Lecture Notes in Computer Science 7194

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

Editorial Board

David Hutchison
Lancaster University, UK

Takeo Kanade
Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler
University of Surrey, Guildford, UK

Jon M. Kleinberg
Cornell University, Ithaca, NY, USA

Alfred Kobsa
University of California, Irvine, CA, USA

Friedemann Mattern
ETH Zurich, Switzerland

John C. Mitchell
Stanford University, CA, USA

Moni Naor
Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz
University of Bern, Switzerland

C. Pandu Rangan
Indian Institute of Technology, Madras, India

Bernhard Steffen
TU Dortmund University, Germany

Madhu Sudan
Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos
University of California, Los Angeles, CA, USA

Doug Tygar
University of California, Berkeley, CA, USA

Gerhard Weikum
Max Planck Institute for Informatics, Saarbruecken, Germany

Ronald Cramer (Ed.)

Theory of Cryptography

9th Theory of Cryptography Conference, TCC 2012
Taormina, Sicily, Italy, March 19-21, 2012
Proceedings

Springer

Volume Editor

Ronald Cramer
Cryptology Group, CWI Amsterdam
and
Mathematical Institute, Leiden University
The Netherlands
E-mail: cramer@cwi.nl, cramer@math.leidenuniv.nl

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-28913-2 e-ISBN 978-3-642-28914-9
DOI 10.1007/978-3-642-28914-9
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012933240

CR Subject Classification (1998): E.3, C.2, D.4.6, K.6.5, G.2, I.1

LNCS Sublibrary: SL 4 – Security and Cryptology

© Springer-Verlag Berlin Heidelberg 2012
This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.
The use of general descriptive names, registered names, trademarks, 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.

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

TCC 2012, the 9th Theory of Cryptography Conference, was held in Taormina (Sicily), Italy, during March 19–21, 2012. It was sponsored by the International Association for Cryptologic Research (IACR). The General Chairs were Nelly Fazio and Rosario Gennaro. The Local Arrangements Chair was Dario Catalano.

By the deadline of September 15, 2011, the Program Committee (PC) had received 131 electronic submissions. As usual, the selection process was carried out using a Web-based interface and consisted of three phases. In the review phase each submission was assigned to at least three PC members for independent review (six in the case of a PC member submission). In the discussion phase, reviews pertaining to the same submission were compared and agreement on a common view was reached where possible. Additional reviews were solicited as needed. The perceived relative merits of all submissions were taken into consideration as a basis for the selection phase. By the December 1 deadline for notification of decisions, the PC had selected 36 submissions for (20-min.) presentation at the conference. Reviewer comments for all submissions were sent out to their respective authors soon after. These proceedings contain the revised versions of the 36 selected submissions, as received by January 3, 2012. These revised versions were not subjected to further review by the PC and authors bear full responsibility for contents.

The program also featured two invited (60-min.) talks. Jens Groth and Sergey Yekhanin treated us to excellent surveys of Non-Interactive Zero-Knowledge and Locally Decodable Codes, respectively. A Best Student Paper Award was shared by Nir Bitansky and Omer Paneth for their paper "Point Obfuscation and 3-round Zero-Knowledge" and by Anindya De for his paper "Lower Bounds in Differential Privacy". In addition, a traditional Rump Session was held, consisting of (5-min.) research announcements. It was organized and chaired by Tal Malkin. The organizers had this evening session well catered for with nice drinks and snacks.

I thank the PC members for their hard work, as well as the external reviewers. Oded Goldreich (TCC Steering Committee Chair) and Yuval Ishai (TCC 2011 Program Chair) provided quick and helpful advice upon my request as well as answers to my questions, for which I am grateful. The PC used Shai Halevi's excellent Web Submission and Review software to handle the submissions. Thanks to Maarten Dijkema of CWI's IT Support for running this software at our system and for his unwavering assistance and thanks to Shai for rendering efficient "customer service" to us. Also, thanks to Tal for running the Rump Session. The

organizers wish to express their gratitude to the TCC 2012 sponsors Alcatel-Lucent Bell Labs, IBM Research and Microsoft Research for generous donations that supported local organization in several ways, including student stipends. In turn, I thank Nelly, Rosario and Dario for our pleasant collaboration. Finally, thanks to all authors of submissions to TCC 2012.

