Lecture Notes in Computer Science 7533

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

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 e-ISSN 1611-3349
ISBN 978-3-642-33480-1 e-ISBN 978-3-642-33481-8
DOI 10.1007/978-3-642-33481-8
Springer Heidelberg Dordrecht London New York

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

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

Cryptographic Protocols I

Implementations

Cryptographic protocols II

Foundations

Symmetric-key Cryptography