Preface

EUROCRYPT 2001, the twentieth annual Eurocrypt conference, was sponsored by the IACR, the International Association for Cryptologic Research, see `http://www.iacr.org/`, this year in cooperation with the Austrian Computer Society (OCG). The General Chair, Reinhard Posch, was responsible for local organization, and registration was handled by the IACR Secretariat at the University of California, Santa Barbara.

In addition to the papers contained in these proceedings, we were pleased that the conference program also included the presentation by the 2001 IACR distinguished lecturer, Andrew Odlyzko, on "Economics and Cryptography" and an invited talk by Silvio Micali, "Zero Knowledge Has Come of Age." Furthermore, there was the rump session for presentations of recent results and other (possibly satirical) topics of interest to the crypto community, which Jean-Jacques Quisquater kindly agreed to run.

The Program Committee received 155 submissions and selected 33 papers for presentation; one of them was withdrawn by the authors. The review process was therefore a delicate and challenging task for the committee members, and I wish to thank them for all the effort they spent on it. Each committee member was responsible for the review of at least 20 submissions, so that each paper was carefully evaluated by at least three reviewers, and submissions with a program committee member as a (co-)author by at least six. Final decisions, after intensive web discussions, were taken at a one-day face-to-face meeting of the committee. The selection was based on originality, quality, and relevance to cryptology. In most cases, the reviewers provided extensive comments to the authors. Subsequently, the authors have made a substantial effort to take these comments into account. I was pleased to see that the field was continuing to flourish and believe that we were able to select a varied and high-quality program, and wish to thank all the authors who submitted papers, thus making such a choice possible, and those of accepted papers for their cooperation in timely producing revised versions.

Many thanks also go to the additional colleagues who reviewed submissions in their area of expertise: Joy Algesheimer, Seigo Arita, Giuseppe Ateniese, Olivier Baudron, Charles Bennett, Dan Boneh, Annalisa De Bonis, Wieb Bosma, Marco Bucci, Ran Canetti, Anne Canteaut, Suresh Chari, Philippe Chose, Christophe Clavier, Scott Contini, Don Coppersmith, Jean-Sébastien Coron, Ronald Cramer, Nora Dabbous, Ivan Damgård, Giovanni Di Crescenzo, Markus Dichtl, Yevgeniy Dodis, Paul Dumais, Serge Fehr, Marc Fischlin, Roger Fischlin, Matthias Fitzi, Pierre-Alain Fouque, Jun Furukawa, Pierre Girard, Clemente Gladi, Daniel Gottesman, Clemens Holenstein, Rosario Gennaro, Nick Howgrave-Graham, James Hughes, Yuval Ishai, Markus Jakobsson, Eliane Jaulmes, Antoine Joux, Olaf Keller, Ki Hyoung Ko, Reto Kohlas, Takeshi Koshiba, Eyal Kushilevitz, Yehuda Lindell, Helger Lipmaa, Anna Lysyanskaya, Subhamoy

Maitra, Tal Malkin, Daniel Mall, Barbara Masucci, Dominic Mayers, Alfred Menezes, Renato Menicocci, Daniele Micciancio, Markus Michels, Miodrag Mihaljevic, Phong Nguyen, Svetla Nikova, Satoshi Obana, Kazuo Ohta, Pino Persiano, David Pointcheval, Bartosz Przydatek, Michael Quisquater, Omer Reingold, Leonid Reyzin, Jean-Marc Robert, Pankaj Rohatgi, Alon Rosen, Ludovic Rousseau, Daniel Simon, Nigel Smart, Adam Smith, Othmar Staffelbach, Martijn Stam, Michael Steiner, Katsuyuki Takashima, Alain Tapp, Christophe Tymen, Shigenori Uchiyama, Frédéric Valette, Ramarathnam Venkatesan, Eric Verheul, Stefan Wolf, Akihiro Yamamura, Yuliang Zheng. I apologize for any inadvertent omissions.

The review process was greatly simplified by submission software written by Mihir Bellare and Chanathip Namprempre for Crypto 2000, and review software developed for Eurocrypt 2000 by Bart Preneel, Wim Moreau and Joris Claessens.

I am very grateful to André Adelsbach. Skillfully and patiently, he carried the main load of background work of the Program Chair role, in particular setting up the submission and review servers, providing technical help to the authors and committee members, and the preparation of these proceedings. I would also like to thank Michael Steiner and Martin Wanke for technical support, Matthias Schunter for organizing the program committee meeting, and Mihir Bellare and Michael Waidner for advice.

