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

-1	2	3	-4		+		-7	-2	3	6		=		-8	0	6	2	

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

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

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

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

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

-1	2	3	-4

+

-7	-2	3	6

=

-8	0	6	2

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

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

-1	2	3	-4

1	-2	-3	4

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

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

-1	2	3	-4	$-1+2x+3x^2-4x^3$
-4	-1	2	3	$(-1+2x+3x^2-4x^3)x=-4-x+2x^2+3x^3$
3	-4	-1	2	$(-1+2x+3x^2-4x^3)x^2 =3-4x-x^2+2x^3$
2	3	-4	-1	$(-1+2x+3x^2-4x^3)x^3 =2+3x-4x^2-x^3$

Why Cyclic Lattices?

- Succinct representations
  - Can represent an n-dimensional lattice with 1 vector

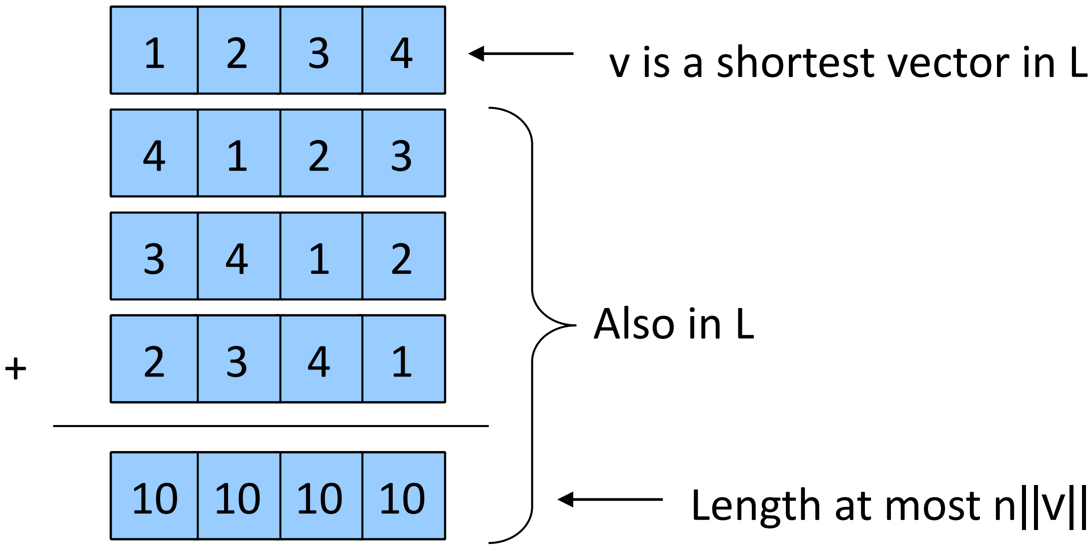
- Algebraic structure
  - Allows for fast arithmetic (using FFT)
  - Makes proofs possible

- NTRU cryptosystem
- One-way functions based on worst-case hardness of SVP in ideal lattices [Mic02]

Is $SVP_{poly(n)}$ 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?

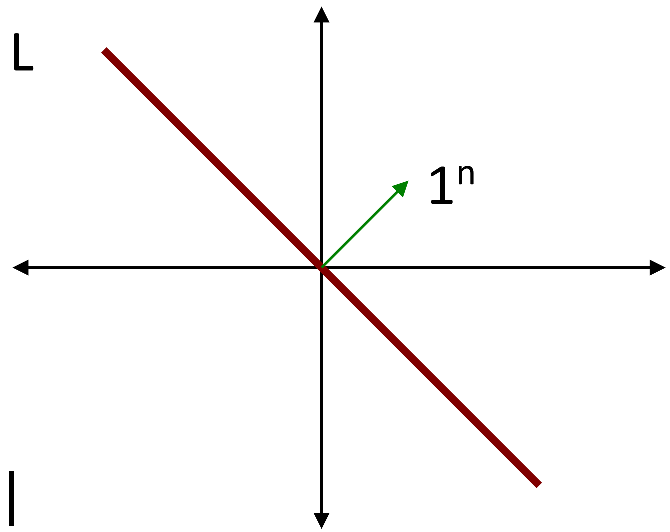


Algorithm for solving $SVP_n(L)$ for a cyclic lattice L:

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

The Hard Cyclic Lattice Instances

	-1	2	3	-4	← v is a shortest vector in L
	-4	-1	2	3	
	3	-4	-1	2	Also in L
+	2	3	-4	-1	
	0	0	0	0	← Length at most n‖v‖



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

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

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

f-Ideal Lattices = Ideals in **Z**[x]/(f)

<u>Want f to have 3 properties:</u>

1) Monic (i.e. coefficient of largest exponent is 1)
2) Irreducible over **Z**
3) For all polynomials g,h $||gh \bmod f|| < \text{poly}(n)||g|| \cdot ||h||$

<u>Conjecture:</u> For all f that satisfy the above 3 properties, solving $SVP_{poly(n)}$ for ideals in **Z**[x]/(f) takes time $2^{\Omega(n)}$.

