

Orr Dunkelman  
Stefan Dziembowski (Eds.)

LNCS 13275

# Advances in Cryptology – EUROCRYPT 2022

41st Annual International Conference on the Theory  
and Applications of Cryptographic Techniques  
Trondheim, Norway, May 30 – June 3, 2022, Proceedings, Part I

1  
Part I



 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>


Orr Dunkelman · Stefan Dziembowski (Eds.)

# Advances in Cryptology – EUROCRYPT 2022

41st Annual International Conference on the Theory  
and Applications of Cryptographic Techniques  
Trondheim, Norway, May 30 – June 3, 2022  
Proceedings, Part I

*Editors*

Orr Dunkelman   
University of Haifa  
Haifa, Haifa, Israel

Stefan Dziembowski   
University of Warsaw  
Warsaw, Poland

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-031-06943-7

ISBN 978-3-031-06944-4 (eBook)

<https://doi.org/10.1007/978-3-031-06944-4>

© 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 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Eurocrypt 2022, was held in Trondheim, Norway. Breaking tradition, the conference started on the evening of Monday, May 30, and ended at noon on Friday, June 3, 2022. Eurocrypt is one of the three flagship conferences of the International Association for Cryptologic Research (IACR), which sponsors the event. Colin Boyd (NTNU, Norway) was the general chair of Eurocrypt 2022 who took care of all the local arrangements.

The 372 anonymous submissions we received in the IACR HotCRP system were each reviewed by at least three of the 70 Program Committee members (who were allowed at most two submissions). We used a rebuttal round for all submissions. After a lengthy and thorough review process, 85 submissions were selected for publication. The revised versions of these submissions can be found in these three-volume proceedings.

In addition to these papers, the committee selected the “EpiGRAM: Practical Garbled RAM” by David Heath, Vladimir Kolesnikov, and Rafail Ostrovsky for the best paper award. Two more papers — “On Building Fine-Grained One-Way Functions from Strong Average-Case Hardness” and “Quantum Algorithms for Variants of Average-Case Lattice Problems via Filtering” received an invitation to the Journal of Cryptology. Together with presentations of the 85 accepted papers, the program included two invited talks: The IACR distinguished lecture, carried by Ingrid Verbauwhede, on “Hardware: an essential partner to cryptography”, and “Symmetric Cryptography for Long Term Security” by María Naya-Plasancia.

We would like to take this opportunity to thank numerous people. First of all, the authors of all submitted papers, whether they were accepted or rejected. The Program Committee members who read, commented, and debated the papers generating more than 4,500 comments(!) in addition to a large volume of email communications. The review process also relied on 368 subreviewers (some of which submitted more than one subreview). We cannot thank you all enough for your hard work.

A few individuals were extremely helpful in running the review process. First and foremost, Kevin McCurley, who configured, solved, answered, re-answered, supported, and did all in his (great) power to help with the IACR system. Wkdqn Brx! We are also extremely grateful to Gaëtan Leurent for offering his wonderful tool to make paper assignment an easy task. The wisdom and experience dispensed by Anne Canteaut, Itai Dinur, Bart Preneel, and François-Xavier Standaert are also noteworthy and helped usher the conference into a safe haven. Finally, we wish to thank the area chairs—Sonia Belaïd, Carmit Hazay, Thomas Peyrin, Nigel Smart, and Martijn Stam. You made our work manageable.

Finally, we thank all the people who were involved in the program of Eurocrypt 2022: the rump session chairs, the session chairs, the speakers, and all the technical support staff in Trondheim. We would also like to mention the various sponsors and thank them

for the generous support. We wish to thank the continuous support of the Cryptography Research Fund for supporting student speakers.

