Introduction to Ring Learning with Errors

Lin Xuangeng

South China Normal University

April 23, 2018

Contents

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 and R_q denote the rings $\mathbb{Z}[x]/(x^n+1)$ and $\mathbb{Z}_q[x]/(x^n+1)$, 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

Why we need RLWE? Trapdoor function trap for adv but door for honest party and now i can explain what is errors. Probability indistinguish. 1/2+negl. can't do better. Information statistics and entropy.(explain: looks like uniform randomness)

2. Applications of ring learning with errors

we have rlwe as a trapdoor function, we can use this cryptographic tools to do something, such as to construct some public key encryption(PKE) schemes, to construct digital signature schemes, to consturct authentication key exchange protocols. Toy Example

3. Security proof

proof

4. Summary

summary

Thanks