<u>Some "good" f to use:</u>

$f=x^{n-1}+x^{n-2}+\ldots+1$ 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

-1	2	3	-4	+	-7	-2	3	6	=	-8	0	6	2

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

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

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

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

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

-1	2	3	-4	$-1+2x+3x^2-4x^3$
4	-1	2	3	$(-1+2x+3x^2-4x^3)x=4-x+2x^2+3x^3$
-3	4	-1	2	$(-1+2x+3x^2-4x^3)x^2 =-3+4x-x^2+2x^3$
-2	-3	4	-1	$(-1+2x+3x^2-4x^3)x^3 =-2-3x+4x^2-x^3$

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 **Z**[x]/(f) where f is a monic, irreducible polynomial of degree n, then

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

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.

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

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

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

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

Proof of fact:

1. $\lambda_1(L) \le \sqrt{n}\,\det(L)^{1/n}$ is Minkowski's theorem.
2. Let v be the shortest vector of L. Define L'=(v).

   (i.e. L' is generated by vectors $v, vx, vx^2, \ldots vx^{n-1}$)

   L' is a sublattice of L, so we have

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

RING-SIS AND HASH FUNCTIONS

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

SIS Source of Inefficiency

$$n\left\{\overset{A}{\underbrace{\begin{bmatrix} 4 & 11 & 6 & 8 & 10 & 7 & 6 & 14 \\ 7 & 7 & 1 & 2 & 13 & 0 & 3 & 0 \\ 2 & 9 & 12 & 5 & 1 & 2 & 5 & 9 \\ 1 & 3 & 14 & 9 & 7 & 1 & 11 & 1 \end{bmatrix}}_{m}}\right. \overset{z}{\begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}} = h(z)$$

Requires O(nm) storage

Computing the function takes O(nm) time

A More Efficient Idea

$$n\left\{\overset{A}{\underbrace{\begin{bmatrix} 4 & -1 & -2 & -7 & 10 & -7 & -1 & -13 \\ 7 & 4 & -1 & -2 & 13 & 10 & -7 & -1 \\ 2 & 7 & 4 & -1 & 1 & 13 & 10 & -7 \\ 1 & 2 & 7 & 4 & 7 & 1 & 13 & 10 \end{bmatrix}}_{m}}\right. \overset{z}{\begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}} = h(z)$$

Now A only requires O(m) storage

Az can be computed faster as well

A More Efficient Idea

$$\underbrace{\begin{bmatrix} 4 & -1 & -2 & -7 & 10 & -7 & -1 & -13 \\ 7 & 4 & -1 & -2 & 13 & 10 & -7 & -1 \\ 2 & 7 & 4 & -1 & 1 & 13 & 10 & -7 \\ 1 & 2 & 7 & 4 & 7 & 1 & 13 & 10 \end{bmatrix}}_{A} \underbrace{\begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}}_{z} = \begin{bmatrix} 4 & -1 & -2 & -7 \\ 7 & 4 & -1 & -2 \\ 2 & 7 & 4 & -1 \\ 1 & 2 & 7 & 4 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 10 & -7 & -1 & -13 \\ 13 & 10 & -7 & -1 \\ 1 & 13 & 10 & -7 \\ 7 & 1 & 13 & 10 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

