On Ideal Lattices and Learning With Errors Over Rings

Vadim Lyubashevsky
Chris Peikert
Oded Regev

Domains in Crypto Protocols

- "Discrete Log": Hard problems in ring $(Z_p,+,*)$ for large p
- "Factoring" : Hard problems in ring $(Z_N,+,*)$ for N=pq
- Other domains?

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

Elements are $z(x)=z_{n-1}x^{n-1}+ \dots +z_1x+z_0$ where z_i are integers mod q

Addition is the usual coordinate-wise addition

Multiplication is the usual polynomial multiplication followed by reduction modulo x^n+1

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

Elements are $z(x)=z_3x^3+z_2x^2+z_1x+z_0$ where z_i are integers mod 17

Addition is the usual coordinate-wise addition

Multiplication is the usual polynomial multiplication followed by reduction modulo x^4+1

A Hard Problem (Ring-LWE)

- Given g,t in R such that t=gs+e where s and e have "small" coefficients, find s (and e).
- Example:

$g = 4x^3 - 6x^2 + 7x + 2$

$t = -5x^3 + x^2 - 5x - 2$

- $t = g * (x^3 - x + 1) + x^2 + x - 1$

(Should remind you of the discrete log problem)

The Decisional Version

- Given g,t in R, determine whether

  (1) there exist s and e with "small" coefficients such that $t=gs+e$

  or

  (2) g, t are uniformly random in R

(Should remind you of the DDH problem)

Encryption Scheme

- sk: s
- pk: g, $t=gs+e_1$
- write msg m in $\{0,1\}^4$ as a polynomial in R
- To Encrypt:
  - pick random r in R with small coefficients
  - output $(v=rg+e_2,\ w=rt+e_3+8m)$
- To Decrypt
  - compute $w-vs$
  - if coefficient is "small", msg bit is 0, otherwise it's 1

(Should remind you of the El-Gamal cryptosystem)

Encryption Scheme

- sk: s
- pk: g, $t=gs+e_1$
- write msg m in $\{0,1\}^4$ as a polynomial in R
- To Encrypt:
  - pick random r in R with small coefficients
  - output $(v=rg+e_2,\ w=rt+e_3+8m)$
- To Decrypt
  - compute $w-vs = (rt+e_3+8m) - (rg+e_2)s$

$$= (rgs+re_1+e_3+8*m)-(rgs+e_2s) = re_1+e_3+e_2s+8m$$

Efficiency of Encryption Scheme

- sk: s
- pk: g, $t=gs+e_1$
- write msg m in $\{0,1\}^4$ as a polynomial in R
- To Encrypt:
  - pick random r in R with small coefficients
  - output $(v=rg+e_2, w=rt+e_3+8m)$ takes O(n log n) time
- To Decrypt
  - compute $w-vs$ takes O(n log n time)

Security of Encryption Scheme

- sk: s
- pk: g, $t=gs+e_1$ (looks uniformly random)
- write msg m in $\{0,1\}^4$ as a polynomial in R
- To Encrypt:
  - pick random r in R with small coefficients
  - output $(v=rg+e_2,\ w=rt+e_3+8m)$ (looks uniformly random)
- To Decrypt
  - compute $w-vs$

Decision vs. Search

- Discrete Log = DDH ?????
- Ring-LWE = Decisional Ring-LWE

  (will show in this talk)
- SVP in Ideal Lattices < Ring-LWE

  see [LPR '10]

Ring-LWE

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

  $g_1, g_1 s+e_1$

  $g_2, g_2 s+e_2$

  ...

  $g_k, g_k s+e_k$

- Find: s

e_i are "small" (distribution symmetric around 0)

s can be small or random in R (it's equivalent [ACPS '09])

