

# **Studies in Computational Intelligence**

Volume 1122

## **Series Editor**

Janusz Kacprzyk, Polish Academy of Sciences, Warsaw, Poland

The series “Studies in Computational Intelligence” (SCI) publishes new developments and advances in the various areas of computational intelligence—quickly and with a high quality. The intent is to cover the theory, applications, and design methods of computational intelligence, as embedded in the fields of engineering, computer science, physics and life sciences, as well as the methodologies behind them. The series contains monographs, lecture notes and edited volumes in computational intelligence spanning the areas of neural networks, connectionist systems, genetic algorithms, evolutionary computation, artificial intelligence, cellular automata, self-organizing systems, soft computing, fuzzy systems, and hybrid intelligent systems. Of particular value to both the contributors and the readership are the short publication timeframe and the world-wide distribution, which enable both wide and rapid dissemination of research output.

Indexed by SCOPUS, DBLP, WTI Frankfurt eG, zbMATH, SCImago.

All books published in the series are submitted for consideration in Web of Science.

Shishir Kumar Shandilya · Agni Datta ·  
Atulya K. Nagar

# A Nature-Inspired Approach to Cryptology

Shishir Kumar Shandilya  
School of Data Science and Forecasting  
Devi Ahilya University (DAVV)  
Indore, Madhya Pradesh, India

Agni Datta  
Cryptologist, SECURE—CoE  
VIT Bhopal University  
Bhopal, Madhya Pradesh, India

Atulya K. Nagar  
School of Mathematics, Computer Science  
and Engineering  
Liverpool Hope University  
Liverpool, UK

ISSN 1860-949X ISSN 1860-9503 (electronic)  
Studies in Computational Intelligence  
ISBN 978-981-99-7080-3 ISBN 978-981-99-7081-0 (eBook)  
<https://doi.org/10.1007/978-981-99-7081-0>

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2023

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd. The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Paper in this product is recyclable.

*There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files.*

*—Bruce Schneier*

*To my lifelines, Samarth and Nityaa*

*Shishir Kumar Shandilya*

*To my beloved parents, my dearest and  
irreplaceable sister, and to the one who has  
departed*

*Agni Datta*

*To Jyoti, and lovely daughters, Kopal and  
Priyel*

*Atulya K. Nagar*

# Preface

## “Scientia potentia est”

As humans, we understand that our cognitive processes and behavioural patterns are influenced by the surrounding environmental circumstances in which we reside. A wide array of natural occurrences and processes have a significant effect on and drive the field of cryptography, which pertains to the study of concealing information via various techniques. There is a significant need for research in this field due to the emergence of quantum computing and low-resource embedded systems, since both technologies pose challenges that need to be addressed. The primary objective is to develop efficient cryptographic techniques that provide data safety while optimising system resources. The field of study we are engaged in is greatly impacted by the complex patterns seen in the natural world, posing considerable obstacles for traditional cryptographic methods.

To improve cryptographic algorithms, we apply an extensive range of techniques. Using genetic algorithms, it is possible to mimic natural selection. In addition, we apply methods of swarm intelligence to simulate the group activities of social insects. We intend to establish secure and practical systems. With the development of modern society, the importance of cryptography has only grown, and it now plays a crucial role in safeguarding the digital infrastructure of today. As a consequence, we examine how unconventional computing and cryptography may be implemented in the real world.

Following the pandemic, we altered the paradigm by integrating cutting-edge technology into cyber defences. Cybercriminals, despite technological safeguards, are developing new and sophisticated methods of attack, necessitating an adaptable security system. A novel approach to cybersecurity challenges draws inspiration from the natural world. The primary objective of the Nature-inspired Cyber Security (NICS) framework is to design and construct a robust security system that can withstand covert attacks.

To this end, research has focused on developing a network intrusion detection system (NIDS) that imitates nature’s strategies. This text provides an overview of

cryptography with an emphasis on algorithms inspired by the natural world. The primary focus of our book is cryptography's mathematical foundations. Our exhaustive evaluation of the utility of each cryptographic technology also distinguishes us. In light of current research and evolving theoretical frameworks, we acknowledge that it is impossible to include all in-use algorithms. Due to the scope of the topic and the rapidity of its development, a thorough analysis was beyond the scope of this text.