May 2022

Orr Dunkelman  
Stefan Dziembowski





Rafael Dowsley	Monash University, Australia
Antonio Faonio	EURECOM, France
Pooya Farshim	Durham University, UK
Sebastian Faust	TU Darmstadt, Germany
Ben Fuller	University of Connecticut, USA
Pierrick Gaudry	Loria, France
Esha Ghosh	Microsoft Research, Redmond, USA
Paul Grubbs	University of Michigan, USA
Divya Gupta	Microsoft Research India, India
Felix Günther	ETH Zurich, Switzerland
Iftach Haitner	Tel Aviv University, Israel
Shai Halevi	Algorand Foundation, USA
Carmit Hazay	Bar-Ilan University, Israel
Pavel Hubáček	Charles University, Czech Republic
Tibor Jager	University of Wuppertal, Germany
Dmitry Khovratovich	Ethereum Foundation, Luxembourg
Gregor Leander	Ruhr University Bochum, Germany
Gaëtan Leurent	Inria, France
Helger Lipmaa	Simula UiB, Norway
Shengli Liu	Shanghai Jiao Tong University, China
Alex Lombardi	Massachusetts Institute of Technology, USA
Hemanta K. Maji	Purdue University, USA
Giulio Malavolta	Max Planck Institute for Security and Privacy, Germany
Peihan Miao	University of Illinois at Chicago, USA
Pratyay Mukherjee	Visa Research, USA
David Naccache	ENS Paris, France
Svetla Nikova	KU Leuven, Belgium
Miyako Ohkubo	National Institute of Information and Communications, Japan
Arpita Patra	Indian Institute of Science, India
Alice Pellet-Mary	CNRS and University of Bordeaux, France
Thomas Peyrin	Nanyang Technological University, Singapore
Josef Pieprzyk	CSIRO Data61, Australia, and Institute of Computer Science, PAS, Poland
Bertram Poettering	IBM Research Europe - Zurich, Switzerland
Peter Rindal	Visa Research, USA
Carla Ràfols	Universitat Pompeu Fabra, Spain
Amin Sakzad	Monash University, Australia
Alessandra Scafuro	North Carolina State University, USA
Nigel Smart	KU Leuven, Belgium
Martijn Stam	Simula UiB, Norway

Meltem Sönmez Turan	National Institute of Standards and Technology, USA
Daniele Venturi	Sapienza University of Rome, Italy
Ivan Visconti	University of Salerno, Italy
Gaoli Wang	East China Normal University, China
Stefan Wolf	University of Italian Switzerland, Switzerland
Sophia Yakoubov	Aarhus University, Denmark
Avishay Yanai	VMware Research, Israel
Bo-Yin Yang	Academia Sinica, Taiwan
Arkady Yerukhimovich	George Washington University, USA
Yu Yu	Shanghai Jiao Tong University, China
Mark Zhandry	NTT Research and Princeton University, USA

## Subreviewers

Behzad Abdolmaleki	Christof Beierle
Ittai Abraham	Pascal Bemmam
Damiano Abram	Fabrice Benhamouda
Anasuya Acharya	Francesco Berti
Alexandre Adomnicai	Tim Beyne
Amit Agarwal	Rishabh Bhadauria
Shweta Agrawal	Adithya Bhat
Thomas Agrikola	Sai Lakshmi Bhavana Obbattu
Akshima	Alexander Bienstock
Navid Alapati	Erica Blum
Alejandro Cabrera Aldaya	Jan Bobolz
Bar Alon	Xavier Bonnetain
Miguel Ambrona	Cecilia Boschini
Hiroaki Anada	Raphael Bost
Diego F. Aranha	Vincenzo Botta
Victor Arribas	Katharina Boudgoust
Tomer Ashur	Christina Boura
Gennaro Avitabile	Zvika Brakerski
Matilda Backendal	Luís Brandão
Saikrishna Badrinarayanan	Lennart Braun
Shi Bai	Jacqueline Brendel
Ero Balsa	Gianluca Brian
Augustin Bariant	Anne Broadbent
James Bartusek	Marek Broll
Balthazar Bauer	Christopher Brzuska
Carsten Baum	Chloe Cachet
Ämin Baumeler	Matteo Campanelli
Arthur Beckers	Federico Canale
Charles Bédard	Anne Canteaut

