

Yevgeniy Dodis
Thomas Shrimpton (Eds.)

LNCS 13510

Advances in Cryptology – CRYPTO 2022

42nd Annual International Cryptology Conference, CRYPTO 2022
Santa Barbara, CA, USA, August 15–18, 2022
Proceedings, Part IV

4
Part IV



 Springer

Founding Editors

Gerhard Goos

Karlsruhe Institute of Technology, Karlsruhe, Germany

Juris Hartmanis

Cornell University, Ithaca, NY, USA


Editorial Board Members

Elisa Bertino

Purdue University, West Lafayette, IN, USA

Wen Gao

Peking University, Beijing, China

Bernhard Steffen 

TU Dortmund University, Dortmund, Germany

Moti Yung 

Columbia University, New York, NY, USA

More information about this series at <https://link.springer.com/bookseries/558>

Yevgeniy Dodis · Thomas Shrimpton (Eds.)

Advances in Cryptology – CRYPTO 2022

42nd Annual International Cryptology Conference, CRYPTO 2022
Santa Barbara, CA, USA, August 15–18, 2022
Proceedings, Part IV

Editors

Yevgeniy Dodis
New York University
New York, NY, USA

Thomas Shrimpton
University of Florida
Gainesville, FL, USA

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-031-15984-8

ISBN 978-3-031-15985-5 (eBook)

<https://doi.org/10.1007/978-3-031-15985-5>

© International Association for Cryptologic Research 2022

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, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

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

Preface

The 42nd International Cryptology Conference (CRYPTO 2022) was held at the University of California, Santa Barbara, California, USA, during August 15–18, 2022. The conference had a hybrid format, with some presentations made in person, and some delivered virtually. CRYPTO 2022 was sponsored by the International Association for Cryptologic Research (IACR). The conference was preceded by two days of workshops on various topics.

The conference set new records for both submissions and publications: 455 papers were submitted, and 100 were accepted. Two papers were merged into a single joint paper. Three pairs of papers were soft-merged, meaning that they were written separately, but only one paper in each pair was given a presentation slot at the conference. This resulted in 96 presentations, a record by some margin for a non-virtual edition of Crypto. It took a Program Committee of 72 cryptography experts working with 435 external reviewers almost three months to select the accepted papers. We Chairs extend our heartfelt gratitude for the effort and professionalism displayed by the Program Committee; it was our pleasure to be your Chairs.

We experimented with some new policies and mechanisms this year. The most important had to do with the quality of reviewing, author feedback and interaction with the authors.

Shortly after the standard doubly-blind reviewing stage, we assigned a unique discussion leader (DL) to every paper. The DL’s job was to make sure the paper received a thorough and fair treatment, and to moderate interactive communication between the reviewers and authors (described below). The DL also prepared a “Reviewers’ consensus summary”, which provided the authors with a concise summary of the discussion, the decision, and overall trajectory of the paper throughout the process. Many authors expressed gratitude for receiving the Reviewers’ consensus summary, in addition to the usual reviews and scores. Overall, feedback on our DL experiment was quite positive, and we recommend it to future chairs to adopt this process as well.

We also experimented with an “interactive rebuttal” process. Traditionally, the rebuttal process has consisted of a single round: the authors were provided with the initial reviews, and had one opportunity to respond prior to the final decision. While better than no opportunity to rebut, our opinion is that the traditional process suffers from several important flaws. First, the authors were left to respond in (say) 750 words to multiple reviews that are, each, much longer. Too often, the authors are left to divine what are the *crucial* points to address; getting this wrong can lead to reviewers feeling that the rebuttal has missed (or dismissed) what mattered to them. In any case, the authors had no idea if their rebuttal was correctly focused, let alone convincing, until the decisions and final reviews were released. In many instances, the final reviews gave no signal that the rebuttal had been thoughtfully considered. In our view, and personal experience, the traditional rebuttal process led to frustration on both sides, with reviewers and authors feeling that their time had been wasted. Moreover, it had unclear benefits in terms of helping the PC to pick the best possible program.

To address this, we created a review form that required reviewers to make explicit what were their core concerns and criticisms; and we allowed for multiple, DL-moderated, rounds of communication between the reviewers and the authors.

