

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 Zurich, 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>

Marc Fischlin · Jean-Sébastien Coron (Eds.)

Advances in Cryptology – EUROCRYPT 2016

35th Annual International Conference
on the Theory and Applications of Cryptographic Techniques
Vienna, Austria, May 8–12, 2016
Proceedings, Part II

Editors

Marc Fischlin
Technische Universität Darmstadt
Darmstadt
Germany

Jean-Sébastien Coron
University of Luxembourg
Luxembourg
Luxembourg

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-662-49895-8 ISBN 978-3-662-49896-5 (eBook)
DOI 10.1007/978-3-662-49896-5

Library of Congress Control Number: 2016935585

LNCS Sublibrary: SL4 – Security and Cryptology

© International Association for Cryptologic Research 2016

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

This Springer imprint is published by Springer Nature
The registered company is Springer-Verlag GmbH Berlin Heidelberg

Preface

Eurocrypt 2016, the 35th annual International Conference on the Theory and Applications of Cryptographic Techniques, was held in Vienna, Austria, during May 8–12, 2016. The conference was sponsored by the International Association for Cryptologic Research (IACR). Krzysztof Pietrzak (IST Austria), together with Joël Alwen, Georg Fuchsbauer, Peter Gaži (all IST Austria), and Eike Kiltz (Ruhr-Universität Bochum), were responsible for the local organization. They were supported by a local organizing team consisting of Hamza Abusalah, Chethan Kamath, and Michal Rybár (all IST Austria). We are indebted to them for their support and smooth collaboration.

The conference program followed the now established parallel track system where the works of the authors were presented in two concurrently running tracks. As in the previous edition of Eurocrypt, one track was labeled \mathcal{R} (for real) and the other one was labeled \mathcal{I} (for ideal). Only the invited talks, the tutorial, the best paper, papers with honorable mentions, and the final session of the conference spanned over both tracks.

The proceedings of Eurocrypt contain 62 papers selected from 274 submissions, which corresponds to a record number of submissions in the history of Eurocrypt. Each submission was anonymized for the reviewing process and was assigned to at least three of the 55 Program Committee members. Submissions co-authored by committee members were assigned to at least four members. Committee members were allowed to submit at most one paper, or two if both were co-authored. The reviewing process included a first-round notification followed by a rebuttal for papers that made it to the second round. After extensive deliberations the Program Committee accepted 62 papers. The revised versions of these papers are included in these two-volume proceedings.

The committee decided to give the Best Paper Award to “Tightly Secure CCA-Secure Encryption Without Pairings” by Romain Gay, Dennis Hofheinz, Eike Kiltz, and Hoeteck Wee. The two runners-up to the award, “Indistinguishability Obfuscation from Constant-Degree Graded Encoding Schemes” by Huijia Lin and “Essentially Optimal Robust Secret Sharing with Maximal Corruptions” by Allison Bishop, Valerio Pastro, Rajmohan Rajaraman, Daniel Wichs, received honorable mentions. All three papers received invitations for the *Journal of Cryptology*.

The program also included invited talks by Karthikeyan Bhargavan, entitled “Protecting Transport Layer Security from Legacy Vulnerabilities”, Bart Preneel, entitled “The Future of Cryptography” (IACR distinguished lecture), and Christian Collberg, entitled “Engineering Code Obfuscation.” In addition, Emmanuel Prouff gave a tutorial about “Securing Cryptography Implementations in Embedded Systems.” All the speakers were so kind as to also provide a short abstract for the proceedings.

We would like to thank all the authors who submitted papers. We know that the Program Committee’s decisions, especially rejections of very good papers that did not find a slot among the sparse number of accepted papers, can be very disappointing. We sincerely hope that the rejected works eventually get the attention they deserve.

We are also indebted to the Program Committee members and all external reviewers for their voluntary work, especially since the newly established and unified page limits and the increasing number of submissions induce quite a workload. It has been an honor to work with everyone. The committee's work was tremendously simplified by Shai Halevi's submission software and his support, including running the service on IACR servers.

Finally, we thank everyone else—speakers, session chairs, and rump session chairs—for their contribution to the program of Eurocrypt 2016.

