Lecture Notes in Computer Science 11445

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

Editorial Board Members

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

Claude Carlet · Sylvain Guilley ·
Abderrahmane Nitaj · El Mamoun Souidi (Eds.)

Codes, Cryptology and Information Security

Third International Conference, C2SI 2019
Rabat, Morocco, April 22–24, 2019, Proceedings
In Honor of Said El Hajji

Springer

Editors
Claude Carlet
Université Paris 8
Saint-Denis, France

Sylvain Guilley
Institut MINES-TELECOM
Paris, France

Abderrahmane Nitaj
Université de Caen
Caen, France

El Mamoun Souidi
Mohammed V University
Rabat, Morocco

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-16457-7 ISBN 978-3-030-16458-4 (eBook)
https://doi.org/10.1007/978-3-030-16458-4

Library of Congress Control Number: 2019935476

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 Third International Conference on the Theory and Applications of Cryptographic Techniques, Coding Theory, and Information Security was held at the Faculty of Sciences at the University of Mohammed V in Rabat, Morocco during April 22–24, 2019. This volume contains the papers accepted for presentation at C2SI-El Hajji 2019, in honor of Professor Said El Hajji, from this university.

One aim of C2SI-El Hajji 2019 was to pay homage to Professor Said El Hajji for his valuable contribution to research, teaching, and disseminating knowledge in numerical analysis, modeling, and information security in Morocco, Africa, and worldwide. We are deeply grateful to him for his great services in contributing to the establishment of a successful research group in coding theory, cryptography, and information security at Mohammed V University in Rabat, organizing a master's course in this field and many other academic activities.

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 to discuss all forms of cryptology, coding theory, and information security.

The organization of C2SI-El Hajji 2019 was initiated by the Moroccan Laboratory of Mathematics, Computing Sciences, Applications, and Information Security (LabMIA-SI), 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.

C2SI-El Hajji 2019 was the third of the C2SI series. The first conference of the C2SI series was held at the University Mohammed V in Rabat during May 26–28, 2015, in honor of Professor Thierry Berger from Limoges University, and the second conference of the series was held at the same university during April 10–12, 2017, in honor of Professor Claude Carlet, from Paris 8 University. The proceedings of both conferences were published in Springer's *Lecture Notes in Computer Science*.

The C2SI-El Hajji 2019 Program Committee consisted of 46 members. There were 90 papers submitted to the conference. Each paper was assigned to three members of the Program Committee on average and reviewed anonymously. The review process was challenging and the Program Committee, aided by reports from 38 external reviewers, produced a total of 240 reviews in all. After this period, 19 papers were accepted on January 20, 2019. Authors then had the opportunity to update their papers until February 15, 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 the invited speakers Abdelmalek Azizi from Mohammed First University in Oujda, Morocco, Thomas Johansson from Lund University, Sweden, Grigory Kabatiansky from Skolkovo Institute of Science and Technology (Skoltech), Sihem Mesnager from University of Paris 8, France, and

Amr Youssef from Concordia University, Canada. They gave talks on various topics in cryptography, coding theory, and information security and contributed to the success of the conference, and will contribute to the success of these proceedings. We are grateful to them.

The conference hosted a co-located one-day Workshop on Side-Channel Analysis (SCA). This workshop was held on April 21, 2019. It introduced the audience to the non-invasive test methodology compliant with international standard ISO/IEC 17825, through practice exercises on vulnerability analysis of hardware and software AES implementation, software RSA implementation, and classic and post-quantum cryptography implementation. Then, it featured three talks on recent research issues concerning the field of side-channel analysis SCA, namely, Boolean-level SCA, cache-timing attacks on a software cryptographic library, and side-channel attack on multiplications. The three papers related to the workshop are printed in the "Side-Channel Analysis" part of the proceedings. Please note that these papers went through a separate selection process.

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 as the participants. They all contributed to the success of the conference.

We also would like to thank Professor Said Amzazi, Minister of National Education, Vocational Training, Higher Education and Scientific Research, for his support in teaching and research in the field of cryptology and information security when he was professor, and Dean of Faculty of Sciences, and president of Mohammed V University in Rabat. Similarly, we would like to thank Professor Mohamed El Ghachi, President 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 the Faculty of Sciences in Rabat.

Along with these individuals, we wish to thank all 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 the 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 2019

Claude Carlet
Sylvain Guilley
Abderrahmane Nitaj
El Mamoun Souidi

Organization

C2SI-El Hajji 2019 was organized by the Moroccan Laboratory of Mathematics, Computing Sciences, Applications, and Information Security (LabMIA-SI) at the Faculty of Sciences of the Mohammed V University in Rabat.

