LNCS 13203

Riham AlTawy
Andreas Hülsing (Eds.)

Selected Areas in Cryptography

28th International Conference
Virtual Event, September 29 – October 1, 2021
Revised Selected Papers

Springer

Lecture Notes in Computer Science 13203

More information about this series at https://link.springer.com/bookseries/558

Riham AlTawy · Andreas Hülsing (Eds.)

Selected Areas in Cryptography

28th International Conference
Virtual Event, September 29 – October 1, 2021
Revised Selected Papers

Springer

Editors

Riham AlTawy
University of Victoria
Victoria, BC, Canada

Andreas Hülsing
Eindhoven University of Technology
Eindhoven, The Netherlands

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-99276-7 ISBN 978-3-030-99277-4 (eBook)
https://doi.org/10.1007/978-3-030-99277-4

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

Selected Areas in Cryptography (SAC) is Canada's annual research conference on cryptography, held since 1994. The 28th edition of SAC was supposed to take place at the University of Victoria in British Columbia, Canada. However, due to the ongoing COVID-19 pandemic, SAC 2021 was held as a virtual event from September 29 to October 1, 2021.

There are four areas covered at each SAC conference. Three of the areas are permanent:

- Design and analysis of symmetric key primitives and cryptosystems, including block and stream ciphers, hash functions, MAC algorithms, cryptographic permutations, and authenticated encryption schemes.
- Efficient implementations of symmetric, public key, and post-quantum cryptography.
- Mathematical and algorithmic aspects of applied cryptology, including post-quantum cryptology.

The fourth area is selected as a special topic for each edition. The special topic for SAC 2021 was

- Privacy enhancing mechanisms and techniques.

We received 60 submissions that were reviewed in a double-blind review process. Regular submissions received three reviews whereas submissions by Program Committee (PC) members were reviewed by five PC members. All in all, 190 reviews were written by our Program Committee, consisting of 38 members, and of course with the help of 28 subreviewers. Eventually, 23 papers were accepted for publication in these proceedings and presentation at the conference.

There were two invited talks at SAC 2021. The Stafford Taveres Lecture was given by Sofía Celi, talking about "How private is secure messaging?". The second invited talk was given by Eyal Ronen on the topic of "Privacy-Preserving Bluetooth Based Contact Tracing—One Size Does Not Fit All". The program of SAC 2021 was completed by a preceding two-day summer school on September 27 and 28, 2021. During the summer school, there was one day of lectures about "Machine-Checked Cryptography with EasyCrypt and Jasmin" held by François Dupressoir, Benjamin Grégoire, and Vincent Laporte. The second day focused on "Communication Privacy" with lectures by Ania M. Piotrowska and Britta Hale. The advantage of an online conference is that almost all lectures as well as the talks were recorded. Therefore, we want to point the interested reader to the YouTube channel of the conference https://www.youtube.com/channel/UCiPgSZ0ho0LQEENlRmhwbBQ.

We would like to thank all our colleagues who helped to make SAC 2021 a success. Especially, we would like to thank the Program Committee members, and their subreviewers, for their hard work during these daring times. We would also like to thank the invited speakers and the summer school lecturers for making the time to give a talk at yet another online conference. Finally, we would like to thank Orr Dunkelman and Michael J. Jacobson, Jr. for their help and advice.

January 2022

Andreas Hülsing
Riham AlTawy

Organization

SAC 2021 was held in cooperation with The International Association for Cryptologic Research (IACR).

Program Chairs

Riham AlTawy	University of Victoria, Canada
Andreas Hülsing	Eindhoven University of Technology, The Netherlands

