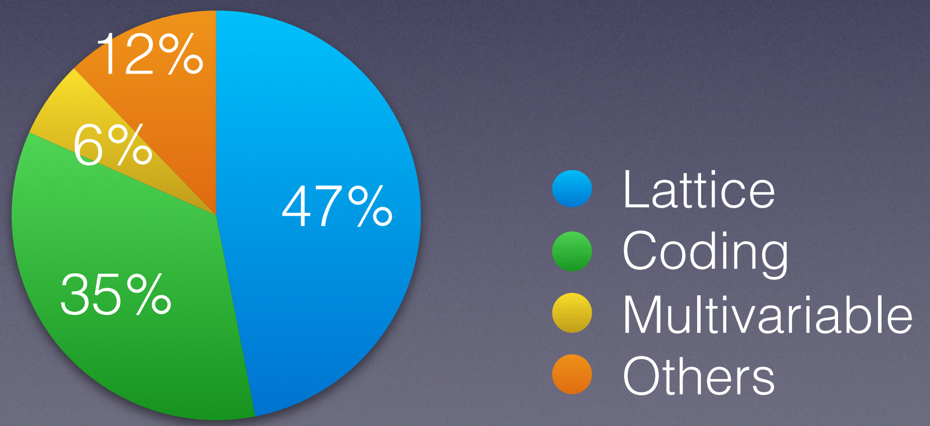
On the Hardness of the Computational Ring-LWR Problem and its Applications

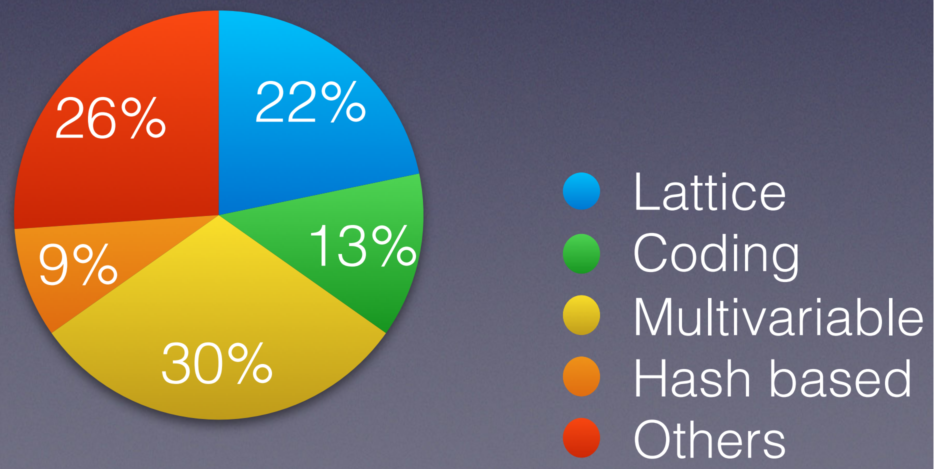
Long Chen, Zhenfeng Zhang, Zhenfei Zhang

