

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

Gerhard Woeginger 

RWTH Aachen, Aachen, Germany

Moti Yung

Columbia University, New York, NY, USA

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

Anne Canteaut · Yuval Ishai (Eds.)

Advances in Cryptology – EUROCRYPT 2020

39th Annual International Conference on the Theory
and Applications of Cryptographic Techniques
Zagreb, Croatia, May 10–14, 2020
Proceedings, Part III

Editors

Anne Canteaut 
Équipe-projet COSMIQ
Inria
Paris, France

Yuval Ishai
Computer Science Department
Technion
Haifa, Israel

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-45726-6 ISBN 978-3-030-45727-3 (eBook)
<https://doi.org/10.1007/978-3-030-45727-3>

LNCS Sublibrary: SL4 – Security and Cryptology

© International Association for Cryptologic Research 2020

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

Eurocrypt 2020, the 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, was held in Zagreb, Croatia, during May 10–14, 2020.¹ The conference was sponsored by the International Association for Cryptologic Research (IACR). Lejla Batina (Radboud University, The Netherlands) and Stjepan Picek (Delft University of Technology, The Netherlands) were responsible for the local organization. They were supported by a local organizing team consisting of Marin Golub and Domagoj Jakobovic (University of Zagreb, Croatia). Peter Schwabe acted as the affiliated events chair and Simona Samardjiska helped with the promotion and local organization. We are deeply indebted to all of 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. The invited talks and the talks presenting the best paper/best young researcher spanned over both tracks.

We received a total of 375 submissions. Each submission was anonymized for the reviewing process and was assigned to at least three of the 57 Program Committee (PC) members. PC members were allowed to submit at most two papers. The reviewing process included a rebuttal round for all submissions. After extensive deliberations the PC accepted 81 papers. The revised versions of these papers are included in these three volume proceedings, organized topically within their respective track.

The PC decided to give the Best Paper Award to the paper “Optimal Broadcast Encryption from Pairings and LWE” by Shweta Agrawal and Shota Yamada and the Best Young Researcher Award to the paper “Private Information Retrieval with Sublinear Online Time” by Henry Corrigan-Gibbs and Dmitry Kogan. Both papers, together with “Candidate iO from Homomorphic Encryption Schemes” by Zvika Brakerski, Nico Döttling, Sanjam Garg, and Giulio Malavolta, received invitations for the *Journal of Cryptology*.

The program also included invited talks by Alon Rosen, titled “Fine-Grained Cryptography: A New Frontier?”, and by Alice Silverberg, titled “Mathematics and Cryptography: A Marriage of Convenience?”.

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

We are also indebted to the members of the PC and all external reviewers for their voluntary work. The PC work is quite a workload. It has been an honor to work with

¹ This preface was written before the conference took place, under the assumption that it will take place as planned in spite of travel restrictions related to the coronavirus.

everyone. The PC's work was 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 2020. We would also like to thank the many sponsors for their generous support, including the Cryptography Research Fund that supported student speakers.

May 2020

Anne Canteaut
Yuval Ishai

Eurocrypt 2020

The 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques

Sponsored by *the International Association for Cryptologic Research (IACR)*

May 10–14, 2020
Zagreb, Croatia

General Co-chairs

Lejla Batina
Stjepan Picek

Radboud University, The Netherlands
Delft University of Technology, The Netherlands

Program Co-chairs

Anne Canteaut
Yuval Ishai

Inria, France
Technion, Israel

Program Committee

Divesh Aggarwal
Benny Applebaum
Fabrice Benhamouda
Elette Boyle
Zvika Brakerski
Anne Broadbent
Nishanth Chandran
Yilei Chen
Aloni Cohen
Ran Cohen
Geoffroy Couteau
Joan Daemen
Luca De Feo
Léo Ducas
Maria Eichlseder
Thomas Eisenbarth
Thomas Fuhr
Romain Gay
Benedikt Gierlichs
Rishab Goyal

