2^{10i}\{-2,-1,0,1,2\}$; Pr $1,32,62,32,1$; *	256-dim subcode (see spec) of $\sum_{0\le i<274}\{0,512\}2^{10i}$
$\mathbf{Z}$; $\sum_{0\le i<312}2^{10i}\{-1,0,1\}$; Pr $13,38,13$; *	256-dim subcode (see spec) of $\sum_{0\le i<274}\{0,512\}2^{10i}$
$\mathbf{Z}$; $\sum_{0\le i<312}2^{10i}\{-1,0,1\}$; Pr $5,22,5$; *	256-dim subcode (see spec) of $\sum_{0\le i<274}\{0,512\}2^{10i}$

)

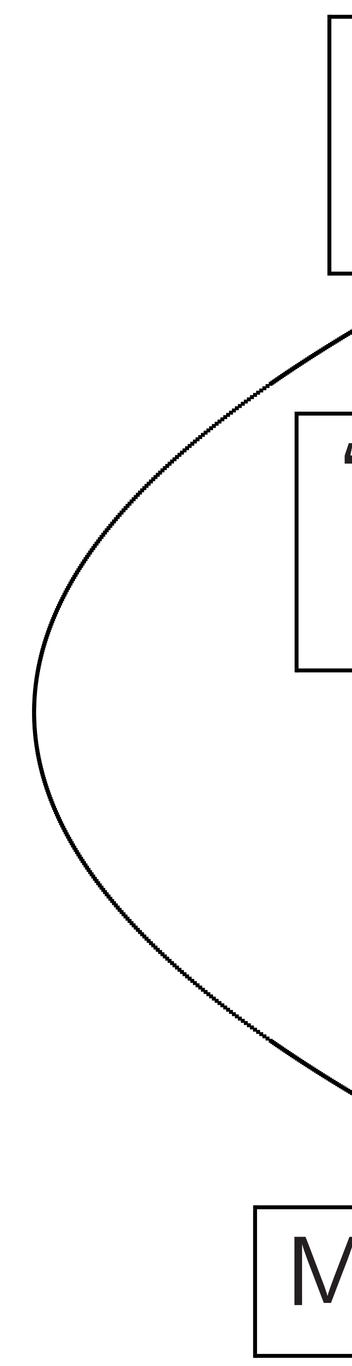
ciphertext offset (noise or rounding method)
$\mathbf{Z}^{8\times 8}$; $\{-12,\dots,12\}$; Pr $1, 4, 17, \dots$ (spec page 23)
$\mathbf{Z}^{8\times 8}$; $\{-10,\dots,10\}$; Pr $1, 6, 29, \dots$ (spec page 23)
$\mathbf{Z}^{8\times 8}$; $\{-6,\dots,6\}$; Pr $2, 40, 364, \dots$ (spec page 23)
$\mathbf{Z}[x]/(x^{256}+1)$;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

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

(noise or rounding method)	set of encoded messages
, 12}; Pr 1, 4, 17, . . . (spec page 23)	8×8 matrix over $\{0, 8192, 16384, 24576\}$
, 10}; Pr 1, 6, 29, . . . (spec page 23)	8×8 matrix over $\{0, 8192, \ldots, 57344\}$
6}; Pr 2, 40, 364, . . . (spec page 23)	8×8 matrix over $\{0, 4096, \ldots, 61440\}$
$\sum_{0 \le i < 4}\{-0.5, 0.5\}$	$\sum_{0 \le i < 256}\{0, 1665\}x^i$
$\sum_{0 \le i < 4}\{-0.5, 0.5\}$	$\sum_{0 \le i < 256}\{0, 1665\}x^i$
$\sum_{0 \le i < 4}\{-0.5, 0.5\}$	$\sum_{0 \le i < 256}\{0, 1665\}x^i$
$\{-1, 0, 1\}$; Pr 1, 2, 1	256-dim subcode (see spec) of $\sum_{0 \le i < 512}\{0, 126\}x^i$
); $\{-1, 0, 1\}$; Pr 1, 6, 1	256-dim subcode (see spec) of $\sum_{0 \le i < 1024}\{0, 126\}x^i$
); $\{-1, 0, 1\}$; Pr 1, 2, 1	256-dim subcode (see spec) of $\sum_{0 \le i < 1024}\{0, 126\}x^i$
$\sum_{0 \le i < 16}\{-0.5, 0.5\}$	$\sum_{0 \le i < 256}\{0, 6145\}x^i(1 + x^{256})$
); $\sum_{0 \le i < 16}\{-0.5, 0.5\}$	$\sum_{0 \le i < 256}\{0, 6145\}x^i(1 + x^{256} + x^{512} + x^{768})$
	not applicable
	not applicable
	not applicable
	not applicable
fs; $z \mapsto \lfloor(114(z + 2156) + 16384)/32768\rfloor$	$\sum_{0 \le i < 256}\{0, 2310\}x^i$
fs; $z \mapsto \lfloor(113(z + 2175) + 16384)/32768\rfloor$	$\sum_{0 \le i < 256}\{0, 2295\}x^i$
fs; $z \mapsto \lfloor(101(z + 2433) + 16384)/32768\rfloor$	$\sum_{0 \le i < 256}\{0, 2583\}x^i$
o 64**Z**	8×8 matrix over $\{0, 1024, 2048, 3072\}$
to 512**Z**	8×8 matrix over $\{0, 4096, \ldots, 28672\}$
to 64**Z**	8×8 matrix over $\{0, 2048, \ldots, 30720\}$
fs; round **Z**/8192 to 512**Z**	$\sum_{0 \le i < 128}\{0, 4096\}x^i$
fs; round **Z**/4096 to 128**Z**	$\sum_{0 \le i < 192}\{0, 2048\}x^i$
fs; round **Z**/8192 to 256**Z**	$\sum_{0 \le i < 256}\{0, 4096\}x^i$
fs; round **Z**/1024 to 64**Z**	128-dim subcode (see spec) of $\sum_{0 \le i < 318}\{0, 512\}x^i$
fs; round **Z**/4096 to 512**Z**	192-dim subcode (see spec) of $\sum_{0 \le i < 410}\{0, 2048\}x^i$
fs; round **Z**/2048 to 64**Z**	256-dim subcode (see spec) of $\sum_{0 \le i < 490}\{0, 1024\}x^i$
o 1024**Z**	$\sum_{0 \le i < 256}\{0, 4096\}x^i$
o 512**Z**	$\sum_{0 \le i < 256}\{0, 4096\}x^i$
o 128**Z**	$\sum_{0 \le i < 256}\{0, 4096\}x^i$
	not applicable
	not applicable
	not applicable
$^{i}\{-2, -1, 0, 1, 2\}$; Pr 1, 32, 62, 32, 1; *	256-dim subcode (see spec) of $\sum_{0 \le i < 274}\{0, 512\}2^{10i}$
$^{i}\{-1, 0, 1\}$; Pr 13, 38, 13; *	256-dim subcode (see spec) of $\sum_{0 \le i < 274}\{0, 512\}2^{10i}$
$^{i}\{-1, 0, 1\}$; Pr 5, 22, 5; *	256-dim subcode (see spec) of $\sum_{0 \le i < 274}\{0, 512\}2^{10i}$

