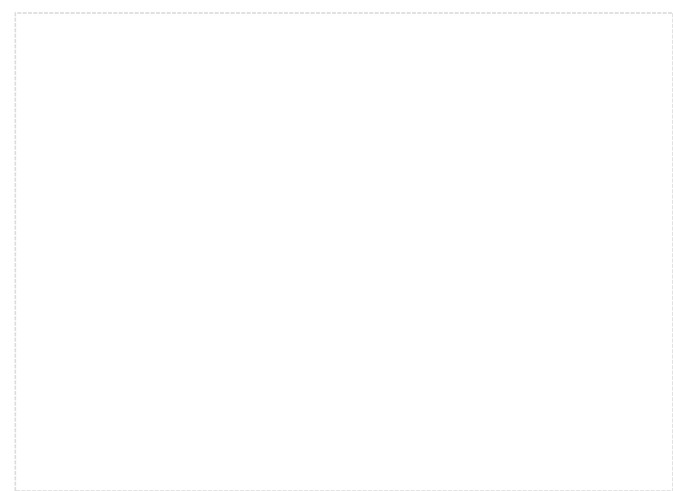


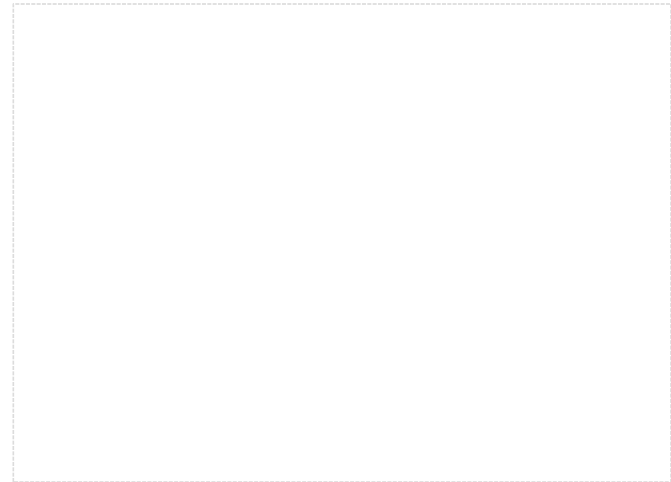
Ideal Lattices and Applications

Vadim Lyubashevsky
INRIA / ENS, Paris

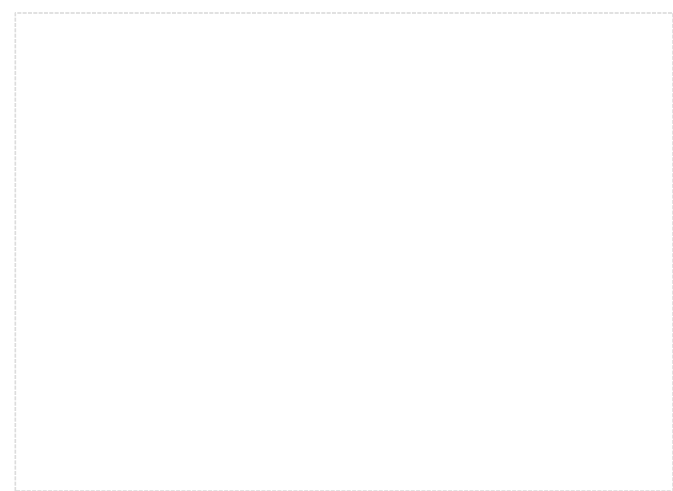


Outline

- Ideal Lattices
- Ring-SIS
- Ring-LWE and a search-decision reduction



IDEAL LATTICES



Ideal Lattice FAQs

Q: What are ideal lattices?

A: They are lattices with some additional algebraic structure.

Lattices are groups

Ideal Lattices are ideals

Q: Why do we need ideal lattices?

A: To build **efficient** cryptographic primitives

Cyclic Lattices

A set L in \mathbf{Z}^n is a *cyclic lattice* if:

1.) For all v, w in L , $v+w$ is also in L

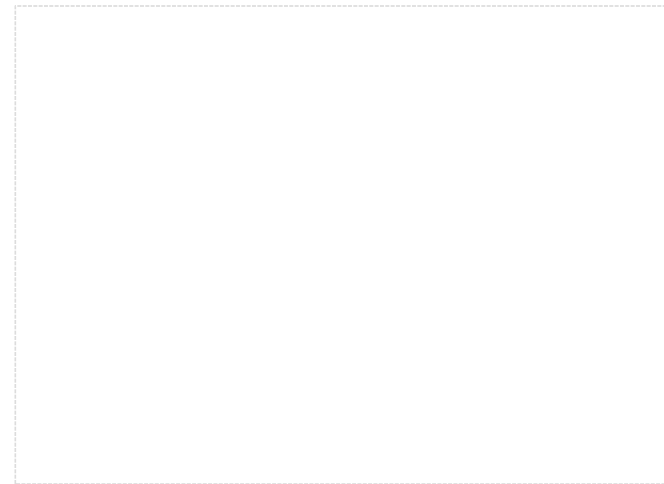
$$\begin{bmatrix} -1 & 2 & 3 & -4 \end{bmatrix} + \begin{bmatrix} -7 & -2 & 3 & 6 \end{bmatrix} = \begin{bmatrix} -8 & 0 & 6 & 2 \end{bmatrix}$$

2.) For all v in L , $-v$ is also in L

$$\begin{bmatrix} -1 & 2 & 3 & -4 \end{bmatrix} \quad \begin{bmatrix} 1 & -2 & -3 & 4 \end{bmatrix}$$

3.) For all v in L , a cyclic shift of v is also in L

$$\begin{bmatrix} -1 & 2 & 3 & -4 \\ -4 & -1 & 2 & 3 \\ 3 & -4 & -1 & 2 \\ 2 & 3 & -4 & -1 \end{bmatrix}$$



Cyclic Lattices = Ideals in $\mathbf{Z}[x]/(x^n-1)$

A set L in \mathbf{Z}^n is a *cyclic lattice* if L is an *ideal* in $\mathbf{Z}[x]/(x^n-1)$

1.) For all v, w in L , $v+w$ is also in L

$$\begin{bmatrix} -1 & 2 & 3 & -4 \end{bmatrix} + \begin{bmatrix} -7 & -2 & 3 & 6 \end{bmatrix} = \begin{bmatrix} -8 & 0 & 6 & 2 \end{bmatrix}$$

$$(-1+2x+3x^2-4x^3) + (-7-2x+3x^2+6x^3) = (-8+0x+6x^2+2x^3)$$

2.) For all v in L , $-v$ is also in L

$$\begin{bmatrix} -1 & 2 & 3 & -4 \end{bmatrix} \quad \begin{bmatrix} 1 & -2 & -3 & 4 \end{bmatrix}$$

$$(-1+2x+3x^2-4x^3) \quad (1-2x-3x^2+4x^3)$$

3.) For all v in L , ~~a cyclic shift of v is also in L~~ vx is also in L

$\begin{bmatrix} -1 & 2 & 3 & -4 \end{bmatrix}$	$-1+2x+3x^2-4x^3$
$\begin{bmatrix} -4 & -1 & 2 & 3 \end{bmatrix}$	$(-1+2x+3x^2-4x^3)x = -4-x+2x^2+3x^3$
$\begin{bmatrix} 3 & -4 & -1 & 2 \end{bmatrix}$	$(-1+2x+3x^2-4x^3)x^2 = 3-4x-x^2+2x^3$
$\begin{bmatrix} 2 & 3 & -4 & -1 \end{bmatrix}$	$(-1+2x+3x^2-4x^3)x^3 = 2+3x-4x^2-x^3$

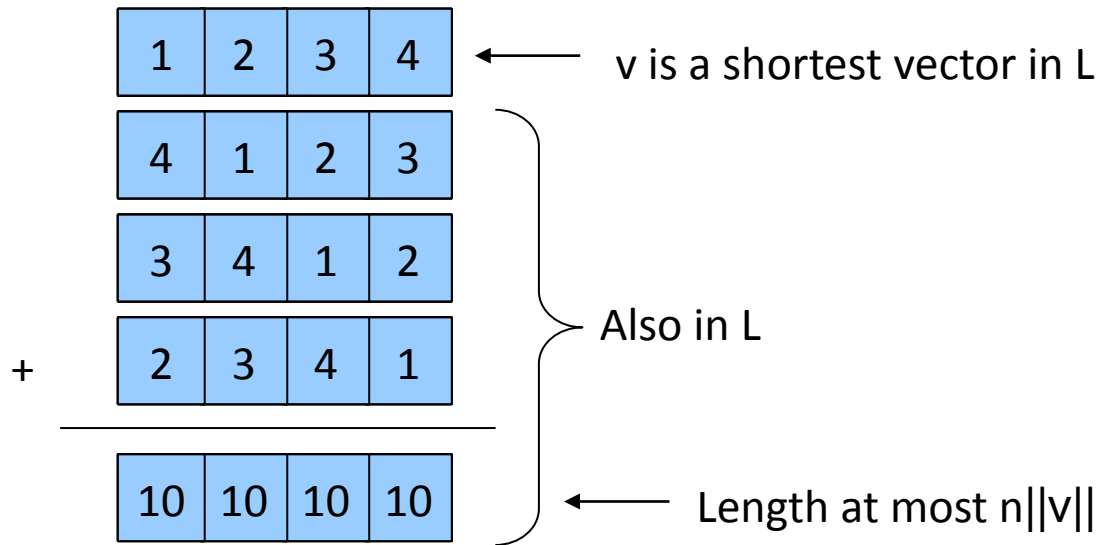
Why Cyclic Lattices?

