Lecture Notes in Computer Science 8043

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

Ran Canetti Juan A. Garay (Eds.)

Advances in Cryptology – CRYPTO 2013

33rd Annual Cryptology Conference
Santa Barbara, CA, USA, August 18-22, 2013
Proceedings, Part II

Springer

Volume Editors

Ran Canetti
Boston University and Tel Aviv University
111 Cummington Street
Boston, MA 02215, USA
E-mail: canetti@bu.edu

Juan A. Garay
AT&T Labs – Research
180 Park Avenue
Florham Park, NJ 07932, USA
E-mail: garay@research.att.com

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-40083-4 e-ISBN 978-3-642-40084-1
DOI 10.1007/978-3-642-40084-1
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2013944216

CR Subject Classification (1998): E.3, F.2, K.6.5, G.2.1, D.4.6, C.2.0, J.1

LNCS Sublibrary: SL 4 – Security and Cryptology

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

CRYPTO 2013, the 33rd Annual International Cryptology Conference, was held August 18–22, 2013, on the campus of the University of California, Santa Barbara. The event was sponsored by the International Association for Cryptologic Research (IACR) in cooperation with the UCSB Computer Science Department and the IEEE Computer Society's Technical Committee on Security and Privacy.

The program represents the recent significant advances in all areas of cryptology. Sixty-one papers were included in the program, a record number for IACR flagship conferences. This two-volume proceedings contains the revised versions of all the papers. One pair of papers shared a single presentation slot in the program. There were also two invited talks. On Monday, Cindy Cohn from the Electronic Frontier Foundation gave a talk entitled "Crypto Wars Part 2 Have Begun." On Wednesday, Adam Langley from Google spoke about "Why the Web Still Runs on RC4," in a joint session with CHES 2013. To accommodate the increase in the number of papers, sessions were held throughout Tuesday and Thursday afternoons. The rump session took place as usual on Tuesday evening, and was chaired by Dan Bernstein and Tanja Lange.

For the Best Paper Award, the Program Committee (PC) unanimously selected the paper "On the Function Field Sieve and the Impact of Higher Splitting Probabilities" by Faruk Gologlu, Robert Granger, Gary McGuire and Jens Zumbragel.

This year we also awarded a *Best Young-Author Paper Award.* To be eligible for the award, all authors of the paper had to either be full-time students or have received their PhDs in 2011 or later. The award was given to the paper "Counter-Cryptanalysis: Reconstructing Flame's New Variant Collision Attack" by Marc Stevens.

Faced with a large number of high-quality submissions, the PC decided to significantly increase the number of papers in the program from last year's 48 papers, at the price of making the program longer and keeping the paper presentations short (20 minutes per paper, including questions and answers). Another option that was seriously considered was to move to parallel sessions on some of the days of the conference. This would have allowed for somewhat longer paper presentations, and an early adjourn on Thursday. In the end, we opted to retain the single-session format, with the hope of keeping the community more unified by allowing participants to attend all talks.

The papers were reviewed by a PC consisting of 40 leading researchers in the field, in addition to the two co-chairs. Each PC member was allowed to submit one paper, plus an additional one if co-authored with a student. PC-authored papers were held to higher standards during the review process. Papers were reviewed in a double-blind fashion. Initially, each paper was assigned to three reviewers (four for PC-authored papers). During the discussion phase, when necessary, extra reviews were solicited. As part of the paper discussion phase, we held a two-day PC meeting on May 2 and 3, at the AT&T building in downtown Manhattan.

We strived to ensure that all papers received a fair and objective evaluation by experts as well as a broader group of PC members. The final decisions were made based on the reviews and discussion, and taking other factors such as balance of the program into account.

This year we initiated an early review and rebuttal process, where authors received preliminary reviews on their submissions about midway through the review period, and were given the option to comment on the reviews within a window of several days. The authors' comments were then taken into account in the discussions within the PC and in the final reviews. This process was labor-intensive; however, we feel it was worthwhile, as it resulted in a significantly better understanding of many submissions.

We would like to sincerely thank the authors of all submissions—those whose papers made it into the program and those whose papers did not. Our sincere gratitude also goes out to the PC members, who have invested an incredible amount of work in reviewing papers, interacting with the authors via the rebuttal mechanism, and participating in so many discussions on papers, their contribution, and the state of the art in their fields of expertise. We also sympathize with the occasional frustration from seeing decisions go against personal recommendations and preferences, in spite of the hard work invested.

We are also indebted to the many external reviewers, who significantly contributed to the comprehensive evaluation of papers. A list of PC members and external reviewers appears after this note. Despite all our efforts, the list of external reviewers may have errors or omissions; we apologize for that in advance.

