

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

Abderrahmane Nitaj David Pointcheval (Eds.)

Progress in Cryptology – AFRICACRYPT 2011

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

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

© 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

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, Tatsuki 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
Djiby Sow

Université Cheikh Anta Diop de Dakar, Senegal
Université Cheikh Anta Diop de Dakar, Senegal

Program Chairs

Abderrahmane Nitaj
David Pointcheval

Université de Caen, France
ENS and CNRS and INRIA, Paris, France

Program Committee

Abdelhak Azhari
Abdelmalek Azizi
Hatem M. Bahig
Colin Boyd
Anne Canteaut
David Cash
Dario Catalano
Riaal Domingues

University of Casablanca, Morocco
University of Oujda, Morocco
Ain Shams University, Cairo, Egypt
Queensland University of Technology, Australia
INRIA, France
UC San Diego, USA
Università di Catania, Italy
South African Communications and Security
Agency, South Africa

Eiichiro Fujisaki
David Galindo
Maria Isabel Gonzalez-Vasco
Aline Gouget
Jens Groth
Martin Hirt
Tetsu Iwata
Stanislaw Jarecki
Seny Kamara
Fabien Laguillaumie
Mark Manulis
Bruno Martin
Keith Martin
Mitsuru Matsui
Kaisa Nyberg
Sami Omar
Ayoub Otmani
Josef Pieprzyk
Vincent Rijmen

NTT Labs, Japan
University of Luxembourg, Luxembourg
Universidad Rey Juan Carlos, Madrid, Spain
CryptoExperts, France
University College London, UK
ETH Zurich, Switzerland
Nagoya University, Japan
UC Irvine, California, USA
Microsoft, Redmond, USA
University of Caen, France
TU Darmstadt and CASED, Germany
I3S, University of Nice-Sophia Antipolis, France
Royal Holloway, University of London, UK
Mitsubishi Electric, Japan
Aalto University and Nokia, Finland
Tunis University, Tunisia
University of Caen, France and INRIA, France
Macquarie University, Australia
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	Sebastiaan Indesteege
Ali Akhavi	Toshiyuki Isshiki
Kazumaro Aoki	Kimmo Järvinen
Kfir Barhum	Noboru Kunihiro
Stephanie Bayer	Christoph Lucas
Rishiraj Bhattacharyya	Vadim Lyubashevsky
Joppe W. Bos	Avradip Mandal
Charles Bouillaguet	Nicolas Meloni
Billy Brumley	Shiho Moriai
Stanislav Bulygin	Adam O'Neill
Sébastien Canard	Somindu C Ramanna
Pierre-Louis Cayrel	Robert Rolland
Sandro Coretti	Greg Rose
Claus Diem	Minoru Saeki
Mario Di Raimondo	Subhabrata Samajder
Orr Dunkelman	Juraj Sarinay
Mohamed Elkadi	Alessandra Scafuro
Nadia El Mrabet	Nicolas Sendrier
Martin Franz	Douglas Stebila
Jun Furukawa	Daisuke Suzuki
Xiao-Shan Gao	Isamu Teranishi Stefano Tessaro
Carlos González Guillén	Elmar Tischhauser
Louis Goubin	Yuuki Tokunaga
Jonanthan Hoch	Keita Xagawa
Michal Hojsík	Bin Zhang
Laurent Imbert	

Table of Contents

Protocols

Secure Outsourced Computation	1
<i>Jake Loftus and Nigel P. Smart</i>	
Fully Simulatable Quantum-Secure Coin-Flipping and Applications	21
<i>Carolin Lunemann and Jesper Buus Nielsen</i>	
Efficient and Secure Generalized Pattern Matching via Fast Fourier Transform	41
<i>Damien Vergnaud</i>	
Identification Schemes from Key Encapsulation Mechanisms	59
<i>Hiroaki Anada and Seiko Arita</i>	

Cryptanalysis

Attacking Bivium and Trivium with the Characteristic Set Method	77
<i>Zhenyu Huang and Dongdai Lin</i>	
Improved Cryptanalysis of the Multi-Prime Φ -Hiding Assumption	92
<i>Mathias Herrmann</i>	
FPGA Implementation of a Statistical Saturation Attack against PRESENT	100
<i>Stéphanie Kerckhof, Baudoin Collard, and François-Xavier Standaert</i>	
Collisions of MMO-MD5 and Their Impact on Original MD5	117
<i>Yu Sasaki</i>	

Secret-Key Cryptography

Really Fast Syndrome-Based Hashing	134
<i>Daniel J. Bernstein, Tanja Lange, Christiane Peters, and Peter Schwabe</i>	
Montgomery's Trick and Fast Implementation of Masked AES	153
<i>Laurie Genelle, Emmanuel Prouff, and Michaël Quisquater</i>	

Efficient Implementations

Memory-Constrained Implementations of Elliptic Curve Cryptography in Co-Z Coordinate Representation	170
<i>Michael Hutter, Marc Joye, and Yannick Sierra</i>	
Efficient Multiplication in Finite Field Extensions of Degree 5	188
<i>Nadia El Mrabet, Aurore Guillevic, and Sorina Ionica</i>	

Cryptographic Schemes

Achieving Optimal Anonymity in Transferable E-Cash with a Judge	206
<i>Olivier Blazy, Sébastien Canard, Georg Fuchsbauer, Aline Gouget, Hervé Sibert, and Jacques Traoré</i>	
Revocable Attribute-Based Signatures with Adaptive Security in the Standard Model	224
<i>Alex Escala, Javier Herranz, and Paz Morillo</i>	

Algorithmic Problems

Using the Inhomogeneous Simultaneous Approximation Problem for Cryptographic Design	242
<i>Frederik Armknecht, Carsten Elsner, and Martin Schmidt</i>	
Analyzing Standards for RSA Integers	260
<i>Daniel Loebenberger and Michael Nüsken</i>	

Elliptic Curves

Hashing into Hessian Curves	278
<i>Reza Rezaeian Farashahi</i>	
On Randomness Extraction in Elliptic Curves	290
<i>Abdoul Aziz Ciss and Djiby Sow</i>	

Fault Analysis

Fault Analysis of Grain-128 by Targeting NFSR	298
<i>Sandip Karmakar and Dipanwita Roy Chowdhury</i>	
Differential Fault Analysis of Sosemanuk	316
<i>Yaser Esmaili Salehani, Aleksandar Kircanski, and Amr Youssef</i>	
An Improved Differential Fault Analysis on AES-256	332
<i>Subidh Ali and Debdeep Mukhopadhyay</i>	

Security Proofs

Benaloh's Dense Probabilistic Encryption Revisited	348
<i>Laurent Fousse, Pascal Lafourcade, and Mohamed Alnuaimi</i>	
On the Security of the Winternitz One-Time Signature Scheme	363
<i>Johannes Buchmann, Erik Dahmen, Sarah Ereth, Andreas Hülsing, and Markus Rückert</i>	

Invited Talks

Efficient Zero-Knowledge Proofs (Abstract)	379
<i>Jens Groth</i>	
Some Key Techniques on Pairing Vector Spaces	380
<i>Tatsuaki Okamoto and Katsuyuki Takashima</i>	
The NIST SHA-3 Competition: A Perspective on the Final Year	383
<i>Bart Preneel</i>	
Author Index	387