

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, Lancaster, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Zurich, Switzerland

John C. Mitchell

Stanford University, Stanford, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Dortmund, Germany

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbrücken, Germany

More information about this series at <http://www.springer.com/series/7410>

Marc Joye · Abderrahmane Nitaj (Eds.)

Progress in Cryptology - AFRICACRYPT 2017

9th International Conference on Cryptology in Africa
Dakar, Senegal, May 24–26, 2017
Proceedings

Editors

Marc Joye
NXP Semiconductors
San Jose, CA
USA

Abderrahmane Nitaj
University of Caen
Caen
France

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-57338-0 ISBN 978-3-319-57339-7 (eBook)
DOI 10.1007/978-3-319-57339-7

Library of Congress Control Number: 2017937579

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer International Publishing AG 2017

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, 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.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

The 9th International Conference on the Theory and Application of Cryptographic Techniques in Africa, Africacrypt 2017, took place May 24–26, 2017, in Dakar, Senegal. The conference was organized by Cheikh Anta Diop University, Dakar, Senegal, in cooperation with the International Association for Cryptologic Research (IACR). We heartily thank our general chairs, Mamadou Sangharé, Djiby Sow, and Abdoul Aziz Ciss, as well as the whole Organizing Committee for their efforts in making the conference a success.

The aim of Africacrypt is to provide an international forum for practitioners and researchers from industry, academia, and government from all over the world for a wide-ranging discussion of all forms of cryptography and its applications.

The conference received a total of 40 full papers, out of which 13 papers were selected for publication in these proceedings. Each submission was assigned at least three Program Committee (PC) members. In addition to the PC members, many external reviewers joined the review process in their particular areas of expertise. We were fortunate to have this energetic team of experts, and are deeply grateful to all of them for their hard work, which included a very active discussion phase. The paper submission, review, and discussion processes were effectively and efficiently made possible by the Web-based system developed by Shai Halevi. We thank him for his support and the IACR for hosting the review system. The program was completed with two keynote talks by Johannes Buchmann and Damien Stehlé, and by an invited talk by Luca De Feo. We are very grateful to them for accepting our invitation.

Last but not least, we would like to thank all the authors who submitted papers to this conference, the Organizing Committee members, colleagues, and student helpers for their valuable time and effort, and all the conference attendees who made this event a truly intellectually stimulating one through their active participation.

March 2017

Marc Joye
Abderrahmane Nitaj

Organization

AFRICACRYPT 2017

**9th International Conference on Cryptology in Africa, Dakar,
Senegal, May 24–26, 2017**

Africacrypt is the annual International Conference on the Theory and Applications of Security and Cryptography.

General Chairs

Mamadou Sangharé	Université Cheikh Anta Diop de Dakar, Senegal
Djiby Sow	Université Cheikh Anta Diop de Dakar, Senegal
Abdoul Aziz Ciss	École Polytechnique de Thiès, Senegal

Program Chairs

Marc Joye	NXP Semiconductors, USA
Abderrahmane Nitaj	Université de Caen, France

Program Committee

Riham Altawy	University of Waterloo, Canada
Muhammad R.K. Ariffin	UPM Kuala Lumpur, Malaysia
Abdelhak Azhari	Université de Casablanca, Morocco
Hussain Benazza	Université de Meknes, Morocco
Colin Boyd	NTNU, Norway
Dario Catalano	Università di Catania, Italy
Pierre-Louis Cayrel	Université Saint Etienne, France
Sherman S.M. Chow	CU Hong Kong, SAR China
Nadia El Mrabet	EMSE, France
Pierre-Alain Fouque	Université Rennes I, France
Georg Fuchsbauer	ENS Paris, France
Jens Groth	University College London, UK
Javier Herranz	Universidad Politècnica de Catalunya, Spain
Tetsu Iwata	Nagoya University, Japan
Saqib Kakvi	University of Bristol, UK
Seny Kamara	Brown University, USA
Fabien Laguillaumie	Université de Lyon I, France
Mark Manulis	University of Surrey, UK
Tarik Moataz	Brown University, USA
Ayoub Otmani	Université de Rouen, France

