INDIAN INSTITUTE OF TECHNOLOGY GUWAHATI
SHORT ABSTRACT OF THESIS

Name of the Student	:	UDDIPANA DOWERAH
Roll Number	:	136102006
Programme of Study	:	Ph.D.
Thesis Title: On Lattice based Cryptographic Algorithms		
Name of Thesis Supervisor(s)	:	Dr. Srinivasan Krishnaswamy
Thesis Submitted to the Department/ Center	:	Electronics and Electrical Engineering
Date of completion of Thesis Viva-Voce Exam	:	21st June 2021
Key words for description of Thesis Work	:	Lattice based Cryptography, Fully Homomorphic Encryption, Learning with Errors, Multivariate polynomials, Hidden Subspace Membership..

SHORT ABSTRACT

In this thesis, we propose a few algorithms in the area of lattice-based cryptography. Lattice based cryptography is the construction of cryptographic algorithms the security of which, can be based on the conjectured hardness of lattice problems. Some of the important features of lattice-based cryptography are simple and efficient constructions, resistance to attacks by quantum algorithms, strong security proofs based on the worst-case hardness of lattice problems, etc.

First, we propose a Fully Homomorphic Encryption (FHE) scheme using multivariate polynomial evaluations. The scheme is designed in the framework of LWE (Learning with Errors) based schemes and its security depends on the hardness of the LWE problem. In this thesis, we have tried to utilize the intrinsic homomorphism in polynomial rings in order to perform homomorphic multiplication. Unlike other LWE based schemes, the size of the ciphertext does not grow with multiplication. Further, the noise associated with the ciphertexts increases only linearly.

We then show that the multiplication technique used in the FHE scheme can be extended to previous LWE-based schemes. By doing this, we can avoid the process of relinearization and the associated change of key after homomorphic multiplication. The evaluation key for the proposed multiplication technique is a third order tensor. In order to recover the secret key from the evaluation key, a system of non-linear equations must be solved.

Finally, we introduce a decision problem called the Hidden Subspace Membership problem and prove its hardness with respect to the LWE problem.