Learning With Errors Over Rings

Vadim Lyubashevsky

Chris Peikert

Oded Regev

Appeared in Eurocrypt 2010; see also talk and survey prepared for CCC'2010

Overview of the

Learning With Errors Problem

Learning With Errors (LWE) Problem

- A secret vector $\mathbf{s}$ in $\mathbb{Z}_{17}^4$
- We are given an arbitrary number of equations, each correct up to ± 1
- Can you find $\mathbf{s}$?

$$
\begin{aligned}
14s_1 + 15s_2 + 5s_3 + 2s_4 &\approx 8 \pmod{17} \\
13s_1 + 14s_2 + 14s_3 + 6s_4 &\approx 16 \pmod{17} \\
6s_1 + 10s_2 + 13s_3 + 1s_4 &\approx 3 \pmod{17} \\
10s_1 + 4s_2 + 12s_3 + 16s_4 &\approx 12 \pmod{17} \\
9s_1 + 5s_2 + 9s_3 + 6s_4 &\approx 9 \pmod{17} \\
3s_1 + 6s_2 + 4s_3 + 5s_4 &\approx 16 \pmod{17} \\
6s_1 + 7s_2 + 16s_3 + 2s_4 &\approx 3 \pmod{17}
\end{aligned}
$$

LWE's Claim to Fame

- ✓ Known to be as hard as worst-case lattice problems, which are believed to be exponentially hard (even against quantum computers)
- ✓ Extremely versatile
- ✓ Basis for provably secure and efficient cryptographic constructions

Applications of LWE

- Public Key Encryption [R05, KawachiTanakaXagawa07, PeikertVaikuntanathanWaters08]
- CCA-Secure PKE [PeikertWaters08, Peikert09]
- Identity-Based Encryption [GentryPeikertVaikuntanathan08]
- Oblivious Transfer [PeikertVaikuntanathanWaters08]
- Circular-Secure Encryption [ApplebaumCashPeikertSahai09]
- Leakage Resilient Encryption [AkaviaGoldwasserVaikunathan09, DodisGoldwasserKalaiPeikertVaikuntanathan10, GoldwasserKalaiPeikertVaikuntanathan10]
- Hierarchical Identity-Based Encryption [CashHofheinzKiltzPeikert09, AgrawalBonehBoyen09]
- Learning Theory [KlivansSherstov06]
- And more…

LWE Problem: More Precisely

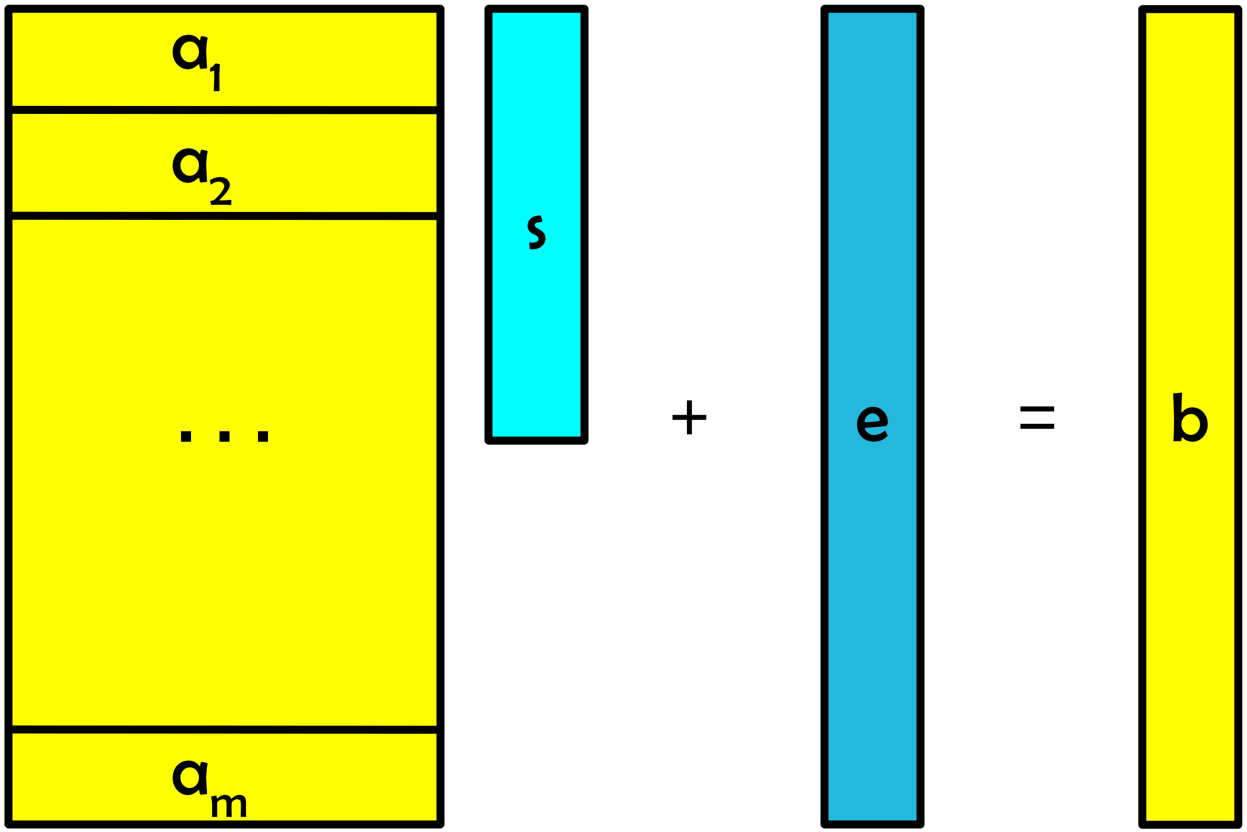
- There is a secret vector s in $\mathbb{Z}_q^n$ (we'll use $\mathbb{Z}_{17}^4$ as a running example)
- An oracle (who knows s) generates a random vector a in $\mathbb{Z}_q^n$ and "small" noise element e in $\mathbb{Z}$
- The oracle outputs (a, $b = a \cdot s + e \bmod 17$)
- This procedure is repeated with the same s and fresh a and e
- Our task is to find s

