

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

Alejandro Hevia Gregory Neven (Eds.)

Progress in Cryptology – LATINCRYPT 2012

2nd International Conference on Cryptology
and Information Security in Latin America
Santiago, Chile, October 7-10, 2012
Proceedings



Springer

Volume Editors

Alejandro Hevia
University of Chile
Department of Computer Science
Blanco Encalada 2120
Tercer Piso, Santiago, Chile
E-mail: ahevia@dcc.uchile.cl

Gregory Neven
IBM Research - Zurich
Säumerstrasse 4
8803 Rüschlikon, Switzerland
E-mail: nev@zurich.ibm.com

ISSN 0302-9743
ISBN 978-3-642-33480-1
DOI 10.1007/978-3-642-33481-8
Springer Heidelberg Dordrecht London New York

e-ISSN 1611-3349
e-ISBN 978-3-642-33481-8

Library of Congress Control Number: 2012946763

CR Subject Classification (1998): E.3, K.6.5, D.4.6, C.2, G.2, E.4

LNCS Sublibrary: SL 4 – Security and Cryptology

© Springer-Verlag Berlin Heidelberg 2012

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

Latincrypt 2012 was the Second International Conference on Cryptology and Information Security in Latin America and took place from October 7th to 10th, 2012, in Santiago, Chile. The conference was organized by the Group of Applied Cryptography and Security (CLCERT) of the University of Chile and the NIC Chile Research Labs in cooperation with The International Association for Cryptologic Research (IACR). The General Chairs of the conference were Javier Bustos and Alejandro Hevia.

By the submission deadline on May 18th, 2012, the conference had received 47 submissions. Each submission was reviewed by at least three committee members, submissions co-authored by members of the Program Committee were assigned to at least five committee members. The reviewing process was challenging due to the high quality of the submissions, and we are deeply grateful to the committee members and external reviewers for their outstanding work. After meticulous deliberation, the Program Committee, which was chaired by Alejandro Hevia and Gregory Neven, selected 17 submissions for presentation at the conference. These are the articles included in this volume. In addition to these presentations, the program also included four invited talks and a student poster session.

The reviewing process was run using the iChair software written by Thomas Baignères and Matthieu Finiasz. We are especially grateful to them for letting us use their software and for their prompt responses to our questions on how to use the system. Also, we thank Sergio Miranda from the CLCERT for his help in setting up the reviewing system.

Finally, we would like to thank our sponsors Intel & McAfee Chile, NIC Chile, Certivox, the Center for Mathematical Modeling (CMM) of the University of Chile, INRIA Chile, CLEI, Yahoo Research Chile, and Orand Chile, for their financial support, as well as all the people who contributed to the success of this conference. In particular, we are indebted to the members of the Latincrypt Steering Committee, especially to Michel Abdalla, who we regularly consulted for his experience from Latincrypt 2010; the General Co-chair Javier Bustos; Jacqueline Araya; and everyone in the Local Organizing Committee for their diligent work and for making this conference possible. Finally, we would like to thank Springer for publishing the proceedings in their *Lecture Notes in Computer Science* series.

October 2012

Alejandro Hevia
Gregory Neven

LATINCRYPT 2012

**Second International Conference on
Cryptography and Information Security in Latin America**

**Santiago, Chile
October 7–10, 2012**

Organized by

Grupo de Criptografía Aplicada y Seguridad (CLCERT), NIC Chile Research
Labs & Dept. of Computer Science, Universidad de Chile

In Cooperation with

The International Association for Cryptologic Research (IACR)

General Chairs

Javier Bustos
Alejandro Hevia

NIC Chile Research Labs, Chile
CLCERT & Department of Computer Science,
Universidad de Chile, Chile

Program Chairs

Alejandro Hevia
Gregory Neven

CLCERT & Department of Computer Science,
Universidad de Chile, Chile
IBM Research – Zurich, Switzerland

Steering Committee

Michel Abdalla
Paulo Barreto
Ricardo Dahab
Alejandro Hevia
Julio López
Daniel Panario
Alfredo Viola

