شبكة المعلومات الجامعية

بسم اللّه الرحمن الرحيم

Ain Shams University Information Network

جامعة عين شمس

شبكة المعلومات الجامعية

@ ASUNET

شبكة المعلومات الجامعية

التوثيق الالكتروني والميكروفيلم

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

Ain Shams University
Faculty of Engineering
Computers and Systems Department

A Quantum Attack-Immune Public Key Cipher

by
Ayman Wagih Mohsen Ahmed Mohamed
Bachelor Degree in Computers and Systems Engineering
Ain Shams University 2014

A THESIS
SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF (MASTERS OF ELECTRICAL ENGINEERING, COMPUTERS AND SYSTEMS)

DEPARTMENT OF (COMPUTERS AND SYSTEMS)

Supervised by:
Prof. Dr. Ayman Mohamed Bahaa Eldin
Dr. Mohamed Ali Ali Sobh

Cairo, Egypt
December 2019

Faculty of Engineering
Ain Shams University
Computers and Systems

Examiners Committee

Name	**:**	**Ayman Wagih Mohsen Ahmed Mohamed**
Thesis	**:**	**A Quantum Attack-Immune Public Key Cipher**
Degree	**:**	**Master's of Computer Engineering - Computers and Systems**

Name, Title, and Affiliate	Signature
Prof. Dr. Amr Galal El-Din Ahmed Wassal Professor of Computer Engineering, Cairo University	....
Prof. Dr. Mohamed Ali Kamel Watheq El Kharashi Professor of Computer Engineering, Ain Shams University	....
Prof. Dr. Ayman Mohamed Bahaa Eldin Sadek Professor of Computer Engineering, Ain Shams University	....
Dr. Mohamed Ali Ali Mustafa Sobh Professor of Computer Engineering, Ain Shams University	....

Date: 2019-12-14

Abstract

Ayman Wagih Mohsen Ahmed Mohamed
A Quantum Attack-Immune Public Key Cipher
Master's in Electrical Engineering, Computers and Systems
Ain Shams University 2019

In this work we discuss the history of lattice-based cryptography, study the recently developed lattice-based cryptosystems, and compare the performance of the HewHope, Kyber, Saber and Round5 CPA public key cryptosystems and CCA key encapsulation mechanisms. These cryptosystems are among the candidates of the second round of the NIST post-quantum cryptography standardization competition. We concentrate on the performance of these cryptosystems. And the main factors affecting the performace are: polynomial multiplication and random buffer generation.

There are several methods to perform polynomial multiplication such as Karatsuba, Toom-Cook, index-based and NTT methods. The NTT method is the fastest, but it limits the choice of the cryptosystem parameters.

Random buffer generation can be sped up by using AES128 in counter mode or any fast stream cipher instead of the SHA3 function shake128. High performance can be achieved on modern processors by using the new AES instructions AES-NI.

We also profile the Kyber CPA cryptosystem to show the impact of random buffer generation using extendable output functions on the performance of such cryptosystems. We make all our code available at http://github.com/a1024/pqc.

Keywords:
Post-quantum, lattice-based crypto, asymmetric crypto, key encapsulation mechanisms

Summary

A Quantum Attack-Immune Public Key Cipher

Ayman Wagih Mohsen Ahmed Mohamed

Masters of Science in Electrical Engineering (Computers and Systems Engineering)

Keywords -- Post-quantum, lattice-based crypto, asymmetric crypto, key encapsulation mechanisms

In chapter 1 we present the general idea of the field of lattice-based cryptography and the motivation behind this work. Followed by the preliminaries explaining the notations used in the literature of lattice-based cryptography. Then some of the lattice-based problems are explained.

Chapter 2 discusses various examples of lattice-based cryptosystems. Beginning with the old lattice-based cryptosystems that are now depreciated. Then we discuss the cryptosystems based on the learning with errors (LWE) problem. Then the ring-LWE cryptosystem, and the underlying problem: learning with errors over polynomial rings. Then we discuss the modern ring-LWE based key encapsulation mechanisms (KEMs) that appeared in 2012 and afterwards. Leading to the newest KEMs NewHope, Kyber, Saber, and Round5.

In chapters 3 we discuss the underlying operations such as polynomial multiplication and modular reduction methods, and other implementation details.

In chapter 4 we present our implementations of various functions for lattice-based cryptography including the NTT polynomial multiplication method.

In chapter 5 we present and compare the results of benchmarking of different cryptosystems on different SIMD architectures. We also profiled

the Kyber cryptosystem as an example to show what operations have the major effect on performance. Then we present other methods for random buffer generation and compare them for speed. These methods include: SHA3 functions, AES128 in counter mode, and some of the fastest stream ciphers available as of time of writing. Then we present the results of randomness tests applied for these methods of random buffer generation.

In chapter 6 we make conclusions and discuss future work.

Thesis supervisors:

Prof. Dr. Ayman Bahaa El-Din

Dr. Mohamed Ali Sobh

Acknowledgements

I would like to thank God for His blessings and that I'm able to finish this thesis.

Also I'd like to thank mom and dad for their continuous encouragement.

I also would like to thank my supervisors Dr Ayman Bahaa and Dr Mohamed Sobh for their advice, guidance and inspiration.

Statement

This dissertation is submittedto Ain Shams University for the degree of Master's in Electrical Engineering in Computers and Systems department.

The work included in this thesis was out by the author at Computers and Systems Department, Ain Shams University.

No part of this thesis has been submitted for a degree of qualification at other university or institution.

Date : 2019-12-14

Signature :

Name : Ayman Wagih Mohsen Ahmed Mohamed

Table of Contents

List of Figures

List of Tables