$$\begin{bmatrix}2 & 13 & 7 & 3\\ 4 & 7 & 9 & 1\\ 6 & 14 & 5 & 11\end{bmatrix} \cdot \begin{bmatrix}8\\ 3\\ 12\\ 5\end{bmatrix} + \begin{bmatrix}1\\ -1\\ 2\end{bmatrix} = \begin{bmatrix}13\\ 12\\ 3\end{bmatrix}$$

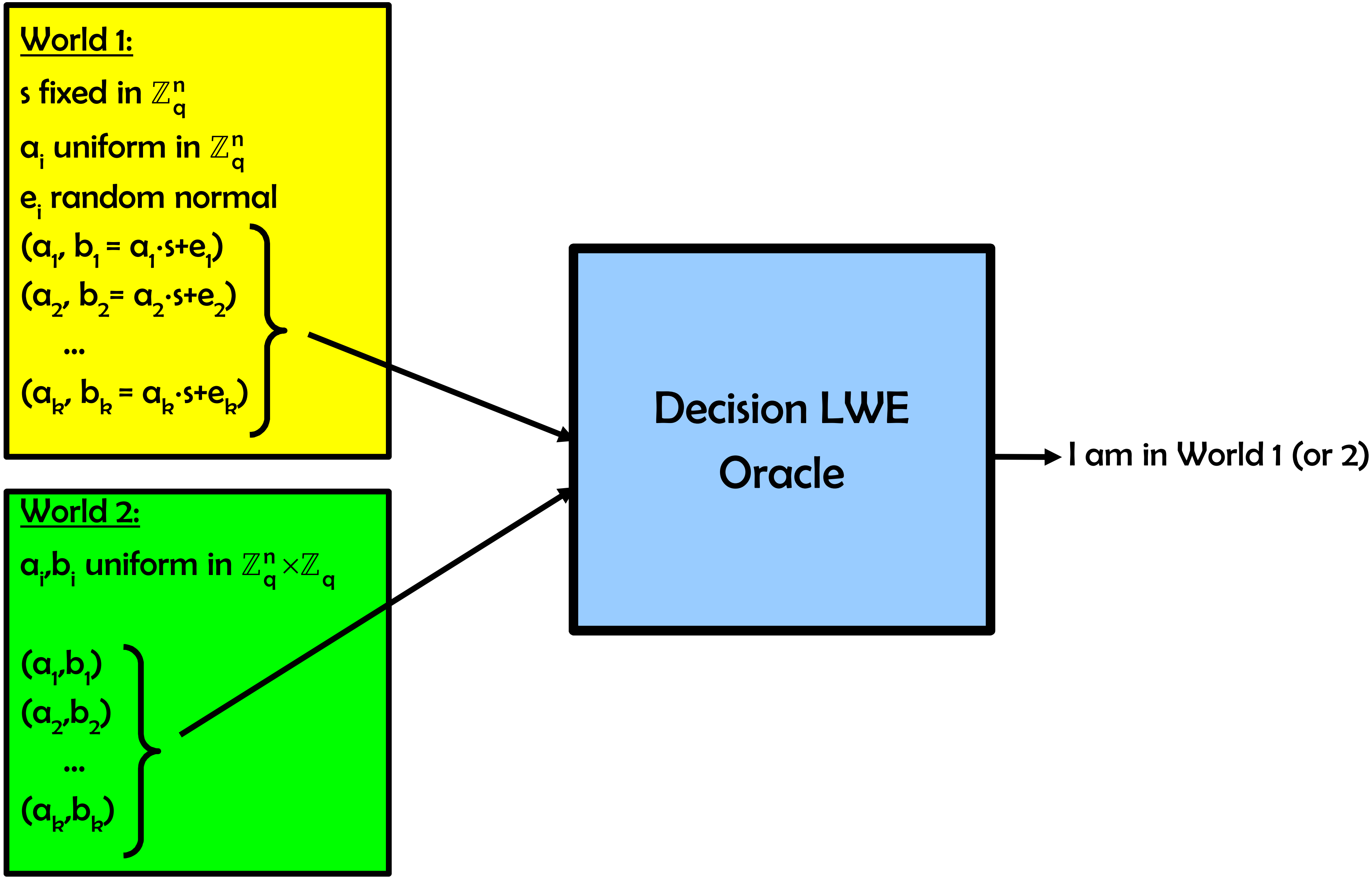
- Once there are enough a_i, the s is uniquely determined

