ENHANCED FULLY HOMOMORPHIC ENCRYPTION SCHEME USING MODIFIED KEY GENERATION FOR CLOUD ENVIRONMENT

WAMDA ABDELRAHMAN ELHAG NAGMELDIN

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Doctor of Philosophy (Computer Science)

School of Computing
Faculty of Engineering
Universiti Teknologi Malaysia

MARCH 2020

DEDICATION

This thesis is dedicated to:

- My Mom and Dad
- My husband and my kids
- My family and friends, who have always been so proud of me. May they also be motivated and inspired to fly towards their dreams.

Without their endless love and infinitely support throughout my life I could not have accomplished my dreams. Their continued encouragement and inspiration lead me through the deep valley of darkness with the light of hope, trust and belief.

To all of you, a piece of my heart is yours.

Wamda

ACKNOWLEDGEMENT

First and foremost, I thank the Almighty Allah SWT for guiding me and giving me the strength to chase my dreams. There are no words to describe my wholehearted gratitude and appreciation to my supervisor Prof Dr. Siti Maryam Shamsuddin for her guidance, immense knowledge and sheer patience. I thank the Almighty Allah SWT for giving me a supportive advisor like her. I would like to thanks my supervisor Dr. Shafaatunur binti Hassan for her continued support. I would like to express a deep thanks to Dr. Subariah Ibrahim for her advice and supervising me during the first stage of this research. I would like to express my deepest gratitude to my colleagues in the Information Assurance & Security research group at the Universiti Teknologi Malaysia for the fruitful discussion and collaboration. I would like to express my extremely profound gratitude to my family for their understanding to my unique situation. I cannot imagine my current stature without their prayers, unconditional love and enormous support throughout my entire life. No words come close to describe my faithful gratitude to my beloved friends, who have been there for me always. This journey would never have completed without their incredible encouragement, unwavering faith and countless support. I would like to thank the International University of Africa and Universiti Teknologi Malaysia for giving me the chance to conduct this research. I would like to take this opportunity to thank those who have contributed therein by any direct or indirect means. To all of you: thank you.

ABSTRACT

Fully homomorphic encryption (FHE) is a special class of encryption that allows performing unlimited mathematical operations on encrypted data without decrypting it. There are symmetric and asymmetric FHE schemes. The symmetric schemes suffer from the semantically security property and need more performance improvements. While asymmetric schemes are semantically secure however, they pose two implicit problems. The first problem is related to the size of key and ciphertext and the second problem is the efficiency of the schemes. This study aims to reduce the execution time of the symmetric FHE scheme by enhancing the key generation algorithm using the Pick-Test method. As such, the Binary Learning with Error lattice is used to solve the key and ciphertext size problems of the asymmetric FHE scheme. The combination of enhanced symmetric and asymmetric algorithms is used to construct a multi-party protocol that allows many users to access and manipulate the data in the cloud environment. The Pick-Test method of the Sym-Key algorithm calculates the matrix inverse and determinant in one instance requires only $n-1$ extra multiplication for the calculation of determinant which takes $O(N^3)$ as a total cost, while the Random method in the standard scheme takes $O(N^3)$ to find matrix inverse and $O(N!)$ to calculate the determinant which results in $O(N^4)$ as a total cost. Furthermore, the implementation results show that the proposed key generation algorithm based on the pick-test method could be used as an alternative to improve the performance of the standard FHE scheme. The secret key in the Binary-LWE FHE scheme is selected from $\{0,1\}^n$ to obtain a minimal key and ciphertext size, while the public key is based on learning with error problem. As a result, the secret key, public key and tensored ciphertext is enhanced from $\log q$, $O(n^2\log^2 q)$ and $\big((n+1)\lceil\log q\rceil\big)^2\log q$ to n, $(n+1)^2\log q$ and $(n+1)^2\log q$ respectively. The Binary-LWE FHE scheme is a secured but noise-based scheme. Hence, the modulus switching technique is used as a noise management technique to scale down the noise from e and c to e/B and c/B respectively thus, the total cost for noise management is enhanced from $O(n^3\log^2 q)$ to $O(n^2\log q)$. The Multi-party protocol is constructed to support the cloud computing on Sym-Key FHE scheme. The asymmetric Binary-LWE FHE scheme is used as a small part of the protocol to verify the access of users to any resource. Hence, the protocol combines both symmetric and asymmetric FHE schemes which have the advantages of efficiency and security. FHE is a new approach with a bright future in cloud computing.

