
Contents

1 Cryptography and Cryptanalysis Through Computational Intelligence

<i>E.C. Laskari, G.C. Meletiou, Y.C. Stamatiou, M.N. Vrahatis</i>	1
1.1 Introduction	2
1.1.1 Block ciphers	2
1.1.2 Public key cryptographic schemes	5
1.1.3 Elliptic Curve based cryptosystems	7
1.2 Computational Intelligence Background and Methods	8
1.2.1 Evolutionary Computation	8
1.2.2 Artificial Neural Networks	13
1.2.3 Fuzzy systems	15
1.3 Review of Cryptography and Cryptanalysis Through Computational Intelligence	16
1.4 Applying Computational Intelligence in Cryptanalysis	18
1.4.1 Cryptanalysis as Discrete Optimization Task	18
1.4.2 Cryptanalysis of Feistel Ciphers through Evolutionary Computation Methods	23
1.4.3 Utilizing Artificial Neural Networks to Address Cryptographic Problems	31
1.4.4 Artificial Neural Networks Applied on Problems Related to Elliptic Curve Cryptography	34
1.5 Ridge Polynomial Networks for Cryptography	37
1.6 Summary	42
References	43

2 Multimedia Content Protection Based on Chaotic Neural Networks

<i>Shiguo Lian</i>	51
2.1 Introduction	52
2.2 Chaotic neural networks' generation and properties	54
2.2.1 Chaotic neural network's generation	54

2.2.2	Chaotic neural network's properties suitable for data encryption	55
2.3	Multimedia content encryption based on chaotic neural networks .	59
2.3.1	Introduction to multimedia content encryption	59
2.3.2	The cipher based on chaotic neural network	60
2.3.3	Selective video encryption based on Advanced Video Coding .	64
2.4	Multimedia content authentication based on chaotic neural networks	66
2.4.1	Introduction to multimedia content authentication	66
2.4.2	The hash function based on chaotic neural network	67
2.4.3	The proposed image authentication scheme	69
2.4.4	Performance analysis	70
2.5	Future work and discussions	73
2.6	Conclusions	74
2.7	Acknowledgements	75
	References	75

3 Evolutionary Regular Substitution Boxes

	<i>Nadia Nedjah, Luiza de Macedo Mourelle</i>	79
3.1	Introduction	79
3.2	Preliminaries for Substitution Boxes	80
3.3	Nash Equilibrium-based Evolutionary Algorithms	82
3.4	Evolving Resilient S-Boxes	82
3.4.1	S-Box encoding and genetic operators	83
3.4.2	S-Box evaluation	84
3.5	Performance Results	87
3.6	Conclusion	88
	References	88

4 Industrial Applications Using Wavelet Packets for Gross Error Detection

	<i>Paolo Mercorelli, Alexander Frick</i>	89
4.1	Introduction	90
4.1.1	Modules	91
4.1.2	Gross Error Types and Examples	93
4.2	Problem Specification	95
4.2.1	Mathematical Preliminary	95
4.2.2	Noise Level Detection Problem (NLDP) and Algorithm (NLDA)	97
4.2.3	Some Remarks Regarding Wavelet Based Algorithms	97
4.3	Wavelet Based Noise Level Determination	97
4.3.1	Background and State of the Art	98
4.3.2	Noise Level Estimation: State of the Art	99
4.3.3	The Proposed New Procedure for Peak-Noise Level Detection .	100
4.3.4	Validation of Peak Noise Level Estimation	103

4.4	The Wavelet Algorithm for GEDR	106
4.4.1	Validation and Simulations	109
4.4.2	Outlier Detection Algorithm: MAD Algorithm	110
4.5	Results	111
4.5.1	Algorithm Parameterization	114
4.6	Experimental Data Sources	116
4.6.1	Dryer, Distillation and Mining Data with Outliers	118
4.6.2	Artificially Contaminated Data and Off-line, On-line Mode ..	122
4.7	Summary, Conclusions and Outlook	125
	References	126

