GUIDE

Table of Contents

Preface

Program Committee

Other Reviewers

Preface

Crypto 2000 is the Twentieth Annual Crypto conference. It is sponsored by the International Association for Cryptologic Research (IACR) in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy and the Computer Science Department of the University of California at Santa Barbara.

The conference received 120 submissions, and the program committee selected 32 of these for presentation. Extended abstracts of revised versions of these papers are in these proceedings. The authors bear full responsibility for the contents of their papers.

The conference program includes two invited lectures. Don Coppersmith's presentation "The development of DES" records his involvement with one of the most important cryptographic developments ever, namely the Data Encryption Standard, and is particularly apt given the imminent selection of the Advanced Encryption Standard. Martín Abadi's presentation "Taming the Adversary" is about bridging the gap between useful but perhaps simplistic threat abstractions and rigorous adversarial models, or perhaps, even more generally, between viewpoints of the security and cryptography communities. An abstract corresponding to Martín's talk is included in these proceedings.

The conference program also includes its traditional "rump session" of short, informal or impromptu presentations, chaired this time by Stuart Haber. These presentations are not reflected in these proceedings.

An electronic submission process was available and recommended, but for the first time used a web interface rather than email. (Perhaps as a result, there were no hardcopy submissions.) The submission review process had three phases. In the first phase, program committee members compiled reports (assisted at their discretion by sub-referees of their choice, but without interaction with other program committee members) and entered them, via web forms, into web-review software running at UCSD. In the second phase, committee members used the software to browse each other's reports, discuss, and update their own reports. Lastly there was a program committee meeting to discuss the difficult cases.

I am extremely grateful to the program committee members for their enormous investment of time, effort and adrenaline in the difficult and delicate process of review and selection. (A list of program committee members and subreferees they invoked can be found in succeeding pages of this volume.) I also thank the authors of submitted papers —in equal measure regardless of whether their papers were accepted or not— for their submissions. It is the work of this body of researchers that makes this conference possible.

I thank Rebecca Wright for hosting the program committee meeting at the AT&T building in New York City and managing the local arrangements, and Ran Canetti for organizing the post-PC-meeting dinner with his characteristic gastronomic and oenophilic flair.

The web-review software we used was written for Eurocrypt 2000 by Wim Moreau and Joris Claessens under the direction of Eurocrypt 2000 program chair Bart Preneel, and I thank them for allowing us to deploy their useful and colorful tool.

I am most grateful to Chanathip Namprempre (aka. Meaw) who provided systems, logistical and moral support for the entire Crypto 2000 process. She wrote the software for the web-based submissions, adapted and ran the web-review software at UCSD, and compiled the final abstracts into the proceedings you see here. She types faster than I speak.

I am grateful to Hugo Krawczyk for his insight and advice, provided over a long period of time with his usual combination of honesty and charm, and to him and other past program committee chairs, most notably Michael Wiener and Bart Preneel, for replies to the host of questions I posed during the process. In addition I received useful advice from many members of our community including Silvio Micali, Tal Rabin, Ron Rivest, Phil Rogaway and Adi Shamir. Finally thanks to Matt Franklin who as general chair was in charge of the local organization and finances, and, on the IACR side, to Christian Cachin, Kevin McCurley, and Paul Van Oorschot.

Chairing a Crypto program committee is a learning process. I have come to appreciate even more than before the quality and variety of work in our field, and I hope the papers in this volume contribute further to its development.

Mihir Bellare

Program Chair, Crypto 2000
San Diego, June 2000

CRYPTO 2000

August 20–24,2000, Santa Barbara, California, USA

Sponsored by the
International Association for Cryptologic Research (IACR)

in cooperation with
IEEE Computer Society Technical Committee on Security and Privacy,
Computer Science Department, University of California, Santa Barbara