ABSTRAK

Penyulitan homomorfik penuh (FHE) merupakan kelas khas penyulitan yang membolehkan pelaksanaan operasi matematik yang tidak terhad pada data yang disulitkan tanpa menyahsulitkannya. Terdapat skema (FHE) simetri dan tidak simetri. Skema simetri tiada ciri keselamatan semantik dan memerlukan lebih banyak penambahbaikan prestasi. Walaupun skema tidak simetri adalah selamat tetapi ia mempunyai dua masalah tersirat. Masalah pertama berkaitan dengan saiz kekunci dan teks sifer manakala masalah kedua adalah kecekapan skema. Kajian ini bertujuan untuk mengurangkan masa pelaksanaan skema (FHE) simetri dengan meningkatkan algoritma penjanaan kekunci menggunakan kaedah Pilih-Uji. Oleh itu, Pembelajaran Perduaan dengan Kekisi Ralat digunakan untuk menyelesaikan masalah saiz kekunci dan teks sifer skema (FHE) tidak simetri. Gabungan algoritma simetri dan tidak simetri yang dipertingkatkan digunakan untuk membina protokol berbilang pihak yang membolehkan ramai pengguna mengakses dan memanipulasi data dalam persekitaran awan. Kaedah Pilih-Uji bagi algoritma *Sym-Key* mengira balikan matriks dan penentu dalam satu tika dan hanya memerlukan $n-1$ pendaraban tambahan untuk pengiraan penentu yang menggunakan $O(N^3)$ sebagai kos keseluruhan, manakala kaedah Rawak dalam skema standard menggunakan $O(N^3)$ untuk mencari balikan matriks dan $O(N!)$ untuk mengira penentu yang terhasil dalam $O(N^4)$ sebagai kos keseluruhan. Tambahan pula, keputusan pelaksanaan menunjukkan bahawa algoritma penjanaan kekunci yang dicadangkan berdasarkan kaedah Pilih-Uji boleh digunakan sebagai alternatif untuk meningkatkan prestasi skema *FHE* standard. Kekunci rahsia dalam skema Perduaan-*LWE FHE* dipilih daripada $\{0,1\}^n$ untuk mendapatkan kekunci minimum dan saiz teks sifer, manakala kekunci awam berdasarkan pada pembelajaran dengan masalah ralat. Hasilnya, kekunci rahsia, kekunci awam dan teks sifer bertensor masing-masing dipertingkatkan daripada $\log q$, $O(n^2\log^2 q)$ dan $\big((n+1)\lceil\log q\rceil\big)^2\log q$ kepada n, $(n+1)^2\log q$ dan $(n+1)^2\log q$. Skema Perduaan-*LWE FHE* merupakan satu skema berdasarkan hingar tetapi selamat. Oleh itu, teknik pertukaran modulus digunakan sebagai teknik pengurusan hingar untuk menurunkan skala hingar masing-masing daripada e dan c kepada e/B dan c/B dan kos keseluruhan bagi pengurusan hingar dipertingkatkan daripada $O(n^3\log^2 q)$ kepada $O(n^2\log q)$. Protokol Berbilang pihak dibina untuk menyokong pengkomputeran awan pada skema *Sym-Key FHE*. Skema Perduaan-*LWE FHE* tidak simetri digunakan sebagai bahagian kecil protokol tersebut untuk mengesahkan akses pengguna kepada mana-mana sumber. Oleh itu, protokol ini menggabungkan kedua-dua skema *FHE* simetri dan tidak simetri yang mempunyai kelebihan kecekapan dan keselamatan. *FHE* merupakan satu pendekatan yang masih baru dengan masa depan yang cerah dalam pengkomputeran awan.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ABAC	-	Attribute-Based Access Control
AES	-	Advanced Encryption Standard
AGCD	-	Approximate Greatest Common Divisor
AS	-	Adversary structure
Binary-LWE	-	Binary Learning With Error
CIA	-	Confidentiality, Integrity, and Availability
CPA	-	Chosen -plaintext attack
CRT	-	Chinese remainder theorem
CSP	-	Cloud service provider
Dec	-	Decryption Algorithm
DES	-	Data Encryption Standard
DGHV	-	Van Dijk et al. , 2010b Scheme
ECC	-	Elliptic curve cryptosystems
ECDLP	-	Elliptic curve discrete logarithm problem
ELP	-	Euclidean lattices problems
Enc	-	Encryption Algorithm
Eva	-	Evaluate Algorithm
FHE	-	Fully Homomorphic Encryption
GCD	-	Greatest Common Divisor
HNF	-	Hermite normal form
IDC	-	International Data Corporation
IFP	-	Integer Factorization problem
KD	-	Key distributor
KeyGen	-	Key generation Algorithm
KM	-	The key manager
KPA	-	Known-plaintext attack
LIF	-	Large Integer Factorization Problem
LWE	-	Learning With Error
MAGCD	-	Matrix Approximate Greatest Common Divisor
MHE	-	Multiplicatively Homomorphic Encryption

MORE	-	Matrix Operation for Randomization or Encryption
MPAC	-	Multi-party Protocol with Access Control
MP-protocol	-	Multi-party protocol
PIR	-	Private Information Retrieval
PORE	-	Polynomial Operation for Randomization or Encryption
PRB	-	Policy Rule Base
RLWE	-	Ring Learning With Error
RSA	-	R. Rivest, A. Shamir, and L. Adleman. Scheme
SIMD	-	Single Instruction Multiple Data
SSSP	-	Sparse Subset Sum Problem
SWHE	-	Somewhat homomorphic Encryption
Sym-Key	-	Symmetric Key
TFHE	-	Threshold Fully Homomorphic Encryption
TP	-	The trusted party

LIST OF SYMBOLS

pk	-	Public key
sk	-	Secret key
m_i	-	The plaintext
c_i	-	The ciphertexts
λ	-	The security parameter
Ψ	-	Circuit operation
$\ominus$	-	Some operation
poly(λ)	-	The polynomial size
Γ	-	group of gates
R	-	Ring for polynomial $f, R = \mathbb{Z}[x]/f$
I	-	Coprime ideal
J	-	Coprime ideal
B_I	-	Ideal basis
B_J^{sk}	-	Secret basis
B_J^{pk}	-	Public basis
π_1	-	The plaintexts
$a_1, a_2, \ldots, a_n$	-	Group of positive integers
α	-	Integer number
$modulo\ p$	-	$modulo\ p$
Z_N	-	Integers modulus Z
$M_4(\mathbb{Z}_N)$	-	4- dimensions square matrix of integer modulus Z
$p_i$and q_i	-	Prime numbers
$\varphi(n)$	-	Euler's phi function
O	-	Big Oh notation
Ω	-	Big Omega notation
Θ	-	Big theta notation
o	-	Little oh notation
$\tilde{O}$	-	Fit approximation notation
K	-	Key matrix

K^{-1}	-	The inverse of Key matrix
p_i	-	The probability
$det(k)$	-	Matrix's determinant
$adj(k)$	-	Matrix's adjacent
$diag$	-	Diagonal matrix
k	-	Master key
sk_i	-	User key
$sk_i{}'$	-	First match of the user key
$sk_i{}''$	-	Second match of the user key
V	-	vector space
$\|v\|$	-	length of the vector v
e_i	-	Error value
$f(x)$	-	Polynomial function
P^T	-	Matrix Transpose
$[\ ]_2$	-	Mod 2
$[\ ]_q$	-	Mod q
$\lfloor\ \rceil$	-	Round to nearest number
$\langle v, u \rangle$	-	Inner product
$\otimes$	-	Tensored product

CHAPTER 1

INTRODUCTION

1.1 Overview

In cryptography, encryption is the method of obscuring information to make it illegible without specialized knowledge called the key. This is usually done for privacy and typically for confidential communications. Encryption systems permit clients to secure classified in their information, for instance, healthy or monetary records whether the information is in the storage, client's PC, cloud, or in transit. Cryptography is used in the cloud to employ encryption techniques for protecting data that is utilized or saved in the cloud. Cryptography permits users to reach distributed cloud services conveniently and securely. Using encryption in the cloud environment preserves users' sensitive data without affecting the data transferring process and increases the security of cloud computing.