Hardness of LWE

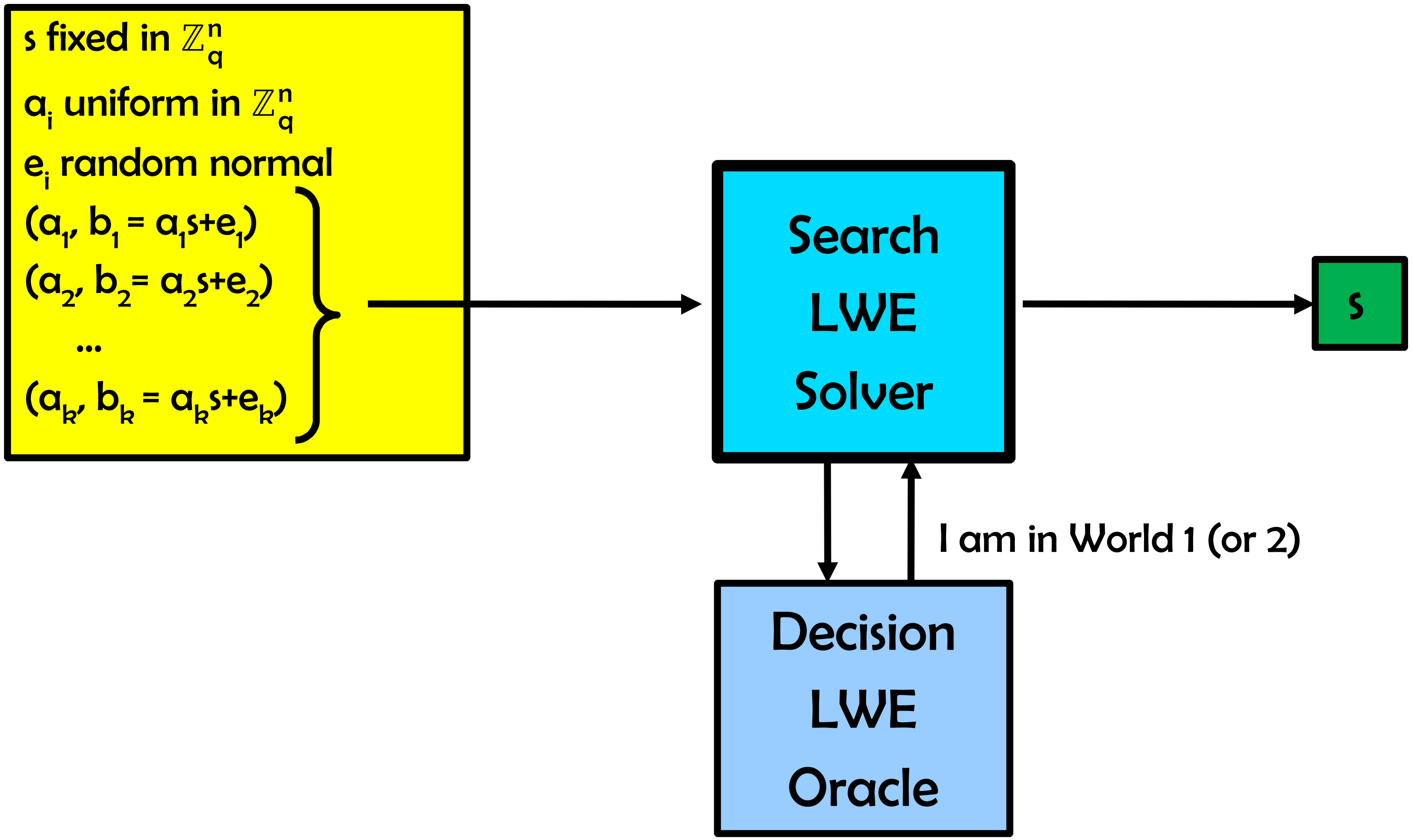
- Thm [R'05] : There is a polynomial-time quantum reduction from solving lattice problems in the worst case to solving LWE



Decision LWE Problem



What We Want to Construct



Search LWE < Decision LWE

- Idea: Use the Decision oracle to figure out the coordinates of s one at a time

- Let $g \in \mathbb{Z}_q$ be our guess for the first coordinate of s
- Repeat the following:
  - Receive LWE pair (a,b)

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

  - Pick random r in $\mathbb{Z}_q$
  - Send $(a+(r,0,\ldots,0), b+rg)$ to the decision oracle:

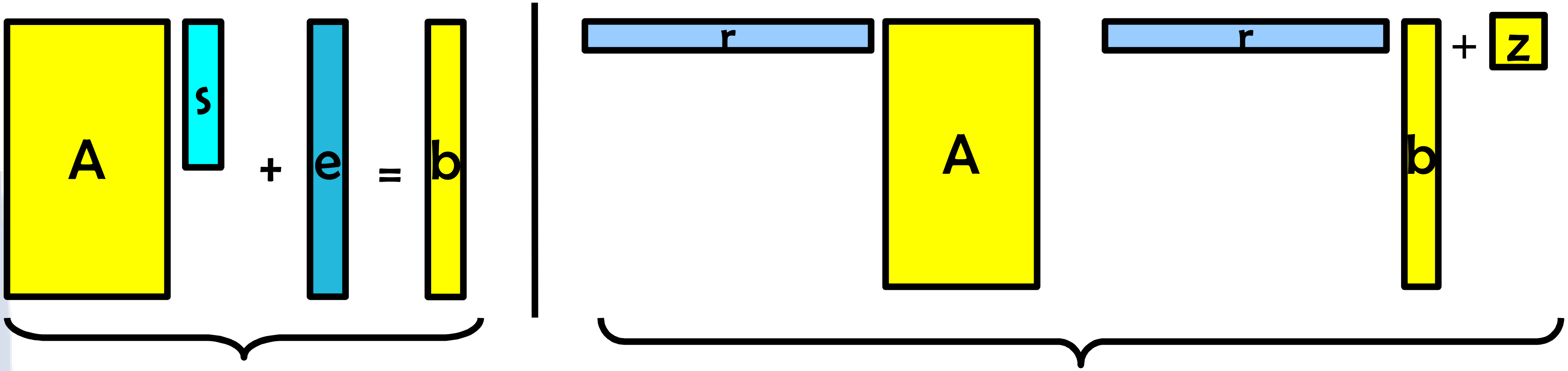
$$\boxed{2+r}\boxed{13}\boxed{7}\boxed{3} \qquad \boxed{13+rg}$$