March 2001

Birgit Pfitzmann
Program Chair

EUROCRYPT 2001

May 6 – 10, 2001, Innsbruck (Tyrol), Austria

Sponsored by the
International Association for Cryptologic Research (IACR)
in cooperation with the
Austrian Computer Society (OCG)

General Chair

Reinhard Posch, Institute for Applied Information Processing and Communications (IAIK), Austria

Program Chair

Birgit Pfitzmann, Saarland University, Saarbrücken, Germany

Program Committee

Josh Benaloh ..... Microsoft Research, USA
Carlo Blundo ..... Università di Salerno, Italy
Jan Camenisch ..... IBM Zürich Research Laboratory, Switzerland
Matt Franklin ..... UC Davis, USA
Shai Halevi ..... IBM T. J. Watson Research Center, USA
Martin Hirt ..... ETH Zürich, Switzerland
Thomas Johansson ..... Lund University, Sweden
Neal Koblitz ..... Univ. of Washington, USA
Hugo Krawcyk ..... Technion, Israel
Kaoru Kurosawa ..... Tokyo Institute of Technology, Japan
Arjen Lenstra ..... Citicorp, USA
Willi Meier ..... Fachhochschule Aargau, Switzerland
David Naccache ..... Gemplus, France
Kaisa Nyberg ..... Nokia, Finland
Torben Pryds Pedersen ..... Cryptomathic, Denmark
Guillaume Poupard ..... DCSSI Crypto Lab, France
Tal Rabin ..... IBM T. J. Watson Research Center, USA
Vincent Rijmen ..... K. U. Leuven, Belgium
Amit Sahai ..... Princeton University, USA
Kazue Sako ..... NEC, Japan
Louis Salvail ..... BRICS, University of Århus, Denmark
Claus-Peter Schnorr ..... University of Frankfurt, Germany
David Wagner ..... UC Berkeley, USA
Michael Waidner ..... IBM Zürich Research Laboratory, Switzerland

Table of Contents

Elliptic Curves

A Memory Efficient Version of Satoh's Algorithm 1
Frederik Vercauteren (K. U. Leuven, Belgium)
Bart Preneel (K. U. Leuven, Belgium)
Joos Vandewalle (K. U. Leuven, Belgium)

Finding Secure Curves with the Satoh-FGH Algorithm and an Early-Abort Strategy 14
Mireille Fouquet (LIX, École polytechnique, France)
Pierrick Gaudry (LIX, École polytechnique, France)
Robert Harley (ArgoTech, France)

How Secure are Elliptic Curves over Composite Extension Fields? 30
Nigel P. Smart (University of Bristol, UK)

Commitments

Efficient and Non-Interactive Non-Malleable Commitment 40
Giovanni Di Crescenzo (Telcordia Technologies Inc., USA)
Jonathan Katz (Telcordia Technologies Inc. and Columbia University, USA)
Rafail Ostrovsky (Telcordia Technologies Inc., USA)
Adam Smith (Massachusetts Institute of Technology, USA)

How to Convert the Flavor of a Quantum Bit Commitment 60
Claude Crépeau (McGill University, Canada)
Frédéric Légaré (Zero-Knowledge Systems Inc., Canada)
Louis Salvail (BRICS, University of Århus, Denmark)

Anonymity

Cryptographic Counters and Applications to Electronic Voting 78
Jonathan Katz (Telcordia Technologies Inc. and Columbia University, USA)
Steven Myers (University of Toronto, Canada)
Rafail Ostrovsky (Telcordia Technologies Inc., USA)

An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation 93
Jan Camenisch (IBM Zürich Research Laboratory, Switzerland)
Anna Lysyanskaya (Massachusetts Institute of Technology, USA)

Priced Oblivious Transfer: How to Sell Digital Goods 118
Bill Aiello (AT&T Labs – Research, USA)
Yuval Ishai (DIMACS and AT&T Labs – Research, USA)
Omer Reingold (AT&T Labs – Research, USA)

Signatures and Hash Functions

A Secure Three-move Blind Signature Scheme for Polynomially Many Signatures 135
Masayuki ABE (NTT Laboratories, Japan)

Practical Threshold RSA Signatures Without a Trusted Dealer 151
Ivan Damgård (BRICS, University of Århus, Denmark)
Maciej Koprowski (BRICS, University of Århus, Denmark)