January 2012 Ronald Cramer

TCC 2012

9th IACR Theory of Cryptography Conference

Taormina, Sicily, Italy
March 19–21, 2012

Sponsored by the *International Association for Cryptologic Research (IACR)*

General Chairs

Nelly Fazio	City University of New York (CUNY), USA
Rosario Gennaro	IBM Thomas J. Watson Research Center, USA

Local Arrangements Chair

Dario Catalano	Università di Catania, Italy

Program Chair

Ronald Cramer	CWI Amsterdam and Leiden University, The Netherlands

Program Committee

Masayuki Abe	NTT, Japan
Amos Beimel	Ben-Gurion University, Israel
Alexandra Boldyreva	Georgia Tech, USA
Iftach Haitner	Tel Aviv University, Israel
Martin Hirt	ETH Zurich, Switzerland
Dennis Hofheinz	Karlsruhe Institute of Technology, Germany
Jonathan Katz	University of Maryland, USA
Vadim Lyubashevsky	ENS, France
Tal Malkin	Columbia University, USA
Daniele Micciancio	UCSD, USA
Jesper Buus Nielsen	Aarhus University, Denmark
Carles Padró	Nanyang Technological University, Singapore
Mike Rosulek	University of Montana, USA
Amit Sahai	UCLA, USA
Berry Schoenmakers	TU Eindhoven, The Netherlands

Vinod Vaikuntanathan	University of Toronto, Canada
Daniel Wichs	IBM T.J. Watson Research Center, USA
Jürg Wullschleger	Université de Montréal and McGill University, Canada
Moti Yung	Google Research, New York, USA

Steering Committee

Mihir Bellare	UCSD, USA
Ivan Damgård	Aarhus University, Denmark
Oded Goldreich (Chair)	Weizmann Institute of Science, Israel
Shafi Goldwasser	MIT, USA
Shai Halevi	IBM T.J. Watson Research Center, USA
Russell Impagliazzo	UCSD, USA
Ueli Maurer	ETH Zurich, Switzerland
Silvio Micali	MIT, USA
Moni Naor	Weizmann Institute of Science, Israel
Tatsuaki Okamoto	NTT, Japan

External Reviewers

Michel Abdalla
Divesh Aggarwal
Shweta Agrawal
Joël Alwen
Elena Andreeva
Kazumaro Aoki
Benny Applebaum
Claudio Orlandi
Seiko Arita
Gilad Asharov
Endre Bangerter
Boaz Barak
Kfir Barhum
Raef Bassily
Itay Berman
Gaetan Bisson
Nir Bitansky
Niek J. Bouman
Elette Boyle
Zvika Brakerski
Jan Camenisch
Ran Canetti
Igor Carboni Oliveira
Ignacio Cascudo
David Cash
Nishanth Chandran
Mahdi Cheraghchi
Kai-Min Chung
Sandro Coretti
Dana Dachman-Soled
Bernardo David
Gregory Demay
Yi Deng
Alex Dent
Yevgeniy Dodis
Leo Ducas
Stefan Dziembowski
Nico Döttling
Pooya Farshim
Sebastian Faust
Serge Fehr
Dario Fiore
Eiichiro Fujisaki
Dave Freeman
Jakob Funder
David Galindo
Sanjam Garg
Rosario Gennaro

