Lecture Notes in Computer Science 10194

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

Editorial Board

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

Said El Hajji · Abderrahmane Nitaj
El Mamoun Souidi (Eds.)

Codes, Cryptology and Information Security

Second International Conference, C2SI 2017
Rabat, Morocco, April 10–12, 2017, Proceedings
In Honor of Claude Carlet

Springer

Editors
Said El Hajji
University Mohamed V in Rabat
Rabat
Morocco

El Mamoun Souidi
University Mohamed V in Rabat
Rabat
Morocco

Abderrahmane Nitaj
University of Caen Normandie
Caen
France

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-55588-1 ISBN 978-3-319-55589-8 (eBook)
DOI 10.1007/978-3-319-55589-8

Library of Congress Control Number: 2017934218

LNCS Sublibrary: SL4 – Security and Cryptology

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

This volume contains the papers accepted for presentation at C2SI-Carlet 2017, in honor of Professor Claude Carlet, from the University of Paris 8, France. C2SI-Carlet is an international conference on the theory and applications of cryptographic techniques, coding theory, and information security. One aim of this conference is to pay homage to Claude Carlet for his valuable contribution in teaching and disseminating knowledge in coding theory and cryptography worldwide, especially in Africa. The other aim of the conference is to provide an international forum for researchers from academia and practitioners from industry from all over the world for discussion of all forms of cryptology, coding theory, and information security.

The initiative of organizing C2SI-Carlet 2017 was initiated by the Moroccan Laboratory of Mathematics, Computing Sciences and Applications (LabMIA) at the Faculty of Sciences of the Mohammed V University in Rabat and performed by an active team of researchers from Morocco and France. The conference was organized in cooperation with the International Association for Cryptologic Research (IACR), and the proceedings are published in Springer's *Lecture Notes in Computer Science* series.

The first conference in this series was held at the same university during May 26–28, 2015, for which the proceedings were published in Springer's *Lecture Notes in Computer Sciences* as volume 9084.

The C2SI-Carlet 2017 Program Committee consisted of 49 members. There were 72 papers submitted to the conference. Each paper was assigned to two or three members of the Program Committee and was reviewed anonymously. The review process was challenging and the Program Committee, aided by reports from 26 external reviewers, produced a total of 164 reviews in all. After this period, 19 papers were accepted on January 28, 2017. Authors then had the opportunity to update their papers until February 6, 2017. 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 the invited speakers Mohammed Essaaidi, Caroline Fontaine, Maria Isabel Garcia Planas, Sylvain Guilley, and Tor Helleseth. They gave talks on various topics in cryptography, coding theory, and information security and contributed to the success of the conference.

We had the privilege to chair the Program Committee. We would like to thank all committee members for their work on the submissions, as well as all external reviewers for their support. We thank the authors of all submissions and all the speakers as well all the participants. They all contributed to the success of the conference.

We also would like to thank Professor Saaid Amzazi, Head of Mohammed V University in Rabat, for his unwavering support to research and teaching in the areas of cryptography, coding theory, and information security. We also want to thank Professor Mourad El Belkacemi, Dean of Faculty of Sciences in Rabat.

We are deeply grateful to Professor Claude Carlet for the great service in contributing to the establishment of a successful research group in coding theory, cryptography, and information security at the Faculty of Sciences of Mohammed V University in Rabat. We would like to take this opportunity to acknowledge his professional work.

Along with these individuals, we wish to thank our local colleagues and students who contributed greatly to the organization and success of the conference.

Finally, we heartily thank all the local Organizing Committee members, all sponsors, and everyone who contributed to the success of this conference. 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.

April 2017

S. El Hajji
A. Nitaj
E.M. Souidi

Organization

C2SI-Carlet 2017 was organized by the Moroccan Laboratory of Mathematics, Computing Sciences and Applications (LabMIA) at the Faculty of Sciences of the Mohammed V University in Rabat.

