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

Program Chairs
Alejandro Hevia
CLCERT & Department of Computer Science, Universidad de Chile, Chile
Gregory Neven
IBM Research – Zurich, Switzerland

Steering Committee
Michel Abdalla
École Normale Supérieure, France
Paulo Barreto
Universidade de São Paulo, Brazil
Ricardo Dahab
Universidade Estadual de Campinas, Brazil
Alejandro Hevia
Universidad de Chile, Chile
Julio López
Universidade Estadual de Campinas, Brazil
Daniel Panario
Carleton University, Canada
Alfredo Viola
Universidad de la República, Uruguay

Local Organizing Committee
Jacqueline Araya
NIC Chile Research Labs, Chile
Sergio Miranda
CLCERT, Chile
Alonso González
Universidad de Chile, Chile
Philippe Camacho
Universidad de Chile, Chile
Rodrigo Abarzúa
Universidade Estadual de Campinas, Brazil
Program Committee

Michel Abdalla  
Roberto Avanzi  
Paulo Barreto  
Lejla Batina  
Philippe Camacho  
Claude Carlet  
Carlos Cid  
Ricardo Dahab  
Joan Daemen  
Orr Dunkelman  
Stefan Dziembowski  
Sebastian Faust  
Georg Fuchsbauer  
Philippe Gaborit  
Joachim von zur Gathen  
Tibor Jager  
Seny Kamara  
Stefan Katzenbeisser  
Vladimir Kolesnikov  
Sven Laur  
Vadim Lyubashevsky  
Daniel Panario  
Giuseppe Persiano  
Carla Ràfols  
Christian Rechberger  
Tamara Rezk  
Matt Robshaw  
Francisco Rodríguez-Henríquez  
Nicolas Thériault  
Maribel Gonzalez Vasco  
Alfredo Viola  
Ivan Visconti  
Scott Yilek  
Santiago Zanella–Béguelin

École Normale Supérieure, France  
Ruhr-University Bochum, Germany  
University of São Paulo, Brazil  
Radboud University Nijmegen, The Netherlands  
Universidad de Chile, Chile  
Université Paris 8, France  
Royal Holloway, University of London, UK  
Universidade Estadual de Campinas, Brazil  
ST Microelectronics, Belgium  
University of Haifa, Israel  
University of Warsaw, Poland, and University of Rome “La Sapienza”, Italy  
Aarhus University, Denmark  
University of Bristol, UK  
Université de Limoges, France  
B-IT, Universität Bonn, Germany  
Karlsruhe Institute of Technology, Germany  
Microsoft Research, USA  
Technische Universität Darmstadt, Germany  
Bell Labs, USA  
University of Tartu, Estonia  
École Normale Supérieure, France  
Carleton University, Canada  
Università di Salerno, Italy  
Ruhr-Universität Bochum, Germany  
DTU, Denmark  
INRIA Sophia Antipolis-Méditerranée, France  
Orange Labs, France  
Centro de Investigación y de Estudios Avanzados del I.P.N., México  
Universidad del Bío-Bío, Chile  
Universidad Rey Juan Carlos, Spain  
Universidad de la República, Uruguay  
Università di Salerno, Italy  
University of St. Thomas, USA  
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 Loebenberger  Marcin Wójcik
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
Pierre-Alain Fouque and Mehdi Tibouchi

Semi-bent Functions with Multiple Trace Terms and Hyperelliptic
Curves .................................................................................... 18
Sihem Mesnager

Complete Atomic Blocks for Elliptic Curves in Jacobian Coordinates
over Prime Fields ................................................................. 37
Rodrigo Abarzúa and Nicolas Thériault

Cryptographic Protocols I

Message-Based Traitor Tracing with Optimal Ciphertext Rate .......... 56
Duong Hieu Phan, David Pointcheval, and Mario Strehler

Leakage-Resilient Spatial Encryption ........................................... 78
Michel Abdalla and Jill-Jênn Vie

On the Pseudorandom Function Assumption in (Secure) Distance-
Bounding Protocols: PRF-ness alone Does Not Stop the Frauds! ...... 100
Ioana Boureanu, Aikaterini Mitrokotsa, and Serge Vaudenay

Lattice-Based Hierarchical Inner Product Encryption .................... 121
Michel Abdalla, Angelo De Caro, and Karina Mochetti

Implementations

Towards Efficient Arithmetic for Lattice-Based Cryptography on
Reconfigurable Hardware .......................................................... 139
Thomas Pöppelmann and Tim Güneysu

The Security Impact of a New Cryptographic Library ....................... 159
Daniel J. Bernstein, Tanja Lange, and Peter Schwabe

Faster Implementation of Scalar Multiplication on Koblitz Curves ...... 177
Diego F. Aranha, Armando Faz-Hernández, Julio López, and
Francisco Rodríguez-Henríquez
Cryptographic protocols II

Zero-Knowledge for Multivariate Polynomials .......................... 194
Valérie Nachef, Jacques Patarin, and Emmanuel Volte

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

Foundations

UOWHFs from OWFs: Trading Regularity for Efficiency ............... 234
Kfir Barhum and Ueli Maurer

Random Mappings with Restricted Preimages ............................ 254
Andrew MacFie and Daniel Panario

Symmetric-key Cryptography

On the Sosemanuk Related Key-IV Sets ................................. 271
Aleksandar Kircanski and Amr M. Youssef

High Speed Implementation of Authenticated Encryption for the MSP430X Microcontroller ........................................ 288
Conrado P.L. Gouvêa and Julio López

Infected Computation and Dummy Rounds: Fault Protection for Block Ciphers without Check-before-Output ........................... 305
Benedikt Gierlichs, Jörn-Marc Schmidt, and Michael Tunstall

Author Index ........................................................................ 323