Attackin

Attack s
of usuall
strategy.
Normal



method)
(spec page 23)
(spec page 23)
(spec page 23)
}
}
}
1
, 1
, 1
5}
.5}

156) + 16384)/32768⌋
175) + 16384)/32768⌋
433) + 16384)/32768⌋

512**Z**
128**Z**
256**Z**
64**Z**
512**Z**
64**Z**

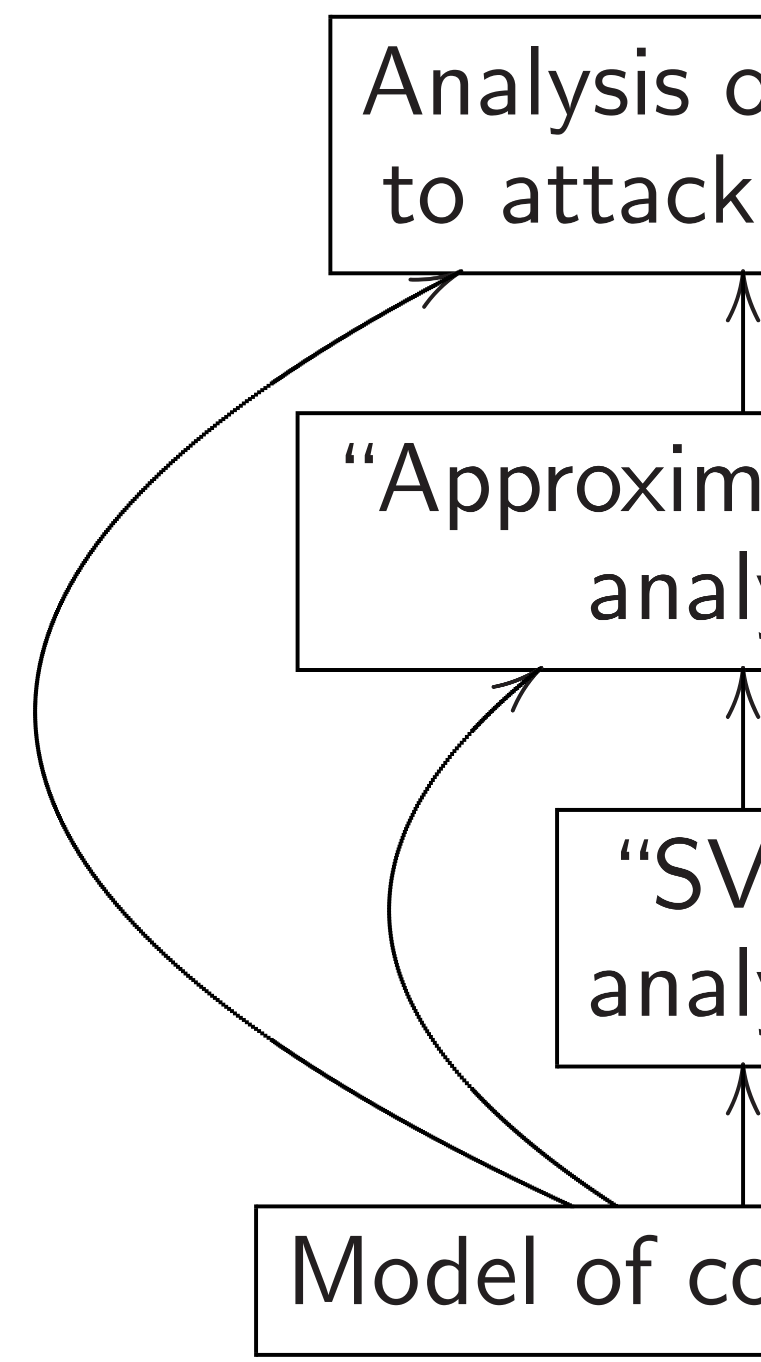
Pr 1, 32, 62, 32, 1; *
38, 13; *
2, 5; *

set of encoded messages

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

Attacking these pr

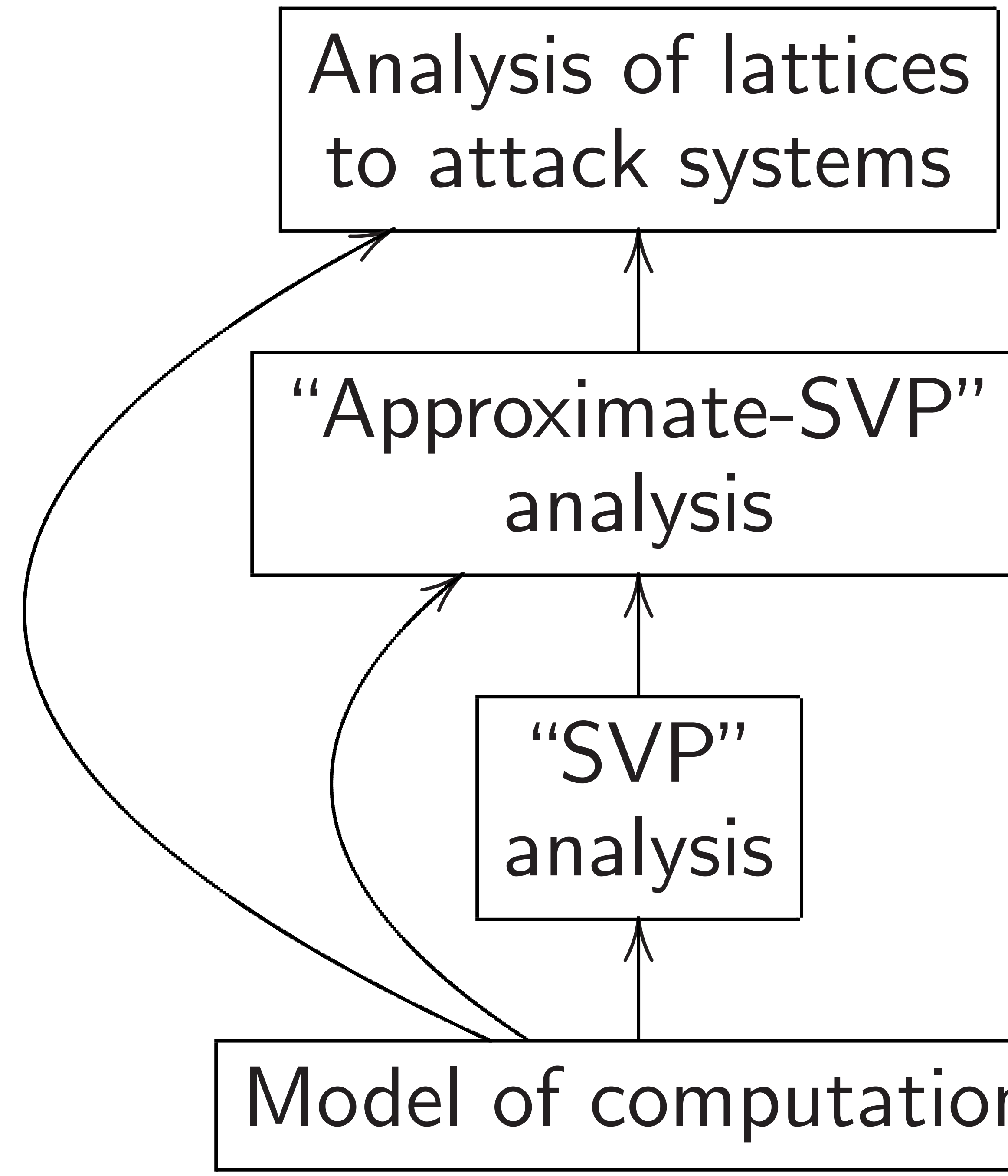
Attack strategy wi
of usually being be
strategy. Focus of
Normal layers in a



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

Attacking these problems

Attack strategy with reputat
of usually being best: "prim
strategy. Focus of this talk.
Normal layers in analysis:

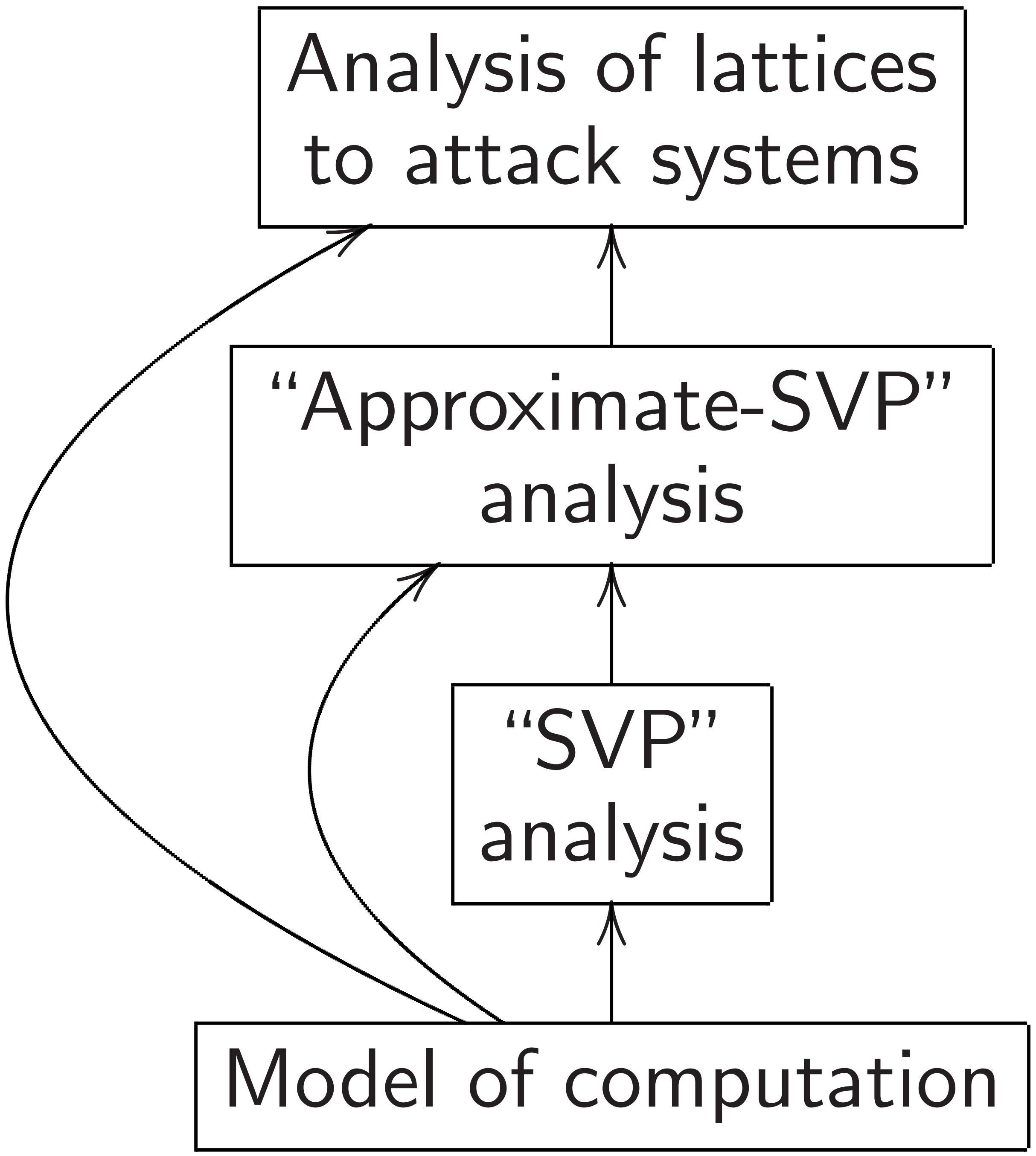


set of encoded messages
8×8 matrix over $\{0, 8192, 16384, 24576\}$
8×8 matrix over $\{0, 8192, \ldots, 57344\}$
8×8 matrix over $\{0, 4096, \ldots, 61440\}$
$\sum_{0 \le i < 256} \{0, 1665\} x^i$
$\sum_{0 \le i < 256} \{0, 1665\} x^i$
$\sum_{0 \le i < 256} \{0, 1665\} x^i$
256-dim subcode (see spec)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

Attacking these problems

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

Normal layers in analysis:



nessages

r $\{0, 8192, 16384, 24576\}$

r $\{0, 8192, \ldots, 57344\}$

r $\{0, 4096, \ldots, 61440\}$

$55\}x^i$

$55\}x^i$

$55\}x^i$

e (see spec) of $\sum_{0 \le i < 512} \{0, 126\} x^i$

e (see spec) of $\sum_{0 \le i < 1024} \{0, 126\} x^i$

e (see spec) of $\sum_{0 \le i < 1024} \{0, 126\} x^i$

$45\}x^i(1 + x^{256})$

$45\}x^i(1 + x^{256} + x^{512} + x^{768})$

$10\}x^i$

$95\}x^i$

$33\}x^i$

r $\{0, 1024, 2048, 3072\}$

r $\{0, 4096, \ldots, 28672\}$

r $\{0, 2048, \ldots, 30720\}$

$96\}x^i$

$48\}x^i$

$96\}x^i$

e (see spec) of $\sum_{0 \le i < 318} \{0, 512\} x^i$

e (see spec) of $\sum_{0 \le i < 410} \{0, 2048\} x^i$

e (see spec) of $\sum_{0 \le i < 490} \{0, 1024\} x^i$

$96\}x^i$

$96\}x^i$

$96\}x^i$

e (see spec) of $\sum_{0 \le i < 274} \{0, 512\} 2^{10i}$

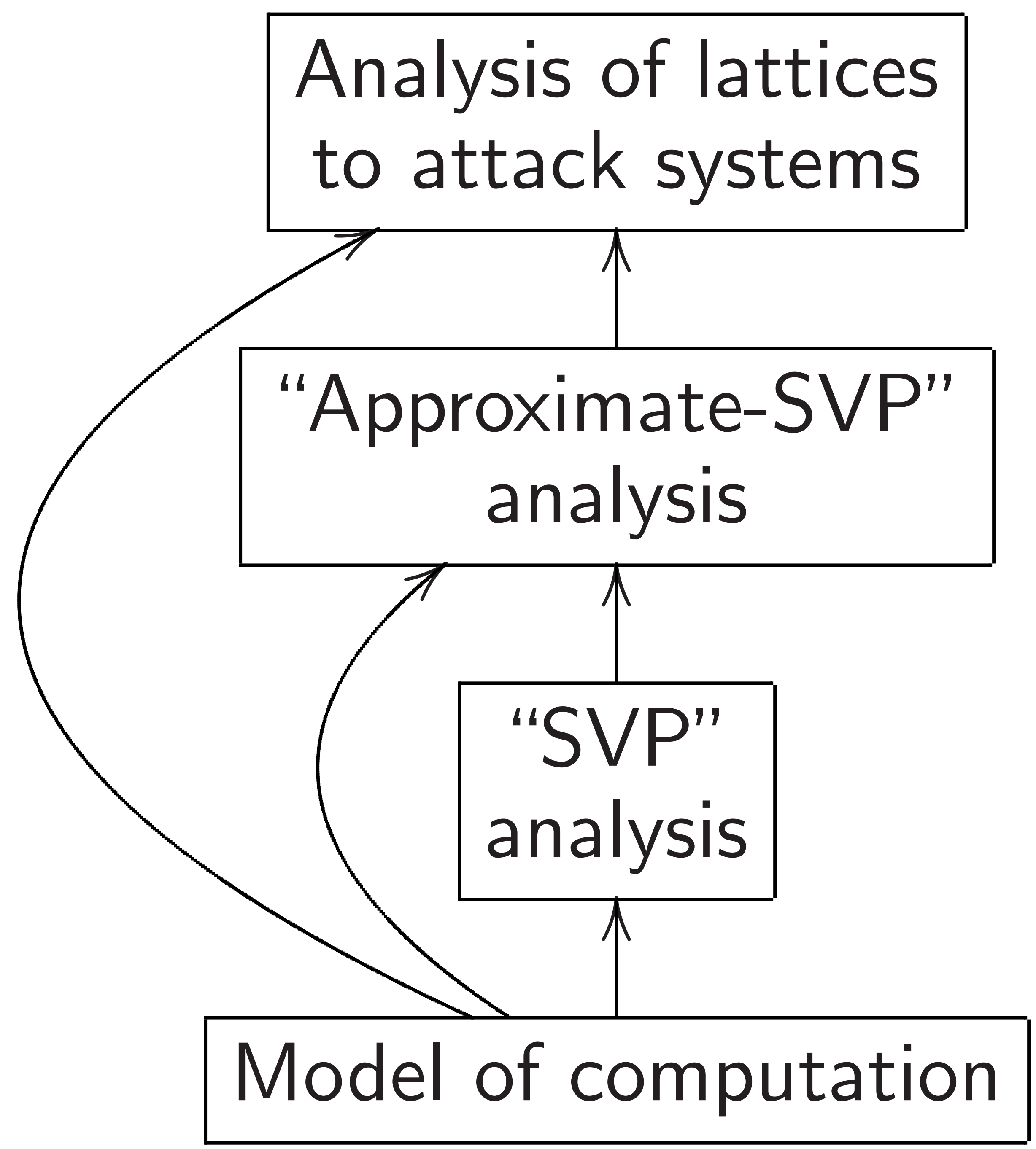
e (see spec) of $\sum_{0 \le i < 274} \{0, 512\} 2^{10i}$

e (see spec) of $\sum_{0 \le i < 274} \{0, 512\} 2^{10i}$

Attacking these problems

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

Normal layers in analysis:



Models o

Multitap

sort N in

time N^{1}

4576}
4}
0}

$_{i<512}\{0,126\}x^i$
$_{i<1024}\{0,126\}x^i$
$_{i<1024}\{0,126\}x^i$

$^{512}+x^{768})$

72}
2}
0}

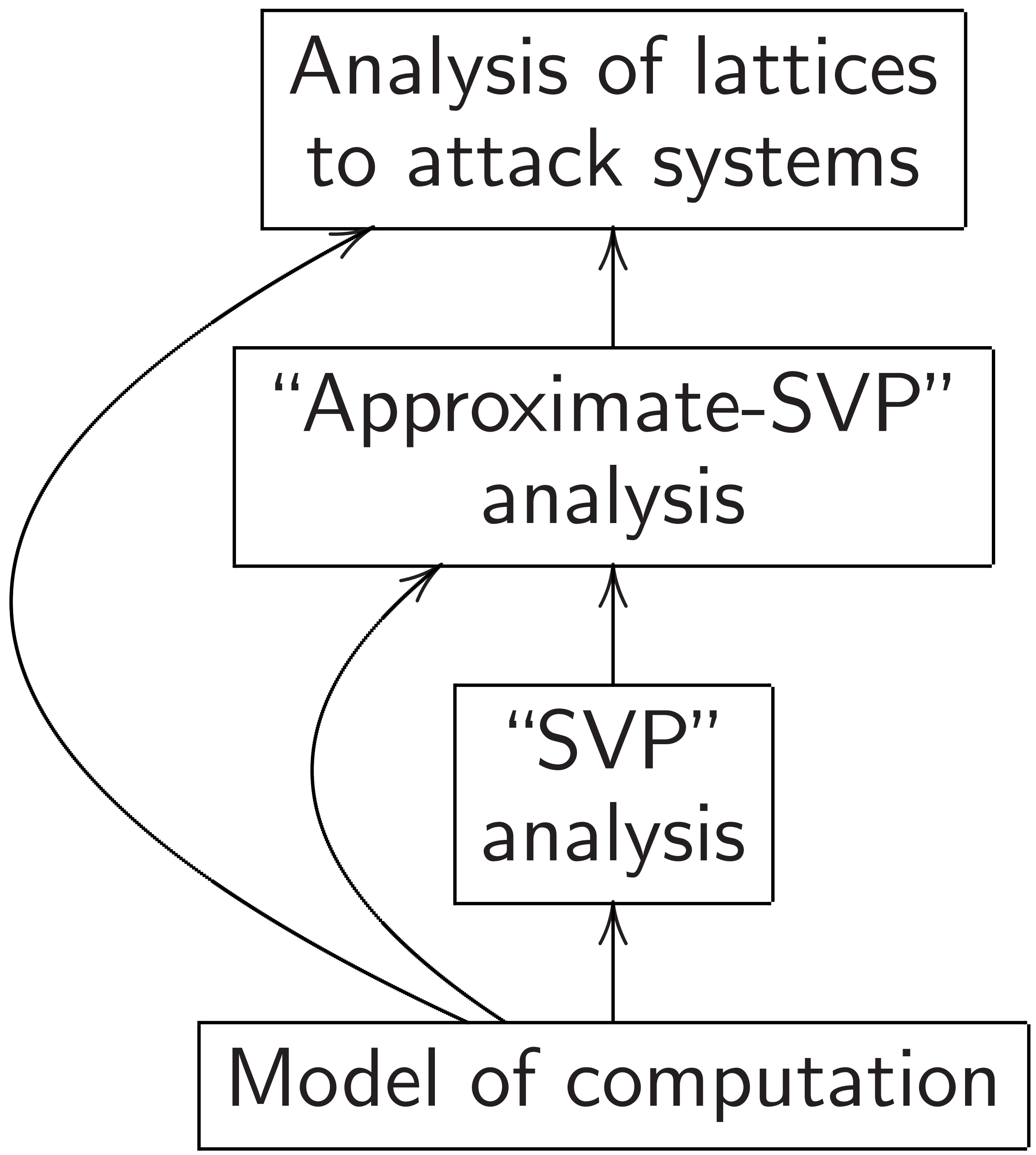
$_{i<318}\{0,512\}x^i$
$_{i<410}\{0,2048\}x^i$
$_{i<490}\{0,1024\}x^i$

$_{i<274}\{0,512\}2^{10i}$
$_{i<274}\{0,512\}2^{10i}$
$_{i<274}\{0,512\}2^{10i}$

Attacking these problems

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

Normal layers in analysis:



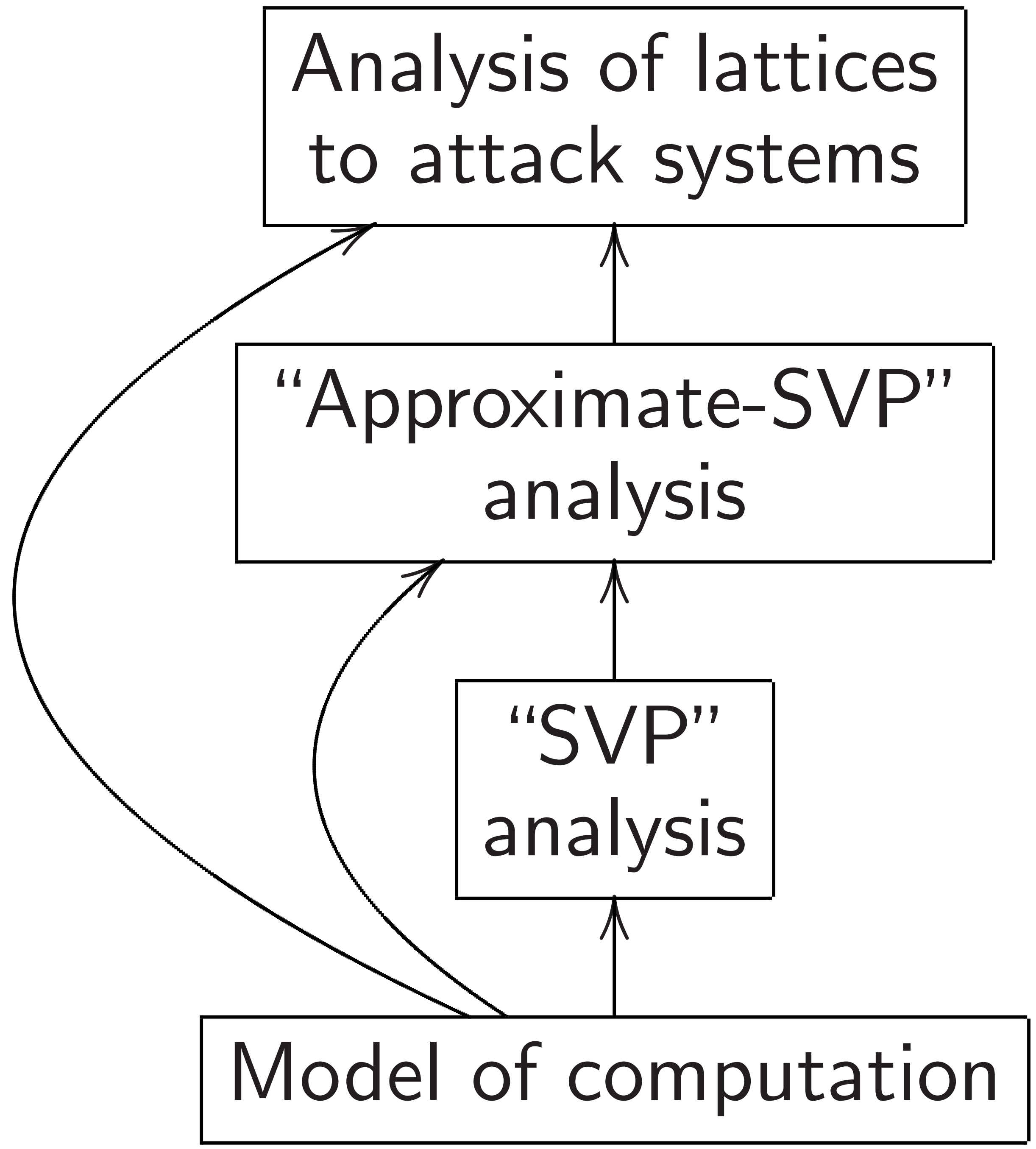
Models of comput

Multitape Turing
sort N ints, each
time $N^{1+o(1)}$, spa

Attacking these problems

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

Normal layers in analysis:



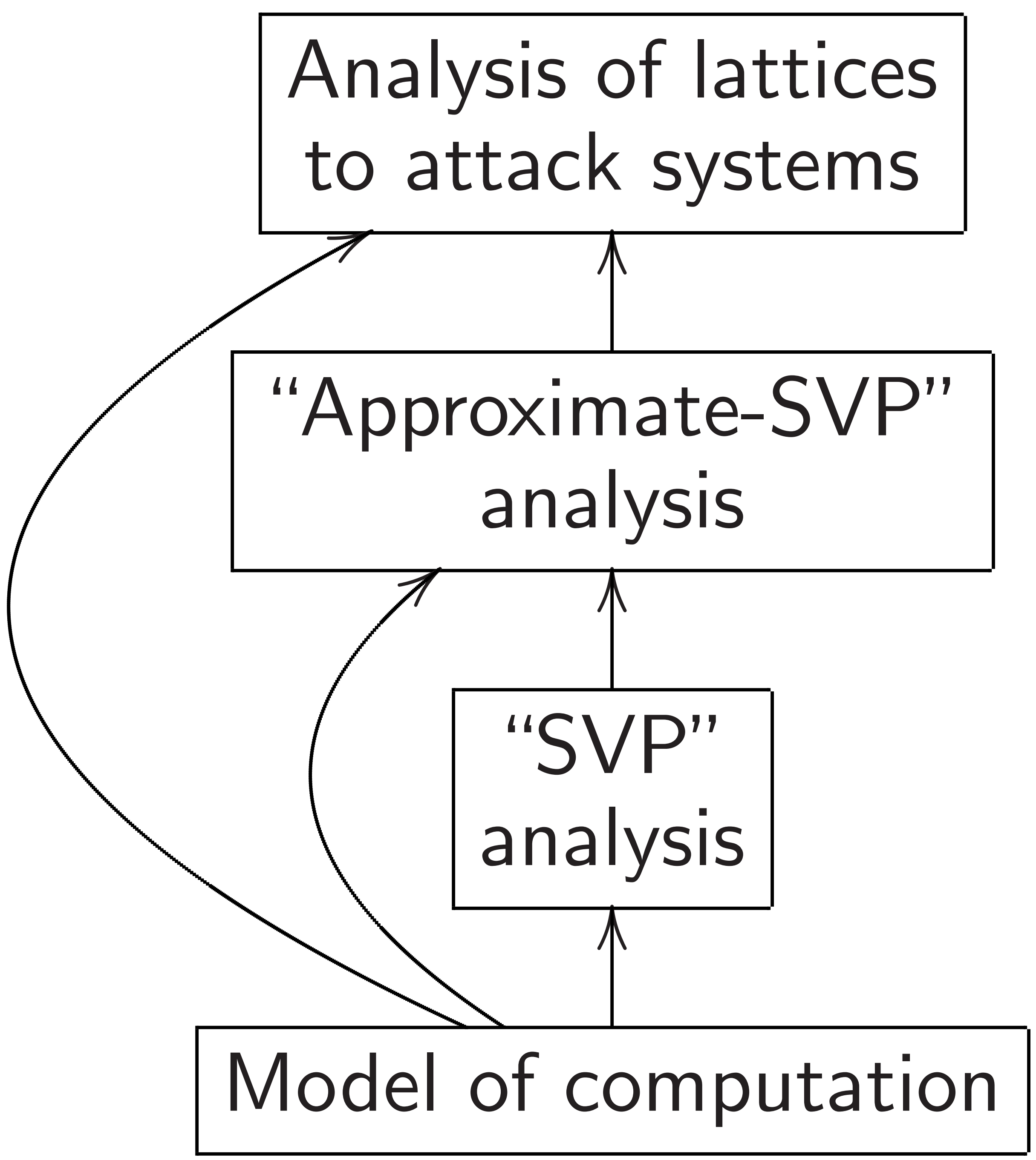
Models of computation

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

Attacking these problems

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

Normal layers in analysis:



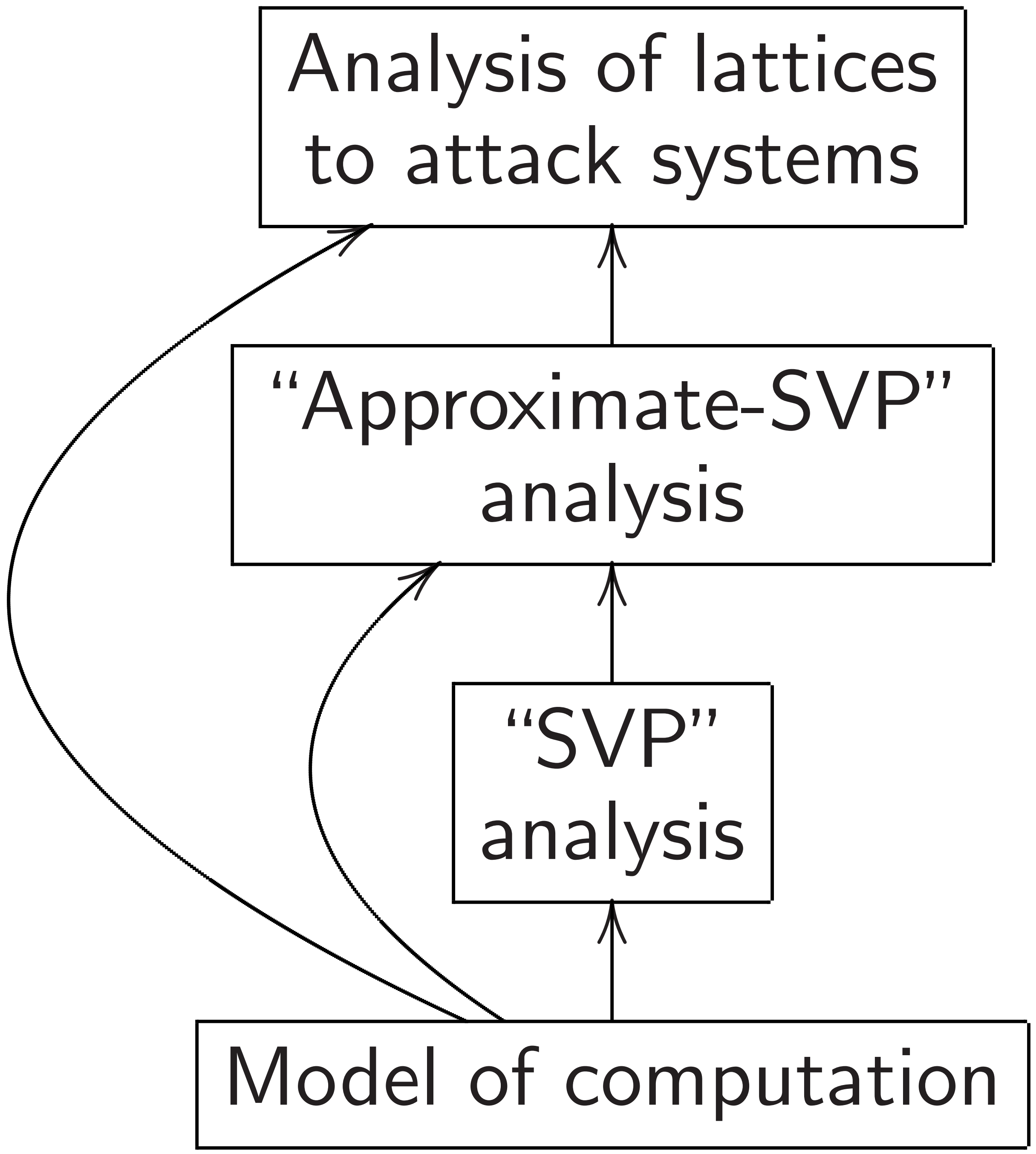
Models of computation

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

Attacking these problems

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

Normal layers in analysis:



Models of computation

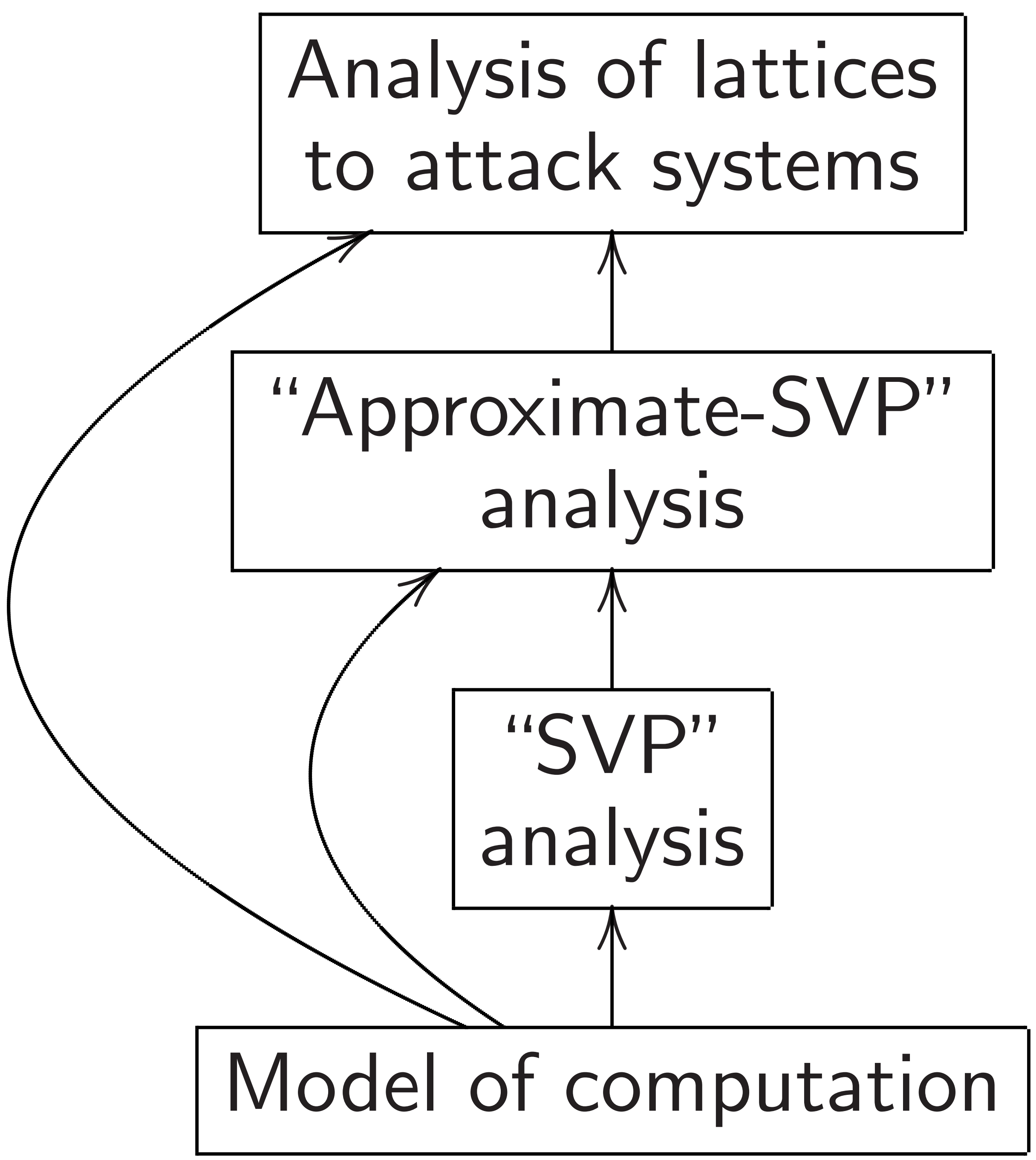
Multitape Turing machine: e.g., sort N ints, each $N^{o(1)}$ bits, in time $N^{1+o(1)}$, space $N^{1+o(1)}$.