Our review form had *exactly one* field visible to the authors during the initial rebuttal round. The field was called “Question/Clarifications for Authors”, and reviewers were instructed to include *only* those things that had significant bearing upon the reviewer’s accept/reject stance. We gave all reviewers detailed guidance on things that *must* be included. For example, any claimed errors, crucial prior work that was not cited, or other objective weaknesses that appeared in the detailed review comments. In addition, the reviewers were instructed to clearly state less objective concerns that factored into their initial score and disposition towards the paper. Thus, the authors should know exactly what to focus upon in their response. While not perfect, the new rebuttal format was a resounding success. Very strong/weak papers typically had very short rebuttals, allowing the PC to focus their time and energy on papers in need of extensive discussion or additional reviews.

In concert with the new review form and detailed review instructions, we also implemented *interactive discussions* between the reviewers and authors. The traditional rebuttal round became the first round of the interactive discussion. One round was enough for a fraction of the papers (primarily papers that were very strong or very weak), but the evaluation of most submissions benefited from numerous rounds: reviewers were able to sharpen their questions, authors were able to address points directly and in greater detail. The whole review process shifted more towards a collegial technical exchange. We did not encounter any problems that we initially feared, e.g., authors spamming the PC with comment. We believe that having the DLs moderate these interactions was important for keeping emotions and egos in check, and for encouraging reviewers to share any significant new concerns with the authors.

A few minor hiccups notwithstanding, the focused review forms and the “interactive rebuttal” mechanism received a lot of positive feedback, and we strongly encourage future chairs to adopt this tradition.

We also mention several smaller details which worked well. First, our review form included a “Brief Score Justification” field that remained reviewer-visible (only) for the entire process. This was a space for reviewers to speak freely, but concisely, about how they came to their scores. As Chairs, we found this extremely useful for getting a quick view of each paper’s reviews. Second, we had an early rejection round roughly in the middle of our reviewing process. This allowed us to reject roughly half of submissions, i.e., those that clearly had no chance of being accepted to the final program. The process generally worked, and we tried to err on the side of caution, keeping papers alive if the PC was unsure of their seemingly negative views. For example, we allowed PC members to tag papers that they wanted to keep alive, even to the point of overturning a preliminary decision to early reject. However, we did feel slightly rushed in finalizing the early reject decisions, as we made them after less than two weeks after the initial reviewing round, and less than a week after the initial rebuttal round. Part of this rush was due to late reviews. Thus, we recommend that future chairs give themselves a bit more slack in the schedule, and perhaps add a second (less) early rejection round. Third, we experimented with allowing PC members to have a variable number of submissions,

rather than the usual hard limits (e.g., at most one or two). Concretely, at most 4 papers could be submitted; the first paper was “free”, but every subsequent paper submitted by the PC member resulted in this PC member getting roughly three more papers to review, and one additional DL appointment. We adopted this policy to make it easier for experts to accept our invitation to join the PC. (As always, the chairs were not allowed to submit papers.) Despite some unexpected difficulties and complaints about this system, most having to do with the logistic difficulty of assigning DLs to PC members with late initial reviews, many PC members told us that they appreciated the flexibility to submit more papers, especially when students were involved. We found no evidence that our system resulted in more accepted papers that were co-authored by the PC members, or any other biases and irregularities. Hence, we found it to be positive, overall.

The Program Committee recognized three papers and their authors for particularly outstanding work

- “Batch Arguments for NP and More from Standard Bilinear Group Assumptions,” by Brent Waters and David Wu
- “Breaking Rainbow Takes a Weekend on a Laptop”, by Ward Beullens
- “Some Easy Instances of Ideal-SVP and Implications to the Partial Vandermonde Knapsack Problem”, by Katharina Boudgoust, Erell Gachon, and Alice Pellet-Mary

We were very pleased to have Yehuda Lindell as the Invited Speaker at CRYPTO 2022, who spoke about “The MPC journey from theoretical foundations to commercial success: a story of science and business”.

We would like to express our sincere gratitude to all the reviewers for volunteering their time and knowledge in order to select a great program for 2022. Additionally, we are grateful to the following people for helping to make CRYPTO 2022 a success: Allison Bishop (General Chair, CRYPTO 2022), Kevin McCurley and Kay McKelly (IACR IT experts), Carmit Hazay (Workshops Chair), and Whitney Morris and her staff at UCSB conference services.