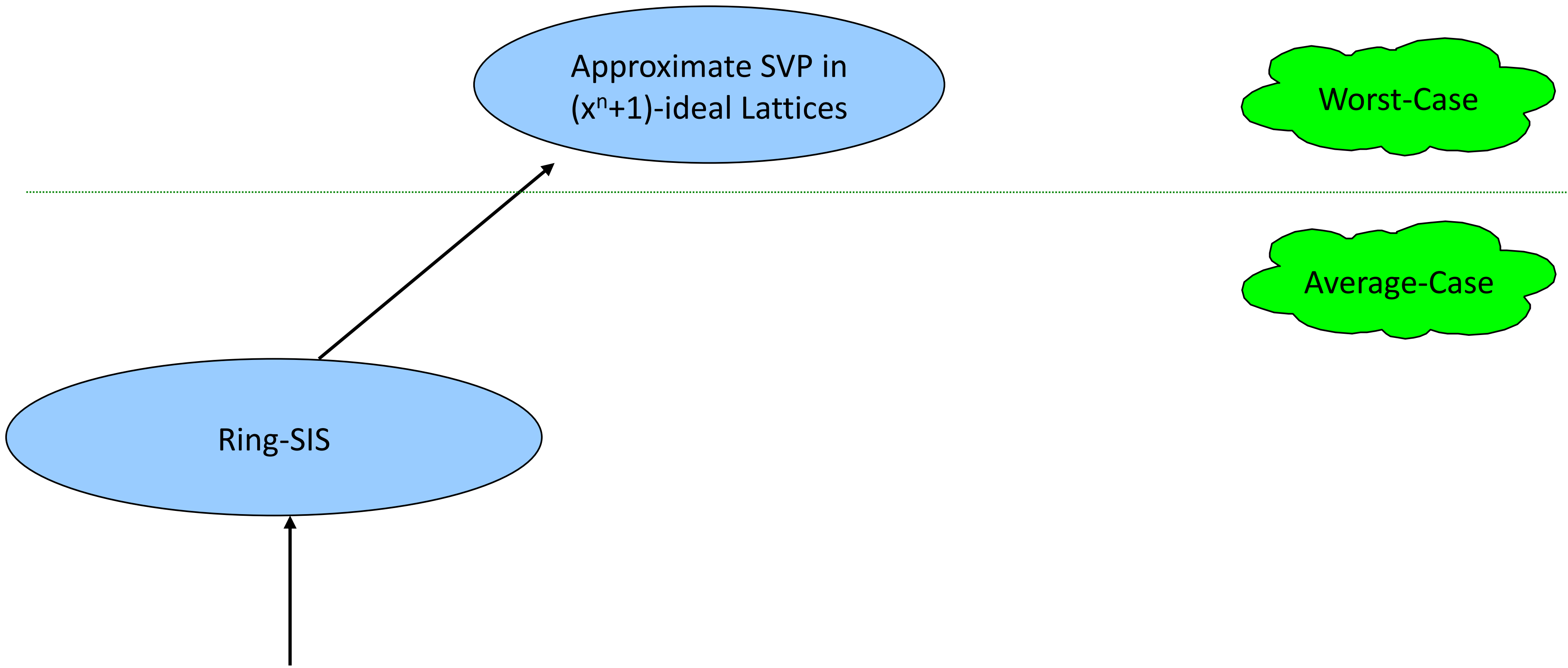
$$(4+7x+2x^2+x^3)(1+x^3) + (10+13x+x^2+7x^3)(x+x^2)$$

