Ideal Lattices

Vadim Lyubashevsky

INRIA / ENS, Paris

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

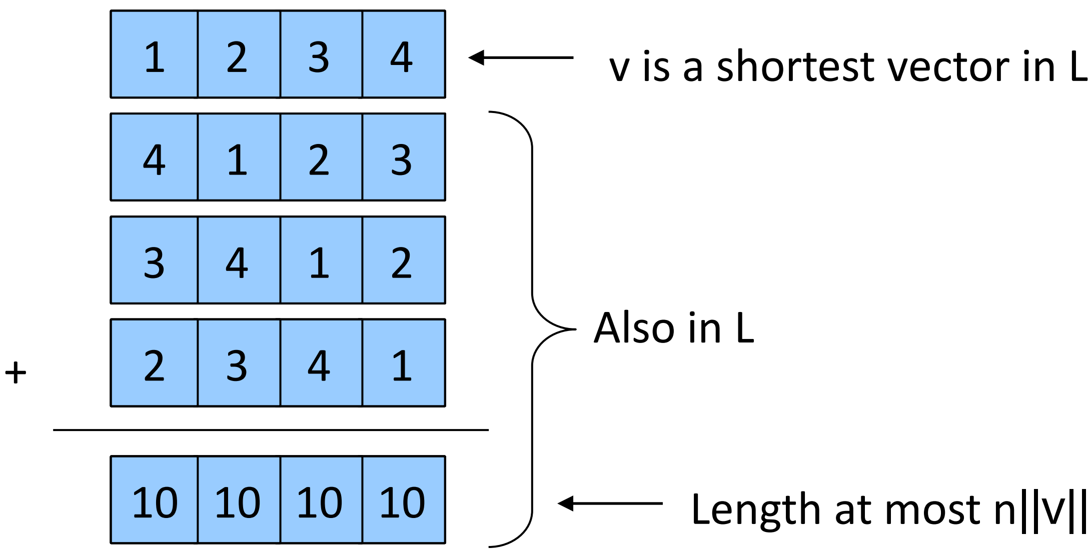
- Algebraic structure
  - Allows for fast arithmetic (using FFT)
  - Makes proofs possible

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

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

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

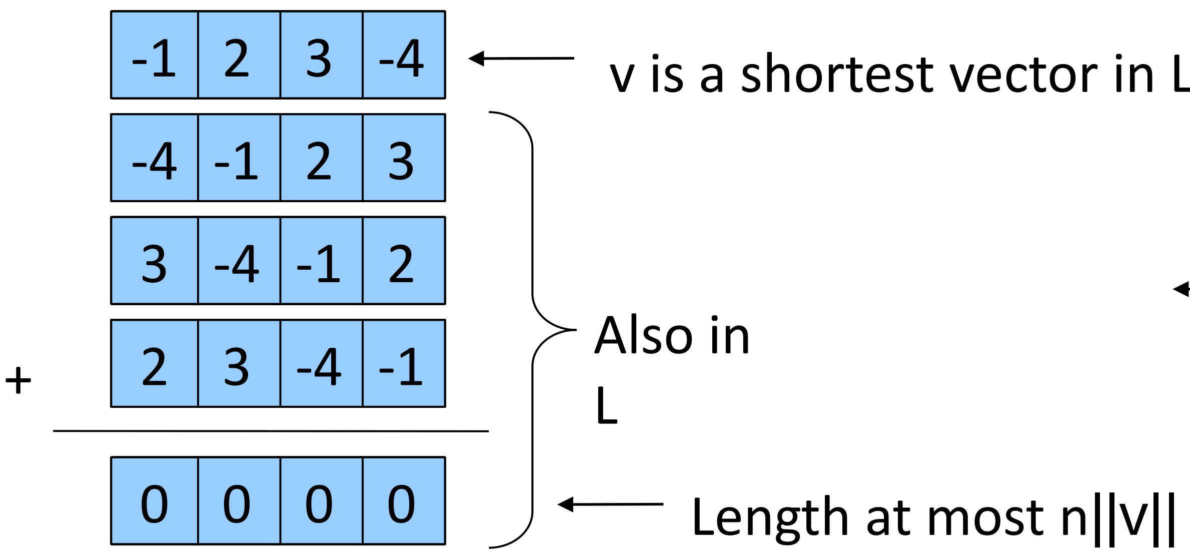
What's wrong with the following argument that SVP_n is easy?

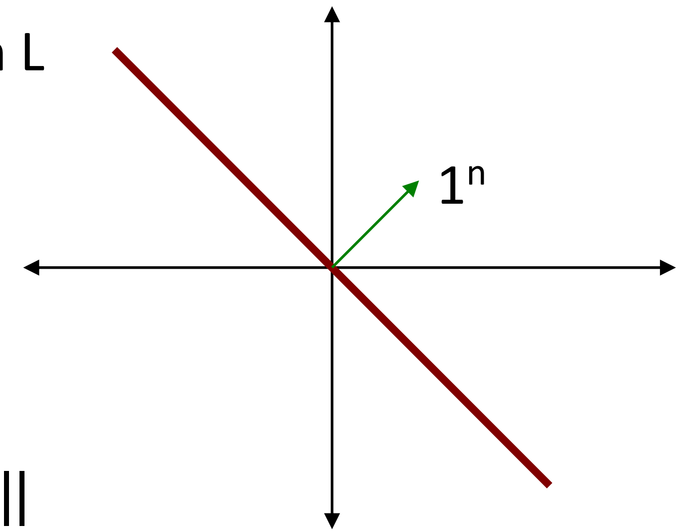


Algorithm for solving $SVP_n(L)$ for a cyclic lattice L:

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

The Hard Cyclic Lattice Instances





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)

Want f to have 3 properties:

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

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

Some "good" f to use:

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

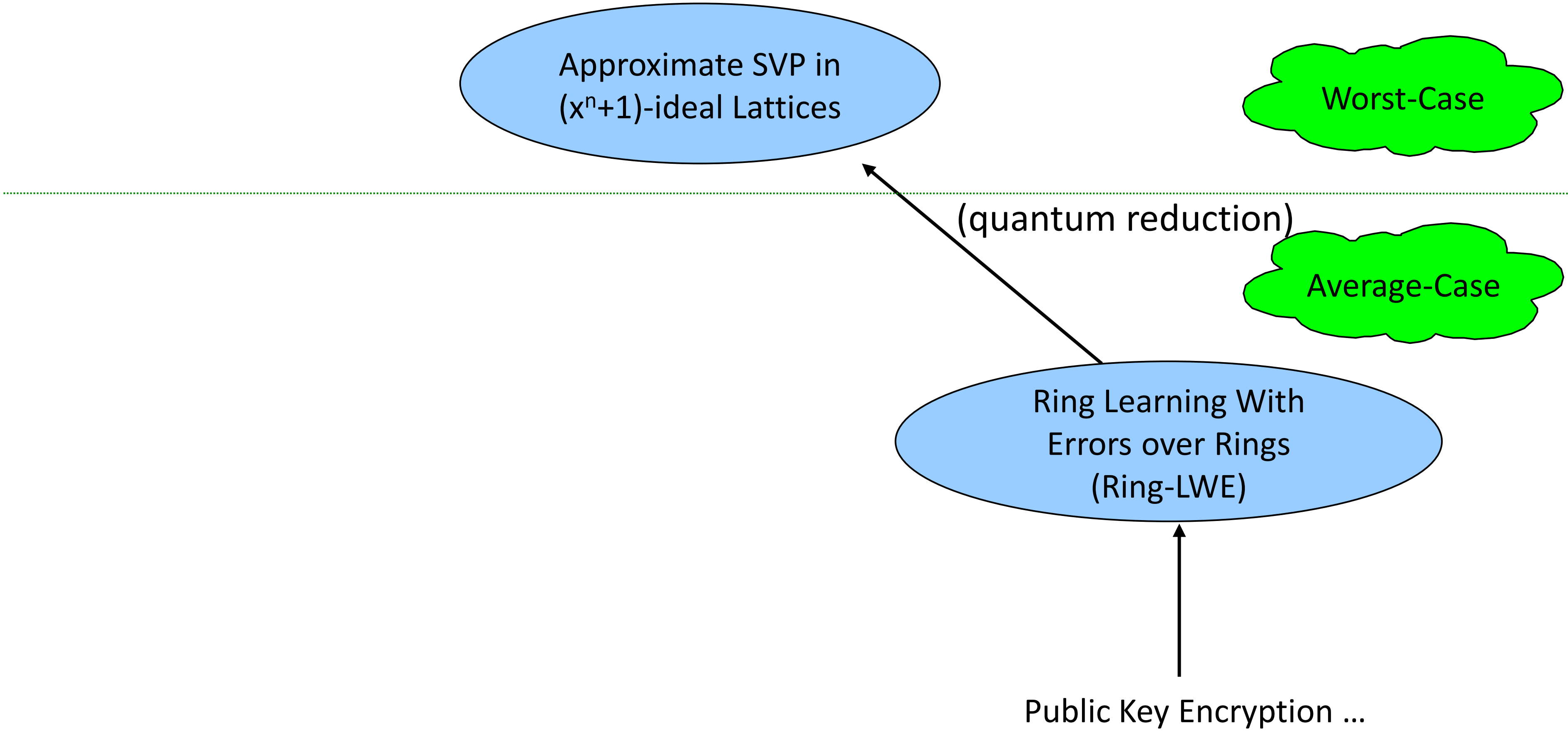
$(-1+2x+3x^2-4x^3)$ $(1-2x-3x^2+4x^3)$

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

RING-LWE

[LyuPeiReg '10]


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

Ring-LWE

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

Given:

a_1, a_1s+e_1

a_2, a_2s+e_2

…

a_k, a_ks+e_k

Find: s

a_i are random in R

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

…

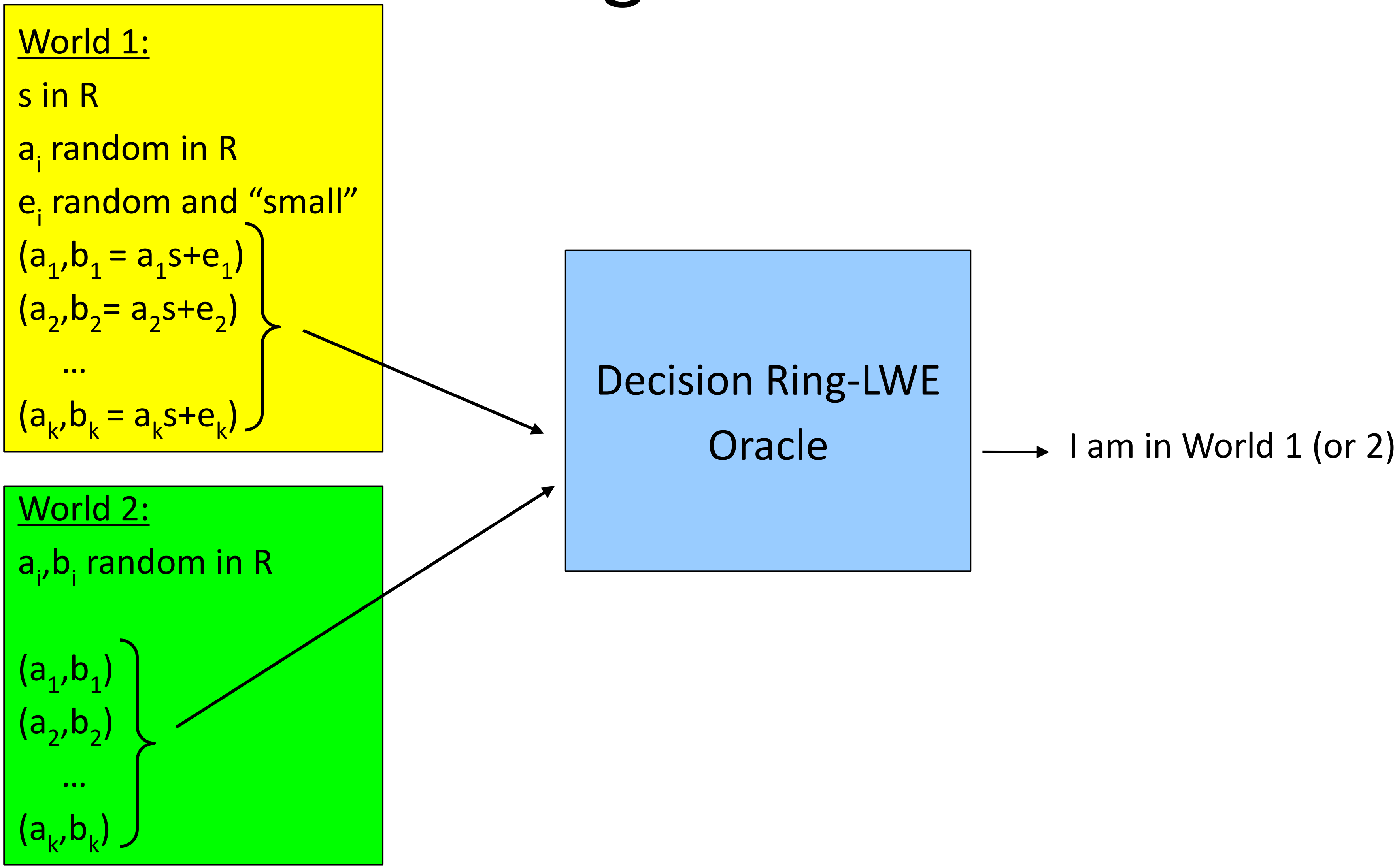
a_k, b_k

Question: Does there exist an s and "small"

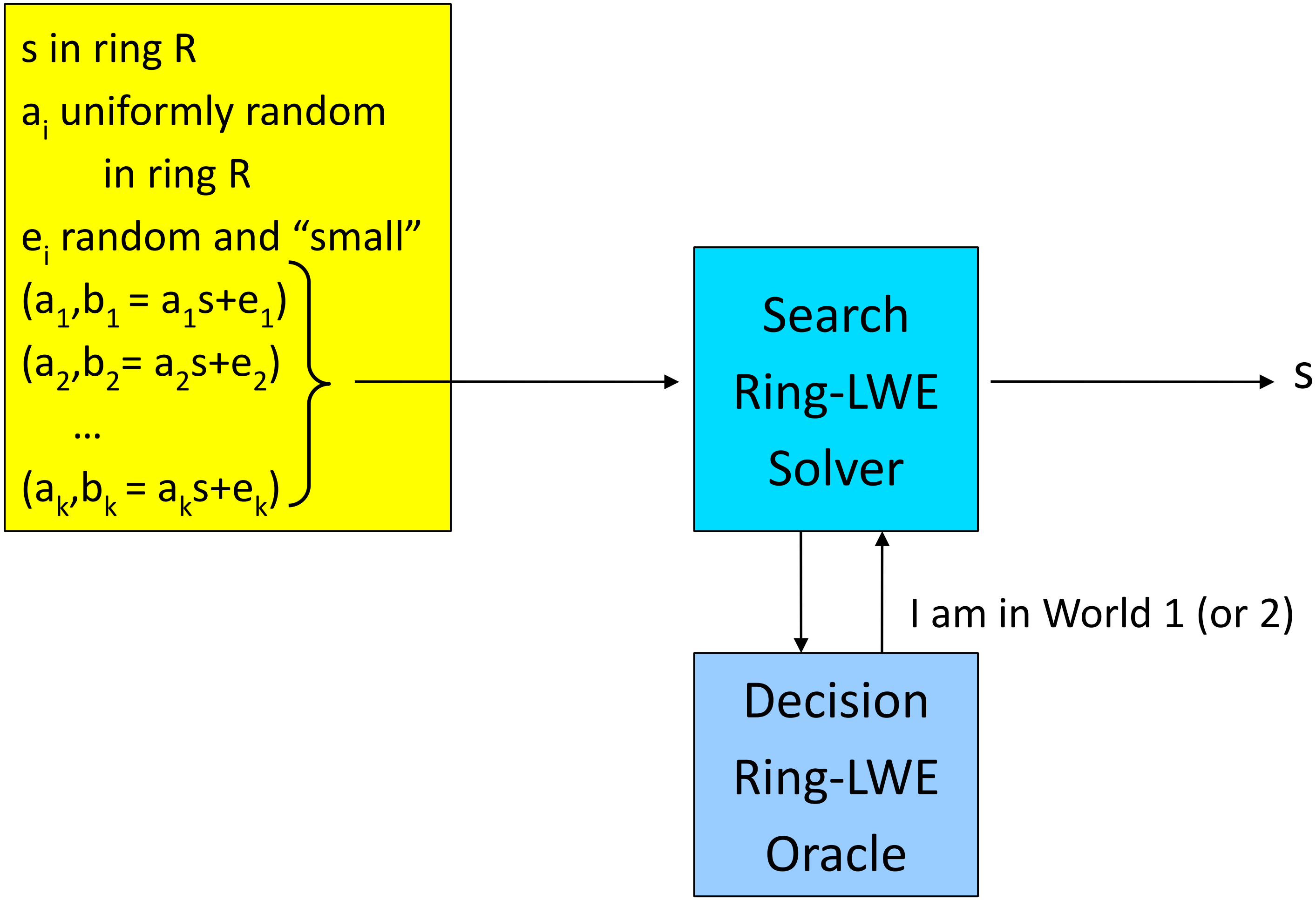
$e_1, \ldots, e_k$ such that $b_i=a_is+e_i$

or are all b_i uniformly random in R?

Decision Ring-LWE Problem



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)·z'(c) = (z·z')(c)