National University of Singapore, Singapore
Tel Aviv University, Israel
Algorand Foundation, USA
IDC Herzliya, Israel
Weizmann Institute of Science, Israel
University of Ottawa, Canada
MSR India, India
Visa Research, USA
Boston University, USA
Boston University and Northeastern University, USA
CNRS, IRIF, Université de Paris, France
Radboud University, The Netherlands
IBM Research Zurich, Switzerland
CWI Amsterdam, The Netherlands
Graz University of Technology, Austria
University of Lübeck and WPI, Germany
ANSSI, France
Cornell Tech, USA
KU Leuven, Belgium
UT Austin, USA

Vipul Goyal	Carnegie Mellon University, USA
Tim Güneysu	Ruhr-Universität Bochum and DFKI, Germany
Jian Guo	Nanyang Technological University, Singapore
Mohammad Hajiabadi	UC Berkeley, USA
Carmit Hazay	Bar-Ilan University, Israel
Susan Hohenberger	Johns Hopkins University, USA
Pavel Hubáček	Charles University Prague, Czech Republic
Abhishek Jain	Johns Hopkins University, USA
Marc Joye	Zama, France
Bhavana Kanukurthi	IISc Bangalore, India
Nathan Keller	Bar-Ilan University, Israel
Susumu Kiyoshima	NTT Research, USA
Eyal Kushilevitz	Technion, Israel
Gregor Leander	Ruhr-Universität Bochum, Germany
Tancrède Lepoint	Google, USA
Tal Malkin	Columbia University, USA
Alexander May	Ruhr-Universität Bochum, Germany
Bart Mennink	Radboud University, The Netherlands
Kazuhiko Minematsu	NEC Corporation, Japan
María Naya-Plasencia	Inria, France
Ryo Nishimaki	NTT Secure Platform Laboratories, Japan
Cécile Pierrot	Inria and Université de Lorraine, France
Sondre Rønjom	University of Bergen, Norway
Ron Rothblum	Technion, Israel
Alessandra Scafuro	North Carolina State University, USA
Peter Schwabe	Radboud University, The Netherlands
Adam Smith	Boston University, USA
François-Xavier Standaert	KU Leuven, Belgium
Yosuke Todo	NTT Secure Platform Laboratories, Japan
Gilles Van Assche	STMicroelectronics, Belgium
Prashant Nalini Vasudevan	UC Berkeley, USA
Muthuramakrishnan Venkitasubramaniam	University of Rochester, USA
Frederik Vercauteren	KU Leuven, Belgium
Damien Vergnaud	Sorbonne Université and Institut Universitaire de France, France
Eylon Yogev	Technion, Israel
Yu Yu	Shanghai Jiao Tong University, China
Gilles Zémor	Université de Bordeaux, France

External Reviewers

Aysajan Abidin
 Ittai Abraham
 Thomas Agrikola
 Navid Alamati
 Nils Albartus
 Martin Albrecht
 Ghada Almashaqbeh
 Joël Alwen
 Miguel Ambrona
 Ghous Amjad
 Nicolas Aragon
 Gilad Asharov
 Tomer Ashur
 Thomas Attema
 Nuttapong Attrapadung
 Daniel Augot
 Florian Bache
 Christian Badertscher
 Saikrishna
 Badrinarayanan
 Shi Bai
 Josep Balasch
 Foteini Baldimtsi
 Marshall Ball
 Zhenzhen Bao
 James Bartusek
 Lejla Batina
 Enkhtaivan Batnyam
 Carsten Baum
 Gabrielle Beck
 Christof Beierle
 Amos Beimel
 Sebastian Berndt
 Dan J. Bernstein
 Francesco Berti
 Ward Beullens
 Rishabh Bhaduria
 Obbattu Sai Lakshmi
 Bhavana
 Jean-Francois Biasse
 Begül Bilgin
 Nina Bindel
 Nir Bitansky