We would also like to thank the generous sponsors, all of the authors of the submissions, the rump session chair, the regular session chairs, and the speakers.

August 2022

Yevgeniy Dodis
Thomas Shrimpton

Nadia Heninger	University of California San Diego, USA
Viet Hoang	Florida State University, USA
Susan Hohenberger	Johns Hopkins University, USA
Joseph Jaeger	Georgia Tech, USA
Tibor Jager	Bergische Universität Wuppertal, Germany
Daniel Jost	New York University, USA
Seny Kamara	Brown University, USA
Aggelos Kiayias	University of Edinburgh and IOHK, UK
Markulf Kohlweiss	University of Edinburgh, UK
Vladimir Kolesnikov	Georgia Tech, USA
Gregor Leander	University Bochum, Germany
Benoît Libert	CNRS and ENS Lyon, France
Feng-Hao Liu	Florida Atlantic University, USA
Anna Lysyanskaya	Brown University, USA
Vadim Lyubashevsky	IBM Research Europe Zurich, Switzerland
Fermi Ma	Simons Institute and UC Berkeley, USA
Bernardo Magri	The University of Manchester, UK
Mohammad Mahmoody	University of Virginia, USA
Hemanta Maji	Purdue University, USA
Alex Malozemoff	Galois Inc., USA
Antonio Marcedone	Zoom, USA
Bart Mennink	Radboud University, Netherlands
Daniele Micciancio	University of California San Diego, USA
Kazuhiko Minematsu	NEC and Yokohama National University, Japan
María Naya-Plasencia	Inria, France
Ryo Nishimaki	NTT Corporation, Japan
Rafael Pass	Cornell Tech, USA
Thomas Peyrin	Nanyang Technological University, Singapore
Antigoni Polychroniadou	J.P. Morgan AI Research, USA
Mariana Raykova	Google, USA
Christian Rechberger	TU Graz, Austria
Leonid Reyzin	Boston University, USA
Lior Rotem	Hebrew University, Israel
Paul Rösler	New York University, USA
Alessandra Scafuro	North Carolina State University, USA
Christian Schaffner	University of Amsterdam and QuSoft, Netherlands
Mark Simkin	Ethereum Foundation, USA
Naomi Sirkin	Cornell Tech, USA
Akshayaram Srinivasan	Tata Institute of Fundamental Research, India
Noah Stephens-Davidowitz	Cornell University, USA
Marc Stevens	CWI, Netherlands

Ni Trieu	Arizona State University, USA
Yiannis Tselekounis	Carnegie Mellon University, USA
Mayank Varia	Boston University, USA
Xiao Wang	Northwestern University, USA
Daniel Wichs	Northeastern University and NTT Research, USA
David Wu	UT Austin, USA
Shota Yamada	AIST, Japan
Kan Yasuda	NTT Labs, Japan
Kevin Yeo	Google and Columbia University, USA
Eylon Yogev	Bar-Ilan University, Israel
Vassilis Zikas	Purdue University, USA

Additional Reviewers

Masayuki Abe	Mihir Bellare
Calvin Abou Haidar	Adrien Benamira
Anasuya Acharya	Fabrice Benhamouda
Divesh Aggarwal	Huck Bennett
Shashank Agrawal	Ward Beullens
Gorjan Alagic	Tim Beyne
Navid Alamati	Rishabh Bhadauria
Martin R. Albrecht	Amit Singh Bhati
Nicolas Alhaddad	Ritam Bhaumik
Bar Alon	Sai Lakshmi Bhavana Obbattu
Estuardo Alpirez Bock	Jean-Francois Biasse
Jacob Alperin-Shreiff	Alexander Bienstock
Joel Alwen	Nina Bindel
Ghous Amjad	Nir Bitansky
Kazumaro Aoki	Olivier Blazy
Gal Arnon	Alexander Block
Rotem Arnon-Friedman	Xavier Bonnetain
Arasu Arun	Jonathan Bootle
Thomas Attema	Katharina Boudgoust
Benedikt Auerbach	Christina Boura
Christian Badertscher	Pedro Branco
David Balbás	Konstantinos Brazitikos
Marco Baldi	Jacqueline Brendel
Gustavo Banegas	Marek Broll
Fabio Banfi	Chris Brzuska
Laaysa Bangalore	Ileana Buhan
James Bartusek	Benedikt Bunz
Andrea Basso	Bin-Bin Cai
Christof Beierle	Federico Canale
Amos Beimel	Ran Canetti