Example

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

8	5	-1	-8

·

5	5	3	7

+

7	-2	4	-5

=

-4	6	1	7

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

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

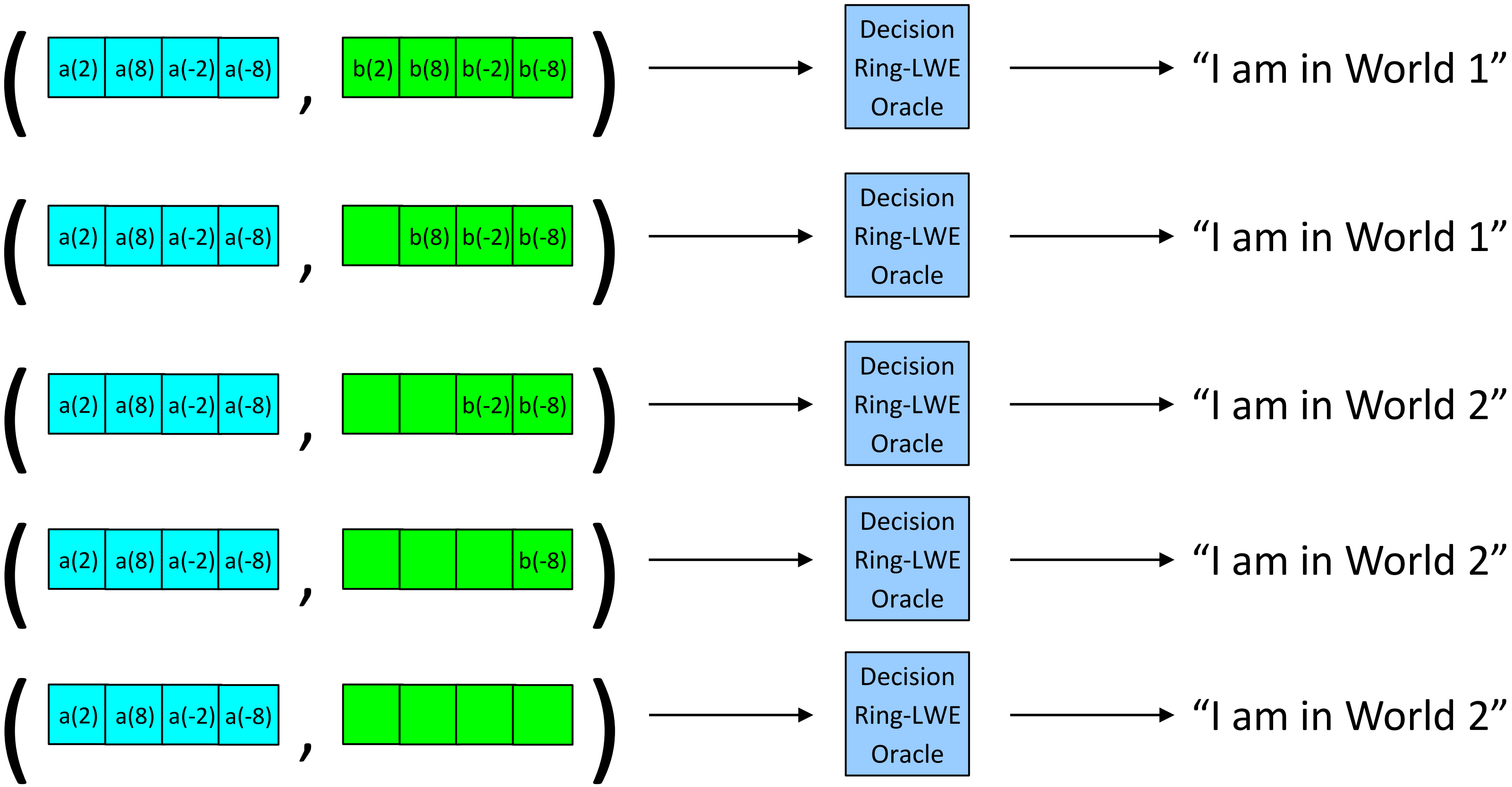
$= (x-2)(x-8)(x+2)(x+8)$

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

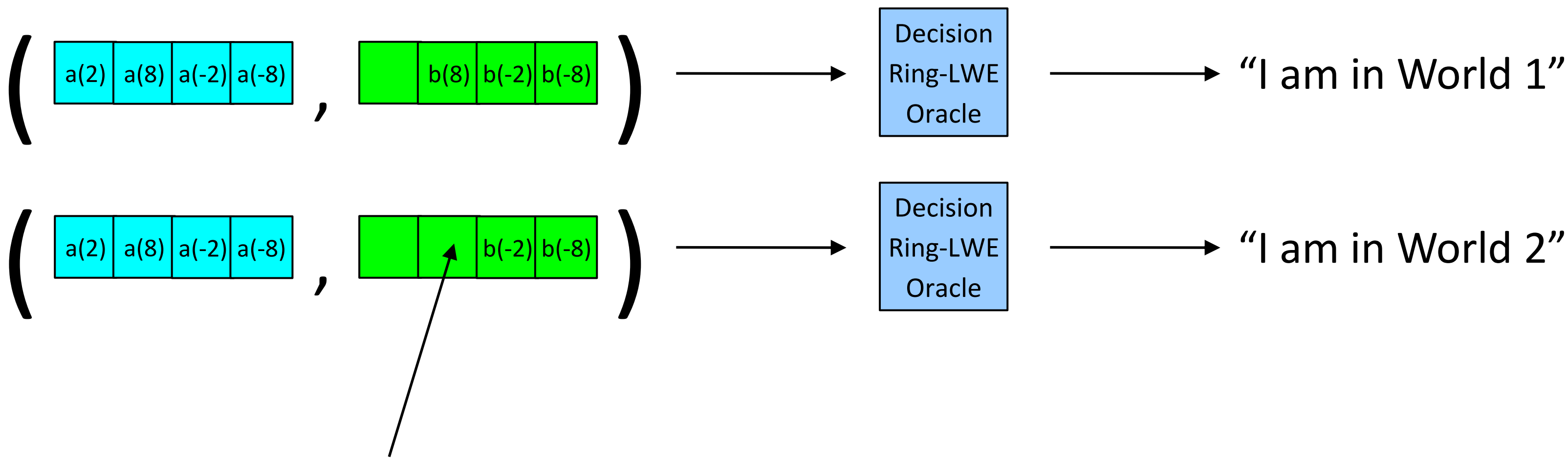
→ (a(x),b(x)) = (| a(2) | a(8) | a(-2) | a(-8) | , | b(2) | b(8) | b(-2) | b(-8) |)

Notation: | | | b(-2) | 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

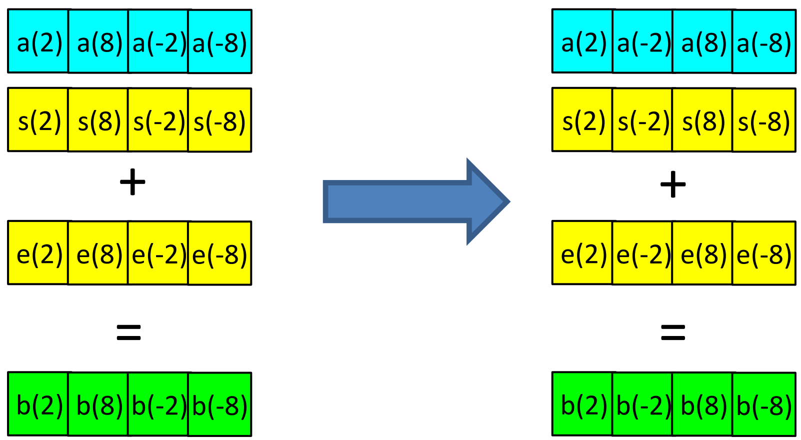
- We can use the decision oracle to learn s(8)
- How do we learn s(2),s(-2), and s(-8)?
- Idea: Permute the input to the oracle

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

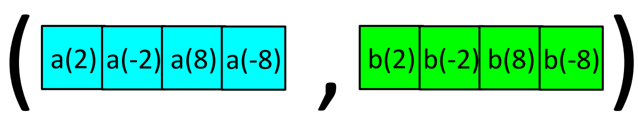
From s'(8) we can recover s(2)

(and s(-2) and s(-8))

A Possible Swap



Send to the decision oracle



Is this a valid distribution??