General Chair
Matthew Franklin, Xerox Palo Alto Research Center, USA

Program Chair
Mihir Bellare, University of California, San Diego, USA

Program Committee

Alex Biryukov ..... Weizmann Institute of Science, Israel
Dan Boneh ..... Stanford University, USA
Christian Cachin ..... IBM Research, Switzerland
Ran Canetti ..... IBM Research, USA
Ronald Cramer ..... ETH Zurich, Switzerland
Yair Frankel ..... CertCo, USA
Shai Halevi ..... IBM Research, USA
Arjen Lenstra ..... Citibank, USA
Mitsuru Matsui ..... Mitsubishi Electric Corporation, Japan
Paul Van Oorschot ..... Entrust Technologies, Canada
Bart Preneel ..... Katholieke Universiteit Leuven, Belgium
Phillip Rogaway ..... University of California, Davis, USA
Victor Shoup ..... IBM Zurich, Switzerland
Jessica Staddon ..... Bell Labs Research, Palo Alto, USA
Jacques Stern ..... Ecole Normale Supérieure, France
Doug Stinson ..... University of Waterloo, Canada
Salil Vadhan ..... Massachusetts Institute of Technology, USA
David Wagner ..... University of California, Berkeley, USA
Rebecca Wright ..... AT&T Laboratories Research, USA

Advisory members

Michael Wiener (Crypto 1999 program chair) .. Entrust Technologies, Canada
Joe Kilian (Crypto 2001 program chair) ..... Intermemory, USA

Sub-Referees

Bill Aiello, Jeehea An, Olivier Baudron, Don Beaver, Josh Benaloh, John Black, Simon Blackburn, Alexandra Boldyreva, Nikita Borisov, Victor Boyko, Jan Camenisch, Suresh Chari, Scott Contini, Don Coppersmith, Claude Crépeau, Ivan Damgård, Anand Desai , Giovanni Di Crescenzo, Yevgeniy Dodis, Matthias Fitzi, Matt Franklin, Rosario Gennaro, Guang Gong, Luis Granboulan, Nick Howgrave-Graham, Russell Impagliazzo, Yuval Ishai, Markus Jakobsson, Stas Jarecki, Thomas Johansson, Charanjit Jutla, Joe Kilian, Eyal Kushilevitz, Moses Liskov, Stefan Lucks, Anna Lysyanskaya, Philip MacKenzie, Subhamoy Maitra, Tal Malkin, Barbara Masucci, Alfred Menezes, Daniele Micciancio, Sara Miner, Ilia Mironov, Moni Naor , Phong Nguyen, Rafail Ostrovsky, Erez Petrank, Birgit Pfitzmann, Benny Pinkas, David Pointcheval, Guillaume Poupard, Tal Rabin, Charlie Rackoff, Zulfikar Ramzan, Omer Reingold, Leo Reyzin, Pankaj Rohatgi, Amit Sahai, Louis Salvail, Claus Schnorr, Mike Semanko, Bob Silverman, Joe Silverman, Dan Simon, Nigel Smart, Ben Smeets, Adam Smith, Martin Strauss, Ganesh Sundaram, Serge Vaudenay, Frederik Vercauteren, Bernhard von Stengel, Ruizhong Wei, Susanne Gudrun Wetzel, Colin Williams, Stefan Wolf, Felix Wu, Yiqun Lisa Yin, Amir Youssef, Robert Zuccherato

Table of Contents

XTR and NTRU

The XTR public key system 21
Arjen K. Lenstra, Eric R. Verheul

A Chosen-Ciphertext Attack against NTRU 37
Éliane Jaulmes, Antoine Joux

Privacy for databases

Privacy Preserving Data Mining 38
Yehuda Lindell, Benny Pinkas

Reducing the Servers Computation in Private Information Retrieval: PIR with Preprocessing 56
Amos Beimel, Yuval Ishai, Tal Malkin

Secure distributed computation and applications

Parallel Reducibility for Information-Theoretically Secure Computation . . . 75
Christian Cachin, Jan Camenisch

Optimistic Fair Secure Computation 94
Christian Cachin, Jan Camenisch

A Cryptographic Solution to a Game Theoretic Problem 113
Yevgeniy Dodis, Shai Halevi, Tal Rabin

Algebraic cryptosystems

Differential Fault Attacks on Elliptic Curve Cryptosystems 131
Ingrid Biehl, Bernd Meyer, Volker Müller

Quantum Public-Key Cryptosystems 166
Tatsuaki Okamoto, Keisuke Tanaka, Shigenori Uchiyama

New Public-key Cryptosystem Using Braid Groups 184
Ki Hyoung Ko, Sang Jin Lee, Jung Hee Cheon, Jae Woo Han, Ju-sung Kang, Choonsik Park

Message authentication

Key recovery and forgery attacks on the MacDES MAC algorithm 197
Don Coppersmith, Lars R. Knudsen, Chris J. Mitchell

