Said El Hajji
Abderrahmane Nitaj
Claude Carlet
El Mamoun Souidi (Eds.)

LNCS 9084

Codes, Cryptology, and Information Security

First International Conference, C2SI 2015
Rabat, Morocco, May 26–28, 2015, Proceedings
In Honor of Thierry Berger

Lecture Notes in Computer Science **9084**

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

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

Codes, Cryptology, and Information Security

First International Conference, C2SI 2015 Rabat, Morocco, May 26–28, 2015, Proceedings

In Honor of Thierry Berger

Springer

Editors
Said El Hajji
University of Mohammed V
Rabat
Morocco

Claude Carlet
LAGA, Universities of Paris 8 and Paris 13, France
Saint-Denis Cedex 02
France

Abderrahmane Nitaj
University of Caen
Caen
France

El Mamoun Souidi
University of Mohammed V
Rabat
Morocco

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-18680-1 ISBN 978-3-319-18681-8 (eBook)
DOI 10.1007/978-3-319-18681-8

Library of Congress Control Number: 2015938320

LNCS Sublibrary: SL4 – Security and Cryptology

Springer Cham Heidelberg New York Dordrecht London

Printed on acid-free paper

Springer International Publishing AG Switzerland is part of Springer Science+Business Media (www.springer.com)

Preface

This volume contains the papers accepted for presentation at C2SI-Berger2015, in honor of Prof. Thierry Berger, from XLIM Laboratory, University of Limoges, France. C2SI-Berger2015 is an international conference on the theory, and applications of cryptographic techniques, coding theory, and information security. The first aim of this conference is to pay homage to Prof. Thierry Berger for his valuable contribution in teaching and disseminating knowledge in coding theory and cryptography in Morocco since 2003. The second 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-Berger2015 has been started by the Moroccan Laboratory of Mathematics, Computing sciences and Applications (LabMiA) at Faculty of Sciences of the University Mohammed V 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 were published in Springer's Lecture Notes in Computer Science series.

The C2SI-Berger2015 Program Committee consisted of 39 members. There were 59 papers submitted to the conference. Each paper was assigned to at least two members of the Program Committee and was refereed anonymously. The review process was challenging and the Program Committee, aided by reports from 17 external reviewers, produced a total of 130 reviews in all. After this period, 22 papers were accepted on March 20, 2015. Authors then had the opportunity to update their papers until March 25, 2015. 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 François Arnault, Ezedin Barka, Johannes A. Buchmann, Anne Canteaut, Claude Carlet, Jean Louis Lanet, Ayoub Otmani, and Felix Ulmer. 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 invited speakers, and the authors of all submissions. They all contributed to the success of the conference.

We would also like to thank Prof. Saaid Amzazi, President of University Mohammed V in Rabat and Prof. Wail Benjelloun, former Head of University Mohammed V, Agdal in Rabat for their unwavering support to research and teaching in the areas of cryptography, coding theory, and information security.

We are deeply grateful to Prof. Thierry Berger and his laboratory XLIM of the University of Limoges for great services in contributing to the establishment of a successful master's degree in coding theory, cryptography, and information security at

University Mohammed V in Rabat. We would like to take this opportunity to acknowledge their professional work.

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 in producing the proceedings.

May 2015

Said El Hajji
Abderrahmane Nitaj
El Mamoun Souidi

Organization

C2SI-Berger2015 is organized by University Mohammed V, Rabat, Morocco, in cooperation with the International Association for Cryptologic Research (IACR).

Honorary Chairs

Saaid Amzazi	President of University Mohammed V, Rabat, Morocco
Thierry Berger	XLIM, University of Limoges, France

General Chair

Said El Hajji	University Mohammed V, Rabat, Morocco

Program Chairs

Said El Hajji	University Mohammed V, Rabat, Morocco
Abderrahmane Nitaj	University of Caen, France
Claude Carlet	Universities of Paris 8 and Paris 13, France
El Mamoun Souidi	University Mohammed V, Rabat, Morocco