Program Committee

Riham AlTawy	University of Victoria, Canada
Diego Aranha	Aarhus University, Denmark
Tomer Ashur	Eindhoven University of Technology, The Netherlands, and KU Leuven, Belgium
Paulo Barreto	University of Washington Tacoma, USA
Daniel J. Bernstein	University of Illinois at Chicago, USA, and Ruhr University Bochum, Germany
Jean-François Biasse	University of South Florida, USA
Nina Bindel	University of Waterloo and Institute for Quantum Computing, Canada
Claude Carlet	University of Bergen, Norway, and Université Paris 8, France
Chitchanok Chuengsatiansup	University of Adelaide, Australia
Carlos Cid	Royal Holloway, University of London, UK, and Simula UiB, Norway
Christoph Dobraunig	Lamarr Security Research, Austria
Orr Dunkelman	University of Haifa, Israel
Aleksander Essex	Western University, Canada
Maria Eichlseder	Graz University of Technology, Austria
Britta Hale	Naval Postgraduate School, USA
Andreas Hülsing	Eindhoven University of Technology, The Netherlands
Michael J. Jacobson, Jr.	University of Calgary, Canada
Christian Janson	Technische Universität Darmstadt, Germany
Marcel Keller	CSIRO’s Data61, Australia
Péter Kutas	University of Birmingham, UK

Subhamoy Maitra	Indian Statistical Institute Kolkata, India
Christian Majenz	QuSoft and CWI Amsterdam, The Netherlands
Kalikinkar Mandal	University of New Brunswick, Fredericton, Canada
Maria Mendez Real	Université de Nantes, France
Ruben Niederhagen	University of Southern Denmark, Denmark
Abderrahmane Nitaj	University of Caen Normandy, France
Lorenz Panny	Academia Sinica, Taiwan
Christiane Peters	IBM, Belgium
Elizabeth Quaglia	Royal Holloway, University of London, UK
Simona Samardjiska	Radboud University, The Netherlands
Tobias Schneider	NXP Semiconductors, Austria
Nicolas Sendrier	Inria, France
Leonie Simpson	Queensland University of Technology, Australia
Benjamin Smith	Inria and École polytechnique, Institut Polytechnique de Paris, France
Djiby Sow	Cheikh Anta Diop University of Dakar, Senegal
Tyge Tiessen	Technical University of Denmark, Denmark
Yosuke Todo	NTT Corporation, Japan
Yuntao Wang	Japan Advanced Institute of Science and Technology, Japan
Huapeng Wu	University of Windsor, Canada

Additional Reviewers

Kazumaro Aoki
James Bartusek
Matthew Dodd
Jelle Don
Shuichi Katsumata
Liliya Kraleva
Leah Krehling
Norman Lahr
Angelique Loe
Mohammad Mahzoun
Liam Medley
Tabitha Ogilvie
Richard Petri
Raluca Posteuca
Mounika Pratapa
Robert Primas
Joost Renes
Raghvendra Rohit
Sumanta Sarkar
Yu Sasaki
Markus Schofnegger
Tjerand Silde
Patrick Struck
Ha Tran
Fernando Virdia
Julian Wälde
Yuval Yarom
Randy Yee

Invited Talks

How Private is Secure Messaging?

Sofía Celi

Cloudflare, Portugal

Abstract. Secure messaging is on the rise: applications want to implement it, parties want to regulate it, users want to understand it. With a broad arrange of protocols, applications and options, how do users choose the secure messaging option to use? How do they know which security properties they provide? While these initial questions focus on the security part of the secure messaging sphere and its interaction with users, the privacy part is often left out from the discourse. For many, thinking about the privacy notion is integral when talking about secure messaging; while, for others, it is an optional thought. On this talk, we will explore what privacy means in the secure messaging sphere and why we think it is vital to it. We will answer questions such as: what privacy properties are missing from this security idea? Is it only about protecting metadata? what is their impact in the real-world and its policies? Do they translate to a user interface perspective?

Privacy-Preserving Bluetooth Based Contact Tracing—One Size Does Not Fit All

Eyal Ronen

Tel Aviv University, Israel

Abstract. In recent months multiple proposals for contact tracing schemes for combating the spread of COVID-19 have been published. Many of those proposals try to implement this functionality in a decentralized and privacy-preserving manner using Bluetooth Low Energy (BLE). The different schemes provide different trade-offs between privacy, security, and explainability. We claim that different countries, with different needs and cultural norms may require different trade-offs. We present "Hashomer", a contact tracing scheme that has been tailored to needs and cultural norms in Israel. In this talk, we will explain the specific trade-offs we made and the different challenges we faced. Our scheme was adopted by the Israeli Ministry of Health (MoH) and released as part of the national contact tracing application—"Hamagen".