May 2016

Marc Fischlin
Jean-Sébastien Coron

Eurocrypt 2016

The 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques

Vienna, Austria
May 8–12, 2016

Track *I*

General Chair

Krzysztof Pietrzak IST Austria

Program Chairs

Marc Fischlin Technische Universität Darmstadt, Germany
Jean-Sébastien Coron University of Luxembourg, Luxembourg

Program Committee

Michel Abdalla Ecole Normale Supérieure and CNRS, France
Shweta Agrawal IIT Delhi, India
Elette Boyle IDC Herzliya, Israel
Christina Brzuska TU Hamburg-Harburg, Germany
Ran Canetti Tel Aviv University, Israel, and Boston University, USA
David Cash Rutgers University, USA
Dario Catalano University of Catania, Italy
Jean-Sébastien Coron University of Luxembourg, Luxembourg
Cas Cremers University of Oxford, UK
Yevgeniy Dodis New York University, USA
Nico Döttling Aarhus University, Denmark
Pooya Farshim Queen's University Belfast, UK
Jean-Charles Faugère Inria Paris-Rocquencourt, France
Sebastian Faust Ruhr University Bochum, Germany
Dario Fiore IMDEA Software Institute, Spain
Marc Fischlin TU Darmstadt, Germany
Georg Fuchsbauer IST, Austria
Juan A. Garay Yahoo Labs, USA
Vipul Goyal Microsoft Research, India
Tim Güneysu University of Bremen, Germany
Shai Halevi IBM, USA

Goichiro Hanaoka	AIST, Japan
Martin Hirt	ETH Zurich, Switzerland
Dennis Hofheinz	Karlsruhe KIT, Germany
Tibor Jager	Ruhr University Bochum, Germany
Abhishek Jain	Johns Hopkins University, USA
Aniket Kate	Purdue University, USA
Dmitry Khovratovich	University of Luxembourg, Luxembourg
Vadim Lyubashevsky	Ecole Normale Supérieure, France
Sarah Meiklejohn	University College London, UK
Mridul Nandi	Indian Statistical Institute, Kolkata, India
María Naya-Plasencia	Inria, France
Svetla Nikova	KU Leuven, Belgium
Adam O'Neill	Georgetown University, USA
Claudio Orlandi	Aarhus University, Denmark
Josef Pieprzyk	Queensland University of Technology, Australia
Mariana Raykova	Yale University, USA
Thomas Ristenpart	Cornell Tech, USA
Matthieu Rivain	CryptoExperts, France
Arnab Roy	Fujitsu Laboratories of America, USA
Benedikt Schmidt	IMDEA Software Institute, Spain
Thomas Schneider	TU Darmstadt, Germany
Berry Schoenmakers	TU Eindhoven, The Netherlands
Peter Schwabe	Radboud University, The Netherlands
Yannick Seurin	ANSSI, France
Thomas Shrimpton	University of Florida, USA
Nigel P. Smart	University of Bristol, UK
John P. Steinberger	Tsinghua University, China
Ron Steinfeld	Monash University, Australia
Emmanuel Thomé	Inria Nancy, France
Yosuke Todo	NTT, Japan
Dominique Unruh	University of Tartu, Estonia
Daniele Venturi	Sapienza University of Rome, Italy
Ivan Visconti	University of Salerno, Italy
Stefan Wolf	USI Lugano, Switzerland

External Reviewers

Divesh Aggarwal	Kazumaro Aoki	Subhadeep Banik
Shashank Agrawal	Afonso Arriaga	Harry Bartlett
Adi Akavia	Gilad Asharov	Lejla Batina
Martin Albrecht	Gilles Van Assche	Carsten Baum
Joël Alwen	Nuttapong Attrapadung	Aemin Baumeler
Prabhanjan Ananth	Christian Badertscher	Christof Beierle
Ewerton Rodrigues	Thomas Baignères	Sonia Belaïd
Andrade	Josep Balasch	Fabrice Benhamouda
Elena Andreeva	Foteini Baldimtsi	David Bernhard