Homomorphic encryption is a particular class of encryption presented by Rivest *et al.* (1978) that allows performing mathematical operations on the ciphertexts without decrypting all of them, essentially, with no knowledge of the decryption key. In the last several years, homomorphic encryption systems are actually studied and analysed thoroughly given that they have grown to be increasingly more important in several cryptographic protocols such as lottery protocols, e-voting protocols, anonymity, security, as well as electronic auctions. For instance, given ciphertexts $C = Enc_k(P)$ and $C' = Enc_k(P')$, an additively homomorphic encryption scheme permits to add C and C' to obtain $Enc_k(P + P')$. This kind of encryption scheme is enormously valuable in the model of intricate cryptographic systems and protocols. For example, an electronic voting scheme might accumulate encrypted votes $C_i = Enc_k(P_i)$ in which each and every vote P_i is possibly 0 or 1, to obtain the final encrypted result $C = Enc_k(P_1 + \cdots + P_n)$. The result may be decrypted by an appropriate authority which has the decryption key and the ability to publish the final result.

Homomorphic cryptosystems are ones where mathematical operations on the encrypted data have normal effects as on the original data. The symmetric cipher such as Data Encryption Standard (DES) which discovered in Standard (1977) and Advanced Encryption Standard (AES) in Standard (2001) are not homomorphic. Rivest–Shamir–Adleman **(**RSA)'s homomorphism is proposed by Rivest *et al.* (1978) which performs multiplication operation on the ciphertexts and reflected in the plaintext. Some algorithms that are homomorphic concerning to addition have been known since the 1980s but fully homomorphic under both multiplication and addition and still secure discovered by (Gentry, 2009). A homomorphic scheme that permits homomorphic computation of only one operation (either multiplication or addition) on ciphertexts is called a partial homomorphic scheme. There are several efficient partially homomorphic cryptosystems such as RSA Rivest *et al.* (1978) and ElGamal encryption system (ElGamal, 1985).

1.2 Problem Background

The scheme proposed in Gentry (2009) is the first fully homomorphic encryption (FHE) scheme that permits any person to manipulate the ciphertexts without having an ability to decrypt it. Gentry utilized mathematical object referred to as an ideal lattice. His public key scheme possesses several algorithms Key Generation, Encryption, Decryption as well as an extra algorithm referred to as Evaluation algorithm that requires pk which represents the public key, an operation Ψ that perform on the ciphertexts as well as ciphertexts $(\mathrm{c}_1, \ldots, \mathrm{c}_t)$ as inputs, it produces an another ciphertext c. The complexity of Key Generation, Encryption, Decryption and Evaluation algorithms ought to be polynomial in security parameter λ along with the $c's$ dimensions.

Regrettably, Gentry's FHE scheme is totally impractical, and both the ciphertext size and the complexity of the encryption and decryption calculations become colossally with the size of operations performed on the ciphertext. The authors of Smart and Vercauteren (2010) tackled with this issue by proposing a fully homomorphic encryption scheme which has both generally small key and ciphertext

size by utilizing the little two component representation $\langle \alpha, p \rangle$, prime p and integer number α modulo p, rather than the bigger Hermite Norm Form (HNF) representation that utilized by Gentry in the first FHE scheme. They followed the same way of Gentry's scheme by utilizing the principal of ideal lattices and in addition, require a prime number to represent the lattice determinant. In particular, the key-generation algorithm executed more than once to picks irregular key goals until the comparing lattice section has a prime determinant. They could actualize the basic somewhat homomorphic scheme and still they were not ready to support sufficiently extensive parameters to make Gentry's squashing process works. Accordingly, they couldn't get a bootstrappable or a fully homomorphic scheme. The FHE scheme that is presented in Gentry and Halevi (2011) introduced the improvements of the basic Gentry's work. They proposed various enhancements that permit all stages of the FHE scheme to be executed, including the bootstrapping usefulness but still needs more improvements.

Most of the schemes are stated earlier determined by lattice problems, to assist the simplicity functionality of the fully homomorphic scheme, the authors of Van Dijk *et al.* (2010b) offered a FHE scheme based on integers as opposed to the lattice. The security of the scheme is dependent upon the hardness of choosing an estimate integer Greatest Common Divisor Problem (GCD). The most important open issue of the scheme is always to enhance the performance.

Until recently, the majority of FHE schemes followed the same direction of Gentry's original construction. The original construction of Gentry divided into three steps to obtain the FHE:

Step1 *Somewhat homomorphic encryption (SWHE):* Construct a SWHE that restricted by a limited number of addition and multiplication operation and can evaluate low-degree polynomials.

Step2 *Bootstrapping:* The SWHE scheme can handle circuits up to a certain depth d. (Plus, an additional operation), apply Gentry's alteration to get an equalized FHE scheme. Bootstrapping refreshes a ciphertext by functioning the decryption

operation about it homomorphically, utilizing an encrypted hidden key which is provided in the public key by means of re-encryption algorithm.

Step 3 *Squashing:* Squash the decryption operation of the SWHE scheme, until decryption could be stated as a polynomial of degree minimal enough to be taken care of within the homomorphic capability of the SWHE scheme.

Though Gentry's invention Gentry (2009) gives a solution, but it is very important to develop improvements of Gentry's and related schemes to obtain more practical and feasible FHE schemes. The primary problems of using FHE schemes which based on the original Gentry's work are the size of the public key, multiple keys are used in the process of the scheme, the size of ciphertext is growing after computational operations as well as the accumulation of the noise. However, the delegation of computation is the main application of fully homomorphic encryption due to the limitation or lack of the resources at the user's side. The majority of the schemes have intensive computations which make the schemes impractical (Moore *et al.*, 2014). Reducing key sizes to a controllable level considered an open problem (Martins *et al.*, 2018). The procedure of the fully homomorphic scheme requires, in any case, three keys (encryption key, decryption key, and evaluation key).

The main issue concerns to improve the fully homomorphic schemes with specialized features, such as efficiency, light-weight, noise-free, fast, short key size, multiparty as well as semantic security property. Majority of applications such as private information retrieval PIR and e-voting do not need to use fully homomorphic schemes, but only use somewhat or partial homomorphic schemes. Somewhat homomorphic encryption scheme (SWHE) supports only a limited number of operations homomorphically. While the partial homomorphic scheme supports either addition or multiplication operations but not both. Thus, these schemes are restricted to limited applications, and cannot be generalized or extended to all application categories. Fully homomorphic encryption is used in cloud computing applications and allows performing unlimited number of operations on the encrypted data.