- Succinct representations
 - Can represent an n -dimensional lattice with 1 vector
- Algebraic structure
 - Allows for fast arithmetic (using FFT)
 - Makes proofs possible
- NTRU cryptosystem
- One-way functions based on worst-case hardness of SVP in ideal lattices [Mic02]

Is $SVP_{\text{poly}(n)}$ Hard for Cyclic Lattices?

Short answer: we don't know but conjecture it is.

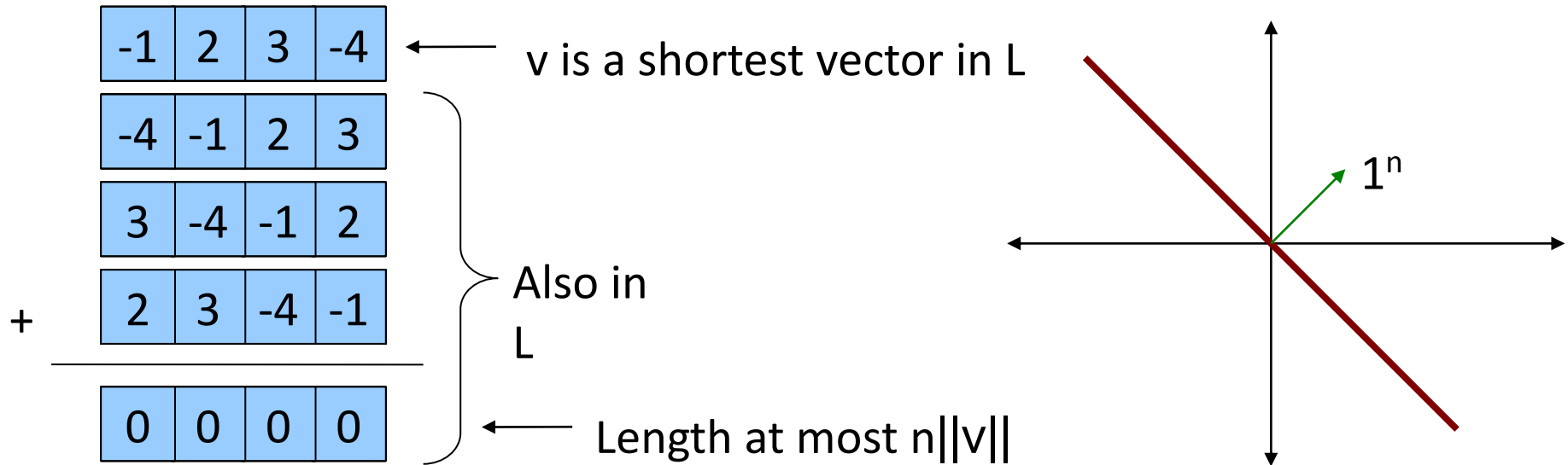
What's wrong with the following argument that SVP_n is easy?



Algorithm for solving $SVP_n(L)$ for a cyclic lattice L :

1. Construct 1-dimensional lattice $L' = L \cap \{1^n\}$
2. Find and output the shortest vector in L'

The Hard Cyclic Lattice Instances



The “hard” instances of cyclic lattices lie on plane P perpendicular to the 1^n vector

In algebra language:

If $R = \mathbf{Z}[x]/(x^n - 1)$, then

$$1^n = (x^{n-1} + x^{n-2} + \dots + 1) \approx \mathbf{Z}[x]/(x-1)$$

$$P = (x-1) \approx \mathbf{Z}[x]/(x^{n-1} + x^{n-2} + \dots + 1)$$

f-Ideal Lattices = Ideals in $\mathbf{Z}[x]/(f)$

Want f to have 3 properties:

1) Monic (i.e. coefficient of largest exponent is 1)

2) Irreducible over \mathbf{Z}

3) For all polynomials g, h $\|gh \bmod f\| < \text{poly}(n) \|g\| \cdot \|h\|$

Conjecture: For all f that satisfy the above 3 properties, solving $\text{SVP}_{\text{poly}(n)}$ for ideals in $\mathbf{Z}[x]/(f)$ takes time $2^{\Omega(n)}$.

Some “good” f to use:

$f = x^{n-1} + x^{n-2} + \dots + 1$ where n is prime

$f = x^n + 1$ where n is a power of 2

(x^n+1) -Ideal Lattices = Ideals in $\mathbf{Z}[x]/(x^n+1)$

A set L in \mathbf{Z}^n is a (x^n+1) -ideal lattice if L is an ideal in $\mathbf{Z}[x]/(x^n+1)$

1.) For all v, w in L , $v+w$ is also in L

$$\begin{bmatrix} -1 & 2 & 3 & -4 \end{bmatrix} + \begin{bmatrix} -7 & -2 & 3 & 6 \end{bmatrix} = \begin{bmatrix} -8 & 0 & 6 & 2 \end{bmatrix}$$

$$(-1+2x+3x^2-4x^3) + (-7-2x+3x^2+6x^3) = (-8+0x+6x^2+2x^3)$$

2.) For all v in L , $-v$ is also in L

$$\begin{bmatrix} -1 & 2 & 3 & -4 \end{bmatrix} \quad \begin{bmatrix} 1 & -2 & -3 & 4 \end{bmatrix}$$

$$(-1+2x+3x^2-4x^3) \quad (1-2x-3x^2+4x^3)$$

3.) For all v in L , vx is also in L

$$\begin{bmatrix} -1 & 2 & 3 & -4 \end{bmatrix} \quad -1+2x+3x^2-4x^3$$

$$\begin{bmatrix} 4 & -1 & 2 & 3 \end{bmatrix} \quad (-1+2x+3x^2-4x^3)x=4-x+2x^2+3x^3$$

$$\begin{bmatrix} -3 & 4 & -1 & 2 \end{bmatrix} \quad (-1+2x+3x^2-4x^3)x^2 = -3+4x-x^2+2x^3$$

$$\begin{bmatrix} -2 & -3 & 4 & -1 \end{bmatrix} \quad (-1+2x+3x^2-4x^3)x^3 = -2-3x+4x^2-x^3$$

Hardness of Problems for General and (x^n+1) -Ideal Lattices

Exact Versions

	General	(x^n+1) -ideal
SVP	NP-hard	?
SIVP	NP-hard	?
GapSVP	NP-hard	?
uSVP	NP-hard	N/A
BDD	NP-hard	?

Poly(n)-approximate Versions

	General	(x^n+1) -ideal
SVP	?	?
SIVP	?	?
GapSVP	?	Easy
uSVP	?	N/A
BDD	?	?

Legend:

?: *No hardness proofs nor sub-exponential time algorithms are known.*

Colored boxes: *Problems are equivalent*

SVP = SIVP

Lemma: If v is a vector in $\mathbf{Z}[x]/(f)$ where f is a monic, irreducible polynomial of degree n , then

$$v, vx, vx^2, \dots, vx^{n-1}$$

are linearly independent.

1	2	3	4
---	---	---	---

Shortest vector v

-4	1	2	3
----	---	---	---

vx

-3	-4	1	2
----	----	---	---

vx^2

-2	-3	-4	1
----	----	----	---

vx^3

$$\|v\| = \|vx\| = \|vx^2\| = \|vx^3\|$$

Corollary: A (x^n+1) -ideal lattice cannot have a unique shortest vector.