Ignacio Cascudo  
 Andre Chailloux  
 Nishanth Chandran  
 Donghoon Chang  
 Binyi Chen  
 Shan Chen  
 Weikeng Chen  
 Yilei Chen  
 Jung Hee Cheon  
 Jesus-Javier Chi-Dominguez  
 Seung Geol Choi  
 Wutichai Chongchitmate  
 Arka Rai Choudhuri  
 Sherman S. M. Chow  
 Jeremy Clark  
 Xavier Coiteux-Roy  
 Andrea Coladangelo  
 Nan Cui  
 Benjamin R. Curtis  
 Jan Czajkowski  
 Jan-Pieter D'Anvers  
 Hila Dahari  
 Thinh Dang  
 Quang Dao  
 Poulami Das  
 Pratish Datta  
 Bernardo David  
 Gareth T. Davies  
 Hannah Davis  
 Lauren De Meyer  
 Gabrielle De Micheli  
 Elke De Mulder  
 Luke Demarest  
 Julien Devevey  
 Siemen Dhooghe  
 Denis Diemert  
 Jintai Ding  
 Jack Doerner  
 Xiaoyang Dong  
 Nico Döttling  
 Benjamin Dowling  
 Yang Du  
 Leo Ducas  
 Julien Duman  
 Betul Durak

Oğuzhan Ersoy  
 Andreas Erwig  
 Daniel Escudero  
 Muhammed F. Esgin  
 Saba Eskandarian  
 Prastudy Fauzi  
 Patrick Felke  
 Thibauld Feneuil  
 Peter Fenteany  
 Diodato Ferraioli  
 Marc Fischlin  
 Nils Fleischhacker  
 Cody Freitag  
 Daniele Friolo  
 Tommaso Gagliardoni  
 Steven D. Galbraith  
 Pierre Galissant  
 Chaya Ganesh  
 Cesar Pereida García  
 Romain Gay  
 Kai Gellert  
 Craig Gentry  
 Marilyn George  
 Hossein Ghodosi  
 Satrajit Ghosh  
 Jan Gilcher  
 Aarushi Goel  
 Eli Goldin  
 Junqing Gong  
 Dov Gordon  
 Jérôme Govinden  
 Lorenzo Grassi  
 Johann Großschädl  
 Jiaxin Guan  
 Daniel Guenther  
 Milos Gujic  
 Qian Guo  
 Cyril Guyot  
 Mohammad Hajiabadi  
 Ariel Hamlin  
 Shuai Han  
 Abida Haque  
 Patrick Harasser  
 Dominik Hartmann  
 Phil Hebborn

Alexandra Henzinger  
Javier Herranz  
Julia Hesse  
Justin Holmgren  
Akinori Hosoyamada  
Kai Hu  
Andreas Hülsing  
Shih-Han Hung  
Vincenzo Iovino  
Joseph Jaeger  
Aayush Jain  
Christian Janson  
Samuel Jaques  
Stanislaw Jarecki  
Corentin Jeudy  
Zhengzhong Jin  
Daniel Jost  
Saqib Kakvi  
Vukašin Karadžić  
Angshuman Karmakar  
Shuichi Katsumata  
Jonathan Katz  
Mahimna Kelkar  
Nathan Keller  
John Kelsey  
Mustafa Khairallah  
Hamidreza Amini Khorasgani  
Dongwoo Kim  
Miran Kim  
Elena Kirshanova  
Fuyuki Kitagawa  
Michael Kloob  
Sebastian Kolby  
Lukas Kölsch  
Yashvanth Kondi  
David Kretzler  
Veronika Kuchta  
Marie-Sarah Lacharité  
Yi-Fu Lai  
Baptiste Lambin  
Mario Lorangeira  
Rio LaVigne  
Quoc-Huy Le  
Jooyoung Lee  
Julia Len  
Antonin Leroux  
Hanjun Li  
Jianwei Li  
Yiming Li  
Xiao Liang  
Damien Ligier  
Chengyu Lin  
Dongxi Liu  
Jiahui Liu  
Linsheng Liu  
Qipeng Liu  
Xiangyu Liu  
Chen-Da Liu Zhang  
Julian Loss  
Vadim Lyubashevsky  
Lin Lyu  
You Lyu  
Fermi Ma  
Varun Madathil  
Akash Madhusudan  
Bernardo Magri  
Monosij Maitra  
Nikolaos Makriyannis  
Mary Maller  
Giorgia Marson  
Christian Matt  
Noam Mazor  
Nikolas Melissaris  
Bart Mennink  
Antonis Michalas  
Brice Minaud  
Kazuhiko Minematsu  
Alberto Montina  
Amir Moradi  
Marta Mularczyk  
Varun Narayanan  
Jade Nardi  
Patrick Neumann  
Ruth Ng  
Hai H. Nguyen  
Kirill Nikitin  
Ryo Nishimaki  
Anca Nitulescu  
Ariel Nof  
Julian Nowakowski

