Lecture Notes in Computer Science **11627**

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

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

Johannes Buchmann · Abderrahmane Nitaj ·
Tajjeeddine Rachidi (Eds.)

Progress in Cryptology – AFRICACRYPT 2019

11th International Conference on Cryptology in Africa
Rabat, Morocco, July 9–11, 2019
Proceedings

Springer

Editors
Johannes Buchmann
Technical University of Darmstadt
Darmstadt, Germany

Abderrahmane Nitaj
Université de Caen
Caen, France

Tajjeeddine Rachidi
Al Akhawayn University
Ifrane, Morocco

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-23695-3 ISBN 978-3-030-23696-0 (eBook)
https://doi.org/10.1007/978-3-030-23696-0

LNCS Sublibrary: SL4 – Security and Cryptology

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

Preface

The 11th edition of the International Conference on the Theory and Applications of Cryptographic Techniques, Africacrypt 2019 was held in Rabat, Morocco, during July 9–11, 2019. The conference was organized by Al Akhawayn University in Ifrane (AUI), Morocco, in cooperation with the International Association for Cryptologic Research (IACR). Tajjeeddine Rachidi (AUI, Morocco) was responsible for the local organization, supported by a local organizing team consisting of Dr. Latifa ElMortaji, Ibtissam Latachi, and Bouchra Saad. We are indebted to them for their support and smooth collaboration.

The aim of Africacrypt 2019 was to provide an international forum for researchers from academia and practitioners from industry from all over the world, for discussions regarding all forms of cryptology, coding theory, and information security.

We had the privilege of chairing the Program Committee, which consisted of 35 members. There were 53 papers submitted to the conference. Each paper was assigned to at least three members of the Program Committee and was reviewed anonymously. The review process was challenging and the Program Committee, aided by reports from 59 external reviewers, produced a total of 166 reviews in all. In total, 22 papers were accepted on May 2, 2019. Authors then had the opportunity to update their papers until May 10, 2019. The present proceedings include all the revised papers. We are indebted to the members of the Program Committee and the external reviewers for their diligent work.

The conference was honored by the presence of two invited speakers, namely, Martin R. Albrecht, who spoke on "So How Hard Is Solving Hard Lattice Problems Anyway?" and Sebastian Faust with his talk "Scaling Blockchains with Off-chain Protocols." We are grateful to them.

We also would like to thank the authors of all submissions and all the speakers, as well all the participants. They all contributed to the success of the conference, and to making Africacrypt conference series an excellent forum for the advancement of cryptology.

We are also thankful to the staff at Springer for their help with producing the proceedings and to the staff of EasyChair for the use of their conference management system.

Last but not least, we thank Professor Driss Ouaouicha, President of Al Akhawayn University in Ifrane, Morocco, for his unconditional support of Africacrypt. We extend our gratitude to Group OCP and Les Eaux Minérales d'Oulmès, gold and bronze sponsors of the conference.

May 2019

Johannes Buchmann
Abderrahmane Nitaj
Tajjeeddine Rachidi

Organization

Africacrypt 2019 was organized by Al Akhawayn University in Ifrane, Morocco.

General Chair

Tajjeeddine Rachidi	Al Akhawayn University in Ifrane, Morocco

Program Chairs

Johannes Buchmann	TU Darmstadt, Germany
Abderrahmane Nitaj	University of Caen Normandie, France
Tajjeeddine Rachidi	Al Akhawayn University in Ifrane, Morocco

Invited Speakers

Martin R. Albrecht	Royal Holloway, University of London, UK
Sebastian Faust	TU Darmstadt, Germany

Organizing Committee

Tajjeeddine Rachidi (Chair)	Al Akhawayn University in Ifrane, Morocco
Latifa ElMortaji	Al Akhawayn University in Ifrane, Morocco
Ibtissam Latachi	FSDM, USMBA, Morocco
Bouchra Saad	Al Akhawayn University in Ifrane, Morocco

Program Committee

Elena Andreeva	Katholieke Universiteit Leuven, Belgium
Muhammad Rezal Kamel Ariffin	Institute for Mathematical Research, UPM, Malaysia
Hatem M. Bahig	Ain Shams University, Egypt
Magali Bardet	University of Rouen Normandie, France
Lejla Batina	Radboud University, The Netherlands
Hussain Ben-Azza	ENSAM, Meknes, Morocco
Olivier Blazy	University of Limoges, France
Colin Boyd	Norwegian University of Science and Technology, Norway
Sébastien Canard	Orange Labs, Caen, France
Sherman S. M. Chow	The Chinese University of Hong Kong, SAR China
Nicolas Courtois	University College London, UK
Joan Daemen	Radboud University, The Netherlands