Decision Ring-LWE

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

  g_1, t_1

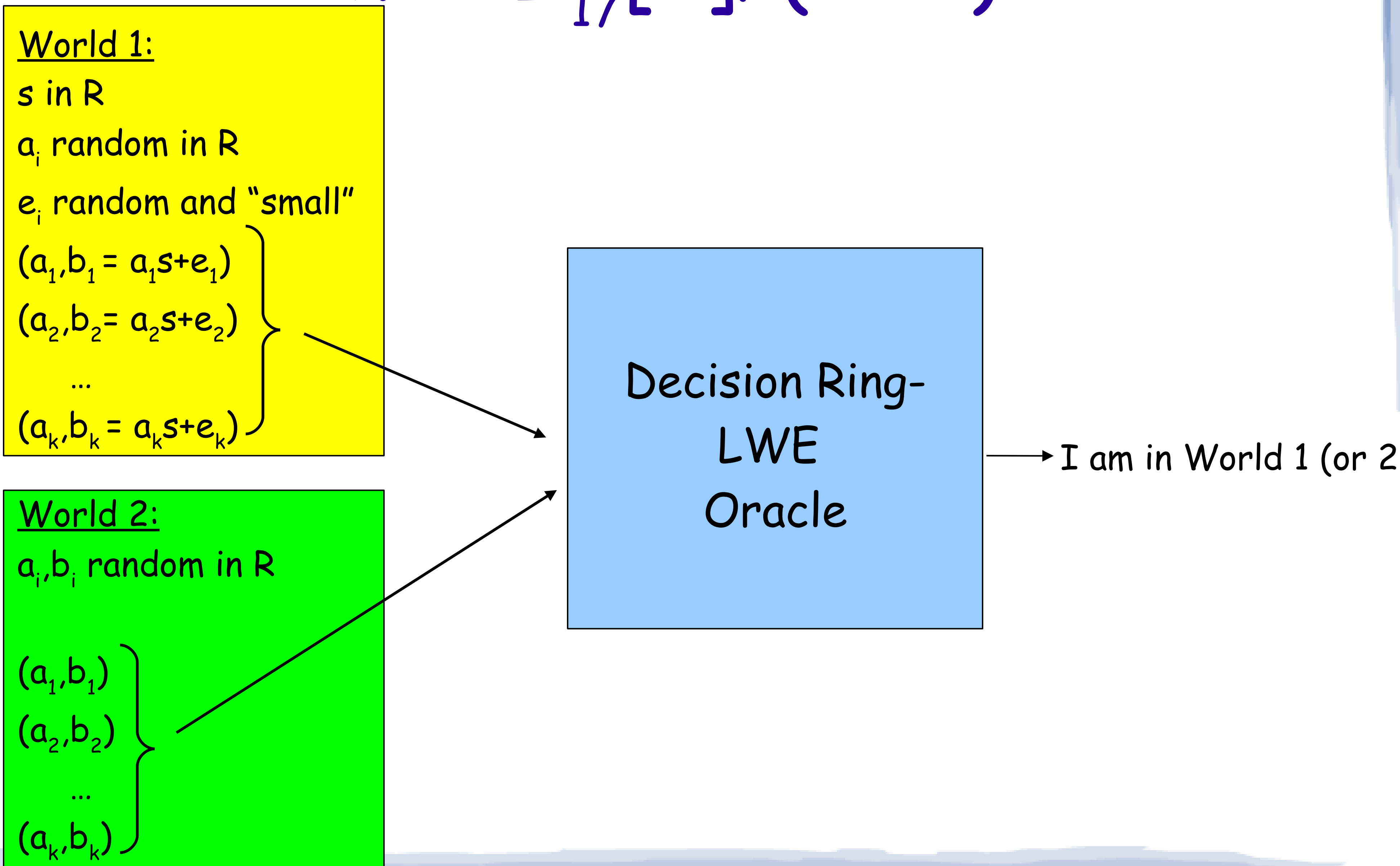
  g_2, t_2

  ...

