1. Record Nr. UNINA9910768441803321

Titolo	Sequences and Their Applications - SETA 2008 : 5th International Conference Lexington, KY, USA, September 14-18, 2008, Proceedings / / edited by Solomon W. Golomb, Matthew G. Parker, Alexander Pott, Arne Winterhof
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2008
ISBN	3-540-85912-8
Edizione	[1st ed. 2008.]
Descrizione fisica	1 online resource (XII, 421 p.)
Collana	Theoretical Computer Science and General Issues, , 2512-2029 ; ; 5203
Disciplina	515.24
Soggetti	Computer science - Mathematics Discrete mathematics Computer science Mathematical models Algebra Coding theory Information theory Discrete Mathematics in Computer Science Theory of Computation Mathematical Modeling and Industrial Mathematics Symbolic and Algebraic Manipulation Coding and Information Theory
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	Probabilistic Methods and Randomness Properties of Sequences -- Comparison of Point Sets and Sequences for Quasi-Monte Carlo and for Random Number Generation -- On Independence and Sensitivity of Statistical Randomness Tests -- New Distinguishers Based on Random Mappings against Stream Ciphers -- A Probabilistic Approach on Estimating the Number of Modular Sonar Sequences -- A Study on the Pseudorandom Properties of Sequences Generated Via the Additive Order -- On the Average Distribution of Power Residues and Primitive

Elements in Inversive and Nonlinear Recurring Sequences -- Correlation -- Some Results on the Arithmetic Correlation of Sequences -- A Class of Nonbinary Codes and Sequence Families -- Results on the Crosscorrelation and Autocorrelation of Sequences -- m-Sequences of Lengths 22k ??1 and 2 k ???1 with at Most Four-Valued Cross Correlation -- On the Correlation Distribution of Kerdock Sequences -- Two New Families of Low-Correlation Interleaved QAM Sequences -- Combinatorial and Algebraic Foundations -- The Combinatorics of Differentiation -- Group Representation Design of Digital Signals and Sequences -- Projective de Bruijn Sequences -- Multiplicative Character Sums of Recurring Sequences with Rédei Functions -- On the Connection between Kloosterman Sums and Elliptic Curves -- A Class of Optimal Frequency Hopping Sequences Based upon the Theory of Power Residues -- Security Aspects of Sequences -- Sequences, DFT and Resistance against Fast Algebraic Attacks -- Expected ?-Adic Security Measures of Sequences -- Distance-Avoiding Sequences for Extremely Low-Bandwidth Authentication -- On the Number of Linearly Independent Equations Generated by XL -- 2 n -Periodic Binary Sequences with Fixed k-Error Linear Complexity for k?=?2 or 3 -- Generalized Joint LinearComplexity of Linear Recurring Multisequences -- Algorithms -- A Lattice-Based Minimal Partial Realization Algorithm -- A Fast Jump Ahead Algorithm for Linear Recurrences in a Polynomial Space -- Parallel Generation of ?-Sequences -- Correlation of Sequences over Rings -- Design of M-Ary Low Correlation Zone Sequence Sets by Interleaving -- The Peak to Sidelobe Level of the Most Significant Bit of Trace Codes over Galois Rings -- On Partial Correlations of Various Z 4 Sequence Families -- Nonlinear Functions over Finite Fields -- On the Higher Order Nonlinearities of Boolean Functions and S-Boxes, and Their Generalizations -- On a Class of Permutation Polynomials over -- On 3-to-1 and Power APN S-Boxes -- Negabent Functions in the Maiorana–McFarland Class -- New Perfect Nonlinear Multinomials over F for Any Odd Prime p -- A New Tool for Assurance of Perfect Nonlinearity.

Sommario/riassunto

This book constitutes the refereed proceedings of the 5th International Conference on Sequences and Their Applications, SETA 2008, held in Lexington, KY, USA in September 2008. The 32 revised full papers presented were carefully reviewed and selected. The papers are organized in topical sections on probabilistic methods and randomness properties of sequences; correlation; combinatorial and algebraic foundations; security aspects of sequences; algorithms; correlation of sequences over rings; nonlinear functions over finite fields.