Luca De Feo	University of Versailles, France
Sow Djiby	University Cheikh Anta Diop, Dakar, Senegal
Nadia El Mrabet	SAS - CGCP - EMSE, Saint Etienne, France
Javier Herranz	Universitat Politècnica de Catalunya, Spain
Sorina Ionica	University of Picardie, France
Tetsu Iwata	Nagoya University, Japan
Juliane Krämer	TU Darmstadt, Germany
Subhamoy Maitra	Indian Statistical Institute, India
Abderrahmane Nitaj	University of Caen Normandie, France
Yanbin Pan	Chinese Academy of Sciences, Beijing, China
Christophe Petit	University of Oxford, UK
Elizabeth Quaglia	Royal Holloway, University of London, UK
Tajjeeddine Rachidi	Al Akhawayn University of Ifrane, Morocco
Adeline Roux-Langlois	CNRS - IRISA, France
Palash Sarkar	Indian Statistical Institute, India
Alessandra Scafuro	North Carolina State University, USA
Ali Aydin Selcuk	TOBB University, Turkey
Pantelimon Stanica	Naval Postgraduate School, Monterey, USA
Noah Stephens-Davidowitz	Massachusetts Institute of Technology, USA
Joseph Tonien	University of Wollongong, Australia
Damien Vergnaud	Pierre and Marie Curie University/Institut Universitaire de France, Paris, France
Vanessa Vitse	University of Grenoble Alpes, France
Amr Youssef	Concordia University, Montreal, Canada

Additional Reviewers

Khalid Abdelmoumen	Saqib A. Kakvi	Constanza Riera
Alexandre Adomnicai	Orhun Kara	Yann Rotella
Guy Barwell	Robin Larrieu	Simona Samardjiska
Jean Belo Klamti	Rio LaVigne	Olivier Sanders
Pauline Bert	Ela Lee	Patrick Struck
Carl Bootland	Isis Lovecruft	Halil Kemal Taskin
Laura Brouilhet	Jack P. K. Ma	Yannick Teglia
Ahmet Burak Can	Ramiro Martínez	Oleksandr Tkachenko
Ilaria Chillotti	Pedro Maat Massolino	Jacques Traoré
Thomas Debris	Simon-Philipp Merz	Marloes Venema
Christoph Dobraunig	Romy Minko	Jorge Villar
Gautier Eberhart	Lina Mortajine	Jiafan Wang
Pierre-Alain Fouque	Suleyman Ozarslan	Xiuhua Wang
Ashley Fraser	Kostas Papagiannopoulos	Léo Weissbart
Ariel Gabizon	Albrecht Petzoldt	Weiqiang Wen
Lydia Garms	Robert Primas	Yang Yu
Chris Hicks	Chen Qian	Yongjun Zhao
Murat Ilter	Sebastian Ramacher	

Sponsoring Institutions

- OCP Group, Morocco (Gold sponsor)

- Les Eaux Minérales d'Oulmès, Morocco (Bronze sponsor)

Origin of Submissions

Australia
Austria
Belgium
Brazil
Canada
China
Cyprus
Estonia
Finland
France
Germany
Hong Kong
India
Italy
Japan
Morocco
The Netherlands
Norway
Spain
Switzerland
Tunisia
Turkey
United Arab Emirates
United Kingdom
United States

Abstracts of Invited Talks

So How Hard Is Solving Hard Lattice Problems Anyway?

Martin R. Albrecht

Information Security Group, Royal Holloway, University of London

Abstract. Establishing the cost of solving hard lattice problems is a pressing concern at the moment owing to schemes reliant on these problems being considered for deployment. In this talk, I discuss recent advances in this area in recent years, both in the classic and in the quantum world, to arrive at the current state of the art.

Keywords: Lattice-based cryptography · Post-quantum · Learning with errors

Scaling Blockchains with Off-Chain Protocols

Sebastian Faust

TU Darmstadt, Germany

Abstract. One of the main challenges of decentralized blockchain systems is scalability. For instance, in Bitoin – the most popular blockchain system – transactions can take up to 10 minutes until they are processed, and throughput is limited to five to seven transactions per second. A promising approach to improve scalability of blockchains is represented by off-chain protocols. Off-chain protocols work by building a second layer network over the blockchain, thereby allowing that the massive amount of transactions is carried out directly between the involved users. There has recently been a plethora of different constructions for off-chain protocols proposed by industry and academia. Examples of such systems are the Lightning network for Bitcoin, state channel constructions such as Counterfactual or Perun, and various types of Plasma systems for Ethereum. In this talk, we summarize some of the recent progress that has been made in the field of off-chain protocols.

Keywords: Blockchain · Off-chain protocols · State channels

Contents