1.	Record Nr.	UNINA9910484837203321
	Titolo	Sequences and Their Applications – SETA 2006 : 4th International Conference, Beijing, China, September 24-28, 2006, Proceedings / / edited by Guang Gong, Tor Helleseth, Hong-Yeop Song, Kyeongcheol Yang
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2006
	ISBN	3-540-44524-2
	Edizione	[1st ed. 2006.]
	Descrizione fisica	1 online resource (XII, 436 p.)
	Collana	Theoretical Computer Science and General Issues, , 2512-2029 ; ; 4086
	Altri autori (Persone)	GongGuang <1956->
	Disciplina	515/.24
	Soggetti	Coding theory Information theory Cryptography Data encryption (Computer science) Computer science Algorithms Numerical analysis Computer science - Mathematics Coding and Information Theory Cryptology Theory of Computation Numerical Analysis Symbolic and Algebraic Manipulation
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Bibliographic Level Mode of Issuance: Monograph
	Nota di bibliografia	Includes bibliographical references and index.
	Nota di contenuto	Invited Papers -- Shift Register Sequences – A Retrospective Account -- The Probabilistic Theory of the Joint Linear Complexity of Multisequences -- Multi-Continued Fraction Algorithms and Their Applications to Sequences -- Codes for Optical CDMA -- Linear Complexity of Sequences -- On the Linear Complexity of Sidel’nikov Sequences over -- Linear Complexity over F p of Ternary Sidel’nikov Sequences -- Bounds on the Linear Complexity and the 1-Error Linear

Complexity over F p of M-ary Sidel’nikov Sequences -- The Characterization of 2 n -Periodic Binary Sequences with Fixed 1-Error Linear Complexity -- Correlation of Sequences -- Crosscorrelation Properties of Binary Sequences with Ideal Two-Level Autocorrelation -- Extended Hadamard Equivalence -- Analysis of Designing Interleaved ZCZ Sequence Families -- Stream Ciphers and Transforms -- Security of Jump Controlled Sequence Generators for Stream Ciphers -- Improved Rijndael-Like S-Box and Its Transform Domain Analysis -- Topics in Complexities of Sequences -- Nonlinear Complexity of Binary Sequences and Connections with Lempel-Ziv Compression -- On Lempel-Ziv Complexity of Sequences -- Computing the k-Error N-Adic Complexity of a Sequence of Period p n -- On the Expected Value of the Joint 2-Adic Complexity of Periodic Binary Multisequences -- Linear/Nonlinear Feedback Shift Register Sequences -- On the Classification of Periodic Binary Sequences into Nonlinear Complexity Classes -- Sequences of Period 2 N –2 -- A New Algorithm to Compute Remote Terms in Special Types of Characteristic Sequences -- Multi-sequence Synthesis -- Implementation of Multi-continued Fraction Algorithm and Application to Multi-sequence Linear Synthesis -- The Hausdorff Dimension of the Set of r-Perfect M-Multisequences -- Filtering Sequences andPseudorandom Sequence Generators -- Lower Bounds on Sequence Complexity Via Generalised Vandermonde Determinants -- Construction of Pseudo-random Binary Sequences from Elliptic Curves by Using Discrete Logarithm -- On the Discrepancy and Linear Complexity of Some Counter-Dependent Recurrence Sequences -- Sequences and Combinatorics -- Nonexistence of a Kind of Generalized Perfect Binary Array -- FCSR Sequences -- On the Distinctness of Decimations of Generalized l-Sequences -- On FCSR Memory Sequences -- Periodicity and Distribution Properties of Combined FCSR Sequences -- Aperiodic Correlation and Applications -- Generalized Bounds on Partial Aperiodic Correlation of Complex Roots of Unity Sequences -- Chip-Asynchronous Version of Welch Bound: Gaussian Pulse Improves BER Performance -- Boolean Functions -- On Immunity Profile of Boolean Functions -- Reducing the Number of Homogeneous Linear Equations in Finding Annihilators -- The Algebraic Normal Form, Linear Complexity and k-Error Linear Complexity of Single-Cycle T-Function -- Partially Perfect Nonlinear Functions and a Construction of Cryptographic Boolean Functions -- Construction of 1-Resilient Boolean Functions with Very Good Nonlinearity.

Sommario/riassunto

This book constitutes the refereed proceedings of the 4th International Conference on Sequences and Their Applications, SETA 2006. The book presents 32 revised full papers together with 4 invited lectures. The papers are organized in topical sections on linear complexity of sequences, correlation of sequences, stream ciphers and transforms, topics in complexities of sequences, multi-sequence synthesis, sequences and combinatorics, FCSR sequences, aperiodic correlation and applications, and boolean functions, and more.