1. Record Nr. UNINA9910770275703321

Autore	Shandilya Shishir Kumar
Titolo	A Nature-Inspired Approach to Cryptology
Pubbl/distr/stampa	Singapore : , : Springer, , 2024 ©2023
ISBN	9789819970810 9819970814
Edizione	[1st ed.]
Descrizione fisica	1 online resource (325 pages)
Collana	Studies in Computational Intelligence Series ; ; v.1122
Altri autori (Persone)	DattaAgni NagarAtulya K
Soggetti	Cryptography Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- "Scientia potentia est" -- Contents -- About the Authors -- List of Figures -- List of Tables -- Part I Preliminaries -- 1 Nature-inspired Algorithms -- 1.1 Introduction -- 1.2 Soft Computing -- 1.3 Nature-inspired Computing -- 1.4 Bioinformatics -- 1.5 Bio-inspired Computing -- 1.6 Relations Between the Paradigms -- 1.7 Key Concepts in Nature-inspired Algorithms -- 1.7.1 Fitness Function -- 1.7.2 Convergence and Optimization Criterion -- 1.7.3 Crossover and Mutation Operators -- 1.7.4 Selection Mechanism -- 1.7.5 Local Search -- 1.8 Taxonomy of Nature-inspired Algorithms -- 1.8.1 Physical Systems-inspired Algorithms -- 1.8.2 Swarm Intelligence Algorithms -- 1.8.3 Evolutionary Algorithms -- 1.9 Advantages and Challenges -- 1.9.1 Advantages: Optimization Efficiency and Robustness -- 1.9.2 Challenges: Parameter Tuning and Convergence -- 1.9.3 Traditional Versus Nature-inspired Algorithms -- 1.10 Applications of Nature-inspired Algorithms -- 1.11 Nature-inspired Cybersecurity -- 1.12 Future Research -- 1.13 Summary -- References -- 2 Cryptography Background -- 2.1 Introduction -- 2.2 Principles -- 2.2.1 Kerckhoffs' Principles -- 2.2.2 Provable Security -- 2.3 Objectives -- 2.3.1 Authentication -- 2.3.2 Authorization -- 2.3.3 Confidentiality -- 2.3.4 Integrity -- 2.3.5 Non-repudiation -- 2.3.6 Key Management

-- 2.3.7 Cryptographic Algorithms -- 2.3.8 Continuous Evaluation and Improvement -- 2.3.9 CIA Triad -- 2.4 Preliminaries -- 2.4.1 Cryptosystem -- 2.4.2 Cipher -- 2.5 Block Versus Stream Ciphers -- 2.5.1 Block Cipher -- 2.5.2 Stream Cipher -- 2.6 Symmetric Versus Asymmetric Ciphers -- 2.7 Cryptographic Hash Function -- 2.7.1 Application: Password Storage -- 2.7.2 Application: Message Integrity -- 2.7.3 Application: Digital Signatures -- 2.7.4 Application: Blockchain -- 2.8 Cryptanalytic Attacks -- 2.9 Common Attack Mechanisms.
2.9.1 Brute-Force Attack -- 2.9.2 Man-in-the-Middle Attack -- 2.9.3 Replay Attack -- 2.9.4 Side-Channel Attack -- 2.9.5 Birthday Attack -- 2.10 Nature-Inspired Approach to Cryptography -- 2.11 Future Research -- 2.12 Summary -- Bibliography -- Part II Approaches -- 3 Learning-Based Cryptography -- 3.1 Introduction -- 3.2 Computational Learning Theory -- 3.3 CoLT and Cryptography -- 3.4 Neural Networks -- 3.5 Artificial Neural Networks -- 3.6 Types of Neural Networks -- 3.6.1 Feedforward Neural Networks (FFNNs) -- 3.6.2 Convolutional Neural Networks (CNNs) -- 3.6.3 Recurrent Neural Networks (RNNs) -- 3.6.4 Long Short-Term Memory Networks (LSTMs) -- 3.6.5 Autoencoder Networks -- 3.6.6 Generative Adversarial Networks (GANs) -- 3.7 Advantages and Limitations of Neural Networks -- 3.7.1 Advantages of Neural Networks -- 3.7.2 Limitations of Neural Networks -- 3.8 Neural Cryptography -- 3.9 Neural Cryptosystems -- 3.9.1 Wolfram's Original Proposal -- 3.9.2 Neural Protocol -- 3.9.3 Tree Parity Machine -- 3.9.4 Tree Parity Protocol -- 3.9.5 Permutation Parity Machine -- 3.9.6 Cryptosystems Based on Permutation Parity Machine -- 3.9.7 Biometric-Based Neural Cryptography -- 3.9.8 Learning Parity with Noise -- 3.9.9 Cryptosystems Based on Learning Parity with Noise -- 3.10 Future Research -- 3.10.1 Neural Network-Based Cryptanalysis -- 3.10.2 Neural Network-Based Cryptographic Primitives -- 3.10.3 Privacy-Preserving Machine Learning -- 3.11 Summary -- Bibliography -- 4 DNA-Based Cryptography -- 4.1 Introduction -- 4.2 DNA -- 4.3 DNA Computing -- 4.3.1 DNA Storage -- 4.3.2 DNA Encrypting -- 4.4 DNA Cryptography -- 4.5 DNA Encryption -- 4.5.1 GLR Cryptosystem -- 4.5.2 Verma et al. Cryptosystem -- 4.5.3 DNA XOR Cryptography -- 4.6 Future Research -- 4.7 Summary -- Bibliography -- 5 Biometric and Bio-Cryptography -- 5.1 Introduction -- 5.2 Biometrics.
5.3 Biometric Template -- 5.4 Biometric Systems -- 5.5 Bio-Cryptography -- 5.6 Relationship with Biometrics -- 5.7 Examples of Bio-Cryptography -- 5.7.1 Explanation of Bio-Cryptography -- 5.7.2 Formalism of Bio-Cryptography -- 5.7.3 Types of Biometric Modalities -- 5.7.4 Fingerprint Recognition -- 5.7.5 Iris Recognition -- 5.7.6 Facial Recognition -- 5.7.7 Voice Recognition -- 5.7.8 Other Biometric Modalities -- 5.8 Biometric System Components -- 5.8.1 Sensor Acquisition -- 5.8.2 Feature Extraction -- 5.8.3 Matching and Verification -- 5.8.4 Template Storage and Management -- 5.8.5 System Integration -- 5.9 Biometric Template Protection -- 5.9.1 Template Encryption Techniques -- 5.9.2 Secure Storage and Transmission -- 5.9.3 Template Update and Revocation -- 5.9.4 Cryptographic Key Generation from Biometrics -- 5.10 Bio-Cryptographic Protocols and Applications -- 5.10.1 Secure Authentication -- 5.10.2 Privacy-Preserving Biometric Systems -- 5.10.3 Multi-Factor Authentication -- 5.11 Biometric System Attacks -- 5.12 Significance -- 5.13 Challenges and Concerns -- 5.13.1 Security and Privacy Problems -- 5.13.2 Performance and Usability -- 5.14 Future Directions and Research Trends -- 5.14.1 Advances in Biometric Technology -- 5.14.2 Emerging Techniques Applied to Bio-Cryptographic -- 5.14.3 Mitigating Security and Privacy Concerns --