CBC MACs for Arbitrary-Length Messages: The Three-Key Constructions 216
John Black, Phillip Rogaway

L-collision Attacks against Randomized MACs 229
Michael Semanko

Digital signatures

On the exact security of Full Domain Hash 237
Jean-Sébastien Coron

Timed Commitments 256
Dan Boneh, Moni Naor

A Practical and Provably Secure Coalition-Resistant Group Signature Scheme 272
Giuseppe Ateniese, Jan Camenisch, Marc Joye, Gene Tsudik

Provably Secure Partially Blind Signatures 288
Masayuki Abe and Tatsuaki Okamoto

Cryptanalysis

Weaknesses in the $SL_2(\mathbb{F}_{2^n})$ Hashing Scheme of Tillich and Zémor 302
Rainer Steinwandt, Markus Grassl, Willi Geiselmann, Thomas Beth

Fast Correlation Attacks Through Reconstruction of Linear Polynomials . 318
Thomas Johansson and Fredrik Jönsson

Traitor tracing and broadcast encryption

Sequential Traitor Tracing 335
Reihaneh Safavi-Naini and Yejing Wang

Long-Lived Broadcast Encryption 354
Juan A. Garay, Jessica Staddon, Avishai Wool

Invited talk

Taming the Adversary 360
Martín Abadi

Symmetric encryption

The Security of All-Or-Nothing Encryption: Protecting Against Exhaustive Key Search 377
Anand Desai

On the Round Security of Symmetric-Key Cryptographic Primitives 395
Zulfikar Ramzan, Leonid Reyzin

New Paradigms for Constructing Symmetric Encryption Schemes Secure Against Chosen-Ciphertext Attack 414
Anand Desai

To Commit or not to Commit

Efficient Non-Malleable Commitment Schemes 433
Marc Fischlin and Roger Fischlin

Improved Non-Committing Encryption Schemes based on a General Complexity Assumption 452
Ivan Damgård, Jesper Buus Nielsen

Protocols

A note on the round-complexity of Concurrent Zero-Knowledge 470
Alon Rosen

An Improved Pseudo-Random Generator Based on Discrete Log 483
Rosario Gennaro

Linking Classical and Quantum Key Agreement: Is There "Bound Information"? 502
Nicolas Gisin, Stefan Wolf

Stream ciphers and boolean functions

Maximum Correlation Analysis of Nonlinear S-boxes in Stream Ciphers . . . 516
Muxiang Zhang, Agnes Chan

Nonlinearity Bounds and Constructions of Resilient Boolean Functions . . . 534
Palash Sarkar, Subhamoy Maitra

Almost Independent and Weakly Biased Arrays: Efficient Constructions and Cryptologic Applications 546
Jürgen Bierbrauer, Holger Schellwat

Author Index 546

The XTR public key system

Arjen K. Lenstra[1], Eric R. Verheul[2]

[1] Citibank, N.A., 1 North Gate Road, Mendham, NJ 07945-3104, U.S.A.,
arjen.lenstra@citicorp.com
[2] PricewaterhouseCoopers, GRMS Crypto Group, Goudsbloemstraat 14, 5644 KE Eindhoven, The Netherlands,
Eric.Verheul@[nl.pwcglobal.com, pobox.com]

A Chosen-Ciphertext Attack against NTRU

Éliane Jaulmes[1] and Antoine Joux[2]

[1] SCSSI, 18 rue du Docteur Zamenhof
F-92131 Issy-les-Moulineaux cedex, France
eliane.jaulmes@wanadoo.fr
[2] SCSSI, 18 rue du Docteur Zamenhof
F-92131 Issy-les-Moulineaux cedex, France
Antoine.Joux@ens.fr

Privacy Preserving Data Mining

Yehuda Lindell[1] and Benny Pinkas[2⋆]

[1] Department of Computer Science and Applied Math, Weizmann Institute of Science, Rehovot, Israel. lindell@wisdom.weizmann.ac.il
[2] School of Computer Science and Engineering, Hebrew University of Jerusalem, Jerusalem, Israel. bpinkas@cs.huji.ac.il

⋆ Supported by an Eshkol grant of the Israel Ministry of Science.