GapSVP $_{\sqrt{n}}$ is easy

Fact: For all (x^n+1) -ideal lattices L ,

$$\det(L)^{1/n} \leq \lambda_1(L) \leq \sqrt{n} \det(L)^{1/n}$$

So $\det(L)^{1/n}$ is a \sqrt{n} – approximation of $\lambda_1(L)$

Proof of fact:

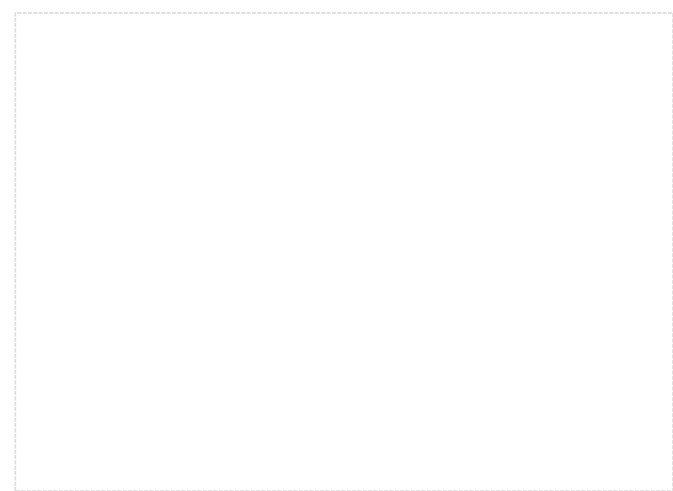
1. $\lambda_1(L) \leq \sqrt{n} \det(L)^{1/n}$ is Minkowski's theorem.
2. Let v be the shortest vector of L . Define $L'=(v)$.
(i.e. L' is generated by vectors $v, vx, vx^2, \dots vx^{n-1}$)

L' is a sublattice of L , so we have

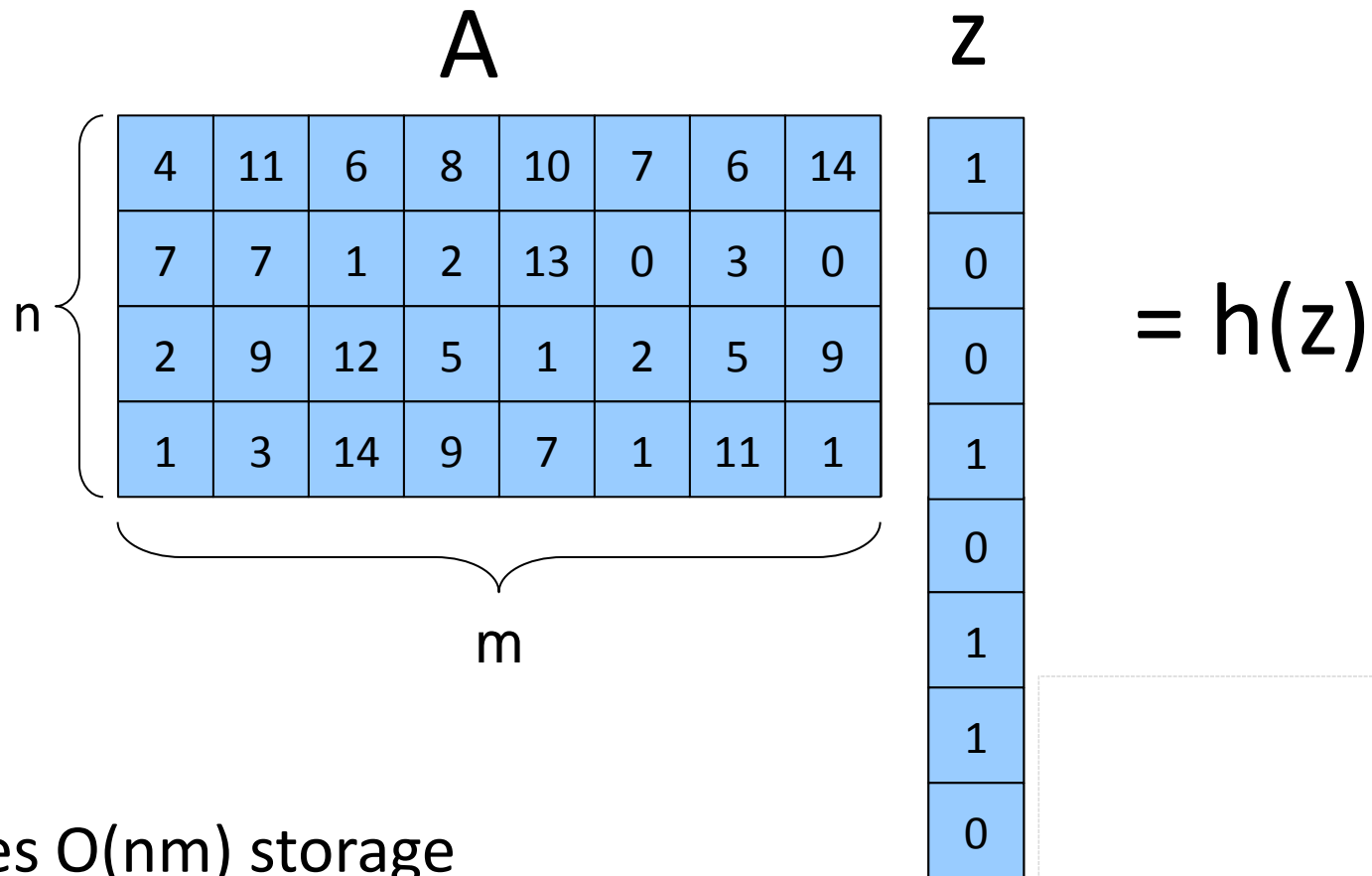
$$\det(L) \leq \det(L') \leq \|v\|^n = (\lambda_1(L))^n$$

RING-SIS AND HASH FUNCTIONS

[Mic '02, PeiRos '06, LyuMic '06]



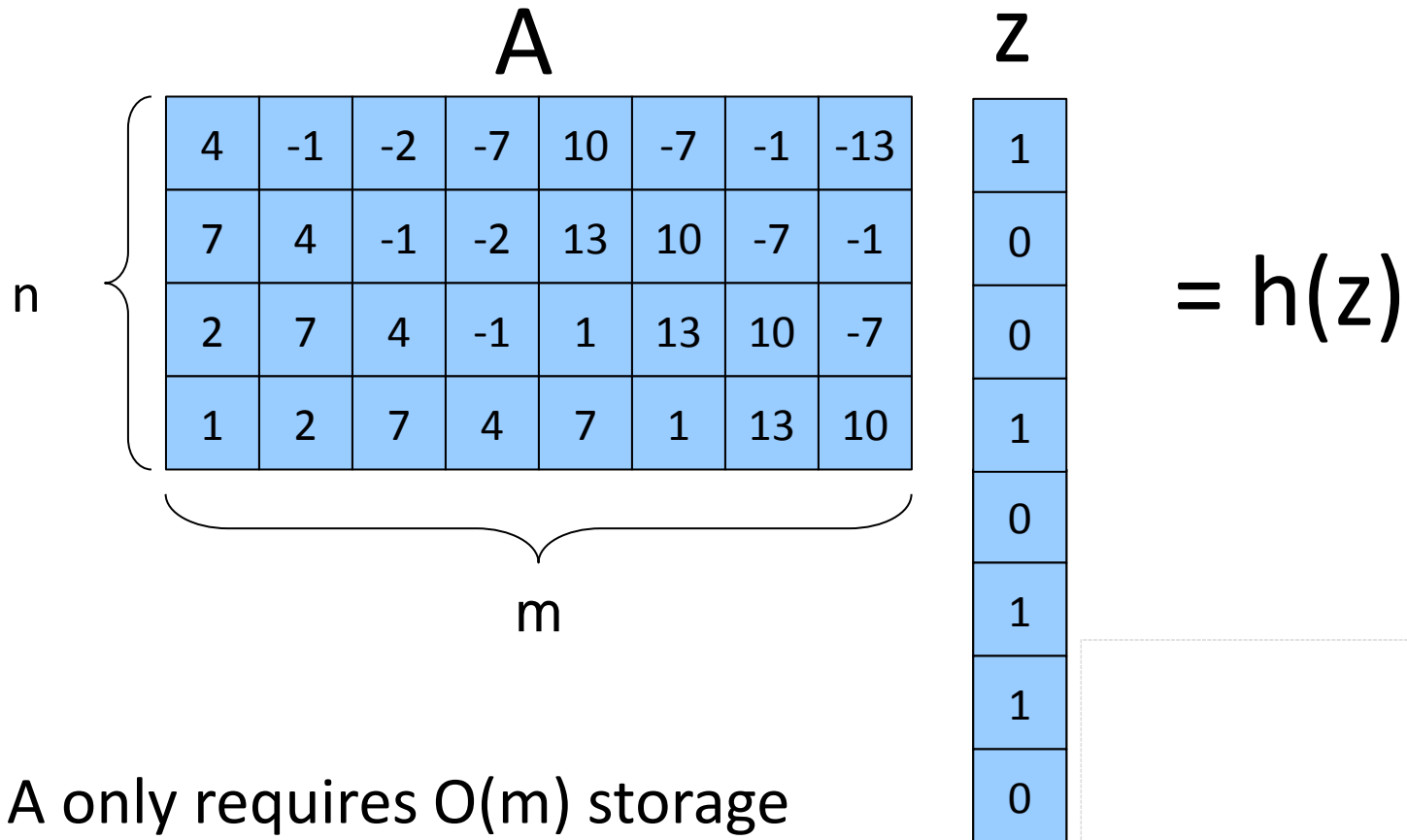
SIS Source of Inefficiency



Requires $O(nm)$ storage

Computing the function takes $O(nm)$ time

A More Efficient Idea



Now A only requires $O(m)$ storage
Az can be computed faster as well

A More Efficient Idea

A **z**

4	-1	-2	-7	10	-7	-1	-13
7	4	-1	-2	13	10	-7	-1
2	7	4	-1	1	13	10	-7
1	2	7	4	7	1	13	10

