Release: Special Issue on Combinatorics, Coding Theory and Cryptography

Science China-Mathematics will release in Vol. 56, No. 7, 2013 a special issue on Combinatorics, Coding Theory and Cryptography. This issue is organized and invited by Professors Keqin Feng (Tsinghua University, China), Qing Xiang (University of Delaware, USA) and Chaoping Xing (Nanyang Technological University, Singapore).

In this issue, 17 contributions are collected. As briefly reviewed in the following preface, they cover a wide range of areas within Combinatorics, Coding theory and Cryptography. If you are interested in the rapid growth and recent research in the relevant fields, please find this special issue at http://www.springerlink.com/content/1674-7283/

Contact

Editorial staff: Zhao Chai chaizhao@scichina.org

Preface: Combinatorics, Coding Theory and Cryptography

The present issue of Science China Mathematics is devoted to the themes of Combinatorics, Coding theory and Cryptography (C^3).

Combinatorics, coding theory and (modern) cryptography are relatively young as subjects of mathematics. These areas enjoyed tremendous growth in the second half of the twentieth century, and the trend shows no signs of abating. Moreover, the first decade of the twenty-first century also witnessed intensified interactions between these subjects. This special issue showcases some aspects of C^3 and connections among them. The purpose is two-fold. On the one hand, we want to introduce audience inside China to recent research in C^3 done by mathematicians outside China. On the other hand, we would like to increase awareness of the work in C^3 done by mathematicians residing in China. It is hoped that the special issue will stimulate cross-fertilization of ideas leading to new research collaborations and breakthroughs.

The editors selected seventeen contributions covering a wide range of areas within the aforementioned themes. Below we review these contributions briefly.

Maarten de Boeck and Leo Storme give a survey of Erdös-Ko-Rado type theorems in geometric settings.

Claude Carlet studies further the menthod of concatenating the outputs to two functions for designing an APN or a differentially 4-uniform (n,n)-function for every even n.

Yu Chen, Liqun Chen, and Dongdai Lin present a new proof of the Boneh-Franklin identity-based encryption scheme.

Tao Feng, Ka Hing Leung and Qing Xiang make some progress towards a well-known conjecture on

the minimum weights of binary cyclic codes with two primitive nonzeros.

Fangwei Fu and Zhihan Gao study the relations between linear recurring sequences and subfield subcodes and derive Delsarte's theorem with the help of the theory of linear recurrence sequences.

Ming-Deh Huang investigates the discrete logarithm problem from a local duality perspective.

Wenjie Jia, Xiangyong Zeng, Chunlei Li, Tor Helleseth and Lei Hu propose a construction of functions with low differential uniformity based on known perfect nonlinear functions over finite fields of odd characteristic.

Li Kang and Xiaohu Tang investigate a generic construction of low correlation zone sequences based on interleaved technique.

Gábor Korchmáros studies lower bounds on minimum distance of Hermtian differential codes.

Jin Li, Shixin Zhu and Keqin Feng present explicit evaluations of Gauss sums and Jacobi sums over Galois ring GR(p^2,r).

Harald Niederreiter and Anderson Yeo introduce a direct construction of Halton-type low-discrepancy sequences from function fields.

Enver Ozdemir describes how to use singular hyperelliptic curves for the primality test.

Carles Padró and Ronald Cramer give a survey on algebraic manipulation detection codes.

Longjiang Qu, Chao Li, Qingping Dai and Zhiyin Kong discuss possible values of differential uniformity of certain function over finite fields.

Peter Sin surveys recent work on Smith normal forms of incidence matrices arising from association schemes, finite geometries and combinatorial designs.

Jing Yang and Lingli Xia explicitly determine the cyclotomic numbers of order l and $2l$, for odd prime l, over finite field $\mathbb{F}_q$ in the index 2 case, utilizing the explicit formulas on the corresponding Gauss sums.

Liwei Zeng, Zhao Chai, Rongquan Feng, and Changli Ma introduce the generalized symplectic graph, and determine its the full automorphism group.

We warmly thank all authors and reviewers for contributing to this special issue. Especially we thank the editorial staff, Zhao Chai, for her continual encouragement and support.

Guest Editors:
Keqin Feng
Qing Xiang
Chaoping Xing

http://www.springer.com/journal/11425

Science China Mathematics
Editor-in-Chief: Yuan, Y.-X. - Editorial Director: Yang, Z.
ISSN: 1674-7283 (print version)
ISSN: 1869-1862 (electronic version)
Journal no. 11425