

Lecture Notes in Computer Science

14064

Founding Editors

Gerhard Goos

Juris Hartmanis

Editorial Board Members

Elisa Bertino, *Purdue University, West Lafayette, IN, USA*

Wen Gao, *Peking University, Beijing, China*

Bernhard Steffen , *TU Dortmund University, Dortmund, Germany*

Moti Yung , *Columbia University, New York, NY, USA*

The series Lecture Notes in Computer Science (LNCS), including its subseries Lecture Notes in Artificial Intelligence (LNAI) and Lecture Notes in Bioinformatics (LNBI), has established itself as a medium for the publication of new developments in computer science and information technology research, teaching, and education.

LNCS enjoys close cooperation with the computer science R & D community, the series counts many renowned academics among its volume editors and paper authors, and collaborates with prestigious societies. Its mission is to serve this international community by providing an invaluable service, mainly focused on the publication of conference and workshop proceedings and postproceedings. LNCS commenced publication in 1973.

Nadia El Mrabet · Luca De Feo ·
Sylvain Duquesne
Editors

Progress in Cryptology - AFRICACRYPT 2023

14th International Conference
on Cryptology in Africa, Sousse, Tunisia, July 19–21, 2023
Proceedings

Editors

Nadia El Mrabet 
EMSE
Saint-Étienne, France

Luca De Feo 
IBM Research Europe
Rüschlikon, Switzerland

Sylvain Duquesne 
Université de Rennes 1
Rennes Cedex, France

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-031-37678-8

ISBN 978-3-031-37679-5 (eBook)

<https://doi.org/10.1007/978-3-031-37679-5>

© The Editor(s) (if applicable) and The Author(s), under exclusive license
to Springer Nature Switzerland AG 2023

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, expressed 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.

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

Preface

This volume contains the papers accepted for presentation at Africacrypt 2023, the 14th International Conference on the Theory and Application of Cryptographic Techniques in Africa. The aim of this series of conferences is to provide an international forum for practitioners and researchers from industry, academia, and government agencies for a discussion of all forms of cryptography and its applications. The initiative of organizing Africacrypt started in 2008 and it was first held in Morocco. Subsequent yearly events were held in Tunisia, South Africa, Senegal, Morocco, Egypt and Tunisia. This year, Africacrypt 2023 is organized by the University of Monastir and the Tunisian Mathematical Society in cooperation with the International Association for Cryptologic Research (IACR). It was held in Sousse, during July 19–21, under the high patronage of the Tunisian minister of communication technologies.

We received 59 submissions authored by researchers from countries from all over the world. After a double-blind reviewing process that included online discussion and involved 47 Program Committee members and 23 external reviewers, we decided to accept 21 papers resulting in an acceptance rate of around 35%. All submitted papers received at least three reviews. We thank the Program Committee and the external reviewers for their diligent work and fruitful discussions and we thank the authors of all submitted papers for supporting the conference.

The conference program featured three keynote speakers, Ward Beullens from IBM Research Europe, Switzerland, Anne Canteaut from INRIA Paris, France and Koray Karabina from the National Research Council of Canada. We were happy that they agreed to attend and deliver their keynotes physically. The technical program was also enriched by a poster session organized by Abderrahmane Nitaj and Hoda Alkhzaimi. We thank them for taking this part of the program fully out of our hands and taking care of submissions, final versions, and chairing the poster session. A Capture the Flag (CTF) competition was introduced in the conference this year and was organized by Souheib Youssfi, Alyssa Berriche and Ahmed Belkahla.

The General Chairs, Leila Ben Abdelghani from the University of Monastir, Tunisia and Loubna Ghammam from ITK Engineering GmbH (Bosch), Germany, were a pleasure to work with. We thank the staff at Springer for their help with the proceedings production. Without our sponsors, in particular the Technology Innovation Institute from Abu Dhabi as a platinum sponsor, not all of the support for speakers and local organization facilities would have been possible and we thank them for that.

Acting as program chairs for Africacrypt 2023 was a privilege and a great experience, thanks go to all those people who helped us make this conference a big success.