Honorary Chair

Said El Hajji	University Mohammed V, Rabat, Morocco

General Chair

El Mamoun Souidi	Mohammed V University in Rabat, Morocco

Program Chairs

Claude Carlet	LAGA, University of Paris 8, France and University of Bergen, Norway
Sylvain Guilley	Secure-IC and Télécom-ParisTech, Paris, France
Abderrahmane Nitaj	University of Caen Normandie, France
El Mamoun Souidi	Mohammed V University in Rabat, Morocco

Invited Speakers

Abdelmalek Azizi	University Mohammed the First, Oujda, Morocco
Said El Hajji	Mohammed V University in Rabat, Morocco
Thomas Johansson	Lund University, Sweden
Grigory Kabatiansky	Skolkovo Institute of Science and Technology, Russia
Sihem Mesnager	University of Paris 8, France
Amr Youssef	Concordia University, Canada

Organizing Committee

El Mamoun Souidi (Chair)	Mohammed V University in Rabat, Morocco
Ghizlane Orhanou (Co-chair)	Mohammed V University in Rabat, Morocco
Souad El Bernoussi (Co-chair)	Mohammed V University in Rabat, Morocco
Abderrahim Benazzouz	ENS, LabMIA-SI, Rabat, Morocco
Hafida Benazza	FSR, LabMIA-SI, Rabat, Morocco
Hicham Bensaid	INPT, Morocco
Youssef Bentaleb	ENSA, Kenitra, Morocco
Mohammed Boulmalf	UIR, Rabat, Morocco

Azzouz Cherrabi	FSR, LabMIA-SI, Rabat, Morocco
Sidi Mohamed Douiri	FSR, LabMIA-SI, Rabat, Morocco
Abderrahim El Abdllaoui	FSR, LabMIA-SI, Rabat, Morocco
Said El Hajji	FSR, LabMIA-SI, Rabat, Morocco
Mustapha Esghir	FSR, LabMIA-SI, Rabat, Morocco
Hassan Essanouni	FSR, LabMIA-SI, Rabat, Morocco
Touria Ghemires	FSR, LabMIA-SI, Rabat, Morocco
Ahmed Hajji	FSR, LabMIA-SI, Rabat, Morocco
Samir Hakam	FSR, LabMIA-SI, Rabat, Morocco
Aiz Hilali	INPT, Morocco
El Mostafa Jabbouri	FSR, LabMIA-SI, Rabat, Morocco
Abderrahim Messaoudi	ENS, Rabat, LabMIA-SI, Rabat, Morocco
Hassan Mharzi	ENSA de Kenitra (CMRPI), Morocco
Jilali Mikram	FSR, LabMIA-SI, Rabat, Morocco
Mounia Mikram	ESI, Rabat, Morocco
Ali Ouadfel	FSR, LabMIA-SI, Rabat, Morocco
Bouchta Rhanizar	ENS, Rabat, LabMIA-SI, Rabat, Morocco
Rachid Sadaka	ENS, Rabat, LabMIA-SI, Rabat, Morocco
Aoutif Sayah	FSR, LabMIA-SI, Rabat, Morocco
Fouad Zinoun	FSR, LabMIA-SI, Rabat, Morocco
Karim Zkik	UIR, Rabat, Morocco

Program Committee

Elena Andreeva	Katholieke Universiteit Leuven, Belgium
François Arnault	University of Limoges, France
Emanuele Bellini	Darkmatter LLC, Abu Dhabi, UAE
Thierry Berger	XLIM, University of Limoges, France
Lilya Budaghyan	University of Bergen, Norway
Claude Carlet	University of Paris 8, France
Miguel Carriegos	RIASC, Spain
Chen-Mou Cheng	Osaka University, Japan
Alain Couvreur	LIX, Ecole Polytechnique, France
Pierre Dusart	XLIM UMRS 7252, University of Limoges, France
Said El Hajji	Mohammed V University in Rabat, Morocco
Nadia El Mrabet	SAS, CGCP, EMSE, Saint-Etienne, France
Caroline Fontaine	CNRS, France
Maria Isabel Garcia Planas	Universitat Politecnica de Catalunya, Spain
Sanaa Ghouzali	King Saud University, Saudi Arabia
Kenza Guenda	UVIC/USTHB, Algiers, Algeria
Cheikh Thiecoumba Gueye	Universite Cheikh Anta Diop, Dakar, Senegal
Sylvain Guilley	Secure-IC S.A.S. and Télécom-ParisTech, Paris, France
Abdelkrim Haqiq	FST, Hassan 1st University, Settat, Morocco
Tor Helleseth	University of Bergen, Norway
Shoichi Hirose	University of Fukui, Japan

