

1. Record Nr.	UNINA9910338252303321
Autore	Díaz Cardell Sara
Titolo	Cryptography with Shrinking Generators : Fundamentals and Applications of Keystream Sequence Generators Based on Irregular Decimation / / by Sara Díaz Cardell, Amparo Fúster-Sabater
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2019
ISBN	3-030-12850-4
Edizione	[1st ed. 2019.]
Descrizione fisica	1 online resource (xi, 101 pages) : illustrations
Collana	SpringerBriefs in Mathematics, , 2191-8198
Disciplina	652.8 005.824
Soggetti	Discrete mathematics Coding theory Information theory Algebra Data encryption (Computer science) Computers Discrete Mathematics Coding and Information Theory Cryptology Models and Principles
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Chapter 1- Introduction to stream ciphers -- Chapter 2- Keystream generators based on irregular decimation -- Chapter 3- Modelling through linear cellular automata -- Chapter 4- Cryptanalysis -- References.
Sommario/riassunto	This book offers a broad survey of all information made public - from 1993 until today - on keystream sequence generators based on irregular decimation, which are referred to as shrinking generators. Starting with an overview of cryptography, it describes each type of generator - shrinking, self-shrinking, modified self-shrinking, generalized self-shrinking and the DECIM algorithm - with examples

and references. Further, the book discusses several attacks on these generators and applications. It concludes by demonstrating how the output sequences can be modeled by means of different families of one-dimensional cellular automata, rendering the generators vulnerable to attacks. Intended for researchers and graduate students, the book will hopefully inspire them to search for more details on this family of generators and to address the open problems in this field. .

2. Record Nr.

Titolo

UNINA9910495160203321

Machine Learning and Knowledge Extraction : 5th IFIP TC 5, TC 12, WG 8.4, WG 8.9, WG 12.9 International Cross-Domain Conference, CD-MAKE 2021, Virtual Event, August 17–20, 2021, Proceedings // edited by Andreas Holzinger, Peter Kieseberg, A Min Tjoa, Edgar Weippl

Pubbl/distr/stampa Cham : , : Springer International Publishing : , : Imprint : Springer, , 2021

ISBN 3-030-84060-3

Edizione [1st ed. 2021.]

Descrizione fisica 1 online resource (X, 365 p. 119 illus., 96 illus. in color.)

Collana Information Systems and Applications, incl. Internet/Web, and HCI, , 2946-1642 ; ; 12844

Disciplina 001.6

Soggetti Artificial intelligence
Education - Data processing
Database management
Data mining
Artificial Intelligence
Computers and Education
Database Management
Data Mining and Knowledge Discovery

Lingua di pubblicazione Inglese

Formato Materiale a stampa

Livello bibliografico Monografia

Nota di contenuto Digital Transformation for Sustainable Development Goals (SDGs) - a Security, Safety and Privacy Perspective on AI -- When in Doubt, Ask: Generating Answerable and Unanswerable Questions, Unsupervised --

Self-Propagating Malware Containment via Reinforcement Learning -- Text2PyCode : Machine Translation of Natural Language Intent to Python Source Code -- Automated Short Answer Grading using Deep Learning : A Survey -- Fair and Adequate Explanations -- Mining Causal Hypotheses in Categorical Time Series by Iterating on Binary Correlations -- Active Finite Reward Automaton Inference and Reinforcement Learning Using Queries and Counterexamples -- Rice seed image-to-image translation using Generative Adversarial Networks to improve weedy rice image classification -- Reliable AI through SVDD and rule extraction -- Airbnb Price Prediction Using Machine Learning and Sentiment Analysis -- Towards Financial Sentiment Analysis in a South African Landscape -- Decisions are not all equal. Introducing a utility metric based on the case-wise raters' perceptions -- Deep Convolutional Neural Network(CNN) design for pathology detection of COVID-19 in chest X-Ray Images -- Anomaly detection for skin lesion images using replicator neural networks -- On the overlap between Grad-CAM saliency maps and explainable visual features in skin cancer images -- From Explainable to Reliable Artificial Intelligence -- Explanatory Pluralism in Explainable AI -- On the Trustworthiness of Tree Ensemble Explainability Methods -- Human-in-the-loop model explanation via verbatim boundary identification in generated neighborhoods -- MAIRE - A Model-Agnostic Interpretable Rule Extraction Procedure for Explaining Classifiers -- Transparent Ensembles for Covid-19 Prognosis.

Sommario/riassunto

This book constitutes the refereed proceedings of the 5th IFIP TC 5, TC 12, WG 8.4, WG 8.9, WG 12.9 International Cross-Domain Conference, CD-MAKE 2021, held in virtually in August 2021. The 20 full papers and 2 short papers presented were carefully reviewed and selected from 48 submissions. The cross-domain integration and appraisal of different fields provides an atmosphere to foster different perspectives and opinions; it will offer a platform for novel ideas and a fresh look on the methodologies to put these ideas into business for the benefit of humanity.
