Lecture Notes in Computer Science 12704

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

Kenneth G. Paterson (Ed.)

Topics in Cryptology – CT-RSA 2021

Cryptographers' Track at the RSA Conference 2021
Virtual Event, May 17–20, 2021
Proceedings

Springer

Editor
Kenneth G. Paterson
ETH Zürich
Zürich, Switzerland

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-75538-6 ISBN 978-3-030-75539-3 (eBook)
https://doi.org/10.1007/978-3-030-75539-3

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 RSA conference has been a major international event for information security experts since its inception in 1991. It is an annual event that attracts several hundred vendors and over 40,000 participants from industry, government, and academia. Since 2001, the RSA conference has included the Cryptographer's Track (CT-RSA). This track, essentially a sub-conference of the main event, provides a forum for the dissemination of current research in cryptography.

This volume represents the proceedings of the 2021 edition of the RSA Conference Cryptographer's Track. Due to the COVID-19 pandemic, the conference was held online during May 17–20, 2021. The unusual circumstances provided an opportunity to revisit the format of the event and try to integrate it more fully into the main RSA conference. This was done by partnering each presentation session with a more informal, broader discussion session involving the presented papers' authors and invited guests. I am grateful to the authors and guests for engaging with this experimental approach.

A total of 100 submissions were received for review, of which 27 were selected for presentation and publication. The selection process was a difficult task since there were many more high quality submissions than we could accept. The submissions were anonymous, and each submission was assigned to at least three reviewers (four if the paper included a Program Committee member as an author or if it was a "Systemisation of Knowledge" paper). I am thankful to all Program Committee members for producing high-quality reviews and for actively participating in discussions. My appreciation also goes to all external reviewers. I am also grateful to the Program Committee members who acted as shepherds for some of the submissions.

The submission and review process, as well as the editing of these proceedings, were greatly simplified by using the webreview software written by Dr. Shai Halevi, which we used with the permission of the International Association for Cryptologic Research (IACR). My thanks go to Shai. I am also grateful to Prof. Stanislaw Jarecki, my predecessor as Program Chair for CT-RSA. Stas provided a wealth of advice and insights based on his experience. I hope to be able to pass on to my successor as much as I obtained from Stas.

My sincere thanks go also to Dr. Guido Zosimo-Landolfo from Springer Verlag and everyone on the team there for their assistance in preparing and producing these proceedings.

Last, but not least, on behalf of all CT-RSA participants, I would like to thank Tara Jung and Britta Glade who acted as RSA Conference liaison to the Cryptographer's Track. In this capacity, Tara and Britta essentially played the role of General Chairs for

the CT-RSA conference, and I am very grateful to them for all the work they did in helping to organise the conference and making it run smoothly.

March 2021 Kenneth G. Paterson

Organization

Program Chair

Kenneth G. Paterson	ETH Zürich, Switzerland

Program Committee

Masayuki Abe	NTT Secure Platform Labs, Japan
Shi Bai	Florida Atlantic University, USA
Paulo Barreto	University of Washington, USA
Lejla Batina	Radboud University, The Netherlands
Elif Bilge Kavun	University of Passau, Germany
Olivier Blazy	Université de Limoges, XLim, France
Chris Brzuska	Aalto University, Finland
Céline Chevalier	CRED, Université Paris II Panthéon-Assas, France
Craig Costello	Microsoft Research, USA
Jean Paul Degabriele	TU Darmstadt, Germany
Luca De Feo	IBM Research – Zürich, Switzerland
Ben Fuller	University of Connecticut, USA
Steven Galbraith	University of Auckland, New Zealand
Lydia Garms	Royal Holloway, University of London, UK
Daniel Genkin	University of Michigan, USA
Paul Grubbs	NYU, Cornell Tech, University of Michigan, USA
Goichiro Hanaoka	AIST, Japan
Helena Handschuh	Rambus Cryptography Research, USA
Carmit Hazay	Bar-Ilan University, Israel
Andreas Hülsing	Eindhoven University of Technology, The Netherlands
Takanori Isobe	University of Hyogo, Japan
Marcel Keller	CSIRO's Data61, Australia
Tancrède Lepoint	Google, USA
Benoit Libert	CNRS and ENS de Lyon, France
Brice Minaud	Inria and ENS, France
Tarik Moataz	Aroki Systems, USA
Svetla Nikova	KU Leuven, Belgium
Jiaxin Pan	NTNU Norway, Norway
Charalampos Papamanthou	University of Maryland, USA
Bertram Poettering	IBM Research – Zürich, Switzerland
Bart Preneel	KU Leuven, Belgium
Eyal Ronen	Tel Aviv University, Israel
Andy Rupp	University of Luxembourg, Luxembourg
Alexander Russell	University of Connecticut, USA
Jacob Schuldt	AIST, Japan

Nigel Smart	KU Leuven, Belgium
Juraj Somorovsky	Paderborn University, Germany
Martijn Stam	Simula UiB, Norway
Douglas Stebila	University of Waterloo, Canada
Fernando Virdia	Royal Holloway, University of London, UK
Michael Walter	IST Austria, Austria
Yuval Yarom	University of Adelaide and Data61, Australia

Additional Reviewers

Miguel Ambrona	Gunnar Hartung	Thomas Peters
Benedikt Auerbach	Shoichi Hirose	Chen Qian
Gustavo Banegas	Le Phi Hung	Yuan Quan
Laasya Bangalore	Ilia Iliashenko	Markus Raiber
Subhadeep Banik	Akiko Inoue	Adrian Ranea
Tim Beyne	Samuel Jaques	Simon Rastikian
Rishabh Bhadauria	Saqib A. Kakvi	Krijn Reijnders
Nina Bindel	Vukasin Karadzic	Vincent Rijmen
Estuardo Alpirez Bock	Shuichi Katsumata	Yusuke Sakai
Ryann Rose Carter	Michael Klooss	John Schanck
Shan Chen	Lilia Kraleva	Berry Schoenmakers
Ilaria Chillotti	Kaoru Kurosawa	Madura Shelton
Ana Costache	Gregor Leander	Tjerand Silde
Anamaria Costache	Chaoyun Li	Yongsoo Song
Thomas Debris-Alazard	Fukang Liu	Jessica Sorrell
Ioannis Demertzis	Patrick Longa	Christoph Striecks
Amit Deo	Vadim Lyubashevsky	Younes Talibi
Siemen Dhooghe	Akash Madhusudan	Ida Tucker
Samuel Dobson	Takahiro Matsuda	Qingju Wang
Keita Emura	Alireza Mehrdad	Yunhua Wen
Eiichiro Fujisaki	Nadia El Mrabet	Keita Xagawa
Alonso Gonzalez	Kazuma Ohara	Jianhua Yan
Jérôme Govinden	Satsuya Ohata	Avishay Yanai
Felix Günther	Miyako Ohkubo	Greg Zaverucha
Fabrice Ben Hamouda	Elisabeth Oswald	Lukas Zobernig
Keisuke Hara	Guillermo Pascual Perez	Marcus Brinkmann

Contents