Tetsu Iwata	Nagoya University, Japan
Thomas Johansson	Lund University, Sweden
Grigory Kabatyansky	Skolkovo Institute of Science and Technology (Skoltech) Moscow, Russia
Muhammad Rezal Kamel Ariffin	Institute for Mathematical Research, UPM, Malaysia
Ahmed Khoumsi	University of Sherbrooke, Canada
Juliane Krämer	TU Darmstadt, Germany
Jalal Laassiri	Ibn Tofail University, Morocco
Jean-Louis Lanet	Inria-RBA, France
Juan Lopez-Ramos	University of Almeria, Spain
Sihem Mesnager	University of Paris 8 and LAGA, France
Marine Minier	University of Nancy, France
Tarik Moataz	Brown University, USA
Abderrahmane Nitaj	LMNO, University of Caen, France
Ghizlane Orhanou	Mohammed V University in Rabat, Morocco
Emmanuel Prouff	ANSSI, France
Palash Sarkar	Indian Statistical Institute, India
El Mamoun Souidi	Mohammed V University in Rabat, Morocco
Pantelimon Stanica	Naval Postgraduate School, Monterey, USA
Noah Stephens-Davidowitz	New York University, USA
Joseph Tonien	University of Wollongong, Australia
Alev Topuzoglu	Sabanci University, Istanbul, Turkey
Amr Youssef	Concordia University, Montreal, Canada
Yongjun Zhao	The Chinese University of Hong Kong, SAR China

Additional Reviewers

Maryem Ait El Hadj	Hisham Galal	Baslam Mohamed
Nurdagül Anbar	Aurore Guillevic	Lina Mortajine
Meryeme Ayache	Cem Güneiri	Ousmane Ndiaye
Sébastien Bardin	Vincent Herbert	Ferruh Özbudak
Nina Bindel	Hind Idrissi	Buket Ozkaya
Olivier Blazy	Nikolay Kaleyski	Enes Pasalic
Delphine Boucher	Karim Khalfallah	Simon Pontié
Pierre-Louis Cayrel	Jean Belo Klamti	Olivier Potin
Ayca Cesmelioglu	Adrien Koutsos	Olivier Ruatta
Ilaria Chillotti	Chunlei Li	Essaid Sabir
Abderrahman Daif	Nian Li	Patrick Struck
Ahmed El Kiram	Pierrick Méaux	Karim Zkik
Thomas Fuhr	Wilfried Meidl	

Sponsoring Institutions

Ministère de l'Education Nationale, de la Formation Professionnelle, de l'Enseignement Supérieur et de la Recherche Scientifique, Kingdom of Morocco
Ministère de l'Industrie, du Commerce de l'Investissement, et de l'Economie Numérique, Kingdom of Morocco
Université Mohammed V de Rabat, Morocco
Faculté des Sciences de Rabat, Morocco
L'Académie Hassan II des Sciences et Techniques, Morocco
Islamic Educational, Scientific and Cultural Organization – ISESCO
Centre National pour la Recherche Scientifique et Technique – CNRST, Morocco
Le Centre Marocain de Recherches Polytechniques et d'Innovation (CMRPI), Morocco
Le Groupement d'Assurance des enseignants du Supérieur – GASUP, Morocco
Centre de Mathématique de Rabat, Morocco

Origin of Submissions

Algeria
Belgium
Cameroon
Canada
China
Colombia
Finland
France
Germany
Honduras
Hong Kong
India
Italy
Japan
Lebanon
Luxembourg
Mexico
Morocco
Poland
Qatar
Romania
Russia
Senegal
Singapore
Slovenia
South Africa
Spain
Sweden
Tunisia
Turkey
United Arab Emirates
USA
Venezuela

Biography of Said El Hajji

Professor Said El Hajji graduated from Pierre and Marie Curie University (Paris VI, France) and received his PhD from Laval University in Quebec (Canada). He subsequently became senior lecturer (Maître Assistant) at "Ecole Normale Supérieure" of Rabat and then associate professor (Maître de Conférences) at the same institute. Until 2018, he was professor at the Faculty of Sciences, Mohammed V University in Rabat, Morocco.