Reducing the Servers Computation in Private Information Retrieval: PIR with Preprocessing

Amos Beimel[1], Yuval Ishai[2], and Tal Malkin[3]

[1] Dept. of Computer Science, Ben-Gurion University, Beer-Sheva 84105, Israel. beimel@cs.bgu.ac.il.
[2] DIMACS and AT&T Labs – Research, USA. yuval@dimacs.rutgers.edu.
[3] AT&T Labs – Research, 180 Park Ave., Florham Park, NJ 07932, USA. tal@research.att.com.

Parallel Reducibility for Information-Theoretically Secure Computation

Christian Cachin and Jan Camenisch

IBM Research, Zurich Research Laboratory
CH-8803 Rüschlikon, Switzerland
{cca,jca}@zurich.ibm.com

Optimistic Fair Secure Computation

Christian Cachin and Jan Camenisch

IBM Research, Zurich Research Laboratory
CH-8803 Rüschlikon, Switzerland
{cca,jca}@zurich.ibm.com

A Cryptographic Solution to a Game Theoretic Problem

Yevgeniy Dodis[1], Shai Halevi[2], and Tal Rabin[2]

[1] Laboratory for Computer Science, MIT, 545 Tech Square, Cambridge, MA 02139, USA. Email: yevgen@theory.lcs.mit.edu.
[2] IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, New York 10598, USA. Email: {shaih,talr}@watson.ibm.com.

Differential Fault Attacks on Elliptic Curve Cryptosystems

Ingrid Biehl[1], Bernd Meyer[2], and Volker Müller[3]

[1] University of Technology, Computer Science Department, Alexanderstraße 10, 64283 Darmstadt, Germany, Email: biehl@informatik.tu-darmstadt.de

[2] Siemens AG, Corporate Technology, 81730 München, Germany, Email: bernd.meyer@mchp.siemens.de

[3] Universitas Kristen Duta Wacana, Jl. Dr. Wahidin 5–19, Yogyakarta 55224, Indonesia, Email: vmueller@ukdw.ac.id

Quantum Public-Key Cryptosystems

Tatsuaki Okamoto, Keisuke Tanaka, and Shigenori Uchiyama

NTT Laboratories
1-1 Hikari-no-oka Yokosuka-shi, Kanagawa-ken 239-0847, Japan
{okamoto, keisuke, uchiyama}@isl.ntt.co.jp
Tel: +81-468-59-2511
Fax: +81-468-59-3858

New Public-key Cryptosystem Using Braid Groups

Ki Hyoung Ko[1], Sang Jin Lee[1], Jung Hee Cheon[2],
Jae Woo Han[3], Ju-sung Kang[3], and Choonsik Park[3]

[1] Department of Mathematics, Korea Advanced Institute of Science and Technology,
Taejon, 305-701, Korea
{knot,sjlee}@knot.kaist.ac.kr
[2] Department of Mathematics, Brown university, Providence, RI 02912, USA
and Securepia, Korea
jhcheon@math.brown.edu
[3] Section 8100, Electronics and Telecommunications Research Institute,
Taejon, 305-600, Korea
{jwhan,jskang,csp}@etri.re.kr

Key recovery and forgery attacks on the MacDES MAC algorithm

Don Coppersmith[1], Lars R. Knudsen[2], and Chris J. Mitchell[3]

[1] IBM Research, T.J. Watson Research Center, Yorktown Heights, NY 10598, USA
copper@watson.ibm.com
[2] Department of Informatics, University of Bergen, N-5020, Bergen, Norway
lars.knudsen@ii.uib.no, http://www.ii.uib.no/∼larsr
[3] Information Security Group, Royal Holloway, University of London, Egham, Surrey TW20 0EX, UK
c.mitchell@rhbnc.ac.uk, http://isg.rhbnc.ac.uk/cjm

CBC MACs for Arbitrary-Length Messages: The Three-Key Constructions

John Black[1] and Phillip Rogaway[2]

[1] Dept. of Computer Science, University of Nevada, Reno NV 89557, USA, blackj@cs.ucdavis.edu

[2] Dept. of Computer Science, University of California at Davis, Davis, CA 95616, USA, rogaway@cs.ucdavis.edu, WWW home page: http://www.cs.ucdavis.edu/~rogaway

L-collision Attacks against Randomized MACs

Michael Semanko

Department of Computer Science & Engineering,
University of California at San Diego,
9500 Gilman Drive,
La Jolla, California 92093, USA.
msemanko@cs.ucsd.edu

