Contents

1 Introduction **1**

1.1 Research background and significance 1

1.2 State-of-the-art of chaos-based cryptography 2

1.3 About the dissertation 4

2 CML and Spatiotemporal Chaos **7**

2.1 Introduction 7

2.2 A spatiotemporal chaotic system 8

2.3 Li-Yorke chaos and Marotto theorem 8

2.4 Li-Yorke chaos in a CML 11

3 Chaotification of CML **17**

3.1 Introduction 17

3.2 Chaofitication: background and algorithms 18

3.3 Chaotification algorithm designed for a CML 19

3.4 Devaney chaos in the controlled CML 22

3.5 Simulations 23

4 Multiple-Output Pseudo-Random-Bit Generators **28**

4.1 Introduction 28

4.2 State-of-the-art of chaos-based PRBGs 29

4.2.1 Chaotic maps 29

4.2.2 Digitization methods 29

4.2.3 Configurations 30

4.2.4 Analysis of PRBGs' properties 31

4.2.5 Techniques for improving PRBGs' properties 31

4.3 Design of a multiple-output PRBG based on a CML 32

4.4 Properties of the PRBG 33

4.4.1 Dynamical properties of the CML 33

4.4.2 Random-like statistical properties 36

4.5 PRBGs based on various CMLs 37

4.5.1 Statistical properties of the PRBGs 38

4.5.2 Comparison of PRBGs based on various CMLs 42

5 Stream Cipher Based on CML **45**

5.1 Introduction 45

5.2 Design a CML-based stream cipher 46

5.2.1 Algorithm of the cipher 46

5.2.2 Keyspace 47

5.3 Cryptographic properties of the keystream 48

5.3.1 Probability distribution . . . 48
5.3.2 Run . . . 49
5.3.3 Auto-correlation . . . 49
5.3.4 Statistical tests . . . 50
5.4 Security Analysis . . . 51
5.4.1 Confusion and diffusion . . . 51
5.4.2 Error function attack . . . 52
5.4.3 Differential attack . . . 52
5.4.4 Known-plaintext attack . . . 53
5.4.5 Chosen-plaintext/ciphertext attack . . . 53
5.5 High Efficiency . . . 54
5.6 Discussion . . . 55

6 CML-based Multimedia Cryptosystems 57
6.1 Introduction . . . 57
6.2 CML-based multimedia cryptosystem . . . 59
6.2.1 EPP communication between PC and FPGA . . . 59
6.2.2 FPGA implementation of the CML-based cipher . . . 61
6.2.3 The cryptosystem with EPP communication . . . 64
6.2.4 User interface . . . 65
6.2.5 Profile of the cryptosystem . . . 65
6.3 Performance analysis . . . 69
6.3.1 Properties of the cryptosystem . . . 69
6.3.2 Effect of encrypting multimedia . . . 72
6.4 Secure CML-based video conferencing system . . . 78
6.4.1 A video encryption algorithm based on a CML . . . 78
6.4.2 The real-time video conferencing system . . . 80
6.4.3 Performance of the video conferencing system . . . 80

7 Conclusion 82

References 85