1. If g is right, then we are sending a distribution from World 1
2. If g is wrong, then we are sending a distribution from World 2 (here we use that q is prime)

- We will find the right g after at most q attempts

- Use the same idea to recover all coefficients of s one at a time

Some Inefficiencies of LWE-Based Schemes



public key is $O(n^2)$

encryption of 1 bit requires $O(n^2)$ (or $O(n)$) operations

Source of Inefficiency

$$\begin{bmatrix} 2 & 13 & 7 & 3 \end{bmatrix} \cdot \begin{bmatrix} 8 \\ 3 \\ 12 \\ 5 \end{bmatrix} + \begin{bmatrix} 1 \end{bmatrix} = \begin{bmatrix} 13 \end{bmatrix}$$

- Getting just one extra random-looking number requires n random numbers!

- Wishful thinking: get n random numbers and produce O(n) pseudo-random numbers in "one shot"

$$\begin{bmatrix} 2 \\ 13 \\ 7 \\ 3 \end{bmatrix} * \begin{bmatrix} 8 \\ 3 \\ 12 \\ 5 \end{bmatrix} + \begin{bmatrix} 1 \\ -1 \\ 2 \\ -1 \end{bmatrix} = \begin{bmatrix} \\ \\ \\ \end{bmatrix}$$

Main Question

$$\begin{bmatrix} 2 \\ 13 \\ 7 \\ 3 \end{bmatrix} \star \begin{bmatrix} 8 \\ 3 \\ 12 \\ 5 \end{bmatrix} + \begin{bmatrix} 1 \\ -1 \\ 2 \\ -1 \end{bmatrix} = \begin{bmatrix} \\ \\ \\ \end{bmatrix}$$

- How do we define multiplication so that the resulting distribution is pseudorandom? (Coordinate-wise multiplication is not secure)

- Answer: Define it as multiplication in a polynomial ring
  - Similar ideas used in the heuristic design of NTRU [HPS98], and in compact one-way functions [Mic02,PR06,LM06,...].

Our Results

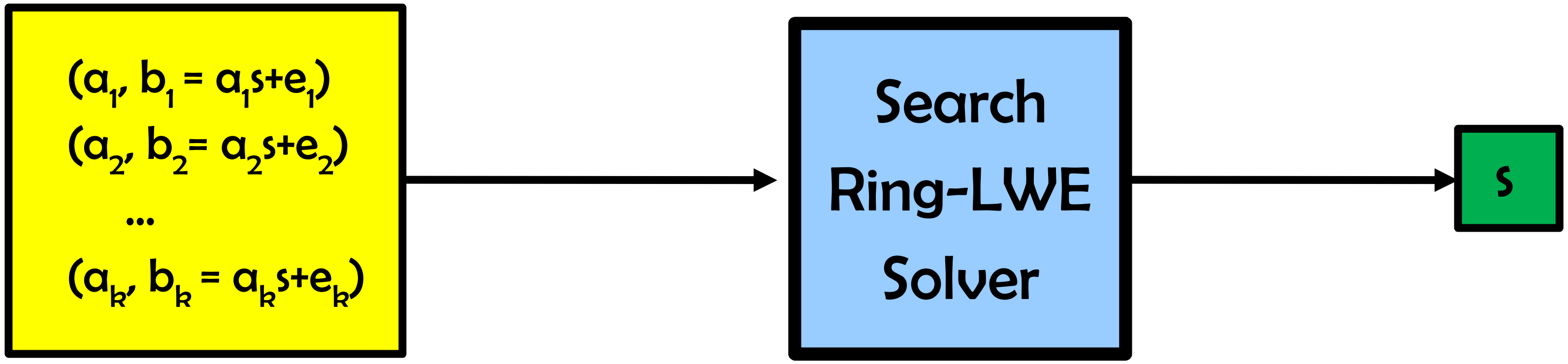
0. We define a compact version of LWE called Ring-LWE
1. We show that Ring-LWE is as hard as (quantumly) solving lattice problems on ideal lattices in the worst case
   - A qualitatively weaker result was independently shown by Stehlé, Steinfeld, Tanaka, and Xagawa [SSTX'09] using different techniques of independent interest.
2. We show that decision Ring-LWE is as hard as (search) Ring-LWE
   - Non-trivial
   - Works with any cyclotomic ring
3. We demonstrate some basic cryptographic applications

Learning With Errors over Rings

The Search Ring-LWE Problem

- Let R be the ring $\mathbb{Z}_q[x]/\langle x^n+1\rangle$ for n a power of 2 and q a prime satisfying q=1 (mod 2n).
    - E.g., q=17, n=4, $\mathbb{Z}_{17}[x]/\langle x^4+1\rangle$
- The secret s is now an element in R
- The elements a are chosen uniformly from R
- The coefficients of the noise polynomial e are chosen as small independent normal vars

$$\begin{array}{ccccccc} a & & s & & e & & b \\ \begin{bmatrix}2\\13\\7\\3\end{bmatrix} & * & \begin{bmatrix}8\\3\\12\\5\end{bmatrix} & + & \begin{bmatrix}1\\-1\\2\\-1\end{bmatrix} & = & \begin{bmatrix}8\\1\\16\\6\end{bmatrix}\end{array}$$



