

ENHANCING CRYPTOGRAPHIC PRIMITIVES WITH
TECHNIQUES FROM ERROR CORRECTING CODES

NATO Science for Peace and Security Series

This Series presents the results of scientific meetings supported under the NATO Programme: Science for Peace and Security (SPS).

The NATO SPS Programme supports meetings in the following Key Priority areas: (1) Defence Against Terrorism; (2) Countering other Threats to Security and (3) NATO, Partner and Mediterranean Dialogue Country Priorities. The types of meeting supported are generally “Advanced Study Institutes” and “Advanced Research Workshops”. The NATO SPS Series collects together the results of these meetings. The meetings are co-organized by scientists from NATO countries and scientists from NATO’s “Partner” or “Mediterranean Dialogue” countries. The observations and recommendations made at the meetings, as well as the contents of the volumes in the Series, reflect those of participants and contributors only; they should not necessarily be regarded as reflecting NATO views or policy.

Advanced Study Institutes (ASI) are high-level tutorial courses to convey the latest developments in a subject to an advanced-level audience.

Advanced Research Workshops (ARW) are expert meetings where an intense but informal exchange of views at the frontiers of a subject aims at identifying directions for future action.

Following a transformation of the programme in 2006 the Series has been re-named and re-organised. Recent volumes on topics not related to security, which result from meetings supported under the programme earlier, may be found in the NATO Science Series.

The Series is published by IOS Press, Amsterdam, and Springer Science and Business Media, Dordrecht, in conjunction with the NATO Public Diplomacy Division.

Sub-Series

A. Chemistry and Biology	Springer Science and Business Media
B. Physics and Biophysics	Springer Science and Business Media
C. Environmental Security	Springer Science and Business Media
D. Information and Communication Security	IOS Press
E. Human and Societal Dynamics	IOS Press

<http://www.nato.int/science>

<http://www.springer.com>

<http://www.iospress.nl>



Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes

Edited by

Bart Preneel

Katholieke Universiteit Leuven and IBBT, Belgium

Stefan Dodunekov

*Institute of Mathematics and Informatics,
Bulgarian Academy of Sciences, Bulgaria*

Vincent Rijmen

Katholieke Universiteit Leuven and IBBT, Belgium and TU Graz, Austria

and

Svetla Nikova

*Katholieke Universiteit Leuven and IBBT, Belgium and U Twente,
the Netherlands*

IOS
Press

Amsterdam • Berlin • Tokyo • Washington, DC

Published in cooperation with NATO Public Diplomacy Division

Proceedings of the NATO Advanced Research Workshop on Enhancing Cryptographic
Primitives with Techniques from Error Correcting Codes
Veliko Tarnovo, Bulgaria
6–9 October 2008

© 2009 IOS Press.

All rights reserved. No part of this book may be reproduced, stored in a retrieval system,
or transmitted, in any form or by any means, without prior written permission from the publisher.

ISBN 978-1-60750-002-5

Library of Congress Control Number: 2009924847

Publisher

IOS Press BV
Nieuwe Hemweg 6B
1013 BG Amsterdam
Netherlands
fax: +31 20 687 0019
e-mail: order@iospress.nl

Distributor in the UK and Ireland

Gazelle Books Services Ltd.
White Cross Mills
Hightown
Lancaster LA1 4XS
United Kingdom
fax: +44 1524 63232
e-mail: sales@gazellebooks.co.uk

Distributor in the USA and Canada

IOS Press, Inc.
4502 Rachael Manor Drive
Fairfax, VA 22032
USA
fax: +1 703 323 3668
e-mail: iosbooks@iospress.com

LEGAL NOTICE

The publisher is not responsible for the use which might be made of the following information.

PRINTED IN THE NETHERLANDS

Preface

The NATO Advanced Research Workshop on *Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes* has been organized on October 6–9, 2008 in Veliko Tarnovo, Bulgaria, by the Institute of Mathematics and Informatics of the Bulgarian Academy of Sciences in cooperation with COSIC, KU Leuven and in the framework of the NATO Science for Peace and Security program. The workshop was sponsored by NATO and the Institute of Mathematics and Informatics of the Bulgarian Academy of Sciences.

Co-directors of the NATO ARW were Prof. Dr. Bart Preneel (Katholieke Universiteit Leuven and IBBT, Belgium) and Prof. Dr. Sc. Stefan Dodunekov (Institute of Mathematics and Informatics, Bulgarian Academy of Sciences). The program committee of the workshop has invited 14 key speakers and 29 participants. All of them gave presentations and participated in the discussions. The ARW had 43 attendees from 16 countries.