Hash Functions: From Merkle-Damgård to Shoup 165
Ilya Mironov (Stanford University, USA)

XTR and NTRU

Key Recovery and Message Attacks on NTRU-Composite 181
Craig Gentry (DoCoMo Communications Laboratories Inc., USA)

Evidence that XTR is more Secure than Supersingular Elliptic Curve Cryptosystems 194
Eric R. Verheul (PricewaterhouseCoopers, The Netherlands)

NSS: An NTRU Lattice-Based Signature Scheme 210
Jeffrey Hoffstein (NTRU Cryptosystems Inc., USA)
Jill Pipher (NTRU Cryptosystems Inc., USA)
Joseph H. Silverman (NTRU Cryptosystems Inc., USA)

Assumptions

The Bit Security of Paillier's Encryption Scheme and its Applications 228
Dario Catalano (University of Catania, Italy)
Rosario Gennaro (IBM T. J. Watson Research Center, USA)
Nick Howgrave-Graham (IBM T. J. Watson Research Center, USA)

Assumptions Related to Discrete Logarithms: Why Subtleties Make a Real Difference 243
Ahmad-Reza Sadeghi (Saarland University, Germany)
Michael Steiner (Saarland University, Germany)

Multiparty Protocols

On Adaptive vs. Non-adaptive Security of Multiparty Protocols 261
Ran Canetti (IBM T. J. Watson Research Center, USA)
Ivan Damgård (BRICS, University of Århus, Denmark)
Stefan Dziembowski (BRICS, University of Århus, Denmark)
Yuval Ishai (DIMACS and AT&T Labs – Research, USA)
Tal Malkin (AT&T Labs – Research, USA)

Multiparty Computation from Threshold Homomorphic Encryption 279
Ronald Cramer (BRICS, University of Århus, Denmark)
Ivan Damgård (BRICS, University of Århus, Denmark)
Jesper B. Nielsen (BRICS, University of Århus, Denmark)

On Perfect and Adaptive Security in Exposure-Resilient Cryptography 299
Yevgeniy Dodis (University of New York, USA)
Amit Sahai (Princeton University, USA)
Adam Smith (Massachusetts Institute of Technology, USA)

Block Ciphers

Cryptanalysis of Reduced-Round MISTY 323
Ulrich Kühn (Dresdner Bank AG, Germany)

The Rectangle Attack – Rectangling the Serpent 338
Eli Biham (Technion, Israel)
Orr Dunkelman (Technion, Israel)
Nathan Keller (Technion, Israel)

Primitives

Efficient Amplification of the Security of Weak Pseudo-Random Function Generators 356
Steven Myers (University of Toronto, Canada)

Min-Round Resettable Zero-Knowledge in the Public-Key Model 371
Silvio Micali (Massachusetts Institute of Technology, USA)
Leonid Reyzin (Massachusetts Institute of Technology, USA)

Symmetric Ciphers

Structural Cryptanalysis of SASAS 392
Alex Biryukov (The Weizmann Institute, Israel)
Adi Shamir (The Weizmann Institute, Israel)

Hyper-Bent Functions 404
Amr M. Youssef (University of Waterloo, Canada)
Guang Gong (University of Waterloo, Canada)

New Method for Upper Bounding the Maximum Average Linear Hull Probability for SPNs 418
Liam Keliher (Queen's University at Kingston, Canada)
Henk Meijer (Queen's University at Kingston, Canada)
Stafford Tavares (Queen's University at Kingston, Canada)

Key Exchange and Multicast

Lower Bounds for Multicast Message Authentication 435
Dan Boneh (Stanford University, USA)
Glenn Durfee (Stanford University, USA)
Matt Franklin (University of California, USA)

Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels 451
Ran Canetti (IBM T. J. Watson Research Center, USA)
Hugo Krawczyk (Technion, Israel)

Efficient Password-Authenticated Key Exchange Using Human-Memorable Passwords 473
Jonathan Katz (Telcordia Technologies Inc. and Columbia University, USA)
Rafail Ostrovsky (Telcordia Technologies Inc., USA)
Moti Yung (CertCo Inc., USA)

Authentication and Identification

Identification Protocols Secure Against Reset Attacks 493
Mihir Bellare (University of California at San Diego, USA)
Marc Fischlin (University of Frankfurt, Germany)
Shafi Goldwasser (Massachusetts Institute of Technology, USA)
Silvio Micali (Massachusetts Institute of Technology, USA)

