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. .