Ignacio Cascudo
Gaëtan Cassiers
Dario Catalano
Pyrros Chaidos
Suvradip Chakraborty
Jeff Champion
Benjamin Chan
Alishah Chator
Shan Chen
Weikeng Chen
Yilei Chen
Yu Long Chen
Nai-Hui Chia
Lukasz Chmielewski
Chongwon Cho
Arka Rai Choudhuri
Miranda Christ
Chitchanok Chuengsatiansup
Peter Chvojka
Michele Ciampi
Benoît Cogliati
Ran Cohen
Alex Cojocar
Sandro Coretti-Drayton
Arjan Cornelissen
Henry Corrigan-Gibbs
Geoffroy Couteau
Elizabeth Crites
Jan Czajkowski
Joan Daemen
Quang Dao
Pratish Datta
Bernardo David
Nicolas David
Hannah Davis
Koen de Boer
Leo de Castro
Luca De Feo
Gabrielle De Micheli
Jean Paul Degabriele
Patrick Derbez
Jesus Diaz
Jack Doerner
Jelle Don
Jesko Dujmovic

Sebastien Duval
Ted Eaton
Nadia El Mrabet
Reo Eriguchi
Llorenç Escolà Farràs
Daniel Escudero
Saba Eskandarian
Thomas Espitau
Antonio Faonio
Pooya Farshim
Serge Fehr
Peter Fenteany
Rex Fernando
Rune Fiedler
Matthias Fitz
Nils Fleischhacker
Danilo Francati
Cody Freitag
Tommaso Gagliardoni
Chaya Ganesh
Rachit Garg
Lydia Garms
Luke Garratt
Adria Gascon
Romain Gay
Peter Gaži
Nicholas Genise
Marios Georgiou
Koustabh Ghosh
Ashrujit Ghoshal
Barbara Gigerl
Niv Gilboa
Emanuele Giunta
Aarushi Goel
Eli Goldin
Junqing Gong
Jesse Goodman
Lorenzo Grassi
Alex Grilo
Alex Bredariol Grilo
Aditya Gulati
Sam Gunn
Aldo Gunsing
Siyao Guo
Yue Guo

Chun Guo
 Julie Ha
 Ben Hamlin
 Ariel Hamlin
 Abida Haque
 Patrick Harasser
 Ben Harsha
 Eduard Hauck
 Julia Hesse
 Clemens Hlauschek
 Justin Holmgren
 Alexander Hoover
 Kai Hu
 Yuval Ishai
 Muhammad Ishaq
 Takanori Isobe
 Tetsu Iwata
 Hakon Jacobsen
 Aayush Jain
 Ashwin Jha
 Dingding Jia
 Zhengzhong Jin
 Nathan Ju
 Fatih Kaleoglu
 Daniel Kales
 Simon Kamp
 Daniel M. Kane
 Dimitris Karakostas
 Harish Karthikeyan
 Shuichi Katsumata
 Marcel Keller
 Thomas Kerber
 Mustafa Khairallah
 Hamidreza Amini Khorasgani
 Hamidreza Khoshakhlagh
 Dakshita Khurana
 Elena Kirshanova
 Fuyuki Kitagawa
 Susumu Kiyoshima
 Dima Kogan
 Lisa Kohl
 Stefan Kolbl
 Dimitris Kolonelos
 Ilan Komargodski
 Chelsea Komlo
 Yashvanth Kondi
 Venkata Koppula
 Daniel Kuijsters
 Mukul Kulkarni
 Nishant Kumar
 Fukang Liu
 Norman Lahr
 Russell W. F. Lai
 Qiqi Lai
 Baptiste Lambin
 David Lanzenberger
 Philip Lazos
 Seunghoon Lee
 Jooyoung Lee
 Julia Len
 Tancredè Lepoint
 Gaëtan Leurent
 Hanjun Li
 Songsong Li
 Baiyu Li
 Xiao Liang
 Yao-Ting Lin
 Han-Hsuan Lin
 Huijia Lin
 Xiaoyuan Liu
 Meicheng Liu
 Jiahui Liu
 Qipeng Liu
 Zeyu Liu
 Yanyi Liu
 Chen-Da Liu-Zhang
 Alex Lombardi
 Sébastien Lord
 Paul Lou
 Donghang Lu
 George Lu
 Yun Lu
 Reinhard Lüftenegger
 Varun Madathil
 Monosij Maitra
 Giulio Malavolta
 Mary Maller
 Jasleen Malvai
 Nathan Manohar
 Deepak Maram