There are two types of the FHE cryptosystems, symmetric and asymmetric. Symmetric FHE schemes are noise-free, efficient and practically feasible but suffers from the semantically security property. Asymmetric FHE schemes are semantically secure, noise-based schemes and complex in implementation. To construct an efficient and secure FHE for cloud, the advantages of symmetric and asymmetric schemes are combined. Xiao *et al.* (2012) introduced one of the best symmetric FHE schemes. However, this scheme needs improvements to enhance its efficiency. The efficiency means the execution time takes to implement the FHE algorithms. Brakerski (2012) introduced asymmetric FHE scheme based on LWE Lattice problem. Ciphertext size in this scheme grows with a degree of function f that performs on a ciphertext. When adding or multiplying ciphertexts, the noise e is increased until it becomes too large and decryption is not correct. The scheme uses a high cost bootstrapping technique to manage this noise.

The majority of the existing FHE schemes are asymmetric which use the public-key cryptography. Asymmetric FHE scheme has a clear benefit because it depends on difficult mathematical problems such as Approximate GCD, Large Integer Factorization or Diffie-Hellman problems. Nevertheless, There are some applications that by their nature require only the use of symmetric keys and do not need to use the public keys in any way. For example, When the user saves his private data on the cloud for personal use only, he uses the symmetric scheme with the secret key because he does not want to share his data with other parties. In contrast, there are many applications require multi-party sharing, such as computation on securing cloud storage using a homomorphic framework in Gupta and Biswas (2018), utilizing FHE to implement secure medical computation in smart cities in Sun *et al.* (2017), outsourced privacy-preserving classification service over encrypted data in Li *et al.* (2018), and using FHE to secure cloud computing in (Jabbar and Najim, 2016). Most of the proposed FHE schemes describe the cryptosystems and have not explained the area of multi-party sharing.

1.3 Problem Statement

Based on the previous studies in the FHE schemes, the symmetric FHE schemes suffer from the semantically security property and need more efficiency enhancements. Efficiency refers to the execution time, while, asymmetric FHE schemes which based on lattice problem are semantically secure but have two implicitly problems. First problem related to the size of key and ciphertext. Ciphertext size grows with a degree of function f that performs on it. When adding or multiplying ciphertexts, the noise e increases until it becomes too large and decryption is not correct, while the second problem is the efficiency of the schemes. The FHE schemes are mainly used in the cloud and there is no efficient and secure implementation in this area. As a result, the major research question is:

"How to improve efficient and secure FHE schemes and uses these schemes as a basis to costruct a multi-party protocol to allow many users access and manipulate data in the cloud or any data center?".

To solve the major research question, the subsequent questions must be answered precisely:

(a) How to to enhance the efficiency of the key generation algorithm of the symmetric key FHE scheme?

(b) Could Binary-LWE improve the key and tensored ciphertext size of the asymmetric key FHE scheme?

(c) What is the appropriate dealing for accumulated noise after homomorphic operation?

(d) How to construct a multi-party protocol that allows many users access and manipulate the data in the cloud using secure and efficient FHE schemes?

1.4 Aim of the Research

This research aims to enhance the efficiency of the fully homomorphic encryption schemes based on symmetric and asymmetric encryption and to implement these proposed enhanced schemes in the cloud environment to support multi-users with access control.

1.5 Research Objectives

The goal of this study is to develop and enhance the FHE schemes for cloud environment. The enhanced schemes are develped to solve the problems related to the efficiency of the key generation algorithms and the noise management of ciphertext size after any computational operations and obtain a correct ciphertext. According to these problems, the main objectives of this study are:

(a) To improve the performance of the key generation algorithm of the Xiao *et al.* (2012) symmetric FHE scheme using the Pick-Test method in order to reduce the execution time, which is more efficient and practically feasible.

(b) To produce the minimal key size of the key generation algorithm using the Binary-LWE lattice problem; manage the noise and ciphertext size after any computational operation in order to obtain a correct ciphertext of the Brakerski (2012) asymmetric FHE scheme; and ensuring that key is still secure.

(c) To construct a protocol for multi-party cloud application using the combination of the proposed symmetric and asymmetric FHE key generation algorithms.

1.6 Scope of the Study

This study is concentrated on the applied sciences, mathematical analysis and the substantial theoretical optimization of the key generation algorithms of the FHE schemes. The scope of this study is limited to:

(a) Sym-FHE uses 4- dimension Matrix ring modulo N to represent the dataset or inputs of the key generation, encryption as well as decryption algorithms.

(b) Binary-LWE FHE scheme is based on lattice-based theory and uses Big O notation to evaluate the performance.

(c) CloudSim simulation is used to evaluate the performance of the proposed MP-Protocol.

1.7 Significance of Study

In this study, the combination of the symmetric and asymmetric FHE is proposed to construct an efficient and secure homomorphic cryptosystem for cloud computing. The key generation algorithm is modified using the proposed Pick-Test method to enhance the efficiency of the Xiao *et al.* (2012) symmetric scheme. Therefore, the key generation algorithm based on the Binary-LWE lattice problem is proposed to enhance Brakerski (2012) scheme, which is a noise-based FHE using the asymmetric key. The noise is controlled using modulo switching technique. The proposed algorithms are efficient and practically feasible and are used to construct a multi-party protocol to allow many users to access and manipulate the data in the cloud.

1.8 Research Contribution

The contributions of this study are as follows:

(a) Improving the key generation algorithm of the Xiao *et al.* (2012) scheme and make it more efficient using the Pick-Test method.

(b) Improving the key generation algorithm on Brakerski (2012) FHE scheme using Binary-LWE lattice-based cryptography problem to produce minimal

key size and ensuring that key is still secure and manage the noise of the modified scheme using modulus switching technique.

(c) Construct a multi-party protocol to support cloud computing using the proposed Sym-Key and Binary-LWE FHE schemes.