May 2023

Luca De Feo
Sylvain Duquesne
Nadia El Mrabet

Organization

General Chairs

Leila Ben Abdelghani
Loubna Ghammam

University of Monastir, Tunisia
ITK Engineering GmbH (Bosch), Germany

Program Chairs

Nadia El Mrabet
Luca De Feo
Sylvain Duquesne

École des Mines de Saint-Étienne, France
IBM Research Europe, Switzerland
University of Rennes, France

Invited Speakers

Ward Beullens
Anne Canteaut
Koray Karabina

IBM Research Europe, Switzerland
INRIA Paris, France
National Research Council, Canada

Steering Committee

Souheib Yousfi (Chair)
Nizar Kerkeni
Lina Mortajine
Abderrahmane Nitaj
Sami Omar
Amal Samti

University of Carthage, Tunisia
University of Monastir, Tunisia
ITK Engineering GmbH (Bosch), Germany
University of Caen Normandie, France
University of Bahrain, Bahrain
University of Monastir, Tunisia

Program Committee

Riham AlTawy
Laila El Aïmani
Hoda Alkhzaimi

University of Victoria, Canada
University of Caddi Ayyad, Morocco
NYU Abu Dhabi, United Arab Emirates

Greg Alpar	Open University, The Netherlands
Kevin Atighechi	University of Clermont-Ferrand, France
Hatem M. Bahig	Ain Shams University, Egypt
Hussain Benazza	UMI, ENSAM Meknes, Morocco
Shivam Bhasin	Temasek Lab, Nanyang Technological University, Singapore
Sebastien Canard	Orange Labs, France
Suvradip Chakraborty	ETH, Switzerland
Chitchanok Chuengsatiansup	University of Melbourne, Australia
Tingting Cui	HangZhou DianZi University, China
Joan Daemen	Radboud University, The Netherlands
Youssef El Housni	ConsenSys R&D, France
Georgios Fotiadis	University of Luxembourg
Emmanuel Fouotsa	University of Bamenda, Cameroon
Gina Gallegos-Garcia	Instituto Politécnico Nacional, Mexico
Romain Gay	IBM Research, Switzerland
Loubna Ghammam	ITK Engineering GmbH (Bosch), Germany
Satrajit Ghosh	IIT Kharagpur, India
Lorenzo Grassi	Radboud University, The Netherlands
Javier Herranz	Universitat Politècnica de Catalunya, Spain
Akinori Hosoyamada	NTT, Japan
Sorina Ionica	University of Picardie, France
Juliane Kramer	TU Darmstadt, Germany
Fabien Laguillaumie	University of Montpellier, France
Patrick Longa	Microsoft Research, Redmond, US
Marc Manzano	SandboxAQ, Spain
Sarah McCarthy	University of Waterloo, Canada
Marine Minier	Université de Lorraine, France
Mainack Mondal	Indian Institute of Technology (IIT), India
Abderrahmane Nitaj	University of Caen Normandie, France
Sami Omar	University of Bahrain, Bahrain
Yanbin Pan	Chinese Academy of Science, China
Sikhar Patranabis	IBM Research, India
Christophe Petit	University of Birmingham, UK
Elizabeth A. Quaglia	Royal Holloway, University of London, UK
Divya Ravi	Aarhus University, Denmark
Joost Renes	NXP, The Netherlands
Yann Rotella	Université Paris-Saclay, France
Simona Samardjiska	Radboud University, The Netherlands
Ali Aydin Selcuk	TOBB University of Economics and Technology, Turkey
Dave Singelee	KU Leuven, Belgium