Lorenzo Martinico
Christian Matt
Sahar Mazloom
Kelsey Melissaris
Nicolas Meloni
Florian Mendel
Rebekah Mercer
Pierre Meyer
Charles Meyer-Hilfiger
Peihan Miao
Brice Minaud
Pratyush Mishra
Tarik Moataz
Victor Mollimard
Andrew Morgan
Tomoyuki Morimae
Travis Morrison
Fabrice Mouhartem
Tamer Mour
Pratyay Mukherjee
Marta Mularczyk
Marcel Nageler
Yusuke Naito
Kohei Nakagawa
Mridul Nandi
Varun Narayanan
Patrick Neumann
Gregory Neven
Samuel Neves
Ngoc Khanh Nguyen
Hai Nguyen
Luca Nizzardo
Ariel Nof
Adam O'Neill
Maciej Obremski
Kazuma Ohara
Miyako Ohkubo
Claudio Orlandi
Michele Orrù
Elisabeth Oswald
Morten Øygarde
Alex Ozdemir
Elena Pagnin
Tapas Pal
Jiaxin Pan

Giorgos Panagiotakos
Omer Paneth
Udaya Parampalli
Anat Paskin-Cherniavsky
Alain Passelègue
Sikhar Patranabis
Chris Peikert
Alice Pellet-Mary
Zachary Pepin
Leo Perrin
Giuseppe Persiano
Edoardo Persichetti
Peter Pessl
Thomas Peters
Stjepan Picek
Maxime Plancon
Bertram Poettering
Christian Porter
Eamonn Postlethwaite
Thomas Prest
Robert Primas
Luowen Qian
Willy Quach
Srinivasan Raghuraman
Samuel Ranellucci
Shahram Rasoolzadeh
Deevashwer Rathee
Mayank Rathee
Divya Ravi
Krijn Reijnders
Doreen Riepel
Peter Rindal
Guilherme Rito
Bhaskar Roberts
Felix Rohrbach
Leah Rosenbloom
Mike Rosulek
Adeline Roux-Langlois
Joe Rowell
Lawrence Roy
Tim Ruffing
Keegan Ryan
Yusuke Sakai
Louis Salvail
Simona Samardjiska

Katerina Samari
Olga Sanina
Amirreza Sarencheh
Pratik Sarkar
Yu Sasaki
Tobias Schmalz
Markus Schofnegger
Peter Scholl
Jan Schoone
Phillipp Schoppmann
André Schrottenloher
Jacob Schuldt
Sven Schäge
Gregor Seiler
Joon Young Seo
Karn Seth
Srinath Setty
Aria Shahverdi
Laura Shea
Yaobin Shen
Emily Shen
Sina Shiehian
Omri Shmueli
Ferdinand Sibleyras
Janno Siim
Jad Silbak
Luisa Siniscalchi
Daniel Slamani
Yifan Song
Min Jae Song
Fang Song
Nicholas Spooner
Lukas Stennes
Igor Stepanovs
Christoph Striecks
Sathya Subramanian
Adam Suhl
George Sullivan
Mehrdad Tahmasbi
Akira Takahashi
Atsushi Takayasu
Abdul Rahman Taleb
Quan Quan Tan
Ewin Tang
Tianxin Tang

