Lecture Notes in Computer Science 829
Edited by G. Goos and J. Hartmanis

Advisory Board: W. Brauer D. Gries J. Stoer

Andrew Chmora Stephen B. Wicker (Eds.)

Error Control, Cryptology, and Speech Compression

Workshop on Information Protection
Moscow, Russia, December 6-9, 1993
Selected Papers

Springer-Verlag
Berlin Heidelberg New York
London Paris Tokyo
Hong Kong Barcelona
Budapest

Series Editors

Gerhard Goos
Universität Karlsruhe
Postfach 69 80
Vincenz-Priessnitz-Straße 1
D-76131 Karlsruhe, Germany

Juris Hartmanis
Cornell University
Department of Computer Science
4130 Upson Hall
Ithaca, NY 14853, USA

Volume Editors

Andrew Chmora
Institute for Information Transmission Problems
19 Yermolovoy St., Moscow 101447 GSP-4 Russia

Stephen B. Wicker
Georgia Institute of Technology, School of Electrical and Computer Engineering
Atlanta, Georgia 30332, USA

CR Subject Classification (1991): E.3-4

ISBN 3-540-58265-7 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-58265-7 Springer-Verlag New York Berlin Heidelberg

CIP data applied for

Printed in Germany

Typesetting: Camera-ready by author
SPIN: 10472623 45/3140-543210 - Printed on acid-free paper

Preface

This book contains selected papers from the Workshop on Information Protection held in Moscow, Russia, on December 6–9, 1993. The Workshop gathered nearly 50 participants. This was possible due to the generous support and enthusiastic encouragement of the Russian Chapter of the IEEE Information Theory Society and the Institute for Information Transmission Problems of the Russian Academy of Sciences. This support is gratefully acknowledged by the Workshop Organizing Committee and the Editors of this volume.

This Workshop was the first open conference in Russia devoted mostly to cryptography and authentication. However, we note that the users of communication systems need various forms of protection for their transmitted data. Therefore, another important direction covered by the Workshop was the protection of information from errors. Another reason for this choice of topics is that both cryptology and error-control coding often employ common theoretical tools. The Organizing Committee hopes that workshops devoted to this joint research area will become traditional.

The papers have been revised and updated by the authors and editors. They are organized in three sections: Cryptology, Error-Control Coding, and Speech Compression.

The papers in the first section are concerned with the following problems of cryptology: algebraic aspects of key generation systems, the susceptibility of digital signature schemes based on error-correcting codes to universal forgery, message protection in cryptosystems modelled as the generalized wire-tap channel II, the avoidance of the Sidel'nikov-Shestakov attack, and a linear algebraic approach to secret sharing schemes.

The second section is devoted to error-control codes. Among the problems covered in this volume are generalizations of the Griesmer bound, coverings for decoding by S-sets, the periodicity of one-dimensional tilings, codes that can correct two-dimensional bursts, self-checking decoding algorithms for Reed-Solomon codes, an interesting construction of unit memory and partial unit memory codes including optimal nonlinear codes, a construction of concatenated codes based on convolutional codes as outer and inner codes, and the investigation of trellis coded modulation for nonlinear channels with intersymbol interference.

The final section is concerned with digital transmission of speech. The first paper considers the problem of reducing the number of multiplications in infinite response filtering. The second paper demonstrates a method for using trellis codes in linear predictive speech compression.

The editors are most grateful to all the authors for their hard work in preparing, presenting, and revising their papers. Without the dedication and enthusiasm of the authors the Workshop itself would not have been possible, let alone this book. Special thanks should be expressed to Professor Stephen B. Wicker, whose intensive support made the appearance of this volume possible.

Victor Zyablov, Chairman of Organizing Committee.

Table of Contents

Cryptology

Error Control Coding

Speech Compression