



TABLE OF CONTENTS

TABLE OF CONTENTS	III
LIST OF TABLES	VI
LIST OF FIGURES	VII
PLAGIARISM STATEMENT	VIII
ABSTRACT	IX
CHAPTER I: INTRODUCTION	1
1.1. Background	1
1.2. Problem Statement	4
1.3. Research Scope	5
1.4. Research Objectives	5
1.5. Research Benefit	5
CHAPTER II: LITERATURE REVIEW	7
CHAPTER III: THEORETICAL BASIS	9
3.1. Fully Homomorphic Encryption	9
3.1.1. Foundational mathematics	10
3.1.2. Lattice cryptography	14
3.1.3. Homomorphic encryption primitives	17
3.1.4. CKKS-Specific concepts	21
3.1.5. TFHE-Specific concepts	26
3.1.6. Scheme Switching Framework	32
3.1.7. Advanced operations	37
3.1.8. Polynomial Approximations	41
3.1.9. Security framework	44
3.2. Convolutional Neural Network	49
3.2.1. Perceptrons and multi-layer perceptrons	49
3.2.2. Activation functions	51
3.2.3. Forward propagation	52
3.2.4. Convolution-Specific concepts	53
3.2.5. Fully connected layer	54
3.2.6. Padding strategies	55
3.2.7. Stride configuration theory	56
CHAPTER IV: RESEARCH METHODOLOGY	58
4.1. Research Methodology Overview	58
4.1.1. FHE memory optimizations	60
4.1.2. FHE pre-compute reduction	61
4.1.3. FHE-DNN computations	61
4.2. Performance Evaluation	63
4.2.1. Test scenarios	63



4.2.2. Metrics	64
CHAPTER V: IMPLEMENTATION	65
5.1. Orion Framework Architecture	66
5.1.1. Core Framework Design	67
5.1.2. Backend Abstraction Layer	68
5.2. OpenFHE Backend Implementation	69
5.2.1. Scheme Initialization and Configuration	70
5.2.2. Cryptographic Context Management	72
5.2.3. Key Generation and Storage Optimization	72
5.3. Homomorphic Encryption Primitives	74
5.3.1. Encoder Implementation for CKKS	75
5.3.2. Encryptor and Decryptor Modules	76
5.3.3. Evaluator for Homomorphic Operations	78
5.3.4. Noise Management and Rescaling	79
5.4. Neural Network Layer Implementations	81
5.4.1. Fully Connected Layer Operations	81
5.4.2. Convolutional Layer Implementation	83
5.4.3. Activation Function Implementations	85
5.4.4. Pooling Operations	86
5.5. Scheme Switching Framework	87
5.5.1. CKKS and TFHE Conversion Protocol	87
5.5.2. Linear Transform Evaluator	89
5.6. Polynomial Evaluation System	91
5.6.1. Minimax Approximation for Nonlinear Functions	92
5.7. Bootstrapping and Noise Management	94
5.7.1. Bootstrapper Implementation	94
5.7.2. Level Management Across Operations	96
5.8. Forward Propagation Pipeline	98
5.8.1. End-to-End Inference Workflow	98
5.8.2. Layer-by-Layer Processing	100
CHAPTER VI: RESULTS AND DISCUSSION	102
6.1. Network Architecture	102
6.2. Performance Evaluation	103
6.2.1. Time Overhead	104
6.2.2. Memory Overhead	105
6.2.3. Accuracy Analysis	106
6.3. Comparing Activation Function Methods	108
6.3.1. Approximated ReLU vs. Scheme-Switched ReLU	108
6.3.2. Precision Analysis of ReLU	110
6.4. Implementation Contributions	111



6.4.1 Inherited from Original Orion Framework	111
6.4.2 Inherited from Original Orion Framework	112
CHAPTER VII CONCLUSION AND FUTURE WORK	113
7.1. Conclusion	113
7.2. Future Work	113
APPENDIX	115
A. Mathematical Symbol Reference Guide	115
A.1. Set Theory & Number Systems	115
A.2. Operators & Operations	115
A.3. Greek Letters	116
A.4. Ring & Field Theory	117
A.5. Matrices & Vectors	117
REFERENCES	118



LIST OF TABLES

Table 4.2 - Test Scenarios	64
Table 4.3 - Metrics	64
Table 6.1 - MAE and bit precision between ReLU methods	106
Table 6.2 - Accepted ranges of each ReLU method	109
Table 6.3 - Multiplicative Depth, MAE and bit precision between methods	110



LIST OF FIGURES

Figure 3.1 - Data privacy in cloud computation	9
Figure 3.2 - Data privacy in cloud computation with FHE	10
Figure 3.3 - NNT example for $p=5$, $a=2$, and $N=4$	11
Figure 4.1 - Overview of FHE CNN inference	58
Figure 4.2 - Overview of FHE CNN training	59
Figure 4.3 - The diagonal method	62
Figure 4.4 - Packed SISO method and its analogous Toeplitz matrix example	62
Figure 5.1 - Orion Framework High-Level Architecture	66
Figure 5.2 - Orion Core Framework Directory Structure	67
Figure 5.3 - Orion Backend Abstraction Layer Architecture	68
Figure 6.1 - Time overhead between approx. and s. switching ReLU model	104
Figure 6.2 - Visualizing approximation and s. switching activation functions	108