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

Ring-SIS

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

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



One-Way Functions

Collision-Resistant Hash Functions

Digital Signatures

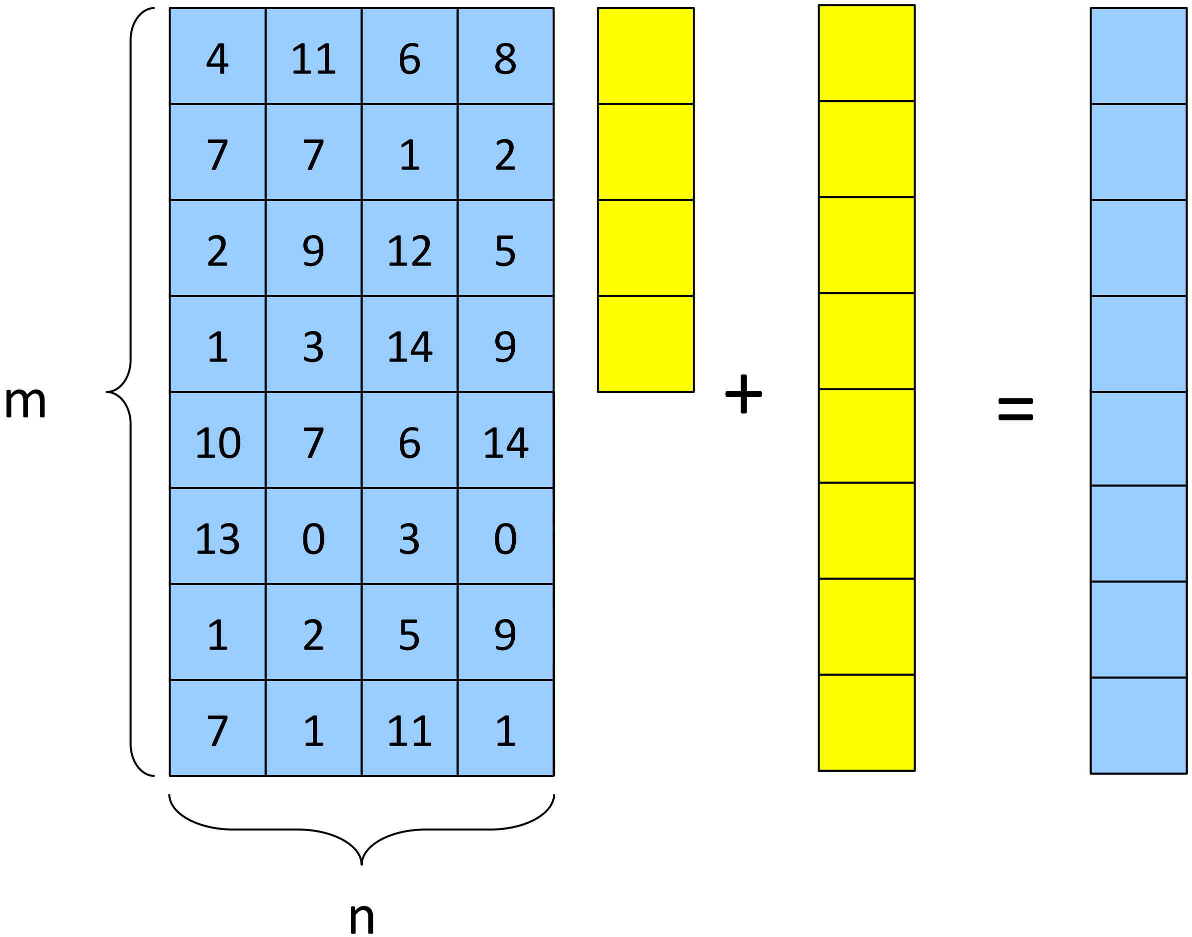
Identification Schemes

(Minicrypt)

RING-LWE

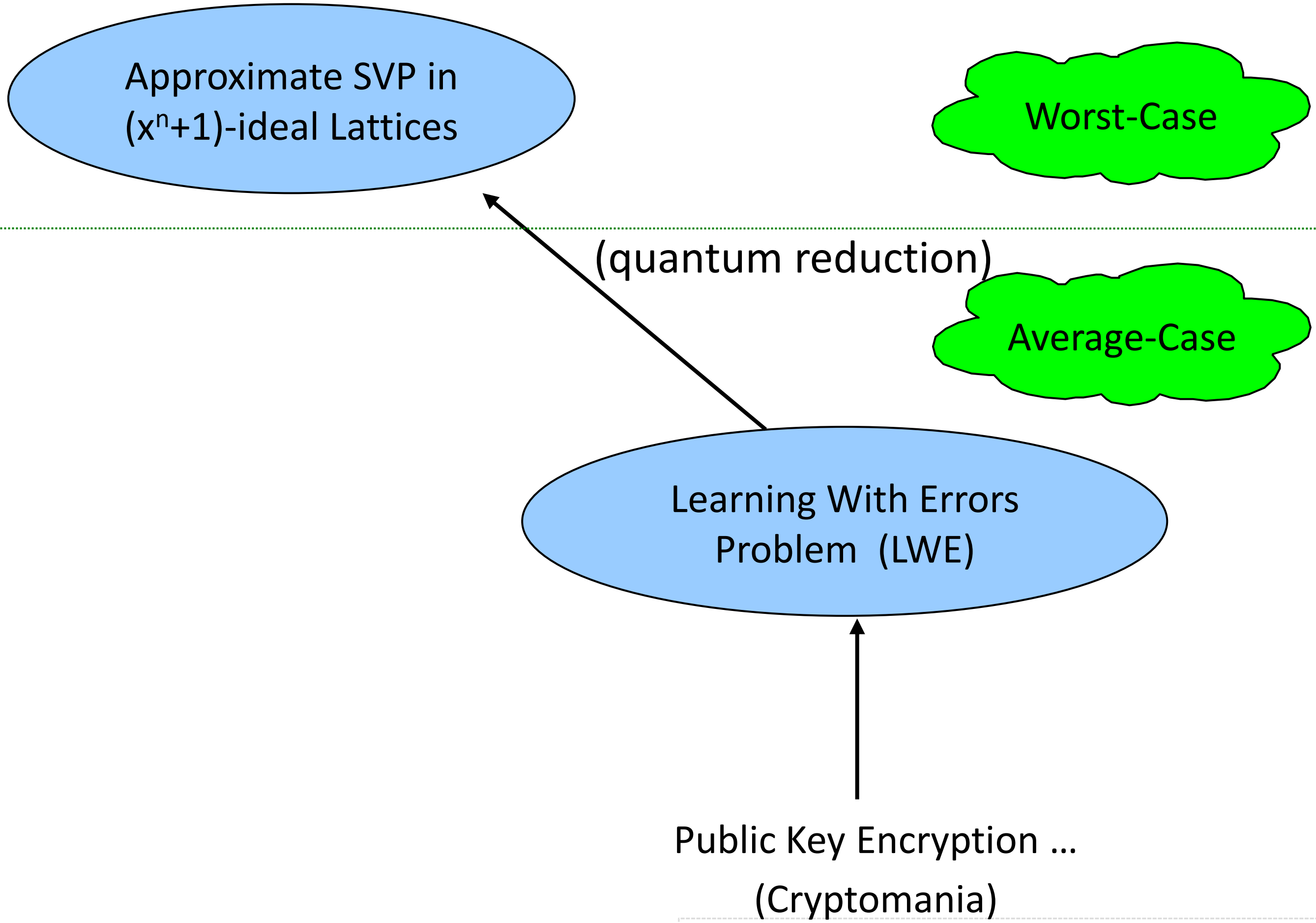
[LyuPeiReg ‘10]