Our First Result: Hardness of Search Ring-LWE

- We show that the search ring-LWE problem is as hard as quantumly solving worst-case lattice problems on *ideal lattices*
  - For our ring, these are lattices satisfying that if $(x_1,\ldots,x_n) \in L$ then also $(x_2,\ldots,x_n,-x_1) \in L$
  - The result applies to rather general rings
- The proof is by adapting the proof of [R05] to rings
  - The quantum part remains the same; only the classical part needs to be adapted

Our First Result:
Hardness of Search Ring-LWE

- One technical issue is that the coefficients of the error polynomial e are not i.i.d. normal, but rather distributed according to a (non-spherical) Gaussian
  - Luckily this does not cause any serious problems, and we ignore it in this talk
  - It is possible to get hardness for the i.i.d. normal case if we restrict the number of ring-LWE samples (as in [SSTX'09] or as a corollary to our main result)

Our Second Result:

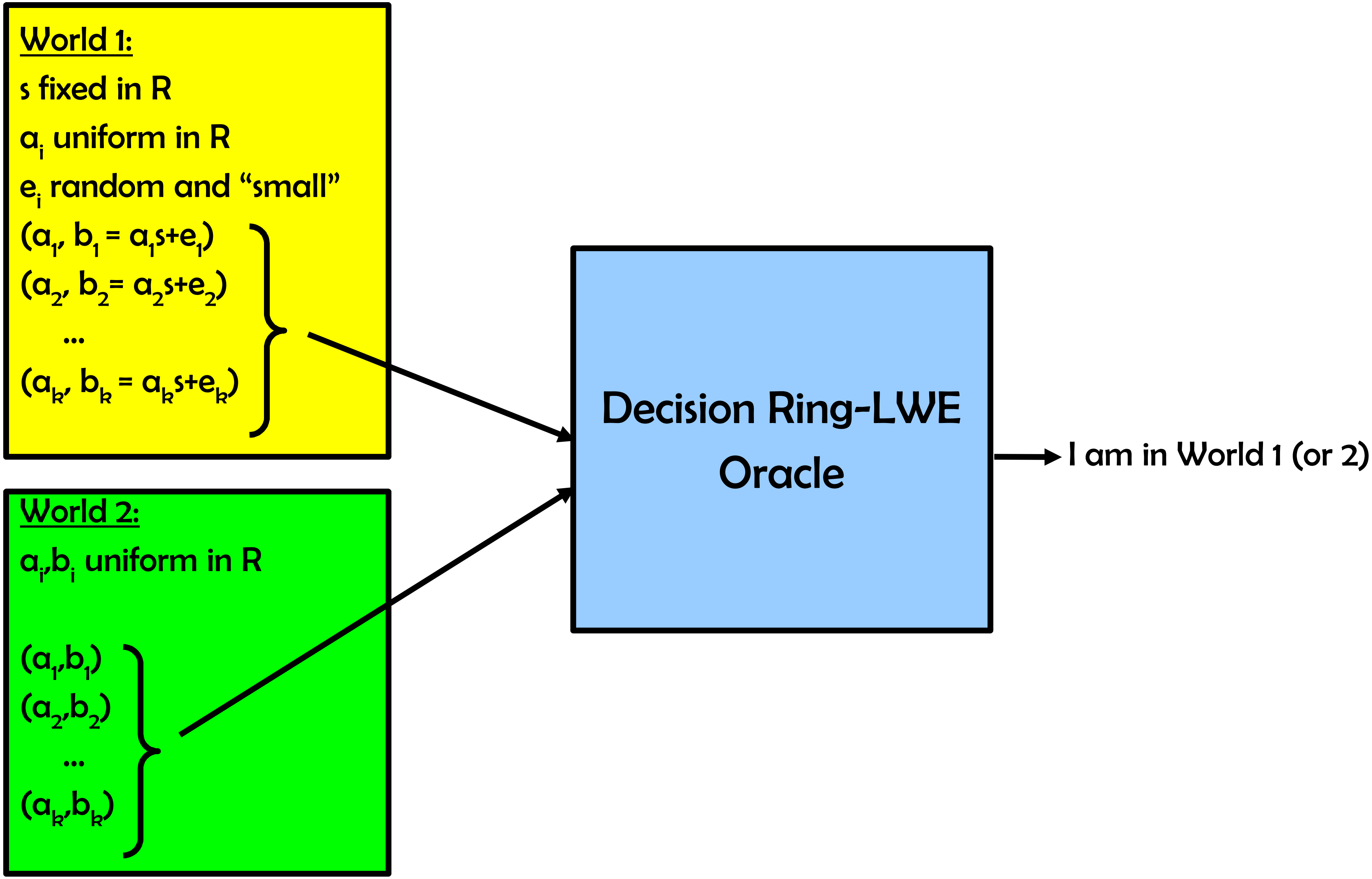
Reducing

Search Ring-LWE

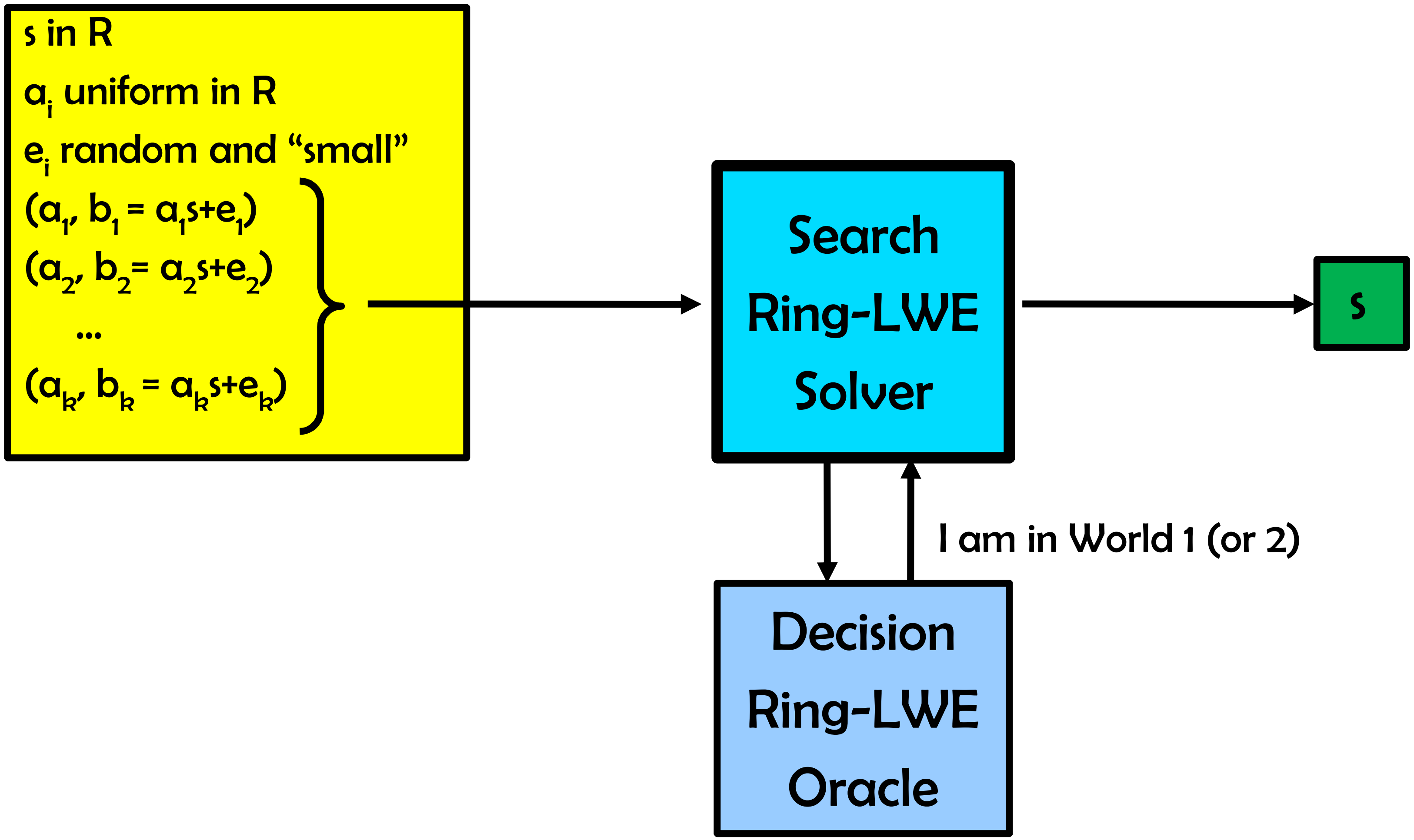
to

Decision Ring-LWE

Decision Ring-LWE Problem



What We Want to Construct



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

- Recall the reduction for LWE:
- Let g be our guess for the first coordinate of s (only 17 possibilities).
- Repeat the following:
  - Receive LWE pair (a,b):