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

Attacking these problems

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

Normal layers in analysis:



Models of computation

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

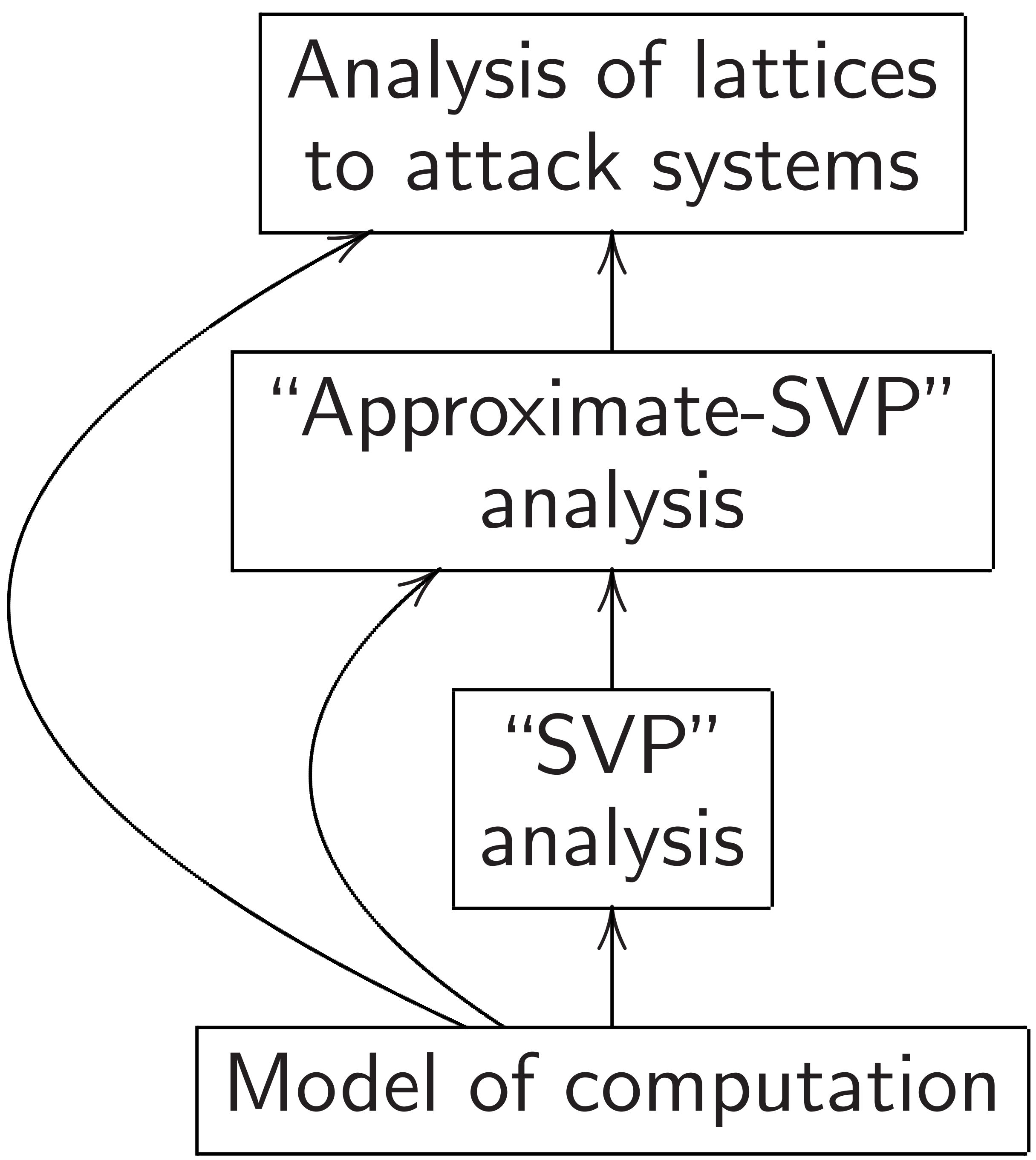
Brent–Kung 2D circuit model allows parallelism—e.g., sort in time $N^{0.5+o(1)}$, space $N^{1+o(1)}$.

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

Attacking these problems

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

Normal layers in analysis:



Models of computation

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

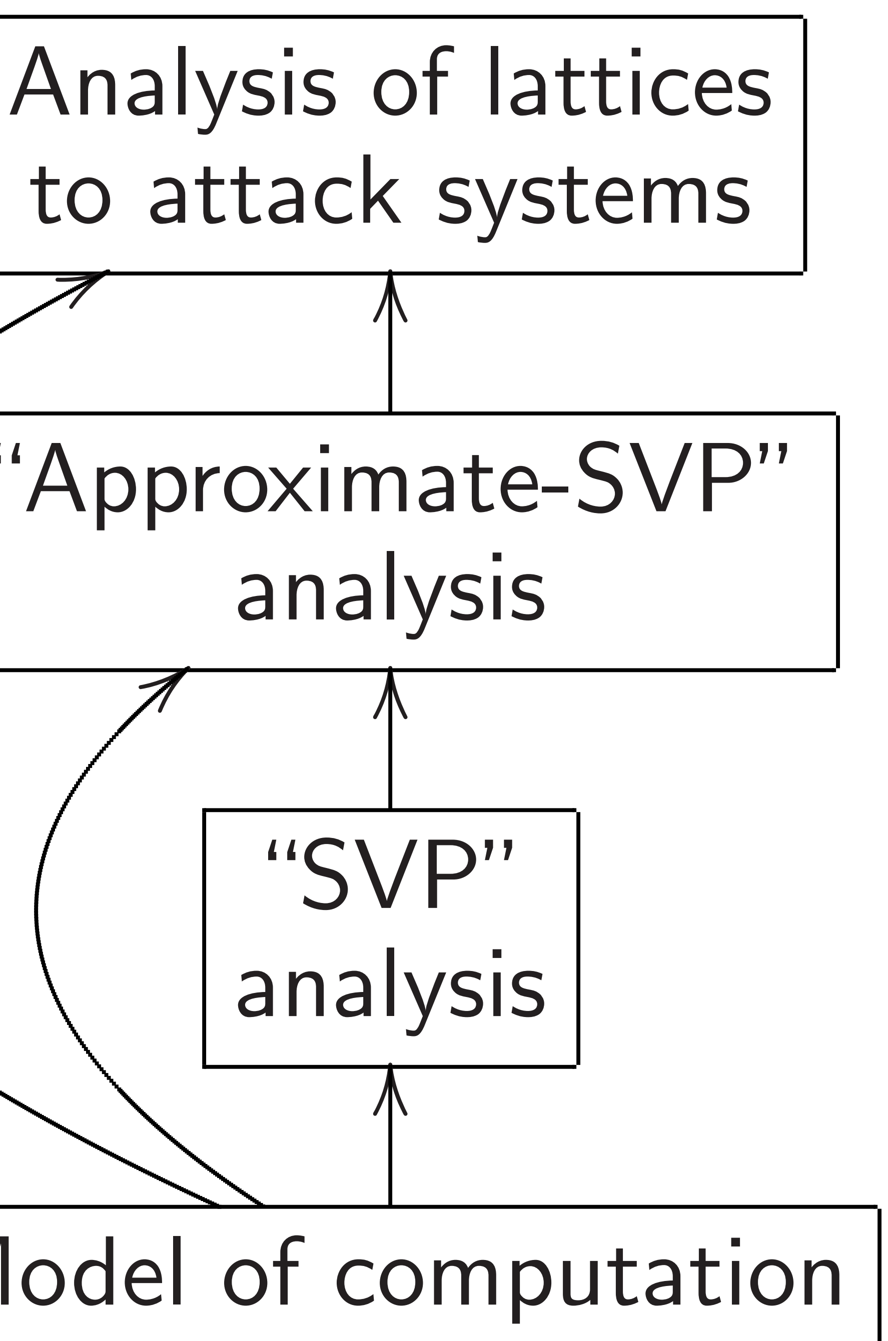
Brent–Kung 2D circuit model allows parallelism—e.g., sort in time $N^{0.5+o(1)}$, space $N^{1+o(1)}$.