However, it is important to keep in mind that this book's scope is not intended to be exhaustive. This book seeks to educate its readers about cryptography from a theoretical rather than practical standpoint. Due to the novelty of the subject matter and its limited industrial application, the book concentrates on fundamental and theoretical techniques. Consequently, the emphasis of the research is on these theoretical and foundational components. While numerous language libraries and implementations support well-known algorithms such as RSA and DSA, the methods presented below are frequently not as well supported or adapted.

In consequence, the book adopts a theoretical and fundamental stance, describing avenues for future research. Each chapter utilises mathematical rigour to enhance readers' comprehension. These models clarify concepts and investigate the cryptographic implications of the current topics. Since comprehending cryptography and its algorithms requires a strong mathematical background, we employ a formal, mathematical approach to explain and define the issue.

We examined a wide range of currently researched cryptographic techniques that draw inspiration from natural phenomena. This textbook provides a comprehensive understanding of the advantages and disadvantages of various methods by investigating their mathematical and computational foundations. This textbook offers a valuable opportunity for individuals interested in the fields of cryptology, academic research, and cybersecurity to enhance their knowledge of cryptography and derive inspiration from natural phenomena.

The presented work is intended to help the reader understand the potential effects of this subject matter within the field of cybersecurity. To participate intelligently in debates on these topics, an in-depth knowledge of number theory, machine learning, and applied cryptography will be advantageous, since a solid foundation in mathematics and computer science will make it a lot simpler for them to understand and interact with the subject matter at hand.

The book also examines the emerging field of nature-inspired cybersecurity and predicts that it will significantly impact security in the near future. Researchers are attempting to enhance information security by employing strategies inspired by natural defensive systems. The book's inclusion of additional reading material enhances this concept.

The objective of this book is to enhance the users' understanding of cryptography while integrating them with the ongoing research in the domain of Nature-inspired Cryptology. Extensive research examines the effectiveness and capabilities of nature-inspired cybersecurity along with NICS and compares them.

The primary objective of the book is to provide a comprehensive examination of cryptography in light of recent discoveries, using natural examples to illustrate how



to enhance cybersecurity systems. In this book, recent advancements in NICS are dissected and compared to other technologies of the same era.

Before concluding, we would like to extend our sincere gratitude to everyone who contributed to making this textbook what it is today. Kadhambari S. Viswanathan, Assistant Vice President of VIT Bhopal, deserves special recognition for her unwavering support and guidance. Also, we would like to mention our research collaborators, Gaurav Choudhary, David (Bong Jun) Choi, Ajit Kumar, Saket Upadhyay, and Chirag Ganguli. Last but not least, the authors would like to thank their parents, loved ones, acquaintances, and colleagues for their unwavering support and insightful feedback. We recognise the value of students at VIT Bhopal University studying cybersecurity and digital forensics, and a special mention goes to our lovely and enthusiastic research team at SECURE-CoE, VIT Bhopal University, presently Aditya Srivastav, Devangana Sujay, GSV Prharsha, Sidarth Panda, Yash Kartik, and Yuvraj Singh along with Akshay Syam.

Everyone who took the time to read this book and provide feedback, ideas, and encouragement is greatly appreciated. Despite this endeavour's numerous challenges and prolonged duration, significant progress was made. We are grateful to the extraordinary individuals who agreed to accompany us on this journey.

Indore, India  
Bhopal, India  
Liverpool, UK

Shishir Kumar Shandilya  
Agni Datta  
Atulya K. Nagar

# Contents

## Part I Preliminaries

<b>1</b>	<b>Nature-inspired Algorithms</b>	<b>3</b>
1.1	Introduction	3
1.2	Soft Computing	5
1.3	Nature-inspired Computing	7
1.4	Bioinformatics	9
1.5	Bio-inspired Computing	12
1.6	Relations Between the Paradigms	14
1.7	Key Concepts in Nature-inspired Algorithms	15
1.7.1	Fitness Function	16
1.7.2	Convergence and Optimization Criterion	17
1.7.3	Crossover and Mutation Operators	18
1.7.4	Selection Mechanism	19
1.7.5	Local Search	21
1.8	Taxonomy of Nature-inspired Algorithms	22
1.8.1	Physical Systems-inspired Algorithms	23
1.8.2	Swarm Intelligence Algorithms	24
1.8.3	Evolutionary Algorithms	25
1.9	Advantages and Challenges	27
1.9.1	Advantages: Optimization Efficiency and Robustness	27
1.9.2	Challenges: Parameter Tuning and Convergence	28
1.9.3	Traditional Versus Nature-inspired Algorithms	28
1.10	Applications of Nature-inspired Algorithms	29
1.11	Nature-inspired Cybersecurity	30
1.12	Future Research	32
1.13	Summary	33
	References	34