A Possible Swap

Polynomial	Coefficients		Coefficients	Polynomial
$5 - 3x + 4x^2 + 3x^3$	5 | 5 | 3 | 7	→	5 | 3 | 5 | 7	$5 + x + 8x^3$
$1 + x + 7x^2 - 5x^3$	8 | 5 | -1 | -8		8 | -1 | 5 | -8	$1 - x - 5x^2 - 7x^3$
	+		+	
$1 + x - x^2 + x^3$	7 | -2 | 4 | -5		7 | 4 | -2 | -5	$1 + 3x - 6x^2 + 3x^3$
	=		=	
$-6 + 2x - x^2 - 4x^3$	-4 | 6 | 1 | 7		-4 | 1 | 6 | 7	$-6 + 6x + 6x^2$

WRONG DISTRIBUTION !!

Send to the decision oracle

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

Is this a valid distribution??

Automorphisms of R

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

z(x) → z(x), z(x³), z(x⁵), z(x⁷)

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

← roots of x^4+1

Automorphisms of R

$z(x) = z_0 + z_1 x + z_2 x^2 + z_3 x^3$

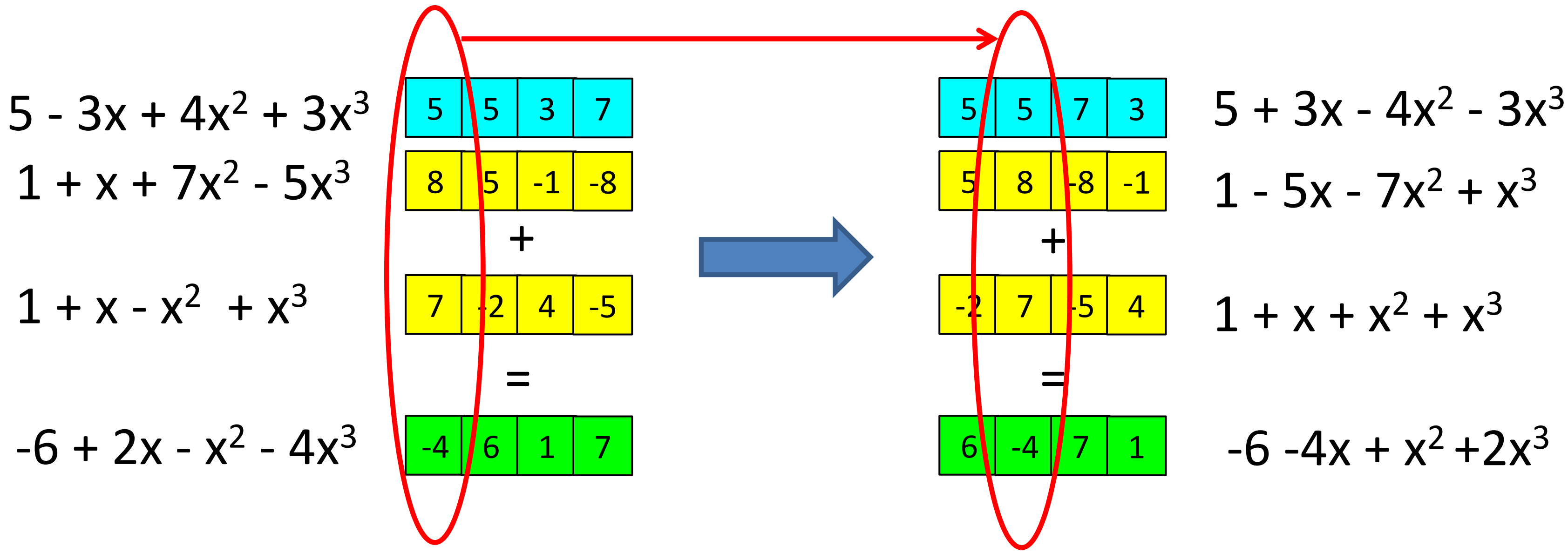
$z(x^3) = z_0 + z_1 x^3 + z_2 x^6 + z_3 x^9 = z_0 + z_3 x - z_2 x^2 + z_1 x^3$

$z(x^5) = z_0 + z_1 x^5 + z_2 x^{10} + z_3 x^{15} = z_0 - z_1 x + z_2 x^2 - z_3 x^3$

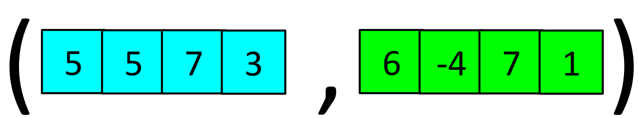
$z(x^7) = z_0 + z_1 x^7 + z_2 x^{14} + z_3 x^{21} = z_0 - z_3 x - z_2 x^2 - z_1 x^3$

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



This will recover s(2).