1
0
0
1
1
0

=

4	-1	-2	-7
7	4	-1	-2
2	7	4	-1
1	2	7	4

1
0
0
1

+

10	-7	-1	-13
13	10	-7	-1
1	13	10	-7
7	1	13	10

0
1
1
0

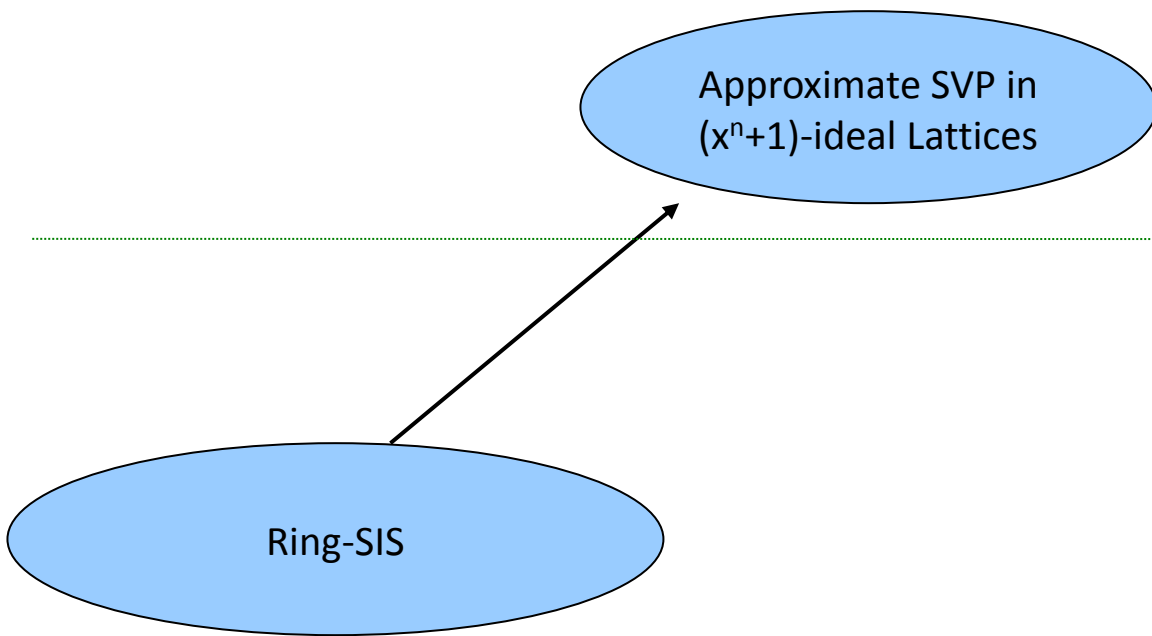
$$(4+7x+2x^2+x^3)(1+x^3) + (10+13x+x^2+7x^3)(x+x^2)$$

in $\mathbb{Z}_p[x]/(x^n+1)$

Ring-SIS

Given k random polynomials a_1, \dots, a_k in $\mathbf{Z}_p[x]/(x^n+1)$,
find “small” polynomials z_1, \dots, z_k such that

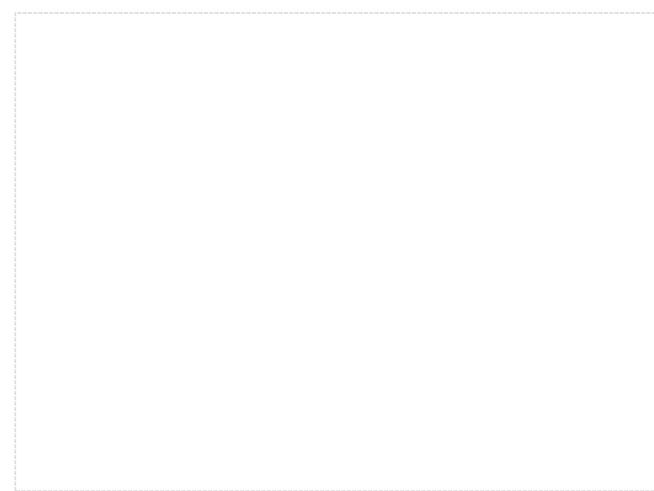
$$a_1 z_1 + \dots + a_k z_k = 0$$



Worst-Case

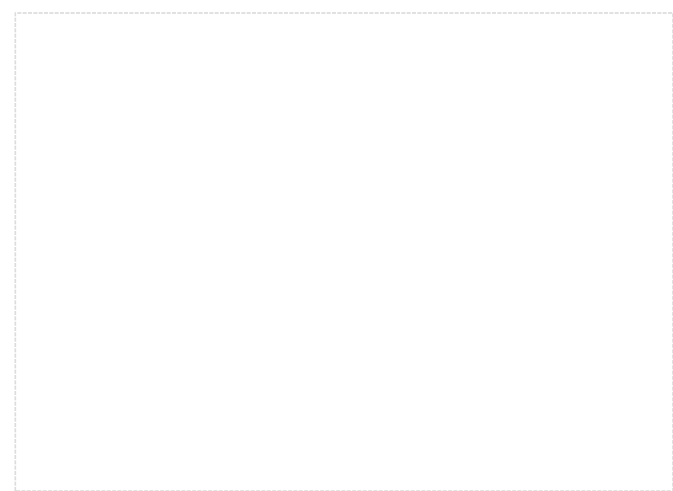
Average-Case

One-Way Functions
Collision-Resistant Hash Functions
Digital Signatures
Identification Schemes
(Minicrypt)