Source of Inefficiency in LWE Constructions



Use the Same “Efficient Idea”?

$$m\left\{\underbrace{\begin{bmatrix}4&-1&-2&-7\\7&4&-1&-2\\2&7&4&-1\\1&2&7&4\\10&-7&-1&-13\\13&10&-7&-1\\1&13&10&-7\\7&1&13&10\end{bmatrix}}_{n}\right. \begin{bmatrix}\ \\ \ \\ \ \\ \ \end{bmatrix} + \begin{bmatrix}\ \\ \ \\ \ \\ \ \\ \ \\ \ \\ \ \\ \ \end{bmatrix} = \begin{bmatrix}\ \\ \ \\ \ \\ \ \\ \ \\ \ \\ \ \\ \ \end{bmatrix}$$


Approximate SVP in
(x^n+1)-ideal Lattices
Worst-Case
(quantum reduction)
Average-Case
Learning With Errors
Problem (LWE)
Public Key Encryption …
(Cryptomania)

Ring-LWE

Ring $R = Z_q[x]/(x^n+1)$

Given:

$a_1, a_1 s + e_1$

$a_2, a_2 s + e_2$

…

$a_k, a_k s + e_k$

Find: s

s is random in R

e_i are "small" (distribution symmetric around 0)

Decision Ring-LWE

Ring $R=Z_q[x]/(x^n+1)$

Given:

a_1, b_1

a_2, b_2

…

a_k, b_k

Question: Does there exist an s and "small"

$e_1, \ldots, e_k$ such that $b_i=a_is+e_i$

or are all b_i uniformly random in R?

Decision Ring-LWE Problem

World 1:

s in R

a_i random in R

e_i random and "small"

$$\left.\begin{array}{l}(a_1, b_1 = a_1 s + e_1)\\ (a_2, b_2 = a_2 s + e_2)\\ \quad \ldots \\ (a_k, b_k = a_k s + e_k)\end{array}\right\}$$

World 2:

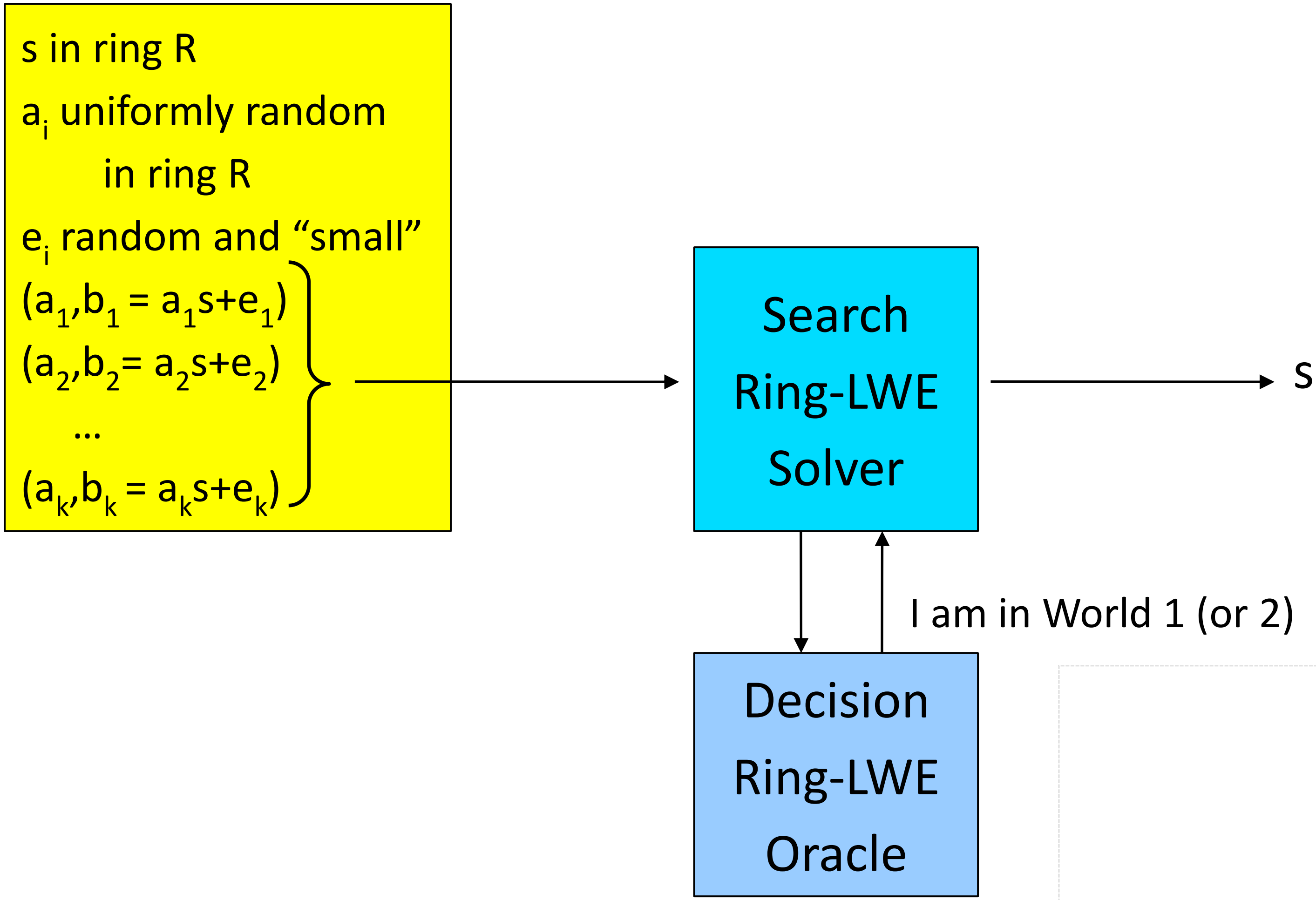
a_i, b_i random in R

$$\left.\begin{array}{l}(a_1, b_1)\\ (a_2, b_2)\\ \quad \ldots \\ (a_k, b_k)\end{array}\right\}$$

Decision Ring-LWE Oracle

$\longrightarrow$ I am in World 1 (or 2)

What We Want to Construct



The Ring $R=Z_{17}[x]/(x^4+1)$

$x^4+1 = (x-2)(x-8)(x+2)(x+8) \bmod 17$

$= (x-2)(x-2^3)(x-2^5)(x-2^7) \bmod 17$

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

For any c in Z_{17}, and two polynomials z, z'

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

Example

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

$$\begin{array}{|c|c|c|c|}\hline 8 & 5 & -1 & -8 \\ \hline\end{array} \cdot \begin{array}{|c|c|c|c|}\hline 5 & 5 & 3 & 7 \\ \hline\end{array} + \begin{array}{|c|c|c|c|}\hline 7 & -2 & 4 & -5 \\ \hline\end{array} = \begin{array}{|c|c|c|c|}\hline -4 & 6 & 1 & 7 \\ \hline\end{array}$$

Representation of Elements in $R=Z_{17}[x]/(x^4+1)$

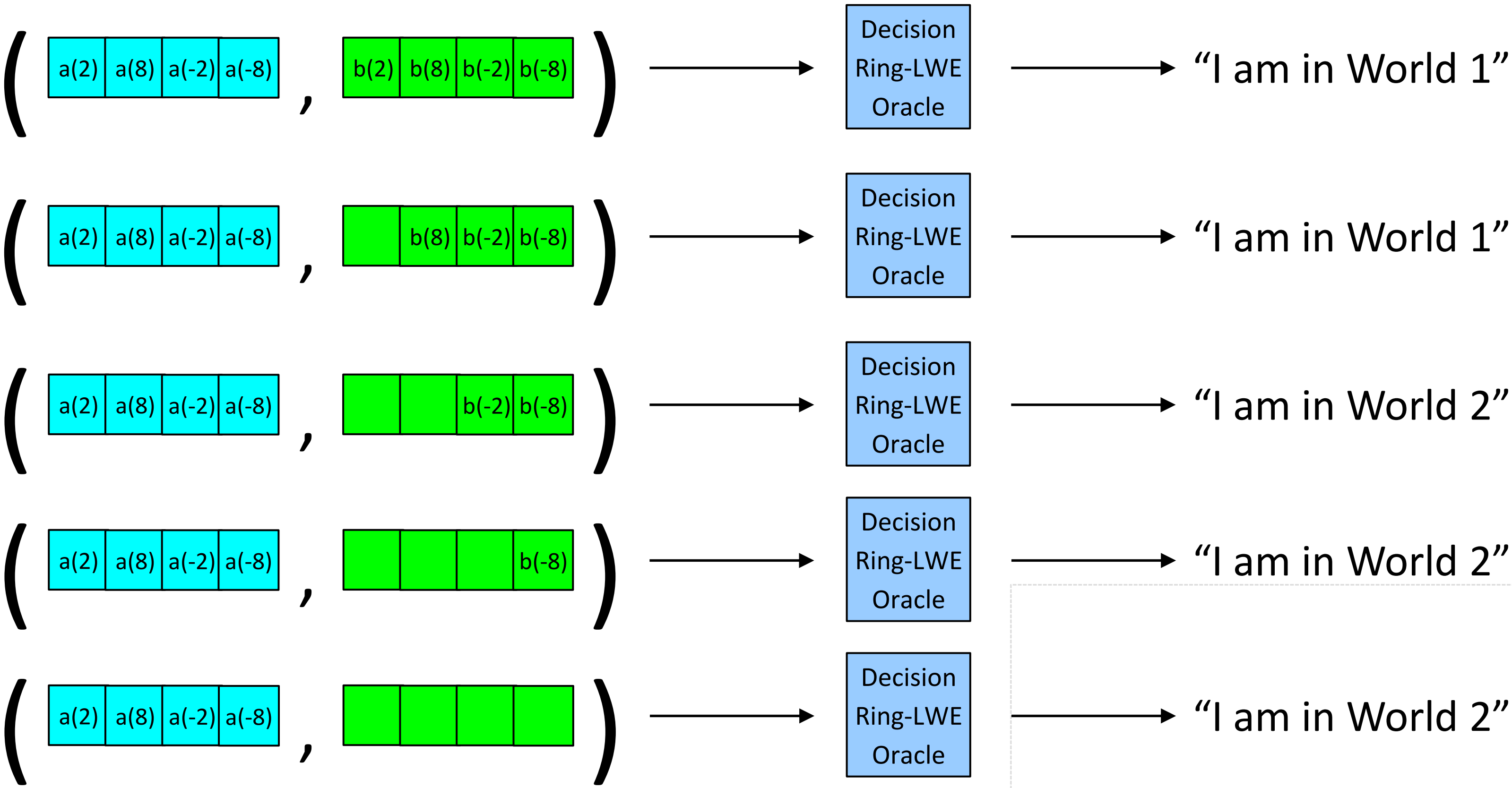
$$(x^4+1) = (x-2)(x-2^3)(x-2^5)(x-2^7) \bmod 17$$
$$= (x-2)(x-8)(x+2)(x+8)$$