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

A Caveat …

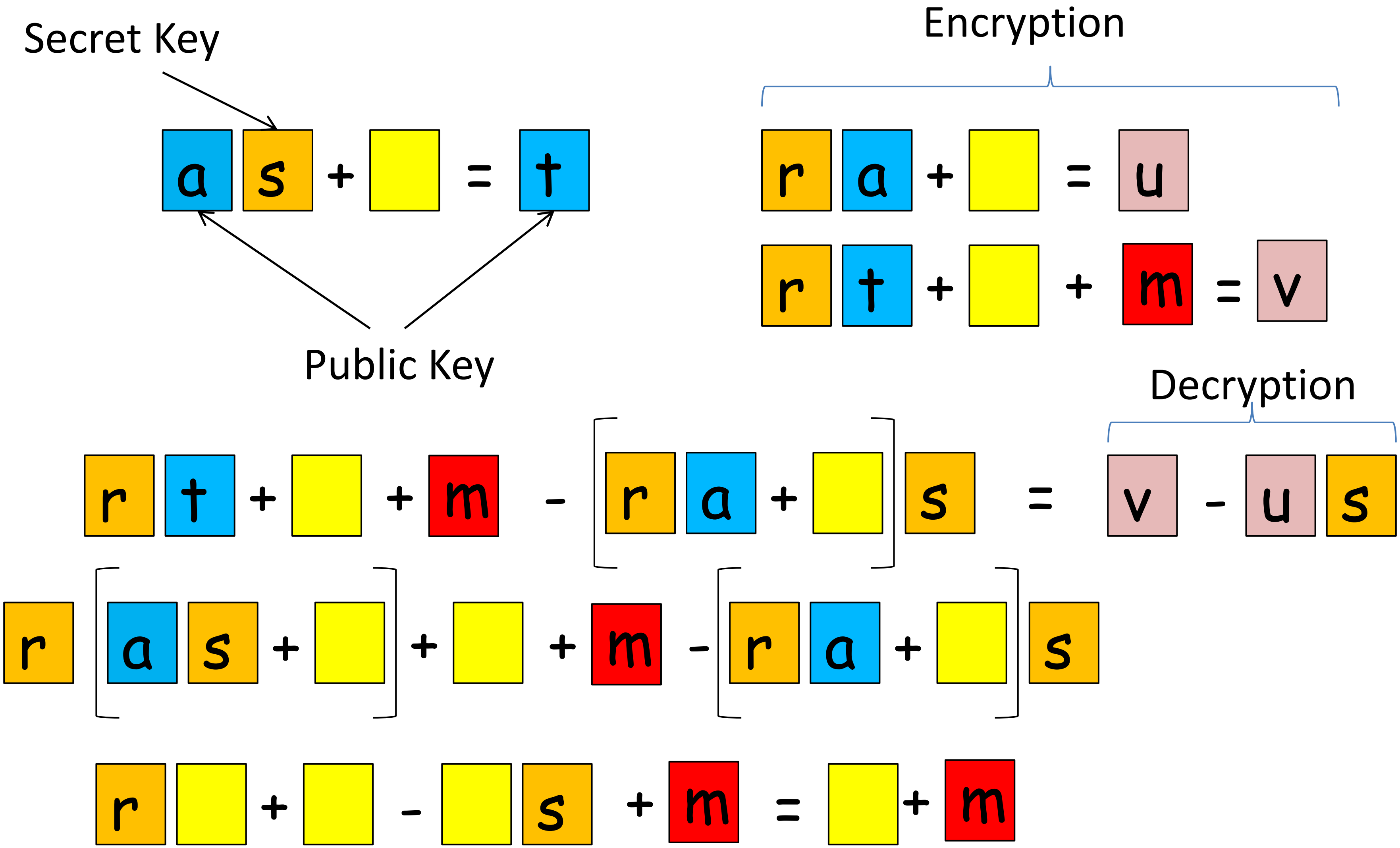
"If coefficients of $z(x)$ have distribution D symmetric around 0, then so do the coefficients of $z(x^3)$, $z(x^5)$, $z(x^7)$!! "

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

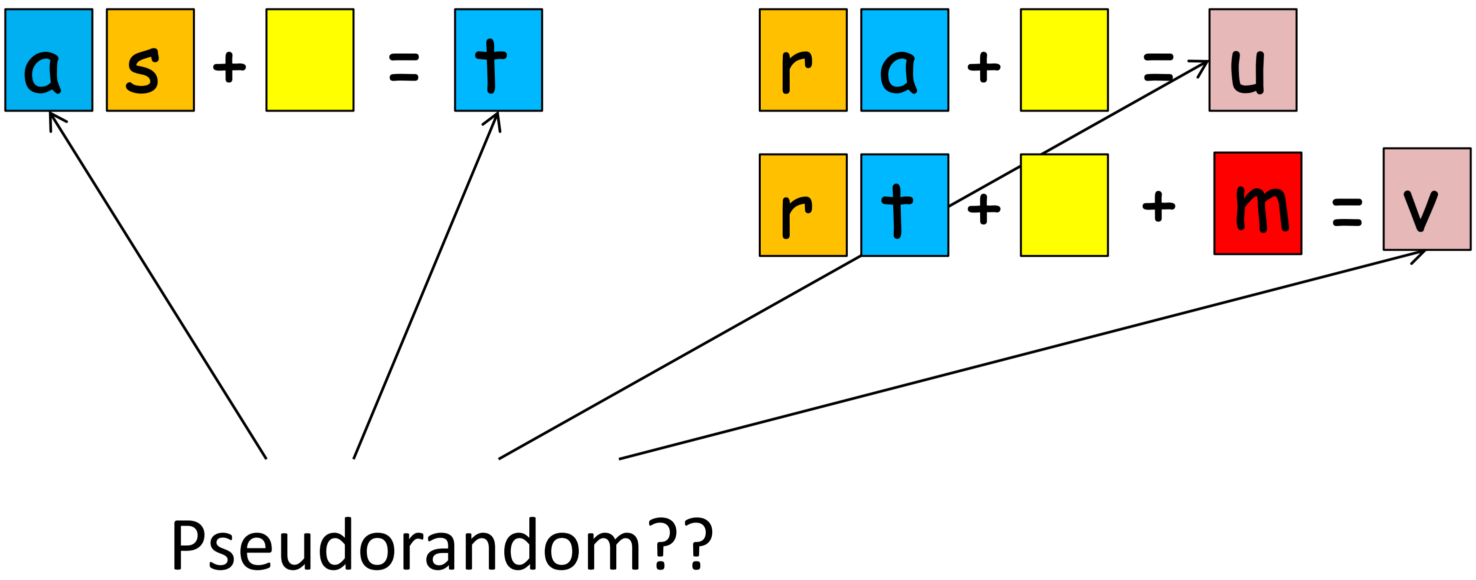
The correct error distribution is somewhat different for other polynomials.

Can work with all *cyclotomic* polynomials.