Contents

Privacy and Applications

On Evaluating Anonymity of Onion Routing 3
Alessandro Melloni, Martijn Stam, and Øyvind Ytrehus

Revisiting Driver Anonymity in ORide 25
Deepak Kumaraswamy, Shyam Murthy, and Srinivas Vivek

The Boneh-Katz Transformation, Revisited: Pseudorandom/Obliviously-Samplable PKE from Lattices and Codes and Its Application 47
Keita Xagawa

ZKAttest: Ring and Group Signatures for Existing ECDSA Keys 68
Armando Faz-Hernández, Watson Ladd, and Deepak Maram

Implementation, PUFs and MPC

A Low-Randomness Second-Order Masked AES 87
Tim Beyne, Siemen Dhooghe, Adrián Ranea, and Danilo Šijačić

How Do the Arbiter PUFs Sample the Boolean Function Class? 111
Animesh Roy, Dibyendu Roy, and Subhamoy Maitra

MPC for $\mathcal{Q}_2$ Access Structures over Rings and Fields 131
Robin Jadoul, Nigel P. Smart, and Barry Van Leeuwen

Secret-Key Cryptography: Design and Proofs

Multi-user Security of the Elephant v2 Authenticated Encryption Mode 155
Tim Beyne, Yu Long Chen, Christoph Dobraunig, and Bart Mennink

Designing S-Boxes Providing Stronger Security Against Differential Cryptanalysis for Ciphers Using Byte-Wise XOR 179
Yosuke Todo and Yu Sasaki

Parallel Verification of Serial MAC and AE Modes 200
Kazuhiko Minematsu, Akiko Inoue, Katsuya Moriwaki, Maki Shigeri, and Hiroyasu Kubo

Secret-Key Cryptography: Cryptanalysis

Related-Tweak Impossible Differential Cryptanalysis of Reduced-Round `TweAES` 223
Chao Niu, Muzhou Li, Meiqin Wang, Qingju Wang, and Siu-Ming Yiu

Improved Attacks on `GIFT-64` 246
Ling Sun, Wei Wang, and Meiqin Wang

A Simpler Model for Recovering Superpoly on Trivium 266
Stéphanie Delaune, Patrick Derbez, Arthur Gontier, and Charles Prud'homme

Automated Truncation of Differential Trails and Trail Clustering in ARX 286
Alex Biryukov, Luan Cardoso dos Santos, Daniel Feher, Vesselin Velichkov, and Giuseppe Vitto

Quantum Cryptanalysis

Improved Quantum Algorithms for the k-XOR Problem 311
André Schrottenloher

Quantum Boomerang Attacks and Some Applications 332
Paul Frixons, María Naya-Plasencia, and André Schrottenloher

Post-quantum Cryptography

MAYO: Practical Post-quantum Signatures from Oil-and-Vinegar Maps 355
Ward Beullens

Simple and Memory-Efficient Signature Generation of XMSS^{MT} 377
Haruhisa Kosuge and Hidema Tanaka

Zaytun: Lattice Based PKE and KEM with Shorter Ciphertext Size 398
Parhat Abla and Mingsheng Wang

A Polynomial Time Key-Recovery Attack on the Sidon Cryptosystem 419
Pierre Briaud, Jean-Pierre Tillich, and Javier Verbel

Isogenies

Verifiable Isogeny Walks: Towards an Isogeny-Based Postquantum VDF 441
Jorge Chavez-Saab, Francisco Rodríguez-Henríquez, and Mehdi Tibouchi

Towards Post-Quantum Key-Updatable Public-Key Encryption via Supersingular Isogenies 461
Edward Eaton, David Jao, Chelsea Komlo, and Youcef Mokrani

Secret Keys in Genus-2 SIDH 483
Sabrina Kunzweiler, Yan Bo Ti, and Charlotte Weitkämper

Author Index 509