Contents

1 Introduction 1
- 1.1 Introduction 1
- 1.2 Literature Review 1
- 1.3 Aim of the Project 2
- 1.4 Discussion 3

2 Background of the Work 4
- 2.1 Introduction 4
- 2.2 Theoretical Background of Threshold Cryptography 4
  - 2.2.1 Secret Sharing Scheme 4
  - 2.2.2 Function Sharing Scheme 5
- 2.3 Characteristics of Threshold Cryptography 5
- 2.4 Theoretical Background of Cellular Automata 6
  - 2.4.1 Different types of sequences produced by 3-NCA 7
  - 2.4.2 Sparse Matrix 9
- 2.5 Discussion 9

3 Related Work 10
- 3.1 Introduction 10
- 3.2 Existing Approaches 10
- 3.3 Discussion 12

4 Architecture of the proposed work 13
- 4.1 Introduction 13
- 4.2 Proposed Scheme 13
  - 4.2.1 Creation of Shared Secret 14
  - 4.2.2 Secret Reconstruction 14
  - 4.2.3 Algorithm 14
- 4.3 Placement of a rule in Sparse Matrix 17
  - 4.3.1 Generation of rules 17
  - 4.3.2 Rule Placement 18
- 4.4 Discussion 19

5 Effectiveness of the proposed algorithm 20
5.1 Introduction 20
5.2 Efficiency 20
5.3 Scalability 20
5.4 Correctness 21
5.5 Secret reconstruction with incorrect or unauthorized subset($< k$) of correct shares 21
5.6 Discussion 22

6 Applications of CellTCS 23
6.1 Introduction 23
6.1.1 Multi-party computation protocol 23
6.1.2 Group-oriented cryptographic application 23
6.1.3 Visual cryptography 24
6.1.4 Fault Tolerant Network 24
6.2 Discussion 24

7 Conclusions and Future Research Directions 25

List of Figures

2.1 A Typical Cell of a CA 6
2.2 The state transition diagram of a maximum-length group CA . . 7
2.3 The state transition diagram of a non maximum-length group CA 8
2.4 Basin structure showing aperiodic behavior 8

4.1 A flow diagram of CellTCS 13

List of Tables

4.1 List of mathematical symbols 14
4.2 Truth Table 17
4.3 Using XOR gate 18
4.4 Using NAND gate 18