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

Quantum computing: similar divergence of models.

g these problems

strategy with reputation
y being best: "primal"
. Focus of this talk.
layers in analysis:



Models of computation

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

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

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

Quantum computing: similar divergence of models.

Lattices

Rewrite
short nc
of homo

Problem
with aG

roblems

ith reputation
est: “primal”
this talk.
nalysis:

f lattices
systems

ate-SVP”
ysis

P”
ysis

mputation

Models of computation

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

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

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

Quantum computing:
similar divergence of models.

Lattices

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

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

tion

al"

n

Models of computation

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

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

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

Quantum computing: similar divergence of models.

Lattices

Rewrite each problem as fin

short nonzero solution to sy

of homogeneous $\mathcal{R}/q$ equat

Problem 1: Find $(a, e) \in \mathcal{R}^2$

with $aG + e = 0$, given $G \in$

Models of computation

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

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

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

Quantum computing: similar divergence of models.

Lattices

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

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

Models of computation

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

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

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

Quantum computing: similar divergence of models.

Lattices

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

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

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

Models of computation

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

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

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

Quantum computing: similar divergence of models.

Lattices

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

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

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

of computation

pe Turing machine: e.g.,
nts, each $N^{o(1)}$ bits, in
$^{+o(1)}$, space $N^{1+o(1)}$.

ung 2D circuit model
arallelism—e.g., sort in
$^{.5+o(1)}$, space $N^{1+o(1)}$.

multiple inequivalent
ns, untethered to physical
ions. Sort in time $N^{o(1)}$.

m computing:
livergence of models.

Lattices

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

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

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

Recogni
as a full-

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

ation

machine: e.g.,
$N^{o(1)}$ bits, in
ce $N^{1+o(1)}$.

rcuit model
—e.g., sort in
ace $N^{1+o(1)}$.

nequivalent
ered to physical
in time $N^{o(1)}$.

ng:
of models.

Lattices

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

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

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 $\mathcal{R}^2$.

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

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

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 inc

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

<u>Module structure</u>

Each of these latti
module, and thus
many independent

ding
ystem
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

$(\overline{a}, \overline{r}) \mapsto (\overline{a}, q\overline{r} - \overline{a}G)$

^{2} 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., $((x+1)a, (x+1)t, (x+1)e)$.

2001 Ma

1: Force

a to be (

rank, sp

despite l

lution space

ce:

e is image of

$(\overline{a}, q\overline{r} - \overline{a}G)$

e is

$(\overline{a}, \overline{t}, \overline{r}) \mapsto$

$G)$.

e is image of

$\overline{r_1}, \overline{r_2}) \mapsto$

$\overline{r_1} - \overline{a}G_1$,

).

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

2001 May–Silverm

1: Force a few coe

a to be 0. This re

rank, speeding up

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

2001 May–Silverman, for Pr
1: Force a few coefficients o
a to be 0. This reduces latti
rank, speeding up various at
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., $((x+1)a, (x+1)t, (x+1)e)$.

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

Module structure

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

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

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

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

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

Module structure

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

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

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

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

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

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

(Also slowdown if q is very large?)

structure

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

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

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

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

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

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

(Also slowdown if q is very large?)

Standard

Lattice

Uniform
secret a

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

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

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

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

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

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

(Also slowdown if q is very large?)

Standard analysis

Lattice has rank 2

Uniform random s
secret a has length

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

).
$x^2 e$).

s

$+1)e$).

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

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

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

(Also slowdown if q is very large?)

Standard analysis for Proble

Lattice has rank $2 \cdot 761 = 1$

Uniform random small weigh

secret a has length $\sqrt{w} \approx 1$

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

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

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

(Also slowdown if q is very large?)

Standard analysis for Problem 1

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

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

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

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

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

(Also slowdown if q is very large?)

Standard analysis for Problem 1

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

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

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

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

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

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

(Also slowdown if q is very large?)

Standard analysis for Problem 1

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

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

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

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

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

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

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

roblems: same speedup.
blem 2: Force many
nts of (a, t) to be 0.
raith special case:
$= 1$, and force
efficients of a to be 0.

wdown if q is very large?)

Standard analysis for Problem 1

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

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

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

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

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

Attacker
another

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

? Seems to be
very large.)

ame speedup.
orce many
t) to be 0.
cial case:
orce
of a to be 0.

q is very large?)

Standard analysis for Problem 1

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

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

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

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

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

Attacker is just as
another solution s

oblem
of
ice
tacks,
e.

to be
e.)

dup.

.

0.

large?)

Standard analysis for Problem 1

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

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

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

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

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

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

Standard analysis for Problem 1

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

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

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

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

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

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

Standard analysis for Problem 1

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

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

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

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

Pr[a 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.)

Standard analysis for Problem 1

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

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

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

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

Pr[a 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.)

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

Standard analysis for Problem 1

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

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

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

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

Pr[a 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.)

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

has rank $2 \cdot 761 = 1522$.

random small weight-w

has length $\sqrt{w} \approx 17$.

random small secret

ngth usually close to

$\overline{3} \approx 23$. (What if it's

What if it's larger? Does

ight change security?)

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.)

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

$\cdot\, 761 = 1522$.

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

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

$k = 13$.
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.)

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 c

m 1

522.

nt-w

7.

t

's

Does

?)

0:

1509.

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

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

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

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

Write equation $e = qr - aG$

as 761 equations on 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 ≈0.2% of being in sublattice. These 761 chances are independent. (No, they aren't; also, total Pr depends on attacker's choice of positions.)

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

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

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

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

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

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

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

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

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 (xa, xe).

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

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

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.

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

Attack parameter: $\lambda = 1.331876$.

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

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 ≈0.2% of being in
ce. These 761 chances
pendent. (No, they
lso, total Pr depends on
's choice of positions.)

igger solutions $(\alpha a, \alpha e)$.
rd 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.

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

Attack parameter: $\lambda = 1.331876$.

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

Lattice-b

Attack p

Use BKZ
lattice b
alternati

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.)

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.

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

Attack parameter: $\lambda = 1.331876$.

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

Lattice-basis reduc

Attack parameter:

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

find
a, xe).

, $x^j e$)
in
es

s on
s.)

αe).
?)

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.

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

Attack parameter: $\lambda = 1.331876$.

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

Lattice-basis reduction

Attack parameter: $\beta = 525$.

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

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

Attack parameter: $m = 600$.

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

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

Attack parameter: $\lambda = 1.331876$.

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

Lattice-basis reduction

Attack parameter: $\beta = 525$.

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

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

Attack parameter: $m = 600$.

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

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

Attack parameter: $\lambda = 1.331876$.

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

Lattice-basis reduction

Attack parameter: $\beta = 525$.

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

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

Attack parameter: $m = 600$.

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

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

Attack parameter: $\lambda = 1.331876$.

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

<u>Lattice-basis reduction</u>

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 $e = qr - aG$
equations on coefficients.

parameter: $m = 600$.

$61 - m = 161$ equations:
ect e onto 600 positions.

d sublattice rank
$9 - 161 = 1348$; det q^{600}.

parameter: $\lambda = 1.331876$.

g: Assign weight λ to
s in a. Increases length
$\lambda\sqrt{w} \approx 23$; increases det
q^{600}. (Is this λ optimal?
on with e size variation?)

Lattice-basis reduction

Attack parameter: $\beta = 525$.

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

Standard analysis of BKZ-β:

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

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

Standard

"Geome
holds. (
identifie

$= qr - aG$

on coefficients.

$m = 600$.

161 equations:

600 positions.

ce rank

1348; det q^{600}.

$\lambda = 1.331876$.

weight λ to

reases length

3; increases det

his λ optimal?

size variation?)

Lattice-basis reduction

Attack parameter: $\beta = 525$.

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

Standard analysis of BKZ-β:

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

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

Standard analysis,

"Geometric-series

holds. (What abo

identified in 2018

/

ents.

.

tions:

tions.

t q^{600}.

1876.

to

gth

s det

nal?

tion?)

