شبكة المعلومات الجامعية

# بسم الله الرحمن الرحيم



# شبكة المعلومات الجامعية

# التوثيق الالكتروني والميكروفيلم


شبكة المعلومات الجامعية

# جامعة عين شمس

## التوثيق الإلكتروني والميكروفيلم

# قسم

## نقسم بالله العظيم أن المادة التي تم توثيقها وتسجيلها علي هذه الأقراص المدمجة قد أعدت دون أية تغيرات


# يجب أن

## تحفظ هذه الأقراص المدمجة بعيدا عن الغبار


# IMPROVING CRYPTANALYSIS OF LATTICE-BASED CRYPTOGRAPHY USING GPU

Presented By

Mohamed Sidi Mohamed Esseissah

Supervised By

*Assoc. Prof.* Sameh S. Daoud

*Assoc. Prof.* Hatem M. Bahig

*Dr.* Ashraf M. Kamal

SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENT FOR THE **Ph.D.** DEGREE
(COMPUTER SCIENCE)
SUBMITTED TO
DEPARTEMENT OF MATHAMETICS
FACULTY OF SCIENCE
AIN SHAMS UNIVERSITY
CAIRO, EGYPT

AIN SHAMS UNIVERSITY

Author: **Mohamed Sidi Mohamed Esseissah**

Title: **Improving Cryptanalysis of Lattice-Based Cryptography Using GPU**

Division: **Computer Science**

Department: **Department of Mathematics**

Faculty: **Faculty of Science**

Degree: **Ph.D.** Year: **2021**

# Contents

# List of Tables

# List of Figures

# Acknowledgements

First of all, I would like to express my gratitude and thanks to ***my mother*** and ***my father***, who have been very supportive for me not only during my doctorate preparation but also throughout all my life. I would not have been able to pursue my Ph.D degree or complete this dissertation without their support and encouragement. May God bless my father's soul, forgive him, and reward him the highest place in paradise. Secondly, I am very thankful to ***my wife*** for her continuous support to complete my study. I would like to express my sincere gratitude to Dr. ***Hatem*** and Dr. ***Ashraf*** for their continuous support, valuable discussion, and supervision, I really appreciate their great effort for helping me to achieve my Ph.D degree. In addition, I am thankful to Dr. ***Sameh*** for his kind help and valuable discussion.