1.9 Thesis Organization

Accordingly, to achieve the aforementioned objectives, this thesis is distributed within seven chapters. Chapter 2: Literature Review. This chapter presents the concepts and the background information and reviews the related works in the area of fully homomorphic encryption. This chapter reviews the previous surveys and displays the strength and gaps of the previous FHE studies. Chapter 3: Research Methodology. This chapter defines the methodology followed in this thesis to achieve the study's objectives. A methodology is general rules or principles to solve the research problems. It includes the research framework and the steps needed to progress the research systematically. It contains the discussion on the research components such as the phases, techniques, tools as well as datasets. Chapter 4: Symmetric Key Generation Algorithm of fully homomorphic encryption scheme (SYM-KEY). This chapter provides the symmetric key generation algorithm (SYM-KEY) base on the pick-test method to improve the performance. It provides the evaluation of the encryption and decryption algorithms to verify the validity of the proposed algorithm and provides the Evaluation of the Performance and security. Chapter 5: Asymmetric key generation algorithm based on Binary learning with error lattice problem (Binary-LWE). This chapter introduces the optimization method to improve the key generation algorithm using Binary learning with error problem and manage the noise using the modulo switching technique. Chapter 6: Multi-party Protocol using Sym-Key FHE and Binary-LWE FHE schemes for the cloud environment. This chapter introduces the multi-party protocol with access control based on the proposed symmetric fully homomorphic scheme (Sym-Key FHE) and Binary-LWE FHE to allow many users access and manipulate the data in the cloud. Chapter 7: Conclusion and Future Work. This chapter discusses and highlights the summary, contributions and findings of the research work, and it provides suggestions and recommendations for future studies.

REFERENCES

Ajtai, M., and Dwork, C. (1997). *A public-key cryptosystem with worst-case/average-case equivalence.* Paper presented at the STOC, 284-293.

Albrecht, M. R., Faugere, J.-C., Fitzpatrick, R., and Perret, L. (2014). *Lazy modulus switching for the BKW algorithm on LWE.* Paper presented at the International Workshop on Public Key Cryptography, 429-445.

Alperin-Sheriff, J., Ding, J., Petzoldt, A., and Smith-Tone, D. (2017). Total Break of the Fully Homomorphic Multivariate Encryption Scheme of 2017/458: Decryption can not be of low degree. *IACR Cryptology ePrint Archive, 2017*, 471.

Anderson, J. H., Kelley, E. E., and Motika, F. (2005). SECURE VOTING SYSTEM: US Patent App. 20,070/051,804.

Anderson, R., Biham, E., and Knudsen, L. (1998). Serpent: A proposal for the advanced encryption standard. *NIST AES Proposal*.

Baharon, M. R., Shi, Q., Abdollah, M. F., Yassin, S. W. M. S., and Idris, A. (2018). An Improved Fully Homomorphic Encryption Scheme for Cloud Computing. *International Journal of Communication Networks and Information Security, 10*(3), 502.

Bai, S., and Galbraith, S. D. (2014). *Lattice decoding attacks on binary LWE.* Paper presented at the Australasian Conference on Information Security and Privacy, 322-337.

Becker, A., and Laarhoven, T. (2016). *Efficient (ideal) lattice sieving using cross-polytope LSH.* Paper presented at the International Conference on Cryptology in Africa, 3-23.

Bilakanti, A., Anjana, N., Divya, A., Divya, K., Chakraborty, N., and Patra, G. (2016). *Secure computation over cloud using fully homomorphic encryption.* Paper presented at the 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), 633-636.

Boneh, D., Goh, E.-J., and Nissim, K. (2005). *Evaluating 2-DNF formulas on ciphertexts.* Paper presented at the Theory of Cryptography Conference, 325-341.

Bos, J. W., Lauter, K. E., Loftus, J., and Naehrig, M. (2013). *Improved Security for a Ring-Based Fully Homomorphic Encryption Scheme.* Paper presented at the IMA Int. Conf., 45-64.

Brakerski, Z. (2012). *Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP.* Paper presented at the CRYPTO, 868-886.

Brakerski, Z., Gentry, C., and Vaikuntanathan, V. (2014). (Leveled) fully homomorphic encryption without bootstrapping. *ACM Transactions on Computation Theory (TOCT), 6*(3), 13.

Brakerski, Z., and Vaikuntanathan, V. (2011a). *Efficient Fully Homomorphic Encryption from (Standard) LWE.* Paper presented at the LWE, FOCS 2011, IEEE 52ND ANNUAL SYMPOSIUM ON FOUNDATIONS OF COMPUTER SCIENCE, IEEE.

Brakerski, Z., and Vaikuntanathan, V. (2011b). *Fully homomorphic encryption from ring-LWE and security for key dependent messages.* Paper presented at the Annual Cryptology Conference, 505-524.

Brakerski, Z., and Vaikuntanathan, V. (2014). *Lattice-based FHE as secure as PKE.* Paper presented at the Proceedings of the 5th conference on Innovations in theoretical computer science, 1-12.

Cai, J., and Cusick, T. (1999). *A lattice-based public-key cryptosystem*, 632-632.

Calheiros, R. N., Ranjan, R., Beloglazov, A., De Rose, C. A., and Buyya, R. (2011). CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms. *Software: Practice and experience, 41*(1), 23-50.

Chen, J. (2016). *Cloud storage third-party data security scheme based on fully homomorphic encryption.* Paper presented at the 2016 International Conference on Network and Information Systems for Computers (ICNISC), 155-159.

Chen, Z., Wang, J., Chen, L., and Song, X. (2014a). A Regev-type fully homomorphic encryption scheme using modulus switching. *The Scientific World Journal, 2014*.

Chen, Z., Wang, J., Zhang, Z., and Xinxia, S. (2014b). A fully homomorphic encryption scheme with better key size. *China Communications, 11*(9), 82-92.

Cheon, J. H., Coron, J.-S., Kim, J., Lee, M. S., Lepoint, T., Tibouchi, M., et al. (2013). *Batch fully homomorphic encryption over the integers.* Paper presented at the

Annual International Conference on the Theory and Applications of Cryptographic Techniques, 315-335.

Choi, D. (2016). A generalization of the Cauchy-Schwarz inequality. *J. Math. Inequal, 10*(4), 1009-1012.

Chunsheng, G. (2011a). Fully Homomorphic Encryption Based on Approximate Matrix GCD. *Aavailable at eprint. iacr. org/2011/645*.

Chunsheng, G. (2011b). New fully homomorphic encryption over the integers. *School of Computer Engineering, Jiangsu Teachers Univ. of Technology, 9*.

Chunsheng, G. (2012). More Practical Fully Homomorphic Encryption. *International Journal of Cloud Computing and Services Science, 1*(4), 199.