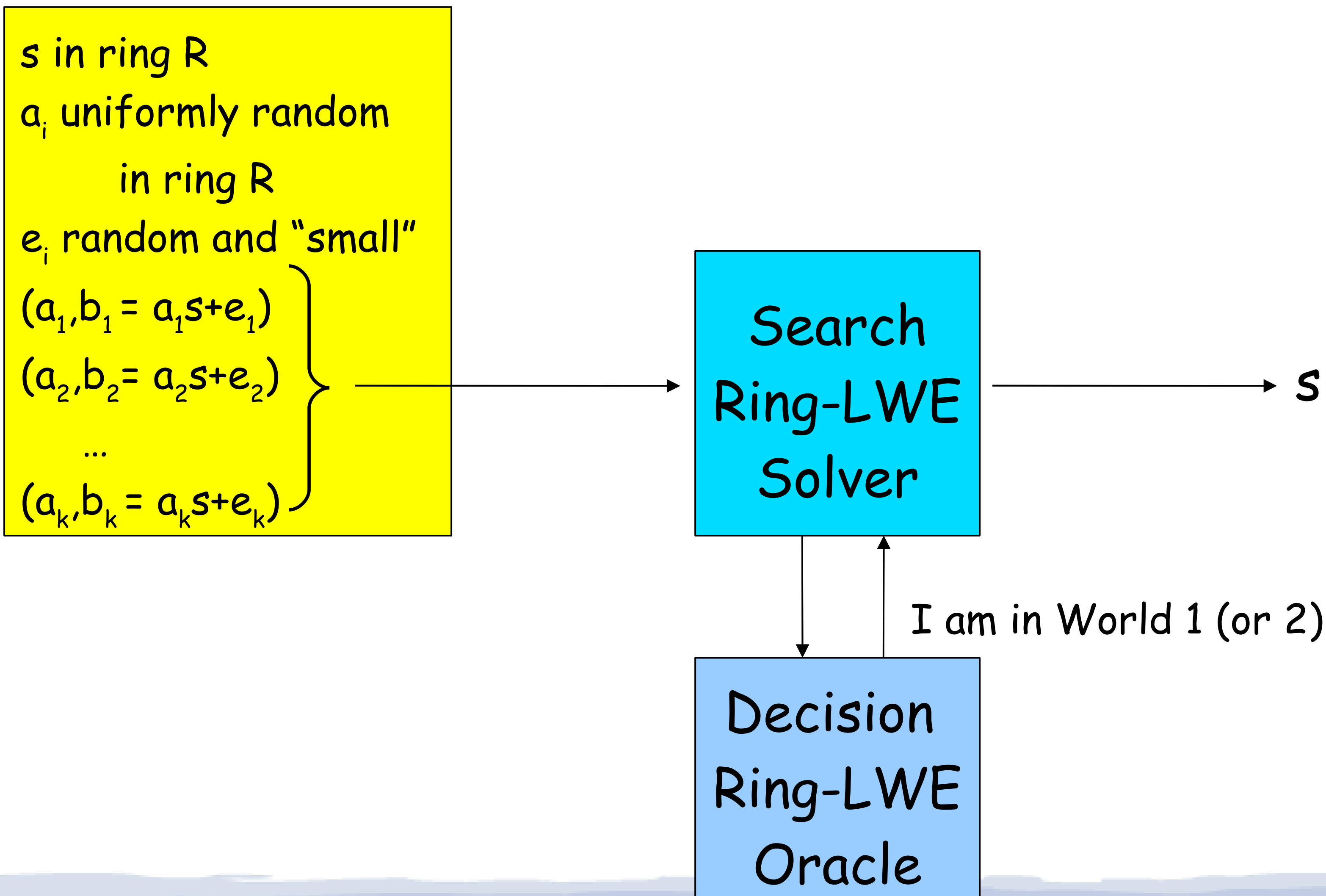
  g_k, t_k

- Question: Does there exist an s and "small" $e_1, \ldots, e_k$ such that $t_i=g_is+e_i$ or are all t_i uniformly random in R?

Decision Ring-LWE Problem in $R=Z_{17}[x]/(x^4+1)$



What We Want to Construct



Why Does the Search-to-Decision Reduction for LWE not Work?

Let g be our guess for the first coefficient of s

Repeat the following:

Receive LWE pair (a,b)

$$\underbrace{\begin{bmatrix} 2 & 13 & 7 & 3 \end{bmatrix}}_{a} * \begin{bmatrix} 8 \\ 3 \\ 12 \\ 5 \end{bmatrix} + \begin{bmatrix} 1 \end{bmatrix} = \underbrace{\begin{bmatrix} 13 \end{bmatrix}}_{b}$$

Pick random r in Z_{17}

Send sample below to the Decision Oracle

$$\begin{bmatrix} 2+r & 13 & 7 & 3 \end{bmatrix} \qquad \begin{bmatrix} 13+rg \end{bmatrix}$$

$$\underbrace{\begin{bmatrix} 2 & 13 & 7 & 3 \end{bmatrix}}_{a} * \begin{bmatrix} 8 \\ 3 \\ 12 \\ 5 \end{bmatrix} + \begin{bmatrix} -1 \\ -1 \\ 2 \\ 1 \end{bmatrix} = \underbrace{\begin{bmatrix} \ \\ \ \\ \ \\ \ \end{bmatrix}}_{b}$$

$$\begin{bmatrix} 2+r & 13 & 7 & 3 \end{bmatrix}$$

all coefficients of s act on this part of a.

we would need to guess all coefficients of s!

