Permutation Polynomials and Their Applications in Cryptography

Permutation polynomials have been a subject of study for many years and have applications in many areas of science and engineering. This monograph contains some results related to permutation polynomials over finite rings and finite fields. A survey of known results and detailed bibliography is provided. A special feature is the applications of permutation polynomials in multivariate public key cryptography. Multivariate public key cryptography is a branch of public key cryptography in which the cryptosystems are based on the problem of solving nonlinear equations over finite fields. This monograph contains design and analysis of some efficient multivariate public key cryptosystems using permutation polynomials over finite fields.

Finite Automata and Application to Cryptography mainly deals with the invertibility theory of finite automata and its application to cryptography. In addition, autonomous finite automata and Latin arrays, which are relative to the canonical form for one-key cryptosystems based on finite automata, are also discussed. Finite automata are regarded as a natural model for ciphers. The Ra Rb transformation method is introduced to deal with the structure problem of such automata; then public key cryptosystems based on finite automata and a canonical form for one-key ciphers implementable by finite automata with bounded-error-propagation and without data expansion are proposed. The book may be used as a reference for computer science and mathematics majors, including seniors and graduate students. Renji Tao is a Professor at the Institute of Software, Chinese Academy of Sciences, Beijing.
Multivariate Public Key Cryptography

File Type PDF Permutation Polynomials And Their Applications In Cryptography Permutation Polynomials And

volume were carefully reviewed and selected from numerous submissions. The program of the 2018 meeting consisted of 20 topical sessions, each of which providing an overview of

This book constitutes the proceedings of the 6th International Conference on Mathematical Software, ICMS 2018, held in South Bend, IN, USA, in July 2018. The 59 papers included in this

prime numbers in sequences, OFDM and CDMA, and frequency-hopping sequences.

Boolean functions, perfect sequences, correlation of arrays, relative difference sets, aperiodic correlation, pseudorandom sequences and stream ciphers, crosscorrelation of sequences,

2014. The 24 full papers presented together with 2 invited papers were carefully reviewed and selected from 36 submissions. The papers have been organized in topical sections on

This book constitutes the refereed proceedings of the 8th International Conference on Sequences and Their Applications, SETA 2014, held in Melbourne, VIC, Australia, in November

uses the free GAP computational package, allowing the reader to develop intuition about computationally hard problems and giving insights into how computational complexity can be

applications such as cryptography, secret sharing, error-correcting, fingerprinting, and compression of information. It explains in detail how these applications really work. The book

an undergraduate lecture course, this textbook provides all of the background in arithmetic, polynomials, groups, fields, and elliptic curves that is required to understand real-life

unauthorised access, and transmitted over unreliable channels. All of these operations are based on algebra and number theory and can only be properly understood with a good

Mathematics available.

This book investigates the permutation polynomial (PP) based interleavers for turbo codes, including all the main theoretical and practical findings related to topics such as full

enhance readers' understanding. The book is intended for engineers in the telecommunications field, but the chapters dealing with the PP coefficient conditions and with the number

with PP interleavers; specific methods to design and find PP interleavers with good bit/frame error rate (BER/FER) performance. The theoretical results are explained in great detail to

number of PP coefficient conditions for PPs up to fifth; the number of all true different PPs up to fifth degree; the number of true different PPs under Zhao and Fan sufficient conditions, for any degree

This book constitutes the refereed proceedings of the 7th International Conference on Sequences and Their Applications, SETA 2012, held in Waterloo, Canada, in June 2012. The 28 full

of PP are of interest to mathematicians working in the field.
Multivariate Public Key Cryptography

Permutation Polynomials and Their Applications in Cryptography

Permutation Polynomials and the cryptographic properties of Boolean functions are introduced. This book can serve as a reference for cryptographic algorithm designers, particularly the designers of stream ciphers and of block ciphers, and for academics with interest in cryptography. The book is not meant to be comprehensive, but with its own focus on some original research of the authors in the past. To be self-contained, some basic concepts and properties are presented. More specifically, Walsh spectrum description of the traditional cryptographic properties of Boolean functions, including linear structure, propagation criterion, nonlinearity, and correlation immunity are presented. Constructions of symmetric Boolean functions and of Boolean permutations with good cryptographic properties are specifically studied. This book focuses on the different representations and cryptographic properties of Boolean functions, presents constructions of Boolean functions with some good cryptographic properties, and discusses the properties of Boolean functions.

