Lecture Notes in Computer Science 10401

More information about this series at http://www.springer.com/series/7410

Jonathan Katz · Hovav Shacham (Eds.)

Advances in Cryptology – CRYPTO 2017

37th Annual International Cryptology Conference Santa Barbara, CA, USA, August 20–24, 2017 Proceedings, Part I

Springer

Editors
Jonathan Katz
University of Maryland
College Park, MD
USA

Hovav Shacham
UC San Diego
La Jolla, CA
USA

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-63687-0 ISBN 978-3-319-63688-7 (eBook)
DOI 10.1007/978-3-319-63688-7

Library of Congress Control Number: 2017947035

LNCS Sublibrary: SL4 – Security and Cryptology

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

The 37th International Cryptology Conference (Crypto 2017) was held at the University of California, Santa Barbara, USA, during August 20–24, 2017, sponsored by the International Association for Cryptologic Research.

There were 311 submissions to Crypto 2017, a substantial increase from previous years. The Program Committee, aided by nearly 350 external reviewers, selected 72 papers to appear in the program. We are indebted to all the reviewers for their service. Their reviews and discussions, if printed out, would consume about a thousand pages.

Two papers—"Identity-Based Encryption from the Diffie-Hellman Assumption," by Nico Döttling and Sanjam Garg, and "The first Collision for Full SHA-1," by Marc Stevens, Elie Bursztein, Pierre Karpman, Ange Albertini, and Yarik Markov—were honored as best papers. A third paper—"Watermarking Cryptographic Functionalities from Standard Lattice Assumptions," by Sam Kim and David J. Wu—was honored as best paper authored exclusively by young researchers.

Crypto was the venue for the 2017 IACR Distinguished Lecture, delivered by Shafi Goldwasser. Crypto also shared an invited speaker, Cédric Fournet, with the 30th IEEE Computer Security Foundations Symposium (CSF 2017), which was held jointly with Crypto.

We are grateful to Steven Myers, the Crypto general chair; to Shai Halevi, author of the IACR Web Submission and Review system; to Alfred Hofmann, Anna Kramer, and their colleagues at Springer; to Sally Vito of UCSB Conference Services; and, of course, everyone who submitted a paper to Crypto and everyone who attended the conference.

August 2017

Jonathan Katz
Hovav Shacham

Crypto 2017

The 37th IACR International Cryptology Conference

University of California, Santa Barbara, CA, USA
August 20–24, 2017

Sponsored by the *International Association for Cryptologic Research*

General Chair

Steven Myers	Indiana University, USA

Program Chairs

Jonathan Katz	University of Maryland, USA
Hovav Shacham	UC San Diego, USA

Program Committee

Masayuki Abe	NTT Secure Platform Laboratories, Japan
Shweta Agrawal	IIT Madras, India
Adi Akavia	The Academic College of Tel Aviv-Yaffo, Israel
Elena Andreeva	KU Leuven, Belgium
Mihir Bellare	UC San Diego, USA
Dan Boneh	Stanford University, USA
Elette Boyle	IDC Herzliya, Israel
Ran Canetti	Boston University, USA, and Tel Aviv University, Israel
Jung Hee Cheon	Seoul National University, Korea
Dana Dachman-Soled	University of Maryland, USA
Ivan Damgård	Aarhus University, Denmark
Nico Döttling	UC Berkeley, USA
Orr Dunkelman	University of Haifa, Israel
Eiichiro Fujisaki	NTT Secure Platform Laboratories, Japan
Sergey Gorbunov	University of Waterloo, Canada
Vipul Goyal	Carnegie Mellon University, USA
Matthew Green	Johns Hopkins University, USA
Nadia Heninger	University of Pennsylvania, USA
Viet Tung Hoang	Florida State University, USA
Dennis Hofheinz	Karlsruhe Institute of Technology, Germany
Sorina Ionica	Université de Picardie, France

Tetsu Iwata	Nagoya University, Japan
Seny Kamara	Brown University, USA
Gaëtan Leurent	Inria, France
Rachel Lin	UC Santa Barbara, USA
Stefan Lucks	Bauhaus-Universität Weimar, Germany
Vadim Lyubashevsky	IBM Zurich, Switzerland
Mohammad Mahmoody	University of Virginia, USA
Payman Mohassel	Visa Research, USA
Claudio Orlandi	Aarhus University, Denmark
Elisabeth Oswald	University of Bristol, UK
Rafael Pass	Cornell University, USA
Gregory G. Rose	TargetProof LLC, USA
Christian Schaffner	University of Amsterdam and CWI and QuSoft, The Netherlands
Gil Segev	Hebrew University, Israel
Yannick Seurin	ANSSI, France
Douglas Stebila	McMaster University, Canada
Stefano Tessaro	UC Santa Barbara, USA
Mehdi Tibouchi	NTT Secure Platform Laboratories, Japan
Eran Tromer	Tel Aviv University, Israel, and Columbia University, USA
Dominique Unruh	University of Tartu, Estonia
Vassilis Zikas	Rensselaer Polytechnic Institute, USA