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

  - Pick random r in Z_{17}
  - Send sample below to the Decision Oracle:

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

- Then:
  1. If g is correct, we have legal LWE samples;
  2. If g is incorrect, we have uniform samples

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

- Now consider what happens in ring-LWE:

$$\begin{array}{ccccccc} a & & s & & e & & b \\ \begin{bmatrix} 2 \\ 13 \\ 7 \\ 3 \end{bmatrix} & * & \begin{bmatrix} 8 \\ 3 \\ 12 \\ 5 \end{bmatrix} & + & \begin{bmatrix} -1 \\ -1 \\ 2 \\ 1 \end{bmatrix} & = & \begin{bmatrix} 8 \\ 16 \\ 8 \\ 1 \end{bmatrix} \end{array}$$

- Repeat the following:
  - Receive LWE pair (a,b):
  - Pick random r in Z_{17}
  - Send sample to the Decision Oracle:

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

- How do we satisfy (1), namely, output legal ring-LWE samples? It seems we have to guess all of s !

The Ring $\mathbb{Z}_q[x]/\langle x^n+1\rangle$

- Let $t \in \mathbb{Z}_q$ be such that $t^n=-1$ (i.e., a root of x^n+1).
- Then, for any $p_1,p_2 \in \mathbb{Z}_q[x]/\langle x^n+1\rangle$, $p_1(t)\cdot p_2(t)=(p_1\cdot p_2)(t)$, and obviously $p_1(t)+p_2(t)=(p_1+p_2)(t)$, hence the function mapping p to p(t) is a ring homomorphism
- By our assumption that q=1 (mod 2n), the polynomial x^n+1 has n roots in the field $\mathbb{Z}_q$,