Adam O'Neill  
Maciej Obremski  
Eran Omri  
Maximilian Orlt  
Bijeeta Pal  
Jiaxin Pan  
Omer Paneth  
Lorenz Panny  
Dimitrios Papadopoulos  
Jongeun Park  
Anat Paskin-Cherniavsky  
Sikhar Patranabis  
Marcin Pawłowski  
Hilder Pereira  
Ray Perlner  
Clara Pernot  
Léo Perrin  
Giuseppe Persiano  
Edoardo Persichetti  
Albrecht Petzoldt  
Duong Hieu Phan  
Krzysztof Pietrzak  
Jeroen Pijnenburg  
Rachel Player  
Antigoni Polychroniadou  
Willy Quach  
Anaïs Querol  
Srinivasan Raghuraman  
Adrián Ranea  
Simon Rastikian  
Divya Ravi  
Francesco Regazzoni  
Maryam Rezapour  
Mir Ali Rezazadeh Bae  
Siavash Riahi  
Joao Ribeiro  
Vincent Rijmen  
Bhaskar Roberts  
Francisco Rodriguez-Henríquez  
Paul Rösler  
Arnab Roy  
Iftekhar Salam  
Paolo Santini  
Roozbeh Sarenche  
Yu Sasaki

Matteo Scarlata  
Tobias Schmalz  
Mahdi Sedaghat  
Vladimir Sedlacek  
Nicolas Sendrier  
Jae Hong Seo  
Srinath Setty  
Yaobin Shen  
Sina Shiehian  
Omri Shmueli  
Janno Siim  
Jad Silbak  
Leonie Simpson  
Rohit Sinha  
Daniel Slamang  
Fang Song  
Yongsoo Song  
Damien Stehle  
Ron Steinfeld  
Noah Stephens-Davidowitz  
Christoph Striecks  
Fatih Sulak  
Chao Sun  
Ling Sun  
Siwei Sun  
Koutarou Suzuki  
Katsuyuki Takashima  
Hervé Tale Kalachi  
Quan Quan Tan  
Yi Tang  
Je Sen Teh  
Cihangir Tezcan  
Aishwarya Thiruvengadam  
Orfeas Thyfronitis  
Mehdi Tibouchi  
Ni Trieu  
Yiannis Tselekounis  
Michael Tunstall  
Nicola Tuveri  
Nirvan Tyagi  
Sohaib ul Hassan  
Wessel van Woerden  
Kerem Varc  
Prashant Vasudevan  
Damien Vergnaud

Jorge L. Villar  
Giuseppe Vitto  
Sameer Wagh  
Hendrik Waldner  
Alexandre Wallet  
Ming Wan  
Xiao Wang  
Yuyu Wang  
Zhedong Wang  
Hoeteck Wee  
Mor Weiss  
Weiqiang Wen  
Daniel Wicks  
Mathias Wolf  
Lennert Wouters  
Michał Wroński  
David Wu  
Yusai Wu  
Keita Xagawa  
Yu Xia

