

Steven D. Galbraith (Ed.)

# Cryptography and Coding

11th IMA International Conference  
Cirencester, UK, December 18-20, 2007  
Proceedings

Volume Editor

Steven D. Galbraith  
Royal Holloway University of London  
Mathematics Department  
Egham, Surrey, TW20 0EX, UK  
E-mail: steven.galbraith@rhul.ac.uk

Library of Congress Control Number: 2007940956

CR Subject Classification (1998): E.3-4, G.2.1, C.2, J.1

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743  
ISBN-10 3-540-77271-5 Springer Berlin Heidelberg New York  
ISBN-13 978-3-540-77271-2 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](http://springer.com)

© Springer-Verlag Berlin Heidelberg 2007  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India  
Printed on acid-free paper SPIN: 12203093 06/3180 5 4 3 2 1 0

# Preface

The 11th IMA Conference on Cryptography and Coding was held at the Royal Agricultural College, Cirencester, UK during December 18–20, 2007. As usual, the venue provided a relaxed and convivial atmosphere for attendees to enjoy the conference programme and discuss current and future research ideas.

The programme comprised three invited talks and 22 contributed papers. The invited speakers were Jonathan Katz (University of Maryland, USA), Patrick Solé (Ecole Polytechnique de l'Université de Nice-Sophia Antipolis, France) and Whit Diffie (Sun Microsystems, USA). Special thanks are due to these speakers. Two of the invited speakers provided papers, included in this volume, which highlight the connections between cryptography, coding theory and discrete mathematics.

The contributed talks were selected from 48 submissions. The accepted papers cover a range of topics in mathematics and computer science, including symmetric and public key cryptography, Boolean functions, sequences, efficient implementation and side-channel analysis.

I would like to thank all the people who helped with the conference programme and organization. First, I thank the Steering Committee for their guidance on the general format of the conference and for suggestions of members of the Programme Committee. I also heartily thank the Programme Committee and the sub-reviewers listed on the following pages for their thoroughness during the review process. Each paper was reviewed by at least three people. There was significant online discussion about a number of papers.

The submission and review process was greatly simplified by the ichair software developed by Thomas Baignères and Matthieu Finiasz. Thanks also to Jon Hart for running the submissions Web server and Sriram Srinivasan for designing and maintaining the conference Web page.

Thanks go to the authors of all submitted papers. I also thank the authors of accepted papers for revising their papers according to referee suggestions and returning latex source files in good time. The revised versions were not checked by the Programme Committee so authors bear full responsibility for their contents. I thank the staff at Springer for their help with producing the proceedings.

I thank Hewlett-Packard and Vodafone for their sponsorship of this event.

Finally, I wish to thank the conference staff of the Institute for Mathematics and its Applications, especially Lucy Nye and Sammi Lauesen, for their help with running the conference and handling the finances.

# Cryptography and Coding 2007

Royal Agricultural College, Cirencester, UK  
December 18–20, 2007

Sponsored by  
*The Institute of Mathematics and its Applications*  
in cooperation with  
*Hewlett-Packard Laboratories* and *Vodafone Ltd.*

## Programme Chair

Steven Galbraith                      Royal Holloway University of London

## Steering Committee

Bahram Honary	Lancaster University
Chris Mitchell	Royal Holloway
Kenny Paterson	Royal Holloway
Fred Piper	Royal Holloway
Nigel Smart	University of Bristol
Mike Walker	Vodafone Ltd. and Royal Holloway

## Programme Committee

Steve Babbage	Vodafone Group Services Ltd.
Nigel Boston	South Carolina/Wisconsin
Pascale Charpin	INRIA Rocquencourt
Liqun Chen	Hewlett-Packard
Carlos Cid	Royal Holloway
YoungJu Choie	Postech, Korea
Arjen Lenstra	EPFL, Lausanne
Alexander May	Ruhr Universität Bochum
Gary McGuire	University College Dublin
Alfred Menezes	University of Waterloo
David Naccache	Ecole Normale Supérieure
Matthew Parker	University of Bergen
Matt Robshaw	France Telecom
Ana Sălăgean	Loughborough University
Berry Schoenmakers	Technical University Eindhoven
Michael Scott	Dublin City University
Amin Shokrollahi	EPFL, Lausanne
Nigel Smart	University of Bristol
Frederik Vercauteren	K. U. Leuven
Gilles Zemor	Université Bordeaux