On the exact security of Full Domain Hash

Jean-Sébastien Coron

Ecole Normale Supérieure
Gemplus Card International
45 rue d'Ulm
34 rue Guynemer
Paris, F-75230, France
Issy-les-Moulineaux, F-92447, France
coron@clipper.ens.fr

Timed Commitments

Dan Boneh[1] and Moni Naor[2]

[1] Stanford University, dabo@cs.stanford.edu
[2] Weizmann institute, naor@wisdom.weizmann.ac.il

A Practical and Provably Secure Coalition-Resistant Group Signature Scheme

Giuseppe Ateniese[1], Jan Camenisch[2], Marc Joye[3], and Gene Tsudik[4]

[1] Department of Computer Science, The Johns Hopkins University
3400 North Charles Street, Baltimore, MD 21218, USA
ateniese@cs.jhu.edu
[2] IBM Research, Zurich Research Laboratory
Säumertrasse 4, CH-8803 Rüschlikon, Switzerland
jca@zurich.ibm.com
[3] Gemplus Card International, Card Security Group
Parc d'Activités de Gémenos, B.P. 100, F-13881 Gémenos, France
marc.joye@gemplus.com
[4] Department of Information and Computer Science,
University of California, Irvine, Irvine, CA 92697-3425, USA
gts@ics.uci.edu

Provably Secure Partially Blind Signatures

Masayuki Abe and Tatsuaki Okamoto

NTT Laboratories
Nippon Telegraph and Telephone Corporation
1-1 Hikari-no-oka Yokosuka-shi Kanagawa-ken, 239-0847 Japan
E-mail: {abe,okamoto}@isl.ntt.co.jp

Weaknesses in the $\mathrm{SL}_2(\mathbb{F}_{2^n})$ Hashing Scheme of Tillich and Zémor

Rainer Steinwandt, Markus Grassl, Willi Geiselmann, and Thomas Beth

Institut für Algorithmen und Kognitive Systeme,
Fakultät für Informatik, Universität Karlsruhe,
Am Fasanengarten 5, 76 128 Karlsruhe, Germany,
{steinwan,grassl,geiselma,EISS_Office}@ira.uka.de.

Fast Correlation Attacks Through Reconstruction of Linear Polynomials

Thomas Johansson and Fredrik Jönsson

Dept. of Information Technology
Lund University, P.O. Box 118, 221 00 Lund, Sweden
{thomas, fredrikj}@it.lth.se

Sequential Traitor Tracing

Reihaneh Safavi-Naini and Yejing Wang

School of IT and CS, University of Wollongong,
Wollongong 2522, Australia
email: [rei/yw17]@uow.edu.au

Long-Lived Broadcast Encryption

Juan A. Garay[1], Jessica Staddon[2], and Avishai Wool[1]

[1] Bell Labs, 600 Mountain Ave., Murray Hill, NJ 07974, USA.
E-mail: {garay,yash}@research.bell-labs.com.
[2] Bell Labs Research Silicon Valley, 3180 Porter Drive, Palo Alto, CA 94304, USA.
E-mail: staddon@research.bell-labs.com.

Taming the Adversary

Martín Abadi

Bell Labs Research, Lucent Technologies
abadi@lucent.com
www.pa.bell-labs.com/~abadi

The Security of All-Or-Nothing Encryption: Protecting Against Exhaustive Key Search

Anand Desai

Department of Computer Science & Engineering,
University of California at San Diego,
9500 Gilman Drive, La Jolla, California 92093, USA.
adesai@cs.ucsd.edu

On the Round Security of Symmetric-Key Cryptographic Primitives

Zulfikar Ramzan and Leonid Reyzin

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

New Paradigms for Constructing Symmetric Encryption Schemes Secure Against Chosen-Ciphertext Attack

Anand Desai

Department of Computer Science & Engineering,
University of California at San Diego,
9500 Gilman Drive, La Jolla, California 92093, USA.
adesai@cs.ucsd.edu

Efficient Non-Malleable Commitment Schemes

Marc Fischlin and Roger Fischlin

Fachbereich Mathematik (AG 7.2)
Johann Wolfgang Goethe-Universität Frankfurt am Main
Postfach 111932
D–60054 Frankfurt/Main, Germany

{marc,fischlin}@mi.informatik.uni-frankfurt.de
http://www.mi.informatik.uni-frankfurt.de/

Improved Non-Committing Encryption Schemes based on a General Complexity Assumption

Ivan Damgård and Jesper Buus Nielsen

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

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

A note on the round-complexity of Concurrent Zero-Knowledge

Alon Rosen

Department of Computer Science
Weizmann Institute of Science
Rehovot 76100, Israel
alon@wisdom.weizmann.ac.il

An Improved Pseudo-Random Generator Based on Discrete Log

Rosario Gennaro

IBM T.J.Watson Research Center, P.O. Box 704, Yorktown Heights, NY 10598,
rosario@watson.ibm.com

Linking Classical and Quantum Key Agreement: Is There "Bound Information"?