Olivier Blazy
 Naresh Boddu
 Koen de Boer
 Alexandra Boldyreva
 Xavier Bonnetain
 Carl Bootland
 Jonathan Bootle
 Adam Boulund
 Christina Boura
 Tatiana Bradley
 Marek Broll
 Olivier Bronchain
 Ileana Buhan
 Mark Bun
 Sergiu Bursuc
 Benedikt Bünz
 Federico Canale
 Sébastien Canard
 Ran Canetti
 Xavier Caruso
 Ignacio Cascudo
 David Cash
 Gaëtan Cassiers
 Guilhem Castagnos
 Wouter Castryck
 Hervé Chabanne
 André Chailloux
 Avik Chakraborti
 Hubert Chan
 Melissa Chase
 Cong Chen
 Hao Chen
 Jie Chen
 Ming-Shing Chen
 Albert Cheu
 Jérémy Chotard
 Arka Rai Choudhuri
 Kai-Min Chung
 Michele Ciampi
 Benoit Cogliati
 Sandro Coretti-Drayton
 Jean-Sébastien Coron
 Adriana Suarez Corona

Alain Couvreur
 Jan-Pieter D’Anvers
 Bernardo David
 Thomas Decru
 Claire Delaplace
 Patrick Derbez
 Apoorva Deshpande
 Siemen Dhooghe
 Denis Diemert
 Itai Dinur
 Christoph Dobraunig
 Yevgeniy Dodis
 Jack Doerner
 Jelle Don
 Nico Döttling
 Benjamin Dowling
 John Schank
 Markus Duermuth
 Orr Dunkelman
 Frédéric Dupuis
 Iwan Duursma
 Sébastien Duval
 Stefan Dziembowski
 Aner Moshe Ben Efraim
 Naomi Ephraim
 Thomas Espitau
 Andre Esser
 Brett Hemenway Falk
 Antonio Faonio
 Serge Fehr
 Patrick Felke
 Rex Fernando
 Dario Fiore
 Ben Fisch
 Marc Fischlin
 Nils Fleischhacker
 Cody Freitag
 Benjamin Fuller
 Ariel Gabizon
 Philippe Gaborit
 Steven Galbraith
 Chaya Ganesh
 Juan Garay

Rachit Garg	Gabe Kaptchuk	Shengli Liu
Pierrick Gaudry	Martti Karvonen	Tianren Liu
Nicholas Genise	Shuichi Katsumata	Pierre Loidreau
Essam Ghadafi	Raza Ali Kazmi	Alex Lombardi
Satrajit Ghosh	Florian Kerschbaum	Patrick Longa
Kristian Gjøsteen	Dakshita Khurana	Sébastien Lord
Aarushi Goel	Jean Kieffer	Julian Loss
Junqing Gong	Ryo Kikuchi	George Lu
Alonso Gonzalez	Eike Kiltz	Atul Luykx
Lorenzo Grassi	Sam Kim	Vadim Lyubashevsky
Jens Groth	Elena Kirshanova	Fermi Ma
Aurore Guillevic	Fuyuki Kitagawa	Varun Madathil
Berk Gulmezoglu	Dima Kogan	Roel Maes
Aldo Günsing	Lisa Kohl	Bernardo Magri
Chun Guo	Markulf Kohlweiss	Saeed Mahloujifar
Qian Guo	Ilan Komargodski	Christian Majenz
Siyao Guo	Yashvanth Kondi	Eleftheria Makri
Shai Halevi	Venkata Koppula	Giulio Malavolta
Shuai Han	Lucas Kowalczyk	Mary Maller
Abida Haque	Karel Kral	Alex Malozemoff
Phil Hebborn	Ralf Küesters	Nathan Manohar
Brett Hemenway	Ashutosh Kumar	Daniel Masny
Shoichi Hirose	Ranjit Kumaresan	Simon Masson
Dennis Hofheinz	Srijita Kundu	Takahiro Matsuda
Justin Holmgren	Peter Kutas	Noam Mazor
Akinori Hosoyamada	Thijs Laarhoven	Audra McMillan
Senyang Huang	Gijs Van Laer	Lauren De Meyer
Paul Huynh	Russell Lai	Peihan Miao
Kathrin Hövelmanns	Virginie Lallemand	Gabrielle De Micheli
Andreas Hülsing	Baptiste Lambin	Ian Miers
Iliia Iliashenko	Julien Lavauzelle	Brice Minaud
Laurent Imbert	Phi Hung Le	Pratyush Mishra
Takanori Isobe	Eysa Lee	Ahmad Moghimi
Tetsu Iwata	Hyung Tae Lee	Esfandiar Mohammadi
Håkon Jacobsen	Jooyoung Lee	Victor Mollimard
Tibor Jager	Antonin Leroux	Amir Moradi
Aayush Jain	Gaëtan Leurent	Tal Moran
Samuel Jaques	Xin Li	Andrew Morgan
Jérémy Jean	Xiao Liang	Mathilde de la Morinerie
Yanxue Jia	Chengyu Lin	Nicky Mouha
Zhengzhong Jin	Huijia (Rachel) Lin	Tamer Mour
Thomas Johansson	Wei-Kai Lin	Pratyay Mukherjee
Kimmo Järvinen	Eik List	Marta Mularczyk
Saqib Kakvi	Guozhen Liu	Koksal Mus
Daniel Kales	Jiahui Liu	Pierrick Méaux
Seny Kamara	Qipeng Liu	Jörn Müller-Quade