Reducing Search Ring-LWE to Decision Ring-LWE

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} such that $c^4+1=0$, and two polynomials z, z' in R
  - $z(c)+z'(c) = (z+z')(c)$
  - $z(c)*z'(c) = (z*z')(c)$

  (because z*z' in R is $z*z' + y*(x^4+1)$ in $Z_{17}[x]$, so

  $z*z'(c) = (z*z')(c) + y*(c^4+1) = (z*z')(c)$)

Operations in R

"Chinese remainder" representation of sum and product

- $z+z' \rightarrow (z(2)+z'(2), z(8)+z'(8), z(-2)+z'(-2), z(-8)+z'(-8)$
- $z*z' \rightarrow (z(2)*z'(2), z(8)*z'(8), z(-2)*z'(-2), z(-8)*z'(-8))$

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

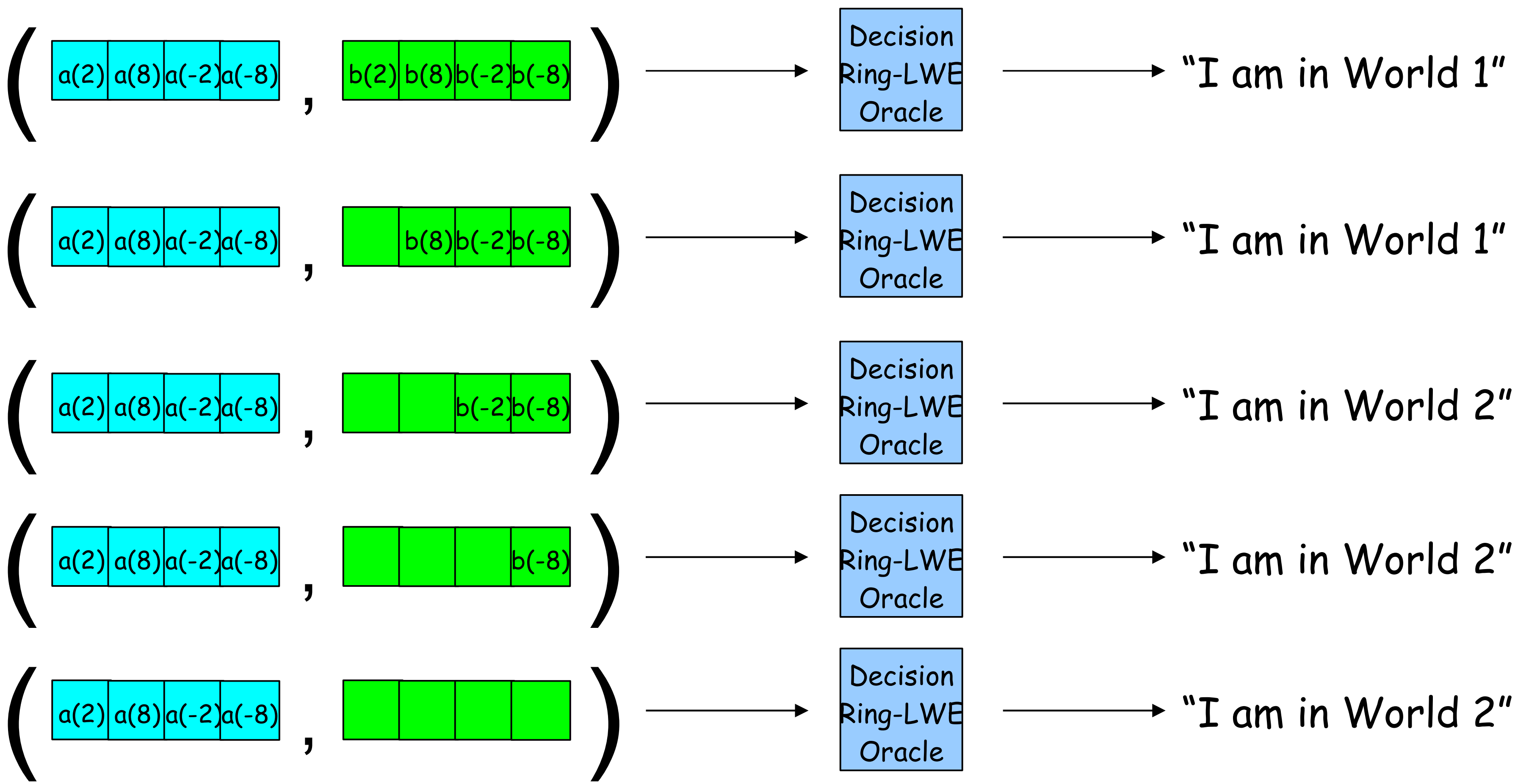
$$(x^4+1) = (x-2)(x-2^3)(x-2^5)(x-2^7) \bmod 17$$
$$= (x-2)(x-8)(x+2)(x+8)$$