The Institute of Mathematics and Informatics of the Bulgarian Academy of Sciences, has been responsible for the local organization. We would like to thank specially to Tsonka Baicheva, Stela Zhelezova, Yuri Borissov, Nikolai Manev and all the members of the department of Mathematical Foundations of Informatics for the perfect organization of the workshop. All the participants enjoyed the intensive scientific and social program.

We would like also to thank all the key speakers and participants for their interesting talks and for their contribution to the proceedings. We believe that we have achieved our goal, namely to gather international experts from both fields – coding theory and cryptography – in order to exchange ideas, define new challenges and open problems for future research. These proceedings present the state-of-the-art in the current research on cryptography applying techniques and results from coding theory.

The proceedings of the ARW are divided into two parts. The first part includes the papers based on the lectures of the invited speakers and the second part includes the papers based on the talks of the participants in the workshop. The order of appearance of the papers in the proceedings corresponds to the scientific program of the workshop.

February, 2009

Bart Preneel
Stefan Dodunekov
Vincent Rijmen
Svetla Nikova

Contents

Preface	v
<i>Bart Preneel, Stefan Dodunekov, Vincent Rijmen and Svetla Nikova</i>	
Invited Talks	
Authentication Codes from Error-Correcting Codes; An Overview	3
<i>Henk van Tilborg</i>	
Coded Modulation and the Arrival of Signcryption	17
<i>Yuliang Zheng</i>	
Secret Sharing and Error Correcting	28
<i>Svetla Nikova and Ventsislav Nikov</i>	
Algebraic Attacks on Filter and Combiner Generators	39
<i>Tor Helleseth, Michal Hojsik and Sondre Rønjom</i>	
S-Boxes, APN Functions and Related Codes	49
<i>Rafael Alvarez and Gary McGuire</i>	
Coding Theory and Hash Function Design	63
<i>Sebastiaan Indestege and Bart Preneel</i>	
Codes and Provable Security of Ciphers	69
<i>Joan Daemen and Vincent Rijmen</i>	
Applications of Near MDS Codes in Cryptography	81
<i>Stefan Dodunekov</i>	
On the Equivalence of Nonlinear Functions	87
<i>Yves Edel and Alexander Pott</i>	
On the Algebraic Immunities and Higher Order Nonlinearities of Vectorial Boolean Functions	104
<i>Claude Carlet</i>	
A Framework for Stream Ciphers Based on Pseudorandomness, Randomness and Coding	117
<i>Miodrag J. Mihaljević</i>	
On the Studies Related to Linear Codes in Generalized Construction of Resilient Functions with Very High Nonlinearity	140
<i>Subhamoy Maitra</i>	
Participants' Talks	
Reconstruction of Highly Non Linear Sboxes from Linear Codes	153
<i>Peter Beelen and Gregor Leander</i>	

LDPC Codes in the McEliece Cryptosystem: Attacks and Countermeasures <i>Marco Baldi</i>	160
On a Family of Planar Mappings <i>Gohar Kyureghyan and Yin Tan</i>	175
Linearities in Cascade Jump Controlled Stream Ciphers <i>Cees J.A. Jansen</i>	179
New Results on the Algebraic Immunity of Boolean Functions <i>Panagiotis Rizomiliotis</i>	192
Equivalence Between Certain Complementary Pairs of Types I and III <i>Tor E. Bjørstad and Matthew G. Parker</i>	203
Symbolic Dynamics, Codes, and Perfectly Balanced Functions <i>Oleg A. Logachev, Alexei A. Salnikov, Stanislav V. Smyshlyaev and Valery V. Yashchenko</i>	222
Algebraic Immunity of Boolean Power Functions with Kasami and Niho Exponents <i>Agnes Andics</i>	234
Some Comments on Bossert-Mahr-Heilig Scheme <i>Yuri L. Borissov and Nikolai L. Manev</i>	244
Linear Codes of Good Error Control Performance <i>Tsonka Baicheva</i>	250
Classification of Doubly Resolvable Designs and Orthogonal Resolutions <i>Svetlana Topalova and Stela Zhelezova</i>	260
Self-Dual Codes with Some Applications to Cryptography <i>Stefka Bouyuklieva</i>	265
Subject Index	271
Author Index	273