5.15 Summary -- Bibliography -- 6 Nature-Inspired Lightweight Cryptosystems -- 6.1 Introduction -- 6.2 Lightweight Cryptography -- 6.3 Importance of Lightweight Cryptography -- 6.4 Traditional Lightweight Cryptographic Algorithms -- 6.5 Security Analysis -- 6.5.1 Threat Model -- 6.5.2 Security Evaluation Metrics -- 6.5.3 Performance Analysis -- 6.5.4 Hardware Implementations -- 6.5.5 Software Implementations -- 6.6 Future Research -- 6.7 Summary -- Bibliography -- 7 Chaos Cryptography -- 7.1 Introduction. 7.2 Dynamical System -- 7.2.1 State Space -- 7.2.2 Time -- 7.2.3 Evolution Rule -- 7.2.4 Maps -- 7.2.5 Iterated Function System -- 7.2.6 Flows -- 7.3 Nonlinear Dynamical Systems -- 7.4 Linear Dynamical System -- 7.5 Chaos Theory -- 7.6 Chaotic Maps -- 7.7 Chaotic Systems -- 7.7.1 Butterfly Effect -- 7.8 An Example of Chaotic System: Lorenz System -- 7.9 An Example of Chaotic System: Rössler System -- 7.10 Chaos Computing -- 7.11 Chaos Cryptography -- 7.12 Logistic Maps -- 7.13 Logistic Map-Based Cryptography -- 7.14 Tent Map -- 7.15 Tent Map Cryptosystem -- 7.16 Henon Map -- 7.17 Henon Map-Based Cryptography -- 7.18 Security Evaluation of Henon Map Cryptography -- 7.18.1 Expansive Key Space -- 7.18.2 Confusion and Diffusion -- 7.18.3 Cryptographic Attacks -- 7.19 Baker's Map -- 7.20 Baker's Map-Based Cryptography -- 7.21 Chaos-Based Hash Algorithm (CHA-1) -- 7.22 Lorenz Chaotic Key Exchange -- 7.23 Future Research -- 7.24 Summary -- Bibliography.

Sommario/riassunto

This book explores the theoretical aspects of cryptography, emphasizing algorithms inspired by natural phenomena. It addresses challenges posed by quantum computing and low-resource embedded systems, focusing on developing efficient cryptographic techniques for data safety and system optimization. The text provides a comprehensive examination of cryptography, emphasizing mathematical foundations and the potential of nature-inspired cybersecurity strategies. It is intended for readers with a strong background in mathematics and computer science, aiming to enhance their understanding of cryptography and its implications in cybersecurity.