## External Reviewers

Joppe Bos	Christophe De Cannière	Anne Canteaut
Claude Carlet	Mahdi Cheraghchi	Alex Dent
Fabien Galand	Philippe Guillot	Darrel Hankerson
Marcelo Kaihara	Cedric Lauradoux	Lorenz Minder
Marine Minier	Stephane Manuel	Ashley Montanaro
Sean Murphy	Dag Arne Osvik	Gregory Neven
Dan Page	Kenny Paterson	Benny Pinkas
Louis Salvail	Amin Shokrollahi	Andrey Sidorenko
Patrick Solé	Martijn Stam	Søren Steffen Thomsen
Eran Tromer	José Villegas	

# Table of Contents

## Invited Papers

Efficient Cryptographic Protocols Based on the Hardness of Learning Parity with Noise . . . . .	1
<i>Jonathan Katz</i>	
Galois Rings and Pseudo-random Sequences . . . . .	16
<i>Patrick Solé and Dmitrii Zinoviev</i>	

## Signatures I

Finding Invalid Signatures in Pairing-Based Batches . . . . .	34
<i>Laurie Law and Brian J. Matt</i>	
How to Forge a Time-Stamp Which Adobe's Acrobat Accepts . . . . .	54
<i>Tetsuya Izu, Takeshi Shimoyama, and Masahiko Takenaka</i>	

## Boolean Functions

Efficient Computation of the Best Quadratic Approximations of Cubic Boolean Functions . . . . .	73
<i>Nicholas Kolokotronis, Konstantinos Limniotis, and Nicholas Kalouptsidis</i>	
On the Walsh Spectrum of a New APN Function . . . . .	92
<i>Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire</i>	
Non-linear Cryptanalysis Revisited: Heuristic Search for Approximations to S-Boxes . . . . .	99
<i>Juan M.E. Tapiaador, John A. Clark, and Julio C. Hernandez-Castro</i>	

## Block Cipher Cryptanalysis

Cryptanalysis of the EPBC Authenticated Encryption Mode . . . . .	118
<i>Chris J. Mitchell</i>	
Blockwise-Adaptive Chosen-Plaintext Attack and Online Modes of Encryption . . . . .	129
<i>Gregory V. Bard</i>	
Algebraic Cryptanalysis of the Data Encryption Standard . . . . .	152
<i>Nicolas T. Courtois and Gregory V. Bard</i>	

## Side Channels

Cryptographic Side-Channels from Low Power Cache Memory . . . . .	170
<i>Philipp Grabher, Johann Großschädl, and Daniel Page</i>	
New Branch Prediction Vulnerabilities in OpenSSL and Necessary Software Countermeasures . . . . .	185
<i>Onur Aciçmez, Shay Gueron, and Jean-Pierre Seifert</i>	

## Linear Complexity

Remarks on the New Attack on the Filter Generator and the Role of High Order Complexity . . . . .	204
<i>Panagiotis Rizomiliotis</i>	
Modified Berlekamp-Massey Algorithm for Approximating the $k$ -Error Linear Complexity of Binary Sequences . . . . .	220
<i>Alexandra Alecu and Ana Sălăgean</i>	

## Public Key Encryption

Efficient KEMs with Partial Message Recovery . . . . .	233
<i>Tor E. Bjrstad, Alex W. Dent, and Nigel P. Smart</i>	
Randomness Reuse:Extensions and Improvements . . . . .	257
<i>Manuel Barbosa and Pooya Farshim</i>	
On the Connection Between Signcryption and One-Pass Key Establishment . . . . .	277
<i>M. Choudary Gorantla, Colin Boyd, and Juan Manuel González Nieto</i>	

## Curves

Optimised Versions of the Ate and Twisted Ate Pairings . . . . .	302
<i>Seiichi Matsuda, Naoki Kanayama, Florian Hess, and Eiji Okamoto</i>	
Extractors for Jacobian of Hyperelliptic Curves of Genus 2 in Odd Characteristic . . . . .	313
<i>Reza Rezaeian Farashahi</i>	
Constructing Pairing-Friendly Elliptic Curves Using Gröbner Basis Reduction . . . . .	336
<i>Waldyr D. Benits Junior and Steven D. Galbraith</i>	

## RSA Implementation

Efficient 15,360-bit RSA Using Woop-Optimised Montgomery Arithmetic .....	346
<i>Kamel Bentahar and Nigel P. Smart</i>	
Toward Acceleration of RSA Using 3D Graphics Hardware .....	364
<i>Andrew Moss, Daniel Page, and Nigel P. Smart</i>	

## Signatures II

Multi-key Hierarchical Identity-Based Signatures .....	384
<i>Hoon Wei Lim and Kenneth G. Paterson</i>	
Verifier-Key-Flexible Universal Designated-Verifier Signatures .....	403
<i>Raylin Tso, Juan Manuel González Nieto, Takeshi Okamoto, Colin Boyd, and Eiji Okamoto</i>	
<b>Author Index</b> .....	423