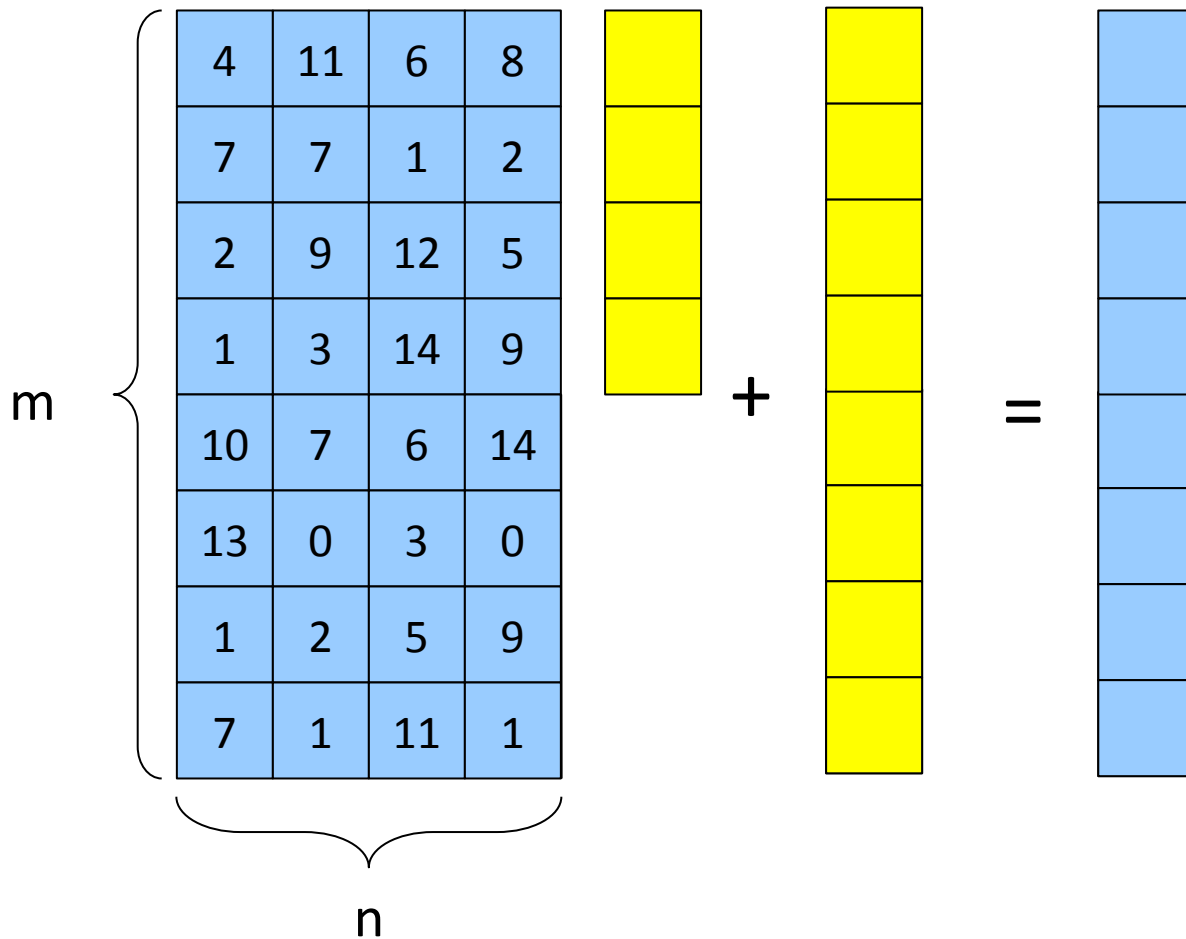


RING-LWE

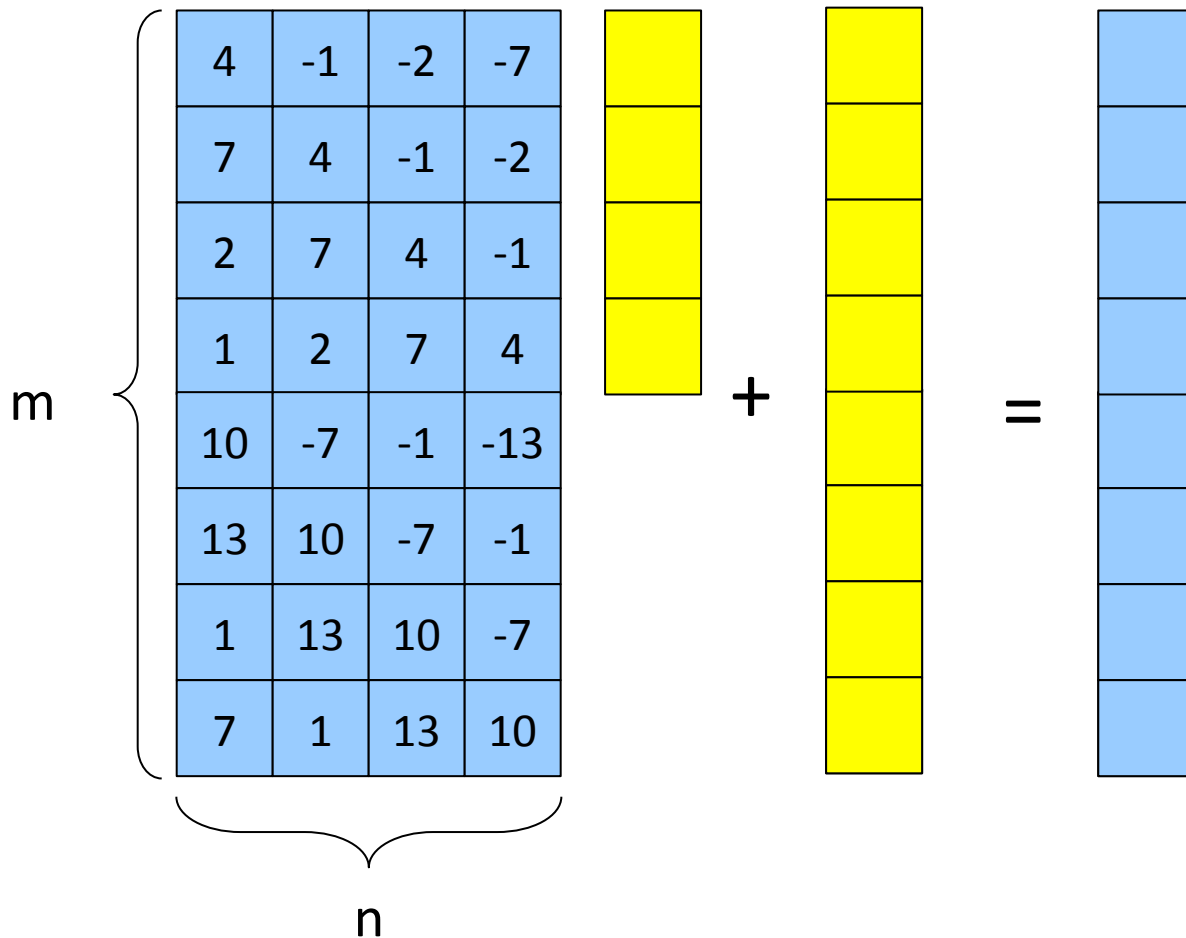
[LyuPeiReg '10]



Source of Inefficiency in LWE Constructions



Use the Same “Efficient Idea”?



Approximate SVP in
(x^n+1)-ideal Lattices

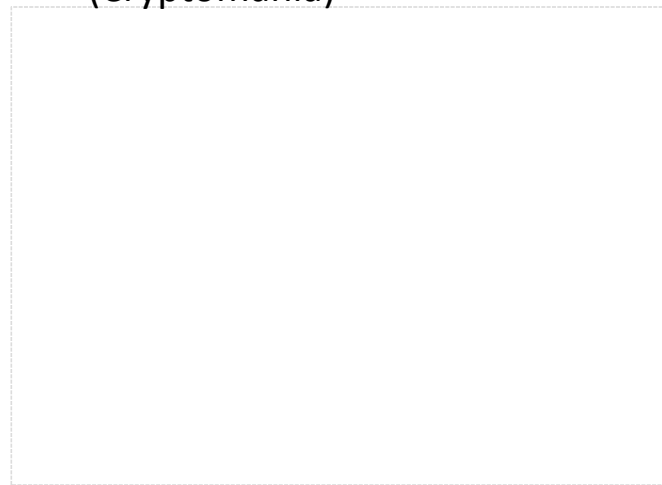
Worst-Case

Average-Case

(quantum reduction)

Learning With Errors
Problem (LWE)

Public Key Encryption ...
(Cryptomania)



Ring-LWE

Ring $R = \mathbb{Z}_q[x]/(x^n+1)$

Given:

$$a_1, a_1s + e_1$$

$$a_2, a_2s + e_2$$

...

$$a_k, a_k s + e_k$$

Find: s

s is random in R

e_i are “small” (distribution symmetric around 0)

Decision Ring-LWE

Ring $R = \mathbb{Z}_q[x]/(x^n+1)$

Given:

a_1, b_1

a_2, b_2

...