Honorary Chairs

Saaid Amzazi	President of Mohammed V University in Rabat, Morocco
Claude Carlet	Paris 8 University, Paris, France

General Chair

Said El Hajji	Mohammed V University in Rabat, Morocco

Program Chairs

Said El Hajji	Mohammed V University in Rabat, Morocco
Abderrahmane Nitaj	University of Caen Normandie, France
El Mamoun Souidi	Mohammed V University in Rabat, Morocco

Organizing Committee

Said El Hajji (Chair)	LabMIA, Mohammed V University in Rabat, Morocco
El Mamoun Souidi (Co-chair)	LabMIA, Mohammed V University in Rabat, Morocco
Ghizlane Orhanou (Co-chair)	LabMIA, Mohammed V University in Rabat, Morocco
Abdelmalek Azizi	Mohammed I University, Morocco
Hicham Bensaid	INPT, Rabat, Morocco
Hafssa Benaboud	Mohammed V University in Rabat, Morocco
Redouane Benaini	Mohammed V University in Rabat, Morocco
Youssef Bentaleb	Ibn Tofail University, Kenitra, Morocco
Souad EL Bernoussi	Mohammed V University in Rabat, Morocco
Sidi Mohamed Douiri	Mohammed V University in Rabat, Morocco
Abelkrim Haqiq	Hassan I University, Settat, Morocco
Hicham Laanaya	Mohammed V University in Rabat, Morocco
Jalal Laassiri	Ibn Tofail University, Kenitra, Morocco
Mounia Mikram	Information Science School, Rabat, Morocco
Faissal Ouardi	Mohammed V University in Rabat, Morocco

Program Committee

Anas Aboulkalam	Cadi Ayyad University, Morocco
Amr Youssef	Concordia University, Canada
Muhammad Rezal Kamel Ariffin	University Putra Malaysia, Malaysia
François Arnault	University of Limoges, France
Hafssa Benaboud	Mohammed V University in Rabat, Morocco
Abdelmalek Azizi	Mohammed I University, Morocco
Youssef Bentaleb	Ibn Tofail University, Kenitra, Morocco
Thierry Berger	University of Limoges, France
Mohamed Bouhdadi	Mohammed V University in Rabat, Morocco
Mohammed Boulmalf	UIR, Rabat, Morocco
Lilya Budaghyan	University of Bergen, Norway
Anne Canteaut	Inria Rocquencourt, France
Claude Carlet	Paris 8 University, France
Pierre Louis Cayrel	University of Saint Etienne, France
Sherman S.M. Chow	The Chinese University of Hong Kong, SAR China
Pierre Dusart	University of Limoges, France
Nadia El Mrabet	SAS Ecole des Mines de Saint Etienne, Gardanne, France
Caroline Fontaine	Telecom Bretagne, Rennes, France
Philippe Gaborit	University of Limoges, France
Maria Isabel Garcia Planas	Catalonia University, Barcelona, Spain
Sanaa Ghouzali	King Saud University, Riyadh, Saudi Arabia
Guang Gong	University of Waterloo, Canada
Aline Gouget	Gemalto, France
Sylvain Guilley	TELECOM ParisTech and SecureIC S.A.S., France
Tor Helleseth	Bergen University, Norway
Mohammed Essaaidi	IEEE Section Morocco, Mohammed V University in Rabat, Morocco
Sidi Mohamed Douiri	Mohammed V University in Rabat, Morocco
Abelkrim Haqiq	Hassan I University, Settat, Morocco
Zoubida Jadda	Defense Department Vannes Coëtquidan, France
JonLark Kim	Sogang University, Seoul, South Korea
Salahddine Krit	IbnZohr University, Ouarzazate, Morocco
Jalal Laassiri	Ibn Tofail University, Kenitra, Morocco
Jean Louis Lanet	Inria Bretagne Atlantique, France
Sihem Mesnager	University of Paris 8, France
Mounia Mikram	Information Sciences School in Rabat, Morocco
Marine Minier	Laboratoire LORIA, University of Lorraine, Nancy, France
Ghizlane Orhanou	Mohammed V University in Rabat, Morocco
Faissal Ouardi	Mohammed V University in Rabat, Morocco
Ali Ouadfel	LabMIA, Mohammed V University in Rabat, Morocco
Francesco Sica	Nazarbayev University, Kazakhstan