In the world of cryptography and number theory, finite fields continue to play increasingly important roles in various branches of modern mathematics, including number theory, coding theory, and cryptography. This book is based on the invited talks of the "RICAM-Workshop on Finite Fields and Their Applications: Character Sums and Polynomials" held at the Federal Institute for Adult Education (BIfEB) in Strobl, Austria, from September 2-7, 2012. Finite fields play important roles in many application areas such as coding theory, cryptography, Monte Carlo and quasi-Monte Carlo methods, pseudorandom number generation, quantum computing, and wireless communication. In this book we will focus on sequences, character sums, and polynomials over finite fields in view of the above mentioned application areas.
Aimed at the level of a beginning graduate student or advanced undergraduate, this book could serve well as a supplementary text for a course in finite field theory. It is accessible to the reader with only the basic theory of groups, rings, and fields. The first two chapters provide a gentle introduction to the subject. The remaining chapters are more advanced and cover a range of topics, including:

- Several classes of permutation polynomials, including the $q$-polynomials and the Dickson polynomials. Also included is a brief chapter describing two of many potential applications.
- Using the notion of an explicit basis for $GF(q^N)$ over $GF(q)$. Another chapter considers polynomials and polynomial-like functions on $GF(q^N)$ and contains a description of the finite field results concerning $GF(q^n)$.
- One chapter is devoted to giving explicit algorithms for computing in several of the infinite fields $GF(q^N)$. When $N$ is an ordinary integer $n$, this notation agrees with the usual notation $GF(q^n)$ for a dimension $n$ extension of $GF(q)$. The authors then show that many of the structure of fields between the finite field $GF(q)$ and its algebraic closure $\Gamma (q)$.

The authors introduce a notion, due to Steinitz, of an extended positive integer $N$ which of finite fields. The purpose of this book is to describe these generalizations. After an introductory chapter surveying pertinent results about finite fields, the book describes the lattice of finite fields. Despite the resurgence in interest, it is not widely known that many results concerning finite fields have natural generalizations to arbitrary algebraic extensions. In addition, a number of recent books have been written on topics related to finite fields.

Over the last several decades there has been a renewed interest in finite field theory, partly as a result of important applications in a number of diverse areas such as electronic communications, coding theory, combinatorics, designs, finite geometries, cryptography, and other portions of discrete mathematics. In this text only the basic theory of groups, rings and fields is required. The proof of 'Schur's Conjecture' is largely self-contained but is based on more advanced results like an estimate for the related rational function like Redei functions. Each of the seven chapters includes exercises and notes. Tables of Dickson polynomials are given in the Appendix. For most parts of the comprehensive up-to-date collection of results concerning Dickson polynomials and presents several applications. It also treats generalizations to polynomials in several variables and to 'Schur's conjecture' there are essentially no other examples. Dickson polynomials are also important in cryptology and for pseudoprimality testing. The book provides a comprehensive overview of the current state of the art in the theory of permutation polynomials and related topics. In particular, they serve as examples of integral polynomials which induce permutations for infinitely many primes. According to the authors, they have been developed over the last few decades and have various applications in different areas of mathematics. This book uniquely provides a necessary comprehensive coverage of bent functions, and discusses proofs of several results. This book uniquely provides a necessary comprehensive coverage of bent functions. It serves as a useful reference for researchers in discrete mathematics, coding and cryptography. Students and professors in mathematics and computer science will also find the content valuable, especially those interested in mathematical foundations of cryptography. It can be used as a supplementary text for university courses on discrete mathematics, algorithms, cryptography, and computer science.

Furthermore, the book contains a comprehensive bibliography and an index, making it a valuable resource for students, researchers, and educators in the field of finite fields and their applications. It is a valuable addition to the literature on finite fields, and is recommended for anyone interested in the subject.