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

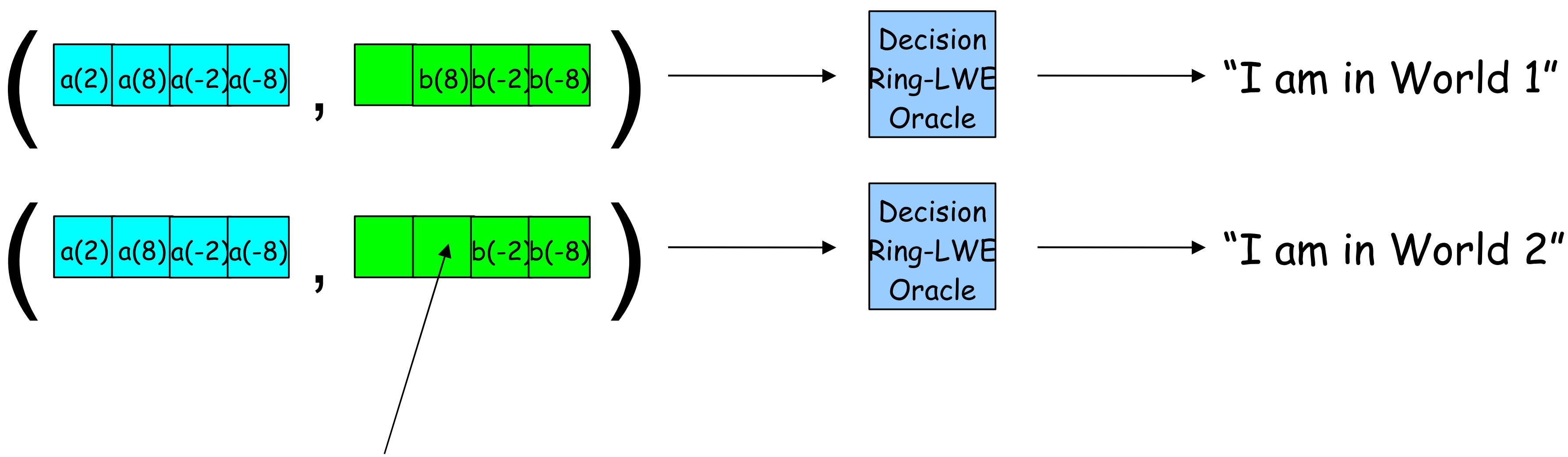
$$(a(x),b(x)) = \left(\boxed{a(2)}\boxed{a(8)}\boxed{a(-2)}\boxed{a(-8)} \, , \, \boxed{b(2)}\boxed{b(8)}\boxed{b(-2)}\boxed{b(-8)} \right)$$

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

$$\Rightarrow \Big(\boxed{a(2)}\boxed{a(8)}\boxed{a(-2)}\boxed{a(-8)} \,,\, \boxed{b(2)}\boxed{b(8)}\boxed{b(-2)}\boxed{b(-8)} \Big)$$

Make the first position uniformly random in Z_{17}

$$\Big(\boxed{a(2)}\boxed{a(8)}\boxed{a(-2)}\boxed{a(-8)} \,,\, \boxed{}\boxed{b(8)}\boxed{b(-2)}\boxed{b(-8)} \Big)$$

Pick random r in Z_{17}

$$\Big(\boxed{a(2)}\boxed{a(8)+r}\boxed{a(-2)}\boxed{a(-8)} \,,\, \boxed{}\boxed{b(8)+gr}\boxed{b(-2)}\boxed{b(-8)} \Big) \Rightarrow$$

Send to the decision oracle

If g=s(8), then (a(8)+r)*s(8)+e(8)=b(8)+gr (Oracle will say "World 1")

If g≠s(8), then b(8)+gr is uniformly random in Z_{17} (Oracle will say "World 2")

