

*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*

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

© International Association for Cryptologic Research 2013

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. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

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.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

*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 Zumborgel.

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

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



# Table of Contents – Part II

## Session 11: Implementation-Oriented Protocols

Fast Cut-and-Choose Based Protocols for Malicious and Covert Adversaries .....	1
<i>Yehuda Lindell</i>	
Efficient Secure Two-Party Computation Using Symmetric Cut-and-Choose .....	18
<i>Yan Huang, Jonathan Katz, and David Evans</i>	
Garbled Circuits Checking Garbled Circuits: More Efficient and Secure Two-Party Computation .....	36
<i>Payman Mohassel and Ben Riva</i>	
Improved OT Extension for Transferring Short Secrets .....	54
<i>Vladimir Kolesnikov and Ranjit Kumaresan</i>	
Time-Optimal Interactive Proofs for Circuit Evaluation .....	71
<i>Justin Thaler</i>	
SNARKs for C: Verifying Program Executions Succinctly and in Zero Knowledge .....	90
<i>Eli Ben-Sasson, Alessandro Chiesa, Daniel Genkin, Eran Tromer, and Madars Virza</i>	

## Invited Talk: Why the Web Still Runs on RC4

## Session 12: Number-Theoretic Hardness

On the Function Field Sieve and the Impact of Higher Splitting Probabilities: Application to Discrete Logarithms in $\mathbb{F}_{2^{1971}}$ and $\mathbb{F}_{2^{3164}}$ .....	109
<i>Faruk Göloğlu, Robert Granger, Gary McGuire, and Jens Zumbrägel</i>	
An Algebraic Framework for Diffie-Hellman Assumptions .....	129
<i>Alex Escala, Gottfried Herold, Eike Kiltz, Carla Ràfols, and Jorge Villar</i>	
Hard-Core Predicates for a Diffie-Hellman Problem over Finite Fields...	148
<i>Nelly Fazio, Rosario Gennaro, Irippuge Milinda Perera, and William E. Skeith III</i>	

## Session 13: MPC — Foundations

Encoding Functions with Constant Online Rate or How to Compress Garbled Circuits Keys . . . . .	166
<i>Benny Applebaum, Yuval Ishai, Eyal Kushilevitz, and Brent Waters</i>	
Efficient Multiparty Protocols via Log-Depth Threshold Formulae . . . . .	185
<i>Gil Cohen, Ivan Bjerre Damgård, Yuval Ishai, Jonas Kölker, Peter Bro Miltersen, Ran Raz, and Ron D. Rothblum</i>	
A Dynamic Tradeoff between Active and Passive Corruptions in Secure Multi-Party Computation . . . . .	203
<i>Martin Hirt, Ueli Maurer, and Christoph Lucas</i>	
What Information Is Leaked under Concurrent Composition? . . . . .	220
<i>Vipul Goyal, Divya Gupta, and Abhishek Jain</i>	

## Session 14: Codes and Secret Sharing

Non-malleable Codes from Two-Source Extractors . . . . .	239
<i>Stefan Dziembowski, Tomasz Kazana, and Maciej Obremski</i>	
Optimal Coding for Streaming Authentication and Interactive Communication . . . . .	258
<i>Matthew Franklin, Ran Gelles, Rafail Ostrovsky, and Leonard J. Schulman</i>	
Secret Sharing, Rank Inequalities and Information Inequalities . . . . .	277
<i>Sebastià Martín, Carles Padró, and An Yang</i>	

## Session 15: Signatures and Authentication

Linearly Homomorphic Structure-Preserving Signatures and Their Applications . . . . .	289
<i>Benoît Libert, Thomas Peters, Marc Joye, and Moti Yung</i>	
Man-in-the-Middle Secure Authentication Schemes from LPN and Weak PRFs . . . . .	308
<i>Vadim Lyubashevsky and Daniel Masny</i>	