We would like to thank Helena Handschuh, the General Chair, for working closely with us throughout the whole process, providing the much-needed support in every step, including creating and maintaining the website, and taking care of all aspects of the conference's logistics.

Special thanks are due to Shai Halevi, who provided us with unlimited support of his *websubrev* software, which we used for the whole conference planning, paper evaluation, and interaction with PC members and authors. Josh Benaloh, was our IACR point of contact, always providing timely and informative answers to our questions. Alfred Hofmann and his colleagues at Springer provided a meticulous service for the timely production of this volume.

Finally, we would like to thank Qualcomm, Microsoft, Google, Good Technologies, and Cryptography Research Inc. for their generous support.

August 2013

Ran Canetti
Juan A. Garay

Crypto 2013
The 33rd International Cryptology Conference

Sponsored by *the International Association for Cryptologic Research*

General Chair

Helena Handschuh	Cryptography Research Inc. and K.U. Leuven

Program Co-chairs

Ran Canetti	Boston University and Tel Aviv University
Juan A. Garay	AT&T Labs — Research

Program Committee

Masayuki Abe	NTT, Japan
Mihir Bellare	UCSD, USA
Zvika Brakerski	Stanford University, USA
Jan Camenisch	IBM Research, Zürich, Switzerland
David Cash	Rutgers University, USA
Kai-Min Chung	Cornell University, USA and Academia Sinica, Taiwan
Jean-Sebastien Coron	University of Luxembourg
Dana Dachman-Soled	Microsoft Research, USA
Stefan Dziembowski	University of Warsaw, Poland and University of Rome I, Italy
Iftach Haitner	Tel Aviv University, Israel
Shai Halevi	IBM Research, USA
Goichiro Hanaoka	AIST, Japan
Dennis Hofheinz	KIT, Germany
Jonathan Katz	University of Maryland, USA
Lars R Knudsen	DTU, Denmark
Eyal Kushilevitz	Technion, Israel
Kristin Lauter	Microsoft Research, USA
Huijia Lin	MIT and Boston University, USA
Yehuda Lindell	Bar Ilan University, Israel
Vadim Lyubashevsky	ENS, France
John Mitchell	Stanford University, USA
Tal Moran	Inter-Disciplinary Center, Israel
Jesper B Nielsen	University of Aarhus, Denmark
Christof Paar	University of Bochum, Germany

Manoj M Prabhakaran	University of Illinois at Urbana-Champaign, USA
Tal Rabin	IBM Research, USA
Charles Rackoff	University of Toronto, Canada
Christian Rechberger	DTU, Denmark
Thomas Ristenpart	University of Wisconsin, USA
Guy Rothblum	Microsoft Research, USA
Rei Safavi	University of Calgary, Canada (advisory member)
Christian Schaffner	University of Amsterdam, The Netherlands
Hovav Shacham	UCSD, USA
Vitaly Shmatikov	UT Austin, USA
Nigel Smart	University of Bristol, UK
Adam Smith	Penn State University, USA
Martijn Stam	University of Bristol, UK
John P Steinberger	Tsinghua University, China
Frederik Vercauteren	K.U. Leuven, Belgium
Xiaoyun Wang	Tsinghua University, China
Daniel Wichs	Northeastern University, USA

External Reviewers

Divesh Aggarwal
Adi Akavia
Martin Albrecht
Elena Andreeva
Benny Applebaum
Gilad Asharov
Gilles van Assche
Nuttapong Attrapadung
Paulo Barreto
Timo Bartkewitz
Raef Bassily
Amos Beimel
David Bernhard
Dan Bernstein
Nir Bitansky
Andrey Bogdanov
Joppe Bos
Christina Boura
Elette Boyle
Cas Cremers
Christophe De Cannire
Anne Canteaut
Angelo De Caro
Ignacio Cascudo
Nishanth Chandran
Melissa Chase
Nathan Chenette
Alessandro Chiesa
Sherman S.M. Chow
Craig Costello
Scott Coull
Ivan Damgaard
Maria Dubovitskaya
Leo Ducas
Frédéric Dupuis
Konrad Durnoga
Markus Drmuth
Keita Emura
Robert Enderlein
Sebastian Faust
Serge Fehr
Sean Hallgren
Feng-Hao
Dario Fiore
Marc Fischlin
Tore Kasper Frederiksen
Eiichiro Fujisaki
Steven Galbraith
Sanjam Garg
Ran Gelles
Rosario Gennaro
Craig Gentry
Benedikt Gierlichs
Vipul Goyal
Louis Granboulan
Adam Groce
Jens Groth
Kris Haralambiev
Moritz Hardt
Carmit Hazay
Nadia Heninger
Jens Hermans
Gottfried Herold
Martin Hirt
Viet Tung Hoang
Susan Hohenberger
Yuval Ishai
Tibor Jager
Abhishek Jain