Yusuke Naito
 Mridul Nandi
 Samuel Neves
 Ngoc Khanh Nguyen
 Anca Nitulescu
 Ariel Nof
 Sai Lakshmi Bhavana
 Obbattu
 Maciej Obremski
 Tobias Oder
 Frédérique Oggier
 Miyako Ohkubo
 Mateus de Oliveira
 Oliveira
 Tron Omland
 Maximilian Orlt
 Michele Orrù
 Emmanuela Orsini
 Morten Øygarden
 Ferruh Ozbudak
 Carles Padro
 Aurel Page
 Jiaxin Pan
 Omer Paneth
 Lorenz Panny
 Anat Paskin-Cherniavsky
 Alain Passelègue
 Sikhar Patranabis
 Michaël Peeters
 Chris Peikert
 Alice Pellet-Mary
 Olivier Pereira
 Léo Perrin
 Edoardo Persichetti
 Thomas Peters
 George Petrides
 Thi Minh Phuong Pham
 Duong-Hieu Phan
 Krzysztof Pietrzak
 Oxana Poburinnaya
 Supartha Podder
 Bertram Poettering
 Antagoni Polychroniadou
 Claudius Pott
 Bart Preneel
 Robert Primas

Luowen Qian
 Willy Quach
 Ahmadreza Rahimi
 Somindu Ramannai
 Matthieu Rambaud
 Hugues Randriam
 Shahram Rasoolzadeh
 Divya Ravi
 Mariana P. Raykova
 Christian Rechberger
 Ling Ren
 Joost Renes
 Leonid Reyzin
 Joao Ribeiro
 Silas Richelson
 Peter Rindal
 Francisco
 Rodríguez-Henríquez
 Schuyler Rosefield
 Mélissa Rossi
 Mike Rosulek
 Dragos Rotaru
 Lior Rotem
 Arnab Roy
 Paul Rösler
 Reihaneh Safavi-Naini
 Amin Sakzad
 Simona Samardjiska
 Antonio Sanso
 Yu Sasaki
 Pascal Sasdrich
 Or Sattath
 John Schanck
 Sarah Scheffler
 Tobias Schneider
 Markus Schofnegger
 Peter Scholl
 Jan Schoone
 André Schrottenloher
 Sven Schäge
 Adam Sealfon
 Jean-Pierre Seifert
 Gregor Seiler
 Sruthi Sekar
 Okan Seker
 Karn Seth