Thomas Peters	UCL, Belgium
Tajje-eddine Rachidi	Al Akhawayn University in Ifrane, Morocco
Vanishree Rao	PARC, USA
Magdy Saeb	Arab Academy for Science, Egypt
Rei Safavi-Naini	University of Calgary, Canada
Kazue Sako	NEC, Japan
Palash Sarkar	Indian Statistical Institute, India
Peter Schwabe	Radboud Universiteit, The Netherlands
Francesco Sica	Nazarbayev University, Kazakhstan
Djiby Sow	Université de Dakar, Senegal
François-Xavier Standaert	UCL, Belgium
Willy Susilo	University of Wollongong, Australia
Christine Swart	University of Cape Town, South Africa
Joseph Tonien	University of Wollongong, Australia
Amr M. Youssef	Concordia University, Canada

External Reviewers

Ali Akhavi	Elena Kirshanova
Lejla Batina	Stefan Koelbl
Christof Beierle	François Koeune
Olivier Blazy	Baptiste Lambin
Andrea Cerulli	Liran Lerman
Qian Chen	Fuchun Lin
Noureddine Chikouche	Mary Maller
Abdoul Aziz Ciss	Paz Morillo
Michael Clear	Thierry Mefenza Nountu
Edouard Cuvelier	Kazuma Ohara
Gareth Davies	Michele Orrù
Julien Devigne	Romain Poussier
Dario Fiore	Raghendra Rohit
Ryo Furukawa	Olivier Sanders
Romain Gay	Ben Smith
Benoît Gérard	Martin Strand
Essam Ghadafi	Isamu Teranishi
Aurore Guillevic	Nicolas Thériault
Mohammad Hajiabadi	Yosuke Todo
Tsuchida Hikaru	Mohamed Tolba
Vincenzo Iovino	Christine van Vredendaal
Sune K. Jakobsen	Vesselin Velichkov
Jérémy Jean	Alexandre Wallet
Abdel Alim Kamal	Fredrich Wiemer
Sabyasachi Karati	Yongjun Zhao
Ahmed Abdel Khalek	

Contents

Cryptographic Schemes

RingRainbow – An Efficient Multivariate Ring Signature Scheme.	3
<i>Mohamed Saied Emam Mohamed and Albrecht Petzoldt</i>	
Pinocchio-Based Adaptive zk-SNARKs and Secure/Correct Adaptive Function Evaluation.	21
<i>Mei of Veenigen</i>	
Revisiting and Extending the AONT-RS Scheme: A Robust Computationally Secure Secret Sharing Scheme	40
<i>Liqun Chen, Thalia M. Laing, and Keith M. Martin</i>	

Side-Channel Analysis

Climbing Down the Hierarchy: Hierarchical Classification for Machine Learning Side-Channel Attacks	61
<i>Stjepan Picek, Annelie Heuser, Alan Jovic, and Axel Legay</i>	
Multivariate Analysis Exploiting Static Power on Nanoscale CMOS Circuits for Cryptographic Applications	79
<i>Milena Djukanovic, Davide Bellizia, Giuseppe Scotti, and Alessandro Trifiletti</i>	
Differential Bias Attack for Block Cipher Under Randomized Leakage with Key Enumeration.	95
<i>Haruhisa Kosuge and Hidema Tanaka</i>	

Differential Cryptanalysis

Impossible Differential Cryptanalysis of Reduced-Round SKINNY	117
<i>Mohamed Tolba, Ahmed Abdelkhalek, and Amr M. Youssef</i>	
Impossible Differential Attack on Reduced Round SPARX-64/128	135
<i>Ahmed Abdelkhalek, Mohamed Tolba, and Amr M. Youssef</i>	

Applications

Private Conjunctive Query over Encrypted Data	149
<i>Tushar Kanti Saha and Takeshi Koshihira</i>	

Efficient Oblivious Transfer from Lossy Threshold Homomorphic Encryption 165
Isheeta Nargis

Privacy-Friendly Forecasting for the Smart Grid Using Homomorphic Encryption and the Group Method of Data Handling 184
Joppe W. Bos, Wouter Castryck, Ilia Iliashenko, and Frederik Vercauteren

Number Theory

On Indifferentiable Hashing into the Jacobian of Hyperelliptic Curves of Genus 2. 205
Michel Seck, Hortense Boudjou, Nafissatou Diarra, and Ahmed Youssef Ould Cheikh Khilil

Cryptanalysis of Some Protocols Using Matrices over Group Rings. 223
Mohammad Eftekhari

Author Index 231