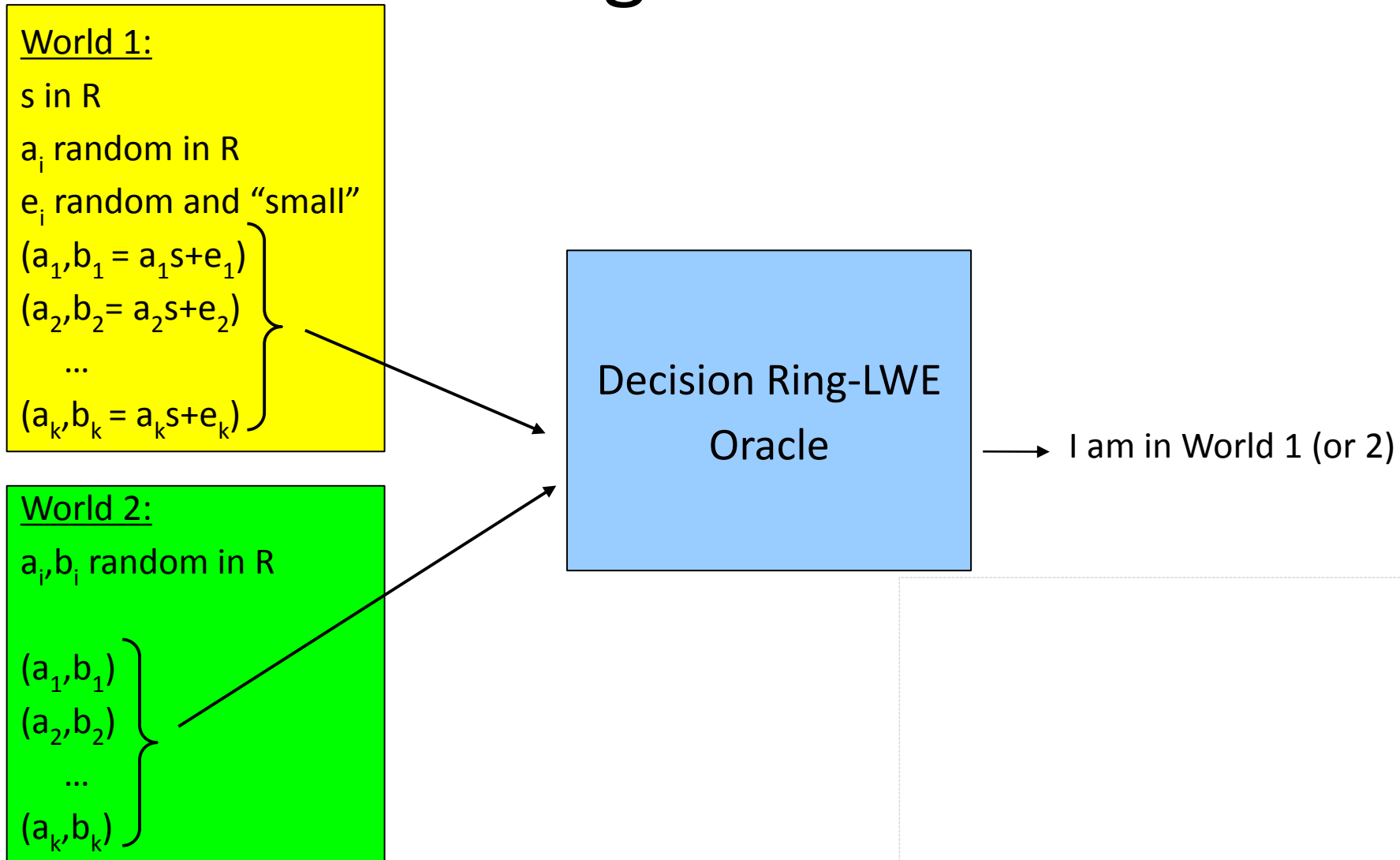
a_k, b_k

Question: Does there exist an s and “small”

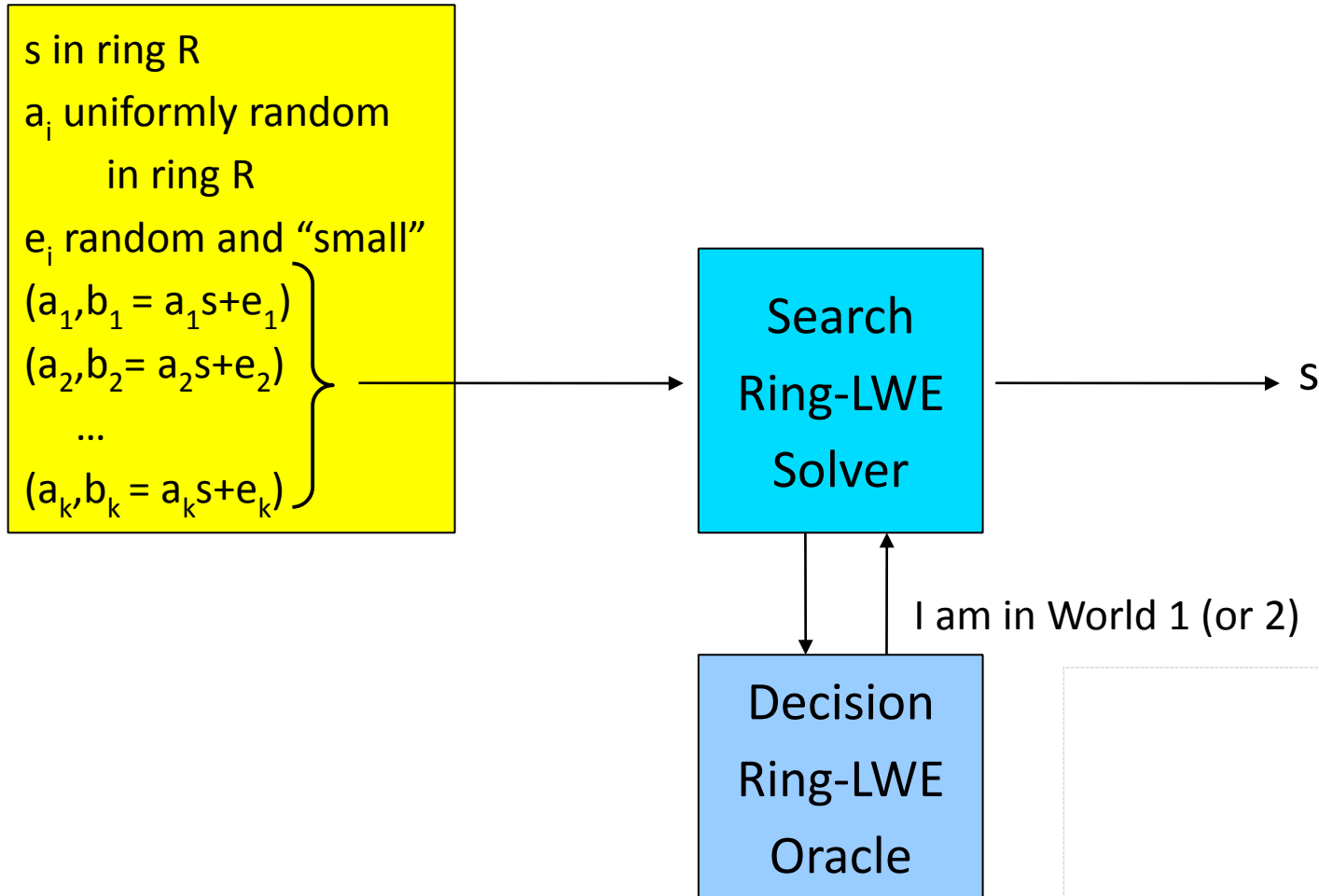
e_1, \dots, e_k such that $b_i = a_i s + e_i$

or are all b_i uniformly random in R ?

Decision Ring-LWE Problem



What We Want to Construct



The Ring $R = \mathbb{Z}_{17}[x]/(x^4+1)$

$$\begin{aligned}x^4+1 &= (x-2)(x-8)(x+2)(x+8) \pmod{17} \\ &= (x-2)(x-2^3)(x-2^5)(x-2^7) \pmod{17}\end{aligned}$$

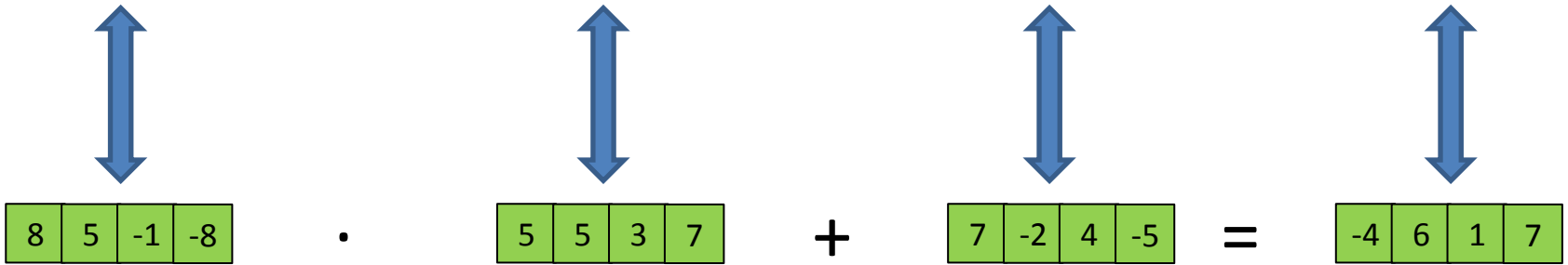
Every polynomial z in R has a unique “Chinese Remainder” representation $(z(2), z(8), z(-2), z(-8))$

For any c in \mathbb{Z}_{17} , and two polynomials z, z'

- $z(c)+z'(c) = (z+z')(c)$
- $z(c)\cdot z'(c) = (z\cdot z')(c)$

Example

$$(1 + x + 7x^2 - 5x^3) \cdot (5 - 3x + 4x^2 + 3x^3) + (1 + x - x^2 + x^3) = (-6 + 2x - x^2 - 4x^3)$$