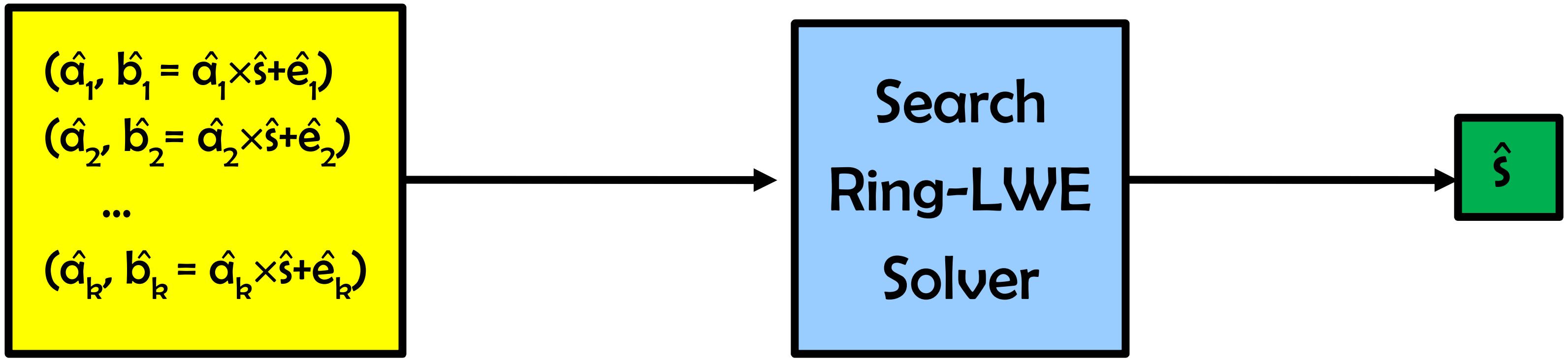
$$t_1=g^{(q-1)/2n},\ t_3=g^{3(q-1)/2n},\ \ldots,\ t_{2n-1}=g^{(2n-1)(q-1)/2n}$$

- Hence the mapping $\varphi: R \to \mathbb{Z}_q^n$ that maps each $p \in R$ to $\hat{p}=(p(t_1),\ldots,p(t_{2n-1})) \in \mathbb{Z}_q^n$ is a ring isomorphism, with both addition and multiplication in $\mathbb{Z}_q^n$ being coordinate-wise

The Search Ring-LWE Problem

- So we can equivalently think of ring-LWE as follows:
- The secret is an element $\hat{s}$ in $\mathbb{Z}_q^n$
- The elements $\hat{a}$ are chosen uniformly from $\mathbb{Z}_q^n$
- Multiplication is coordinate-wise
- The coordinates of the noise vector $\hat{e}$ are chosen from some ‘strange’ distribution

$$\begin{array}{ccccccc} \hat{a} & & \hat{s} & & \hat{e} & & \hat{b} \\ \begin{bmatrix} 2 \\ 13 \\ 7 \\ 3 \end{bmatrix} & \times & \begin{bmatrix} 8 \\ 3 \\ 12 \\ 5 \end{bmatrix} & + & \begin{bmatrix} 9 \\ 11 \\ 9 \\ 3 \end{bmatrix} & = & \begin{bmatrix} 8 \\ 16 \\ 8 \\ 1 \end{bmatrix} \end{array}$$



Search-to-Decision Reduction for Ring-LWE (better attempt)

- Let g be our guess for the first coordinate of $\hat{s}$ (only 17 possibilities).

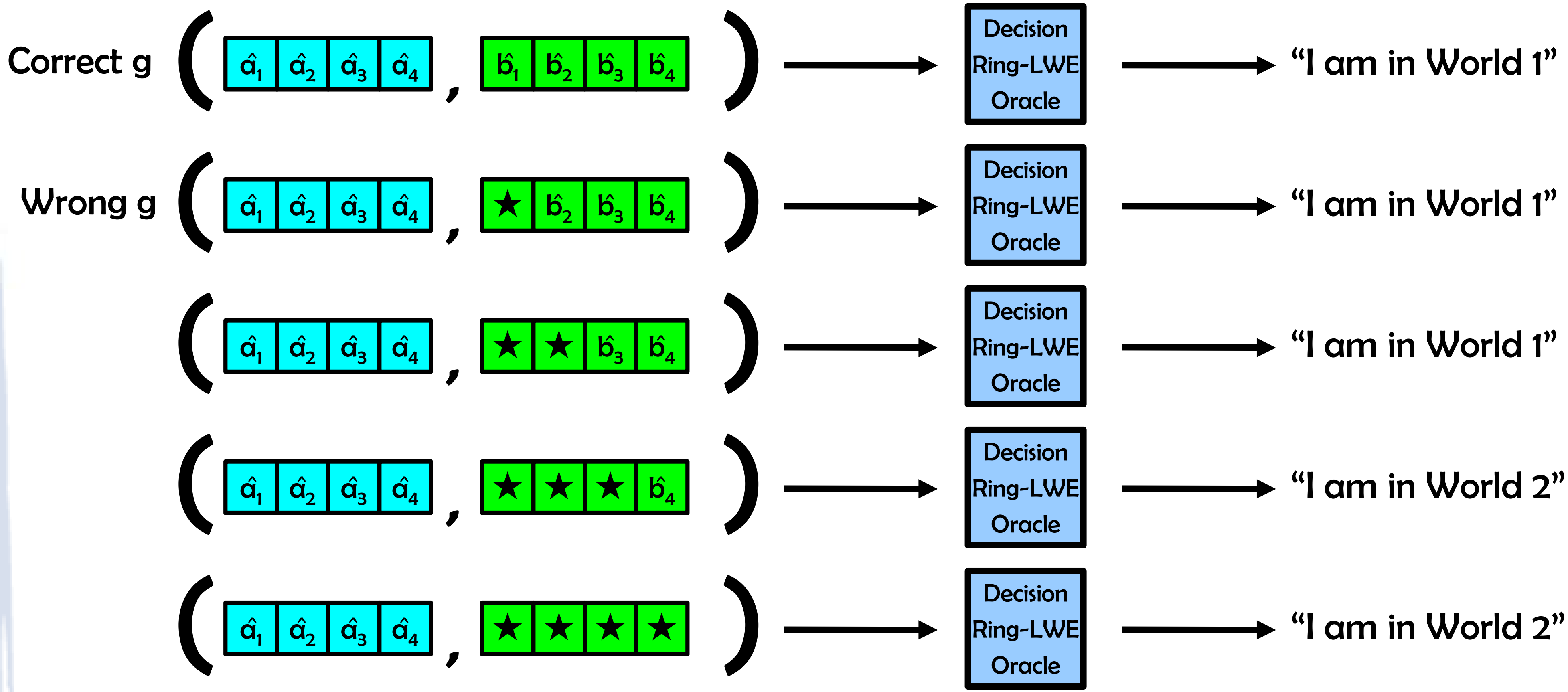
$$\begin{array}{ccccccc} \hat{a} & & \hat{s} & & \hat{e} & & \hat{b} \\ \begin{bmatrix} 2 \\ 13 \\ 7 \\ 3 \end{bmatrix} & \times & \begin{bmatrix} 8 \\ 3 \\ 12 \\ 5 \end{bmatrix} & + & \begin{bmatrix} 9 \\ 11 \\ 9 \\ 3 \end{bmatrix} & = & \begin{bmatrix} 8 \\ 16 \\ 8 \\ 1 \end{bmatrix} \end{array}$$

