Preface

This volume contains the refereed proceedings of the 3rd International Conference on Sequences and Their Applications (SETA 2004), held in Seoul, Korea during October 24–28, 2004. The previous two conferences, SETA 1998 and SETA 2001, were held in Singapore and Bergen, Norway, respectively. These conferences are motivated by the many widespread applications of sequences in modern communication systems. These applications include pseudorandom sequences in spread spectrum systems, code-division multiple-access, stream ciphers in cryptography and several connections to coding theory.

The Technical Program Committee of SETA 2004 received 59 submitted papers, many more than the submissions to previous SETA conferences. The Committee therefore had the difficult task of selecting the 33 papers to be presented at the Conference in addition to four invited papers. The authors of papers presented at the conference were invited to submit full papers that were refereed before appearing in this proceedings.

These proceedings have been edited by the Co-chairs of the Technical Program Committee for SETA 2004: Tor Helleseth of the University of Bergen, Norway, and Dilip Sarwate of the University of Illinois at Urbana-Champaign, USA, and Technical Program Committee members Hong-Yeop Song of Yonsei University, Korea, and Kyeongcheol Yang of Pohang University of Science and Technology, Korea. The editors wish to thank the other members of the Technical Program Committee: Serdar Boztas (Royal Melbourne Institute of Technology, Australia), Claude Carlet (INRIA and University of Paris 8, France), Zongduo Dai (University of Science and Technology of China, Beijing, China), Cunsheng Ding (Hong Kong University of Science and Technology, Hong Kong, China), Hans Dobbertin (Ruhr University Bochum, Germany), Pingzhi Fan (Southwest Jiaotong University, China), Solomon W. Golomb (University of Southern California, USA), Guang Gong (University of Waterloo, Canada), Tom Høholdt (Technical University of Denmark, Denmark), Andrew Klapper (University of Kentucky, USA), P. Vijay Kumar (University of Southern California, USA), Vladimir Levenshtein (Keldysh Institute of Applied Mathematics, Russia), Oscar Moreno (University of Puerto Rico, Puerto Rico), Harald Niederreiter (National University of Singapore, Singapore), Matthew Parker (University of Bergen, Norway), Kenneth G. Paterson (Royal Holloway, University of London, UK), Aleksander Pott (Otto von Guericke University Magdeburg, Germany), Hans Schotten (Qualcomm CDMA Technologies, Nürnberg, Germany), Patrick Sole (CNRS-I3S, ESSI, Sophia Antipolis, France), Naoki Suehiro (University of Tsukuba, Japan) for providing clear, insightful, and prompt reviews of the submitted papers.

In addition to the contributed papers, there were four invited papers. These papers provide an overview of new developments in some important areas related
to sequences. The invited papers by Jedwab and by Parker both include an updated overview and some recent results on the constructions of some exciting new families of sequences with a merit factor more than 6.3. Klapper gives an overview of the fascinating topic of feedback with carry shift registers, while Dobbertin and Leander present new and recent results on bent functions.

We wish to thank Jong-Seon No and Habong Chung for their support as General Co-chairs of SETA 2004; Dong-Joon Shin, Wonjin Sung and Jun Heo for their support as members of the Organizing Committee of SETA 2004. Last but not least, we thank all the authors of the papers presented at SETA 2004 for their help in making this conference a resounding success. Finally, we also thank the Korea Research Foundation (KTF) for its financial support.

March, 2005

Tor Helleseth
Dilip Sarwate
Hong-Yeop Song
Keongcheol Yang
Organization

SETA 2004
October 24–28, 2004, Seoul, Korea

General Co-chairs
Jong-Seon No, Seoul National University, Korea
Habong Chung, Hongik University, Korea

Program Co-chairs
Tor Helleseth, University of Bergen, Norway
Dilip Sarwate, University of Illinois at Urbana-Champaign, USA

Secretary and Treasury
Dong-Joon Shin, Hanyang University, Korea

Local Arrangements
Wonjin Sung, Sogang University, Korea

Registration
Jun Heo, Konkuk University, Korea

Publication Co-editors
Hong-Yeop Song, Yonsei University, Korea
Kyeongcheol Yang, POSTECH, Korea
Technical Program Committee for SETA 2004

Program Co-chairs
Tor Helleseth ......................................................... University of Bergen, Norway
Dilip Sarwate .......................... University of Illinois at Urbana-Champaign, USA

Program Committee
Serdar Boztas ........................................................ RMIT University, Australia
Claude Carlet ....................................................... INRIA and University of Paris 8, France
Zongduo Dai ......... University of Science and Technology of China, Beijing, China
Cunsheng Ding ... Hong Kong University of Science and Technology, Hong Kong, China
Hans Dobbertin ........................................ Ruhr University Bochum, Germany
Pingzhi Fan ............................................. Southwest Jiaotong University, China
Solomon W. Golomb ................................ University of Southern California, USA
Guang Gong ......................................................... University of Waterloo, Canada
Tom Høholdt ........................................... Technical University of Denmark, Denmark
Andrew Klapper ............................................... University of Kentucky, USA
P. Vijay Kumar ........................................ University of Southern California, USA
Vladimir Levenshtein ........ Keldysh Institute of Applied Mathematics, Russia
Oscar Moreno .......................................... University of Puerto Rico, Puerto Rico
Harald Niederreiter ........................ National University of Singapore, Singapore
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 CDMA Technologies, Nürnberg, Germany
Patrick Solé ................................. CNRS-I3S, ESSI, Sophia Antipolis, France
Hong-Yeop Song ................................. Yonsei University, Korea
Naoki Suehiro ........................................ University of Tsukuba, Japan
Kyeongcheol Yang .......................... Pohang University of Science and Technology, Korea
# Table of Contents