Organization Committee

Said El Hajji (Chair)	LabMIA, University Mohammed V, Rabat, Morocco
Ghizlane Orhanou (Co-chair)	LabMIA, University Mohammed V, Rabat, Morocco
El Mamoun Souidi (Co-chair)	LabMIA, University Mohammed V, Rabat, Morocco
Anas Aboulkalam	University Cadi Ayyad, Marrakesh, Morocco
François Arnault	XLIM, University of Limoges, France
Abdelmalek Azizi	University Mohammed I, Oujda, Morocco
Hafssa Benaboud	University Mohammed V, Rabat, Morocco
Redouane Benaini	University Mohammed V, Rabat, Morocco
Youssef Bentaleb	University Ibn Tofail, Kenitra, Morocco
Souad EL Bernoussi	University Mohammed V, Rabat, Morocco

Sidi Mohamed Douiri	University Mohammed V, Rabat, Morocco
Caroline Fontaine	Télécom Bretagne, Rennes, France
Abelkrim Haqiq	University of Settat, Morocco
Hicham Laanaya	University Mohammed V, Rabat, Morocco
Jalal Laassiri	University Mohammed V, Rabat, Morocco
Mounia Mikram	École des Sciences de l'Information, Rabat, Morocco
Ayoub Otmani	University of Rouen, France
Faissal Ouardi	University Mohammed V, Rabat, Morocco

Program Committee

Anas Aboulkalam	University Cadi Ayyad, Marrakesh, Morocco
François Arnault	XLIM, University of Limoges, France
Abdelmalek Azizi	University Mohammed I, Oujda, Morocco and Académie Hassan II, Morocco
Ezedin Barka	College of IT, United Arab Emirates University, Al Ain, UAE
Hafssa Benaboud	University Mohammed V, Rabat, Morocco
Youssef Bentaleb	ENSA, Kenitra, Morocco
Thierry Berger	XLIM, University of Limoges, France
Mohammed Bouhdadi	University Mohammed V, Rabat, Morocco
Mohamed Boulmalf	Université Internationale de Rabat, Morocco
Anne Canteaut	Inria-Rocquencourt, France
Sidi Mohamed Douiri	University Mohammed V, Rabat, Morocco
Pierre Dusart	University of Limoges, France
Mohamed Essaaidi	IEEE Morocco Section, ENSIAS, Rabat, Morocco
Caroline Fontaine	Télécom Bretagne, Rennes, France
Philippe Gaborit	XLIM, University of Limoges, France
Sanaa Ghouzali	College of Computer and Information Sciences, King Saud University, Saudi Arabia
Kenza Guenda	University of Science and Technology, Houari Boumedienne, Algiers, Algeria
Abelkrim Haqiq	University of Settat, Morocco
Maria Isabel Garcia	University of Barcelona, Spain
Zoubida Jadda	St Cyr, France
Salahddine Krit	Ibn Zohr University Polydisciplinary, Ouarzazate, Morocco
Jalal Laassiri	Ibn Tofail University, Kenitra, Morocco
Jean Louis Lanet	Inria Bretagne Atlantique, France
Mounia Mikram	École des Sciences de l'Information, Rabat, Morocco
Marine Minier	INSA, Lyon, France
Ghizlane Orhanou	University Mohammed V, Rabat, Morocco
Ayoub Otmani	University of Rouen, France

Ali Ouadfel	University Mohammed V, Rabat, Morocco
Faissal Ouardi	University Mohammed V, Rabat, Morocco
Patrice Parraud	St Cyr, France
Mohammed Rziza	University Mohammed V, Rabat, Morocco
Abderrahim Saaidi	University Sidi Mohamed Ben Abdellah, Taza, Morocco
Tayeb Sadiki	Université Internationale de Rabat, Morocco
Felix Ulmer	University of Rennes, France
Fouad Zinoun	University Mohammed V, Rabat, Morocco

Additional Reviewers

Hussain Ben-Azza	Johan Nielsen
Delphine Boucher	Tajjeeddine Rachidi
Ilaria Cardinali	Netanel Raviv
Pascale Charpin	Nicolas Sendrier
Willi Geiselmann	Zhang Shiwei
Norafida Ithnin	Anna-Lena Trautmann
Vadim Lyubashevsky	Antonia Wachter-Zeh
Sihem Mesnager	