Chunsheng, G. (2013). Fully Homomorphic Encryption, Approximate Lattice Problem and LWE. *International Journal of Cloud Computing and Services Science, 2*(1), 1.

Clarkson, M. R., Chong, S., and Myers, A. C. (2008). *Civitas: Toward a secure voting system*, 354-368.

Cohen, J. D., and Fischer, M. J. (1985). *A robust and verifiable cryptographically secure election scheme*: Yale University. Department of Computer Science.

Cohn, H., and Heninger, N. (2013). Approximate common divisors via lattices. *The Open Book Series, 1*(1), 271-293.

Cormen, T. H. (2009). *Introduction to algorithms*: MIT press.

Coron, J.-S., Mandal, A., Naccache, D., and Tibouchi, M. (2011). *Fully homomorphic encryption over the integers with shorter public keys.* Paper presented at the Annual Cryptology Conference, 487-504.

Damgard, I., and Jurik, M. (2001). *A generalisation, a simplification and some applications of Paillier's probabilistic public-key system.* Paper presented at the Public Key Cryptography, 119-136.

Dara, S. (2014). Multi-user protocols with access control for computational privacy in public clouds. *arXiv preprint arXiv:1406.1823*.

De Lagrange, J. L. (1773). Recherches d'arithmétique. *Nouveaux Mémoires de l'Académie de Berlin*.

Dhote, C. (2016). Homomorphic encryption for security of cloud data. *Procedia Computer Science, 79*, 175-181.

ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE transactions on information theory, 31*(4), 469-472.

Fan, J., and Vercauteren, F. (2012). Somewhat Practical Fully Homomorphic Encryption. *IACR Cryptology ePrint Archive, 2012*, 144.

Farooq, A., and Hamid, K. (2010). An efficient and simple Algorithm for matrix inversion. *International Journal of Technology Diffusion (IJTD), 1*(1), 20-27.

Gai, K., Qiu, M., Li, Y., and Liu, X.-Y. (2017). *Advanced fully homomorphic encryption scheme over real numbers.* Paper presented at the Cyber Security and Cloud Computing (CSCloud), 2017 IEEE 4th International Conference on, 64-69.

Gauss, C. F. (1801). Disquisitiones arithmeticae, trans. Arthur A. Clarke: New Haven: Yale University Press.

Gentry, C. (2009). *Fully homomorphic encryption using ideal lattices.* Paper presented at the STOC, 169-178.

Gentry, C., and Halevi, S. (2011). *Fully homomorphic encryption without squashing using depth-3 arithmetic circuits.* Paper presented at the Foundations of Computer Science (FOCS), 2011 IEEE 52nd Annual Symposium on, 107-109.

Gentry, C., Halevi, S., and Smart, N. P. (2012). *Better bootstrapping in fully homomorphic encryption.* Paper presented at the International Workshop on Public Key Cryptography, 1-16.

Gentry, C., Sahai, A., and Waters, B. (2013). Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In *Advances in Cryptology–CRYPTO 2013* (pp. 75-92): Springer.

Gentry, C., and Szydlo, M. (2002). *Cryptanalysis of the revised NTRU signature scheme*, 299-320.

Gjøsteen, K., and Strand, M. (2016). Fully homomorphic encryption must be fat or ugly? *IACR Cryptology ePrint Archive, 2016*, 105.

Goldreich, O., Goldwasser, S., and Halevi, S. (1997). Public-key cryptosystems from lattice reduction problems. *Advances in Cryptology—CRYPTO'97*, 112-131.

Goldwasser, S., and Micali, S. (1984). Probabilistic encryption. *Journal of computer and system sciences, 28*(2), 270-299.

Gompf, R. E., Stipsicz, A. I., and Stipsicz, A. (1999). *4-manifolds and Kirby calculus*: American Mathematical Soc.

Goyal, T., Singh, A., and Agrawal, A. (2012). Cloudsim: simulator for cloud computing infrastructure and modeling. *Procedia Engineering, 38*, 3566-3572.

Gupta, D. S., and Biswas, G. (2018). On Securing Cloud Storage Using a Homomorphic Framework. In *Technology Management in Organizational and Societal Contexts* (pp. 99-114): IGI Global.

Hoffstein, J., Howgrave-Graham, N., Pipher, J., Silverman, J. H., and Whyte, W. (2003). *NTRUSIGN: Digital signatures using the NTRU lattice*, 122-140.

Hoffstein, J., Pipher, J., and Silverman, J. (1998). NTRU: A ring-based public key cryptosystem. *Algorithmic number theory*, 267-288.

Hoffstein, J., Pipher, J., and Silverman, J. H. (2014). Lattices and cryptography. In *An Introduction to Mathematical Cryptography* (pp. 373-470): Springer.

Jabbar, I., and Najim, S. (2016). Using fully homomorphic encryption to secure cloud computing. *Internet of Things and Cloud Computing, 4*(2), 13-18.

Jain, A., Rasmussen, P. M., and Sahai, A. (2017). Threshold Fully Homomorphic Encryption. *IACR Cryptology ePrint Archive, 2017*, 257.

Jin, X., Krishnan, R., and Sandhu, R. (2012). *A unified attribute-based access control model covering DAC, MAC and RBAC.* Paper presented at the IFIP Annual Conference on Data and Applications Security and Privacy, 41-55.

Kawachi, A., Tanaka, K., and Xagawa, K. (2007). Multi-bit cryptosystems based on lattice problems. *Public Key Cryptography–PKC 2007*, 315-329.

Kawamura, S., Shimbo, A., and Takabayashi, K. (1991). Server-aided computation method and distributed information processing unit: Google Patents.

Kim, J., Lee, M. S., Yun, A., and Cheon, J. H. (2013). CRT-based Fully Homomorphic Encryption over the Integers. *IACR Cryptology ePrint Archive, 2013*, 57.

Kipnis, A., and Hibshoosh, E. (2012). Efficient Methods for Practical Fully Homomorphic Symmetric-key Encrypton, Randomization and Verification. *IACR Cryptology ePrint Archive, 2012*, 637.

Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of computation, 48*(177), 203-209.

Kohno, T., Stubblefield, A., Rubin, A. D., and Wallach, D. S. (2004). *Analysis of an electronic voting system*, 27-40.

