DECLARATION BY THE CANDIDATE

I hereby certify that the work embodied in this synopsis entitled “Ring-LWE Cryptography for Fingerprint Authentication Security” by Anubhav Singh (15/ICS/012) in partial fulfillment of the requirements for the award of the degree of B.Tech in CSE and M.Tech. in Information and Communication Technology (ICT) with Specialization in Software Engineering submitted to the School of Information and Communication Technology, Gautam Buddha University, Greater Noida is an authentic record of my own work carried out under the supervision of Dr. Pradeep Tomar , School of ICT. The matter presented in this synopsis has not been submitted by me in any other University/ Institute for the award of any other degree or diploma. Responsibility for any plagiarism related issue stands solely with me.

Signature of Student:

Anubhav Singh

This is to certify that the above statement made by the candidates is correct to the best of my knowledge and belief. However, the responsibility of any plagiarism related issue solely stands with the student.

Signature of Supervisor:

Dr. Pradeep Tomar

Date:

ACKNOWLEDGMENTS

I would like to express my deepest appreciation to all those who provided me the possibility to complete this synopsis. A special gratitude I give to my mentor, Dr. Pradeep Tomar, whose contribution in stimulating suggestions and encouragement, helped me to coordinate synopsis of Thesis.

My thanks and appreciations also go to my batch mates in helping me to complete this synopsis and people who have willingly helped me out with their abilities.

Anubhav Singh (15/ICS/012)

ABSTRACT

This paper presents the integration of Ring-LWE cryptographic algorithm with parallel processes in Fingerprint Authentication for security purposes. Ring-LWE is a homomorphic cryptographic algorithm with high level of hardness. To make the Ring-LWE Cryptography more efficient and faster, Number Theoretic Transform polynomial multiplication is used. Thus, making the fingerprint algorithm faster and more secure to protect the user's data. The base paper originally presented Tuy Nguyen Tan and Hanho Lee show that the proposed method outperforms the existing works up to 46% in encryption time and 44% in decryption time and it also shows that the latency of fingerprint authentication is 160ms. This paper revolves around the originally proposed method and to make it more efficient by further reducing the latency by using parallel methods of adder and multipliers, thus generating cypher texts faster and more efficiently.

LIST OF ABBREVIATIONS

LWE	Learn with Errors
R-LWE	Ring Learn with Errors
ECC	Elliptic Curve Cryptography
NTT	Number Theoretic Transform
INTT	Inverse Number Theoretic Transform
RTA	Request-To-Authenticate
RSA	Rivest, Shamir, and Adleman

LIST OF FIGURES

TABLE OF CONTENTS