

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, Lancaster, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zürich, Zürich, Switzerland

John C. Mitchell

Stanford University, Stanford, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Dortmund, Germany

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbrücken, Germany

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

Editor
Kaisa Nyberg
Aalto University School of Science
Espoo
Finland

ISSN 0302-9743
Lecture Notes in Computer Science
ISBN 978-3-319-16714-5
DOI 10.1007/978-3-319-16715-2

ISSN 1611-3349 (electronic)
ISBN 978-3-319-16715-2 (eBook)

Library of Congress Control Number: 2015934581

LNCS Sublibrary: SL4 – Security and Cryptology

Springer Cham Heidelberg New York Dordrecht London

© Springer International Publishing Switzerland 2015

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

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, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

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

Timing Attacks

Just a Little Bit More	3
<i>Joop van de Pol, Nigel P. Smart, and Yuval Yarom</i>	
Cache Storage Attacks.	22
<i>Billy Bob Brumley</i>	

Design and Analysis of Block Ciphers

Analyzing Permutations for AES-like Ciphers: Understanding ShiftRows . . .	37
<i>Christof Beierle, Philipp Jovanovic, Martin M. Lauridsen, Gregor Leander, and Christian Rechberger</i>	
Improved Attacks on Reduced-Round Camellia-128/192/256	59
<i>Xiaoyang Dong, Leibo Li, Keting Jia, and Xiaoyun Wang</i>	

Attribute and Identity Based Encryption

Duality in ABE: Converting Attribute Based Encryption for Dual Predicate and Dual Policy via Computational Encodings	87
<i>Nuttapong Attrapadung and Shota Yamada</i>	
Revocable Hierarchical Identity-Based Encryption: History-Free Update, Security Against Insiders, and Short Ciphertexts.	106
<i>Jae Hong Seo and Keita Emura</i>	

Membership

Revisiting Cryptographic Accumulators, Additional Properties and Relations to Other Primitives	127
<i>David Derler, Christian Hanser, and Daniel Slamanig</i>	
Non-Interactive Zero-Knowledge Proofs of Non-Membership	145
<i>Olivier Blazy, Céline Chevalier, and Damien Vergnaud</i>	

Secure and Efficient Implementation of AES Based Cryptosystems

Implementing GCM on ARMv8	167
<i>Conrado P.L. Gouvêa and Julio López</i>	

Higher-Order Masking in Practice: A Vector Implementation
of Masked AES for ARM NEON 181
*Junwei Wang, Praveen Kumar Vadnala, Johann Großschädl,
and Qiuliang Xu*

Chosen Ciphertext Attacks in Theory and Practice

Completeness of Single-Bit Projection-KDM Security for Public
Key Encryption 201
*Fuyuki Kitagawa, Takahiro Matsuda, Goichiro Hanaoka,
and Keisuke Tanaka*

Format Oracles on OpenPGP 220
Florian Maury, Jean-René Reinhard, Olivier Levillain, and Henri Gilbert

Algorithms for Solving Hard Problems

Finding Shortest Lattice Vectors in the Presence of Gaps 239
Wei Wei, Mingjie Liu, and Xiaoyun Wang

A Simple and Improved Algorithm for Integer Factorization
with Implicit Hints 258
Koji Nuida, Naoto Itakura, and Kaoru Kurosawa

Constructions of Hash Functions and Message Authentication Codes

Hash Functions from Defective Ideal Ciphers. 273
Jonathan Katz, Stefan Lucks, and Aishwarya Thiruvengadam

Using an Error-Correction Code for Fast, Beyond-birthday-bound
Authentication 291
Yusi Zhang

Secure Multiparty Computation

Efficient Leakage Resilient Circuit Compilers 311
*Marcin Andrychowicz, Ivan Damgård, Stefan Dziembowski,
Sebastian Faust, and Antigoni Polychroniadou*

Optimally Efficient Multi-Party Fair Exchange and Fair Secure
Multi-Party Computation 330
Handan Kılınç and Alptekin Küpçü

Authenticated Encryption

How to Incorporate Associated Data in Sponge-Based Authenticated Encryption 353
Yu Sasaki and Kan Yasuda

Cryptanalysis of Ascon 371
Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schl affer

Detecting and Tracing Malicious Activities

Stronger Security Notions for Decentralized Traceable Attribute-Based Signatures and More Efficient Constructions 389
Essam Ghadafi

Re-Encryption Verifiability: How to Detect Malicious Activities of a Proxy in Proxy Re-Encryption 408
Satsuya Ohata, Yutaka Kawai, Takahiro Matsuda, Goichiro Hanaoka, and Kanta Matsuura

Implementation Attacks on Exponentiation Algorithms

Exploiting Collisions in Addition Chain-Based Exponentiation Algorithms Using a Single Trace. 429
Neil Hanley, HeeSeok Kim, and Michael Tunstall

Cold Boot Attacks in the Discrete Logarithm Setting 447
Bertram Poettering and Dale L. Sibborn

Homomorphic Encryption and Its Applications

Communication Optimal Tardos-Based Asymmetric Fingerprinting 465
Aggelos Kiayias, Nikos Leonardos, Helger Lipmaa, Kateryna Pavlyk, and Qiang Tang

Linearly Homomorphic Encryption from DDH. 484
Guilhem Castagnos and Fabien Laguillaumie

Author Index 503