

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Germany

Madhu Sudan

Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbruecken, Germany

Liqun Chen (Ed.)

Cryptography and Coding

13th IMA International Conference, IMACC 2011
Oxford, UK, December 12-15, 2011
Proceedings

Volume Editor

Liqun Chen
Hewlett Packard Labs
Long Down Avenue, Stoke Gifford
Bristol, BS34 8QZ, UK
E-mail: liqun.chen@hp.com

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-25515-1 e-ISBN 978-3-642-25516-8
DOI 10.1007/978-3-642-25516-8
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011941505

CR Subject Classification (1998): E.3, D.4.6, K.6.5, G.1.3, J.1, G.2

LNCS Sublibrary: SL 4 – Security and Cryptology

© Springer-Verlag Berlin Heidelberg 2011

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.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

The 13th IMA Conference on Cryptography and Coding was held at the Lady Margaret Hall, University of Oxford, UK, during December 12–15, 2011. This event was a 25th anniversary celebration of the very successful biennial IMA conference series. Traditionally, the conference has taken place at the Royal Agricultural College, Cirencester, UK. Despite the change of venue, we managed to maintain both the style and atmosphere of the previous 12 events at this lovely location.

The conference programme consisted of four invited talks and 27 contributed papers. Special thanks to the invited speakers, namely, Ivan Damgård (Aarhus University, Denmark), Paddy Farrell (Lancaster University and University of Kent, UK), Jonathan Jedwab (Simon Fraser University, Canada) and David Naccache (ENS, France), who gave very enlightening talks. David Naccache also very kindly provided a paper, included in the proceedings.

Out of 57 submissions from 22 countries, 27 papers were selected, presented at the conference, and included in the proceedings. The accepted papers cover a wide range of topics in the field of mathematics and computer science, including coding theory, homomorphic encryption, symmetric and public key cryptosystem, cryptographic functions and protocols, efficient pairing and scalar multiplication implementation, knowledge proof, and security analysis.

The success of this event would be impossible without the help and hard work of so many people. Many thanks are due. First, I would like to thank the Steering Committee for their guidance on the general format of the conference. I also heartily thank the Programme Committee and the sub-reviewers, listed on the following pages, for their careful and thorough reviews. Each paper was reviewed by at least three people, most by four. Significant time was spent discussing the papers. Thanks must also go to the hard-working shepherds for their guidance and helpful advice on improving a number of papers.

The authors of all submitted papers must be thanked. I acknowledge the authors of accepted papers for revising papers according to referee suggestions and for 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.

Thank you to the staff at Springer for their help with producing the proceedings. Thanks also to the developers and maintainers of EasyChair software, by which the submission and review process was greatly simplified.

On behalf of the conference organization and participants, I would like to express our appreciation to Cryptomathic, Hewlett-Packard and Vodafone for their generous sponsorship of this event. I would like to give special thanks to Cryptomathic for sharing their 25th anniversary with us.

Finally, I wish to thank the conference staff of the Institute for Mathematics and its Applications, especially Lizzi Lake and Pam Bye, for their help with running the conference and handling the finances.

December 2011

Liqun Chen

Organization

Cryptography and Coding 2011

Lady Margaret Hall, University of Oxford, UK
December 12-15, 2011

Sponsored by
The Institute of Mathematics and its Applications
Cryptomathic Ltd.
Hewlett-Packard Laboratories
Vodafone Ltd.