PQC & Lattice

NIST R1 KEM



NIST R1 Signature



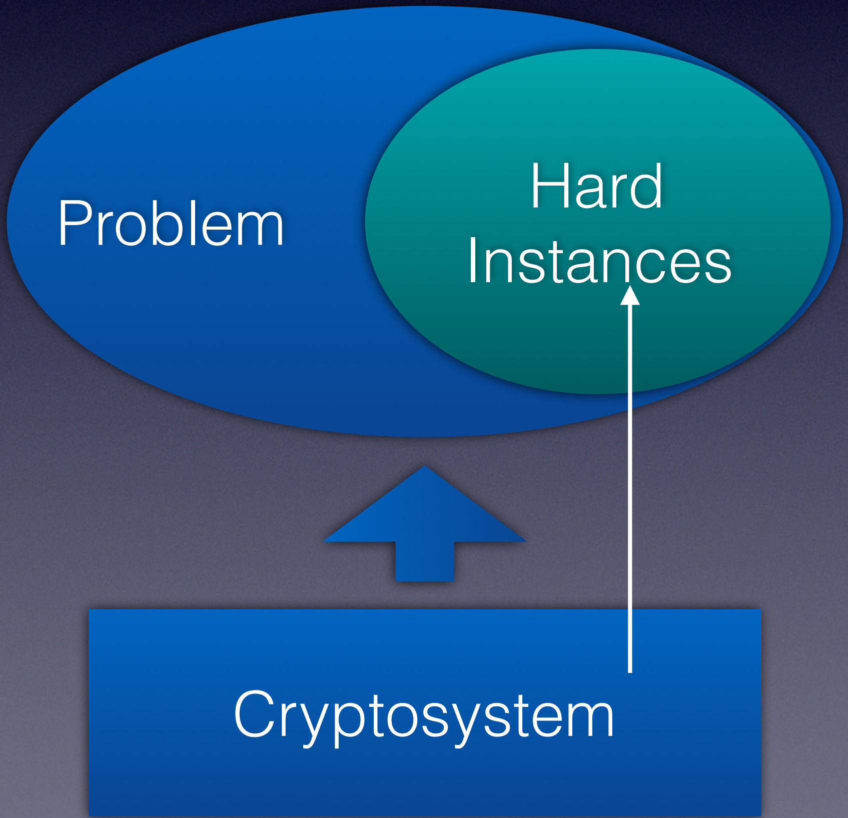
LWE Assumption

$$\{ A , A S + E \} \approx \{ A , U \}$$

- Benefits:
  - Quantum Resistance
  - Worst Case Hardness

Average Case

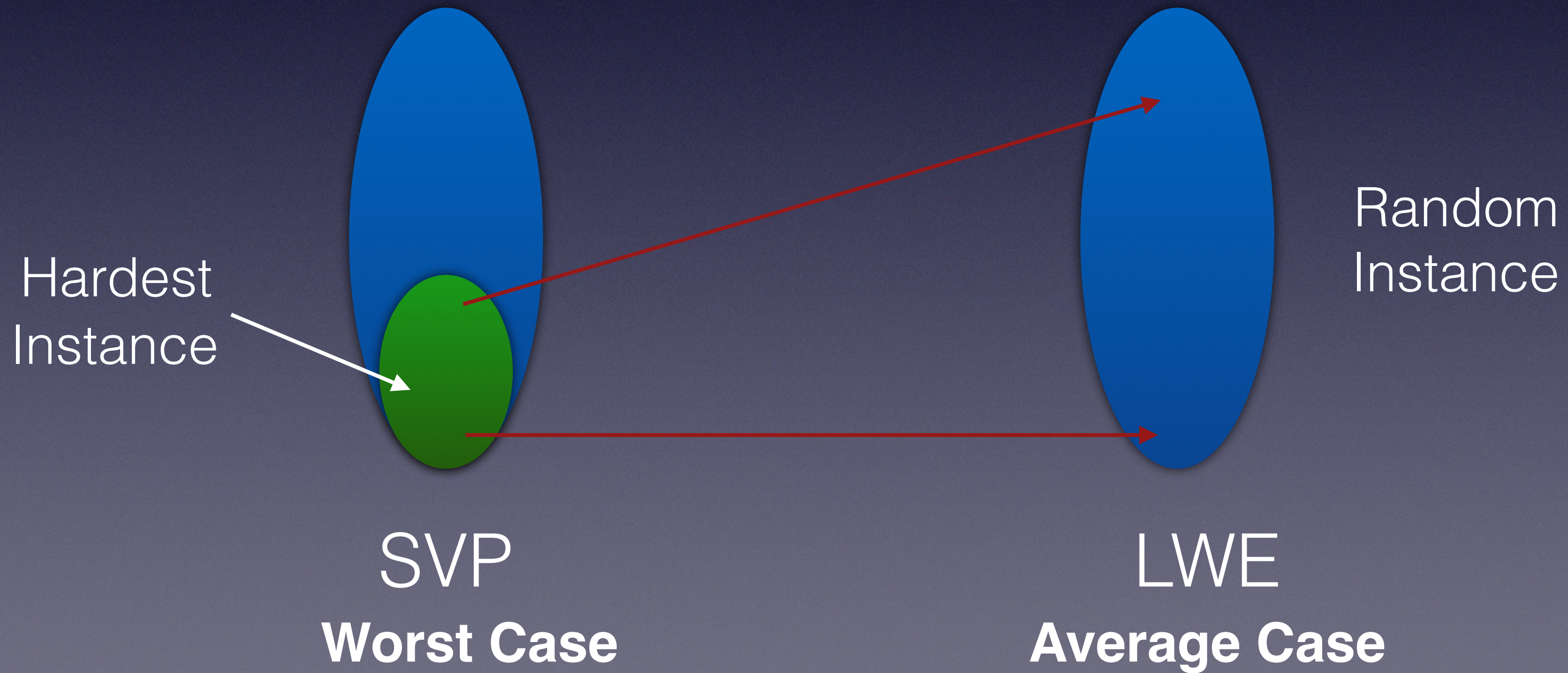
- Computation Complexity Theory



-

Worst Case to Average Case

Any (hardest) instance of SVP can be reduced to the average case of LWE problem (Regev 05)



