

*Commenced Publication in 1973*

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

## Editorial Board

David Hutchison

*Lancaster University, UK*

Takeo Kanade

*Carnegie Mellon University, Pittsburgh, PA, USA*

Josef Kittler

*University of Surrey, Guildford, UK*

Jon M. Kleinberg

*Cornell University, Ithaca, NY, USA*

Friedemann Mattern

*ETH Zurich, Switzerland*

John C. Mitchell

*Stanford University, CA, USA*

Moni Naor

*Weizmann Institute of Science, Rehovot, Israel*

Oscar Nierstrasz

*University of Bern, Switzerland*

C. Pandu Rangan

*Indian Institute of Technology, Madras, India*

Bernhard Steffen

*University of Dortmund, Germany*

Madhu Sudan

*Massachusetts Institute of Technology, MA, USA*

Demetri Terzopoulos

*University of California, Los Angeles, CA, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

Moshe Y. Vardi

*Rice University, Houston, TX, USA*

Gerhard Weikum

*Max-Planck Institute of Computer Science, Saarbruecken, Germany*

Guang Gong Tor Hellesest  
Hong-Yeop Song Kyeongcheol Yang (Eds.)

# Sequences and Their Applications – SETA 2006

4th International Conference  
Beijing, China, September 24-28, 2006  
Proceedings

## Volume Editors

Guang Gong  
University of Waterloo  
Department of Electrical and Computer Engineering  
200 University Avenue West, Waterloo, ON, N2L 3G1, Canada  
E-mail: ggong@calliope.uwaterloo.ca

Tor Helleseth  
University of Bergen  
Department of Informatics  
Thormohlensgate 55, 5020 Bergen, Norway  
E-mail: tor.helleseth@ii.uib.no

Hong-Yeop Song  
Center for Information Technology of Yonsei University  
School of Electrical and Electronics Engineering  
Seoul, 120-749, Korea  
E-mail: hy.song@coding.yonsei.ac.kr

Kyeongcheol Yang  
Pohang University of Science and Technology (POSTECH)  
Dept. of Electronic and Electrical Engineering  
Pohang, Gyungbuk 790-784, Korea  
E-mail: kcyang@postech.ac.kr

Library of Congress Control Number: 2006932045

CR Subject Classification (1998): E.4, F.2, I.1, E.3, F.1, G.1

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

ISSN	0302-9743
ISBN-10	3-540-44523-4 Springer Berlin Heidelberg New York
ISBN-13	978-3-540-44523-4 Springer Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media  
springer.com

© Springer-Verlag Berlin Heidelberg 2006  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India  
Printed on acid-free paper SPIN: 11863854 06/3142 5 4 3 2 1 0

# Preface

This volume contains the refereed proceedings of the Fourth International Conference on Sequences and Their Applications (SETA 2006), held in Beijing, China during September 24–28, 2006. The previous three conferences SETA '98, SETA 2001, and SETA 2004 were held in Singapore, Bergen, and Seoul, respectively. The SETA conferences are motivated by the numerous applications of sequences in modern communication systems. These applications include pseudorandom sequences in spread spectrum, code-division-multiple-access, stream ciphers in cryptography, and several connections to coding theory and boolean functions.

The Technical Program Committee of SETA 2006 refereed 70 submitted papers. This represented more submissions than to any of the previous SETA conferences. The committee therefore had the challenging task of selecting 32 papers to be presented at the conference in addition to 4 invited papers.

The Co-chairs of the Technical Program Committee for SETA 2006, were Guang Gong (University of Waterloo) and Tor Helleseth (University of Bergen), with Hong-Yeop Song (Yonsei University, Korea) and Kyeongcheol Yang (Pohang University of Science and Technology, Korea) as the co-editors for these proceedings.