<b>2</b>	<b>Cryptography Background</b>	<b>37</b>
2.1	Introduction	37
2.2	Principles	39
2.2.1	Kerckhoffs' Principles	39
2.2.2	Provable Security	40
2.3	Objectives	41
2.3.1	Authentication	41
2.3.2	Authorization	42
2.3.3	Confidentiality	42
2.3.4	Integrity	43
2.3.5	Non-repudiation	43
2.3.6	Key Management	43
2.3.7	Cryptographic Algorithms	44
2.3.8	Continuous Evaluation and Improvement	44
2.3.9	CIA Triad	44
2.4	Preliminaries	46
2.4.1	Cryptosystem	48
2.4.2	Cipher	49
2.5	Block Versus Stream Ciphers	50
2.5.1	Block Cipher	50
2.5.2	Stream Cipher	52
2.6	Symmetric Versus Asymmetric Ciphers	54
2.7	Cryptographic Hash Function	58
2.7.1	Application: Password Storage	59
2.7.2	Application: Message Integrity	60
2.7.3	Application: Digital Signatures	61
2.7.4	Application: Blockchain	62
2.8	Cryptanalytic Attacks	63
2.9	Common Attack Mechanisms	65
2.9.1	Brute-Force Attack	65
2.9.2	Man-in-the-Middle Attack	66
2.9.3	Replay Attack	67
2.9.4	Side-Channel Attack	68
2.9.5	Birthday Attack	70
2.10	Nature-Inspired Approach to Cryptography	71
2.11	Future Research	72
2.12	Summary	74
	Bibliography	75

## Part II Approaches

<b>3</b>	<b>Learning-Based Cryptography</b>	<b>79</b>
3.1	Introduction	79
3.2	Computational Learning Theory	81
3.3	CoLT and Cryptography	83

3.4	Neural Networks	85
3.5	Artificial Neural Networks	88
3.6	Types of Neural Networks	89
3.6.1	Feedforward Neural Networks (FFNNs)	89
3.6.2	Convolutional Neural Networks (CNNs)	90
3.6.3	Recurrent Neural Networks (RNNs)	91
3.6.4	Long Short-Term Memory Networks (LSTMs)	92
3.6.5	Autoencoder Networks	93
3.6.6	Generative Adversarial Networks (GANs)	94
3.7	Advantages and Limitations of Neural Networks	95
3.7.1	Advantages of Neural Networks	96
3.7.2	Limitations of Neural Networks	97
3.8	Neural Cryptography	99
3.9	Neural Cryptosystems	100
3.9.1	Wolfram's Original Proposal	101
3.9.2	Neural Protocol	105
3.9.3	Tree Parity Machine	108
3.9.4	Tree Parity Protocol	110
3.9.5	Permutation Parity Machine	111
3.9.6	Cryptosystems Based on Permutation Parity Machine	112
3.9.7	Biometric-Based Neural Cryptography	114
3.9.8	Learning Parity with Noise	116
3.9.9	Cryptosystems Based on Learning Parity with Noise	118
3.10	Future Research	119
3.10.1	Neural Network-Based Cryptanalysis	120
3.10.2	Neural Network-Based Cryptographic Primitives	120
3.10.3	Privacy-Preserving Machine Learning	121
3.11	Summary	121
	Bibliography	122
<b>4</b>	<b>DNA-Based Cryptography</b>	<b>125</b>
4.1	Introduction	125
4.2	DNA	127
4.3	DNA Computing	129
4.3.1	DNA Storage	132
4.3.2	DNA Encrypting	132
4.4	DNA Cryptography	134
4.5	DNA Encryption	135
4.5.1	GLR Cryptosystem	138
4.5.2	Verma et al. Cryptosystem	141
4.5.3	DNA XOR Cryptography	144
4.6	Future Research	146
4.7	Summary	148
	Bibliography	149

