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

Springer

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

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, the 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 — Shishir Kumar Shandilya
Bhopal, India — Agni Datta
Liverpool, UK — Atulya K. Nagar

Contents

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* (IJAISC) 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

List of Tables