Invited Speakers

François Arnault	XLIM, University of Limoges, France
Ezedin Barka	College of IT, United Arab Emirates, Al Ain, UAE
Johannes A. Buchmann	Technische Universität Darmstadt, Germany
Anne Canteaut	Inria-Rocquencourt, France
Claude Carlet	LAGA, Universities of Paris 8 and Paris 13, France
Jean Louis Lanet	Inria Bretagne Atlantique, France
Ayoub Otmani	University of Rouen, France
Felix Ulmer	University of Rennes, France

Sponsoring Institutions

Ministère de l'Enseignement Supérieur, de la Recherche Scientifique et de la Formation des Cadres
Faculty of Sciences, Rabat, Morocco
University Mohammed V, Rabat, Morocco
Académie Hassan II des Sciences et Techniques, Morocco
Centre National de Recherche Scientifiques et Techniques, Morocco
IEEE Morocco Section

Association Marocaine de Confiance Numérique (AMAN), Morocco
Centre Marocain de Recherches Polytechniques et d'Innovation, Morocco
Equipe Protection de l'Information, Codage et Cryptographie du Laboratoire XLIM de Limoges, France
Laboratoire de Mathématiques, Informatique et Applications (LabMiA), Rabat, Morocco

Origin of Submissions

Algeria
Brazil
Cameroon
Canada
France
Germany
Mauritius
Mexico
Morocco
Norway
Pakistan
Russian Federation
Saudi Arabia
Senegal
Spain
Syrian Arab Republic
Tunisia
Turkey
UAE

Biography of Thierry Berger

Thierry P. Berger received the Ph.D. degree and the French Habilitation (Mathematics) from the University of Limoges, France.

From 1992, he has been with the University of Limoges. He is currently Professor in the Department of Mathematics and Informatics, Xlim Laboratory. He is the scientific head of the Protection of Information, Coding and Cryptography group of this department. His research interests include finite algebra, automorphism group of codes, links between coding and cryptography, stream cipher and pseudorandom generators, design and cryptanalysis of lightweight block ciphers.

Invited Papers

François Arnault	Multidimensional Bell inequalities and quantum cryptography
Ezedin Barka	Securing the Web of Things With Role-Based Access Control
Johannes A. Buchmann	On the Security of Long-lived Archiving Systems based on the Evidence Record Syntax
Anne Canteaut	Differential attacks against SPN: a thorough analysis
Claude Carlet	On the properties of vectorial functions with plateaued components and their consequences on APN functions
Jean Louis Lanet	Beyond Cryptanalysis is Software Security the Next Threat for Smart Cards
Ayoub Otmani	Key-Recovery Techniques in Code-Based Cryptography
Felix Ulmer	Codes as modules over skew polynomial rings

Multidimensional Bell Inequalities and Quantum Cryptography

François Arnault

Université de Limoges, Laboratoire XLIM/DMI, France
arnault@unilim.fr

Abstract. The laws of quantum physics allow the design of cryptographic protocols for which the security is based on physical principles. The main cryptographic quantum protocols are key distribution schemes, in which two parties generate a shared random secret string. The privacy of the key can be checked using Bell inequalities. However, the Bell inequalities initial purpose was a fundamental one, as they showed how quantum rules are incompatible with our intuition of reality.

This paper begins with an introduction about quantum information theory, Bell inequalities, quantum cryptography. Then it presents the use of qudits for Bell inequalities and cryptography.

Securing the Web of Things with Role-Based Access Control

Ezedine Barka, Sujith Samuel Mathew, and Yacine Atif

College of IT, UAE University, Al Ain, UAE
ebarka@uaeu.ac.ae

Abstract. Real-world things are increasingly becoming fully qualified members of the Web. From, pacemakers and medical records to children's toys and sneakers, things are connected over the Web and publish information that is available for the whole world to see. It is crucial that there is secure access to this Web of Things (WoT) and to the related information published by things on the Web. In this paper, we introduce an architecture that encompasses Web-enabled things in a secure and scalable manner. Our architecture utilizes the features of the well-known role-based access control (RBAC) to specify the access control policies to the WoT, and we use cryptographic keys to enforce such policies. This approach enables prescribers to WoT services to control who can access what things and how access can continue or should terminate, thereby enabling privacy and security of large amount of data that these things are poised to flood the future Web with.