5 Immune-inspired Algorithm for Anomaly Detection

	<i>Ki-Won Yeom</i>	129
5.1	Introduction	129
5.2	Background	131
5.2.1	The Danger Theory	131
5.2.2	Dendritic Cells as Initiator of Primary Immune Response ...	133
5.3	IDS based on Danger Theory and DCs Properties	136
5.3.1	Properties of DCs for IDS	136
5.3.2	Abstraction of Anomaly Detection Algorithm	138
5.4	DCs based Implementation of Practical Applications	141
5.4.1	A Detection of DoM Attack	142
5.4.2	Experiments and Results	145
5.4.3	A Detection of Port Scan Attack	147
5.4.4	Experiments and Results	149
5.5	Conclusion	153
	References	153

6 How to Efficiently Process Uncertainty within a Cyberinfrastructure without Sacrificing Privacy and Confidentiality

	<i>Luc Longpré, Vladik Kreinovich</i>	155
6.1	Cyberinfrastructure and Web Services	155
6.1.1	Practical Problem	155
6.1.2	Centralization of Computational Resources	156
6.1.3	Cyberinfrastructure	156
6.1.4	What Is Cyberinfrastructure: The Official NSF Definition ...	157
6.1.5	Web Services: What They Do – A Brief Summary	157
6.2	Processing Uncertainty Within a Cyberinfrastructure	158
6.2.1	Formulation of the problem	158
6.2.2	Description of uncertainty: general formulas	160
6.2.3	Error Estimation for the Results of Data Processing	162
6.2.4	How This Problem Is Solved Now	162
6.3	Need for Privacy Makes the Problem More Complex	162
6.4	Solution for Statistical Setting: Monte-Carlo Simulations	164

XII Contents

6.5	Solution for Interval and Fuzzy Setting	165
6.6	Summary	169
	References	170

7 Fingerprint Recognition Using a Hierarchical Approach

	<i>Chengfeng Wang, Yuan Luo, Marina L. Gavrilova and Jon Rokne</i>	175
7.1	Introduction	175
7.2	Coarse Fingerprint Matching	179
	7.2.1 Fingerprint Foreground Segmentation	180
	7.2.2 Singular Points Extraction	181
	7.2.3 Singular Points Matching	185
7.3	Topology-based Fine Matching	185
	7.3.1 Delaunay Triangulation of Minutiae Set	188
	7.3.2 Modeling Fingerprint Deformation	190
	7.3.3 Maximum Bipartite Matching	192
7.4	Experimental Results	194
7.5	Conclusions	197
	References	198

8 Smart Card Security

	<i>Kostas Markantonakis, Keith Mayes, Michael Tunstall, Damien Sauveron and Fred Piper</i>	201
8.1	Introduction	201
8.2	Smart Card Specific Attacks	203
	8.2.1 Side Channel Attacks	203
	8.2.2 Fault Attacks	209
8.3	Smart Card Platform Security	214
	8.3.1 The Evolution of Smart Card Platforms	214
	8.3.2 The Different Multi-application smart card Platforms	215
	8.3.3 Java Card	217
	8.3.4 Java Card Security	219
8.4	GSM and 3G Security	221
	8.4.1 1G - TACS	222
	8.4.2 2G - GSM	222
	8.4.3 3G - UMTS	226
8.5	Summary	228
	References	229

9 Governance of Information Security: New Paradigm of Security Management

	<i>Sangkyun Kim</i>	235
9.1	Introduction	236
9.2	Rise of the Governance	237
	9.2.1 Definitions of the Governance	237
	9.2.2 Implications of the Governance	238
	9.2.3 Success Factors of the Governance	239

9.3	Why the Security Management Fails	240
9.3.1	What the Security Management Can Do	240
9.3.2	What the Security Management Cannot Do	242
9.4	Governance of Corporate Security	244
9.4.1	General Frameworks for the Governance	244
9.4.2	Integrated Framework for the Governance of Corporate Security	244
9.5	Summary	251
	References	252
	Author Index	255



<http://www.springer.com/978-3-540-71077-6>

Computational Intelligence in Information Assurance
and Security

Abraham, A. (Ed.)

2007, XX, 255 p., Hardcover

ISBN: 978-3-540-71077-6