Ritam Bhaumik	Daniel Demmler	Susan Hohenberger
Begül Bilgin	David Derler	Justin Holmgren
Nir Bitansky	Vasil Dimitrov	Pavel Hubacek
Matthieu Bloch	Yarkin Doroz	Tsung-Hsuan Hung
Andrey Bogdanov	Léo Ducas	Christopher Huth
Cecilia Boschini	François Dupressoir	Michael Hutter
Vitor Bosshard	Frederic Dupuis	Andreas Hülsing
Christina Boura	Avijit Dutta	Vincenzo Iovino
Florian Bourse	Stefan Dziembowski	Håkon Jacobsen
Cerys Bradley	Keita Emura	Aayush Jain
Zvika Brakerski	Antonio Faonio	Jérémy Jean
Anne Broadbent	Serge Fehr	Claude-Pierre Jeannerod
Dan Brown	Claus Fieker	Evan Jeffrey
Seyit Camtepe	Matthieu Finiasz	Ashwin Jha
Anne Canteaut	Viktor Fischer	Daniel Jost
Angelo De Caro	Jean-Pierre Flori	Charanjit Jutla
Avik Chakraborti	Pierre-Alain Fouque	Ali El Kaafarani
Nishanth Chandran	Tore Kasper Frederiksen	Liang Kaitai
Melissa Chase	Tommaso Gagliardini	Saqib A. Kakvi
Rahul Chatterjee	Steven Galbraith	Chethan Kamath
Yilei Chen	David Galindo	Bhavana Kanukurthi
Jung Hee Cheon	Chaya Ganesh	Pierre Karpman
Céline Chevalier	Luke Garratt	Elham Kashefi
Alessandro Chiesa	Romain Gay	Tomasz Kazana
Seung Geol Choi	Peter Gaži	Marcel Keller
Tom Chothia	Daniel Genkin	Dakshita Khurana
Arka Rai Choudhuri	Craig Gentry	Aggelos Kiayias
Kai-Min Chung	Hossein Ghodosi	Paul Kirchner
Yu-Chi Chen	Satrajit Ghosh	Elena Kirshanova
Michele Ciampi	Benedikt Gierlichs	Ágnes Kiss
Michael Clear	Kristian Gjøsteen	Fuyuki Kitagawa
Aloni Cohen	Aleksandr Golovnev	Ilya Kizhvatov
Ran Cohen	Alonso Gonzalez	Thorsten Kleinjung
Katriel Cohn-Gordon	Dov Gordon	Vlad Kolesnikov
Sandro Coretti	Louis Goubin	Venkata Koppala
Cas Cremers	Jens Groth	Luke Kowalczyk
Dana Dachman-Soled	Aurore Guillevic	Ranjit Kumaresan
Yuanxi Dai	Sylvain Guilley	Kaoru Kurosawa
Nilanjan Datta	Siyao Guo	Felipe Lacerda
Bernardo Machado David	Divya Gupta	Virginie Lallemand
Gareth T. Davies	Sourav Sen Gupta	Adeline Langlois
Ed Dawson	Helene Flyvholm Haagh	Enrique Larraia
Jean Paul Degabriele	Tzipora Halevi	Sebastian Lauer
Martin Dehnel-Wild	Michael Hamburg	Gregor Leander
Jeroen Delvaux	Carmit Hazay	Chin Ho Lee
Grégory Demay	Gottfried Herold	Tancrede Lepoint

