Lecture Notes in Computer Science 6737

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

Abderrahmane Nitaj David Pointcheval (Eds.)

Progress in Cryptology – AFRICACRYPT 2011

4th International Conference on Cryptology in Africa
Dakar, Senegal, July 5-7, 2011
Proceedings

Springer

Volume Editors

Abderrahmane Nitaj
Université de Caen
Département de Mathématiques
Campus II, Boulevard Maréchal Juin, BP 5186 - 14032 Caen Cedex, France
E-mail: nitaj@math.unicaen.fr

David Pointcheval
École Normale Supérieure
Département d'Informatique
45 rue d'Ulm, 75230 Paris Cedex 05, France
E-mail: david.pointcheval@ens.fr

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-21968-9 e-ISBN 978-3-642-21969-6
DOI 10.1007/978-3-642-21969-6
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011929658

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

AFRICACRYPT 2011, the 4th International Conference on the Theory and Application of Cryptographic Techniques in Africa took place July 5–7, 2011 in Dakar, Senegal. The conference was organized by the LACGAA team of Université Cheikh Anta Diop de Dakar and the STCC team of "Présidence de la République – Service Technique Central des Chiffres et de la Sécurité des Télécommunications" in cooperation with the International Association for Cryptologic Research.

The conference received 76 submissions, and all were reviewed by the Program Committee. Each paper was assigned at least three reviewers, while submissions co-authored by Program Committee members were reviewed by at least five people. The Program Committee, aided by reports from 52 external reviewers, produced a total of 240 reviews in all. After highly interactive discussions and a careful deliberation, the Program Committee selected 23 papers for presentation. The authors of accepted papers were given 3 weeks to prepare final versions for these proceedings. We would like to note that the African paper entitled "On Randomness Extraction in Elliptic Curves" written by Abdoul Aziz Ciss and Djiby Sow was accepted as one of the best papers. The program was completed with invited talks by Jens Groth, Tatsuaki Okamoto and Bart Preneel. We would like to thank everyone who contributed to the success of AFRICACRYPT 2011. We are deeply grateful to the Program Committee for their hard work, enthusiasm, and conscientious efforts to ensure that each paper received a thorough and fair review. These thanks are of course extended to the external reviewers, listed on the following pages, who took the time to help out during the evaluation process. We would also like to thank Thomas Baignères and Matthieu Finiasz for writing the iChair software and Springer for agreeing to an accelerated schedule for printing the proceedings. We also wish to heartily thank Mamadou Sangharé, the General Chair, and Djiby Sow, the General Co-chair, as well as the LACGAA and STCC teams, for their efforts in the organization of the conference. Last but not the least, we extend our sincere thanks to all those who contributed to AFRICACRYPT 2011 and especially to the participants, submitters, authors, presenters and invited speakers.

AFRICACRYPT has been emerging as a powerful forum for researchers to interact, share their work and knowledge with others for the overall growth and development of cryptology research in the world, and more specifically in Africa.

July 2011

Abderrahmane Nitaj
David Pointcheval

Organization

General Chairs

Mamadou Sangharé	Université Cheikh Anta Diop de Dakar, Senegal
Djiby Sow	Université Cheikh Anta Diop de Dakar, Senegal

Program Chairs

Abderrahmane Nitaj	Université de Caen, France
David Pointcheval	ENS and CNRS and INRIA, Paris, France

Program Committee

Abdelhak Azhari	University of Casablanca, Morocco
Abdelmalek Azizi	University of Oujda, Morocco
Hatem M. Bahig	Ain Shams University, Cairo, Egypt
Colin Boyd	Queensland University of Technology, Australia
Anne Canteaut	INRIA, France
David Cash	UC San Diego, USA
Dario Catalano	Università di Catania, Italy
Riaal Domingues	South African Communications and Security Agency, South Africa
Eiichiro Fujisaki	NTT Labs, Japan
David Galindo	University of Luxembourg, Luxembourg
Maria Isabel Gonzalez-Vasco	Universidad Rey Juan Carlos, Madrid, Spain
Aline Gouget	CryptoExperts, France
Jens Groth	University College London, UK
Martin Hirt	ETH Zurich, Switzerland
Tetsu Iwata	Nagoya University, Japan
Stanislaw Jarecki	UC Irvine, California, USA
Seny Kamara	Microsoft, Redmond, USA
Fabien Laguillaumie	University of Caen, France
Mark Manulis	TU Darmstadt and CASED, Germany
Bruno Martin	I3S, University of Nice-Sophia Antipolis, France
Keith Martin	Royal Holloway, University of London, UK
Mitsuru Matsui	Mitsubishi Electric, Japan
Kaisa Nyberg	Aalto University and Nokia, Finland
Sami Omar	Tunis University, Tunisia
Ayoub Otmani	University of Caen, France and INRIA, France
Josef Pieprzyk	Macquarie University, Australia
Vincent Rijmen	K.U. Leuven, Belgium and TU Graz, Austria

Magdy Saeb	AST, Alexandria, Egypt
Kazue Sako	NEC, Japan
Palash Sarkar	Indian Statistical Institute, India
Francesco Sica	University of Calgary, Canada
Martijn Stam	EPFL, Switzerland
Christine Swart	University of Cape Town, South Africa
Damien Vergnaud	ENS, Paris, France
Ivan Visconti	University of Salerno, Italy and UCLA, USA
Bogdan Warinschi	Bristol University, UK
Duncan Wong	City University of Hong Kong, China
Scott Yilek	University of St. Thomas, USA
Amr M. Youssef	Concordia University, Montreal, Quebec, Canada

External Reviewers

Divesh Aggarwal
Ali Akhavi
Kazumaro Aoki
Kfir Barhum
Stephanie Bayer
Rishiraj Bhattacharyya
Joppe W. Bos
Charles Bouillaguet
Billy Brumley
Stanislav Bulygin
Sébastien Canard
Pierre-Louis Cayrel
Sandro Coretti
Claus Diem
Mario Di Raimondo
Orr Dunkelman
Mohamed Elkadi
Nadia El Mrabet
Martin Franz
Jun Furukawa
Xiao-Shan Gao
Carlos González Guillén
Louis Goubin
Jonanthan Hoch
Michal Hojsík
Laurent Imbert
Sebastiaan Indesteege
Toshiyuki Isshiki
Kimmo Järvinen
Noboru Kunihiro
Christoph Lucas
Vadim Lyubashevsky
Avradip Mandal
Nicolas Meloni
Shiho Moriai
Adam O'Neill
Somindu C Ramanna
Robert Rolland
Greg Rose
Minoru Saeki
Subhabrata Samajder
Juraj Sarinay
Alessandra Scafuro
Nicolas Sendrier
Douglas Stebila
Daisuke Suzuki
Isamu Teranishi Stefano Tessaro
Elmar Tischhauser
Yuuki Tokunaga
Keita Xagawa
Bin Zhang

Table of Contents

Protocols

Cryptanalysis

Secret-Key Cryptography

Efficient Implementations

Cryptographic Schemes

Algorithmic Problems

Elliptic Curves

Fault Analysis

Security Proofs

Invited Talks