Nicolas Gisin[1] and Stefan Wolf[2]

[1] Group of Applied Physics, University of Geneva, CH-1211 Geneva, Switzerland.
E-mail: Nicolas.Gisin@physics.unige.ch
[2] Department of Computer Science, ETH Zürich, CH-8092 Zürich, Switzerland.
E-mail: wolf@inf.ethz.ch

Maximum Correlation Analysis of Nonlinear S-boxes in Stream Ciphers

Muxiang Zhang[1] and Agnes Chan[2]

[1] GTE Laboratories Inc., 40 Sylvan Road LA0MS59, Waltham, MA 02451
mzhang@gte.com
[2] College of Computer Science, Northeastern University, Boston, MA 02115
ahchan@ccs.neu.edu

Nonlinearity Bounds and Constructions of Resilient Boolean Functions

Palash Sarkar[1] and Subhamoy Maitra[2]

[1] Applied Statistics Unit, Indian Statistical Institute,
203, B T Road, Calcutta 700 035, INDIA
palash@isical.ac.in
[2] Computer and Statistical Service Center, Indian Statistical Institute,
203, B T Road, Calcutta 700 035, INDIA
subho@isical.ac.in

Almost Independent and Weakly Biased Arrays: Efficient Constructions and Cryptologic Applications

Jürgen Bierbrauer[1] and Holger Schellwat[2]

[1] Department of Mathematical Sciences, Michigan Technological University, Houghton, Michigan 49931, USA
jbierbra@mtu.edu
[2] Department of Natural Sciences, Örebro University, SE-70182 Örebro, Sweden
holger.schellwat@nat.oru.se

Author Index

Abadi, Martín 354
Abe, Masayuki 272
Ateniese, Giuseppe 256

Beimel, Amos 56
Beth, Thomas 288
Biehl, Ingrid 131
Bierbrauer, Jürgen 534
Black, John 197
Boneh, Dan 237

Cachin, Christian 94
Camenisch, Jan 94, 256
Chan, Agnes 502
Cheon, Jung Hee 166
Coppersmith, Don 184
Coron, Jean-Sébastien 229

Damgård, Ivan 433
Desai, Anand 360, 395
Dodis, Yevgeniy 75, 113

Fischlin, Marc 414
Fischlin, Roger 414

Garay, Juan A. 335
Geiselmann, Willi 288
Gennaro, Rosario 470
Gisin, Nicolas 483
Grassl, Markus 288

Halevi, Shai 113
Han, Jae Woo 166

Ishai, Yuval 56

Jönsson, Fredrik 302
Jaulmes, Éliane 21
Johansson, Thomas 302
Joux, Antoine 21
Joye, Marc 256

Kang, Ju-sung 166
Knudsen, Lars R. 184
Ko, Ki Hyoung 166

Lee, Sang Jin 166
Lenstra, Arjen 1
Lindell, Yehuda 37

Müller, Volker 131
Maitra, Subhamoy 516
Malkin, Tal 56
Meyer, Bernd 131
Micali, Silvio 75
Mitchell, Chris J. 184

Naor, Moni 237
Nielsen, Jesper Buus 433

Okamoto, Tatsuaki 147, 272

Park, Choonsik 166

Pinkas, Benny 37

Rabin, Tal 113
Ramzan, Zulfikar 377
Reyzin, Leonid 377
Rogaway, Phillip 197
Rosen, Alon 452

Safavi-Naini, Reihaneh 318
Sarkar, Palash 516
Schellwat, Holger 534
Semanko, Michael 216
Staddon, Jessica 335
Steinwandt, Rainer 288

Tanaka, Keisuke 147
Tsudik, Gene 256

Uchiyama, Shigenori 147

Verheul, Eric R. 1

Wang, Yejing 318
Wolf, Stefan 483
Wool, Avishai 335

Zhang, Muxiang 502