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

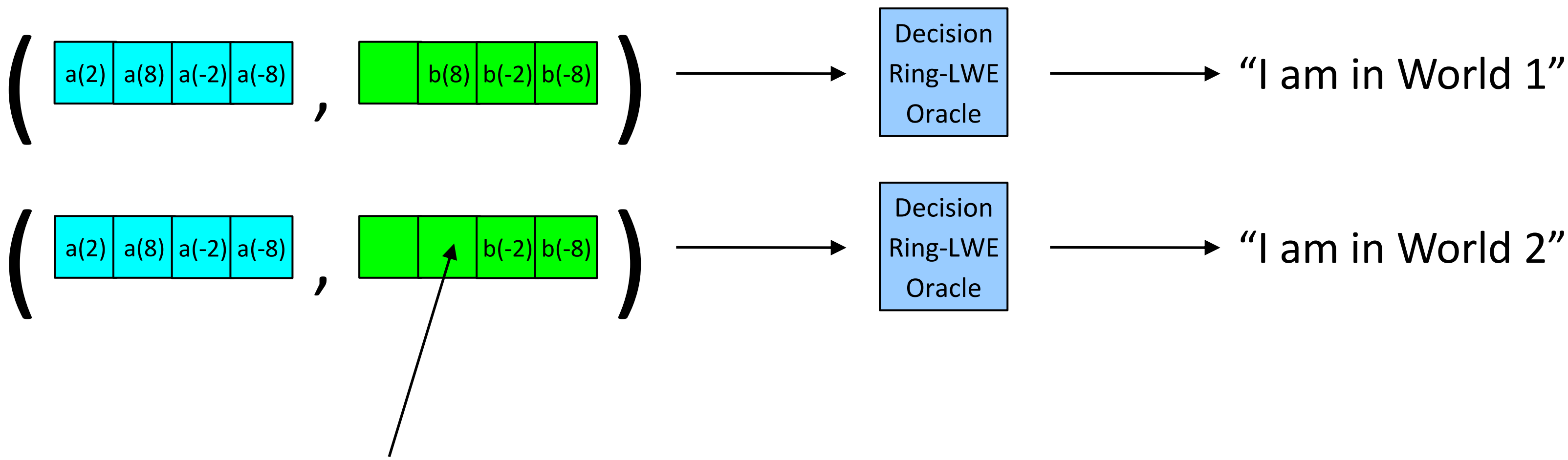
$$\longrightarrow \quad (a(x),b(x)) \quad = \quad \left(\boxed{a(2)}\boxed{a(8)}\boxed{a(-2)}\boxed{a(-8)} \; , \; \boxed{b(2)}\boxed{b(8)}\boxed{b(-2)}\boxed{b(-8)} \right)$$

Notation: $\boxed{}\boxed{}\boxed{b(-2)}\boxed{b(-8)}$ 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)·s(8)+e(8)

This can be used to learn s(8)

Learning One Position of the Secret

Let g in Z_{17} be our guess for s(8)   (there are 17 possibilities)

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

(| a(2) | a(8) | a(-2) | a(-8) | , | b(2) | b(8) | b(-2) | b(-8) |)

Make the first position of f(b) uniformly random in Z_{17}

(| a(2) | a(8) | a(-2) | a(-8) | , | | b(8) | b(-2) | b(-8) |)

Pick random r in Z_{17}

(| a(2) | a(8)+r | a(-2) | a(-8) | , | | b(8)+gr | b(-2) | b(-8) |)

Send to the decision oracle

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

If g≠s(8), then b(8)+gr is uniformly random in 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

a(2)	a(8)	a(-2)	a(-8)
s(2)	s(8)	s(-2)	s(-8)

+

e(2)	e(8)	e(-2)	e(-8)

=

b(2)	b(8)	b(-2)	b(-8)

a(2)	a(-2)	a(8)	a(-8)
s(2)	s(-2)	s(8)	s(-8)

+

e(2)	e(-2)	e(8)	e(-8)

=

b(2)	b(-2)	b(8)	b(-8)

Send to the decision oracle

(a(2) | a(-2) | a(8) | a(-8) , b(2) | b(-2) | b(8) | b(-8))

Is this a valid distribution??