Yannick Seurin
 Ido Shahaf
 Ronen Shaltiel
 Barak Shani
 Sina Shiehian
 Omri Shmueli
 Jad Silbak
 Thierry Simon
 Luisa Sinischalchi
 Veronika Slivova
 Benjamin Smith
 Yifan Song
 Pratik Soni
 Jessica Sorrell
 Nicholas Spooner
 Akshayaram Srinivasan
 Damien Stehlé
 Ron Steinfeld
 Noah
 Stephens-Davidowitz
 Martin Strand
 Shifeng Sun
 Ridwan Syed
 Katsuyuki Takashima
 Titouan Tanguy
 Stefano Tessaro
 Enrico Thomae
 Jean-Pierre Tillich
 Benjamin Timon
 Junichi Tomida
 Deniz Toz
 Rotem Tsabary
 Daniel Tschudi
 Yiannis Tselekounis
 Yi Tu
 Dominique Unruh
 Bogdan Ursu
 Vinod Vaikuntanathan
 Kerem Varici
 Philip Vejre
 Marloes Venema
 Daniele Venturi
 Fernando Virdia
 Vanessa Vitse
 Damian Vizár
 Chrysoula Vlachou

Mikhail Volkhov
Satyanarayana Vusirikala
Hendrik Waldner
Alexandre Wallet
Michael Walter
Haoyang Wang
Meiqin Wang
Weijia Wang
Xiao Wang
Yohei Watanabe
Hoeteck Wee
Mor Weiss
Weiqiang Wen
Benjamin Wesolowski
Jan Wichelmann
Daniel Wicks

Friedrich Wiemer
Christopher Williamson
Jonas Wloka
Wessel van Woerden
Lennert Wouters
David J. Wu
Shai Wyborski
Brecht Wyseur
Keita Xagawa
Xiang Xie
Chaoping Xing
Sophia Yakoubov
Shota Yamada
Takashi Yamakawa
Avishay Yanai
Kang Yang

Kevin Yeo
Arkady Yerukhimovich
Øyvind Ytrehus
Aaram Yun
Mohammad Zaheri
Mark Zhandry
Jiayu Zhang
Liangfeng Zhang
Ren Zhang
Zhenfei Zhang
Zhongxiang Zheng
Hong-Sheng Zhou
Vassilis Zikas
Giorgos Zirdelis
Vincent Zucca

Contents – Part III

Asymmetric Cryptanalysis

<i>(One) Failure Is Not an Option: Bootstrapping the Search for Failures in Lattice-Based Encryption Schemes</i>	<i>3</i>
<i>Jan-Pieter D’Anvers, Mélissa Rossi, and Fernando Virdia</i>	
<i>Key Recovery from Gram–Schmidt Norm Leakage in Hash-and-Sign Signatures over NTRU Lattices.</i>	<i>34</i>
<i>Pierre-Alain Fouque, Paul Kirchner, Mehdi Tibouchi, Alexandre Wallet, and Yang Yu</i>	
<i>An Algebraic Attack on Rank Metric Code-Based Cryptosystems</i>	<i>64</i>
<i>Magali Bardet, Pierre Briaud, Maxime Bros, Philippe Gaborit, Vincent Neiger, Olivier Ruatta, and Jean-Pierre Tillich</i>	
<i>Low Weight Discrete Logarithm and Subset Sum in $2^{0.65n}$ with Polynomial Memory.</i>	<i>94</i>
<i>Andre Esser and Alexander May</i>	

Verifiable Delay Functions

<i>Continuous Verifiable Delay Functions</i>	<i>125</i>
<i>Naomi Ephraim, Cody Freitag, Ilan Komargodski, and Rafael Pass</i>	
<i>Generic-Group Delay Functions Require Hidden-Order Groups.</i>	<i>155</i>
<i>Lior Rotem, Gil Segev, and Ido Shahaf</i>	