- Repeat the following:
    - Receive LWE pair $(\hat{a},\hat{b})$:
    - Pick random r in Z_{17}
    - Send sample to the Decision Oracle:

$$\begin{bmatrix} 2+r \\ 13 \\ 7 \\ 3 \end{bmatrix} \quad \begin{bmatrix} 8+rg \\ 16 \\ 8 \\ 1 \end{bmatrix}$$

- Then:
    1. If g is correct, we have legal ring-LWE samples! ☺
    2. BUT if g is incorrect, we don't have uniform samples ☹

A Hybrid Argument



- To summarize, using the decision oracle, we are able to find $\hat{s}_i$ for one *fixed* i
- But how can we recover all of $\hat{s}$?

Recovering All of s

- Idea: permute the coordinates of (the unknown) $\hat{s}$ by permuting $\hat{a}$ and $\hat{b}$

$$\begin{array}{ccccccc} \hat{a} & & \hat{s} & & \hat{e} & & \hat{b} \\ \begin{bmatrix} 2 \\ 13 \\ 7 \\ 3 \end{bmatrix} & \times & \begin{bmatrix} 8 \\ 3 \\ 12 \\ 5 \end{bmatrix} & + & \begin{bmatrix} 9 \\ 11 \\ 9 \\ 3 \end{bmatrix} & = & \begin{bmatrix} 8 \\ 16 \\ 8 \\ 1 \end{bmatrix} \end{array}$$

- Repeat the following:
  - Receive ring-LWE pair $(\hat{a},\hat{b})$:
  - Output the pair $(\pi(\hat{a}),\ \pi(\hat{b})= \pi(\hat{a})\times\pi(\hat{s})+\pi(\hat{e}))$:

$$\begin{bmatrix} 13 \\ 2 \\ 3 \\ 7 \end{bmatrix} \quad \begin{bmatrix} 16 \\ 8 \\ 1 \\ 8 \end{bmatrix}$$

- If the output pairs were legal ring-LWE samples with secret $\pi(\hat{s})$, we would be done
- But why would $\pi(\hat{e})$ be distributed correctly??

Recovering All of s

- It turns out that there are n special permutations $\pi_1,\dots,\pi_n$ that have the remarkable property that they preserve the error distribution!
- For instance, assume q=17 and n=4.
    - In this case, the mapping φ maps each polynomial $p(x)\in\mathbb{Z}_{17}[x]/\langle x^4+1\rangle$ to $\hat{p}=(p(2),p(2^3),p(2^5),p(2^7)) \in\mathbb{Z}_{17}^4$
- Now assume we permute this to $(p(2^3),p(2),p(2^7),p(2^5))$
    - I.e., π switches locations 1 and 2, and 3 and 4.
- This is equal to $\hat{p}'$ where $p'(x)=p(x^3)$
- Hence, if $p(x)=c_0+c_1x+c_2x^2+c_3x^3$ then $p'(x)= c_0+c_3x-c_2x^2+c_1x^3$
- We see that the permutation simply permutes the coefficients of the polynomial and possibly negates their sign.
- In particular, it preserves the error distribution!
- We can similarly take the permutations corresponding to $p'(x)=p(x^5)$, $p'(x)=p(x^7)$, and the identity permutation

Summary of Reduction

- By using a hybrid argument on the decision oracle, we are able to recover one fixed coordinate of $\hat{s}$
- Repeating this procedure with all n permutations allows us to recover all of $\hat{s}$, and hence also s, as required
  - Actually, one also need several delicate amplification steps and random self reductions… details in the paper!

- The reduction might seem mysterious and ad-hoc…
  - In fact, we are relying here on properties of the cyclotomic number field $\mathbb{Q}(\zeta_{2n})$, its n Galois automorphisms, its canonical embedding, and the factorization of the ideal $\langle q \rangle$
  - Viewed this way, the reduction is easy to extend to all cyclotomic polynomials (and not just x^n+1)

Final Summary

- Search Ring-LWE is as hard as (quantumly) solving lattice problems on ideal lattices in the worst case
- Decision Ring-LWE (in cyclotomic rings) is as hard as Search Ring-LWE
- Ring-LWE allows for much more efficient cryptographic constructions than regular LWE
- Open questions:
  - Attack ring-LWE
  - 'Upgrade' existing crypto constructions to ring-LWE
  - Theoretically sound fully-homomorphic encryption scheme based on ring-LWE?
  - Factor numbers given an algorithm for lattice problems