Does Encryption with Redundancy Provide Authenticity? 509
Jee Hea An (University of California at San Diego, USA)
Mihir Bellare (University of California at San Diego, USA)

Encryption Modes with Almost Free Message Integrity 525
Charanjit S. Jutla (IBM T. J. Watson Research Center, USA)

Author Index 543

A Memory Efficient Version of Satoh's Algorithm

Frederik Vercauteren, Bart Preneel, and Joos Vandewalle

K.U. Leuven, Dept. Elektrotechniek-ESAT/COSIC, Kasteelpark Arenberg 10,
B-3001 Leuven-Heverlee, Belgium.
{Frederik.Vercauteren, Bart.Preneel, Joos.Vandewalle}@esat.kuleuven.ac.be

Finding Secure Curves with the Satoh-FGH Algorithm and an Early-Abort Strategy

Mireille Fouquet[1], Pierrick Gaudry[1], and Robert Harley[2]

[1] LIX, École polytechnique, 91128 Palaiseau Cedex, France
[2] ArgoTech, 26 ter rue Nicolaï, 75012 Paris, France

How Secure are Elliptic Curves over Composite Extension Fields?

N.P. Smart

Dept. Computer Science,
University of Bristol,
Merchant Venturers Building,
Woodland Road,
Bristol, BS8 1UB
nigel@cs.bris.ac.uk

Efficient and Non-Interactive Non-Malleable Commitment

Giovanni Di Crescenzo[1], Jonathan Katz[2], Rafail Ostrovsky[1], and Adam Smith[3]

[1] Telcordia Technologies, Inc.
{giovanni,rafail}@research.telcordia.com
[2] Telcordia Technologies and
Department of Computer Science, Columbia University.
jkatz@cs.columbia.edu
[3] Laboratory for Computer Science, MIT.
Work done while the author was at Telcordia Technologies.
asmith@theory.lcs.mit.edu

How to Convert the Flavor of a Quantum Bit Commitment

Claude Crépeau[1], Frédéric Légaré[2], and Louis Salvail[3]

[1] School of Computer Science, McGill University[†], crepeau@cs.mcgill.ca
[2] ZKLabs[‡], Zero-Knowledge Systems Inc., frederic@zeroknowledge.com
[3] BRICS[§], Dept. of Computer Science, University of Århus, salvail@brics.dk

[†] Part of this research was funded by Québec's Fonds FCAR and Canada's NSERC.
[‡] This research was done as part of the M.Sc. requirements at McGill University.
[§] Basic Research in Computer Science (www.brics.dk), funded by the Danish National Research Foundation.

Cryptographic Counters and Applications to Electronic Voting

Jonathan Katz[1], Steven Myers[2], and Rafail Ostrovsky[3]

[1] Telcordia Technologies and
Department of Computer Science, Columbia University.
jkatz@cs.columbia.edu
[2] Department of Computer Science, University of Toronto.
Work done while the author was at Telcordia Technologies.
myers@cs.toronto.edu
[3] Telcordia Technologies, Inc., 445 South Street, Morristown, NJ 07960.
rafail@research.telcordia.com

An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation

Jan Camenisch
IBM Research
Zurich Research Laboratory
CH–8803 Rüschlikon
jca@zurich.ibm.com

Anna Lysyanskaya*
MIT LCS
545 Technology Square
Cambridge, MA 02139 USA
anna@theory.lcs.mit.edu

* This research was carried out while the author was visiting IBM Zürich Research Laboratory.

Priced Oblivious Transfer: How to Sell Digital Goods

Bill Aiello, Yuval Ishai, and Omer Reingold

No Institute Given

A Secure Three-move Blind Signature Scheme for Polynomially Many Signatures

Masayuki ABE

NTT Laboratories. 1-1 Hikari-no-oka, Yokosuka-shi, 239-0847 JAPAN
abe@isl.ntt.co.jp

Practical Threshold RSA Signatures Without a Trusted Dealer

Ivan Damgård and Maciej Koprowski

BRICS*, Aarhus University

* Basic Research in Computer Science,
Centre of the Danish National Research Foundation.