Gaëtan Leurent	Mohammad Ali	Alessandra Scafuro
Benoît Libert	Orumiehchi	Christian Schaffner
Huijia (Rachel) Lin	Elisabeth Oswald	Tobias Schneider
Wei-Kai Lin	Ekin Ozman	Peter Scholl
Bin Liu	Jiaxin Pan	Jacob Schuldt
Dongxi Liu	Giorgos Panagiotakos	Gil Segev
Yunwen Liu	Omkant Pandey	Nicolas Sendrier
Steve Lu	Omer Paneth	Abhi Shelat
Atul Luykx	Dimitris Papadopoulos	Leonie Simpson
Bernardo Magri	Kostas Papagiannopoulos	Shashank Singh
Mohammad Mahmoody	Bryan Parno	Luisa Siniscalchi
Subhamoy Maitra	Valerio Pastro	Boris Skoric
Hemanta Maji	Chris Peikert	Ben Smith
Giulio Malavolta	Ludovic Perret	Juraj Somorovsky
Avradip Mandal	Leo Paul Perrin	John Steinberger
Daniel Masny	Christophe Petit	Noah
Takahiro Matsuda	Krzysztof Pietrzak	Stephens-Dawidovitz
Christian Matt	Benny Pinkas	Björn Tackmann
Willi Meier	Oxana Poburinnaya	Vanessa Teague
Sebastian Meiser	Bertram Poettering	Sidharth Telang
Florian Mendel	Joop van de Pol	R. Seth Terashima
Bart Mennink	Antigoni Polychroniadou	Stefano Tessaro
Eric Miles	Manoj Prabhakaran	Adrian Thillard
Kevin Milner	Thomas Prest	Susan Thomson
Ilya Mironov	Emmanuel Prouff	Mehdi Tibouchi
Arno Mittelbach	Jörn Müller-Quade	Jacques Traoré
Ameer Mohammad	Tal Rabin	Daniel Tschudi
Payman Mohassel	Kenneth Radke	Hoang Viet Tung
Hart Montgomery	Carla Rafols	Aleksei Udovenko
Amir Moradi	Mario Di Raimondo	Margarita Vald
François Morain	Samuel Ranellucci	Maria Isabel Gonzalez
Paweł Morawiecki	Pavel Raykov	Vasco
Pedro Moreno-Sanchez	Francesco Regazzoni	MeiLoF Veenigen
Nicky Mouha	Omer Reingold	Vesselin Velichkov
Pratyay Mukherjee	Michał Ren	Alexandre Venelli
Elke De Mulder	Guénaël Renault	Muthuramakrishnan
Anderson Nascimento	Oscar Reparaz	Venkatasubramaniam
Muhammad Naveed	Vincent Rijmen	Frederik Vercauteren
Phong Nguyen	Ben Riva	Marion Videau
Ivica Nikolic	Tim Ruffing	Vinod Vikuntanathan
Tobias Nilges	Ulrich Rührmair	Gilles Villard
Peter Sebastian Nordholt	Yusuke Sakai	Damian Vizar
Koji Nuida	Amin Sakzad	Emmanuel Volte
Maciej Obremski	Benno Salwey	Christine van Vredendaal
Frederique Elise Oggier	Kai Samelin	Niels de Vreede
Emmanuela Orsini	Yu Sasaki	Qingju Wang

Bogdan Warinschi
Hoeteck Wee
Carolyn Whitnall
Daniel Wichs
Alexander Wild
David Wu

Jürg Wullschleger
Masahiro Yagisawa
Shota Yamada
Kan Yasuda
Scott Yilek
Kazuki Yoneyama

Ching-Hua Yu
Samee Zahur
Mark Zhandry
Zongyang Zhang
Vassilis Zikas
Michael Zohner

Contents – Part II

Lattice-Based Schemes

Zero-Knowledge Arguments for Lattice-Based Accumulators: Logarithmic-Size Ring Signatures and Group Signatures Without Trapdoors	1
<i>Benoît Libert, San Ling, Khoa Nguyen, and Huaxiong Wang</i>	
Adaptively Secure Identity-Based Encryption from Lattices with Asymptotically Shorter Public Parameters	32
<i>Shota Yamada</i>	

Zero-Knowledge I

Online/Offline OR Composition of Sigma Protocols	63
<i>Michele Ciampi, Giuseppe Persiano, Alessandra Scafuro, Luisa Siniscalchi, and Ivan Visconti</i>	
Constant-Round Leakage-Resilient Zero-Knowledge from Collision Resistance.	93
<i>Susumu Kiyoshima</i>	

Pseudorandom Functions

Constrained Pseudorandom Functions for Unconstrained Inputs	124
<i>Apoorva Deshpande, Venkata Koppula, and Brent Waters</i>	
Pseudorandom Functions in Almost Constant Depth from Low-Noise LPN. . .	154
<i>Yu Yu and John Steinberger</i>	

Multi-Party Computation I

Secure Computation from Elastic Noisy Channels	184
<i>Dakshita Khurana, Hemanta K. Maji, and Amit Sahai</i>	
All Complete Functionalities are Reversible	213
<i>Dakshita Khurana, Daniel Kraschewski, Hemanta K. Maji, Manoj Prabhakaran, and Amit Sahai</i>	

Separations

On the Power of Hierarchical Identity-Based Encryption 243
Mohammad Mahmoody and Ameer Mohammed

On the Impossibility of Tight Cryptographic Reductions 273
Christoph Bader, Tibor Jager, Yong Li, and Sven Schäge