Korkin, A., and Zolotarev, E. (1873). Surun certainminimum, Nouv. *Ann. Math. Ser, 2*(12), 337-355.

Kummert, H. (1998). The PPP Triple-DES Encryption Protocol (3DESE).

Kushilevitz, E., and Ostrovsky, R. (1997). *Replication is not needed: Single database, computationally-private information retrieval.* Paper presented at the

Proceedings 38th Annual Symposium on Foundations of Computer Science, 364-373.

Li, J., Song, D., Chen, S., and Lu, X. (2012). *A simple fully homomorphic encryption scheme available in cloud computing.* Paper presented at the 2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems, 214-217.

Li, J., and Wang, L. (2015). Noise-free Symmetric Fully Homomorphic Encryption based on noncommutative rings. *IACR Cryptology ePrint Archive, 2015*, 641.

Li, T., Huang, Z., Li, P., Liu, Z., and Jia, C. (2018). Outsourced privacy-preserving classification service over encrypted data. *Journal of Network and Computer Applications*.

Lin, M. C. J., and Lin, Y. L. (2000). *A VLSI implementation of the blowfish encryption/decryption algorithm*, 1-2.

Lindner, R., and Peikert, C. (2011). *Better Key Sizes (and Attacks) for LWE-Based Encryption.* Paper presented at the CT-RSA, 319-339.

Liu, Z., Pöppelmann, T., Oder, T., Seo, H., Roy, S. S., Güneysu, T., et al. (2017). High-Performance Ideal Lattice-Based Cryptography on 8-Bit AVR Microcontrollers. *ACM Transactions on Embedded Computing Systems (TECS), 16*(4), 117.

Long, W., Yuqing, L., and Qingxin, X. (2013). *Using cloudsim to model and simulate cloud computing environment.* Paper presented at the 2013 Ninth International Conference on Computational Intelligence and Security, 323-328.

Longa, P., and Naehrig, M. (2016). *Speeding up the number theoretic transform for faster ideal lattice-based cryptography.* Paper presented at the International Conference on Cryptology and Network Security, 124-139.

Lu, C. C., and Tseng, S. Y. (2002). Integrated design of AES (advanced encryption standard) encrypter and decrypter.

Lyubashevsky, V., Peikert, C., and Regev, O. (2010). On ideal lattices and learning with errors over rings. *Advances in Cryptology–EUROCRYPT 2010*, 1-23.

Malhotra, R., and Jain, P. (2013). Study and comparison of various cloud simulators available in the cloud computing. *International Journal, 3*(9).

Marshall, C., and Naffah, R. S. (2003). Programming with GNU Crypto. *Free Software Foundation*.

Martins, P., Sousa, L., and Mariano, A. (2018). A survey on fully homomorphic encryption: An engineering perspective. *ACM Computing Surveys (CSUR), 50*(6), 83.

May, A. (2002). Cryptanalysis of unbalanced RSA with small CRT-exponent. *Advances in Cryptology—CRYPTO 2002*, 221-244.

Melchor, C. A., Gaborit, P., and Herranz, J. (2010). *Additively Homomorphic Encryption with d-Operand Multiplications.* Paper presented at the CRYPTO, 138-154.

Mell, P., and Grance, T. (2011). The NIST definition of cloud computing.

Merkle, R., and Hellman, M. (1978). Hiding information and signatures in trapdoor knapsacks. *Information Theory, IEEE Transactions on, 24*(5), 525-530.

Meshram, C. (2015). An efficient ID-based cryptographic encryption based on discrete logarithm problem and integer factorization problem. *Information Processing Letters, 115*(2), 351-358.

Micciancio, D. (2001). Improving lattice based cryptosystems using the Hermite normal form. *Cryptography and Lattices*, 126-145.

Micciancio, D., and Peikert, C. (2013). Hardness of SIS and LWE with small parameters. In *Advances in Cryptology–CRYPTO 2013* (pp. 21-39): Springer.

Michalski, A., Gaj, K., and El-Ghazawi, T. (2003). *An implementation comparison of an IDEA encryption cryptosystem on two general-purpose reconfigurable computers*, 204-219.

Miller, V. S. (1985). *Use of elliptic curves in cryptography.* Paper presented at the Conference on the Theory and Application of Cryptographic Techniques, 417-426.

Mirza, F., and Murphy, S. (1999). *An observation on the key schedule of Twofish*, 151-154.

Moore, C., O'Neill, M., O'Sullivan, E., Doröz, Y., and Sunar, B. (2014). *Practical homomorphic encryption: A survey.* Paper presented at the 2014 IEEE International Symposium on Circuits and Systems (ISCAS), 2792-2795.

Mousa, A., and Hamad, A. (2006). Evaluation of the RC4 Algorithm for Data Encryption. *International Journal of Computer Science & Applications, 3*(2), 44-56.

Naccache, D., and Stern, J. (1997). *A new public-key cryptosystem.* Paper presented at the International Conference on the Theory and Applications of Cryptographic Techniques, 27-36.

Nakajima, C. H., and Ohzeki, M. (2016). Statistical Mechanical Models of Integer Factorization Problem. *Journal of the Physical Society of Japan, 86*(1), 014001.

Naor, M., and Yung, M. (1990). *Public-key cryptosystems provably secure against chosen ciphertext attacks.* Paper presented at the Proceedings of the twenty-second annual ACM symposium on Theory of computing, 427-437.

Neumann, O. (2005). Carl Friedrich Gauss, Disquisitiones Arithmeticae (1801). *Landmark Writings in Western Mathematics, 1640–1940*, 303-315.

Newman, D. J. (1980). Simple analytic proof of the prime number theorem. *The American Mathematical Monthly, 87*(9), 693-696.

Nguyen, P. (1999). *Cryptanalysis of the goldreich-goldwasser-halevi cryptosystem from crypto'97*, 790-790.

Nuida, K., Itakura, N., and Kurosawa, K. (2015). *A simple and improved algorithm for integer factorization with implicit hints.* Paper presented at the Cryptographers' Track at the RSA Conference, 258-269.

Ogura, N., Yamamoto, G., Kobayashi, T., and Uchiyama, S. (2010). *An improvement of key generation algorithm for Gentry's homomorphic encryption scheme.* Paper presented at the International Workshop on Security, 70-83.

Okamoto, T., and Uchiyama, S. (1998). A new public-key cryptosystem as secure as factoring. *Advances in Cryptology—EUROCRYPT'98*, 308-318.