Wesley George
Sergey Gorbunov
Dov Gordon
Vipul Goyal
Matthew Green
Jens Groth
Robbert de Haan
Shai Halevi
Moritz Hardt
David Harris
Carmit Hazay
Brett Hemenway
Javier Herranz
Viet Tung Hoang
Susan Hohenberger
Thomas Holenstein
Perry Hooker
Pavel Hubacek
Yuval Ishai
Abhishek Jain
Yael Tauman Kalai
Eike Kiltz
Vladimir Kolesnikov
Daniel Kraschewski
Hugo Krawczyk
Stephan Krenn
Ralf Küsters
Virendra Kumar
Eyal Kushilevitz
Robin Künzler
Allison Bishop Lewko
Hendrik Lenstra
Xin Li
Peter van Liesdonk
Huijia Rachel Lin
Adriana López-Alt
Christoph Lucas
Hemanta Maji
Takahiro Matsuda
Sigurd Torkel Meldgaard
Josep M. Miret
Petros Mol
Tal Moran
Ryo Nishimaki
Kobbi Nissim
Peter Sebastian Nordholt
Miyako Ohkubo
Tatsuaki Okamoto
Anat Paskin-Cherniavsky
Rafael Pass
Kenny Paterson
Arpita Patra
Serdar Pehlivanoglu
Chris Peikert
Duong Hieu Phan
Krzysztof Pietrzak
Benny Pinkas
Manoj Prabhakaran
Pavel Raykov
Mariana Raykova
Omer Reingold
Oded Regev
Leonid Reyzin
Alon Rosen
Aaron Roth
Guy Rothblum
Yannis Rouselakis
Louis Salvail
Yu Sasaki
Christian Schaffner
Dominique Schröder
Gil Segev
Ronen Shaltiel
Elaine Shi
Nigel Smart
Bart de Smit
Martijn Stam
Damien Stehlé
John Steinberger
Ron Steinfeld
Marc Stevens
Björn Tackmann
Katsuyuki Takashima
Kunal Talwar
Aris Tentes
Stefano Tessaro
Tomas Toft
Marco Tomamichel
Boaz Tsaban
Dominique Unruh

Yevgeniy Vahlis
Muthu Venkitasubramaniam
Jorge L. Villar
Ivan Visconti
Akshay Wadia
Bogdan Warinschi
Brent Waters
Hoeteck Wee
Benne de Weger
Douglas Wikström
Severin Winkler
Keita Xagawa
David Xiao
Kan Yasuda
Arkady Yerukhimovich
Scott Yilek
Kazuki Yoneyama
Hila Zarosim
Hong-Sheng Zhou
Michael Zieve
Vassilis Zikas
Angela Zottarel

Table of Contents

Secure Computation

Computing on Authenticated Data 1
Jae Hyun Ahn, Dan Boneh, Jan Camenisch, Susan Hohenberger, abhi shelat, and Brent Waters

Identifying Cheaters without an Honest Majority 21
Yuval Ishai, Rafail Ostrovsky, and Hakan Seyalioglu

On the Security of the "Free-XOR" Technique 39
Seung Geol Choi, Jonathan Katz, Ranjit Kumaresan, and Hong-Sheng Zhou

Secure Two-Party Computation with Low Communication 54
Ivan Damgård, Sebastian Faust, and Carmit Hazay

(Blind) Signatures and Threshold Encryption

Non-interactive CCA-Secure Threshold Cryptosystems with Adaptive Security: New Framework and Constructions 75
Benoît Libert and Moti Yung

Round-Optimal Privacy-Preserving Protocols with Smooth Projective Hash Functions 94
Olivier Blazy, David Pointcheval, and Damien Vergnaud

On the Instantiability of Hash-and-Sign RSA Signatures 112
Yevgeniy Dodis, Iftach Haitner, and Aris Tentes

Beyond the Limitation of Prime-Order Bilinear Groups, and Round Optimal Blind Signatures 133
Jae Hong Seo and Jung Hee Cheon

Zero-Knowledge and Security Models

On Efficient Zero-Knowledge PCPs 151
Yuval Ishai, Mohammad Mahmoody, and Amit Sahai