Zero-Knowledge II

On the Size of Pairing-Based Non-interactive Arguments 305
Jens Groth

Efficient Zero-Knowledge Arguments for Arithmetic Circuits in the
Discrete Log Setting 327
*Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, Jens Groth,
and Christophe Petit*

Protocols

On the Complexity of Script and Proofs of Space in the Parallel Random
Oracle Model 358
*Joël Alwen, Binyi Chen, Chethan Kamath, Vladimir Kolmogorov,
Krzysztof Pietrzak, and Stefano Tessaro*

Anonymous Traitor Tracing: How to Embed Arbitrary Information
in a Key 388
Ryo Nishimaki, Daniel Wichs, and Mark Zhandry

Round Complexity

Unconditionally Secure Computation with Reduced Interaction 420
Ivan Damgård, Jesper Buus Nielsen, Rafail Ostrovsky, and Adi Rosén

The Exact Round Complexity of Secure Computation 448
*Sanjam Garg, Pratyay Mukherjee, Omkant Pandey,
and Antigoni Polychroniadou*

Commitments

On the Composition of Two-Prover Commitments, and Applications
to Multi-round Relativistic Commitments 477
Serge Fehr and Max Fillinger

Computationally Binding Quantum Commitments 497
Dominique Unruh

Lattices

Structural Lattice Reduction: Generalized Worst-Case to Average-Case Reductions and Homomorphic Cryptosystems. 528
Nicolas Gama, Malika Izabachène, Phong Q. Nguyen, and Xiang Xie

Recovering Short Generators of Principal Ideals in Cyclotomic Rings 559
Ronald Cramer, Léo Ducas, Chris Peikert, and Oded Regev

Leakage

Circuit Compilers with $O(1/\log(n))$ Leakage Rate 586
Marcin Andrychowicz, Stefan Dziembowski, and Sebastian Faust

Randomness Complexity of Private Circuits for Multiplication 616
Sonia Belaïd, Fabrice Benhamouda, Alain Passelègue, Emmanuel Prouff, Adrian Thillard, and Damien Vergnaud

Indifferentiability

10-Round Feistel is Indifferentiable from an Ideal Cipher. 649
Dana Dachman-Soled, Jonathan Katz, and Aishwarya Thiruvengadam

Indifferentiability of Confusion-Diffusion Networks. 679
Yevgeniy Dodis, Martijn Stam, John Steinberger, and Tianren Liu

Multi-Party Computation II

Fair and Robust Multi-party Computation Using a Global Transaction Ledger 705
Aggelos Kiayias, Hong-Sheng Zhou, and Vassilis Zikas

Two Round Multiparty Computation via Multi-key FHE 735
Pratyay Mukherjee and Daniel Wichs

Obfuscation

Post-zeroizing Obfuscation: New Mathematical Tools, and the Case of Evasive Circuits 764
Saikrishna Badrinarayanan, Eric Miles, Amit Sahai, and Mark Zhandry

New Negative Results on Differing-Inputs Obfuscation 792
Mihir Bellare, Igors Stepanovs, and Brent Waters

Automated Analysis, Functional Encryption, and Non-malleable Codes

Automated Unbounded Analysis of Cryptographic Constructions
in the Generic Group Model. 822
Miguel Ambrona, Gilles Barthe, and Benedikt Schmidt

Multi-input Functional Encryption in the Private-Key Setting: Stronger
Security from Weaker Assumptions. 852
Zvika Brakerski, Ilan Komargodski, and Gil Segev

Non-malleable Codes for Bounded Depth, Bounded Fan-In Circuits 881
Marshall Ball, Dana Dachman-Soled, Mukul Kulkarni, and Tal Malkin

Author Index 909

Contents – Part I

Best Paper and Honorable Mentions

Tightly CCA-Secure Encryption Without Pairings	1
<i>Romain Gay, Dennis Hofheinz, Eike Kiltz, and Hoeteck Wee</i>	
Indistinguishability Obfuscation from Constant-Degree Graded Encoding Schemes	28
<i>Huijia Lin</i>	
Essentially Optimal Robust Secret Sharing with Maximal Corruptions	58
<i>Allison Bishop, Valerio Pastro, Rajmohan Rajaraman, and Daniel Wichs</i>	