Additional Reviewers

Aysajan Abidin
Shashank Agrawal
Thomas Agrikola
Ali Akhavi
Gorjan Alagic
Martin Albrecht
Jacob Alperin-Sheriff
Joel Alwen
Joran van Apeldoorn
Daniel Apon
Gilad Asharov
Tomer Ashur
Nuttapong Attrapadung
Christian Badertscher
Saikrishna Badrinarayanan
Shi Bai
Foteini Baldimtsi
Marshall Ball
Achiya Bar-On
Razvan Barbulescu
Guy Barwell
Carsten Baum
Amin Baumeler
Fabrice Benhamouda
Daniel J. Bernstein
Jean-François Biasse
Alex Biryukov
Nir Bitansky
Olivier Blazy
Jeremiah Blocki
Andrej Bogdanov
Xavier Bonnetain
Charlotte Bonte
Carl Bootland
Christina Boura
Zvika Brakerski
Brandon Broadnax
Leon Groot Bruinderink
Benedikt Bunz
Anne Canteaut
Angelo de Caro
Ignacio Cascudo
David Cash
Wouter Castryck
Nishanth Chandran
Eshan Chattopadhyay
Binyi Chen
Jie Chen
Yilei Chen
Alessandro Chiesa
Chongwon Cho
Arka Rai Chouduhri
Heewon Chung
Kai-Min Chung
Benoit Cogliati
Aloni Cohen

Ran Cohen
Katriel Cohn-Gordon
Henry Corrigan-Gibbs
Geoffroy Couteau
Alain Couvreur
Cas Cremers
Jan Czajkowski
Wei Dai
Bernardo David
Jean Paul Degabriele
Jeroen Delvaux
Apoorvaa Deshpande
Bogdan Adrian Dina
Itai Dinur
Yevgeniy Dodis
Benjamin Dowling
Rafael Dowsley
Leo Ducas
Yfke Dulek
Tuyet Duong
Tuyet Thi Anh Duong
Fred Dupuis
Frédéric Dupuis
Alfredo Rial Duran
Sébastien Duval
Aner Moshe Ben Efraim
Maria Eichlseder
Keita Emura
Naomi Ephraim
Saba Eskandarian
Thomas Espitau
Oriol Farràs
Pooya Farshim
Sebastian Faust
Prastudy Fauzi
Nelly Fazio
Serge Fehr
Houda Ferradi
Manuel Fersch
Dario Fiore
Ben Fisch
Joseph Fitzsimons
Nils Fleischhacker
Tore Frederiksen
Rotem Arnon Friedman
Georg Fuchsbauer
Marc Fyrbiak
Tommaso Gagliardoni
Nicolas Gama
Juan Garay
Sanjam Garg
Christina Garman
Romain Gay
Peter Gazi
Alexandre Gelin
Daniel Genkin
Marios Georgiou
Benoit Gerard
Essam Ghadafi
Niv Gilboa
Dov Gordon
Rishab Goyal
Vincent Grosso
Jens Groth
Paul Grubbs
Siyao Guo
Helene Haag
Helene Haagh
Kyoohyung Han
Marcella Hastings
Carmit Hazay
Ethan Heilman
Brett Hemenway
Minki Hhan
Justin Holmgren
Akinori Hosoyamada
Yan Huang
Pavel Hubacek
Ilia Iliashenko
Vincenzo Iovino
Yuval Ishai
Joseph Jaeger
Zahra Jafragholi
Tibor Jager
Aayush Jain
Abhishek Jain
Chethan Kamath
Bhavana Kanukurthi
Angshuman Karmakar
Pierre Karpman
Stefan Katzenbeisser
Xagawa Keita
Marcel Keller
Nathan Keller
Iordanis Kerenidis
Dakshita Khurana
Andrey Kim
Dongwoo Kim
Duhyeong Kim
Eunkyung Kim
Jae-yun Kim
Jihye Kim
Jinsu Kim
Jiseung Kim
Sam Kim
Taechan Kim
Fuyuki Kitagawa
Susumu Kiyoshima
Dima Kogan
Vlad Kolesnikov
Ilan Komargodski
Venkata Koppula
Venkata Kopulla
Evgenios Kornaropoulos
Juliane Kraemer
Mukul Kulkarni
Ashutosh Kumar
Ranjit Kumaresan
Alptekin Küpçü
Lakshmi Kuppusamy
Thijs Laarhoven
Changmin Lee
Joohee Lee
Younho Lee
Nikos Leonardos
Tancrède Lepoint
Baiyu Li
Benoit Libert
Eik List
Yi-Kai Liu
Steve Lu
Yun Lu
Atul Luykx
Saeed Mahloujifar
Giulio Malavolta
Alex Malozemoff
Antonio Marcedone
Daniel P. Martin