Paillier, P. (1999). *Public-key cryptosystems based on composite degree residuosity classes*, 223-238.

Regev, O. (2004). New lattice-based cryptographic constructions. *Journal of the ACM (JACM), 51*(6), 899-942.

Regev, O. (2005). *On Lattices, Learning with Errors, Random Linear Codes, and Cryptography.* Paper presented at the In STOC.

Regev, O. (2009). On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM), 56*(6), 34.

Rivest, R. L., Shamir, A., and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM, 21*(2), 120-126.

Rothblum, R. (2011). *Homomorphic Encryption: From Private-Key to Public-Key.* Paper presented at the TCC, 219-234.

Sander, T., Young, A., and Yung, M. (1999). *Non-interactive cryptocomputing for NC/sup 1*. Paper presented at the Foundations of Computer Science, 1999. 40th Annual Symposium on, 554-566.

Sha, P., and Zhu, Z. (2016). *The modification of RSA algorithm to adapt fully homomorphic encryption algorithm in cloud computing.* Paper presented at the 2016 4th International Conference on Cloud Computing and Intelligence Systems (CCIS), 388-392.

Shan, D., Du, X., Wang, W., and Wang, N. (2018). *A Dynamic Symmetric Fully Homomorphic Encryption Mechanism for Privacy Protection of Cooperative Precision Positioning Cloud Service.* Paper presented at the 2018 International Conference on Computer Science, Electronics and Communication Engineering (CSECE 2018).

Smart, N., and Vercauteren, F. (2010). Fully homomorphic encryption with relatively small key and ciphertext sizes. *Public Key Cryptography–PKC 2010*, 420-443.

Smart, N. P., and Vercauteren, F. (2014). Fully homomorphic SIMD operations. *Designs, codes and cryptography*, 1-25.

Standard, D. E. (1977). Federal Information Processing Standards Publication 46, National Bureau of Standards, Washington, D. *C, January*, *15*.

Standard, N.-F. (2001). Announcing the advanced encryption standard (AES). *Federal Information Processing Standards Publication, 197*, 1-51.

Stehlé, D., and Steinfeld, R. (2010). *Faster fully homomorphic encryption.* Paper presented at the International Conference on the Theory and Application of Cryptology and Information Security, 377-394.

Stehlé, D., Steinfeld, R., Tanaka, K., and Xagawa, K. (2009). Efficient public key encryption based on ideal lattices. *Advances in Cryptology–ASIACRYPT 2009*, 617-635.

Strang, G. (1993). *Introduction to linear algebra* (Vol. 3): Wellesley-Cambridge Press Wellesley, MA.

Sun, X., Zhang, P., Sookhak, M., Yu, J., and Xie, W. (2017). Utilizing fully homomorphic encryption to implement secure medical computation in smart cities. *Personal and Ubiquitous Computing, 21*(5), 831-839.

Sun, Z., Zhang, T., Zheng, X., Yang, L., and Peng, L. (2018). *A Method for Solving Generalized Implicit Factorization Problem.* Paper presented at the International Conference On Signal And Information Processing, Networking And Computers, 284-290.

Takagi, T., and Schmidt-Samoa, K. (2005). Paillier's Cryptosystem Modulo p2q and its Applications to Trapdoor Commitment Scheme.

Tamayo-Rios, M., Faugère, J.-C., Perret, L., How, P. H., and Zhang, R. (2017). Fully Homomorphic Encryption Using Multivariate Polynomials. *IACR Eprint*, *458*.

Van Dijk, M., Gentry, C., Halevi, S., and Vaikuntanathan, V. (2010a). *Fully homomorphic encryption over the integers.* Paper presented at the Annual International Conference on the Theory and Applications of Cryptographic Techniques, 24-43.

Van Dijk, M., Gentry, C., Halevi, S., and Vaikuntanathan, V. (2010b). Fully homomorphic encryption over the integers. *Advances in Cryptology–EUROCRYPT 2010*, 24-43.

Wang, D., Guo, B., Shen, Y., Cheng, S.-J., and Lin, Y.-H. (2017). *A faster fully homomorphic encryption scheme in big data.* Paper presented at the Big Data Analysis (ICBDA), 2017 IEEE 2nd International Conference on, 345-349.

Wang, Y. (2015). Notes on Two Fully Homomorphic Encryption Schemes Without Bootstrapping. *IACR Cryptology ePrint Archive, 2015*, 519.

Wang, Y. (2016). Octonion Algebra and Noise-Free Fully Homomorphic Encryption (FHE) Schemes. *IACR Cryptology ePrint Archive, 2016*, 68.

Xiao, L., Bastani, O., and Yen, I.-L. (2012). An Efficient Homomorphic Encryption Protocol for Multi-User Systems. *IACR Cryptology ePrint Archive, 2012*, 193.

Yagisawa, M. (2015a). Fully Homomorphic Encryption on Octonion Ring. *IACR Cryptology ePrint Archive, 2015*, 733.

Yagisawa, M. (2015b). Fully Homomorphic Encryption without bootstrapping. *IACR Cryptology ePrint Archive, 2015*, 474.

Yagisawa, M. (2016a). Fully Homomorphic Public-key Encryption Based on Discrete Logarithm Problem. *IACR Cryptology ePrint Archive, 2016*, 54.

Yagisawa, M. (2016b). Improved Fully Homomorphic Encryption with Composite Number Modulus. *IACR Cryptology ePrint Archive, 2016*, 50.

Yasuda, M., Shimoyama, T., Kogure, J., and Izu, T. (2016). Computational hardness of IFP and ECDLP. *Applicable Algebra in Engineering, Communication and Computing, 27*(6), 493-521.

Yuan, E., and Tong, J. (2005). *Attributed based access control (ABAC) for web services.* Paper presented at the IEEE International Conference on Web Services (ICWS'05).

Zhou, T., Yang, X., Zhang, W., and Wu, L. (2016). Efficient fully homomorphic encryption with circularly secure key switching process. *International Journal of High Performance Computing and Networking, 9*(5-6), 417-422.

LIST OF PUBLICATIONS

Nagmeldin, W., and Shamsuddin, S. (2016). Multi-Party Protocol with Access Control on Symmetric Fully Homomorphic Encryption Scheme. *Journal of Theoretical & Applied Information Technology*, 88(3).