(Pseudo) Randomness

Provably Robust Sponge-Based PRNGs and KDFs	87
<i>Peter Gaži and Stefano Tessaro</i>	
Reusable Fuzzy Extractors for Low-Entropy Distributions	117
<i>Ran Canetti, Benjamin Fuller, Omer Paneth, Leonid Reyzin, and Adam Smith</i>	

LPN/LWE

Provably Weak Instances of Ring-LWE Revisited	147
<i>Wouter Castryck, Ilia Iliashenko, and Frederik Vercauteren</i>	
Faster Algorithms for Solving LPN	168
<i>Bin Zhang, Lin Jiao, and Mingsheng Wang</i>	

Cryptanalysis I

Provable Security Evaluation of Structures Against Impossible Differential and Zero Correlation Linear Cryptanalysis.	196
<i>Bing Sun, Meicheng Liu, Jian Guo, Vincent Rijmen, and Ruilin Li</i>	
Polytopical Cryptanalysis	214
<i>Tyge Tiessen</i>	

Masking

From Improved Leakage Detection to the Detection of Points of Interests
in Leakage Traces 240
François Durvaux and François-Xavier Standaert

Improved Masking for Tweakable Blockciphers with Applications
to Authenticated Encryption 263
Robert Granger, Philipp Jovanovic, Bart Mennink, and Samuel Neves

Fully Homomorphic Encryption

Sanitization of FHE Ciphertexts 294
Léo Ducas and Damien Stehlé

Towards Stream Ciphers for Efficient FHE with Low-Noise Ciphertexts 311
*Pierrick Méaux, Anthony Journault, François-Xavier Standaert,
and Claude Carlet*

Cryptanalysis II

Improved Differential-Linear Cryptanalysis of 7-Round Chaskey
with Partitioning 344
Gaëtan Leurent

Reverse-Engineering the S-Box of Streebog, Kuznyechik and STRIBOBr1 . . . 372
Alex Biryukov, Léo Perrin, and Aleksei Udovenko

Number Theory

Complete Addition Formulas for Prime Order Elliptic Curves. 403
Joost Renes, Craig Costello, and Lejla Batina

New Complexity Trade-Offs for the (Multiple) Number Field
Sieve Algorithm in Non-Prime Fields 429
Palash Sarkar and Shashank Singh

Hash Functions

Freestart Collision for Full SHA-1. 459
Marc Stevens, Pierre Karpman, and Thomas Peyrin

New Attacks on the Concatenation and XOR Hash Combiners 484
Itai Dinur

Multilinear Maps

Cryptanalysis of the New CLT Multilinear Map over the Integers. 509
*Jung Hee Cheon, Pierre-Alain Fouque, Changmin Lee, Brice Minaud,
and Hansol Ryu*

Cryptanalysis of GGH Map 537
Yupu Hu and Huiwen Jia

Message Authentication Codes

Hash-Function Based PRFs: AMAC and Its Multi-User Security. 566
Mihir Bellare, Daniel J. Bernstein, and Stefano Tessaro

On the Influence of Message Length in PMAC’s Security Bounds 596
Atul Luykx, Bart Preneel, Alan Szepieniec, and Kan Yasuda

Attacks on SSL/TLS

Lucky Microseconds: A Timing Attack on Amazon’s *s2n* Implementation
of TLS 622
Martin R. Albrecht and Kenneth G. Paterson

An Analysis of OpenSSL’s Random Number Generator. 644
Falko Strenzke

Real-World Protocols

Safely Exporting Keys from Secure Channels: On the Security
of EAP-TLS and TLS Key Exporters. 670
Christina Brzuska, Håkon Jacobsen, and Douglas Stebila

Valiant’s Universal Circuit is Practical. 699
Ágnes Kiss and Thomas Schneider

Robust Designs

Nonce-Based Cryptography: Retaining Security When Randomness Fails. . . . 729
Mihir Bellare and Björn Tackmann

Honey Encryption Beyond Message Recovery Security 758
Joseph Jaeger, Thomas Ristenpart, and Qiang Tang

Lattice Reduction

Improved Progressive BKZ Algorithms and Their Precise Cost Estimation
by Sharp Simulator 789
Yoshinori Aono, Yuntao Wang, Takuya Hayashi, and Tsuyoshi Takagi

Practical, Predictable Lattice Basis Reduction 820
Daniele Micciancio and Michael Walter

Author Index 851