Lattice-basis reduction

Attack parameter: $\beta = 525$.

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

Standard analysis of BKZ-β:

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

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

Standard analysis, continued

"Geometric-series assumptio

holds. (What about deviatio

identified in 2018 experimen

Lattice-basis reduction

Attack parameter: $\beta = 525$.

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

Standard analysis of BKZ-β:

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

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

Standard analysis, continued:

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

Lattice-basis reduction

Attack parameter: $\beta = 525$.

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

Standard analysis of BKZ-β:

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

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

Standard analysis, continued:

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

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?)

Lattice-basis reduction

Attack parameter: $\beta = 525$.

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

Standard analysis of BKZ-β:

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

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

Standard analysis, continued:

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

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

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

basis reduction

parameter: $\beta = 525$.

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

d analysis of BKZ-β:

lly" finds nonzero vector
n $\delta^d(\det L)^{1/d}$ 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 (a, e), assuming forcing worked. If it didn't, retry. (Are these tries independent? Should they use new parameters? Grover?)

How lon

Standard
$2^{153.3}$ op

ction

$\beta = 525$.

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 (a, 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:
$2^{153.3}$ operations b

luce

:

ector

e

−1)).

otic

Standard analysis, continued:

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

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

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

How long does BKZ-β take

Standard answer: $2^{0.292\beta} =$

$2^{153.3}$ operations by "sieving

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

How long does BKZ-β take?

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

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

How long does BKZ-β take?

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

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

Standard analysis, continued:

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

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

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

How long does BKZ-β take?

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

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

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

d analysis, continued:

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

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

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

How long does BKZ-β take?

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

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

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

Note fra

$S \leq 43$

$S = 0.3$

0.187β l

continued:

assumption"
ut deviations
experiments?)

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

finds (a, e),
vorked. If it
these tries
uld they use
Grover?)

How long does BKZ-β take?

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

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

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

Note fragility of co

$S \leq 43 \Rightarrow E < S$
$S = 0.396\beta$, $E =$
$0.187\beta\log_2\beta - 1.$

d:

on"

ons

ts?)

)

d/β.

ntified

),

it

s

use

How long does BKZ-β take?

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

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

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

Note fragility of comparison

$S \leq 43 \Rightarrow E < S$ for $S = 0.396\beta$, $E =$
$0.187\beta \log_2 \beta - 1.019\beta + 16$

How long does BKZ-β take?

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

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

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

Note fragility of comparison.

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

How long does BKZ-β take?

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

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

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

Note fragility of comparison.

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

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

How long does BKZ-β take?

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

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

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

Note fragility of comparison.

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

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

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

How long does BKZ-β take?

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

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

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

Note fragility of comparison.

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

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

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

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

g does BKZ-β take?

d answer: $2^{0.292\beta} =$
perations by “sieving”.

g $o(1) = 0$ into the
$o(1))\beta$ *asymptotic* does
ch experiments. What's
al performance? And
actly is an “operation”?)

(fake) cost for “sieving”
tised as being below
og$_2 \beta - 1.019\beta + 16.1$
nable extrapolation of
ents) for “enumeration”.

Note fragility of comparison.

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

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

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

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

`sntrup7`
“NTRU

Ignoring

368	185
368	185
153	139
208	208

Including

230	169
277	169
153	139
208	180

Security

. . .	pre
	. . .

KZ-β take?

$2^{0.292\beta} =$

by "sieving".

0 into the

mptotic does

nents. What's

nance? And

"operation"?)

t for "sieving"

eing below

$019\beta + 16.1$

apolation of

'enumeration".

Note fragility of comparison.

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

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

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

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

`sntrup761` evalua

"NTRU Prime: ro

Ignoring hybrid att

368	185	enum, fr
368	185	enum, re
153	139	sieving,
208	208	sieving,

Including hybrid at

230	169	enum, fr
277	169	enum, re
153	139	sieving,
208	180	sieving,

Security levels:

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

?

g".

oes

at's

d

n"?)

ng"

5.1

of

on".

Note fragility of comparison.

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

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

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

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

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

Ignoring hybrid attacks:

368	185	enum, free memor
368	185	enum, real memor
153	139	sieving, free memo
208	208	sieving, real memo

Including hybrid attacks:

230	169	enum, free memor
277	169	enum, real memor
153	139	sieving, free memo
208	180	sieving, real memo

Security levels:

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

Note fragility of comparison.

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

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

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

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

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

Ignoring hybrid attacks:

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

Including hybrid attacks:

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

Security levels:

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

gility of comparison.

$\Rightarrow E < S$ for

96β, $E =$

$og_2 \beta - 1.019\beta + 16.1$.

$\Rightarrow E < S$ for

69β, $E =$

$\log_2 \beta - 1.019\beta + 16.1)/2$.

$\Rightarrow E < S$ for

65β, $E =$

$\log_2 \beta - 0.545\beta + 10)/2$.

get analyses right!

p: include models

ount for memory cost.

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

Ignoring hybrid attacks:

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

Including hybrid attacks:

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

Security levels:

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

Hybrid a

Extreme

Search a

omparison.

for

$019\beta + 16.1$.

for

$.019\beta + 16.1)/2$.

for

$.545\beta + 10)/2$.

ses right!

models

nemory cost.

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

Ignoring hybrid attacks:

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

Including hybrid attacks:

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

Security levels:

| . . . | pre-quantum

| . . . | post-quantum

<u>Hybrid attacks</u>

Extreme special ca

Search all small w

.

5.1.

5.1)/2.

0)/2.

st.

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

Ignoring hybrid attacks:

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

Including hybrid attacks:

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

Security levels:

| . . . | pre-quantum

| . . . | post-quantum

Hybrid attacks

Extreme special case:

Search all small weight-w a.

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

Ignoring hybrid attacks:

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

Including hybrid attacks:

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

Security levels:

| . . . | pre-quantum

| . . . | post-quantum

Hybrid attacks

Extreme special case:

Search all small weight-w a.

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

Ignoring hybrid attacks:

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

Including hybrid attacks:

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

Security levels:

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

Hybrid attacks

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

Grover reduces cost to $\sqrt{}$.

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

Ignoring hybrid attacks:

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

Including hybrid attacks:

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

Security levels:

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

Hybrid attacks

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

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

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

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

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

Ignoring hybrid attacks:

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

Including hybrid attacks:

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

Security levels:

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

Hybrid attacks

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

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

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

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

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

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

Hybrid attacks

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

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

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

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

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

Seems w

for typic

tions from
und 2" Table 2:

tacks:

ee memory cost
eal memory cost
free memory cost
real memory cost

ttacks:

ee memory cost
eal memory cost
free memory cost
real memory cost

antum

Hybrid attacks

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

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

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

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

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

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

n

ble 2:

y cost
y cost
ory cost
ory cost

y cost
y cost
ory cost
ory cost

Hybrid attacks

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

Grover reduces cost to $\sqrt{}$.

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

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

e.g. Problem 1: aG small so $a_1 G \approx -a_2 G$. (How fast are near-neighbor algorithms?)

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

Hybrid attacks

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

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

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

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

e.g. Problem 1: aG small so $a_1 G \approx -a_2 G$. (How fast are near-neighbor algorithms?)

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

Hybrid attacks

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

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

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

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

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

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

Hybrid attacks

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

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

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

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

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

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

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

Hybrid attacks

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

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

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

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

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

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

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

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

Hybrid attacks

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

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

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

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

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

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

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

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

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

Hybrid attacks

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

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

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

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

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

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

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

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

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

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

ttacks

special case:
ll small weight-w a.

educes cost to $\sqrt{}$.

get "$\sqrt{}$" using memory
quantum computation.

nt a as $a_1 + a_2$. (What
ptimal a_1, a_2 overlap?)
approximate collision
$H_1(a_1)$ and $H_2(a_2)$.

blem 1: aG small
$\approx -a_2G$. (How fast are
ghbor algorithms?)

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

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

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

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

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

Search t
most lik

ase:

eight-w a.

st to $\sqrt{}$.

' using memory

computation.

$+ a_2$. (What

a_2 overlap?)

ate collision

nd $H_2(a_2)$.

G small

(How fast are

rithms?)

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

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

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

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

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

Search through ma

most likely choices

emory
on.
hat
?)
on
.
are

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

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

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

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

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

Search through many of the most likely choices of v.

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

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

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

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

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

Search through many of the most likely choices of v.

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

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

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

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

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

Search through many of the most likely choices of v.

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

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

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

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

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

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

Search through many of the most likely choices of v.

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

Can again do quantum search, or approximate collision search.

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

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

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

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

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

Search through many of the most likely choices of v.

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

Can again do quantum search, or approximate collision search.

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

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

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

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

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

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

Search through many of the most likely choices of v.

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

Can again do quantum search, or approximate collision search.

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

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