# Lecture Notes in Computer Science 4893

*Commenced Publication in 1973*
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Solomon W. Golomb Guang Gong
Tor Helleseth Hong-Yeop Song (Eds.)

# Sequences, Subsequences, and Consequences

International Workshop, SSC 2007
Los Angeles, CA, USA, May 31 - June 2, 2007
Revised Invited Papers

Springer

Volume Editors

Solomon W. Golomb
University of Southern California, Department of EE-Systems
Los Angeles, CA 90089-2565, USA
E-mail: sgolomb@usc.edu

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

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

Hong-Yeop Song
Yonsei University, School of Electrical and Electronic Engineering
134 Sinchon-dong Seodaemun-gu, Seoul, 120-749, Korea
E-mail: hysong@yonsei.ac.kr

Library of Congress Control Number: 2007941501

CR Subject Classification (1998): E.3-4, G.2, F.2.2, C.2, J.1

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-77403-3 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-77403-7 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springer.com

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12208166 06/3180 5 4 3 2 1 0

Dedicated to
Professor Solomon W. Golomb
on his 75th Birthday

# Preface

These are the proceedings of the Workshop on Sequences, Subsequences, and Consequences that was held at the University of Southern California (USC), May 31 - June 2, 2007. There were three one-hour Keynote lectures, 16 invited talks of up to 45 minutes each, and 1 "contributed" paper.

The theory of sequences from discrete symbol alphabets has found practical applications in many areas of coded communications and in cryptography, including: signal patterns for use in radar and sonar; spectral spreading sequences for CDMA wireless telephony; key streams for direct sequence stream-cipher cryptography; and a variety of forward-error-correcting codes.

The workshop was designed to bring leading researchers on "sequences" from around the world to present their latest results, interchange information with one another, and especially to inform the larger audience of interested participants, including faculty, researchers, scholars, and students from numerous institutions, as well as the readers of these proceedings, about recent developments in this important field.

There were invited speakers from Canada, China, Germany, India, Israel, Norway, Puerto Rico, and South Korea, in addition to those from the USA. Support for the workshop was generously provided by the Office of the Dean of the Viterbi School of Engineering, by the Center for Communications Research (CCR-La Jolla), and by the United States National Science Foundation (NSF). This support is hereby gratefully acknowledged.

As the principal organizers of the workshop and its technical program, we wish to thank the speakers, all the participants, and the above-mentioned organizations that provided funding. Our special thanks go to Milly Montenegro, Gerrielyn Ramos, and Mayumi Thrasher at USC for all the arrangements before, during, and after the workshop, and for their considerable help, along with Xinxin Fan and Honggang Hu at the University of Waterloo (Canada) and Young-Joon Kim at Yonsei University (South Korea), in preparing, typing, and formatting many of the manuscripts.

September 2007

Solomon W. Golomb
Guang Gong
Tor Helleseth
Hong-Yeop Song

# Organization

## Technical Program Committee for SSC 2007

## Principal Organizers

| | |
|---|---|
| Solomon Golomb | University of Southern California, USA |
| Guang Gong | University of Waterloo, Canada |
| Tor Helleseth | University of Bergen, Norway |
| Hong-Yeop Song | Yonsei University, Korea |

## Program Committee

| | |
|---|---|
| Tuvi Etzion | Technion IIT, Israel |
| Solomon W. Golomb | University of Southern California, USA |
| Guang Gong | University of Waterloo, Canada |
| Alfred W. Hales | CCR-La Jolla, USA |
| Tor Helleseth | University of Bergen, Norway |
| Alexander Kholosha | University of Bergen, Norway |
| Andrew Klapper | University of Kentucky, USA |
| P. Vijay Kumar | University of Southern California, USA, and IISc Bangalore |
| Robert McEliece | California Institute of Technology, USA |
| Lothrop Mittenthal | Teledyne, USA |
| Oscar Moreno | University of Puerto Rico, Puerto Rico |
| Alexander Pott | Otto von Guericke University Magdeburg, Germany |
| Hong-Yeop Song | Yonsei University, Korea |
| Xiaohu Tang | Southwest Jiao Tong University, China |
| Herbert Taylor | South Pasadena, USA |
| Andrew J. Viterbi | Viterbi Group, LLC, USA |
| Steven Wang | University of Carleton, Canada |
| Lloyd R. Welch | University of Southern California, USA |
| Nam Yul Yu | University of Waterloo, Canada |

## Sponsoring Institutions

University of Southern California, CCR-La Jolla, NSF

# Table of Contents