Programme Chair

Liqun Chen

Hewlett-Packard Laboratories, UK

Steering Committee

Steven Galbraith

University of Auckland, New Zealand

Bahram Honary

Lancaster University, UK

Chris Mitchell

Royal Holloway, University of London, UK

Matthew G. Parker

University of Bergen, Norway

Kenny Paterson

Royal Holloway, University of London, UK

Fred Piper

Royal Holloway, University of London, UK

Nigel Smart

University of Bristol, UK

Mike Walker

Vodafone and Royal Holloway, UK

Programme Committee

Steve Babbage

Vodafone, UK

Mohammed Benaissa

University of Sheffield, UK

Nigel Boston

University of Wisconsin, USA

Colin Boyd

Queensland University of Technology, Australia

Pascale Charpin

INRIA Rocquencourt, France

Carlos Cid

Royal Holloway, University of London, UK

Nicolas Courtois

University College London, UK

James Davenport

University of Bath, UK

Tuvi Etzion

Technion, Israel

Dieter Gollmann

Hamburg University of Technology, Germany

Keith Harrison

Hewlett-Packard Laboratories, UK

David Jao

University of Waterloo, Canada

VIII Organization

Jon-Lark Kim	University of Louisville, USA
Mirosław Kutylowski	Wrocław University of Technology, Poland
Gohar Kyureghyan	University of Magdeburg, Germany
Xuejia Lai	Shanghai Jiaotong University, China
Pil Joong Lee	Pohang University of Science and Technology, South Korea
Dongdai Lin	Institute of Software of Chinese Academy of Sciences, China
Gary Mcguire	University College Dublin, Ireland
Catherine Meadows	Naval Research Laboratory, USA
David Naccache	Ecole Normale Supérieure, France
Siaw-Lynn Ng	Royal Holloway, University of London, UK
Matthew Parker	University of Bergen, Norway
Raphael Phan	Loughborough University, UK
Matt Robshaw	Orange Labs, France
Ana Salagean	Loughborough University, UK
Hans Georg Schaathun	Ålesund University College, Norway
Michael Scott	Dublin City University, Ireland
Martijn Stam	University of Bristol, UK
Frederik Vercauteren	K.U. Leuven, Belgium
Guilin Wang	University of Wollongong, Australia
Bogdan Warinschi	University of Bristol, UK
Kyeongcheol Yang	Pohang University of Science and Technology, South Korea
Jianying Zhou	Institute for Infocomm Research, Singapore

External Reviewers

Al-Kuwari, Saif	Gorantla, M. Choudary
Au, Man Ho	Hu, Lei
Aumasson, Jean-Philippe	Huang, Yun
Burrage, Alex	Khader, Dalia
Chow, Sherman S. M.	Kim, Yeonkyu
Chu, Cheng-Kang	Krzywiecki, Lukasz
Chung, Jin-Ho	Kubiak, Przemyslaw
Coatrieux, Gouenou	Lai, Lifeng
Costello, Craig	Lee, Eun Sung
Duan, Ming	Lee, Woomyo
Dziembowski, Stefan	Lin, Tingting
Eom, Sungwook	Liu, Joseph
Fan, Junfeng	Luo, Yiyuan
Feng, Xiutao	Majcher, Krzysztof
Ghadafi, Essam	Meidl, Wilfried
Gologlu, Faruk	Minier, Marine
Gong, Zheng	Mourouzis, Theodosios

Murphy, Sean	Yang, Yanjiang
Reyhanitabar, Mohammad Reza	Yasmin, Rehana
Safavi, Rei	Yu, Yong
Schaffner, Christian	Zagorski, Filip
Schmidt, Kai-Uwe	Zhang, Xusheng
Shao, Jun	Zhang, Zhifang
Wolf, Christopher	Zhong, Jinmin
Wu, Qianhong	

Table of Contents

Invited Paper

Can a Program Reverse-Engineer Itself?	1
<i>Antoine Amarilli, David Naccache, Pablo Rauzy, and Emil Simion</i>	

Homomorphic Encryption

Improved Key Generation for Gentry's Fully Homomorphic Encryption Scheme	10
<i>Peter Scholl and Nigel P. Smart</i>	
On Constructing Homomorphic Encryption Schemes from Coding Theory	23
<i>Frederik Armknecht, Daniel Augot, Ludovic Perret, and Ahmad-Reza Sadeghi</i>	

