Introduction to Ring Learning with Errors

Lin Xuangeng

South China Normal University

April 23, 2018

Contents

1. What is ring learning with errors
2. Applications of ring learning with errors
3. Security proof
4. Summary

1. What is ring learning with errors

As an variant of learning with errors(LWE), ring learning with errors (RLWE) was first introduced by Vadim, Peikert and Regev in 2010[LPR10]. It is a hard problem which serves as the foundation of new cryptographic algorithms designed to protect against attack by quantum computers.

Definition (RLWE Distribution)

Let R_q denote the rings $\mathbb{Z}_q[x]/(x^n+1)$, where R is an polynomial ring on $\mathbb{Z}$ with rank n, and q is the modulus. Then define χ_α as discrete Gussian distribution with standard deviation α. Let $s \leftarrow_r R_q$, we define A_{s,χ_α} to be the distribution of the pair $(a, as+e) \in R_q \times R_q$, where $a \leftarrow_r R_q$ is uniformly chosen and $e \leftarrow_r \chi_\alpha$ is independent of a.

1. Elements in R_q are polynomials, which can be seen as vectors.
2. Ring is a kind of algerbra structure.

1. What is ring learning with errors

Accorrding to the RLWE distribution, we have a decision version of RLWE assumption(To distinguish with the search version of RLWE assumption).

Definition (Decision RLWE)

The decision RLWE assumption is claimed that it is hard for any probability polynomial time(PPT) algorithm to distinguish A_{s,χ_α} from the uniform distribution on $R_q \times R_q$.

Example:

World One: Given $(a, as + e)$, where $as + e$ is computed accorrding to a, s and e.

World Two:Given (a, b), where b is chosen from R_q uniformly.

Target:Given an input, which is an instance of RLWE, decides that you are in world one or world two.

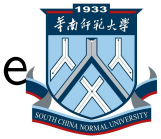
1. What is ring learning with errors

1.1 Why we need RLWE?

- Anti-Quantum Attack
- Strictly proved[LPR10] from other basic assumptions, which had been proved that they are secure by practices.
- Tarpdoor Function

1.2 What 's trapdoor?

- Door for honesty: Honest party can delete errors in an instance of RLWE by methods called Conciliation and Reconciliation(e.g. Rounding).
- Trap for adversary: Errors in RLWE provide high entropy and randomness, which make the instance of RLWE probabilistic indistinguishable with uniform randomness under informatics statistics without secret key.
- Probabilistic Indistinguish(IND): Guessing a bit, adversary win the game with a probability of 1/2+negligible.



2. Applications of ring learning with errors

We have a RLWE trapdoor function now, so we can use this cryptographic tools to do something, such as to construct some public key encryption(PKE) schemes, digital signature schemes(DSS), authentication key exchange protocols(AKE), etc.

Toy Example(IND-CPA secure):

Alice $\quad a \leftarrow R_q;\ s \leftarrow R_q;\ e \leftarrow \chi_\alpha;\ r \leftarrow Uniform \quad$ Bob

pk:=b=as+e; sk:=s

$$\underrightarrow{pk}$$

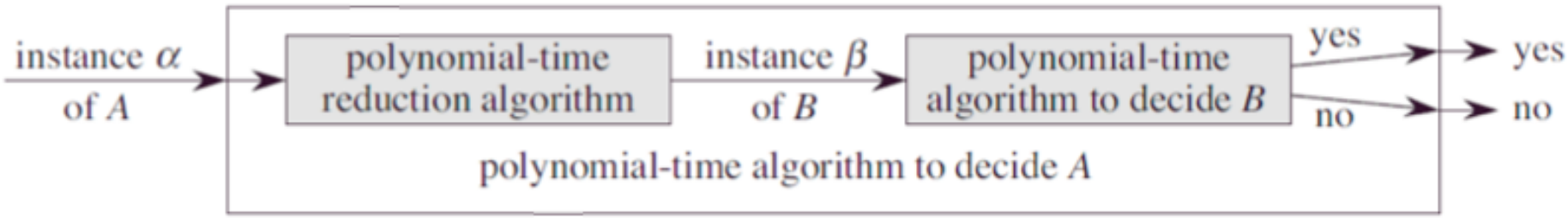
$$\underleftarrow{c = br + m \cdot \lceil \frac{q}{2} \rfloor}$$

$$\underleftarrow{v = ar}$$

Correctness:Because errors are small numbers, so Alice can reconciliate the ciphertext by rounding and then gets Bob's message.

3. Security proof

We proof the security by contraposition, which is called *reduction* in our major. The procedure below is reduction.



- Suppose that a crypto scheme can be cracked (Broken by adversary).
- Simulate environments with potential risks.
- Derive paradox accorrding to RLWE assumption.
- Security proved!

Simple example:Linear equation $y = ax + b$ and quadratic equation $y = ax^2 + bx + c$.

4. Summary

- RLWE is a provable secure assumption.
- Based on RLWE, we can construct many cryptographic schemes effective.
- Facing the growing challenge of quantum computer, RLWE has its practical significance.

Thanks