Hash Functions: From Merkle-Damgård to Shoup

Ilya Mironov

Computer Science Department, Stanford University, Stanford, CA 94305mironov@cs.stanford.edu

Key Recovery and Message Attacks on NTRU-Composite

Craig Gentry

DoCoMo Communications Laboratories USA, Inc.
181 Metro Dr., San Jose, CA 95110, USA cgentry@dcl.docomo-usa.com

Evidence that XTR is more Secure than Supersingular Elliptic Curve Cryptosystems

Eric R. Verheul

PricewaterhouseCoopers, GRMS Crypto group, P.O. Box 85096, 3508 AB Utrecht, The Netherlands, eric.verheul@[nl.pwcglobal.com, pobox.com]

NSS: An NTRU Lattice-Based Signature Scheme

Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman

NTRU Cryptosystems, Inc., 5 Burlington Woods, Burlington, MA 01803 USA,
jhoff@ntru.com, jpipher@ntru.com, jhs@ntru.com

The Bit Security of Paillier's Encryption Scheme and its Applications

Dario Catalano[1], Rosario Gennaro[2], and Nick Howgrave-Graham[2]

[1] Dipartimento di Matematica e Informatica
Università di Catania. Viale A. Doria 6, 95125 Catania.
Email: catalano@dmi.unict.it.
[2] IBM T.J.Watson Research Center
PO Box 704, Yorktown Heights, New York 10598, USA.
Email: {rosario,nahg}@watson.ibm.com

Assumptions Related to Discrete Logarithms: Why Subtleties Make a Real Difference

Ahmad-Reza Sadeghi and Michael Steiner

No Institute Given

On Adaptive vs. Non-adaptive Security of Multiparty Protocols

Ran Canetti, Ivan Damgård, Stefan Dziembowski, Yuval Ishai, and Tal Malkin

No Institute Given

Multiparty Computation from Threshold Homomorphic Encryption

Ronald Cramer, Ivan Damgård, and Jesper B. Nielsen

BRICS[⋆] Department of Computer Science
University of Aarhus
Ny Munkegade
DK-8000 Arhus C, Denmark
{cramer,ivan,buus}@brics.dk

⋆ Basic Research in Computer Science,
Centre of the Danish National Research Foundation.

On Perfect and Adaptive Security in Exposure-Resilient Cryptography

Yevgeniy Dodis[1], Amit Sahai[2], and Adam Smith[3]

[1] Department of Computer Science, New York University, 251 Mercer St, New York, NY 10012, USA. dodis@cs.nyu.edu
[2] Department of Computer Science, Princeton University, 35 Olden St, Princeton, NJ 08540, USA. sahai@cs.princeton.edu
[3] Laboratory for Computer Science, Massachusetts Institute of Technology, 545 Main St, Cambridge, MA 02139, USA. asmith@theory.lcs.mit.edu

Cryptanalysis of Reduced-Round MISTY

Ulrich Kühn

Dresdner Bank AG
Group Information Technology
RS Research
D-60301 Frankfurt
Germany
Ulrich.Kuehn@dresdner-bank.com

The Rectangle Attack – Rectangling the Serpent

Eli Biham, Orr Dunkelman, and Nathan Keller

No Institute Given

Efficient Amplification of the Security of Weak Pseudo-Random Function Generators

Steven Myers

myers@cs.toronto.edu
Department of Computer Science
University of Toronto
Toronto, Ontario, Canada

Min-Round Resettable Zero-Knowledge in the Public-Key Model

Silvio Micali and Leonid Reyzin

Laboratory for Computer Science
Massachusetts Institute of Technology
Cambridge, MA 02139
reyzin@theory.lcs.mit.edu
http://theory.lcs.mit.edu/~reyzin

Structural Cryptanalysis of SASAS

Alex Biryukov and Adi Shamir

Computer Science department
The Weizmann Institute
Rehovot 76100, Israel.

Hyper-Bent Functions

A. M. Youssef and G. Gong

Center for Applied Cryptographic Research
[1]Department of Combinatorics & Optimization
[2]Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, Ontario N2L 3G1, CANADA
{a2youssef,ggong}@cacr.math.uwaterloo.ca

New Method for Upper Bounding the Maximum Average Linear Hull Probability for SPNs

Liam Keliher[1], Henk Meijer[1], and Stafford Tavares[2]

[1] Department of Computing and Information Science
Queen's University at Kingston, Ontario, Canada, K7L 3N6
{keliher,henk}@cs.queensu.ca
[2] Department of Electrical and Computer Engineering
Queen's University at Kingston, Ontario, Canada, K7L 3N6
tavares@ee.queensu.ca