## Invited Papers

A Survey of Some Recent Results on Bent Functions  
*Hans Dobbertin, Gregor Leander*  .................................................. 1

A Survey of the Merit Factor Problem for Binary Sequences  
*Jonathan Jedwab*  ........................................................................... 30

A Survey of Feedback with Carry Shift Registers  
*Andrew Klapper*  ........................................................................... 56

Univariate and Multivariate Merit Factors  
*Matthew G. Parker*  ........................................................................ 72

## Complexity of Sequences I

Discrete Fourier Transform, Joint Linear Complexity and Generalized  
Joint Linear Complexity of Multisequences  
*Wilfried Meidl*  ................................................................................ 101

Expected Value of the Linear Complexity of Two-Dimensional Binary Sequences  
*Xiutao Feng, Zongduo Dai*  ............................................................... 113

Asymptotic Behavior of Normalized Linear Complexity of  
Multi-sequences  
*Zongduo Dai, Kyoki Imamura, Junhui Yang*  .............................. 129

A Unified View on Sequence Complexity Measures as Isometries  
*Michael Vielhaber*  ........................................................................ 143

## Complexity of Sequences II

One-Error Linear Complexity over $F_p$ of Sidelnikov Sequences  
*Yu-Chang Eun, Hong-Yeop Song, Gohar M. Kyureghyan*  ............. 154

On the Generalized Lauder-Paterson Algorithm and Profiles of the $k$-Error Linear Complexity for Exponent Periodic Sequences  
*Takayasu Kaida*  ............................................................................... 166
### Table of Contents

On the Computation of the Linear Complexity and the $k$-error Linear Complexity of Binary Sequences with Period a Power of Two  
*Ana Sălăgean* .................................................. 179

On the 2-Adic Complexity and the $k$-Error 2-Adic Complexity of Periodic Binary Sequences  
*Honggang Hu, Dengguo Feng* ..................................... 185

**Perfect Sequences**

Almost-Perfect and Odd-Perfect Ternary Sequences  
*Evgeny I. Krengel* .................................................. 197

Cross-Correlation Properties of Perfect Binary Sequences  
*Doreen Hertel* ........................................................ 208

**Sequence Constructions**

New Sets of Binary and Ternary Sequences with Low Correlation  
*Evgeny I. Krengel, Andrew Z. Tirkel, Tom E. Hall* ............... 220

Improved $p$-ary Codes and Sequence Families from Galois Rings  
*San Ling, Ferruh Özbudak* ........................................... 236

Quadriphase Sequences Obtained from Binary Quadratic Form Sequences  
*Xiaohu Tang, Parampalli Udaya, Pingzhi Fan* ...................... 243

New Families of $p$-Ary Sequences from Quadratic Form with Low Correlation and Large Linear Span  
*Xiaohu Tang, Parampalli Udaya, Pingzhi Fan* ...................... 255

**Sequences over $\mathbb{Z}_m$**

On the Distribution of Some New Explicit Nonlinear Congruential Pseudorandom Numbers  
*Harald Niederreiter, Arne Winterhof* ............................... 266

Distribution of $r$-Patterns in the Most Significant Bit of a Maximum Length Sequence over $\mathbb{Z}_2^t$  
*Patrick Solé, Dmitrii Zinoviev* ..................................... 275
# Table of Contents

## Sequence Generator Properties and Applications

- Algebraic Feedback Shift Registers Based on Function Fields  
  *Andrew Klapper* ................................................................. 282
- New LFSR-Based Cryptosystems and the Trace Discrete Log Problem  
  *(Trace-DLP)*  
  *Kenneth J. Giuliani, Guang Gong* ........................................ 298
- Cryptanalysis of a Particular Case of Klimov-Shamir Pseudo-Random Generator  
  *Vincent Bénony, François Recher, Éric Wegrzynowski, Caroline Fontaine* ..................................................... 313
- Generating Functions Associated with Random Binary Sequences Consisting of Runs of Lengths 1 and 2  
  *Vladimir B. Balakirsky* ....................................................... 323

## Multi-dimensional Sequences

- Multi-continued Fraction Algorithm and Generalized B-M Algorithm over $F_2$  
  *Zongduo Dai, Xiutao Feng, Junhui Yang* ................................. 339
- A New Search for Optimal Binary Arrays with Minimum Peak Sidelobe Levels  
  *Gummadi S. Ramakrishna, Wai Ho Mow* .................................... 355
- New Constructions of Quaternary Hadamard Matrices  
  *Ji-Woong Jang, Sang-Hyo Kim, Jong-Seon No, Habong Chung* ............ 361
- Spectral Orbits and Peak-to-Average Power Ratio of Boolean Functions with Respect to the $\{I, H, N\}^n$ Transform  
  *Lars Eirik Danielsen, Matthew G. Parker* .................................. 373

## Optics and OFDM Applications

- New Constructions and Bounds for 2-D Optical Orthogonal Codes  
  *Reza Omrani, Petros Elia, P. Vijay Kumar* ................................. 389
- Topics on Optical Orthogonal Codes  
  *Reza Omrani, Oscar Moreno, P. Vijay Kumar* ............................. 396
Weighted Degree Trace Codes for PAPR Reduction
  *Patrick Solé, Dmitrii Zinoviev* ........................................ 406

**Polynomials and Functions**

Which Irreducible Polynomials Divide Trinomials over GF(2)?
  *Solomon W. Golomb, Pey-Feng Lee* ..................................... 414

Autocorrelation Properties of Resilient Functions and Three-Valued Almost-Optimal Functions Satisfying PC($p$)
  *Seunghoon Choi, Kyeongcheol Yang* ..................................... 425

Group Algebras and Correlation Immune Functions
  *Alexander Pott* .............................................................. 437

**Author Index** .............................................................. 451