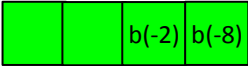
Representation of Elements in

$$R = \mathbb{Z}_{17}[x]/(x^4+1)$$

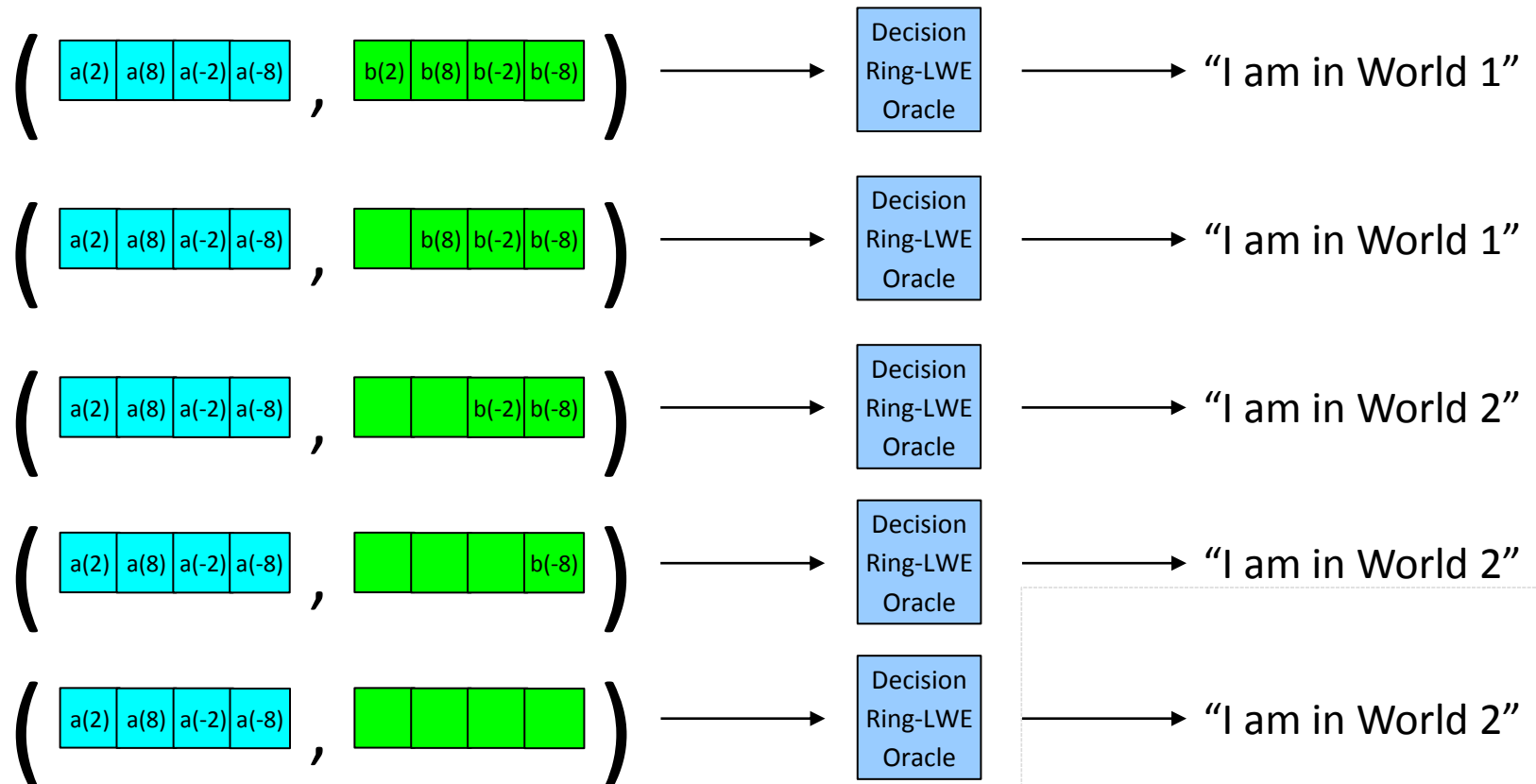
$$\begin{aligned} (x^4+1) &= (x-2)(x-2^3)(x-2^5)(x-2^7) \pmod{17} \\ &= (x-2)(x-8)(x+2)(x+8) \end{aligned}$$

Represent polynomials $z(x)$ as $(z(2), z(8), z(-2), z(-8))$

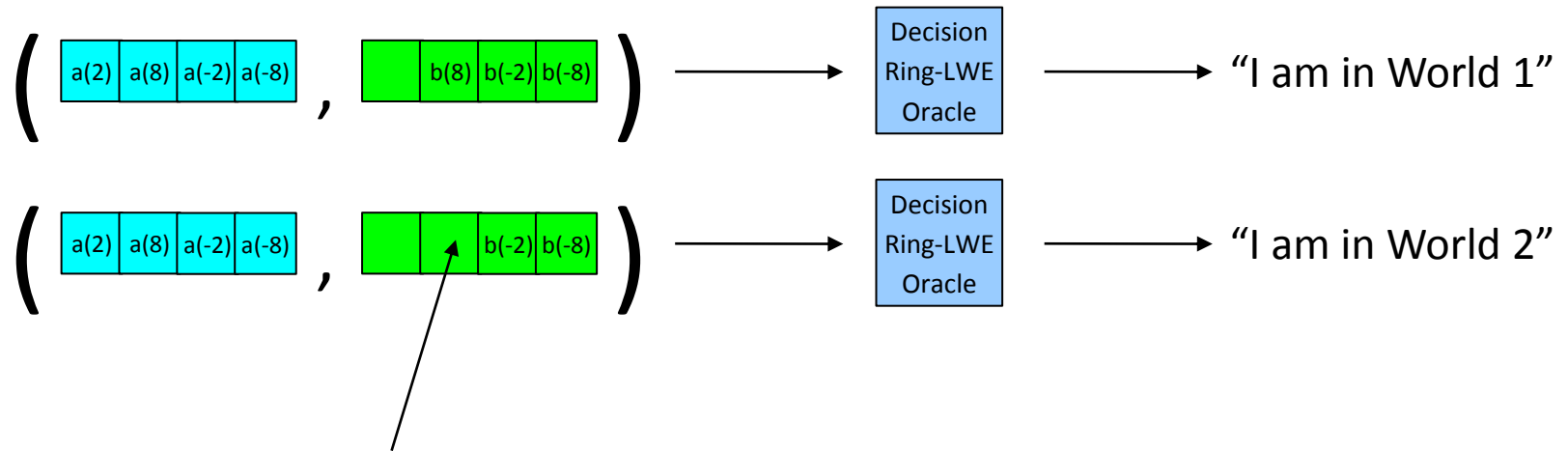
$$\longrightarrow (a(x), b(x)) = \left(\begin{array}{|c|c|c|c|} \hline a(2) & a(8) & a(-2) & a(-8) \\ \hline \end{array}, \begin{array}{|c|c|c|c|} \hline b(2) & b(8) & b(-2) & b(-8) \\ \hline \end{array} \right)$$

Notation:  means that the coefficients that should be $b(2)$ and $b(8)$ are instead uniformly random

Learning One Position of the Secret



Learning One Position of the Secret



Can learn whether this position is random or $b(8)=a(8)\cdot s(8)+e(8)$

This can be used to learn $s(8)$

Learning One Position of the Secret

Let g in \mathbb{Z}_{17} be our guess for $s(8)$ (there are 17 possibilities)

We will use the decision Ring-LWE oracle to test the guess

→ $\left(\begin{array}{|c|c|c|c|} \hline a(2) & a(8) & a(-2) & a(-8) \\ \hline \end{array}, \begin{array}{|c|c|c|c|} \hline b(2) & b(8) & b(-2) & b(-8) \\ \hline \end{array} \right)$

Make the first position of $f(b)$ uniformly random in \mathbb{Z}_{17}

$$\left(\begin{array}{|c|c|c|c|} \hline a(2) & a(8) & a(-2) & a(-8) \\ \hline \end{array}, \begin{array}{|c|c|c|c|} \hline & b(8) & b(-2) & b(-8) \\ \hline \end{array} \right)$$

Pick random r in \mathbb{Z}_{17}

$$\left(\begin{array}{|c|c|c|c|} \hline a(2) & a(8)+r & a(-2) & a(-8) \\ \hline \end{array}, \begin{array}{|c|c|c|c|} \hline & b(8)+gr & b(-2) & b(-8) \\ \hline \end{array} \right)$$

Send to the decision oracle

If $g=s(8)$, then $(a(8)+r) \cdot s(8) + e(8) = b(8) + gr$ (Oracle says “W. 1”)

If $g \neq s(8)$, then $b(8)+gr$ is uniformly random in \mathbb{Z}_{17} (Oracle says “W. 2”)

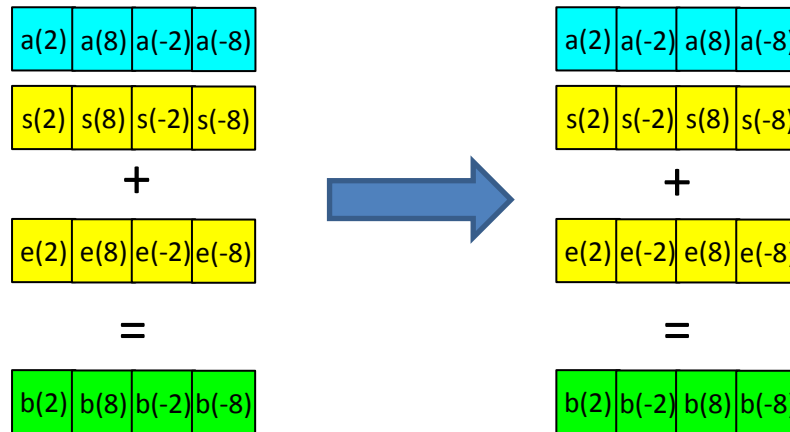
Learning the Other Positions

- We can use the decision oracle to learn $s(8)$
- How do we learn $s(2), s(-2)$, and $s(-8)$?
- Idea: Permute the input to the oracle

Make the oracle give us $s'(8)$ for a different, but related, secret s' .