Learning the Other Positions

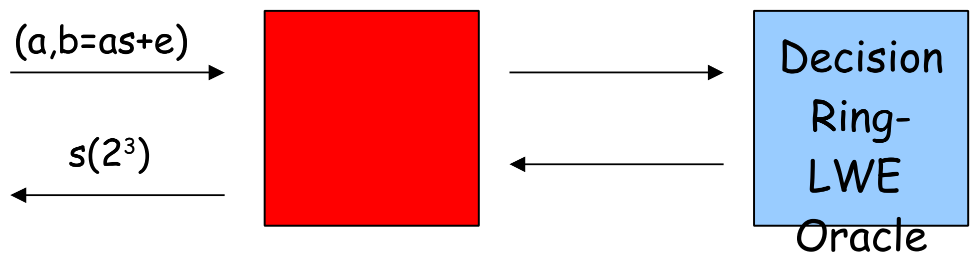
- We can use the decision oracle to learn $s(8)$
- How do we learn $s(2)$, $s(-2)$, and $s(-8)$?
- Idea: Permute the input to the oracle

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

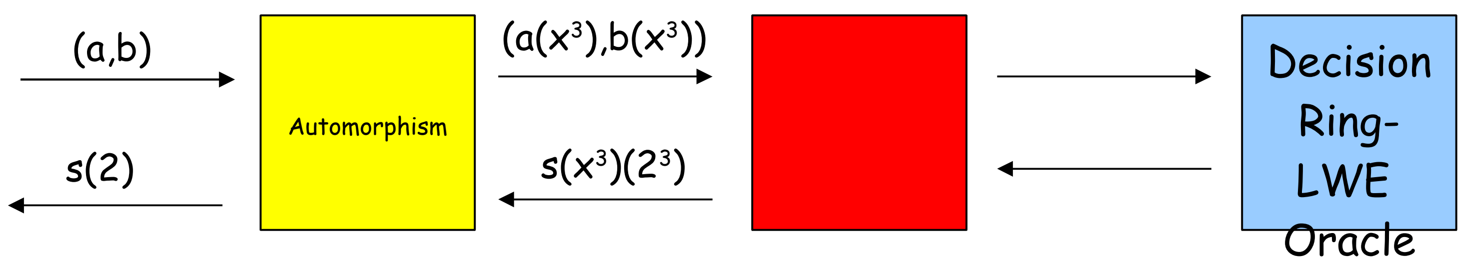
  From $s'(8)$ we can recover $s(2)$ (and $s(-2)$ and $s(-8)$)

Learning the Other Positions

We get samples (a(x), a(x)s(x)+e(x))
We give samples (a(x), a(x)s(x)+e(x)) to the oracle and get $s(2^3)$



We get samples (a(x), a(x)s(x)+e(x))
What if we give samples $(a(x^3), a(x^3)s(x^3)+e(x^3))$ to the oracle?



Assuming that $(a(x^3), a(x^3)s(x^3)+e(x^3))$ has the right distribution, the oracle will work and return $s(x^3)(2^3) = s(2^9)=s(2)$.