Lower Bounds for Multicast Message Authentication

Dan Boneh[1], Glenn Durfee[1], and Matt Franklin[2]

[1] Computer Science Department, Stanford University, Stanford CA 94305-9045
{dabo,gdurf}@cs.stanford.edu
[2] Department of Computer Science, University of California, Davis CA 95616-8562
franklin@cs.ucdavis.edu

Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels

Ran Canetti and Hugo Krawczyk

No Institute Given

Efficient Password-Authenticated Key Exchange Using Human-Memorable Passwords

Jonathan Katz[1], Rafail Ostrovsky[2], and Moti Yung[3]

[1] Telcordia Technologies and
Department of Computer Science, Columbia University.
jkatz@cs.columbia.edu
[2] Telcordia Technologies, Inc., 445 South Street, Morristown, NJ 07960.
rafail@research.telcordia.com
[3] CertCo, Inc.
moti@cs.columbia.edu

Identification Protocols Secure Against Reset Attacks

Mihir Bellare[1], Marc Fischlin[2], Shafi Goldwasser[3], and Silvio Micali[3]

[1] Dept. of Computer Science & Engineering, University of California at San Diego, 9500 Gilman Drive, La Jolla, California 92093, USA.
E-mail: mihir@cs.ucsd.edu.
URL: www-cse.ucsd.edu/users/mihir.
[2] Dept. of Mathematics (AG 7.2), Johann Wolfgang Goethe-University, Postfach 111932, 60054 Frankfurt/Main, Germany.
E-mail: marc@mi.informatik.uni-frankfurt.de
URL: www.mi.informatik.uni-frankfurt.de
[3] MIT Laboratory for Computer Science, 545 Technology Square, Cambridge MA 02139, USA.

Does Encryption with Redundancy Provide Authenticity?

Jee Hea An and Mihir Bellare

Dept. of Computer Science & Engineering, University of California at San Diego,
9500 Gilman Drive, La Jolla, California 92093, USA.
E-mails: {jeehea, mihir}@cs.ucsd.edu.
URLs: www-cse.ucsd.edu/users/{jeehea, mihir}.

Encryption Modes with Almost Free Message Integrity

Charanjit S. Jutla

IBM T. J. Watson Research Center,
Yorktown Heights, NY 10598-704

Author Index

ABE, Masayuki 135
Aiello, Bill 118
An, Jee Hea 509

Bellare, Mihir 493, 509
Biham, Eli 338
Biryukov, Alex 392
Boneh, Dan 435

Camenisch, Jan 93
Canetti, Ran 261, 451
Catalano, Dario 228
Crépeau, Claude 60
Cramer, Ronald 279

Damgård, Ivan 151, 261, 279
Di Crescenzo, Giovanni 40
Dodis, Yevgeniy 299
Dunkelman, Orr 338
Durfee, Glenn 435
Dziembowski, Stefan 261

Fischlin, Marc 493
Fouquet, Mireille 14
Franklin, Matt 435

Gaudry, Pierrick 14
Gennaro, Rosario 228
Gentry, Craig 181
Goldwasser, Shafi 493
Gong, Guang 404

Harley, Robert 14
Hoffstein, Jeffrey 210
Howgrave-Graham, Nick 228

Ishai, Yuval 118, 261

Jutla, Charanjit S. 525

Kühn, Ulrich 323
Katz, Jonathan 40, 78, 473
Keliher, Liam 418
Keller, Nathan 338
Koprowski, Maciej 151
Krawczyk, Hugo 451

Légaré, Frédéric 60
Lysyanskaya, Anna 93

Malkin, Tal 261
Meijer, Henk 418
Micali, Silvio 371, 493
Mironov, Ilya 165
Myers, Steven 78, 356

Nielsen, Jesper B. 279

Ostrovsky, Rafail 40, 78, 473

Pipher, Jill 210
Preneel, Bart 1

Reingold, Omer 118
Reyzin, Leonid 371

Sadeghi, Ahmad-Reza 243
Sahai, Amit 299
Salvail, Louis 60
Shamir, Adi 392
Silverman, Joseph H. 210
Smart, Nigel P. 30
Smith, Adam 40, 299
Steiner, Michael 243

Tavares, Stafford 418

Vandewalle, Joos 1
Vercauteren, Frederik 1
Verheul, Eric R. 194

Youssef, Amr M. 404
Yung, Moti 473