Zejun Xiang  
Tiancheng Xie  
Shota Yamada  
Takashi Yamakawa  
Lisa Yang  
Kevin Yeo  
Eylon Yogeve  
Kazuki Yoneyama  
Yusuke Yoshida  
William Youmans  
Alexandros Zacharakis  
Michał Zając  
Arantxa Zapico  
Greg Zaverucha  
Shang Zehua  
Tina Zhang  
Wentao Zhang  
Yinuo Zhang  
Yu Zhou  
Cong Zuo

## **Abstracts of Invited Talks**

# Hardware: An Essential Partner to Cryptography

Ingrid Verbauwhede

KU Leuven, Leuven, Belgium

**Abstract.** Cryptography is a beautiful branch of mathematics, its aim being to provide information security. To be useful in practical applications, cryptography is mapped to hardware or software, with software ultimately running also on hardware processors.

This presentation covers multiple aspects of this relation between hardware and cryptography. The goal is to provide insights to the cryptographer, so that more efficient and secure algorithms and protocols are designed.

- Hardware provides the means to accelerate the computationally demanding operations, as is currently the case for the new generation of post-quantum algorithms. [We will illustrate this with some numbers.]
- A very nice aspect of cryptography is that it reduces what needs to be kept secret to the keys, while the algorithms can be publicly known. As a consequence, the hardware is responsible to keep the key(s) secret. Side-channel, fault-attacks and other physical attacks make this a challenging task. [We could show some recent results in fault and laser attacks.] [We can also illustrate this with PUFs to generate secret keys.]
- “Provable Secure” mathematical countermeasures against physical attacks rely on models on how the hardware behaves. Unfortunately, the models are often the weak link between theory and practice and it results in broken implementations. [We will illustrate this with successful attacks on several provably secure masking schemes.]
- Hardware also provides essential building blocks to security. Protocols rely on nonces and freshness from random numbers. Generating full entropy random numbers is a challenge. [We can illustrate this with the challenges of designing TRNGs].
- We will end with some trends in hardware that can benefit cryptography. [We will show tricks on how cheap noise can be generated e.g. for learning with error problems.] [Or how light weight crypto should be adapted to the not-so-perfect random but very light weight random number generators.] [What to do with process variations in deep submicron technologies, or with ultra low-power approximate computing.]

We can conclude that hardware is an essential partner to cryptography to provide the promised information security.



# Symmetric Cryptography for Long Term Security

María Naya-Plasencia

Inria, Paris, France

**Abstract.** Symmetric cryptography has made important advances in recent years, mainly due to new challenges that have appeared, requiring some new developments. During this talk we will discuss these challenges and developments, with a particular emphasis on quantum-safe symmetric cryptography and latest results, providing the details of some particularly interesting cases. We will also discuss some related open problems.

# Contents – Part I

## Best Paper Award

EPIGRAM: Practical Garbled RAM .....	3
<i>David Heath, Vladimir Kolesnikov, and Rafail Ostrovsky</i>	

## Secure Multiparty Computation

Garbled Circuits with Sublinear Evaluator .....	37
<i>Abida Haque, David Heath, Vladimir Kolesnikov, Steve Lu, Rafail Ostrovsky, and Akash Shah</i>	

Round-Optimal and Communication-Efficient Multiparty Computation .....	65
<i>Michele Ciampi, Rafail Ostrovsky, Hendrik Waldner, and Vassilis Zikas</i>	

Round-Optimal Byzantine Agreement .....	96
<i>Diana Ghinea, Vipul Goyal, and Chen-Da Liu-Zhang</i>	

A Complete Characterization of Game-Theoretically Fair, Multi-Party Coin Toss .....	120
<i>Ke Wu, Gilad Asharov, and Elaine Shi</i>	

Lightweight, Maliciously Secure Verifiable Function Secret Sharing .....	150
<i>Leo de Castro and Anitoni Polychroniadou</i>	

Highly Efficient OT-Based Multiplication Protocols .....	180
<i>Iftach Haitner, Nikolaos Makriyannis, Samuel Ranellucci, and Eliad Tsfadia</i>	

