

TABLE OF CONTENTS

ABSTRACT	4
PLAGIARISM STATEMENT	5
CHAPTER I INTRODUCTION	6
1.1. Background	6
1.2. Problem Statement	9
1.3. Research Scope	9
1.4. Research Objectives	10
1.5. Research Benefits	10
CHAPTER II LITERATURE REVIEW	12
CHAPTER III THEORETICAL BASIS	17
3.1. Fully Homomorphic Encryption	17
3.1.1. FHE operations and schemes	19
3.1.2. Stages in FHE	21
3.1.3. Matrix Multiplication in FHE	23
3.2. Counter Mode Encryption (CTR)	24
3.2.1. Counter Mode Memory Encryption	26
3.3. Message Authentication Codes	27
3.3.1 Hash-based Message Authentication Code	28
3.4. Merkle Trees	29
3.4.1. Memory Integrity Verification via Merkle Trees	31
3.4.2. Memory Integrity Verification via Bonsai Merkle Trees	32
3.5. Trusted Execution Environments	34
3.6. Keystone Enclave	35
3.6.1 RISC-V Physical Memory Protection	36
3.6.2. Memory Isolation in Keystone	36
3.7. gem5	39
3.8. T2 Benchmark Suite	40
3.9. Execution time	40
CHAPTER IV RESEARCH METHODOLOGY	42
4.1. Research Methodology Overview	42
4.2. gem5 Environment Setup	43
4.3. Memory Integrity Verification Implementation	43
4.4. Memory Controller Integration	45
4.4.1. Read Path	45
4.4.2. Write Path	48
4.5. Performance Evaluation	49
4.5.1. Experimental Setup	50
4.5.2. Benchmark Workload Characteristics	51
4.5.3. Test Scenarios	52



4.5.4. Metric	52
CHAPTER V IMPLEMENTATION	53
5.1. gem5 Environment Setup Implementation	53
5.2. Bonsai Merkle Tree Implementation	54
5.2.1 Cryptographic Primitives Implementation	55
A. SHA-256 Hash Function Implementation	55
B. HMAC Message Authentication Implementation	58
5.2.2 BMT Data Structures and Tree Construction	61
A. Tree Dimension Calculation and Memory Layout	61
B. Tree Node Structure and Physical Memory Integration	63
5.2.3 Integrity Verification and Update Operations	64
A. Block Integrity Verification Process	65
B. Block Update and Tree Maintenance Process	68
5.3. Memory System Integration Implementation	72
5.3.1 AbstractMemory Access Path Modifications	73
A. Enhanced Memory Access Processing	73
B. Read Path Integration with Integrity Verification and Fault Detection	74
C. Write Path Integration with Tree Updates	75
5.3.2 Memory Controller Secure Root Management	77
A. Secure Root Storage Implementation	77
B. Root Hash Management Interface	78
C. AbstractMemory-Memory Controller Connection Establishment	79
5.3.3 Timing and Latency Modeling	80
A. BMT Verification Latency Calculation	80
B. BMT Update Latency Modeling	81
C. Memory Encryption Latency Modeling	81
CHAPTER VI RESULTS AND DISCUSSION	83
6.1. Baseline Performance Analysis	83
6.2. BMT Integrity Protection Performance	85
CHAPTER VII CONCLUSION AND FUTURE WORK	90
7.1. Conclusion	90
7.2. Future Work	91
REFERENCES	93
GLOSSARY	98