Stefano Tessaro
Justin Thaler
Emmanuel Thome
Søren Eller Thomsen
Mehdi Tibouchi
Radu Titiu
Yosuke Todo
Junichi Tomida
Monika Trimoska
Daniel Tschudi
Ida Tucker
Nirvan Tyagi
Rei Ueno
Dominique Unruh
David Urbanik
Wessel van Woerden
Prashant Vasudevan
Serge Vaudenay
Muthu Venkatasubramanian
Damien Vergnaud
Thomas Vidick
Mikhail Volkhov
Satyanarayana Vusirikala
Riad Wahby
Roman Walch
Hendrik Waldner
Michael Walter
Qingju Wang
Han Wang
Haoyang Wang
Mingyuan Wang
Zhedong Wang
Geng Wang
Hoeteck Wee
Shiyi Wei
Mor Weiss
Chenkai Weng
Benjamin Wesolowski
Lichao Wu
Keita Xagawa
Jiayu Xu
Anshu Yadav
Sophia Yakoubov
Takashi Yamakawa
Trevor Yap Hong Eng

Xiuyu Ye
Albert Yu
Thomas Zacharias
Michal Zajac
Hadas Zeilberger

Mark Zhandry
Yupeng Zhang
Cong Zhang
Bingsheng Zhang
Dionysis Zindros

Sponsor Logos



JPMORGAN CHASE & Co.



SUNSCREEN



Western Digital®

Contents – Part IV

Secret Sharing and Secure Multiparty Computation

Sharing Transformation and Dishonest Majority MPC with Packed Secret Sharing	3
<i>Vipul Goyal, Antigoni Polychroniadou, and Yifan Song</i>	
Verifiable Relation Sharing and Multi-verifier Zero-Knowledge in Two Rounds: Trading NIZKs with Honest Majority: (Extended Abstract)	33
<i>Benny Applebaum, Eliran Kachlon, and Arpita Patra</i>	
Authenticated Garbling from Simple Correlations	57
<i>Samuel Dittmer, Yuval Ishai, Steve Lu, and Rafail Ostrovsky</i>	

Unique Topics

Dynamic Local Searchable Symmetric Encryption	91
<i>Brice Minaud and Michael Reichle</i>	
Programmable Distributed Point Functions	121
<i>Elette Boyle, Niv Gilboa, Yuval Ishai, and Victor I. Kolobov</i>	
Snapshot-Oblivious RAMs: Sub-logarithmic Efficiency for Short Transcripts	152
<i>Yang Du, Daniel Genkin, and Paul Grubbs</i>	

Symmetric Key Theory

Tight Preimage Resistance of the Sponge Construction	185
<i>Charlotte Lefevre and Bart Mennink</i>	
Block-Cipher-Based Tree Hashing	205
<i>Aldo Gunsing</i>	
Provably Secure Reflection Ciphers	234
<i>Tim Beyne and Yu Long Chen</i>	
Overloading the Nonce: Rugged PRPs, Nonce-Set AEAD, and Order-Resilient Channels	264
<i>Jean Paul Degabriele and Vukašin Karadžić</i>	

Zero Knowledge

Orion: Zero Knowledge Proof with Linear Prover Time 299
Tiancheng Xie, Yupeng Zhang, and Dawn Song

Moz \mathbb{Z}_{2^k} arella: Efficient Vector-OLE and Zero-Knowledge Proofs over \mathbb{Z}_{2^k} 329
Carsten Baum, Lennart Braun, Alexander Munch-Hansen, and Peter Scholl

Nova: Recursive Zero-Knowledge Arguments from Folding Schemes 359
Abhiram Kothapalli, Srinath Setty, and Ioanna Tzialla

A New Approach to Efficient Non-Malleable Zero-Knowledge 389
Allen Kim, Xiao Liang, and Omkant Pandey

Secure Multiparty Computation III

An Algebraic Framework for Silent Preprocessing with Trustless Setup
 and Active Security 421
Damiano Abram, Ivan Damgård, Claudio Orlandi, and Peter Scholl

Quadratic Multiparty Randomized Encodings Beyond Honest Majority
 and Their Applications 453
Benny Applebaum, Yuval Ishai, Or Karni, and Arpita Patra

Tight Bounds on the Randomness Complexity of Secure Multiparty
 Computation 483
Vipul Goyal, Yuval Ishai, and Yifan Song

Threshold Signatures

Better than Advertised Security for Non-interactive Threshold Signatures 517
Mihir Bellare, Elizabeth Crites, Chelsea Komlo, Mary Maller, Stefano Tessaro, and Chenzhi Zhu

Threshold Signatures with Private Accountability 551
Dan Boneh and Chelsea Komlo

Author Index 583