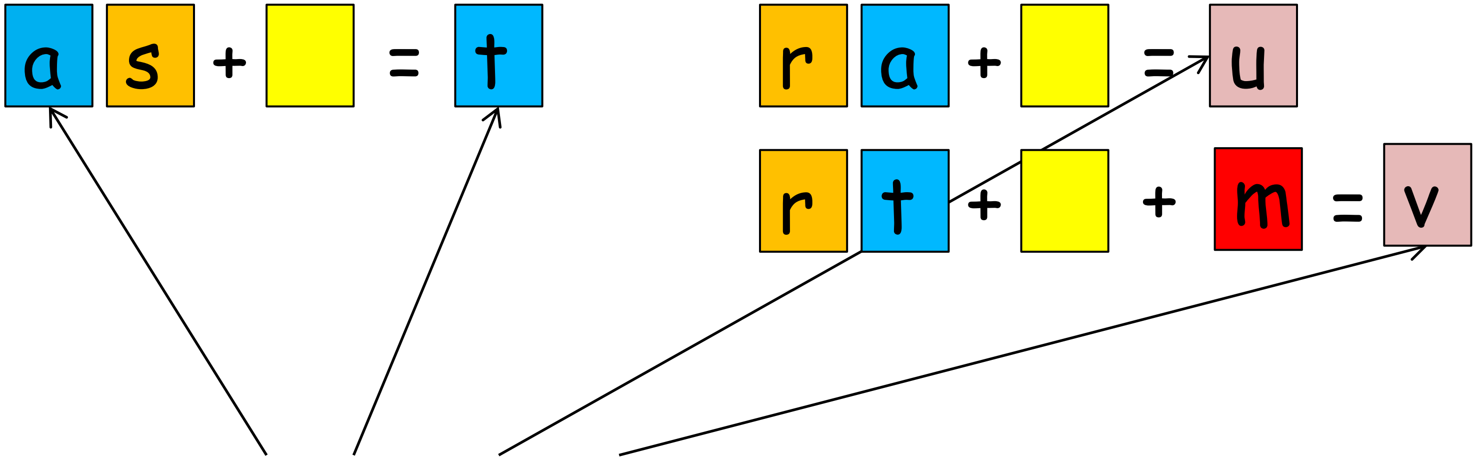
Ring-LWE cryptosystem



Security

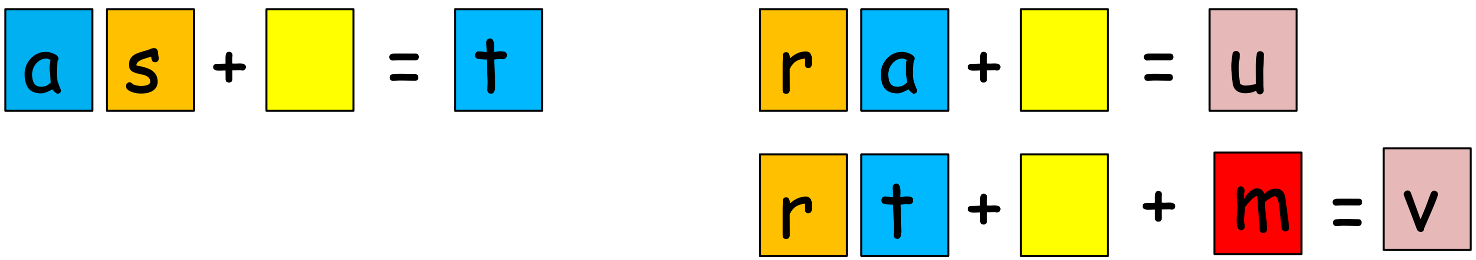


Security



Pseudorandom based on
Decision Ring-LWE!!