Progression-Free Sets and Sublinear Pairing-Based Non-Interactive Zero-Knowledge Arguments 169
Helger Lipmaa

Point Obfuscation and 3-Round Zero-Knowledge 190
Nir Bitansky and Omer Paneth

Confidentiality and Integrity: A Constructive Perspective 209
Ueli Maurer, Andreas Rüedlinger, and Björn Tackmann

Leakage-Resilience

Leakage-Resilient Circuits without Computational Assumptions 230
Stefan Dziembowski and Sebastian Faust

A Parallel Repetition Theorem for Leakage Resilience 248
Zvika Brakerski and Yael Tauman Kalai

Leakage-Tolerant Interactive Protocols 266
Nir Bitansky, Ran Canetti, and Shai Halevi

Hash Functions

On the Public Indifferentiability and Correlation Intractability of the 6-Round Feistel Construction 285
Avradip Mandal, Jacques Patarin, and Yannick Seurin

Collisions Are Not Incidental: A Compression Function Exploiting Discrete Geometry 303
Dimitar Jetchev, Onur Özen, and Martijn Stam

Differential Privacy

Lower Bounds in Differential Privacy 321
Anindya De

Iterative Constructions and Private Data Release 339
Anupam Gupta, Aaron Roth, and Jonathan Ullman

Pseudorandomness I

From Non-adaptive to Adaptive Pseudorandom Functions 357
Itay Berman and Iftach Haitner

Hardness Preserving Constructions of Pseudorandom Functions 369
Abhishek Jain, Krzysztof Pietrzak, and Aris Tentes

Computational Extractors and Pseudorandomness 383
Dana Dachman-Soled, Rosario Gennaro, Hugo Krawczyk, and Tal Malkin

Dedicated Encryption I

Functional Re-encryption and Collusion-Resistant Obfuscation 404
Nishanth Chandran, Melissa Chase, and Vinod Vaikuntanathan

How to Delegate and Verify in Public: Verifiable Computation from Attribute-Based Encryption 422
Bryan Parno, Mariana Raykova, and Vinod Vaikuntanathan

On Black-Box Reductions between Predicate Encryption Schemes 440
Vipul Goyal, Virendra Kumar, Satya Lokam, and Mohammad Mahmoody

Security Amplification

Lossy Functions Do Not Amplify Well 458
Krzysztof Pietrzak, Alon Rosen, and Gil Segev

Counterexamples to Hardness Amplification beyond Negligible 476
Yevgeniy Dodis, Abhishek Jain, Tal Moran, and Daniel Wichs

Resettable and Parallel Zero Knowledge

Resettable Statistical Zero Knowledge 494
Sanjam Garg, Rafail Ostrovsky, Ivan Visconti, and Akshay Wadia

The Knowledge Tightness of Parallel Zero-Knowledge 512
Kai-Min Chung, Rafael Pass, and Wei-Lung Dustin Tseng

Simultaneously Resettable Arguments of Knowledge 530
Chongwon Cho, Rafail Ostrovsky, Alessandra Scafuro, and Ivan Visconti

Dedicated Encryption II

Subspace LWE 548
Krzysztof Pietrzak

Bounded-Collusion IBE from Key Homomorphism 564
Shafi Goldwasser, Allison Lewko, and David A. Wilson

A Unified Approach to Deterministic Encryption: New Constructions and a Connection to Computational Entropy 582
Benjamin Fuller, Adam O'Neill, and Leonid Reyzin

Pseudorandomness II

A Dichotomy for Local Small-Bias Generators 600
Benny Applebaum, Andrej Bogdanov, and Alon Rosen

Randomness Condensers for Efficiently Samplable, Seed-Dependent Sources 618
Yevgeniy Dodis, Thomas Ristenpart, and Salil Vadhan

Uniqueness Is a Different Story: Impossibility of Verifiable Random Functions from Trapdoor Permutations 636
Dario Fiore and Dominique Schröder

Author Index 655