Signatures

<i>Sigma Protocols for MQ, PKP and SIS, and Fishy Signature Schemes.</i>	<i>183</i>
<i>Ward Beullens</i>	
<i>Signatures from Sequential-OR Proofs</i>	<i>212</i>
<i>Marc Fischlin, Patrick Harasser, and Christian Janson</i>	

Attribute-Based Encryption

<i>Compact Adaptively Secure ABE from k-Lin: Beyond NC^1 and Towards NL.</i>	<i>247</i>
<i>Huijia Lin and Ji Luo</i>	

Adaptively Secure ABE for DFA from k -Lin and More	278
<i>Junqing Gong and Hoeteck Wee</i>	

Side-Channel Security

Tornado: Automatic Generation of Probing-Secure Masked Bitsliced Implementations	311
<i>Sonia Belaïd, Pierre-Évariste Dagand, Darius Mercadier, Matthieu Rivain, and Raphaël Wintersdorff</i>	

Side-Channel Masking with Pseudo-Random Generator	342
<i>Jean-Sébastien Coron, Aurélien Greuet, and Rina Zeitoun</i>	

Non-Interactive Zero-Knowledge

Compact NIZKs from Standard Assumptions on Bilinear Maps	379
<i>Shuichi Katsumata, Ryo Nishimaki, Shota Yamada, and Takashi Yamakawa</i>	

New Constructions of Statistical NIZKs: Dual-Mode DV-NIZKs and More	410
<i>Benoît Libert, Alain Passelègue, Hoeteck Wee, and David J. Wu</i>	

Non-interactive Zero-Knowledge in Pairing-Free Groups from Weaker Assumptions	442
<i>Geoffroy Couteau, Shuichi Katsumata, and Bogdan Ursu</i>	

Public-Key Encryption

Everybody's a Target: Scalability in Public-Key Encryption	475
<i>Benedikt Auerbach, Federico Giacon, and Eike Kiltz</i>	

Security Under Message-Derived Keys: Signcryption in iMessage	507
<i>Mihir Bellare and Igors Stepanovs</i>	

Double-Base Chains for Scalar Multiplications on Elliptic Curves	538
<i>Wei Yu, Saud Al Musa, and Bao Li</i>	

Zero-Knowledge

Stacked Garbling for Disjunctive Zero-Knowledge Proofs	569
<i>David Heath and Vladimir Kolesnikov</i>	

Which Languages Have 4-Round Fully Black-Box Zero-Knowledge Arguments from One-Way Functions?	599
<i>Carmit Hazay, Rafael Pass, and Muthuramakrishnan Venkatasubramanian</i>	

Statistical ZAPR Arguments from Bilinear Maps.	620
<i>Alex Lombardi, Vinod Vaikuntanathan, and Daniel Wichs</i>	
Statistical ZAP Arguments	642
<i>Saikrishna Badrinarayanan, Rex Fernando, Aayush Jain, Dakshita Khurana, and Amit Sahai</i>	
Statistical Zaps and New Oblivious Transfer Protocols.	668
<i>Vipul Goyal, Abhishek Jain, Zhengzhong Jin, and Giulio Malavolta</i>	
Quantum II	
Measure-Rewind-Measure: Tighter Quantum Random Oracle Model Proofs for One-Way to Hiding and CCA Security	703
<i>Veronika Kuchta, Amin Sakzad, Damien Stehlé, Ron Steinfeld, and Shi-Feng Sun</i>	
Secure Multi-party Quantum Computation with a Dishonest Majority	729
<i>Yfke Dulek, Alex B. Grilo, Stacey Jeffery, Christian Majenz, and Christian Schaffner</i>	
Efficient Simulation of Random States and Random Unitaries	759
<i>Gorjan Alagic, Christian Majenz, and Alexander Russell</i>	
Quantum-Access-Secure Message Authentication via Blind-Unforgeability . . .	788
<i>Gorjan Alagic, Christian Majenz, Alexander Russell, and Fang Song</i>	
Author Index	819