Round-Optimal Black-Box Protocol Compilers .....	210
<i>Yuval Ishai, Dakshita Khurana, Amit Sahai, and Akshayaram Srinivasan</i>	

Guaranteed Output in $O(\sqrt{n})$ Rounds for Round-Robin Sampling Protocols ...	241
<i>Ran Cohen, Jack Doerner, Yashvanth Kondi, and Abhi Shelat</i>	

Universally Composable Subversion-Resilient Cryptography .....	272
<i>Suvradip Chakraborty, Bernardo Magri, Jesper Buus Nielsen, and Daniele Venturi</i>	

Asymptotically Quasi-Optimal Cryptography .....	303
<i>Leo de Castro, Carmit Hazay, Yuval Ishai, Vinod Vaikuntanathan, and Muthu Venkitasubramaniam</i>	

Round-Optimal Multi-party Computation with Identifiable Abort .....	335
<i>Michele Ciampi, Divya Ravi, Luisa Siniscalchi, and Hendrik Waldner</i>	
On the Security of ECDSA with Additive Key Derivation and Presignatures ...	365
<i>Jens Groth and Victor Shoup</i>	
Secure Multiparty Computation with Free Branching .....	397
<i>Aarushi Goel, Mathias Hall-Andersen, Aditya Hegde, and Abhishek Jain</i>	
Secure Multiparty Computation with Sublinear Preprocessing .....	427
<i>Elette Boyle, Niv Gilboa, Yuval Ishai, and Ariel Nof</i>	
Practical Non-interactive Publicly Verifiable Secret Sharing with Thousands of Parties .....	458
<i>Craig Gentry, Shai Halevi, and Vadim Lyubashevsky</i>	
<b>Homomorphic Encryption</b>	
Sine Series Approximation of the Mod Function for Bootstrapping of Approximate HE .....	491
<i>Charanjit S. Jutla and Nathan Manohar</i>	
Limits of Polynomial Packings for $\mathbb{Z}_{p^k}$ and $\mathbb{F}_{p^k}$ .....	521
<i>Jung Hee Cheon and Keewoo Lee</i>	
High-Precision Bootstrapping for Approximate Homomorphic Encryption by Error Variance Minimization .....	551
<i>Yongwoo Lee, Joon-Woo Lee, Young-Sik Kim, Yongjune Kim, Jong-Seon No, and HyungChul Kang</i>	
Rubato: Noisy Ciphers for Approximate Homomorphic Encryption .....	581
<i>Jincheol Ha, Seongkwang Kim, Byeonghak Lee, Jooyoung Lee, and Mincheol Son</i>	
Field Instruction Multiple Data .....	611
<i>Khin Mi Mi Aung, Enhui Lim, Jun Jie Sim, Benjamin Hong Meng Tan, Huaxiong Wang, and Sze Ling Yeo</i>	
<b>Obfuscation</b>	
Cryptanalysis of Candidate Obfuscators for Affine Determinant Programs .....	645
<i>Li Yao, Yilei Chen, and Yu Yu</i>	

Indistinguishability Obfuscation from LPN over  $\mathbb{F}_p$ , DLIN, and PRGs  
in  $\text{NC}^0$  ..... 670  
*Aayush Jain, Huijia Lin, and Amit Sahai*

Incompressible Cryptography ..... 700  
*Jiaxin Guan, Daniel Wichs, and Mark Zhandry*

COA-Secure Obfuscation and Applications ..... 731  
*Ran Canetti, Suvradip Chakraborty, Dakshita Khurana,  
Nishant Kumar, Oxana Poburinnaya, and Manoj Prabhakaran*

Unclonable Polymers and Their Cryptographic Applications ..... 759  
*Ghada Almashaqbeh, Ran Canetti, Yaniv Erlich, Jonathan Gershoni,  
Tal Malkin, Itsik Pe'er, Anna Roitburd-Berman, and Eran Tromer*

Distributed (Correlation) Samplers: How to Remove a Trusted Dealer  
in One Round ..... 790  
*Damiano Abram, Peter Scholl, and Sophia Yakoubov*

**Author Index** ..... 821