The editors wish to thank the other members of the Technical Program Committee: Anne Canteaut (INRIA, France), Claude Carlet (INRIA and University of Paris 8, France), Habong Chung, (Hongik University, Korea), Zongduo Dai (University of Science and Technology of China, Beijing, China), Cunsheng Ding (Hong Kong University of Science and Technology, Hong Kong), Pingzhi Fan (Southwest Jiaotong University, China), Dengguo Feng (Chinese Academy of Sciences, China), Solomon W. Golomb (University of Southern California, USA), Kyoki Imamura (Kyushu Institute of Technology, Japan), Jonathan Jedwab (Simon Fraser University, Canada), Thomas Johansson (University of Lund, Sweden), Andrew Klapper (University of Kentucky, USA), P. Vijay Kumar (University of Southern California, USA), Wai Ho Mow (Hong Kong University of Science and Technology, Hong Kong), Harald Niederreiter (National University of Singapore, Singapore), Jong-Seon No (Seoul National University, Korea), Matthew G. Parker (University of Bergen, Norway), Kenneth G. Paterson (Royal Holloway, University of London, UK), Alexander Pott (Otto-von-Guericke-University Magdeburg, Germany), Hans Schotten (Qualcomm Germany, Nuremberg, Germany), Parampalli Udaya (University of Melbourne, Australia), and Amr Youssef (Concordia University, Canada) for providing clear, insightful, and prompt reviews of the submitted papers.

The editors are also grateful to Serdar Boztas, Jin-Ho Chung, Deepak Kumar Dalai, Frédéric Didier, Gary Greenfield, Yun-Kyoung Han, Tom Høholdt, Alexander Kholosha, Margreta Kuijper, Gohar Kyureghyan, Cedric Lauradoux, Subhamoy Maitra, Joe Rushanan, Frank Ruskey, Igor Semaev, Jean-Pierre

Tillich, and Nam Yul Yu for their help and assistance in the reviewing of papers for SETA 2006. A special thanks goes to Sondre Rønjom for handling all the submissions and the web-review software during the review process.

In addition to the contributed papers, there are four invited papers. These papers provide a historical overview as well as new developments in important areas of the design and analysis of sequences. The invited contribution by Solomon Golomb presents a retro-perspective of some selected results on sequences. The invited paper by Harald Niederreiter includes an updated overview and some recent important results on the complexity of multisequences. Vijay Kumar provides an overview and new results on optical orthogonal codes. This topic is motivated by applying code division multiple access (CDMA) techniques in optical networks. Zongduo Dai presents an overview of multi-continued fraction algorithms and their applications to sequences.

We wish to thank Pingzhi Fan and Dengguo Feng for their support as General Co-chairs of SETA 2006, and Chuan-Kun Wu for local arrangements and updating the web site of SETA '06. We also thank Yi Qin for her support as secretary of SETA 2006, and Shi Zhang for her support as treasurer of SETA 2006. Last but not least, we thank all the authors of the papers for their help and collaboration in preparing this volume. Finally, we would like to thank the National Science Foundation of China (NSFC) and the Chinese Academy of Sciences (CAS) for their financial support.

September 2006

Guang Gong  
Tor Helleseeth  
Hong-Yeop Song  
Kyeongcheol Yang

# Organization

## SETA 2006

September 24-28, 2006, Beijing, China

### General Co-chairs

Pingzhi Fan, Southwest Jiaotong University, China  
Dengguo Feng, Chinese Academy of Sciences, China

### Program Co-chairs

Guang Gong, University of Waterloo, Canada  
Tor Helleseth, University of Bergen, Norway

### Local Arrangements

Chuan-Kun Wu, Chinese Academy of Sciences, China

### Secretary and Registration

Yi Qin, Chinese Academy of Sciences, China

### Treasurer

Shi Zhang, Chinese Academy of Sciences, China

### Proceedings Co-editors

Guang Gong, University of Waterloo, Canada  
Tor Helleseth, University of Bergen, Norway  
Hong-Yeop Song, Yonsei University, Korea  
Kyeongcheol Yang, Pohang Univ. of Science and Technology, Korea

## Technical Program Committee for SETA 2006

### Program Co-chairs

Guang Gong ..... University of Waterloo, Canada  
Tor Helleseth ..... University of Bergen, Norway