Thomas P. Jakobsen
Chen Jie
Charanjit Jutla
Seny Kamara
Tomasz Kazana
Aoki Kazumaro
Sriram Keelveedhi
Dmitry Khovratovich
Eike Kiltz
Ilya Kizhvatov
Markulf Kohlweiss
Venkata Koppula
Hugo Krawczyk
Stephan Krenn
Ranjit Kumaresan
Kaoru Kurosawa
Tanja Lange
Enrique Larraia
Martin M. Lauridsen
Gregor Leander
Chen-Kuei Lee
Anja Lehmann
Gaetan Leurent
Kevin Lewi
Allison Lewko
Feng-Hao Liu
Feng-hao Liu
Jake Loftus
Steve Lu
Edward Lui
Mohammad Mahmoody
Hemanta Maji
Takahiro Matsuda
Chrysanti Mavrotami
Travis Mayberry
Sarah Meiklejohn
Florian Mendel
Alexander Meurer
Daniele Micciancio
Eric Miles
Kazuhiko Minematsu
Ilya Mironov
Peter Montgomery
Amir Moradi
Paz Morillo
Kirill Morozov
Nicky Mouha
Naveed Muhammad
Michael Naehrig
Maria Naya-Plasencia
Gregory Neven
Phong Nguyen
Ryo Nishimaki
Kobbi Nissim
Adam O'Neill
Tatsuaki Okamoto
Claudio Orlandi
Rafi Ostrovsky
Omer Paneth
Bryan Parno
Anat Paskin-Cherniavsky
Christopher J. Peikert
Yuval Peres
Ludovic Perret
Eduoardo Persichetti
Joop van de Pol
Christopher Portmann
Emmanuel Prouff
Ananth Raghunathan
Kasper B. Rasmussen
Mariana Raykova
Oded Regev
Leonid Reyzin
Ben Riva
Matthieu Rivain
Phillip Rogaway
Mike Rosulek
Ron Rothblum
Yannis Rouselakis
Yusuke Sakai
Koichi Sakumoto
Louis Salvail
Palash Sarkar
Giannicola Scarpa
Dominique Schroeder
Peter Schwabe
Karn Seth
Ronen Shaltiel
Chih-Hao Shen
Thomas Shrimpton
Maciej Skórski
Graeme Smith
Fang Song
Damien Stehle
Ron Steinfeld
Koutarou Suzuki
Katsuyuki Takashima
Sidharth Telang
Aris Tentes
Isamu Teranishi
Seth Terashima
Stefano Tessaro
Susan Thomson
Mehdi Tibouch
Jean-Pierre Tillich
Tomas Toft
Eran Tromer
Max Tuengerthal
Madhur Tulsiani
Vinod Vaikuntanathan
Vesselin Velichkov
K. Venkata
Muthuramakrishnan
Venkitasubramaniam
Thomas Vidick
Colin Walter
Meiqin Wang
Brent Waters
Dirk Westhoff
Carolyn Whitnall
Ronald de Wolf
David Wu
Xiaodi Wu
Keita Xagawa
Shota Yamada
Scott Yilek
Kazuki Yoneyama
Hongbo Yu
Greg Zaverucha
Maciej Zdanowicz
Mark Zhandry
Colin Jia Zheng
Joe Zimmerman
Angela Zottarel

Table of Contents – Part II

Session 11: Implementation-Oriented Protocols

Invited Talk: Why the Web Still Runs on RC4

Session 12: Number-Theoretic Hardness

Session 13: MPC — Foundations

Session 14: Codes and Secret Sharing

Session 15: Signatures and Authentication

Session 16: Quantum Security

Session 17: New Primitives

Session 18: Functional Encryption I

Session 19: Functional Encryption II

Table of Contents – Part I

Session 1: Lattices and FHE

Invited Talk: Crypto Wars Part 2 Have Begun

Session 2: Foundations of Hardness

Session 3: Cryptanalysis I

Session 4: Cryptanalysis II

Session 5: MPC – New Directions

Session 6: Leakage Resilience

Session 7: Symmetric Encryption and PRFs

Session 8: Key Exchange

Session 9: Multi Linear Maps

Session 10: Ideal Ciphers