## Session 16: Quantum Security

Achieving the Limits of the Noisy-Storage Model Using Entanglement Sampling . . . . .	326
<i>Frédéric Dupuis, Omar Fawzi, and Stephanie Wehner</i>	
Quantum One-Time Programs (Extended Abstract) . . . . .	344
<i>Anne Broadbent, Gus Gutoski, and Douglas Stebila</i>	

Secure Signatures and Chosen Ciphertext Security in a Quantum Computing World . . . . .	361
<i>Dan Boneh and Mark Zhandry</i>	

Everlasting Multi-party Computation . . . . .	380
<i>Dominique Unruh</i>	

## Session 17: New Primitives

Instantiating Random Oracles via UCEs . . . . .	398
<i>Mihir Bellare, Viet Tung Hoang, and Sriram Keelveedhi</i>	

Obfuscating Conjunctions . . . . .	416
<i>Zvika Brakerski and Guy N. Rothblum</i>	

## Session 18: Functional Encryption I

Fully, (Almost) Tightly Secure IBE and Dual System Groups . . . . .	435
<i>Jie Chen and Hoeteck Wee</i>	

Function-Private Identity-Based Encryption: Hiding the Function in Functional Encryption . . . . .	461
<i>Dan Boneh, Ananth Raghunathan, and Gil Segev</i>	

Attribute-Based Encryption for Circuits from Multilinear Maps . . . . .	479
<i>Sanjam Garg, Craig Gentry, Shai Halevi, Amit Sahai, and Brent Waters</i>	

## Session 19: Functional Encryption II

Functional Encryption: New Perspectives and Lower Bounds . . . . .	500
<i>Shweta Agrawal, Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee</i>	

On the Achievability of Simulation-Based Security for Functional Encryption . . . . .	519
<i>Angelo De Caro, Vincenzo Iovino, Abhishek Jain, Adam O'Neill, Omer Paneth, and Giuseppe Persiano</i>	

How to Run Turing Machines on Encrypted Data . . . . .	536
<i>Shafi Goldwasser, Yael Tauman Kalai, Raluca Ada Popa, Vinod Vaikuntanathan, and Nikolai Zeldovich</i>	

Author Index . . . . .	555
------------------------	-----

# Table of Contents – Part I

## Session 1: Lattices and FHE

Practical Bootstrapping in Quasilinear Time .....	1
<i>Jacob Alperin-Sheriff and Chris Peikert</i>	
Hardness of SIS and LWE with Small Parameters .....	21
<i>Daniele Micciancio and Chris Peikert</i>	
Lattice Signatures and Bimodal Gaussians .....	40
<i>Léo Ducas, Alain Durmus, Tancrede Lepoint, and Vadim Lyubashevsky</i>	
Learning with Rounding, Revisited: New Reduction, Properties and Applications.....	57
<i>Joël Alwen, Stephan Krenn, Krzysztof Pietrzak, and Daniel Wichs</i>	
Homomorphic Encryption from Learning with Errors: Conceptually- Simpler, Asymptotically-Faster, Attribute-Based .....	75
<i>Craig Gentry, Amit Sahai, and Brent Waters</i>	

## Invited Talk: Crypto Wars Part 2 Have Begun

## Session 2: Foundations of Hardness

A Uniform Min-Max Theorem with Applications in Cryptography.....	93
<i>Salil Vadhan and Colin Jia Zheng</i>	
Limits of Provable Security for Homomorphic Encryption .....	111
<i>Andrej Bogdanov and Chin Ho Lee</i>	

## Session 3: Cryptanalysis I

Counter-Cryptanalysis .....	129
<i>Marc Stevens</i>	
Fuming Acid and Cryptanalysis: Handy Tools for Overcoming a Digital Locking and Access Control System .....	147
<i>Daehyun Strobelt, Benedikt Driessen, Timo Kasper, Gregor Leander, David Oswald, Falk Schellenberg, and Christof Paar</i>	
Real Time Cryptanalysis of Bluetooth Encryption with Condition Masking (Extended Abstract) .....	165
<i>Bin Zhang, Chao Xu, and Dengguo Feng</i>	

