Abstract

This thesis has constructed a threshold public key encryption (ThPKE) scheme based on Regev's lattice cryptosystem[Reg05] utilizing the technique of Boudgoust and Scholl[BS23].

Many quantum algorithms threaten the security and privacy of current (classical) encryption system[Sho94],[Gro96]. Therefore, we must develop alternative schemes with quantum resilience. The lattice cryptosystem is attracting attention as a prominent candidate for post-quantum cryptography due to its hardness and its applicatons.In fact, The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) released draft standards for three lattice-based cryptographic schemes for post-quantum cryptography in 2024[NIS24b]. The Regev cryptosystem discussed in this thesis serves as a prototype for one of them.

The conscept of threshold secret sharing was independently proposed by Shamir[Sha79] and Blakley[Bla99]. In threshold schemes, the secret key is distributed among multiple parties using a secret sharing method. Even if some of these parties (up to a predefined threshod) are corrupted, the secrecy of the key is maintained, even during partial decryption that rely on it. This approach not only enhances security by distributing trust but also elliminates the critical problem of "single point of failure" in public key encryption (PKE) systems. NIST is advancing a project to develop future recommendations and guidelines for threshold cryptosystems[NIS24a].

In ThPKE, the technique of "noise flooding" is typically used to prevent the leakage of information about the secret key during partial decryption. In the early stages, the security provided by noise flooding was measured using statistical distance[BD10],[BGG$^+$18], which resulted in overhead in ciphertext and noise sizes, leading to a deteroration of the LWE parameters and reduced efficiency. In contrast, Boudgoust and Scholl's technique improves the parameters by using the Rényi Divergence. However, Rényi Divergence does not align decisional security notions such as IND-CPA. Therefore, we realize IND-CPA by transfomating from OW-CPA. In this transformation, we use the random oracle model. However, Random oracle model makes a strong assumption about the existence of ideal hash funtion. As future concern, we aim to cunstruct a transfomation in the standard model.

By combining Regev's cryptosystem with a threshold cryptosystem, our scheme achives quantum resitance while enabling trust distribution with improved efficiency. Lastly, We campare various (t, N) linear secret sharing schemes, highlighting potential parameter optimizations and their impact on overall performance.