A Possible Swap

$5 - 3x + 4x^2 + 3x^3$	5	5	3	7
$1 + x + 7x^2 - 5x^3$	8	5	-1	-8
	+			
$1 + x - x^2 + x^3$	7	-2	4	-5
	=			
$-6 + 2x - x^2 - 4x^3$	-4	6	1	7

5	3	5	7	$5 + x + 8x^3$
8	-1	5	-8	$1 - x - 5x^2 - 7x^3$
+				**WRONG DISTRIBUTION !!**
7	4	-2	-5	$1 + 3x - 6x^2 + 3x^3$
=				
-4	1	6	7	$-6 + 6x + 6x^2$

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

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

roots of x^4+1

$z(x)$

	2	2^3	2^5	2^7
$z(x)$	$z(2)$	$z(2^3)$	$z(2^5)$	$z(2^7)$
$z(x^3)$	$z(2^3)$	$z(2)$	$z(2^7)$	$z(2^5)$
$z(x^5)$	$z(2^5)$	$z(2^7)$	$z(2)$	$z(2^3)$
$z(x^7)$	$z(2^7)$	$z(2^5)$	$z(2^3)$	$z(2)$

Automorphisms of R

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

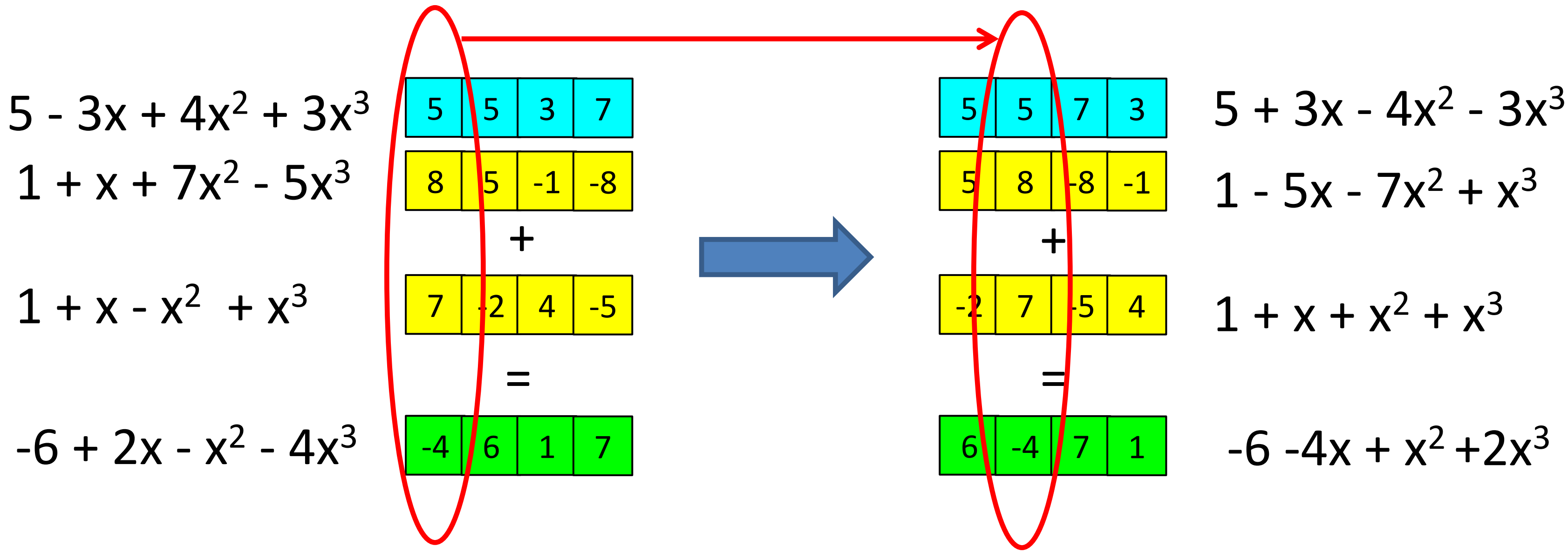
$z(x^3) = z_0 + z_1x^3 + z_2x^6 + z_3x^9 = z_0 + z_3x - z_2x^2 + z_1x^3$

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

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

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

(5 5 7 3 , 6 -4 7 1)

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.