## Session 4: Cryptanalysis II

Structural Evaluation of AES and Chosen-Key Distinguisher of 9-Round AES-128 .....	183
<i>Pierre-Alain Fouque, Jérémy Jean, and Thomas Peyrin</i>	
Bounds in Shallows and in Miseries.....	204
<i>Céline Blondeau, Andrey Bogdanov, and Gregor Leander</i>	
Sieve-in-the-Middle: Improved MITM Attacks .....	222
<i>Anne Canteaut, María Naya-Plasencia, and Bastien Vayssière</i>	
Construction of Differential Characteristics in ARX Designs Application to Skein .....	241
<i>Gaëtan Leurent</i>	

## Session 5: MPC – New Directions

On Fair Exchange, Fair Coins and Fair Sampling.....	259
<i>Shashank Agrawal and Manoj Prabhakaran</i>	
Limits on the Power of Cryptographic Cheap Talk .....	277
<i>Pavel Hubáček, Jesper Buus Nielsen, and Alon Rosen</i>	
Accuracy-Privacy Tradeoffs for Two-Party Differentially Private Protocols .....	298
<i>Vipul Goyal, Ilya Mironov, Omkant Pandey, and Amit Sahai</i>	

## Session 6: Leakage Resilience

Secure Computation against Adaptive Auxiliary Information .....	316
<i>Elette Boyle, Sanjam Garg, Abhishek Jain, Yael Tauman Kalai, and Amit Sahai</i>	
Leakage-Resilient Symmetric Cryptography under Empirically Verifiable Assumptions .....	335
<i>François-Xavier Standaert, Olivier Pereira, and Yu Yu</i>	

## Session 7: Symmetric Encryption and PRFs

Highly-Scalable Searchable Symmetric Encryption with Support for Boolean Queries .....	353
<i>David Cash, Stanislaw Jarecki, Charanjit Jutla, Hugo Krawczyk, Marcel-Cătălin Roşu, and Michael Steiner</i>	
Message-Locked Encryption for Lock-Dependent Messages .....	374
<i>Martín Abadi, Dan Boneh, Ilya Mironov, Ananth Raghunathan, and Gil Segev</i>	

The Mix-and-Cut Shuffle: Small-Domain Encryption Secure against $N$ Queries .....	392
<i>Thomas Ristenpart and Scott Yilek</i>	

Key Homomorphic PRFs and Their Applications.....	410
<i>Dan Boneh, Kevin Lewi, Hart Montgomery, and Ananth Raghunathan</i>	

## Session 8: Key Exchange

On the Security of the TLS Protocol: A Systematic Analysis .....	429
<i>Hugo Krawczyk, Kenneth G. Paterson, and Hoeteck Wee</i>	

New Techniques for SPHF's and Efficient One-Round PAKE Protocols .....	449
<i>Fabrice Benhamouda, Olivier Blazy, Céline Chevalier, David Pointcheval, and Damien Vergnaud</i>	

## Session 9: Multi Linear Maps

Practical Multilinear Maps over the Integers.....	476
<i>Jean-Sébastien Coron, Tancrede Lepoint, and Mehdi Tibouchi</i>	

Full Domain Hash from (Leveled) Multilinear Maps and Identity-Based Aggregate Signatures .....	494
<i>Susan Hohenberger, Amit Sahai, and Brent Waters</i>	

Programmable Hash Functions in the Multilinear Setting .....	513
<i>Eduarda S.V. Freire, Dennis Hofheinz, Kenneth G. Paterson, and Christoph Striecks</i>	

## Session 10: Ideal Ciphers

On the Indifferentiability of Key-Alternating Ciphers .....	531
<i>Elena Andreeva, Andrey Bogdanov, Yevgeniy Dodis, Bart Mennink, and John P. Steinberger</i>	

Plain versus Randomized Cascading-Based Key-Length Extension for Block Ciphers .....	551
<i>Peter Gaži</i>	

Digital Signatures with Minimal Overhead from Indifferentiable Random Invertible Functions .....	571
<i>Eike Kiltz, Krzysztof Pietrzak, and Mario Szegedy</i>	

Author Index .....	589
--------------------	-----