Lecture Notes in Computer Science **9048**

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

Kaisa Nyberg (Ed.)

Topics in Cryptology – CT-RSA 2015

The Cryptographers' Track at the RSA Conference 2015
San Francisco, CA, USA, April 21–24, 2015
Proceedings

Springer

Editor
Kaisa Nyberg
Aalto University School of Science
Espoo
Finland

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-16714-5 ISBN 978-3-319-16715-2 (eBook)
DOI 10.1007/978-3-319-16715-2

Library of Congress Control Number: 2015934581

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

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 hundreds of vendors and thousands of participants from industry, government, and academia. Since 2001, the RSA conference has included the Cryptographers' Track (CT-RSA), which provides a forum for current research in cryptography. CT-RSA has become a major publication venue in cryptography. It covers a wide variety of topics from public-key to symmetric-key cryptography and from cryptographic protocols to primitives and their implementation security.

This volume represents the proceedings of the 2015 RSA Conference Cryptographers' Track which was held in San Francisco, California, during April 21–24, 2015. A total of 111 full papers were submitted for review out of which 26 papers were selected for presentation. As Chair of the Program Committee, I heartily thank all the authors who contributed the results of their innovative research and all the members of the Program Committee and their designated assistants who carefully reviewed the submissions. In the thorough peer-review process that lasted 2 months, each submission had three independent reviewers. The selection process was completed at a discussion among all members of the Program Committee.

In addition to the contributed talks, the program included a panel discussion moderated by Bart Preneel on *Post-Snowden Cryptography* featuring Paul Kocher, Adi Shamir, and Nigel Smart.

February 2015 Kaisa Nyberg

Organization

The RSA Cryptographers' Track is an independently managed component of the annual RSA Conference.

Steering Committee

Josh Benaloh	Microsoft Research, USA
Ed Dawson	Queensland University of Technology, Australia
Kaisa Nyberg	Aalto University School of Science, Finland
Ron Rivest	Massachusetts Institute of Technology, USA
Moti Yung	Google, USA

Program Chair

Kaisa Nyberg	Aalto University School of Science, Finland

Program Committee

Frederik Armknecht	University of Mannheim, Germany
Josh Benaloh	Microsoft Research, USA
John Black	University of Colorado, USA
Jean-Sebastien Coron	University of Luxembourg, Luxembourg
Orr Dunkelman	University of Haifa, Israel
Steven Galbraith	University of Auckland, New Zealand
Henri Gilbert	ANSSI, France
Jens Groth	University College London, UK
Helena Handschuh	Cryptography Research, Inc., USA
Thomas Johansson	Lund University, Sweden
Marc Joye	Technicolor, USA
John Kelsey	National Institute of Standards and Technology, USA
Dmitry Khovratovich	University of Luxembourg, Luxembourg
Kwangjo Kim	Korea Advanced Institute of Science and Technology, Republic of Korea
Lars R. Knudsen	Technical University of Denmark, Denmark
Anna Lysyanskaya	Brown University, USA
María Naya-Plasencia	Inria, France
Kaisa Nyberg (chair)	Aalto University School of Science, Finland
Elisabeth Oswald	University of Bristol, UK
Kenneth Paterson	Royal Holloway University of London, UK

David Pointcheval	École Normal Supérieure, France
Rei Safavi-Naini	University of Calgary, Canada
Kazue Sako	NEC, Japan
Palash Sarkar	Indian Statistical Institute, India
Ali Aydin Selçuk	TOBB University of Economics and Technology, Turkey
Nigel Smart	University of Bristol, UK
Vanessa Teague	University of Melbourne, Australia
Dominique Unruh	University of Tartu, Estonia
Serge Vaudenay	École Polytechnique Fédérale de Lausanne, Switzerland
Huaxiong Wang	Nanyang Technological University, Singapore

External Reviewers

Mohamed Ahmed Abdelraheem	Essam Ghadafi	Kerry McKay
Divesh Aggarwal	Jorge Guajardo	Kazuhiko Minematsu
Murat Ak	Florian Hahn	Khoa Nguyen
James Alderman	Mike Hamburg	Kazuma Ohara
Elena Andreeva	Ghaith Hammouri	Adam O'Neill
Diego Aranha	Haruna Higo	Ray Perlner
Shi Bai	Daniel Hutchinson	Leo Perrin
Foteini Baldimtsi	Toshiyuki Isshiki	Thomas Peters
Subhadeep Banik	Christian Janson	Christophe Petit
Larry Bassham	Angela Jäschke	Duong Hieu Phan
Sanjay Bhattacherjee	Mahavir Jhawar	Rachel Player
Sonia Bogos	Orhun Kara	Jérôme Plût
Christina Boura	Ferhat Karakoc	Emmanuel Prouff
Florian Bourse	Hak Ju Kim	Somindu C. Ramanna
Beyhan Çalışkan	Stefan Koelbl	Jean-René Reinhard
Andrea Cerulli	Alptekin Küpçü	Christian Reuter
Pyrros Chaidos	Adeline Langlois	Reza Reyhanitabar
Debrup Chakraborty	Martin Lauridsen	Thomas Roche
Rakyong Choi	Hyung Tae Lee	Arnab Roy
Ashish Choudhury	Anthony Leverrier	Sumanta Sarkar
Geoffroy Couteau	Gaëtan Leurent	Peter Scholl
Gareth Davies	Kaitai Liang	Yannick Seurin
Angelo De Caro	Fuchun Lin	Siamak Shahandashti
Huseyin Demirci	Zhen Liu	Dale Sibborn
Alexandre Duc	Atul Luykx	Shashank Singh
Sebastian Faust	Ceyda Mangir	Isamu Teranishi
Jun Furukawa	Joana Marim	Cihangir Tezcan
Shishay Gebregiyorgis	Dan Martin	Nicolas Theriault
	Alexander May	Susan Thomson

Tyge Tiessen
Elmar Tischhauser
Meltem Sonmez Turan
Joop van de Pol
Damien Vergnaud
Damian Vizár
Pengwei Wang
Guomin Yang
Hongbo Yu
Emre Yuce
Liangfeng Zhang

Contents

Authenticated Encryption

Detecting and Tracing Malicious Activities

Implementation Attacks on Exponentiation Algorithms

Homomorphic Encryption and Its Applications