### Program Committee

Anne Canteaut ..... INRIA, France  
Claude Carlet ..... INRIA and University of Paris 8, France  
Habong Chung ..... Hongik University, Korea  
Zongduo Dai ..... University of Science and Technology of China, China  
Cunsheng Ding ..... Hong Kong University of Science and Technology, China  
Pingzhi Fan ..... Southwest Jiaotong University, China  
Dengguo Feng ..... Chinese Academy of Sciences, China  
Solomon W. Golomb ..... University of Southern California, USA  
Kyoki Imamura ..... Kyushu Institute of Technology, Japan  
Jonathan Jedwab ..... Simon Fraser University, Canada  
Thomas Johansson ..... University of Lund, Sweden  
Andrew Klapper ..... University of Kentucky, USA  
P. Vijay Kumar ..... University of Southern California, USA  
Wai Ho Mow ..... Hong Kong University of Science and Technology, China  
Harald Niederreiter ..... National University of Singapore, Singapore  
Jong-Seon No ..... Seoul National University, Korea  
Matthew G. Parker ..... University of Bergen, Norway  
Kenneth G. Paterson ..... Royal Holloway, University of London, UK  
Alexander Pott ..... Otto-von-Guericke University Magdeburg, Germany  
Hans Schotten ..... Qualcomm Germany, Germany  
Hong-Yeop Song ..... Yonsei University, Korea  
Parampalli Udaya ..... University of Melbourne, Australia  
Kyeongcheol Yang ..... Pohang University of Science and Technology, Korea  
Amr Youssef ..... Concordia University, Canada

# Table of Contents

## Invited Papers

Shift Register Sequences – A Retrospective Account . . . . .	1
<i>Solomon W. Golomb</i>	
The Probabilistic Theory of the Joint Linear Complexity of Multisequences . . . . .	5
<i>Harald Niederreiter</i>	
Multi-Continued Fraction Algorithms and Their Applications to Sequences . . . . .	17
<i>Zongduo Dai</i>	
Codes for Optical CDMA . . . . .	34
<i>Reza Omrani, P. Vijay Kumar</i>	

## Linear Complexity of Sequences

On the Linear Complexity of Sidel'nikov Sequences over $\mathbb{F}_d$ . . . . .	47
<i>Nina Brandstätter, Wilfried Meidl</i>	
Linear Complexity over $F_p$ of Ternary Sidel'nikov Sequences . . . . .	61
<i>Young-Sik Kim, Jung-Soo Chung, Jong-Seon No, Habong Chung</i>	
Bounds on the Linear Complexity and the 1-Error Linear Complexity over $F_p$ of $M$ -ary Sidel'nikov Sequences . . . . .	74
<i>Jin-Ho Chung, Kyeongcheol Yang</i>	
The Characterization of $2^n$ -Periodic Binary Sequences with Fixed 1-Error Linear Complexity . . . . .	88
<i>Fang-Wei Fu, Harald Niederreiter, Ming Su</i>	

## Correlation of Sequences

Crosscorrelation Properties of Binary Sequences with Ideal Two-Level Autocorrelation . . . . .	104
<i>Nam Yul Yu, Guang Gong</i>	
Extended Hadamard Equivalence . . . . .	119
<i>Doreen Hertel</i>	



Analysis of Designing Interleaved ZCZ Sequence Families .....	129
<i>Jin-Song Wang, Wen-Feng Qi</i>	

## Stream Ciphers and Transforms

Security of Jump Controlled Sequence Generators for Stream Ciphers .....	141
<i>Tor Helleseth, Cees J.A. Jansen, Shahram Khazaei, Alexander Kholosha</i>	

Improved Rijndael-Like S-Box and Its Transform Domain Analysis .....	153
<i>Seok-Yong Jin, Jong-Min Baek, Hong-Yeop Song</i>	

## Topics in Complexities of Sequences

Nonlinear Complexity of Binary Sequences and Connections with Lempel-Ziv Compression .....	168
<i>Konstantinos Limniotis, Nicholas Kolokotronis, Nicholas Kalouptsidis</i>	