École Normale Supérieure, France
Universidade de São Paulo, Brazil
Universidade Estadual de Campinas, Brazil
Universidad de Chile, Chile
Universidade Estadual de Campinas, Brazil
Carleton University, Canada
Universidad de la República, Uruguay

Local Organizing Committee

Jacqueline Araya
Sergio Miranda
Alonso González
Philippe Camacho
Rodrigo Abarzúa

NIC Chile Research Labs, Chile
CLCERT, Chile
Universidad de Chile, Chile
Universidad de Chile, Chile
Universidade Estadual de Campinas, Brazil

Program Committee

| | |
|-------------------------------|--|
| Michel Abdalla | École Normale Supérieure, France |
| Roberto Avanzi | Ruhr-University Bochum, Germany |
| Paulo Barreto | University of São Paulo, Brazil |
| Lejla Batina | Radboud University Nijmegen, The Netherlands |
| Philippe Camacho | Universidad de Chile, Chile |
| Claude Carlet | Université Paris 8, France |
| Carlos Cid | Royal Holloway, University of London, UK |
| Ricardo Dahab | Universidade Estadual de Campinas, Brazil |
| Joan Daemen | ST Microelectronics, Belgium |
| Orr Dunkelman | University of Haifa, Israel |
| Stefan Dziembowski | University of Warsaw, Poland, and University of Rome “La Sapienza”, Italy |
| Sebastian Faust | Aarhus University, Denmark |
| Georg Fuchsbauer | University of Bristol, UK |
| Philippe Gaborit | Université de Limoges, France |
| Joachim von zur Gathen | B-IT, Universität Bonn, Germany |
| Tibor Jager | Karlsruhe Institute of Technology, Germany |
| Seny Kamara | Microsoft Research, USA |
| Stefan Katzenbeisser | Technische Universität Darmstadt, Germany |
| Vladimir Kolesnikov | Bell Labs, USA |
| Sven Laur | University of Tartu, Estonia |
| Vadim Lyubashevsky | École Normale Supérieure, France |
| Daniel Panario | Carleton University, Canada |
| Giuseppe Persiano | Università di Salerno, Italy |
| Carla Ràfols | Ruhr-Universität Bochum, Germany |
| Christian Rechberger | DTU, Denmark |
| Tamara Rezk | INRIA Sophia Antipolis-Méditerranée, France |
| Matt Robshaw | Orange Labs, France |
| Francisco Rodríguez-Henríquez | Centro de Investigación y de Estudios Avanzados del I.P.N., México |
| Nicolas Thériault | Universidad del Bío-Bío, Chile |
| Maribel Gonzalez Vasco | Universidad Rey Juan Carlos, Spain |
| Alfredo Viola | Universidad de la República, Uruguay |
| Ivan Visconti | Università di Salerno, Italy |
| Scott Yilek | University of St. Thomas, USA |
| Santiago Zanella-Béguelin | Microsoft Research, UK |

External Reviewers

| | |
|------------------------------|--------------------|
| Mohamed Ahmed Abdelraheem | Gilles Macario-Rat |
| Diego Aranha | Wilfried Meidl |
| Raoul Blankertz | Marine Minier |
| Anne Canteaut | Michael Naehrig |
| Julio Cesar Hernández Castro | Michael Nüsken |
| Angelo De Caro | Roger Oyono |
| Chun-I Fan | Valerio Pastro |
| Junfeng Fan | Geovandro Pereira |
| Philippe Gaborit | Christiane Peters |
| Steven Galbraith | Jeremy Planul |
| Alonso González | Alex Pott |
| Shay Gueron | Jordi Pujolàs |
| Iftach Haitner | Guénaël Renault |
| Darrel Hankerson | Yannis Rouselakis |
| Jennie Hansen | Peter Schwabe |
| Clemens Heuberger | Christoph Striecks |
| Aggelos Kiayias | Enrico Thomae |
| Markulf Kohlweiss | Viet-Cuong Trinh |
| Daniel Loebenberg | Marcin Wojcik |
| Zhengqin Luo | Konstantin Ziegler |