Marco Martinoli
Daniel Masny
Takahiro Matsuda
Florian Mendel
Bart Mennink
Peihan Miao
Daniele Micciancio
Gabrielle De Micheli
Ian Miers
Andrew Miller
Kazuhiko Minematsu
Tarik Moataz
Ameer Mohammed
Hart Montgomery
Andrew Morgan
Nicky Mouha
Pratyay Mukherjee
Muhammad Naveed
María Naya-Plasencia
Kartik Nayak
Gregory Neven
Ruth Ng
Michael Nielsen
Tobias Nilges
Ryo Nishimaki
Ariel Nof
Kaisa Nyberg
Adam O'Neill
Maciej Obremski
Sabine Oechsner
Miyako Ohkubo
Rafail Ostrovsky
Daniel Page
Jiaxin Pan
Omer Paneth
Dimitris Papadopoulos
Sunno Park
Anat Paskin-Cherniavsky
Kenny Paterson
Arpita Patra
Filip Pawlega
Chris Peikert
Josef Pieprzyk
Cécile Pierrot
Krzysztof Pietrzak
Benny Pinkas
Rafael del Pino
Oxana Poburinnaya
David Pointcheval
Antigoni Polychroniadou
Raluca Ada Popa
Bart Preneel
Thomas Prest
Emmanuel Prouff
Carla Rafols
Srinivasan Raghuraman
Samuel Ranellucci
Mariana Raykova
Oded Regev
Ling Ren
Oscar Reparaz
Leo Reyzin
Silas Richelson
Matt Robshaw
Mike Rosulek
Yann Rotella
Lior Rotem
Ron Rothblum
Arnab Roy
Sujoy Sinha Roy
Olivier Ruatta
Ulrich Rührmair
Yusuke Sakai
Olivier Sanders
Yu Sasaki
Sajin Sasy
Alessandra Scafuro
Patrick Schaumont
Thomas Schneider
Peter Scholl
Gregor Seiler
Ido Shahaf
abhi shelat
Timothy Sherwood
Kyoji Shibutani
Sina Shiehian
Mark Simkin
Leonie Simpson
Maciej Skorski
Nigel Smart
Yongha Son
Fang Song
Yongsoo Song
Pratik Soni
Florian Speelman
Akshayaram Srinivasan
Martijn Stam
François-Xavier Standaert
John Steinberger
Igors Stepanovs
Noah Stephens-Davidowitz
Valentin Suder
Koutarou Suzuki
Björn Tackmann
Alain Tapp
Isamu Teranishi
Benjamin Terner
Aishwarya Thiruvengadam
Sri Aravinda Krishnan Thyagarajan
Yosuke Todo
Junichi Tomida
Luca Trevisan
Roberto Trifiletti
Daniel Tschudi
Nik Unger
Salil Vadhan
Margarita Vald
Luke Valenta
Kerem Varici
Srinivas Vivek Venkatesh
Muthuramakrishnan
Venkitasubramaniam
Daniele Venturi
Damien Vergnaud
Jorge Villar
Dhinakaran Vinayagamurthy
Ivan Visconti
Damian Vizar
Christine van Vreedendal
Michael Walter
Mingyuan Wang
Xiao Wang
Yuyu Wang
Yohei Watanabe

Hoeteck Wee
Avi Weinstock
Mor Weiss
Jakob Wenzel
Daniel Wichs
David Wu
Keita Xagawa
Sophia Yakoubov
Avishay Yanay
Kan Yasuda
Donggeon Yhee
Chen Yilei
Eylon Yogev
Kazuki Yoneyama
Lanqing Yu
Thomas Zacharias
Samee Zahur
Greg Zaverucha
Mark Zhandry
Ren Zhang
Yupeng Zhang
Hong-Sheng Zhou

Platinum Sponsor

NSF

Silver Sponsors

moz://a

FUJITSU

Western Digital®

Contents – Part I

Functional Encryption

Foundations I

Two-Party Computation

Bitcoin

Multiparty Computation

Award Papers

Obfuscation I

Conditional Disclosure of Secrets