On Lempel-Ziv Complexity of Sequences .....	180
<i>Ali Doğanaksoy, Faruk Göloğlu</i>	

Computing the $k$ -Error $N$ -Adic Complexity of a Sequence of Period $p^n$ .....	190
<i>Lihua Dong, Yupu Hu, Yong Zeng</i>	

On the Expected Value of the Joint 2-Adic Complexity of Periodic Binary Multisequences .....	199
<i>Honggang Hu, Lei Hu, Dengguo Feng</i>	

## Linear/Nonlinear Feedback Shift Register Sequences

On the Classification of Periodic Binary Sequences into Nonlinear Complexity Classes .....	209
<i>George Petrides, Johannes Mykkeltveit</i>	

Sequences of Period $2^N - 2$ .....	223
<i>Rainer Göttfert</i>	

A New Algorithm to Compute Remote Terms in Special Types of Characteristic Sequences .....	237
<i>Kenneth J. Giuliani, Guang Gong</i>	

## Multi-sequence Synthesis

Implementation of Multi-continued Fraction Algorithm and Application to Multi-sequence Linear Synthesis .....	248
<i>Quanlong Wang, Kunpeng Wang, Zongduo Dai</i>	

The Hausdorff Dimension of the Set of $r$ -Perfect $M$ -Multisequences .....	259
<i>Michael Vielhaber, Mónica del Pilar Canales Ch.</i>	

## Filtering Sequences and Pseudorandom Sequence Generators

Lower Bounds on Sequence Complexity Via Generalised Vandermonde Determinants .....	271
<i>Nicholas Kolokotronis, Konstantinos Limniotis, Nicholas Kalouptsidis</i>	

Construction of Pseudo-random Binary Sequences from Elliptic Curves by Using Discrete Logarithm .....	285
<i>Zhixiong Chen, Shengqiang Li, Guozhen Xiao</i>	

On the Discrepancy and Linear Complexity of Some Counter-Dependent Recurrence Sequences .....	295
<i>Igor E. Shparlinski, Arne Winterhof</i>	

## Sequences and Combinatorics

Nonexistence of a Kind of Generalized Perfect Binary Array .....	304
<i>Zhang Xiyong, Guo Hua, Han Wenbao</i>	

## FCSR Sequences

On the Distinctness of Decimations of Generalized $l$ -Sequences .....	313
<i>Hong Xu, Wen-Feng Qi</i>	

On FCSR Memory Sequences .....	323
<i>Tian Tian, Wen-Feng Qi</i>	

Periodicity and Distribution Properties of Combined FCSR Sequences .....	334
<i>Mark Goresky, Andrew Klapper</i>	

## Aperiodic Correlation and Applications

Generalized Bounds on Partial Aperiodic Correlation of Complex Roots of Unity Sequences .....	342
<i>Lifang Feng, Pingzhi Fan</i>	

Chip-Asynchronous Version of Welch Bound: Gaussian Pulse Improves BER Performance .....	351
<i>Yutaka Jitsumatsu, Tohru Kohda</i>	

## Boolean Functions

On Immunity Profile of Boolean Functions .....	364
<i>Claude Carlet, Philippe Guillot, Sihem Mesnager</i>	

Reducing the Number of Homogeneous Linear Equations in Finding Annihilators .....	376
<i>Deepak Kumar Dalai, Subhamoy Maitra</i>	

The Algebraic Normal Form, Linear Complexity and k-Error Linear Complexity of Single-Cycle T-Function .....	391
<i>Wenyong Zhang, Chuan-Kun Wu</i>	

Partially Perfect Nonlinear Functions and a Construction of Cryptographic Boolean Functions .....	402
<i>Lei Hu, Xiangyong Zeng</i>	

Construction of 1-Resilient Boolean Functions with Very Good Nonlinearity .....	417
<i>Soumen Maity, Chrisil Arackaparambil, Kezhasono Meyase</i>	

<b>Author Index</b> .....	433
---------------------------	-----