<b>5</b>	<b>Biometric and Bio-Cryptography</b>	153
5.1	Introduction	153
5.2	Biometrics	155
5.3	Biometric Template	155
5.4	Biometric Systems	156
5.5	Bio-Cryptography	162
5.6	Relationship with Biometrics	164
5.7	Examples of Bio-Cryptography	165
5.7.1	Explanation of Bio-Cryptography	166
5.7.2	Formalism of Bio-Cryptography	167
5.7.3	Types of Biometric Modalities	171
5.7.4	Fingerprint Recognition	171
5.7.5	Iris Recognition	173
5.7.6	Facial Recognition	174
5.7.7	Voice Recognition	175
5.7.8	Other Biometric Modalities	176
5.8	Biometric System Components	178
5.8.1	Sensor Acquisition	179
5.8.2	Feature Extraction	180
5.8.3	Matching and Verification	181
5.8.4	Template Storage and Management	183
5.8.5	System Integration	184
5.9	Biometric Template Protection	185
5.9.1	Template Encryption Techniques	186
5.9.2	Secure Storage and Transmission	187
5.9.3	Template Update and Revocation	188
5.9.4	Cryptographic Key Generation from Biometrics	189
5.10	Bio-Cryptographic Protocols and Applications	192
5.10.1	Secure Authentication	192
5.10.2	Privacy-Preserving Biometric Systems	193
5.10.3	Multi-Factor Authentication	195
5.11	Biometric System Attacks	197
5.12	Significance	198
5.13	Challenges and Concerns	200
5.13.1	Security and Privacy Problems	200
5.13.2	Performance and Usability	205
5.14	Future Directions and Research Trends	209
5.14.1	Advances in Biometric Technology	209
5.14.2	Emerging Techniques Applied to Bio-Cryptographic	212
5.14.3	Mitigating Security and Privacy Concerns	217
5.15	Summary	220
	Bibliography	222

<b>6</b>	<b>Nature-Inspired Lightweight Cryptosystems</b>	225
6.1	Introduction	225
6.2	Lightweight Cryptography	227
6.3	Importance of Lightweight Cryptography	229
6.4	Traditional Lightweight Cryptographic Algorithms	231
6.5	Security Analysis	232
6.5.1	Threat Model	232
6.5.2	Security Evaluation Metrics	234
6.5.3	Performance Analysis	235
6.5.4	Hardware Implementations	236
6.5.5	Software Implementations	239
6.6	Future Research	241
6.7	Summary	242
	Bibliography	243
<b>7</b>	<b>Chaos Cryptography</b>	245
7.1	Introduction	245
7.2	Dynamical System	246
7.2.1	State Space	249
7.2.2	Time	250
7.2.3	Evolution Rule	250
7.2.4	Maps	251
7.2.5	Iterated Function System	251
7.2.6	Flows	252
7.3	Nonlinear Dynamical Systems	252
7.4	Linear Dynamical System	254
7.5	Chaos Theory	256
7.6	Chaotic Maps	263
7.7	Chaotic Systems	264
7.7.1	Butterfly Effect	267
7.8	An Example of Chaotic System: Lorenz System	268
7.9	An Example of Chaotic System: Rössler System	270
7.10	Chaos Computing	274
7.11	Chaos Cryptography	276
7.12	Logistic Maps	278
7.13	Logistic Map-Based Cryptography	280
7.14	Tent Map	282
7.15	Tent Map Cryptosystem	284
7.16	Henon Map	287
7.17	Henon Map-Based Cryptography	289
7.18	Security Evaluation of Henon Map Cryptography	290
7.18.1	Expansive Key Space	290
7.18.2	Confusion and Diffusion	291
7.18.3	Cryptographic Attacks	291

7.19	Baker's Map .....	293
7.20	Baker's Map-Based Cryptography .....	295
7.21	Chaos-Based Hash Algorithm (CHA-1) .....	296
7.22	Lorenz Chaotic Key Exchange .....	299
7.23	Future Research .....	302
7.24	Summary .....	304
	Bibliography .....	305

## About the Authors

**Shishir Kumar Shandilya** D.Sc., (Ph.D.,) is an Associate Professor in the School of Data Science and Forecasting at Devi Ahilya University in India. He is also a Visiting Professor at Liverpool Hope University in the United Kingdom. He is a Cambridge University-certified professional teacher and trainer, a TEDx speaker, an ACM Distinguished Speaker, and a senior member of IEEE.