Use Polynomials in $Z_p[x]/(f(x))$

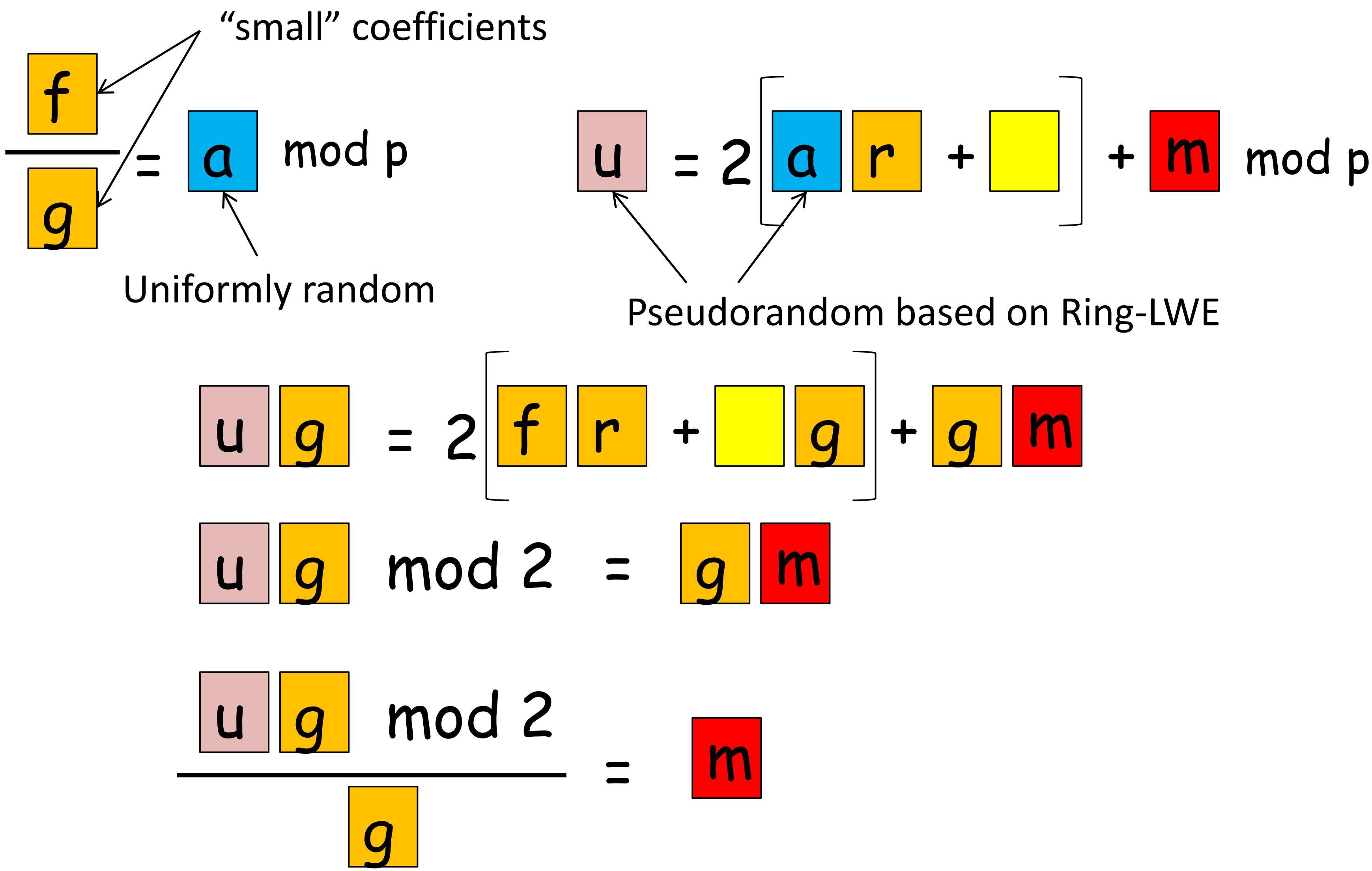


n-bit Encryption	From LWE	From Ring-LWE
Public Key Size	$\tilde{O}(n)$ / $\tilde{O}(n^2)$	$\tilde{O}(n)$
Secret Key Size	$\tilde{O}(n)$ / $\tilde{O}(n^2)$	$\tilde{O}(n)$
Ciphertext Expansion	$\tilde{O}(n)$ / $\tilde{O}(1)$	$\tilde{O}(1)$
Encryption Time	$\tilde{O}(n^3)$ / $\tilde{O}(n^2)$	$\tilde{O}(n)$
Decryption Time	$\tilde{O}(n^2)$	$\tilde{O}(n)$

1-ELEMENT CRYPTOSYSTEM BASED ON RING-LWE

[STEHLE, STEINFELD 2011]

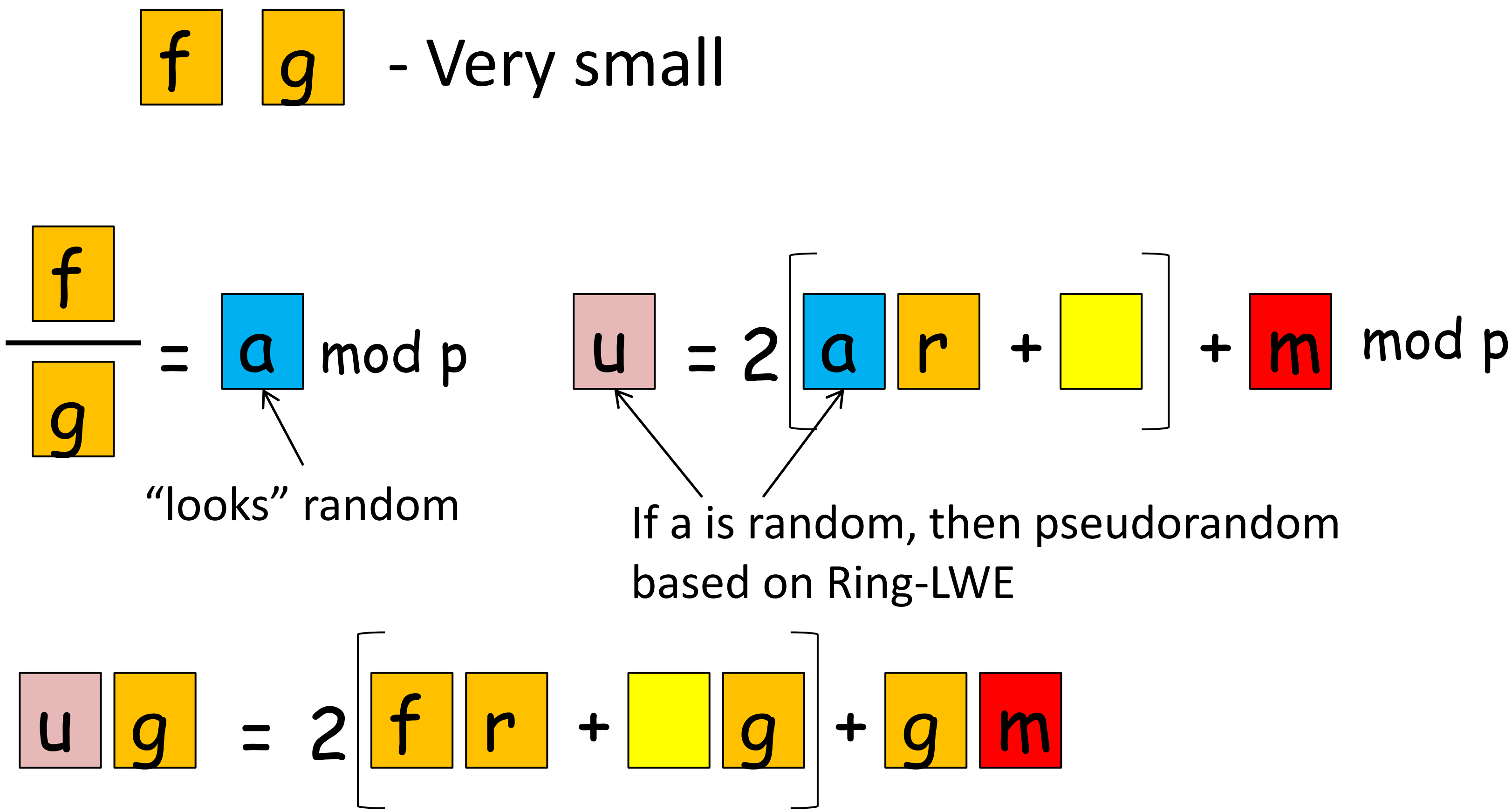
Stehle, Steinfeld Cryptosystem



NTRU CRYPTOSYSTEM

[HOFFSTEIN, PIPHER, SILVERMAN 1998]

NTRU Cryptosystem



Since f, g are smaller, p can be smaller as well

References

- Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman (1998): NTRU: A Ring-Based Public Key Cryptosystem
- 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.
- Damien Stehlé, Ron Steinfeld (2011): Making NTRU as Secure as Worst-Case Problems over Ideal Lattices