Partrice Parraud	Defense Department Vannes Coëtquidan, France
Emmanuel Prouff	Safran Identity and Security and Université Pierre et Marie Curie, Paris, France
Mohamed Rziza	Mohammed V University in Rabat, Morocco
Pantelimon (Pante) Stanica	Naval Postgraduate School, USA
Joseph Tonien	University of Wollongong, Australia
Felix Ulmer	Université de Rennes 1, France
Damien Vergnaud	Ecole Normale Supérieure, Paris, France
Fouad Zinoun	Mohammed V University in Rabat, Morocco

Additional Reviewers

Amit Kumar Chauhan	Mohammed Benabdellah
Cedric Lauradoux	Nian Li
Chunlei Li	Nicolas Gama
David Pointcheval	Rafael Misoczki
Delphine Boucher	Raghvendra Rohit
Edoardo Persichetti	Riham Altawy
Essaid Chanigui	Said El Kafhali
Guillame Barbu	Siham Ezzouak
Guillaume Bouffard	Steve Szabo
Jean Belo Klamti	Thomas Debris-Alazard
Jiafan Wang	Wilfried Meidl
Kalikinkar Mandal	Xiuhua Wang
Matthew Parker	Yongjun Zhao

Invited Speakers

Mohammed Essaaidi	Mohammed V University in Rabat, Morocco
Caroline Fontaine	TELECOM Bretagne, France
Maria Isabel Garcia Planas	UPC, Universitat Politècnica de Catalunya, Spain
Sylvain Guilley	TELECOM-Paris Tech, France
Tor Helleseth	University of Bergen, Norway

Sponsoring Institutions

Ministère de l'Enseignement Supérieur, de la Recherche Scientifique et de la Formation des Cadres
Faculty of Sciences, Mohammed V University in Rabat, Morocco
Centre Marocain de Recherches Polytechniques et d'Innovation, Morocco
Laboratoire de Mathématiques, Informatique et Applications (LabMIA), Rabat, Morocco
Ministère de l'Industrie, du Commerce, de l'Investissement et de l'Economie Numérique, Morocco

Biography of Claude Carlet

Claude Carlet received in 1990 the Ph.D. degree from the University of Paris 6, France and in 1994 the Habilitation to Direct theses from the University of Amiens, France. He was associate professor in the Department of Computer Science at the University of Amiens from 1990 to 1994, and professor in the Department of Computer Science at the University of Caen, France, from 1994 to 2000 and in the department of Mathematics at the University of Paris 8, France, from 2000 to 2017. His research interests include Boolean functions (bent, correlation-immune, algebraic immune, SAC, etc.), vectorial functions (APN, etc.), cryptography (in particular, stream ciphers, block ciphers and side-channel attacks) finite fields and coding theory (in relationship with the domains above). He has participated as chapter author or editor to 11 books, (co-)written 100 journal papers, 60 papers in proceedings and 20 shorter international papers. He has been member of 70 program committees (7 as co-chair). He has been in charge of the French research group "codage-cryptographie C2" during ten years. He has been Associate Editor of IEEE Transactions on Information Theory and is currently editor in chief of the journal Cryptography and Communications (SPRINGER) and editor in the 4 journals DCC (SPRINGER), AMC (American Institute of Mathematical Sciences), IJCM-TCOM (Taylor & Francis) and IJOCT (Inderscience Publishers). He has supervised 13 students and is currently supervising 5. He has been plenary invited speaker in 20 international conferences and invited speaker in 25 other conferences and workshops.

Contents

Invited Papers

Regular Papers