His research interests include modeling and numerical simulation, numerical analysis, operating systems and network security, information security, management of information security.

He has (co-)written more than 100 papers in scientific journals and proceedings and has been chapter (co-)author or (co-)editor of seven books. He has also been a member of more than 20 Program Committees (seven as (co-)chair).

Professor Said El Hajji has been at the Faculty of Sciences in Rabat the head of the Research and Teaching Unit (UFR) DESA CS&ANO, of "DESA Analyse Numérique et Optimisation," of "DESA Mathématiques, Informatique et Applications," of the master's course "Codes, Cryptographie et Sécurité de l'Information," and finally, from 2015 to 2018, the head of the master's course "Cryptographie et Sécurité de l'Information."

He was also the head of "Groupe d'Analyse Numérique et Optimisation" and finally the head of the "Laboratoire de Mathématiques, Informatique et Applications—Sécurité de l'Information", (LabMiA-SI), formerly called LabMiA, from 2005 to 2018.

Professor Said El Hajji has supervised more than 21 theses and is currently supervising five others. He has been plenary invited speaker in four international conferences and invited speaker in ten other conferences and workshops. He has organised four Summer Schools and seven international conferences in relation with his research and teaching interests and he was the initiator and one of the organizers of the C2SI conference series.

Invited Papers and Talks

Abdelmalek Azizi	Arabic Cryptography and Steganography in Morocco
Said El Hajji	Analysis of Neural Network Training and Cost Functions Impact on the Accuracy of IDS and SIEM Systems
Thomas Johansson	An AEAD Variant of the Grain Stream Cipher
Grigory Kabatyansky	On the Tracing Traitors Math, Dedicated to the Memory of Bob Blakley—Pioneer of Digital Fingerprinting and Inventor of Secret Sharing
Sihem Mesnager	On Good Polynomials Over Finite Fields for Optimal Locally Recoverable Codes
Amr Youssef	Privacy Preserving Auctions on Top of Ethereum

Privacy Preserving Auctions on Top of Ethereum (Abstract for Invited Talk)

Amr M. Youssef

Concordia Institute for Information Systems Engineering,
Concordia University, Montréal, QC, Canada

Abstract. Blockchain is an evolving technology with the potential to reshape a variety of industries by allowing mutually distrusting parties to interact with each other without relying on a trusted centralized party. Informally, a blockchain is an immutable append-only distributed ledger that records transactions in a way that greatly increases reliability and removes the need for trust. Nevertheless, many organizations are reluctant to fully adopt this technology owing to several issues such as scalability and privacy. The current transaction throughput in blockchains pales in comparison to the throughput needed to run mainstream payment systems or financial markets. Furthermore, organizations and users are particularly not keen on having all of their transaction information published on a public ledger that can be arbitrarily read without any restrictions by anyone.

In this talk, my focus will be on the privacy issue in blockchains particularly on Ethereum. There are various cryptographic techniques that can realize privacy-preserving applications on top of blockchains. As part of my work, I will show how the privacy requirements of building sealed-bid auctions on top of Ethereum can be addressed. Specifically, I will present three different constructions [1–3] that utilize cryptographic protocols and primitives including zero-knowledge proofs, commitment schemes, and trusted hardware environments such as Intel SGX. Finally, I will show the pros and cons of each construction and draw out conclusions based on the presented schemes.

References

1. Galal, H.S., Youssef, A.M.: Succinctly verifiable sealed-bid auction smart contract. In: Data Privacy Management, Cryptocurrencies and Blockchain Technology - ESORICS 2018 International Workshops, DPM 2018 and CBT 2018, Barcelona, Spain, 6–7 September 2018, Proceedings, pp. 3–19 (2018)
2. Galal, H.S., Youssef, A.M.: Verifiable Sealed-Bid Auction on the Ethereum Blockchain. In: Zohar, A. et al. (eds.) Financial Cryptography and Data Security. FC 2018. LNCS, vol. 10958. Springer, Heidelberg (2019)
3. Galal, H.S., Youssef, A.M.: Trustee: full privacy preserving vickrey auction on top of ethereum. In: International Conference on Financial Cryptography and Data Security, Trusted Smart Contracts Workshop. Springer (2019)

Contents

Secret Sharing

Mathematics for Cryptography

Codes and Their Applications

Homomorphic Encryption

Applied Cryptography

Security