From $s'(8)$ we can recover $s(2)$
(and $s(-2)$ and $s(-8)$)

A Possible Swap



Send to the decision oracle

$$\left(\begin{array}{|c|c|c|c|} \hline a(2) & a(-2) & a(8) & a(-8) \\ \hline \end{array}, \begin{array}{|c|c|c|c|} \hline b(2) & b(-2) & b(8) & b(-8) \\ \hline \end{array} \right)$$

Is this a valid distribution??

A Possible Swap

$5 - 3x + 4x^2 + 3x^3$	<table border="1" style="background-color: cyan; text-align: center;"><tr><td>5</td><td>5</td><td>3</td><td>7</td></tr></table>	5	5	3	7	→	<table border="1" style="background-color: cyan; text-align: center;"><tr><td>5</td><td>3</td><td>5</td><td>7</td></tr></table>	5	3	5	7	$5 + x + 8x^3$
5	5	3	7									
5	3	5	7									
$1 + x + 7x^2 - 5x^3$	<table border="1" style="background-color: yellow; text-align: center;"><tr><td>8</td><td>5</td><td>-1</td><td>-8</td></tr></table>	8	5	-1	-8		<table border="1" style="background-color: yellow; text-align: center;"><tr><td>8</td><td>-1</td><td>5</td><td>-8</td></tr></table>	8	-1	5	-8	$1 - x - 5x^2 - 7x^3$
8	5	-1	-8									
8	-1	5	-8									
$1 + x - x^2 + x^3$	<table border="1" style="background-color: yellow; text-align: center;"><tr><td>7</td><td>-2</td><td>4</td><td>-5</td></tr></table>	7	-2	4	-5	<table border="1" style="background-color: yellow; text-align: center;"><tr><td>7</td><td>4</td><td>-2</td><td>-5</td></tr></table>	7	4	-2	-5	$1 + 3x - 6x^2 + 3x^3$	
7	-2	4	-5									
7	4	-2	-5									
$-6 + 2x - x^2 - 4x^3$	<table border="1" style="background-color: green; text-align: center;"><tr><td>-4</td><td>6</td><td>1</td><td>7</td></tr></table>	-4	6	1	7	<table border="1" style="background-color: green; text-align: center;"><tr><td>-4</td><td>1</td><td>6</td><td>7</td></tr></table>	-4	1	6	7	$-6 + 6x + 6x^2$	
-4	6	1	7									
-4	1	6	7									

WRONG DISTRIBUTION !!

Send to the decision oracle

$$\left(\begin{array}{|c|c|c|c|} \hline 5 & 3 & 5 & 7 \\ \hline \end{array} , \begin{array}{|c|c|c|c|} \hline -4 & 1 & 6 & 7 \\ \hline \end{array} \right)$$

Is this a valid distribution??

Automorphisms of R

$$x^4+1 = (x-2)(x-2^3)(x-2^5)(x-2^7) \pmod{17}$$

	2	2^3	2^5	2^7	← roots of x^4+1
$z(x)$	$z(2)$	$z(2^3)$	$z(2^5)$	$z(2^7)$	
$z(x^3)$	$z(2^3)$	$z(2)$	$z(2^7)$	$z(2^5)$	
$z(x^5)$	$z(2^5)$	$z(2^7)$	$z(2)$	$z(2^3)$	
$z(x^7)$	$z(2^7)$	$z(2^5)$	$z(2^3)$	$z(2)$	

Automorphisms of \mathbb{R}

$$z(x) = z_0 + z_1x + z_2x^2 + z_3x^3$$

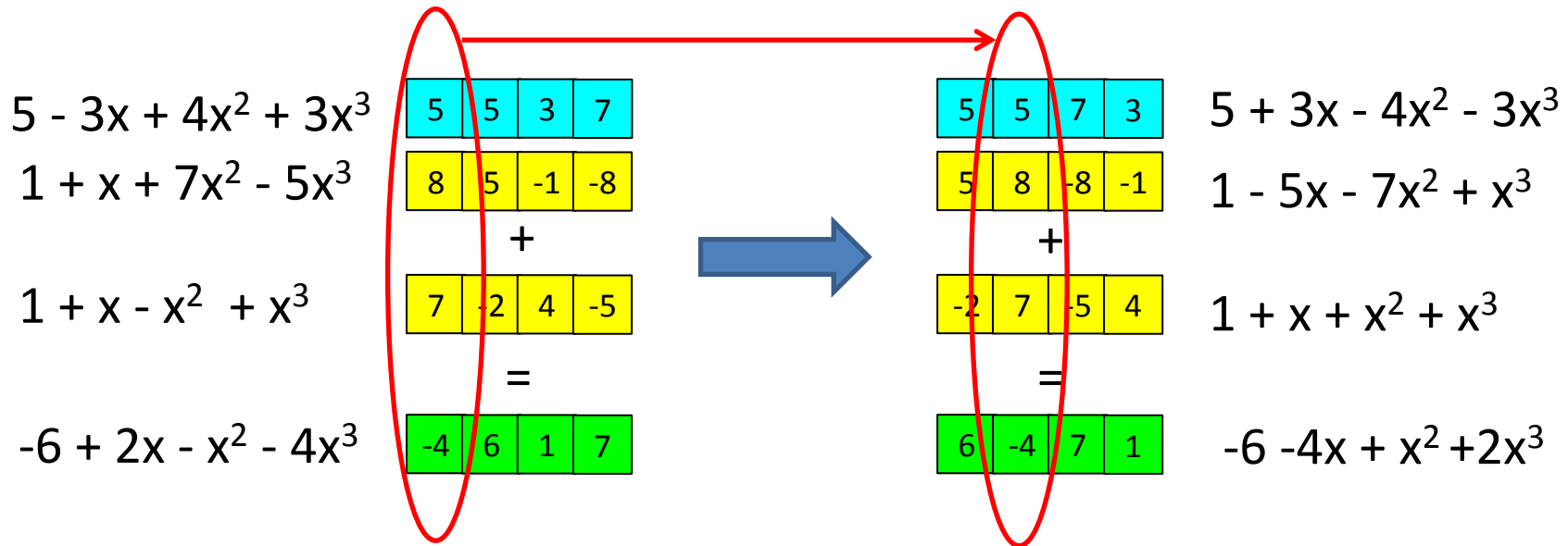
$$z(x^3) = z_0 + z_1x^3 + z_2x^6 + z_3x^9 = z_0 + z_3x - z_2x^2 + z_1x^3$$

$$z(x^5) = z_0 + z_1x^5 + z_2x^{10} + z_3x^{15} = z_0 - z_1x + z_2x^2 - z_3x^3$$

$$z(x^7) = z_0 + z_1x^7 + z_2x^{14} + z_3x^{21} = z_0 - z_3x - z_2x^2 - z_1x^3$$

If coefficients of $z(x)$ have distribution D symmetric around 0, then so do the coefficients of $z(x^3)$, $z(x^5)$, $z(x^7)$!!

A Correct Swap



Send to the decision oracle

$$\left(\begin{array}{|c|c|c|c|} \hline 5 & 5 & 7 & 3 \\ \hline \end{array} , \begin{array}{|c|c|c|c|} \hline 6 & -4 & 7 & 1 \\ \hline \end{array} \right)$$

This will recover $s(2)$.

Repeat the analogous procedure to recover $s(-2)$, $s(-8)$

A Caveat ...

“If coefficients of $z(x)$ have distribution D symmetric around 0, then so do the coefficients of $z(x^3)$, $z(x^5)$, $z(x^7)$!! ”

This only holds true for $Z[x]/(x^n+1)$

The correct error distribution is somewhat different for other polynomials.

Can work with all *cyclotomic* polynomials.

References

- [Daniele Micciancio](#) (2002): Generalized Compact Knapsacks, Cyclic Lattices, and Efficient One-Way Functions
- [Chris Peikert, Alon Rosen](#) (2006): Efficient Collision-Resistant Hashing from Worst-Case Assumptions on Cyclic Lattices.
- [Vadim Lyubashevsky, Daniele Micciancio](#) (2006): Generalized Compact Knapsacks Are Collision Resistant
- [Vadim Lyubashevsky, Chris Peikert, Oded Regev](#) (2010): On Ideal Lattices and Learning with Errors over Rings.