Some Drawbacks

$$\{A, AS + E\} \approx \{A, U\}$$

① The larger size of matrix A makes the size of public keys and ciphertexts too large

Ring-LWE

② Sampling Gaussian noise is complex and consuming

LWR

Ring-LWE

- Let $R = \mathbb{Z}(X)/\Phi_m(X)$, and $R_q = R/qR$
- Ring-LWE is to distinguish

$$(a, as + e) \in R_q^2 \text{ and } (a, u) \in R_q^2$$

- Hardness Reduction (LPR10)

SVP on ideal lattice → Ring-LWE

Worst case **Average case**

Learning With Rounding

- Let $A \in \mathbb{Z}_q^{m \times n}$, $s \in \mathbb{Z}_q^n$, $u \leftarrow \mathbb{Z}_q^M$

- To distinguish

No Gaussian Sampling

$$(A, \lfloor As \rfloor_p) \quad \text{and} \quad (A, \lfloor u \rfloor_p)$$

- Hardness Reduction(BPR12,AKPW13,BGM+16)

SVP → LWE → LWR

Worst case **Average case**

Research Problem

Smaller PK and CT

Ring-LWE

LWR

Easy Sampling

Can we construct crypto system based on Ring-LWR?

What is the hardness about Ring-LWR?

Ring-LWR's Benefits

1. No Gaussian sampling, more efficient for computation

2. The size of public keys and ciphertexts are smaller

3. No decryption failure

In NIST Round 1 PQC Submissions, Saber, Round2 and Lizard adapt Ring-LWR instances instead of Ring LWE

Related Assumptions

- Decisional Assumption:
  - To distinguish $(a, \lfloor as \rceil_p)$ and $(a, \lfloor u \rceil_p)$

No Reduction

- Searchable Assumption:
  - Given $(a, \lfloor as \rceil_p)$, find $f(s)$

No efficient construction

- Computational Assumption:
  - Hope： has worst case reduction & can construct efficient schemes

Our Contributions

- Propose the computational Ring-LWR assumption (RCLWR) **secret is uniform and invertible**
  no Gaussian Sampling
- Provide a reduction from decisional Ring-LWE to computational Ring-LWR (Worst Case Hardness)
- Provide an asymptotically efficient PKE based on computational Ring-LWR
- Provide asymptotically security proofs for Saber, Round2 and Lizard under RCLWR

Intuition for RCLWR

$(a, \lfloor as \rceil_p)$

$(a, \lfloor u \rceil_p)$

Input

Output

Challenger

Adversary

Output=Target?

The adversary can not obtain more information from the Ring-LWR distribution than the uniform distribution !

CRLWR Assumption

Experiment 1:

Challenger $\left(\left(a, \lfloor as \rceil_p\right), ***\right) \rightarrow Input_1, Target_1$

Adversary $\left(Input_1\right) \rightarrow Output_1$

Success iff $Output_1 = Target_1$

Experiment 2:

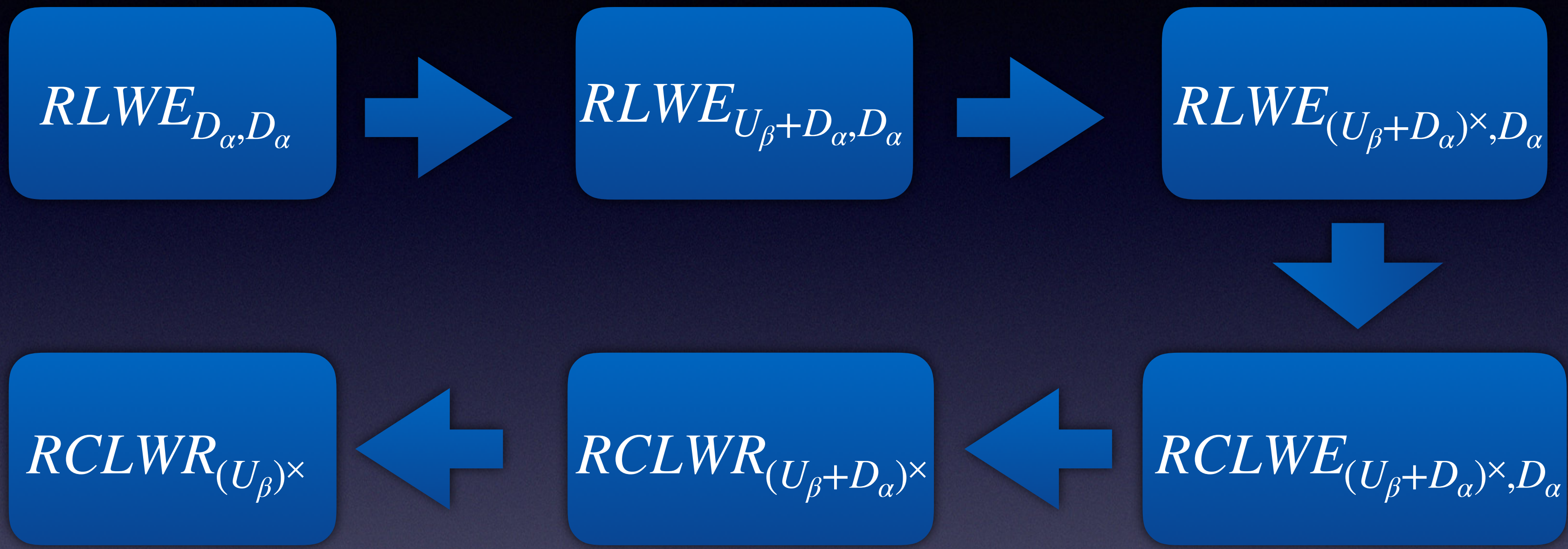
Challenger $\left(\left(a, \lfloor u \rceil_p\right), ***\right) \rightarrow Input_2, Target_2$

Adversary $\left(Input_2\right) \rightarrow Output_2$

Success iff $Output_2 = Target_2$

If Exp 2 is negligible, Exp 1 is also negligible

Reduction Outline



- The Renyi Divergence between $(a, \lfloor as + e \rceil_p)$ and $(a, \lfloor as \rceil_p)$ is small enough when s is invertible

- The Renyi Divergence between U_β and $U_\beta + D_\alpha$ is small

PKE Scheme

- High Level Idea: KEM+One-time Pad
- Our KEM: Similar to Peikert 14, replace Ring-LWE with Ring-LWR

– RCLWR.KeyGen(1^λ): Given the security parameter λ, choose a $seed \leftarrow \{0,1\}^{k'}$ and $a = \mathcal{G}(seed) \in R_q$. Then, sample s from $(U_\beta^n)^\times$ by repeating $s \leftarrow U_\beta^n$ until s is invertible. Output $(seed, b = \lfloor sa \rceil_p)$ as the public key and s as the secret key.

– RCLWR.Encryption($pk = (seed, b)$, $m \in \{0,1\}^k$): Given a message m, sample r from $(U_\beta^n)^\times$ by repeating $r \leftarrow U_\beta^n$ until r is invertible. Compute $\bar{v} = \lfloor \textsc{Inv}(b) r \rceil_p$, $\hat{v} = \textsc{Inv}(\bar{v})$ and $v = \langle \textsc{Dbl}(\hat{v}) \rangle_{2,2q}$. Also compute $a = \mathcal{G}(seed)$, $u = \lfloor ra \rceil_p$ and $w = \mathcal{H}\left([\textsc{Dbl}(\hat{v})]_{2,2q}\right) \oplus m$. The ciphertext is $ct = (u, v, w) \in R_p \times \{0,1\}^n \times \{0,1\}^k$.

– RCLWR.Decryption($ct = (u, v, w)$, $sk = s$): Compute $v' = s\textsc{Inv}(u)$ and output $m' = w \oplus \mathcal{H}(\textsc{Rec}(v', v))$.

Security Proof for PKE

1. Transform the IND-CPA game to compute the pre-image of the hash function using ROM

2. Replace the Ring-LWR instance in the public key with uniform instance

3. Replace the Ring-LWR instance in the ciphertext with uniform instance

4. If both the public key and ciphertext constructed from uniform instances, the probability for the adversary to guess the pre-image is negligible

Comparisons of PKE

- Precondition:
  - Satisfying Worst Case to Average Case Reduction
  - Decryption Failure Probability is Negligible

	Ring-LWE(Pei14)	Ours
Sampling in KeyGen	2	1
Sampling in Encrypt	3	1
Sampling distribution	Gaussian	Uniform & Invertible
Modulus for PK & CT	$\Omega\left(n^{5.5}\log^{0.5} n\right)$	$\Omega(n^{3.75}\log^{0.25} n)$

Thank you !!!