Lecture Notes in Computer Science 7374

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

Aikaterini Mitrokotsa Serge Vaudenay (Eds.)

Progress in Cryptology - AFRICACRYPT 2012

5th International Conference on Cryptology in Africa
Ifrane, Morocco, July 10-12, 2012
Proceedings

Springer

Volume Editors

Aikaterini Mitrokotsa
Serge Vaudenay
École Polytechnique Fédérale de Lausanne, IC LASEC
Bâtiment INF, Station 14, 1015 Lausanne, Switzerland
E-mail: {katerina.mitrokotsa, serge.vaudenay}@epfl.ch

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-31409-4 e-ISBN 978-3-642-31410-0
DOI 10.1007/978-3-642-31410-0
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012940535

CR Subject Classification (1998): E.3, K.6.5, C.2.0, C.2, E.4, K.4.4, H.4, J.1, F.2

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

The 5th Africacrypt conference was held July 10–12, 2012 in Ifrane, Morocco. It followed previous editions in Casablanca, Morocco (2008), Gammarth, Tunisia (2009), Stellenbosch, South Africa (2010), and Dakar, Senegal (2011).

The goal of the conference is to present research advances in the area of cryptography. It aims at bringing together in a friendly atmosphere researchers from all countries, beyond borders and political issues.

The conference received 56 submissions. They went through a doubly anonymous review process aided by 42 Program Committee members and 54 external reviewers. Our submission software invited authors to indicate from which continent they were. We counted 12 papers with at least one co-author from Africa.

Our invited talks were given by:

- Willi Meier (University of Applied Sciences and Arts Northwestern Switzerland) - *Stream Ciphers, A Perspective*
- Craig Gentry (IBM) - *Fully Homomorphic Encryption: Current State of the Art*
- Marc Fischlin (The Darmstadt University of Technology, Germany) - *Black-Box Reductions and Separations in Cryptography*

This volume represents the revised version of the 24 accepted contributed papers which were presented at the conference along with abstracts of invited speakers.

The Program Committee selected a paper to award. Committee members were invited to oppose to nominated papers and to vote on remaining ones. After this selection, the Program Committee decided to give the Africacrypt 2012 Best Paper Award to Elena Andreeva, Bart Mennink, Bart Preneel, and Marjan Skrobot for their paper:

> "Security Analysis and Comparison of the SHA-3 Finalists BLAKE, Groestl, JH, Keccak, and Skein"

The submission and review process was done using the *iChair* Web-based software system developed by Thomas Baignères and Matthieu Finiasz.

We would like to thank the authors of all submitted papers. Moreover, we are indebted to the members of the Program Committee and the external subreviewers for their diligent work. We would also like to acknowledge the conference organizers and the Steering Committee for supporting us and for the excellent collaboration we had.

Finally, we heartily thank the sponsors of Africacrypt 2012 for their generous support.

Aikaterini Mitrokotsa
Serge Vaudenay

Organization

Conference Chairs

General Chairs

Abdelhak Azhari	Ecole Normale Supérieure de Casablanca, Morocco
Tajjeeddine Rachidi	Al Akhawayn University in Ifrane, Morocco

Program Chair

Serge Vaudenay	EPFL, Switzerland

Publication Chair

Aikaterini Mitrokotsa	EPFL, Switzerland

Program Committee

Hatem M. Bahig	Ain Shams University, Egypt
Hussain Ben-Azza	Ensam-Meknès, Moulay Ismail University, Morocco
Alex Biryukov	University of Luxembourg, Luxembourg
Ivan Bjerre Damgård	University of Aarhus, Denmark
Riaal Domingues	South African Communications Security Agency, South Africa
Orr Dunkelman	University of Haifa and Weizmann Institute, Israel
Georg Fuchsbauer	University of Bristol, UK
Mustapha Hedabou	ENSA of Safi, Morocco
Antoine Joux	University of Versailles, France
Mike Just	Glasgow Caledonian University, UK
Seny Kamara	Microsoft Research, USA
Aggelos Kiayias	University of Athens, Greece
Evangelos Kranakis	Carleton University, Canada
Pascal Lafourcade	Verimag, University of Grenoble, France
Pil Joong Lee	Pohang University of Science and Technology (POSTECH), Korea
Reynald Lercier	DGA & University of Rennes, France
Helger Lipmaa	University of Tartu, Estonia
Javier Lopez	University of Malaga, Spain
Bruno Martin	University of Nice-Sophia Antipolis, France
Barbara Masucci	University of Salerno, Italy
Kanta Matsuura	The University of Tokyo, Japan

Aikaterini Mitrokotsa	EPFL, Switzerland
David Naccache	Ecole Normale Supérieure, France
Phong Nguyen	INRIA, France, and Tsinghua University, China
Abderrahmane Nitaj	University of Caen, France
Kaisa Nyberg	Aalto University, Finland
Ayoub Otmani	University of Caen and ENSICAEN, France
Khaled Ouafi	EPFL, Switzerland
Kenny Paterson	Royal Holloway University of London, UK
Goutam Paul	Jadavpur University, India
Christian Rechberger	DTU, Denmark
Magdy Saeb	Arab Academy of Science and Technology, Egypt
Rei Safavi-Naini	University of Calgary, Canada
Taizo Shirai	Sony Corporation, Japan
Djiby Sow	Cheikh Anta Diop University, Senegal
Martijn Stam	University of Bristol, UK
Ron Steinfeld	Macquarie University, Australia
Christine Swart	University of Cape Town, South Africa
Serge Vaudenay	EPFL, Switzerland
Ingrid Verbauwhede	K.U. Leuven, Belgium
Christopher Wolf	Ruhr University Bochum, Germany
Amr Youssef	Concordia University, Canada

External Reviewers

Ahmad Ahmadi	Pooya Farshim	Miodrag Mihaljevic
Hadi Ahmadi	Anna Lisa Ferrara	Shiho Moriai
Toru Akishita	Martin Gagné	Kris Narayan
Mohsen Alimomeni	David Galindo	Svetla Nikova
Tomoyuki Asano	Sourav Sen Gupta	Onur Özen
Josep Balasch	Anthony Van Herrewege	Sumit Kumar Pandey
Rishiraj Bhattacharyya	M. Jason Hinek	Ludovic Perret
Olivier Blazy	Sebastiaan Indesteege	Rodrigo Roman
Julia Borghoff	Kimmo Järvinen	Vladimir Rudskoy
Ioana Boureanu	Saqib A. Kakvi	Katerina Samari
Billy Brumley	Nikos Karvelas	Kyoji Shibutani
Pierre-Louis Cayrel	Geonwoo Kim	Rosemberg Silva
Rafik Chaabouni	Aleksandar Kircanski	Petr Sušil
Ashish Choudhury	Gregor Leander	Bogdan Warinschi
Marion Daubignard	Eun Sung Lee	Bingsheng Zhang
Jean Paul Degabriele	Jin-woo Lee	Wei Zhang
Vivien Dubois	Vadim Lyubashevsky	
Nadia El Mrabet	Roel Maes	
Mohamed Elkadi	Nele Mentens	

Table of Contents

Signature Schemes

Stream Ciphers

Applications of Information Theory

Block Ciphers

Network Security Protocols

Public-Key Cryptography

Cryptanalysis of Hash Functions

Hash Functions: Design and Implementation

Algorithms for Public-Key Cryptography

Cryptographic Protocols

Invited Talks