Automorphisms of R

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

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

evaluated at

polynomial

Learning all of s

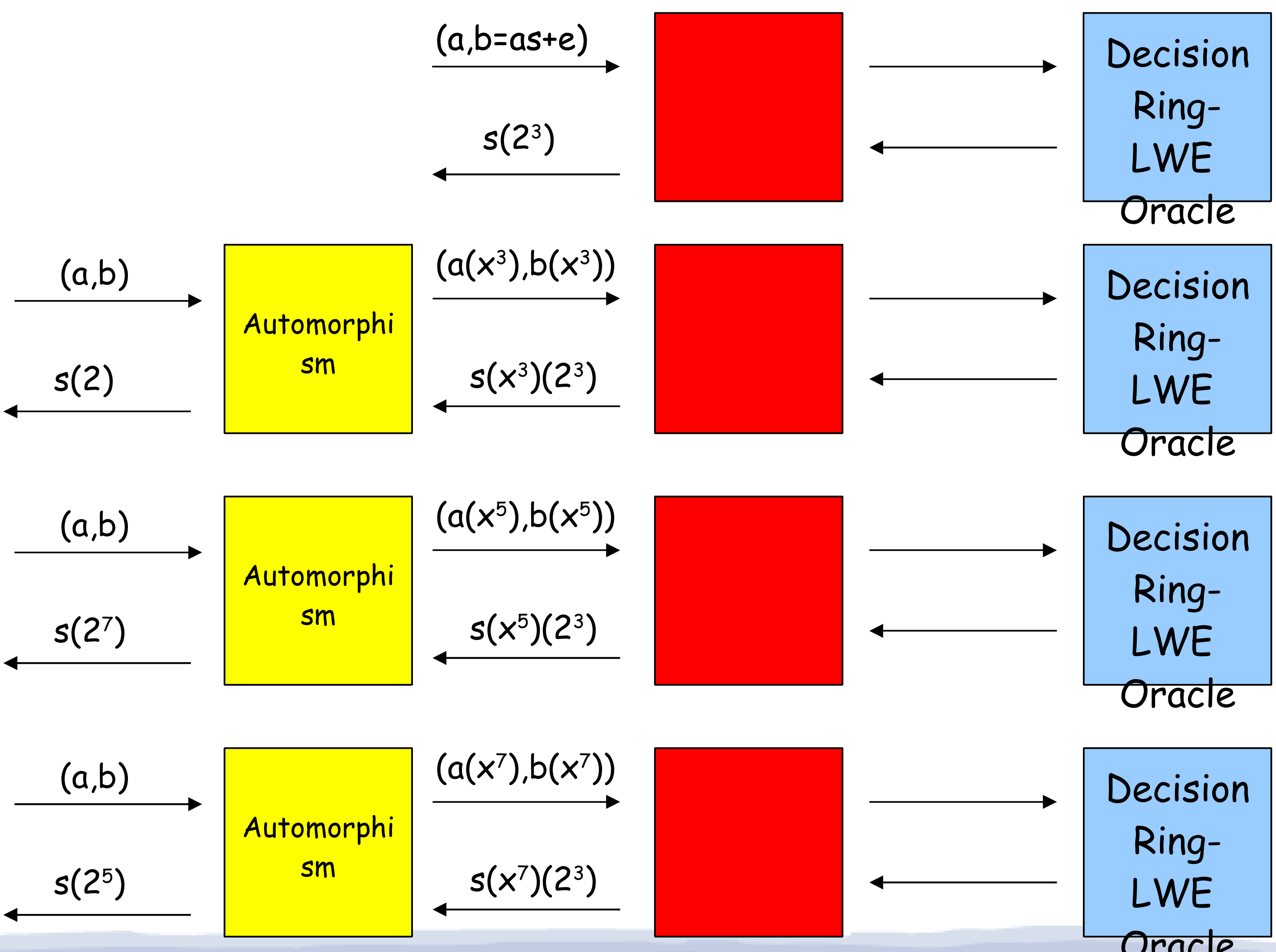
For all z in R:

$z(2)=z(x^3)(2^3)$

$z(2^3)=z(x)(2^3)$

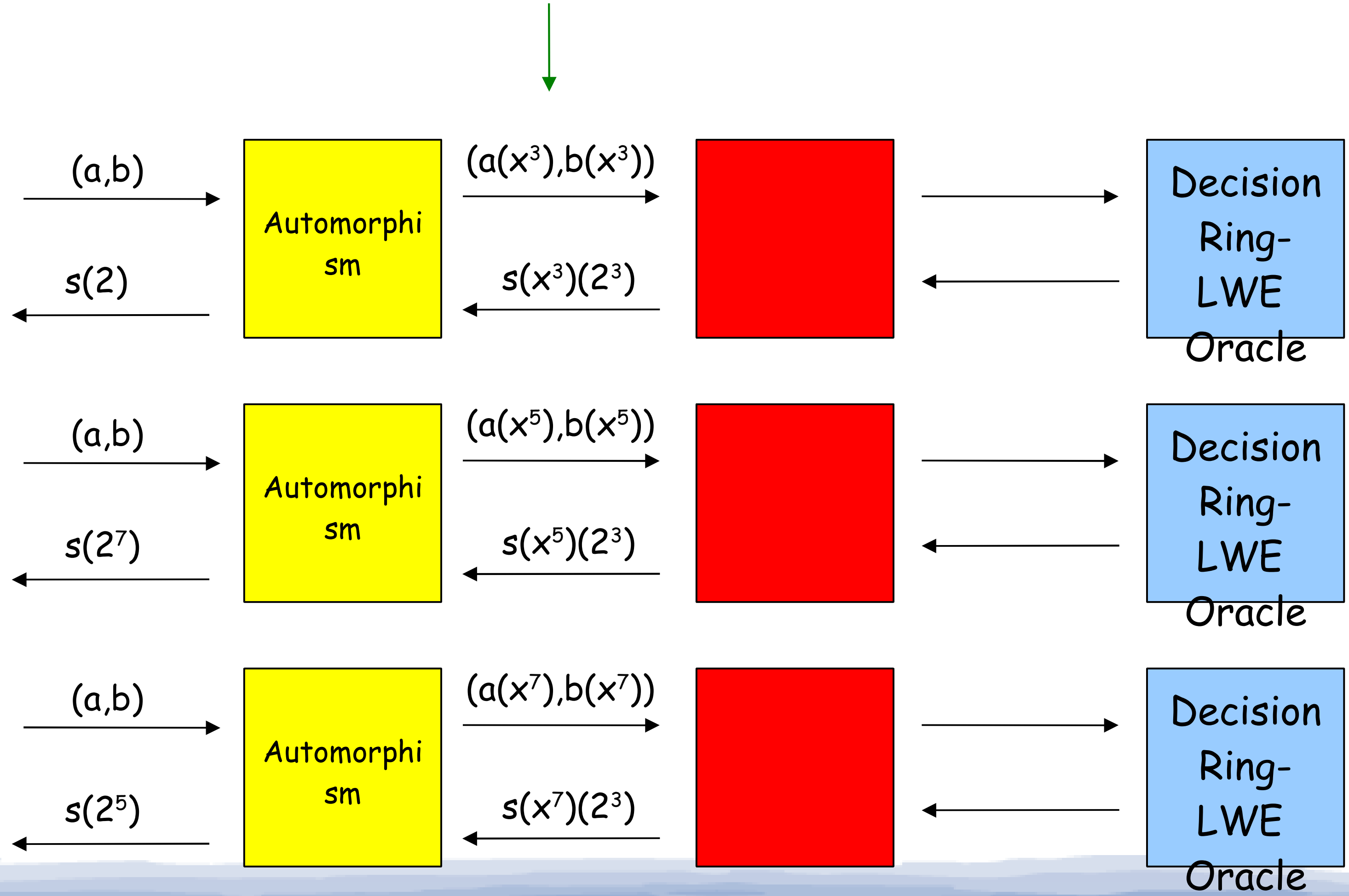
$z(2^5)=z(x^7)(2^3)$

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

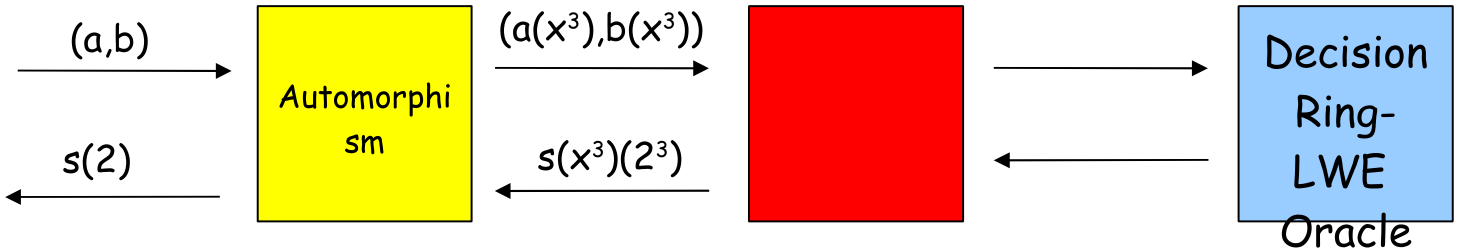


An Important Technicality

Are these distributions valid?



An Important Technicality



If $a(x)$ is uniform, $a(x^3)$ is uniform

$b(x^3)=a(x^3)s(x^3)+e(x^3)$

$e(x^3)$ and $e(x^5)$ and $e(x^7)$ should come from the same distribution as $e(x)$

Error Distribution Under Automorphisms

$e(x) = e_0 + e_1x + e_2x^2 + e_3x^3$

$e(x^3) = e_0 + e_1x^3 + e_2x^6 + e_3x^9 = e_0 + e_3x - e_2x^2 + e_1x^3$

$e(x^5) = e_0 + e_1x^5 + e_2x^{10} + e_3x^{15} = e_0 - e_1x + e_2x^2 - e_3x^3$

$e(x^7) = e_0 + e_1x^7 + e_2x^{14} + e_3x^{21} = e_0 - e_3x - e_2x^2 - e_1x^3$

If coefficients of $e(x)$ have distribution D with mean 0, then so do coefficients of $e(x^3)$, $e(x^5)$, $e(x^7)$!!

Using algebraic number theory, we can generalize to polynomials other than $x^n + 1$ (cyclotomic polynomials)

Summary

- Search Ring-LWE is as hard as solving certain lattice problems in the worst case (with quantum) (also see [SSTX '10])
- Decision Ring-LWE in cyclotomic rings is as hard as Search Ring-LWE
- Allows for much more efficient cryptographic constructions than regular LWE

Thank You!