Coding Theory I

Generalised Complementary Arrays	41
<i>Matthew G. Parker and Constanza Riera</i>	
Binary Kloosterman Sums with Value 4	61
<i>Jean-Pierre Flori, Sihem Mesnager, and Gérard Cohen</i>	
On the Triple-Error-Correcting Cyclic Codes with Zero Set $\{1, 2^i + 1, 2^j + 1\}$	79
<i>Vincent Herbert and Sumanta Sarkar</i>	

Knowledge Proof

A Secure and Efficient Proof of Integer in an Interval Range	97
<i>Kun Peng</i>	
Bit Commitment in the Bounded Storage Model: Tight Bound and Simple Optimal Construction	112
<i>Junji Shikata and Daisuke Yamanaka</i>	

Cryptographic Functions

Self-correctors for Cryptographic Modules	132
<i>Go Yamamoto and Tetsutaro Kobayashi</i>	

The Symbiosis between Collision and Preimage Resistance	152
<i>Elena Andreeva and Martijn Stam</i>	
Enhanced Count of Balanced Symmetric Functions and Balanced Alternating Functions	172
<i>Marc Mouffron and Guillaume Vergne</i>	

Public Key Cryptosystem

Ciphertext-Policy Delegatable Hidden Vector Encryption and Its Application to Searchable Encryption in Multi-user Setting.....	190
<i>Mitsuhiro Hattori, Takato Hirano, Takashi Ito, Nori Matsuda, Takumi Mori, Yusuke Sakai, and Kazuo Ohta</i>	
Constructing Secure Hybrid Encryption from Key Encapsulation Mechanism with Authenticity	210
<i>Yuki Shibuya and Junji Shikata</i>	

Coding Theory II

A Note on the Dual Codes of Module Skew Codes.....	230
<i>Delphine Boucher and Felix Ulmer</i>	
Ensuring Message Embedding in Wet Paper Steganography	244
<i>Daniel Augot, Morgan Barbier, and Caroline Fontaine</i>	
On the Stability of m-Sequences	259
<i>Alex J. Burrage, Ana Sălăgean, and Raphael C.-W. Phan</i>	

Pairing and ECC Implementation

Parallelizing the Weil and Tate Pairings	275
<i>Diego F. Aranha, Edward Knapp, Alfred Menezes, and Francisco Rodríguez-Henríquez</i>	
On the Efficient Implementation of Pairing-Based Protocols	296
<i>Michael Scott</i>	
Efficient Pairing Computation on Ordinary Elliptic Curves of Embedding Degree 1 and 2.....	309
<i>Xusheng Zhang and Dongdai Lin</i>	
Improved Precomputation Scheme for Scalar Multiplication on Elliptic Curves	327
<i>Duc-Phong Le and Chik How Tan</i>	

Security Analysis

Breaking an Identity-Based Encryption Scheme Based on DHIES	344
<i>Martin R. Albrecht and Kenneth G. Paterson</i>	
Analysis of the SSH Key Exchange Protocol	356
<i>Stephen C. Williams</i>	
Cryptanalysis of the Light-Weight Cipher A2U2	375
<i>Mohamed Ahmed Abdelraheem, Julia Borghoff, Erik Zenner, and Mathieu David</i>	

Symmetric Key Cryptosystem

Building Blockcipher from Tweakable Blockcipher: Extending FSE 2009 Proposal	391
<i>Kazuhiko Minematsu and Tetsu Iwata</i>	
Security of Hash-then-CBC Key Wrapping Revisited	413
<i>Yasushi Osaki and Tetsu Iwata</i>	

Cryptographic Protocols

Block-Wise P-Signatures and Non-interactive Anonymous Credentials with Efficient Attributes	431
<i>Malika Izabachène, Benoît Libert, and Damien Vergnaud</i>	
On Forward Secrecy in One-Round Key Exchange	451
<i>Colin Boyd and Juan González Nieto</i>	
Designated Confirmer Signatures with Unified Verification	469
<i>Guilin Wang, Fubiao Xia, and Yunlei Zhao</i>	
Author Index	497