Sponsoring Institutions

Grupo de Criptografía Aplicada y Seguridad (CLCERT), Universidad de Chile
 NIC Chile Research Labs, Universidad de Chile
 Facultad de Ciencias Físicas y Matemáticas, Universidad de Chile
 Intel & McAfee Labs
 Center for Mathematical Modeling, Universidad de Chile
 Certivox
 NIC Chile
 Centro Latinoamericano de Estudios en Informáticas (CLEI)
 INRIA Chile
 Yahoo! Labs
 Orand
 Welcu

Table of Contents

Elliptic Curves

| | |
|--|----|
| Indifferentiable Hashing to Barreto–Naehrig Curves | 1 |
| <i>Pierre-Alain Fouque and Mehdi Tibouchi</i> | |
| Semi-bent Functions with Multiple Trace Terms and Hyperelliptic Curves | 18 |
| <i>Sihem Mesnager</i> | |
| Complete Atomic Blocks for Elliptic Curves in Jacobian Coordinates over Prime Fields | 37 |
| <i>Rodrigo Abarzúa and Nicolas Thériault</i> | |

Cryptographic Protocols I

| | |
|---|-----|
| Message-Based Traitor Tracing with Optimal Ciphertext Rate | 56 |
| <i>Duong Hieu Phan, David Pointcheval, and Mario Strefer</i> | |
| Leakage-Resilient Spatial Encryption | 78 |
| <i>Michel Abdalla and Jill-Jênn Vie</i> | |
| On the Pseudorandom Function Assumption in (Secure) Distance-Bounding Protocols: PRF-ness alone Does Not Stop the Frauds! | 100 |
| <i>Ioana Boureanu, Aikaterini Mitrokotsa, and Serge Vaudenay</i> | |
| Lattice-Based Hierarchical Inner Product Encryption | 121 |
| <i>Michel Abdalla, Angelo De Caro, and Karina Mochetti</i> | |

Implementations

| | |
|---|-----|
| Towards Efficient Arithmetic for Lattice-Based Cryptography on Reconfigurable Hardware | 139 |
| <i>Thomas Pöppelmann and Tim Güneysu</i> | |
| The Security Impact of a New Cryptographic Library | 159 |
| <i>Daniel J. Bernstein, Tanja Lange, and Peter Schwabe</i> | |
| Faster Implementation of Scalar Multiplication on Koblitz Curves | 177 |
| <i>Diego F. Aranha, Armando Faz-Hernández, Julio López, and Francisco Rodríguez-Henríquez</i> | |

Cryptographic protocols II

| | |
|--|-----|
| Zero-Knowledge for Multivariate Polynomials | 194 |
| <i>Valérie Nachez, Jacques Patarin, and Emmanuel Volte</i> | |

| | |
|--|-----|
| Improved Exponentiation and Key Agreement in the Infrastructure of a Real Quadratic Field | 214 |
| <i>Vanessa Dixon, Michael J. Jacobson Jr., and Renate Scheidler</i> | |

Foundations

| | |
|---|-----|
| UOWHFs from OWFs: Trading Regularity for Efficiency | 234 |
| <i>Kfir Barhum and Ueli Maurer</i> | |

| | |
|---|-----|
| Random Mappings with Restricted Preimages | 254 |
| <i>Andrew MacFie and Daniel Panario</i> | |

Symmetric-key Cryptography

| | |
|--|-----|
| On the Sosemanuk Related Key-IV Sets | 271 |
| <i>Aleksandar Kircanski and Amr M. Youssef</i> | |

| | |
|--|-----|
| High Speed Implementation of Authenticated Encryption for the MSP430X Microcontroller | 288 |
| <i>Conrado P.L. Gouvêa and Julio López</i> | |

| | |
|---|-----|
| Infective Computation and Dummy Rounds: Fault Protection for Block Ciphers without Check-before-Output | 305 |
| <i>Benedikt Gierlichs, Jörn-Marc Schmidt, and Michael Tunstall</i> | |

| | |
|-------------------------------|------------|
| Author Index | 323 |
|-------------------------------|------------|