Djiby Sow

Pontelimon Stanica

Vanessa Vitse

Souheib Yousfi

University of Dakar, Senegal

Naval Postgraduate School, Monterey, USA

University of Grenoble, France

University of Carthage, Tunisia

Additional Reviewers

Khalid Abdelmoumen

Ismail Afia

Barbara Jiabao Benedikt

Harishma Boyapally

Guilhem Castagnos

Marwa Chaieb

Alfonso Francisco De Abiega L'Eglise

Kevin Andrae Delgado Vargas

Siemen Dhooghe

Sayon Duttagupta

Samed DüzlÜ

Paul Frixons

Koustabh Ghosh

Tchoffo Saha Gustave

Çağdaş Gül

Jodie Knapp

Matthieu Lequesne

Soundes Marzougui

Lina Mortajine

Georgio Nicolas

Jean-Baptiste Orfila

Aurel Page

Santanu Sarkar

Ugur Sen

Ferdinand Sibleyras

Marloes Venema

Yanhong Xu

Trevor Yap

Steven Yue

Murat Burhan İlter

Contents

Post-quantum Cryptography

MinRank in the Head: Short Signatures from Zero-Knowledge Proofs	3
<i>Gora Adj, Luis Rivera-Zamarripa, and Javier Verbel</i>	
Take Your MEDS: Digital Signatures from Matrix Code Equivalence	28
<i>Tung Chou, Ruben Niederhagen, Edoardo Persichetti, Tovohery Hajatiana Randrianarisoa, Krijn Reijnders, Simona Samardjiska, and Monika Trimoska</i>	
Efficient Computation of $(3^n, 3^n)$ -Isogenies	53
<i>Thomas Decru and Sabrina Kunzweiler</i>	
On the Post-quantum Security of Classical Authenticated Encryption Schemes	79
<i>Nathalie Lang and Stefan Lucks</i>	
A Side-Channel Attack Against <i>Classic McEliece</i> When Loading the Goppa Polynomial	105
<i>Boly Seck, Pierre-Louis Cayrel, Vlad-Florin Dragoi, Idy Diop, Morgan Barbier, Jean Belo Klamti, Vincent Grosso, and Brice Colombier</i>	

Symmetric Cryptography

Universal Hashing Based on Field Multiplication and (Near-)MDS Matrices ...	129
<i>Koustabh Ghosh, Jonathan Fuchs, Parisa Amiri Eliasi, and Joan Daemen</i>	
Invertible Quadratic Non-linear Functions over $\mathbb{F}_p^n$ via Multiple Local Maps ...	151
<i>Ginevra Giordani, Lorenzo Grassi, Silvia Onofri, and Marco Pedicini</i>	
POSEIDON2: A Faster Version of the POSEIDON Hash Function	177
<i>Lorenzo Grassi, Dmitry Khovratovich, and Markus Schafneggger</i>	
From Unbalanced to Perfect: Implementation of Low Energy Stream Ciphers	204
<i>Jikang Lin, Jiahui He, Yanhong Fan, and Meiqin Wang</i>	

Cryptanalysis

The Special Case of Cyclotomic Fields in Quantum Algorithms for Unit Groups 229
Razvan Barbulescu and Adrien Poulalion

Improved Cryptanalysis of the Multi-Power RSA Cryptosystem Variant 252
Abderrahmane Nitaj and Maher Boudabra

Blockchain

The Curious Case of the Half-Half Bitcoin ECDSA Nonces 273
Dylan Rowe, Joachim Breitner, and Nadia Heninger

Maravedí: A Secure and Practical Protocol to Trade Risk for Instantaneous Finality 285
Mario Larangeira and Maxim Jourenko

Lattice-Based Cryptography

ComBo: A Novel Functional Bootstrapping Method for Efficient Evaluation of Nonlinear Functions in the Encrypted Domain 317
Pierre-Emmanuel Clet, Aymen Boudguiga, Renaud Sirdey, and Martin Zuber

Concrete Security from Worst-Case to Average-Case Lattice Reductions 344
Joel Gärtner

Finding and Evaluating Parameters for BGV 370
Johannes Mono, Chiara Marcolla, Georg Land, Tim Güneysu, and Najwa Aaraj

Quantum Search-to-Decision Reduction for the LWE Problem 395
Kyohei Sudo, Masayuki Tezuka, Keisuke Hara, and Yusuke Yoshida

Implementations

Fast Falcon Signature Generation and Verification Using ARMv8 NEON Instructions 417
Duc Tri Nguyen and Kris Gaj

Benchmarking and Analysing the NIST PQC Lattice-Based Signature Schemes Standards on the ARM Cortex M7 442
James Howe and Bas Westerbaan

Theory

Impossibilities in Succinct Arguments: Black-Box Extraction and More 465
 Matteo Campanelli, Chaya Ganesh, Hamidreza Khoshakhlagh,
 and Janno Siim

Applications of Timed-Release Encryption with Implicit Authentication 490
 Angelique Loe, Liam Medley, Christian O’Connell,
 and Elizabeth A. Quaglia

Author Index 517