Dr. Shandilya is a NASSCOM-certified master trainer for security analysts in SOC (SSC/Q0909: NVEQF Level 7). He has received the IDA Teaching Excellence Award for distinctive use of technology in teaching by the Indian Didactics Association in Bangalore (2016), and the Young Scientist Award for two consecutive years, 2005 and 2006, by the MP Science Congress and MP Council of Science and Technology. He is a highly regarded author with published research works in reputable academic publishers such as Springer, IGI-USA, River Denmark, and Prentice Hall of India. Dr. Shandilya also has international and national patents and copyrights granted for adaptive cyber defence methods.

**Agni Datta** is a cryptologist working with SECURE—Centre of Excellence in Cyber Security and a researcher who specializes in theoretical computer science at VIT Bhopal University in India. He is a member of several prestigious professional associations, including ACM, IEEE, AMS, and SIAM. His research interests include various cryptographic primitives like zero-knowledge proofs, multiparty computation, and lattice cryptography. He is particularly focused on security primitives for computing, as well as computational complexity and probabilistic proofs.

**Atulya K. Nagar** holds the foundation chair as a Professor of Mathematical Sciences and is the Pro-Vice-Chancellor for research at Liverpool Hope University, UK. He has been the dean of the Faculty of Science and head of the School of Mathematics, Computer Science, and Engineering, which he established at the university. He was awarded a prestigious Commonwealth Fellowship in 1996 to pursue his doctorate (D.Phil.) in applied nonlinear mathematics at the University of York (UK). Furthermore, he holds a B.Sc. (Hons), an M.Sc. (Mathematics), and an M.Phil. (with distinction) in mathematical physics from the MDS University of Ajmer, India. Prior



to joining Liverpool Hope, he was with the Department of Mathematical Sciences and later with the Department of Systems Engineering at Brunel University, London. He is an internationally respected scholar working at the cutting edge of theoretical computer science, applied mathematical analysis, and systems engineering, with research expertise spanning both applied mathematics and computational methods for nonlinear, complex, and intractable problems arising in science, engineering, and industry. He has edited volumes on intelligent systems and applied mathematics. Furthermore, he is the editor-in-chief of the *International Journal of Artificial Intelligence and Soft Computing* (IJASIS) and serves on the editorial boards of several prestigious journals. Likewise, he is well-published, with over 450 publications in prestigious publishing outlets. Professor Nagar sits on several strategic UK-wide research bodies, including the JISC Research Strategy Group, and he is a fellow of the Institute of Mathematics and its Applications (FIMA) and a fellow of the Higher Education Academy (FHEA).

# List of Figures

Fig. 1.1	Bioinformatics and its branches .....	10
Fig. 1.2	Interdisciplinary connections .....	14
Fig. 1.3	Nature-inspired algorithms classifications .....	23
Fig. 2.1	CIA triad .....	45
Fig. 2.2	Symmetric key ciphers .....	56
Fig. 2.3	Asymmetric key ciphers .....	57
Fig. 2.4	Cryptographic Hash function .....	59
Fig. 2.5	Example: Brute-force attack .....	65
Fig. 2.6	Man-in-the-middle attack .....	67
Fig. 2.7	Replay attack .....	68
Fig. 2.8	Side-channel attack .....	69
Fig. 2.9	Birthday attack .....	71
Fig. 3.1	A schematic of neural network .....	87
Fig. 3.2	Example of the initial state of a cellular automaton .....	103
Fig. 4.1	DNA Double Helix Structure .....	128
Fig. 7.1	Lorentz attractor .....	269
Fig. 7.2	Tent map graph .....	283

# List of Tables

Table 2.1	Types of ciphers .....	50
Table 2.2	Comparison of block and stream ciphers .....	54
Table 2.3	Comparison of symmetric and asymmetric ciphers .....	58
Table 5.1	Comparison of Various Biometric Techniques .....	161